Panduan Pengguna

AWS Control Tower

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

AWS Control Tower: Panduan Pengguna

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

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

Table of Contents

Apa itu Menara Kontrol AWS? 1
Fitur 1
Cara AWS Control Tower berinteraksi dengan yang lain AWS layanan 2
Apakah Anda First-Time Pengguna Menara Kontrol AWS? 3
Cara kerjanya 3
Struktur AWS Control Tower Landing Zone 4
Apa yang terjadi ketika Anda mengatur landing zone 4
Apa saja akun bersama? 6
Bagaimana kontrol bekerja 7
Cara AWS Control Tower bekerja dengan StackSets 7
Terminologi 9
Harga 13
Pengaturan 14
Daftar untuk AWS 14
Mendaftar untuk Akun AWS 14
Langkah berikutnya 14
Memulai 15
Panduan memulai cepat 15
Pre-launch cek 17
Pertimbangan untuk AWS IAM Identity Center Pelanggan (Pusat Identitas IAM) 18
Siapkan lingkungan khusus kontrol Anda 19
Memulai 20
Pertimbangan Konfigurasi AWS 20
Proses Implementasi 20
Catatan Penting 20
Memulai dari konsol 21
Harapan untuk konfigurasi zona pendaratan 21
Langkah 1: Buat alamat email akun bersama 22
Langkah 2. Konfigurasikan dan luncurkan zona pendaratan Anda 24
Langkah 3. Tinjau dan atur zona pendaratan 33
Mulai menggunakan API 33
Harapan untuk konfigurasi landing zone dengan API 34
Langkah 1: Konfigurasikan landing zone 35
Langkah 2: Luncurkan landing zone Anda menggunakan AWS Control Tower API 39

Identifikasi landing zone 42
Perbarui landing zone 43
Setel ulang landing zone untuk mengatasi drift 45
Melihat detail file manifes zona pendaratan Anda 46
Melihat status operasi zona pendaratan Anda 51
Contoh: Menyiapkan zona pendaratan AWS Control Tower hanya dengan API 53
Skema zona pendaratan 61
Luncurkan landing zone menggunakan CloudFormation 84
Langkah selanjutnya 90
Batasan dan kuota 91
Keterbatasan yang diketahui di AWS Control Tower 91
Meminta peningkatan kuota 94
Batasan kontrol 95
Temukan kontrol dan Wilayah yang tersedia 97
Keterbatasan berdasarkan yang mendasarinya AWS layanan 97
Perbedaan regional 98
Panduan Referensi Kontrol 101
Praktik terbaik untuk administrator 102
Menjelaskan akses ke pengguna 102
Menjelaskan akses sumber daya 102
Menjelaskan kontrol preventif 103
Rencanakan landing zone Anda 104
Bandingkan fungsionalitas 105
Luncurkan AWS Control Tower di Organisasi yang Ada 106
Luncurkan AWS Control Tower di Organisasi Baru 107
Praktik terbaik: Siapkan landing AWS zone multi-akun 108
Sejajarkan dengan panduan AWS multi-akun 108
Pedoman untuk mengatur lingkungan yang dirancang dengan baik 109
Sejajarkan struktur OU Anda dengan AWS strategi multi-akun 112
Tentang Root 112
Kiat administratif untuk pengaturan landing zone 113
Panduan migrasi Landing Zone v4.0 114
Perubahan kunci 115
Pembaruan AWS Config 118
Perbandingan fitur dengan dan tanpa AWS Config integrasi 122
Rekomendasi untuk menyiapkan grup, peran, dan kebijakan 123

Panduan tentang sumber daya AWS Control Tower 124
Kapan harus masuk sebagai pengguna root 126
AWS Organizations bimbingan 127
Panduan Pusat Identitas IAM 129
Panduan Account Factory 130
Panduan untuk berlangganan Topik SNS 131
Panduan untuk kunci KMS 132
Pembaruan zona pendaratan 133
Kebijakan untuk AI-based layanan 136
Manajemen pembaruan konfigurasi 137
Tentang pembaruan 139
Perbarui landing zone Anda 140
Prosedur pembaruan standar 140
Pilih versi landing zone 141
Pembaruan akun, versi landing zone, dan baseline 142
Pertahankan jejak akun 142
Selesaikan drift dengan Reset dan Re-register 144
Menyediakan dan memperbarui akun menggunakan otomatisasi 145
Otomatisasi tugas 147
AWS CloudShell dan AWS CLI 149
Dapatkan izin IAM untuk AWS CloudShell 150
Berinteraksi dengan AWS Control Tower lewat AWS CloudShell 151
AWS CloudFormation sumber daya 154
AWS Control Tower and CloudFormation templat 154
Pelajari lebih lanjut tentang CloudFormation 155
Sesuaikan zona pendaratan Anda 156
Kustomisasi dari konsol AWS Control Tower 156
Mengotomatiskan penyesuaian di luar konsol AWS Control Tower 158
Menara Kontrol AWS dan LZA 158
Manfaat Kustomisasi untuk AWS Control Tower (cFCT) 159
Contoh CfCT tambahan 160
Kustomisasi untuk ikhtisar AWS Control Tower (CFCT) 161
Arsitektur 161
Biaya 164
Layanan komponen 164
AWS CodeCommit 164

AWS CodePipeline 165
AWS Key Management Service 165
AWS Lambda 165
Layanan Notifikasi Sederhana Amazon 166
Amazon Simple Storage Service 166
Amazon Simple Queue Service 166
AWS Step Functions 167
AWS Penyimpanan Parameter Systems Manager 167
Pertimbangan deployment 167
Bersiaplah untuk penyebaran 167
Untuk memperbarui Kustomisasi untuk AWS Control Tower 169
Template dan kode sumber 169
Kode sumber 169
Menyebarkan CFCT 170
Prasyarat 170
Langkah-langkah penyebaran 170
Langkah 1. Luncurkan tumpukan 170
Langkah 2. Buat paket kustom 174
Perbarui tumpukan 175
Hapus set tumpukan 176
Siapkan Amazon S3 sebagai sumber konfigurasi 177
Siapkan GitHub sebagai sumber konfigurasi 178
Siapkan GitHub repositori 178
Buat GitHub koneksi 179
Menyebarkan CloudFormation tumpukan 179
Metrik operasional 180
Panduan kustomisasi CfCT 181
Ikhtisar pipa kode 181
Tentukan konfigurasi khusus 183
Root OU 190
OU bersarang 191
Buat kustomisasi Anda sendiri 192
Peningkatan versi untuk manifes cFCT 200
Jaringan 203
VPC dan AWS Wilayah di AWS Control Tower 203
Ikhtisar AWS Control Tower dan VPC 204

CIDR dan Peering untuk VPC dan AWS Control Tower 205
AWS PrivateLink 207
Pertimbangan-pertimbangan 207
Membuat sebuah titik akhir antarmuka 207
Membuat kebijakan titik akhir 208
Peran dan izin 210
Peran dan akun 211
Peran dan pembuatan akun 211
AWSControlTowerExecution peran 211
Kondisi opsional untuk hubungan kepercayaan peran Anda 213
Bagaimana AWS Control Tower digabungkan AWS Config aturan di OU dan akun yang tidak dikelola 216
Peran terprogram dan hubungan kepercayaan untuk akun audit AWS Control Tower 219
Penyediaan Akun Otomatis Dengan Peran IAM 223
Kelola sumber daya 225
Konfigurasikan Wilayah 226
Konfigurasikan Wilayah Menara Kontrol AWS Anda 227
Hindari tata kelola campuran saat mengonfigurasi Wilayah 229
Tentang Wilayah opt-in 231
Konfigurasikan kontrol Penolakan Wilayah 233
Pertimbangan untuk OU-level Wilayah menolak kontrol 235
Tentang akun 236
Apa yang terjadi ketika AWS Control Tower membuat akun 236
Pertimbangan untuk membawa akun keamanan atau pencatatan yang ada 237
Akun integrasi layanan 238
Akun manajemen 238
CloudTrail akun administrator 239
Akun agregator Config 240
Sumber daya akun integrasi layanan 241
Sumber daya akun manajemen 241
CloudTrail sumber daya akun administrator 246
Config sumber daya akun agregator 249
Tentang akun anggota 252
Berinteraksi dengan akun AWS Control Tower dari AWS Service Catalog 253
Membuat dan menyediakan akun 253
Mengotomatiskan Penyediaan Akun di AWS Control Tower menurut Service Catalog API ... 255

Memperbarui produk yang disediakan di Service Catalog 259
Membatalkan pendaftaran akun di Service Catalog 261
Menyediakan dan mengelola akun 262
Izin diperlukan 262
Metode penyediaan 263
Akun penyediaan di konsol 265
Melihat akun Anda 266
Tentang mendaftarkan akun 267
Apa yang terjadi selama pendaftaran akun 267
Daftarkan akun yang ada dengan VPC 269
Daftarkan akun dengan AWS Config sumber daya 269
Prasyarat untuk pendaftaran 270
Auto-enrollment pilihan 272
Mendaftar dari konsol 274
Jika akun tidak memenuhi prasyarat 277
Menambahkan peran IAM yang diperlukan secara manual ke yang sudah ada Akun AWS dan mendaftarkannya 279
Daftarkan akun yang sudah ada AWS Config sumber daya 282
Langkah 1: Hubungi dukungan untuk menambahkan akun ke daftar izinkan 284
Langkah 2: Buat peran IAM baru di akun anggota 285
Langkah 3: Identifikasi AWS Daerah dengan sumber daya yang sudah ada sebelumnya 286
Langkah 4: Identifikasi AWS Daerah tanpa AWS Config sumber daya 286
Langkah 5: Ubah sumber daya yang ada di masing-masing AWS Region 286
Langkah 5a. AWS Config sumber daya perekam 287
Langkah 5b. Memodifikasi AWS Config sumber daya saluran pengiriman 287
Langkah 5c. Memodifikasi AWS Config sumber daya otorisasi agregasi 288
Langkah 6: Buat sumber daya yang tidak ada, di Wilayah yang diatur oleh AWS Control Tower 289
Langkah 7: Daftarkan OU dengan AWS Control Tower 290
Pabrik Akun 290
Izin 291
Pertimbangan akun 292
Perbarui dan pindahkan akun 292
Mengubah alamat email akun yang terdaftar 293
Mengubah nama akun yang terdaftar 294
Konfigurasikan pengaturan Amazon VPC 295

Membatalkan pendaftaran akun 297
Tutup akun 298
Sumber daya Pabrik Akun 300
Kustomisasi Pabrik Akun (AFC) 302
Siapkan untuk penyesuaian 305
Buat akun yang disesuaikan dari cetak biru 311
Sesuaikan akun dengan AFC saat Anda mendaftarkannya 312
Menambahkan cetak biru ke akun AWS Control Tower 313
Memperbarui cetak biru 313
Menghapus cetak biru dari akun 314
Cetak biru mitra 315
Pertimbangan untuk Kustomisasi Pabrik Akun (AFC) 315
Jika terjadi kesalahan cetak biru 315
Menyesuaikan dokumen kebijakan Anda untuk cetak biru AFC berdasarkan CloudFormation 317
Izin tambahan diperlukan untuk membuat produk Katalog Terraform-based Layanan 318
Transisi ke jenis produk eksternal 320
Pabrik Akun Menara Kontrol AWS untuk Terraform (AFT) 321
Prasyarat 321
Ikhtisar AFT 322
Menyebarkan AFT 326
Menyediakan akun baru 335
Beberapa permintaan akun 336
Memperbarui akun yang sudah ada 337
Versi yang didukung 339
Aktifkan opsi fitur 343
Sumber daya untuk AFT 347
Peran yang diperlukan 352
Layanan komponen 356
Saluran penyediaan akun AFT 358
Kustomisasi akun 361
Pemicu kustomisasi 369
VCS Alternatif 372
Perlindungan data 376
Hapus akun 377
Metrik operasional 378

Panduan pemecahan masalah 379
Melayang 384
Mendeteksi drift 384
Melihat drift 386
Menyelesaikan drift 386
Pertimbangan tentang drift dan pemindaian kebijakan 388
Jenis drift untuk segera diselesaikan 389
Perubahan sumber daya yang dapat diperbaiki 390
Drift dan penyediaan akun baru 391
Jenis penyimpangan tata kelola 391
Akun anggota yang dipindahkan 393
Akun anggota yang dihapus 395
Pembaruan yang tidak direncanakan ke SCP terkelola 396
SCP terlepas dari OU terkelola 397
Dihapus Foundational OU 398
Security Hub CSPM kontrol drift 399
Pengendalian kebijakan drift 400
Akses tepercaya dinonaktifkan 401
Pergeseran warisan pada baseline yang diaktifkan 402
Pergeseran warisan pada kontrol yang diaktifkan 402
EventBridge penciptaan 405
Jika Anda mengelola sumber daya di luar AWS Control Tower 406
Mengacu pada sumber daya di luar AWS Control Tower 408
Mengubah nama sumber daya AWS Control Tower secara eksternal 408
Menghapus OU Keamanan 409
Menghapus akun dari OU Keamanan 410
Perubahan eksternal yang diperbarui secara otomatis 412
Organizations 414
Panduan video 415
Topik 415
Memperluas tata kelola ke organisasi yang sudah ada 415
Video: Aktifkan Zona Pendaratan yang ada AWS Organizations 417
Pertimbangan untuk Pusat Identitas IAM dan organisasi yang ada 417
Akses ke yang lain AWS layanan 417
OU bersarang 417
Panduan Video 418

Perluas dari struktur OU datar ke struktur OU bersarang 418
Pra-pemeriksaan pendaftaran OU bersarang 419
OU dan peran bersarang 419
Apa yang terjadi selama pendaftaran dan pendaftaran ulang OU dan akun bersarang 419
Pertimbangan untuk pendaftaran OU bersarang 420
Batasan OU bersarang 420
OU bersarang dan kepatuhan 421
OU bersarang dan drift 421
OU dan kontrol bersarang 422
OU bersarang dan akarnya 423
Daftarkan OU untuk mendaftarkan beberapa akun 423
Daftarkan OU yang ada 425
Buat OU baru 426
Menghapus OU 427
Penyebab umum kegagalan selama pendaftaran atau pendaftaran ulang 428
Perbarui organisasi 431
Kapan harus memperbarui OU dan akun 432
Perbarui beberapa akun dalam satu OU 432
Apa yang terjadi selama pendaftaran ulang 433
Perbarui satu akun 433
Transfer akun 434
Prasyarat 434
Langkah 1: Buka pendaftaran akun dari AWS Control Tower 434
Langkah 2: Transfer akun ke organisasi tujuan 435
Langkah 3: Daftarkan akun di organisasi tujuan 435
Pertimbangan tambahan 436
Layanan terintegrasi 437
AWS Cadangan 437
CloudFormation 438
CloudTrail 438
CloudWatch 438
AWS Config 439
Integrasi AWS Config di Control Tower Landing Zone 4.0 439
AWS Identity and Access Management 442
AWS Key Management Service 443
AWS Lambda 443

AWS Organizations ... 443
Pertimbangan-pertimbangan ... 444
Amazon S3 ... 444
Hub Keamanan CSPM ... 444
AWS Service Catalog ... 445
Amazon SNS ... 445
Fungsi Langkah ... 446
Manajemen identitas dan akses ... 447
Autentikasi ... 447
Kontrol akses ... 449
Pusat Identitas IAM dan AWS Control Tower ... 450
Grup pengguna, peran, dan set izin ... 451
Hal yang perlu diketahui tentang akun IAM Identity Center dan AWS Control Tower ... 452
Grup Pusat Identitas IAM untuk AWS Control Tower ... 452
Ikhtisar pengelolaan akses sumber daya dengan IAM ... 456
Sumber daya dan operasi AWS Control Tower ... 457
Tentang kepemilikan sumber daya ... 457
Kelola akses ke sumber daya ... 458
Tentukan elemen kebijakan: Tindakan, Efek, dan Prinsip ... 468
Menentukan kondisi dalam kebijakan ... 469
Cegah serangan wakil yang membingungkan ... 469
Kebijakan IAM untuk Menara Kontrol AWS ... 470
Izin Diperlukan untuk menggunakan konsol AWS Control Tower ... 470
AWS ControlTowerAdmin peran ... 472
AWS ControlTowerServiceRolePolicy ... 473
AWS ControlTowerIdentityCenterManagementPolicy ... 474
AWS ControlTowerStackSetRole ... 475
AWS ControlTowerCloudTrailRolePolicy ... 476
AWS ControlTowerBlueprintAccess persyaratan peran ... 477
AWSServiceRoleForAWSControlTower ... 478
AWS ControlTowerAccountServiceRolePolicy ... 479
Kebijakan terkelola untuk Menara Kontrol AWS ... 480
Keamanan ... 491
Perlindungan Data ... 491
Enkripsi saat Data Tidak Berpindah ... 493
Enkripsi Saat Data Berpindah ... 493

Batasi Akses ke Konten ... 493
Validasi Kepatuhan ... 494
Ketahanan ... 494
Keamanan Infrastruktur ... 495
Pencatatan dan Pemantauan ... 496
Tentang masuk ke AWS Control Tower ... 497
Kebijakan bucket S3 ... 498
Zona pendaratan versi 3.3 dan sebelumnya ... 498
Zona pendaratan versi 4.0 dan yang lebih baru ... 500
Ikhtisar pemantauan ... 503
Pencatatan Tindakan Menara Kontrol AWS dengan AWS CloudTrail ... 504
Informasi Menara Kontrol AWS di CloudTrail ... 504
Contoh: Entri File Log Menara Kontrol AWS ... 506
Pantau perubahan sumber daya dengan AWS Config ... 508
Kelola biaya Config ... 509
Lihat AWS Config data perekam pada akun terdaftar ... 510
Pemecahan masalah AWS Config di AWS Control Tower ... 511
Acara Siklus Hidup ... 512
`CreateManagedAccount` ... 516
`UpdateManagedAccount` ... 518
`EnableGuardrail` ... 519
`DisableGuardrail` ... 520
`SetupLandingZone` ... 522
`UpdateLandingZone` ... 523
`RegisterOrganizationalUnit` ... 525
`DeregisterOrganizationalUnit` ... 526
`PrecheckOrganizationalUnit` ... 528
`EnableBaseline` ... 530
`ResetEnabledBaseline` ... 531
`UpdateEnabledBaseline` ... 532
`DisableBaseline` ... 534
`EnableControl` ... 536
`ResetEnabledControl` ... 537
`UpdateEnabledControl` ... 538
`DisableControl` ... 539
Notifikasi pengguna ... 541

Pencadangan 544
Prasyarat 545
Aktifkan cadangan 547
Bagian pertama: Siapkan backup untuk landing zone 547
Bagian selanjutnya: Aktifkan cadangan di OU 549
Matikan cadangan 551
Langkah pertama: Matikan cadangan di OU 551
Langkah selanjutnya: Matikan AWS Backup Untuk landing zone 552
Akun yang dipindahkan 553
Backup drift 553
Sumber daya cadangan 554
Kontrol untuk AWS Pencadangan 558
Menonaktifkan landing zone 559
Ikhtisar proses penonaktifan 560
Cara menonaktifkan landing zone 561
Nonaktifkan landing zone Anda dengan API 562
Tugas pembersihan manual diperlukan setelah dinonaktifkan 563
Sumber daya tidak dihapus selama penonaktifan 564
Hapus sumber daya AWS Control Tower 567
Apakah saya perlu menonaktifkan alih-alih menghapus? 568
Tentang menghapus sumber daya AWS Control Tower 569
Hapus SCPs 569
Hapus StackSets dan Tumpukan 570
Hapus Bucket Amazon S3 di Akun Arsip Log 571
Menghapus Portofolio dan Produk Account Factory 572
Hapus Peran dan Kebijakan AWS Control Tower 573
Bantuan sumber daya AWS Control Tower 575
Pengaturan setelah menonaktifkan landing zone 575
Panduan 577
Panduan: Pindah dari ALZ ke AWS Control Tower 577
Panduan: Konfigurasikan Menara Kontrol AWS Tanpa VPC 577
Menghapus VPC Menara Kontrol AWS 578
Secara opsional membersihkan sumber daya VPC di akun 579
Buat Akun di AWS Control Tower Tanpa VPC 579
Panduan: Mengatur Grup Keamanan di AWS Control Tower Dengan AWS Firewall Manager .. 580
Mengatur Grup Keamanan Dengan AWS Firewall Manager 581

Pemecahan Masalah 582
Peluncuran Zona Pendaratan Gagal 582
Pembaruan Zona Pendaratan Gagal dengan Kesalahan KMS 583
Tidak Dapat Memperbarui Zona Pendaratan 584
Kesalahan zona pendaratan tidak mutakhir 585
Penyediaan Akun Baru Gagal 586
Gagal Mendaftarkan Akun yang Ada 587
Tidak Dapat Memperbarui Akun Akun Factory 587
Kesalahan Kegagalan yang Menyebutkan AWS Config 589
Kesalahan portofolio AWS Control Tower Account Factory 591
Menerima Kesalahan Izin Tidak Cukup 591
Kontrol Detektif tidak berlaku pada akun 592
Nilai melebihi kesalahan yang dikembalikan oleh AWS Organizations API 592
Gagal memindahkan akun Account Factory langsung dari satu landing zone AWS Control Tower ke landing zone AWS Control Tower lainnya 593
AWS Support 595
Garis dasar 596
Jenis dasar yang berlaku di tingkat OU 596
Jenis dasar yang berlaku untuk akun integrasi layanan selama penyiapan landing zone 598
Pendaftaran sebagian 600
Bandingkan konsol dan API 600
Diaktifkan baseline dan akun anggota 601
Garis dasar dan default versi 601
AWSControlTowerBaseline meja 602
Contoh: Mendaftarkan OU AWS Control Tower dengan API saja 607
Contoh API dasar 609
`DisableBaseline` 609
`EnableBaseline` 610
`GetBaseline` 612
`GetBaselineOperation` 612
`GetEnabledBaseline` 613
`ListBaselines` 614
`ListEnabledBaselines` 616
`ResetEnabledBaseline` 621
`UpdateEnabledBaseline` 621
Informasi tambahan 623

Tutorial dan lab 623
Jaringan 203
Keamanan, identitas, dan pencatatan 624
Menyebarkan sumber daya dan mengelola beban kerja 625
Bekerja dengan organisasi dan akun yang ada 625
Otomatisasi dan integrasi 625
Migrasi beban kerja 626
Layanan AWS terkait 626
AWS Marketplace jawaban 627
Catatan rilis 628
Januari 2026 - Sekarang 628
Account Factory for Terraform (AFT) mendukung proses penyesuaian khusus paket 628
AWS Control Tower tersedia di European Sovereign Cloud 629
Januari 2025 - Desember 2025 629
Zona pendaratan Menara Kontrol AWS versi 4.0 630
AWS Control Tower menambahkan 279 tambahan AWS Config kontrol ke Katalog Kontrol . 632
AWS Control Tower tersedia di Wilayah Asia Pasifik (Selandia Baru) 632
AWS Control Tower mendukung pendaftaran akun otomatis 632
AWS Control Tower memperbarui versi Python 633
AWS Control Tower mengurangi penyimpangan 633
AWS Control Tower mendukung alamat IPv6 634
Account Factory untuk Terraform versi 1.15.0 tersedia 634
Kontrol yang diperbarui dengan jenis instance Nitro 634
AWS Control Tower tersedia di Wilayah Asia Pasifik (Taipei) 635
Mendukung Menara Kontrol AWS PrivateLink 636
Dukungan untuk kerangka kerja industri tambahan, metadata yang diperbarui 636
Service-linked AWS Config mengendalikan 637
Tampilan konsol kontrol yang diaktifkan memberikan visibilitas terpusat 639
Account Factory for Terraform (AFT) mendukung konfigurasi baru saat penerapan 639
AWS Control Tower memperkenalkan pelaporan tingkat akun untuk API dasar 640
AWS Control Tower tersedia di AWS Wilayah Asia Pasifik (Thailand) dan Meksiko (Tengah) 640
Tambahan AWS Config kontrol tersedia 641
Menghapus pendaftaran dan menghapus tindakan untuk OU 641
Katalog Kontrol mendukung alamat IPv6 642
Januari - Desember 2024 642

Dukungan AWS Control Tower CfCT GitHub dan RCP 643
AWS Control Tower menambahkan kontrol preventif dengan kebijakan deklaratif 643
AWS Control Tower menambahkan opsi paket cadangan preskriptif 644
AWS Control Tower terintegrasi AWS Config mengendalikan 644
AWS Control Tower meningkatkan manajemen hook dan menambahkan Regions kontrol proaktif 644
AWS Control Tower meluncurkan kebijakan kontrol sumber daya terkelola 645
AWS Control Tower melaporkan penyimpangan kebijakan kontrol 646
`ResetEnabledControl`API baru 646
Kontrol pembaruan katalog `GetControl` API 647
Menara Kontrol AWS mendukung AFT GitLab 647
AWS Control Tower tersedia di AWS Wilayah Asia Pasifik (Malaysia) 648
AWS Control Tower mendukung hingga 1000 akun per OU 648
AWS Control Tower menambahkan pilihan versi zona pendaratan 648
API kontrol deskriptif tersedia, akses yang diperluas ke Wilayah dan kontrol 649
AWS Control Tower mendukung AFT dan CfCT di Wilayah pilihan 650
AWS Control Tower menambahkan `ListLandingZone0perations` API 650
AWS Control Tower mendukung hingga 100 operasi kontrol bersamaan 651
AWS Control Tower tersedia di AWS Kanada Barat (Calgary) 651
AWS Control Tower mendukung penyesuaian kuota layanan mandiri 652
AWS Control Tower merilis Panduan Referensi Kontrol 653
AWS Control Tower memperbarui dan mengganti nama dua kontrol proaktif 653
Kontrol yang tidak digunakan lagi tidak tersedia 654
AWS Control Tower mendukung penandaan `EnabledControl` sumber daya di CloudFormation 654
AWS Control Tower mendukung API untuk pendaftaran OU dan konfigurasi dengan garis dasar 655
Januari - Desember 2023 656
Transisi ke baru AWS Service Catalog Jenis produk eksternal (fase 3) 657
Zona pendaratan Menara Kontrol AWS versi 3.3 658
Transisi ke baru AWS Service Catalog Jenis produk eksternal (fase 2) 659
AWS Control Tower mengumumkan kontrol untuk membantu kedaulatan digital 659
API zona pendaratan Menara Kontrol AWS 663
API penandaan kontrol Menara Kontrol AWS 663
AWS Control Tower tersedia di AWS Asia Pacific (Melbourne) 663
Transisi ke yang baru AWS Service Catalog Jenis produk eksternal (fase 1) 663

AWS Control Tower menambahkan API kontrol baru 664
AWS Control Tower menambahkan kontrol baru 664
AWS Control Tower mendeteksi penyimpangan akses tepercaya 664
AWS Control Tower tersedia dalam empat tambahan Wilayah AWS 665
AWS Control Tower tersedia di AWS Israel (Tel Aviv) 665
AWS Control Tower menambahkan 28 kontrol proaktif baru 665
AWS Control Tower menghentikan dua kontrol 666
Zona pendaratan Menara Kontrol AWS versi 3.2 666
AWS Control Tower menambahkan pemetaan Email-to-ID untuk IAM Identity Center 668
AWS Control Tower menambahkan lebih banyak AWS Security Hub CSPM mengendalikan 668
AWS Control Tower menerbitkan metadata untuk AWS Security Hub CSPM mengendalikan 668
AWS Control Tower menambahkan Kustomisasi Pabrik Akun (AFC) untuk Terraform 669
AWS Control Tower menambahkan pusat identitas IAM yang dikelola sendiri 669
AWS Control Tower menambahkan catatan tata kelola campuran 669
AWS Control Tower menambahkan kontrol proaktif baru 670
AWS Control Tower memperbarui kontrol Amazon EC2 670
AWS Control Tower tersedia dalam tujuh tambahan Wilayah AWS 670
Kustomisasi Pabrik Akun AWS Control Tower (AFC) dan pelacakan permintaan secara umum tersedia 671
Zona pendaratan Menara Kontrol AWS versi 3.1 671
Kontrol proaktif AWS Control Tower umumnya tersedia 673
Januari - Desember 2022 673
Operasi akun bersamaan 674
Kustomisasi Pabrik Akun (AFC) 674
Kontrol komprehensif membantu AWS penyediaan dan manajemen sumber daya 675
Status kepatuhan dapat dilihat untuk semua AWS Config aturan 675
API untuk kontrol dan baru CloudFormation sumber daya 676
CfCT mendukung penghapusan set tumpukan 677
Retensi log yang disesuaikan 677
Perbaikan penyimpangan peran tersedia 678
Zona pendaratan Menara Kontrol AWS versi 3.0 678
Halaman Organisasi menggabungkan tampilan OU dan akun 682
Pembuatan dan pendaftaran akun yang disederhanakan 682
AFT mendukung kustomisasi otomatis untuk akun AWS Control Tower bersama 682

Operasi bersamaan untuk semua kontrol opsional 683
Akun keamanan dan logging yang ada 684
Zona pendaratan Menara Kontrol AWS versi 2.9 685
Zona pendaratan Menara Kontrol AWS versi 2.8 685
Januari - Desember 2021 686
Kemampuan wilayah menolak 687
Fitur residensi data 687
AWS Control Tower memperkenalkan penyediaan dan kustomisasi akun Terraform 688
Acara siklus hidup baru tersedia 688
AWS Control Tower mengaktifkan OU bersarang 689
Konkurensi kontrol detektif 689
Dua Wilayah baru tersedia 690
Pemutusan wilayah 691
AWS Control Tower bekerja dengan AWS Sistem Manajemen Kunci 691
Kontrol berganti nama, fungsionalitas tidak berubah 692
AWS Control Tower memindai SCP setiap hari untuk memeriksa penyimpangan 692
Nama yang disesuaikan untuk OU dan akun 693
Zona pendaratan Menara Kontrol AWS versi 2.7 693
Tiga baru AWS Wilayah yang tersedia 695
Hanya mengatur Wilayah yang dipilih 695
AWS Control Tower kini memperluas tata kelola ke OU yang ada di AWS organisasi 696
AWS Control Tower menyediakan pembaruan akun massal 696
Januari - Desember 2020 697
Konsol AWS Control Tower sekarang terhubung ke eksternal AWS Aturan Config 697
AWS Control Tower sekarang tersedia di Wilayah tambahan 698
Pembaruan pagar pembatas 699
Konsol AWS Control Tower menunjukkan detail lebih lanjut tentang OU dan akun 699
Gunakan AWS Control Tower untuk menyiapkan multi-akun baru AWS lingkungan di AWS Organizations 699
Kustomisasi untuk solusi AWS Control Tower 700
Ketersediaan umum AWS Control Tower versi 2.3 701
Single-step penyediaan akun di AWS Control Tower 701
Alat penonaktifan Menara Kontrol AWS 702
Pemberitahuan peristiwa siklus hidup AWS Control Tower 703
Juni - Desember 2019 703
Ketersediaan umum AWS Control Tower versi 2.2 703

Kontrol elektif baru di AWS Control Tower 704
Kontrol detektif baru di AWS Control Tower 705
AWS Control Tower menerima alamat email untuk akun bersama dengan domain berbeda dari akun manajemen 705
Ketersediaan umum AWS Control Tower versi 2.1 705
Riwayat dokumen 707
AWS Glosarium 731
..... dccxxxii

Apa itu Menara Kontrol AWS?

AWS Control Tower menawarkan cara mudah untuk mengatur dan mengatur lingkungan AWS multi-akun, mengikuti praktik terbaik preskriptif. AWS Control Tower mengatur kemampuan beberapa AWS layanan lain, termasuk,, dan AWS Organizations AWS Service Catalog AWS IAM Identity Center, untuk membangun zona pendaratan dalam waktu kurang dari satu jam. Sumber daya diatur dan dikelola atas nama Anda.

Orkestrasi AWS Control Tower memperluas kemampuan. AWS Organizations Untuk membantu menjaga organisasi dan akun Anda dari penyimp angan, yang merupakan perbedaan dari praktik terbaik, AWS Control Tower menerapkan kontrol (kadang-kadang disebut pagar pembatas). Misalnya, Anda dapat menggunakan kontrol untuk membantu memastikan bahwa log keamanan dan izin akses lintas akun yang diperlukan dibuat, dan tidak diubah.

Jika Anda menghosting lebih dari segelintir akun, ada baiknya memiliki lapisan orkestrasi yang memfasilitasi penyebaran akun dan tata kelola akun. Anda dapat mengadopsi AWS Control Tower sebagai cara utama untuk menyediakan akun dan infrastruktur. Dengan AWS Control Tower, Anda dapat lebih mudah mematuhi standar perusahaan, memenuhi persyaratan peraturan, dan mengikuti praktik terbaik.

AWS Control Tower memungkinkan pengguna akhir di tim terdistribusi Anda untuk menyediakan AWS akun baru dengan cepat, melalui templat akun yang dapat dikonfigurasi di Account Factory. Sementara itu, administrator cloud pusat Anda dapat memantau bahwa semua akun selaras dengan kebijakan kepatuhan yang ditetapkan di seluruh perusahaan.

Singkatnya, AWS Control Tower menawarkan cara termudah untuk mengatur dan mengatur AWS lingkungan multi-akun yang aman, patuh, berdasarkan praktik terbaik yang ditetapkan dengan bekerja dengan ribuan perusahaan. Untuk informasi selengkapnya tentang bekerja dengan AWS Control Tower dan praktik terbaik yang diuraikan dalam strategi AWS multi-akun, lihatAWS strategi multi-akun: Panduan praktik terbaik.

Fitur

AWS Control Tower memiliki fitur berikut:

- Zona pendaratan — Zona pendaratan adalah lingkungan multi-akun yang dirancang dengan baik yang didasarkan pada praktik terbaik keamanan dan kepatuhan. Ini adalah wadah di seluruh perusahaan yang menampung semua unit organisasi (OU), akun, pengguna, dan sumber daya lain

yang Anda inginkan tunduk pada peraturan kepatuhan. Zona pendaratan dapat diskalakan agar sesuai dengan kebutuhan perusahaan dari berbagai ukuran.

- Kontrol (kadang-kadang disebut pagar pembatas) adalah aturan tingkat tinggi yang menyediakan tata kelola berkelanjutan untuk lingkungan Anda secara keseluruhan AWS . Ini diungkapkan dalam bahasa sederhana. Ada tiga jenis kontrol: preven tif, detektif, dan proaktif. Tiga kategori panduan berlaku untuk kontrol: wajib, sangat direkomendasikan, atau elektif. Untuk informasi selengkapnya tentang kontrol, lihatBagaimana kontrol bekerja.
- Pabrik Akun — Pabrik Akun adalah template akun yang dapat dikonfigurasi yang membantu standarisasi penyediaan akun baru dengan konfigurasi akun yang telah disetujui sebelumnya. AWS Control Tower menawarkan Account Factory bawaan yang membantu mengotomatiskan alur kerja penyediaan akun di organisasi Anda. Untuk informasi selengkapnya, lihat Menyediakan dan mengelola akun dengan Account Factory.
- Dasbor — Dasbor menawarkan pengawasan berkelanjutan atas zona pendaratan Anda kepada tim administrator cloud pusat Anda. Gunakan dasbor untuk melihat akun yang disediakan di seluruh perusahaan Anda, kontrol yang diaktifkan untuk penegakan kebijakan, kontrol yang diaktifkan untuk deteksi terus-menerus ketidaksesuaian kebijakan, dan sumber daya yang tidak sesuai yang diatur oleh akun dan OU.

Cara AWS Control Tower berinteraksi dengan yang lain AWS layanan

AWS Control Tower dibangun di atas AWS layanan tepercaya dan andal termasuk AWS Service Catalog, AWS IAM Identity Center, dan AWS Organizations. Untuk informasi selengkapnya, lihat Layanan terintegrasi.

Anda dapat menggabungkan AWS Control Tower dengan AWS layanan lain ke dalam solusi yang membantu Anda memigrasikan beban kerja yang ada ke AWS. Untuk informasi selengkapnya, lihat Cara memanfaatkan AWS Control Tower dan memigr CloudEndure asikan beban kerja ke AWS.

Konfigurasi, Tata Kelola, dan Ekstensibilitas

- Konfigurasi akun otomatis: AWS Control Tower mengotomatiskan penyebaran dan pendaftaran akun melalui Pabrik Akun (atau “mesin penjual otomatis”), yang dibangun sebagai abstraksi di atas produk yang disediakan di. AWS Service Catalog Pabrik Akun dapat membuat dan mendaftarkan AWS akun, dan mengotomatiskan proses penerapan kontrol dan kebijakan ke akun tersebut. Untuk informasi selengkapnya tentang membuat dan menyediakan akun, lihat Metode penyediaan.

- Tata kelola terpusat: Dengan menggunakan kemampuan AWS Organizations, AWS Control Tower menyiapkan kerangka kerja yang memastikan kepatuhan dan tata kelola yang konsisten di seluruh lingkungan multi-akun Anda. AWS Organizations Layanan ini menyediakan kemampuan penting untuk mengelola lingkungan multi-akun, termasuk tata kelola pusat dan manajemen akun, pembuatan akun dari AWS Organizations API, kebijakan kontrol layanan (SCP), dan kebijakan kontrol sumber daya (RCP).

- Ekstensibilitas: Anda dapat membangun atau memperluas lingkungan AWS Control Tower Anda sendiri dengan bekerja langsung di AWS Organizations, serta di konsol AWS Control Tower. Anda dapat melihat perubahan yang tercermin di AWS Control Tower setelah mendaftarkan organisasi yang ada dan mendaftarkan akun yang ada ke AWS Control Tower. Anda dapat memperbarui zona pendaratan AWS Control Tower untuk mencerminkan perubahan Anda. Jika beban kerja Anda memerlukan kemampuan lanjutan lebih lanjut, Anda dapat memanfaatkan solusi AWS mitra lainnya bersama dengan AWS Control Tower.

Apakah Anda First-Time Pengguna Menara Kontrol AWS?

Jika Anda pertama kali menggunakan layanan ini, kami sarankan Anda membaca yang berikut ini:

1. Jika Anda memerlukan informasi lebih lanjut tentang cara merencanakan dan mengatur zona pendaratan Anda, lihat Rencanakan landing zone AWS Control Tower danAWS strategi multi-akun untuk landing zone AWS Control Tower.
2. Jika Anda siap untuk membuat zona pendaratan pertama Anda, lihatMemulai dengan AWS Control Tower.
3. Untuk informasi tentang deteksi dan pencegahan penyimpangan, lihatMendeteksi dan mengatasi penyimpangan di AWS Control Tower.
4. Untuk detail keamanan, lihatKeamanan di AWS Control Tower.
5. Untuk informasi tentang memperbarui zona pendaratan dan akun anggota, lihatManajemen pembaruan konfigurasi di AWS Control Tower.

Cara kerja AWS Control Tower

Bagian ini menjelaskan pada tingkat tinggi cara kerja AWS Control Tower. Landing zone Anda adalah lingkungan multi-akun yang dirancang dengan baik untuk semua sumber daya Anda. AWS Anda

dapat menggunakan lingkungan ini untuk menegakkan peraturan kepatuhan pada semua AWS akun Anda.

Struktur AWS Control Tower Landing Zone

Struktur landing zone di AWS Control Tower adalah sebagai berikut:

- Root — Induk yang berisi semua OU lain di landing zone Anda.
- Keamanan OU — Saat meluncurkan landing zone, Anda dapat memilih nama yang disesuaikan untuk akun di Security OU, dan Anda dapat membawa AWS akun yang ada ke AWS Control Tower untuk integrasi layanan.

  Di AWS Control Tower landing zone versi 3.3 dan yang lebih lama, OU ini berisi akun Log Archive dan Audit. Akun ini disebut akun bersama. Di landing zone versi 3.3 dan sebelumnya, Anda tidak dapat menambahkan akun yang ada untuk keamanan dan pencatatan setelah peluncuran awal.

  Di AWS Control Tower landing zone versi 4.0, AWS Control Tower tidak lagi memerlukan OU Keamanan, dan Anda dapat menentukan struktur organisasi Anda sendiri.
- Sandbox OU - Sandbox OU dibuat saat Anda meluncurkan landing zone Anda, jika Anda mengaktifkannya. Ini dan OU terdaftar lainnya berisi akun terdaftar yang digunakan pengguna Anda untuk melakukan beban AWS kerja mereka.
- Direktori IAM Identity Center — Secara default, direktori ini menampung pengguna IAM Identity Center Anda. Ini mendefinisikan ruang lingkup izin untuk setiap pengguna IAM Identity Center. Secara opsional, Anda dapat memilih untuk mengelola sendiri identitas dan kontrol akses Anda. Untuk informasi selengkapnya, lihat Bekerja dengan AWS IAM Identity Center dan AWS Control Tower.
- Pengguna IAM Identity Center — Ini adalah identitas yang dapat diasumsikan pengguna Anda untuk melakukan AWS beban kerja mereka di landing zone Anda.

Apa yang terjadi ketika Anda mengatur landing zone

Saat Anda menyiapkan landing zone, AWS Control Tower melakukan tindakan berikut di akun manajemen Anda atas nama Anda:

- Saat Anda membuat landing zone melalui konsol, AWS Control Tower membuat dua unit AWS Organizations organisasi (OU). Ini adalah OU Keamanan dan Sandbox OU opsional, yang terkandung dalam struktur akar organisasi. Selama penyiapan, AWS Control Tower secara

otomatis memilih Security OU sebagai OU default untuk integrasi layanan. OU ini dikenal sebagai OU integrasi layanan yang ditunjuk. Anda dapat memilih OU yang berbeda selama pengaturan landing zone.

AWS Control Tower mengharuskan semua akun yang dikonfigurasi agar integrasi AWS layanan berada di bawah OU yang sama, bersarang langsung di bawah root. Persyaratan ini tidak berlaku untuk akun manajemen.

Saat membuat landing zone melalui API, Anda tidak secara eksplisit memilih OU untuk integrasi layanan. Akun integrasi layanan harus berada di bawah OU yang sama bersarang langsung di bawah root, dan OU yang berisi akun integrasi layanan Anda adalah OU integrasi layanan yang ditunjuk. Untuk informasi selengkapnya, lihat Memulai AWS Control Tower API.

- AWS Control Tower membuat atau mendaftarkan akun untuk integrasi layanan apa pun yang diaktifkan (seperti AWS Config, AWS CloudTrail, atau AWS Backup) dalam OU integrasi layanan yang ditentukan.
- Membuat direktori cloud-native di IAM Identity Center, dengan grup yang telah dikonfigurasi sebelumnya dan akses masuk tunggal, jika Anda memilih konfigurasi AWS Control Tower default, atau memungkinkan Anda mengelola sendiri penyedia identitas Anda.
- Menerapkan semua kontrol preventif wajib untuk menegakkan kebijakan.
- Menerapkan semua kontrol detektif wajib untuk mendeteksi pelanggaran konfigurasi.
- Kontrol preventif tidak diterapkan ke akun manajemen.
- Kecuali untuk akun manajemen, kontrol diterapkan pada organisasi secara keseluruhan.

Mengelola Sumber Daya dengan Aman dalam Zona Pendaratan AWS Control Tower dan Akun Anda

- Saat Anda membuat landing zone, sejumlah AWS sumber daya dibuat. Untuk menggunakan AWS Control Tower, Anda tidak boleh mengubah atau menghapus sumber daya yang dikelola AWS Control Tower ini di luar metode yang didukung yang dijelaskan dalam panduan ini. Menghapus atau memodifikasi sumber daya ini akan menyebabkan landing zone Anda memasuki status yang tidak diketahui. Untuk detailnya, lihat Panduan untuk membuat dan memodifikasi sumber daya AWS Control Tower
- Saat Anda mengaktifkan kontrol opsional (yang memiliki panduan yang sangat direkomendasikan atau elektif), AWS Control Tower membuat AWS sumber daya yang dikelola di akun Anda. Jangan mengubah atau menghapus sumber daya yang dibuat oleh AWS Control Tower. Melakukannya dapat mengakibatkan kontrol memasuki status yang tidak diketahui.

Apa saja akun bersama?

Di AWS Control Tower, akun bersama di landing zone Anda disediakan selama penyiapan: akun manajemen, akun arsip log, dan akun audit.

Apa akun manajemennya?

Ini adalah akun yang Anda buat khusus untuk landing zone Anda. Akun ini digunakan untuk penagihan untuk semua yang ada di landing zone Anda. Ini juga digunakan untuk penyediaan akun Account Factory, serta untuk mengelola OU dan kontrol.

> **Note**
>
> Tidak disarankan untuk menjalankan semua jenis beban kerja produksi dari akun manajemen AWS Control Tower. Buat akun AWS Control Tower terpisah untuk menjalankan beban kerja Anda.

Untuk informasi selengkapnya, lihat Akun manajemen.

Apa itu akun arsip log?

Akun ini berfungsi sebagai repositori untuk log aktivitas API dan konfigurasi sumber daya dari semua akun di landing zone.

Untuk informasi selengkapnya, lihat CloudTrail akun administrator.

Apa itu akun audit?

Akun audit adalah akun terbatas yang dirancang untuk memberi tim keamanan dan kepatuhan Anda membaca dan menulis akses ke semua akun di landing zone Anda. Dari akun audit, Anda memiliki akses terprogram untuk meninjau akun, melalui peran yang diberikan kepada fungsi Lambda saja. Akun audit tidak memungkinkan Anda untuk masuk ke akun lain secara manual. Untuk informasi selengkapnya tentang fungsi dan peran Lambda, lihat Mengonfigurasi fungsi Lambda untuk mengambil peran dari yang lain. Akun AWS

Untuk informasi selengkapnya, lihat Akun agregator Config.

Bagaimana kontrol bekerja

Kontrol adalah aturan tingkat tinggi yang menyediakan tata kelola berkelanjutan untuk lingkungan Anda secara keseluruhan AWS . Setiap kontrol memberlakukan satu aturan, dan itu diekspresikan dalam bahasa sederhana. Anda dapat mengubah kontrol elektif atau sangat disarankan yang berlaku, kapan saja, dari konsol AWS Control Tower atau AWS Control Tower API. Kontrol wajib selalu diterapkan, dan tidak dapat diubah.

Kontrol preventif mencegah tindakan terjadi. Misalnya, kontrol elektif yang disebut Disallow Changes to Bucket Policy for Amazon S3 Bucket (Sebelumnya disebut Disallow Policy Changes to Log Archive) mencegah perubahan kebijakan IAM dalam akun bersama arsip log. Setiap upaya untuk melakukan tindakan yang dicegah ditolak dan masuk CloudTrail. Sumber daya juga masuk AWS Config.

Kontrol Detektif mendeteksi peristiwa tertentu ketika terjadi dan mencatat tindakan. CloudTrail Misalnya, kontrol yang sangat disarankan yang disebut Deteksi Apakah Enkripsi Diaktifkan untuk Volume Amazon EBS yang Dilampirkan ke Instans Amazon EC2 mendeteksi apakah volume Amazon EBS yang tidak terenkripsi dilampirkan ke instans EC2 di landing zone Anda.

Kontrol proaktif memeriksa apakah sumber daya sesuai dengan kebijakan dan tujuan perusahaan Anda, sebelum sumber daya disediakan di akun Anda. Jika sumber daya di luar kepatuhan, mereka tidak disediakan. Kontrol proaktif memantau sumber daya yang akan digunakan di akun Anda melalui templat. CloudFormation

Bagi mereka yang akrab dengan AWS: Di AWS Control Tower, kontrol preventif diimplementasikan dengan kebijakan kontrol layanan (SCP) dan kebijakan pengendalian sumber daya (RCP). Kontrol detektif diimplementasikan dengan AWS Config aturan. Kontrol proaktif diimplementasikan dengan CloudFormation kait.

Topik Terkait

- Mendeteksi dan mengatasi penyimpangan di AWS Control Tower

Cara AWS Control Tower bekerja dengan StackSets

AWS Control Tower digunakan CloudFormation StackSets untuk menyiapkan sumber daya di akun Anda, secara default. Setiap set tumpukan memiliki StackInstances yang sesuai dengan akun, dan

untuk Wilayah AWS per akun. AWS Control Tower menerapkan satu instans set tumpukan per akun dan Wilayah.

AWS Control Tower menerapkan pembaruan ke akun tertentu dan Wilayah AWS secara selektif, berdasarkan CloudFormation parameter. Ketika pembaruan diterapkan ke beberapa instance tumpukan, instance tumpukan lainnya mungkin dibiarkan dalam status usang. Perilaku ini diharapkan dan normal.

Ketika instance stack masuk ke status Outdated, biasanya berarti bahwa tumpukan yang sesuai dengan instance tumpukan itu tidak selaras dengan template terbaru dalam kumpulan tumpukan. Tumpukan tetap berada di template yang lebih lama, jadi mungkin tidak menyertakan sumber daya atau parameter terbaru. Tumpukan masih sepenuhnya dapat digunakan.

Berikut ringkasan singkat tentang perilaku apa yang diharapkan, berdasarkan CloudFormation parameter yang ditentukan selama pembaruan:

Jika pembaruan set tumpukan menyertakan perubahan pada templat (yaitu, jika `TemplateURL` properti `TemplateBody` atau ditentukan), atau jika `Parameters` properti ditentukan, CloudFormation tandai semua instance tumpukan dengan status Usang sebelum memperbarui instance tumpukan di akun yang ditentukan dan. Wilayah AWS Jika pembaruan set tumpukan tidak menyertakan perubahan pada templat atau parameter, CloudFormation perbarui instance tumpukan di akun dan Wilayah yang ditentukan, sambil meninggalkan semua instance tumpukan lainnya dengan status instance tumpukan yang ada. Untuk memperbarui semua instance tumpukan yang terkait dengan kumpulan tumpukan, jangan tentukan `Regions` properti `Accounts` atau.

Untuk informasi selengkapnya, lihat Memperbarui Set Stack Anda di Panduan CloudFormation Pengguna.

Terminologi

Berikut ulasan singkat tentang beberapa istilah yang akan Anda lihat di dokumentasi AWS Control Tower.

Pertama, ada baiknya mengetahui bahwa AWS Control Tower berbagi banyak terminologi dengan AWS Organizations layanan, termasuk istilah organisasi dan unit organisasi (OU), yang muncul di seluruh dokumen ini.

- Untuk informasi lebih lanjut tentang organisasi dan OU, lihat AWS Organizations terminologi dan konsep. Jika Anda baru mengenal AWS Control Tower, terminologi itu adalah tempat yang baik untuk memulai.
- AWS Organizationsadalah AWS layanan yang membantu Anda mengatur lingkungan secara terpusat saat Anda menumbuhkan dan meningkatkan skala AWS beban kerja Anda. AWS Control Tower mengandalkan AWS Organizations untuk membuat akun, untuk menegakkan kontrol preventif di tingkat OU, dan untuk menyediakan penagihan terpusat.
- Akun AWS Account Factory adalah AWS akun yang disediakan menggunakan Account Factory di AWS Control Tower. Terkadang, Account Factory disebut secara informal sebagai “mesin penjual otomatis” untuk akun.
- Wilayah beranda Men ara Kontrol AWS Anda adalah AWS Wilayah tempat zona pendaratan Menara Kontrol AWS Anda digunakan. Anda dapat melihat Wilayah rumah Anda di pengaturan zona pendaratan Anda.
- AWS Service Catalogmemungkinkan Anda mengelola layanan TI yang umum digunakan, secara terpusat. Dalam konteks dokumen ini, Account Factory menggunakan AWS Service Catalog untuk menyediakan AWS akun baru, termasuk akun dari cetak biru yang disesuaikan.
- AWS CloudFormation StackSetsadalah jenis sumber daya yang memperluas fungsionalitas tumpukan sehingga Anda dapat membuat, memperbarui, atau menghapus tumpukan di beberapa akun dan Wilayah dengan satu operasi dan satu CloudFormation templat.
- Instans tumpukan adalah referensi ke tumpukan di akun target dalam Wilayah.
- Tum pukan adalah kumpulan AWS sumber daya yang dapat Anda kelola sebagai satu unit.
- Agregator adalah jenis AWS Config sumber daya yang mengumpulkan data AWS Config konfigurasi dan kepatuhan dari beberapa akun dan Wilayah dalam organisasi, memungkinkan Anda untuk melihat dan menanyakan data kepatuhan ini dalam satu akun.
- Paket kesesuaian adalah kumpulan AWS Config aturan dan tindakan remediasi yang dapat diterapkan sebagai entitas tunggal dalam akun dan Wilayah, atau di seluruh organisasi di. AWS

Organizations Anda dapat menggunakan paket kesesuaian untuk membantu menyesuaikan lingkungan AWS Control Tower Anda. Untuk blog teknis yang memberikan rincian lebih lanjut, lihat Informasi terkait.

- Baseline di AWS Control Tower adalah sekelompok sumber daya dan konfigurasi spesifik yang dapat Anda terapkan ke target. Target dasar yang paling umum mungkin adalah unit organisasi (OU). Misalnya, baseline yang dipanggil `AWSControlTowerBaseline` tersedia untuk membantu mendaftarkan OU Anda dengan AWS Control Tower. Selama pengaturan dan pembaruan zona pendaratan, target dasar mungkin akun bersama, atau pengaturan khusus untuk zona pendaratan secara keseluruhan.
- Cetak biru: Cetak biru adalah artefak yang merangkum beberapa metadata, yang menjelaskan komponen infrastruktur yang digunakan dalam akun. Misalnya, CloudFormation template dapat berfungsi sebagai cetak biru untuk akun AWS Control Tower.
- Drift: Perubahan sumber daya yang diinstal oleh dan dikonfigurasi oleh AWS Control Tower. Sumber daya tanpa penyimpangan memungkinkan AWS Control Tower berfungsi dengan baik.
- Non-compliant sumber daya: Sumber daya yang melanggar AWS Config aturan yang mendefinisikan kontrol detektif tertentu.
- Akun bersama: Salah satu dari tiga akun yang dibuat AWS Control Tower secara otomatis saat Anda mengatur zona pendaratan: akun manajemen, akun arsip log, dan akun audit. Anda dapat memilih nama yang disesuaikan untuk akun arsip log dan akun audit, selama penyiapan.
- Akun anggota: Akun anggota milik organisasi AWS Control Tower. Akun anggota dapat di daftarkan atau tidak terdaftar di AWS Control Tower. Ketika OU terdaftar berisi campuran akun terdaftar dan tidak terdaftar:
  - Kontrol preventif yang diaktifkan pada (atau diwarisi oleh) OU berlaku untuk semua akun di dalamnya, termasuk yang tidak terdaftar. Ini benar karena kontrol preventif diberlakukan dengan SCP, RCPS, atau kebijakan deklaratif di tingkat OU, bukan tingkat akun. Untuk informasi selengkapnya, lihat War isan untuk kebijakan kontrol layanan dalam AWS Organizations dokumentasi.
  - Kontrol detektif yang diaktifkan pada OU tidak berlaku untuk akun yang tidak terdaftar.
  - Kontrol proaktif diimplementasikan oleh AWS CloudFormation kait. Kontrol ini tidak berlaku untuk akun yang tidak terdaftar di OU.

  Akun dapat menjadi anggota hanya satu organisasi pada satu waktu, dan biayanya ditagih ke akun manajemen untuk organisasi tersebut. Akun anggota dapat dipindahkan ke wadah root organisasi.
- AWS akun: AWS Akun bertindak sebagai wadah sumber daya dan batas isolasi sumber daya. AWS Akun dapat dikaitkan dengan penagihan dan pembayaran. AWS Akun berbeda dari akun

pengguna (kadang-kadang disebut akun pengguna IAM) di AWS Control Tower. Akun yang dibuat melalui proses penyediaan Account Factory adalah AWS akun. AWS akun juga dapat ditambahkan ke AWS Control Tower melalui pendaftaran akun atau proses pendaftaran OU.

- Kontrol: Kontrol (juga dikenal sebagai pagar pembatas) adalah aturan tingkat tinggi yang menyediakan tata kelola berkelanjutan untuk lingkungan Menara Kontrol AWS Anda secara keseluruhan. Setiap kontrol memberlakukan aturan tunggal. Kontrol preventif diimplementasikan dengan kebijakan kontrol layanan (SCP), kebijakan kontrol sumber daya (RCP), dan kebijakan deklaratif. Kontrol detektif diimplementasikan dengan AWS Config aturan. Kontrol proaktif diimplementasikan dengan CloudFormation kait. Untuk informasi selengkapnya, lihat Bagaimana kontrol bekerja.
- Katalog Kontrol: Katalog kontrol Menara Kontrol AWS adalah ringkasan dari semua kontrol yang tersedia melalui AWS Control Tower, di konsol, dan API. Sebelumnya disebut Perpustakaan Kontrol. Kami menyelaraskan terminologi dengan nama namespace, control catalog.
- Zona pendaratan: Zona pendaratan adalah lingkungan cloud yang menawarkan titik awal yang direkomendasikan, termasuk akun default, struktur akun, tata letak jaringan dan keamanan, dan sebagainya. Dari zona pendaratan, Anda dapat menerapkan beban kerja yang memanfaatkan solusi dan aplikasi Anda.
- Kerangka kerja: Kerangka kerja adalah standar peraturan khusus atau persyaratan industri. Dalam ontologi Katalog Kontrol, kerangka kerja diwakili oleh kontrol Standar. Untuk informasi selengkapnya, lihat ikhtisar Ontologi Katalog Kontrol.
- OU bersarang: OU bersarang di AWS Control Tower adalah OU yang terkandung dalam OU lain. OU bersarang dapat memiliki tepat satu OU induk, dan setiap akun dapat menjadi anggota tepat satu OU. OU bersarang membuat hierarki. Ketika Anda melampirkan kebijakan ke salah satu OU dalam hierarki, kebijakan tersebut mengalir ke bawah dan memengaruhi semua OU dan akun di bawahnya. Hirarki OU bersarang di AWS Control Tower dapat memiliki kedalaman maksimal lima tingkat.
- OU induk: OU tepat di atas OU saat ini dalam hierarki. Setiap OU dapat memiliki tepat satu OU induk.
- Child OU: Setiap OU di bawah OU saat ini dalam hierarki. OU dapat memiliki banyak OU anak.
- Hierarki OU: Di Menara Kontrol AWS, hierarki OU bersarang dapat memiliki hingga lima tingkat. Urutan bersarang disebut sebagai Level. Bagian atas hierarki ditetapkan sebagai Level 1.
- Top-level OU: OU tingkat atas adalah OU apa pun yang berada langsung di bawah Root, bukan Root itu sendiri. Root tidak dianggap sebagai OU.

- Diatur: Wilayah yang diatur dikelola dan dikendalikan di lingkungan Anda oleh AWS Control Tower, sesuai dengan kebijakan tata kelola yang ditetapkan oleh organisasi Anda. Ini Wilayah AWS dipantau untuk mematuhi praktik terbaik dan kebijakan organisasi. Sumber daya Anda di Wilayah ini dilindungi saat Anda mengaktifkan kontrol AWS Control Tower.
- Tidak diatur: Wilayah yang menampilkan status Tidak diatur tidak dikendalikan atau dipantau oleh AWS Control Tower. Ini Wilayah AWS biasanya tidak mematuhi kebijakan tata kelola yang sama dengan yang diberlakukan AWS Control Tower. Anda dapat membuat sumber daya di Wilayah ini, tetapi sumber daya tersebut tidak dilindungi oleh kontrol Menara Kontrol AWS.
- Ditolak: Wilayah yang ditolak diblokir secara khusus oleh AWS Control Tower. Dalam lingkungan AWS Control Tower Anda, Anda tidak dapat menyediakan sumber daya di dalamnya Wilayah AWS.

Harga

Tidak ada biaya tambahan untuk menggunakan AWS Control Tower. Anda hanya membayar untuk AWS layanan yang diaktifkan oleh AWS Control Tower, dan layanan yang Anda gunakan di zona pendaratan Anda. Misalnya, Anda membayar Katalog Layanan untuk menyediakan akun dengan Account Factory, dan AWS CloudTrail untuk peristiwa yang dilacak di zona pendaratan Anda. Untuk informasi tentang harga dan biaya yang terkait dengan AWS Control Tower, lihat harga AWS Control Tower.

Jika Anda menjalankan beban kerja sementara dari akun di AWS Control Tower, Anda mungkin melihat peningkatan biaya yang terkait dengan. AWS Config Untuk detailnya, lihat AWS Config harga. Hubungi perwakilan AWS akun Anda untuk informasi lebih spesifik tentang pengelolaan biaya ini. Untuk mempelajari selengkapnya tentang cara AWS Config kerja dengan AWS Control Tower, lihatPantau perubahan sumber daya dengan AWS Config.

Jika Anda menerapkan AWS CloudTrail jejak di luar AWS Control Tower, Anda dapat menggunakannya dengan AWS Control Tower. Namun, Anda mungkin dikenakan biaya duplikat, jika Anda juga memilih untuk mengikuti jejak yang dikelola oleh AWS Control Tower. Kami tidak merekomendasikan pengaturan jalur eksternal, kecuali Anda memiliki persyaratan khusus. Jika Anda memilih untuk ikut serta selama pengaturan atau pembaruan zona pendaratan, AWS Control Tower menyiapkan dan mengaktifkan CloudTrail jejak tingkat organisasi untuk Anda di akun manajemen. Untuk informasi tentang mengelola CloudTrail biaya, lihat M engelola CloudTrail biaya.

Pengaturan

Sebelum Anda menggunakan AWS Control Tower untuk pertama kalinya, ikuti langkah-langkah di bagian ini untuk membuat AWS akun dan melindungi akun AWS Control Tower manajemen Anda. Untuk informasi tentang tugas penyiapan tambahan khusus untuk AWS Control Tower, lihatMemulai dengan AWS Control Tower.

Daftar untuk AWS

Mendaftar untuk Akun AWS

Untuk memulai AWS, Anda membutuhkan Akun AWS. Untuk informasi tentang membuat Akun AWS, lihat Memulai dengan Akun AWS di Panduan AWS Account Management Referensi.

Saat Anda mendaftar ke Amazon Web Services (AWS), AWS akun Anda secara otomatis mendaftar untuk semua layanan AWS, termasuk AWS Control Tower. Jika Anda sudah memiliki AWS akun, lompat ke tugas berikutnya. Jika Anda tidak memiliki AWS akun, gunakan prosedur berikut untuk membuatnya.

Catat nomor AWS akun Anda, karena Anda membutuhkannya untuk tugas lain.

> **Keamanan untuk akun Anda**
>
> Anda dapat menemukan panduan tambahan tentang cara menyiapkan praktik terbaik yang melindungi keamanan AWS Control Tower akun Anda, dalam AWS Organizations dokumentasi.
>
> - Praktik terbaik untuk akun manajemen
> - Praktik terbaik untuk akun anggota

Langkah berikutnya

Memulai dengan AWS Control Tower

Memulai dengan AWS Control Tower

Prosedur memulai ini ditujukan untuk administrator AWS Control Tower. Ikuti prosedur ini saat Anda siap mengatur zona pendaratan menggunakan konsol AWS Control Tower atau API.

Jika Anda adalah AWS pelanggan saat ini, tetapi baru menggunakan AWS Control Tower, Anda mungkin ingin meninjau bagian yang disebutRencanakan landing zone AWS Control Tower, sebelum melanjutkan.

Topik

- Panduan memulai cepat AWS Control Tower
- Prasyarat: Pemeriksaan pra-peluncuran otomatis untuk akun manajemen Anda
- Menyiapkan lingkungan khusus kontrol Anda
- Memulai dengan AWS Control Tower dari konsol
- Memulai AWS Control Tower menggunakan API
- Langkah selanjutnya

Panduan memulai cepat AWS Control Tower

Jika Anda baru mengenal AWS, Anda dapat mengikuti langkah-langkah di bagian ini untuk memulai AWS Control Tower dengan cepat. Jika Anda ingin segera menyesuaikan lingkungan AWS Control Tower, lihatLangkah 2. Konfigurasikan dan luncurkan zona pendaratan Anda.

> **Note**
>
> AWS Control Tower menyiapkan layanan berbayar, seperti AWS CloudTrail, Amazon AWS Config CloudWatch, Amazon S3, dan Amazon VPC. Saat digunakan, layanan ini dapat dikenakan biaya, seperti yang ditunjukkan pada halaman harga. Konsol AWS manajemen menunjukkan kepada Anda penggunaan layanan berbayar dan biaya yang dikeluarkan. Tidak ada biaya tambahan yang dibuat oleh AWS Control Tower itu sendiri.

Sebelum Anda memulai

Keputusan paling penting untuk dibuat sebelum Anda memulai proses penyiapan adalah memilih Wilayah asal Anda. Wilayah asal Anda adalah AWS Wilayah tempat Anda akan menjalankan

sebagian besar beban kerja atau menyimpan sebagian besar data Anda. Ini tidak dapat diubah setelah Anda menyiapkan landing zone AWS Control Tower. Untuk informasi selengkapnya tentang cara memilih Wilayah asal, lihatKiat administratif untuk pengaturan landing zone.

> **Note**
>
> Secara default, AWS Control Tower memilih Wilayah tempat akun Anda beroperasi saat ini sebagai Wilayah asal Anda. Anda dapat melihat Wilayah Anda saat ini di kanan atas layar konsol AWS manajemen Anda.

Prosedur mulai cepat mengasumsikan bahwa Anda akan menerima nilai default untuk sumber daya di lingkungan AWS Control Tower Anda. Banyak dari pilihan ini dapat diubah nanti. Beberapa pilihan satu kali tercantum di bagian yang disebutHarapan untuk konfigurasi zona pendaratan.

Jika Anda telah membuat AWS akun baru, akun tersebut secara otomatis memenuhi prasyarat yang diperlukan untuk menyiapkan AWS Control Tower. Anda dapat melanjutkan melalui langkah-langkah berikut.

Langkah mulai cepat

1. Masuk ke konsol AWS manajemen dengan kredensi pengguna administrator Anda.
2. Arahkan ke konsol AWS Control Tower di https://console.aws.amazon.com/controltower.
3. Verifikasi bahwa Anda bekerja di Wilayah rumah yang Anda inginkan.
4. Pilih Aktifkan AWS Control Tower.
5. Ikuti instruksi di konsol, menerima semua nilai default. Pilih akun yang ada, atau buat akun baru, untuk akun Aggregator dan akun CloudTrail administrator Anda.
6. Tinjau pilihan Anda. Pilih Aktifkan AWS Control Tower.
7. AWS Control Tower membutuhkan waktu sekitar 30 menit untuk menyiapkan semua sumber daya di landing zone Anda.

Untuk versi yang lebih rinci tentang cara menyiapkan AWS Control Tower, termasuk cara menyesuaikan lingkungan Anda, baca dan ikuti prosedur dalam beberapa topik berikutnya.

> **Note**
>
> Jika Anda adalah pelanggan pertama kali dan Anda mengalami masalah pengaturan, hubungi AWS Support untuk bantuan diagnostik.

Prasyarat: Pemeriksaan pra-peluncuran otomatis untuk akun manajemen Anda

Sebelum AWS Control Tower menyiapkan zona pendaratan, AWS secara otomatis menjalankan serangkaian pemeriksaan pra-peluncuran di akun Anda. Tidak ada tindakan yang diperlukan dari pihak Anda untuk pemeriksaan ini, yang memastikan bahwa akun manajemen Anda siap untuk perubahan yang menetapkan zona pendaratan Anda. Berikut adalah pemeriksaan yang dijalankan AWS Control Tower sebelum menyiapkan zona pendaratan:

- Batas layanan yang ada untuk AWS Control Tower Akun AWS harus cukup untuk diluncurkan. Untuk informasi selengkapnya, lihat Batasan dan kuota di AWS Control Tower.
- Akun AWS Harus berlangganan AWS layanan berikut:
  - Amazon Simple Storage Service (Amazon S3)
  - Amazon Elastic Compute Cloud (Amazon EC2)
  - Amazon SNS
  - Amazon Virtual Private Cloud (Amazon VPC)
  - AWS CloudFormation
  - AWS CloudTrail
  - Amazon CloudWatch
  - AWS Config
  - AWS Identity and Access Management (IAM)
  - AWS Lambda

> **Note**
>
> Secara default, semua akun berlangganan layanan ini.

Pertimbangan untuk AWS IAM Identity Center Pelanggan (Pusat Identitas IAM)

- Jika AWS IAM Identity Center (Pusat Identitas IAM) sudah disiapkan, Wilayah rumah AWS Control Tower harus sama dengan Wilayah Pusat Identitas IAM. Namun, jika Pusat Identitas IAM diatur di Wilayah AS Timur (Virginia Utara) (us-east-1), AWS Control Tower menggunakan instance tersebut terlepas dari Wilayah asal yang Anda pilih.
- Pusat Identitas IAM hanya dapat diinstal di akun manajemen organisasi.
- Tiga opsi berlaku untuk direktori Pusat Identitas IAM Anda, berdasarkan sumber identitas yang Anda pilih:
  - Toko Pengguna Pusat Identitas IAM: Jika AWS Control Tower diatur dengan IAM Identity Center, AWS Control Tower membuat grup di direktori Pusat Identitas IAM dan menyediakan akses ke grup ini, untuk pengguna yang Anda pilih, untuk akun anggota.
  - Direktori Aktif: Jika Pusat Identitas IAM untuk Menara Kontrol AWS diatur dengan Active Directory, AWS Control Tower tidak mengelola direktori Pusat Identitas IAM. Itu tidak menetapkan pengguna atau grup ke AWS akun baru.
  - Penyedia Identitas Eksternal: Jika Pusat Identitas IAM untuk Menara Kontrol AWS diatur dengan penyedia identitas eksternal (IdP), AWS Control Tower membuat grup di direktori Pusat Identitas IAM dan menyediakan akses ke grup ini untuk pengguna yang Anda pilih untuk akun anggota. Anda dapat menentukan pengguna yang sudah ada dari IdP eksternal Anda di Account Factory selama pembuatan akun, dan AWS Control Tower memberi pengguna ini akses ke akun yang baru dijual saat menyinkronkan pengguna dengan nama yang sama antara Pusat Identitas IAM dan IdP eksternal. Anda juga dapat membuat grup di IdP eksternal agar sesuai dengan nama grup default di AWS Control Tower. Saat Anda menetapkan pengguna ke grup ini, pengguna ini akan memiliki akses ke akun terdaftar Anda.

  Untuk informasi selengkapnya tentang bekerja dengan IAM Identity Center dan AWS Control Tower, lihat Hal yang perlu diketahui tentang akun IAM Identity Center dan AWS Control Tower

Pertimbangan untuk AWS Config and AWS CloudTrail pelanggan

- Ak Akun AWS ses tepercaya tidak dapat diaktifkan di akun manajemen organisasi untuk AWS Config. Untuk informasi tentang cara menonaktifkan akses tepercaya, lihat AWS Organizations dokument asi tentang cara mengaktifkan atau menonaktifkan akses tepercaya.

- Jika Anda memiliki AWS Config perekam, saluran pengiriman, atau pengaturan agregasi yang ada di akun yang ada yang Anda rencanakan untuk mendaftarkan di AWS Control Tower, Anda harus mengubah atau menghapus konfigurasi ini sebelum mulai mendaftarkan akun, setelah zona pendaratan Anda diatur. Pemeriksaan awal ini tidak berlaku untuk akun manajemen AWS Control Tower selama peluncuran zona pendaratan. Untuk informasi selengkapnya, lihat Daftarkan akun yang sudah ada AWS Config sumber daya.
- Jika Anda menjalankan beban kerja sementara dari akun di AWS Control Tower, Anda mungkin melihat peningkatan biaya yang terkait dengan Config. AWS Hubungi perwakilan AWS akun Anda untuk informasi lebih spesifik tentang pengelolaan biaya ini.
- Saat Anda mendaftarkan akun ke AWS Control Tower, akun Anda diatur oleh AWS CloudTrail jejak organisasi AWS Control Tower. Jika Anda memiliki penerapan CloudTrail jejak yang ada di akun, Anda mungkin melihat biaya duplikat kecuali Anda menghapus jejak yang ada untuk akun tersebut sebelum mendaftarkannya di AWS Control Tower. Untuk informasi tentang jalur tingkat organisasi dan Menara Kontrol AWS, lihat. Harga

> **Note**
>
> Saat meluncurkan, titik akhir Layanan Token AWS Keamanan (STS) harus diaktifkan di akun manajemen, untuk semua Wilayah yang diatur oleh AWS Control Tower. Jika tidak, peluncuran mungkin gagal di tengah proses konfigurasi.

Menyiapkan lingkungan khusus kontrol Anda

Dengan AWS Control Tower landing zone 4.0, Anda sekarang dapat membuat lingkungan khusus kontrol tanpa menerapkan zona pendaratan penuh. Opsi penerapan ini dirancang untuk pelanggan yang memiliki pengaturan AWS Organizations yang mapan dan ingin fokus mengadopsi kontrol terkelola melalui Katalog Kontrol Menara Kontrol AWS.

Topik

- Memulai
- Pertimbangan Konfigurasi AWS
- Proses Implementasi
- Catatan Penting

Memulai

Mulailah dengan meninjau Katalog Kontrol Menara Kontrol AWS dari halaman beranda untuk memahami kontrol terkelola yang tersedia, kerangka kerja kepatuhan terkait, dan metadata kontrol. Untuk mengaktifkan pengalaman ini di AWS Control Tower, pilih Saya memiliki lingkungan yang ada dan ingin mengaktifkan AWS-managed kontrol di konsol. Anda kemudian akan mengonfirmasi wilayah asal Anda dan secara opsional memilih wilayah yang diatur tambahan. Selama penyiapan, Anda dapat mengaktifkan pendaftaran akun otomatis, yang memastikan akun secara otomatis mewarisi kontrol dan konfigurasi dari unit organisasi induk (OU) saat dipindahkan antar OU.

Pertimbangan Konfigurasi AWS

Anda memiliki opsi untuk mengaktifkan AWS Config selama pengaturan awal atau nanti sesuai kebutuhan. AWS Config diperlukan jika Anda berencana untuk menggunakan kontrol detektif di lingkungan Anda. Jika Anda memilih untuk mengaktifkan AWS Config, Anda harus menetapkan akun agregator untuk mengumpulkan data konfigurasi dan kepatuhan. Anda dapat memilih akun yang sudah ada atau membuat yang baru selama penyiapan. Opsi tambahan termasuk mengonfigurasi enkripsi AWS KMS kunci dan menentukan periode retensi log Amazon S3 untuk perekaman.

Proses Implementasi

Jika Anda melanjutkan tanpa AWS Config, lingkungan Anda akan segera siap untuk kontrol preventif dan proaktif dalam Katalog Kontrol.

Namun, ketika Anda siap untuk mengaktifkan kontrol detektif pertama Anda, Anda harus mengaktifkan AWS Config perekaman melalui yang baru `ConfigBaseline` diaktifkan pada OU target. Ini adalah proses penyiapan satu kali per OU dan AWS Config dikenakan harga berdasarkan jumlah akun per OU dan sumber daya per akun, per Wilayah AWS.

Catatan Penting

Membuat lingkungan AWS Control Tower membangun hubungan tepercaya dengan AWS Organizations, memungkinkan deteksi penyimpangan untuk kontrol preventif, dan pelacakan perubahan akun dan OU. Selama penyiapan, AWS Control Tower membuat konfigurasi zona pendaratan yang berfungsi sebagai dasar untuk lingkungan kontrol terkelola Anda.

Untuk membuat lingkungan khusus kontrol Anda melalui API, silakan lihat:. Memulai AWS Control Tower menggunakan API Perhatikan bahwa bidang manifes sekarang opsional dengan zona pendaratan 4.0.

Memulai dengan AWS Control Tower dari konsol

Prosedur memulai ini ditujukan untuk administrator AWS Control Tower. Ikuti prosedur ini saat Anda siap mengatur zona pendaratan menggunakan konsol AWS Control Tower. Dari awal hingga akhir, itu akan memakan waktu sekitar setengah jam. Prosedur ini membutuhkan beberapa prasyarat dan tiga langkah utama.

Jika Anda adalah AWS pelanggan saat ini, tetapi baru menggunakan AWS Control Tower, Anda mungkin ingin meninjau bagian yang disebutRencanakan landing zone AWS Control Tower, sebelum melanjutkan.

Topik

- Harapan untuk konfigurasi zona pendaratan
- Langkah 1: Buat alamat email akun bersama
- Langkah 2. Konfigurasikan dan luncurkan zona pendaratan Anda
- Langkah 3. Tinjau dan atur zona pendaratan

Harapan untuk konfigurasi zona pendaratan

Proses pengaturan zona pendaratan AWS Control Tower Anda memiliki beberapa langkah. Aspek tertentu dari zona pendaratan Menara Kontrol AWS Anda dapat dikonfigurasi. Pilihan lain tidak dapat diubah setelah penyiapan.

Item utama untuk dikonfigurasi selama pengaturan

- Anda dapat memilih nama OU tingkat atas selama penyiapan, dan Anda juga dapat mengubah nama OU setelah Anda mengatur zona pendaratan Anda. Secara default, OU tingkat atas diberi nama Keamanan dan Sandbox. Untuk informasi selengkapnya, lihat Pedoman untuk mengatur lingkungan yang dirancang dengan baik.
- Selama penyiapan, Anda dapat memilih nama yang disesuaikan untuk akun bersama yang dibuat AWS Control Tower, yang disebut akun CloudTrail Administrator dan Agregator secara default.

> **Note**
>
> Di Landing Zone versi sebelum 4.0, akun ini diberi nama “Log Archive” dan “Audit” secara default. Pelanggan yang menggunakan versi sebelumnya mungkin masih melihat nama aslinya.

- Selama penyiapan, Anda dapat secara opsional menentukan AWS akun yang ada untuk AWS Control Tower untuk digunakan sebagai akun arsip audit dan log. Jika Anda berencana untuk menentukan AWS akun yang ada, dan jika akun tersebut memiliki AWS Config sumber daya yang ada, Anda harus menghapus AWS Config sumber daya yang ada sebelum Anda dapat mendaftarkan akun ke AWS Control Tower. (Ini adalah pilihan satu kali.)
- Jika Anda menyiapkan untuk pertama kalinya, atau jika Anda memutakhirkan ke zona pendaratan versi 3.0, Anda dapat memilih apakah akan mengizinkan AWS Control Tower menyiapkan AWS CloudTrail jejak tingkat organisasi untuk organisasi Anda, atau Anda dapat memilih keluar dari jalur yang dikelola oleh AWS Control Tower dan mengelola jalur Anda sendiri CloudTrail . Anda dapat memilih atau memilih keluar dari jalur tingkat organisasi yang dikelola oleh AWS Control Tower setiap kali Anda memperbarui zona pendaratan.
- Secara opsional, Anda dapat menetapkan kebijakan retensi khusus untuk bucket log Amazon S3 dan bucket akses log, saat menyiapkan atau memperbarui zona pendaratan.
- Anda dapat secara opsional menentukan cetak biru yang telah ditentukan sebelumnya untuk digunakan untuk menyediakan akun anggota yang disesuaikan dari konsol AWS Control Tower. Anda dapat menyesuaikan akun nanti jika Anda tidak memiliki cetak biru yang tersedia. Lihat Sesuaikan akun dengan Kustomisasi Pabrik Akun (AFC).

Pilihan konfigurasi yang tidak dapat dibatalkan

- Anda tidak dapat mengubah Wilayah rumah Anda setelah mengatur zona pendaratan.
- Jika Anda menyediakan akun Account Factory dengan VPC, CIDR VPC tidak dapat diubah setelah dibuat.

Langkah 1: Buat alamat email akun bersama

Jika Anda menyiapkan zona pendaratan di zona baru Akun AWS, lihatPengaturan.

- Untuk mengatur zona pendaratan Anda dengan akun bersama baru, AWS Control Tower memerlukan dua alamat email unik yang belum dikaitkan dengan Akun AWS. Masing-masing alamat email ini akan berfungsi sebagai kotak masuk kolaboratif — akun email bersama — yang ditujukan untuk berbagai pengguna di perusahaan Anda yang akan melakukan pekerjaan tertentu yang terkait dengan AWS Control Tower.
- Jika Anda menyiapkan AWS Control Tower untuk pertama kalinya, dan jika Anda membawa akun arsip keamanan dan log yang ada ke AWS Control Tower, Anda dapat memasukkan alamat email saat ini dari AWS akun yang ada.

Alamat email diperlukan untuk:

- Akun audit — Akun ini untuk tim pengguna Anda yang memerlukan akses ke informasi audit yang disediakan oleh AWS Control Tower. Anda juga dapat menggunakan akun ini sebagai titik akses untuk alat pihak ketiga yang akan melakukan audit terprogram terhadap lingkungan Anda untuk membantu Anda mengaudit untuk tujuan kepatuhan.
- Akun arsip log — Akun ini untuk tim pengguna Anda yang membutuhkan akses ke semua informasi logging untuk semua akun terdaftar Anda dalam OU terdaftar di zona pendaratan Anda.

Akun-akun ini diatur di OU Keamanan saat Anda membuat zona pendaratan. Sebagai praktik terbaik, kami menyarankan bahwa ketika Anda melakukan tindakan di akun ini, Anda harus menggunakan pengguna Pusat Identitas IAM dengan izin cakupan yang sesuai.

> **Note**
>
> Jika Anda menentukan AWS akun yang ada sebagai akun arsip audit dan log, akun yang ada harus melewati beberapa pemeriksaan pra-peluncuran untuk memastikan bahwa tidak ada sumber daya yang bertentangan dengan persyaratan AWS Control Tower. Jika pemeriksaan ini tidak berhasil, pengaturan zona pendaratan Anda mungkin tidak berhasil. Secara khusus, akun tidak boleh memiliki AWS Config sumber daya yang ada. Untuk informasi selengkapnya, lihat Pertimbangan untuk membawa akun keamanan atau pencatatan yang ada.

Demi kejelasan, Panduan Pengguna ini selalu mengacu pada akun bersama dengan nama defaultnya: arsip log dan audit. Saat Anda membaca dokumen ini, ingatlah untuk mengganti nama khusus yang Anda berikan pada akun ini pada awalnya, jika Anda memilih untuk menyesuaikannya. Anda dapat melihat akun Anda dengan nama kustomisasi mereka di halaman Detail akun.

> **Note**
>
> Kami mengubah terminologi kami mengenai nama default beberapa unit organisasi AWS Control Tower (OU) agar selaras dengan strategi AWS multi-akun. Anda mungkin melihat beberapa inkonsistensi saat kami melakukan transisi untuk meningkatkan kejelasan nama-nama ini. Security OU sebelumnya disebut Core OU. Sandbox OU sebelumnya disebut Custom OU.

Langkah 2. Konfigurasikan dan luncurkan zona pendaratan Anda

Sebelum meluncurkan zona pendaratan AWS Control Tower, tentukan Wilayah rumah yang paling tepat. Untuk informasi selengkapnya, lihat Kiat administratif untuk pengaturan landing zone.

> **Important**
>
> Mengubah Wilayah asal Anda setelah Anda menerapkan zona pendaratan AWS Control Tower memerlukan penonaktifan serta bantuan AWS Dukungan. Praktek ini tidak dianjurkan.

Pelajari cara mengonfigurasi dan meluncurkan zona pendaratan menggunakan AWS CLI inMemulai AWS Control Tower menggunakan API.

Untuk mengonfigurasi dan meluncurkan zona pendaratan Anda di konsol, lakukan serangkaian langkah berikut.

Persiapkan: Arahkan ke konsol AWS Control Tower

1. Buka browser web, dan navigasikan ke konsol AWS Control Tower di https://console.aws.amazon.com/controltower.
2. Di konsol, verifikasi bahwa Anda bekerja di Wilayah rumah yang diinginkan untuk Menara Kontrol AWS. Kemudian pilih A tur zona pendaratan Anda.

Langkah 2a. Tinjau dan pilih AWS Wilayah

Pastikan Anda telah menetapkan dengan benar Wil AWS ayah yang Anda pilih untuk Wilayah rumah Anda. Setelah menerapkan AWS Control Tower, Anda tidak dapat mengubah Wilayah asal.

Di bagian proses penyiapan ini, Anda dapat menambahkan Wil AWS ayah tambahan yang Anda butuhkan. Anda dapat menambahkan lebih banyak Wilayah di lain waktu, jika diperlukan, dan Anda dapat menghapus Wilayah dari tata kelola.

Untuk memilih tambahan AWS Daerah untuk memerintah

1. Panel menunjukkan pilihan Wilayah saat ini. Buka menu tarik-turun untuk melihat daftar Wilayah tambahan yang tersedia untuk tata kelola.
2. Centang kotak di samping setiap Wilayah untuk dimasukkan ke dalam tata kelola oleh AWS Control Tower. Pilihan Wilayah rumah Anda tidak dapat diedit.

Untuk menolak akses ke Wilayah tertentu

Untuk menolak akses ke AWS sumber daya dan beban kerja di Wil AWS ayah tertentu, pilih Diaktifkan di bagian untuk kontrol Penolakan wilayah. Secara default, pengaturan untuk kontrol ini adalah Tidak diaktifkan.

Langkah 2b. Konfigurasikan unit organisasi Anda (OU)

Jika Anda menerima nama default OU ini, tidak ada tindakan yang perlu Anda lakukan untuk melanjutkan penyiapan. Untuk mengubah nama OU, masukkan nama baru secara langsung di bidang formulir.

- OU Dasar — Menara Kontrol AWS bergantung pada OU Dasar yang awalnya bernama OU Keamanan. Anda dapat mengubah nama OU ini selama pengaturan awal dan setelahnya, dari halaman detail OU. OU Keamanan ini berisi dua akun bersama Anda, yang secara default disebut akun arsip log dan akun audit.
- OU Tam bahan — AWS Control Tower dapat menyiapkan satu atau lebih OU Tambahan untuk Anda. Kami menyarankan Anda menyediakan setidaknya satu OU Tambahan di zona pendaratan Anda, selain OU Keamanan. Jika OU Tambahan ini ditujukan untuk proyek pengembangan, kami sarankan Anda menamainya Sandbox OU, seperti yang diberikan dalamPedoman untuk mengatur lingkungan yang dirancang dengan baik. Jika Anda sudah memiliki OU yang ada AWS Organizations, Anda mungkin melihat opsi untuk melewatkan pengaturan OU Tambahan di AWS Control Tower.

Langkah 2c. Konfigurasikan akun bersama, pencatatan, dan enkripsi Anda

Di bagian proses penyiapan ini, panel menampilkan pilihan default untuk nama-nama akun AWS Control Tower bersama Anda. Akun ini adalah bagian penting dari zona pendaratan Anda. Jangan memindahkan atau menghapus akun bersama ini. Anda dapat memilih nama yang disesuaikan untuk akun arsip audit dan log selama penyiapan. Atau, Anda memiliki opsi satu kali untuk menentukan AWS akun yang ada sebagai akun bersama Anda.

Anda harus memberikan alamat email unik untuk arsip log dan akun audit, dan Anda dapat memverifikasi alamat email yang sebelumnya Anda berikan untuk akun manajemen Anda. Pilih tombol Edit untuk mengubah nilai default yang dapat diedit.

Tentang akun bersama

- Akun manajemen — Akun manajemen AWS Control Tower adalah bagian dari level Root. Akun manajemen memungkinkan penagihan AWS Control Tower. Akun juga memiliki izin administrator untuk zona pendaratan Anda. Anda tidak dapat membuat akun terpisah untuk penagihan dan izin administrator di AWS Control Tower.

  Alamat email yang ditampilkan untuk akun manajemen tidak dapat diedit selama fase penyiapan ini. Ini ditampilkan sebagai konfirmasi, sehingga Anda dapat memeriksa apakah Anda mengedit akun manajemen yang benar, jika Anda memiliki beberapa akun.
- Dua akun bersama — Anda dapat memilih nama yang disesuaikan untuk kedua akun ini, atau membawa akun Anda sendiri, dan Anda harus memberikan alamat email unik untuk setiap akun, baik yang baru atau yang sudah ada. Jika Anda memilih agar AWS Control Tower membuat akun bersama baru untuk Anda, alamat email tersebut harus belum memiliki AWS akun terkait.

Untuk mengkonfigurasi akun bersama, isi informasi yang diminta.

1. Di konsol, masukkan nama untuk akun yang awalnya disebut akun arsip log. Banyak pelanggan memutuskan untuk mempertahankan nama default untuk akun ini.
2. Berikan alamat email unik untuk akun ini.
3. Masukkan nama untuk akun yang awalnya disebut akun audit. Banyak pelanggan memilih untuk menyebutnya akun Keamanan.
4. Berikan alamat email unik untuk akun ini.

Konfigurasikan retensi log secara opsional

Selama fase penyiapan ini, Anda dapat menyesuaikan kebijakan retensi log untuk bucket Amazon S3 yang menyimpan AWS CloudTrail log Anda di AWS Control Tower, dengan penambahan hari atau tahun, hingga maksimum 15 tahun. Jika Anda memilih untuk tidak menyesuaikan retensi log, pengaturan default adalah satu tahun untuk pencatatan akun standar dan 10 tahun untuk logging akses. Fitur ini juga tersedia saat Anda memperbarui atau mengatur ulang zona pendaratan Anda.

Kelola sendiri secara opsional Akun AWS akses

Anda dapat memilih apakah AWS Control Tower menyiapkan Akun AWS akses dengan AWS Identity and Access Management (IAM), atau apakah akan mengelola akses mandiri Akun AWS — baik dengan pengguna, peran, dan izin AWS IAM Identity Center yang dapat Anda atur dan sesuaikan

sendiri, atau dengan metode lain seperti IdP eksternal, baik untuk federasi akun langsung atau federasi ke beberapa akun melalui Pusat Identitas IAM. Anda dapat mengubah pilihan ini nanti.

Secara default, AWS Control Tower menyiapkan Pusat Identitas AWS IAM untuk zona pendaratan Anda, selaras dengan panduan praktik terbaik yang ditentukan dalam Mengatur AWS lingkungan Anda menggunakan beberapa akun. Sebagian besar pelanggan memilih default. Metode akses alternatif terkadang diperlukan, untuk kepatuhan terhadap peraturan di industri atau negara tertentu, atau di Wilayah AWS mana Pusat Identitas AWS IAM tidak tersedia.

Pemilihan penyedia identitas di tingkat akun tidak didukung. Opsi ini hanya berlaku untuk zona pendaratan secara keseluruhan.

Untuk informasi selengkapnya, lihat Panduan Pusat Identitas IAM.

Konfigurasikan secara opsional AWS CloudTrail jalan setapak

Sebagai praktik terbaik, kami sarankan Anda mengatur logging. Jika Anda ingin mengizinkan AWS Control Tower menyiapkan CloudTrail jejak tingkat organisasi dan mengelolanya untuk Anda, pilih Opt in. Jika Anda ingin mengelola pencatatan dengan CloudTrail jalur Anda sendiri atau alat pencatatan pihak ketiga, pilih Opt out. Konfirmasikan pilihan Anda saat diminta untuk melakukannya di konsol. Anda dapat mengubah pilihan Anda, dan memilih, atau memilih keluar dari, jalur tingkat organisasi saat memperbarui zona pendaratan Anda.

Anda dapat mengatur dan mengelola CloudTrail jalur Anda sendiri kapan saja, termasuk jalur tingkat organisasi dan tingkat akun. Jika Anda mengatur CloudTrail jalur duplikat, Anda mungkin dikenakan biaya duplikat saat CloudTrail peristiwa dicatat.

Konfigurasikan secara opsional AWS KMS keys

Jika Anda ingin mengenkripsi dan mendekripsi sumber daya Anda dengan kunci AWS KMS enkripsi, pilih kotak centang. Jika Anda memiliki kunci yang ada, Anda akan dapat memilihnya dari pengenal yang ditampilkan di menu dropdown. Anda dapat menghasilkan kunci baru dengan memilih Buat kunci. Anda dapat menambahkan atau mengubah kunci KMS setiap kali memperbarui zona pendaratan.

Saat Anda memilih Si apkan zona pendaratan, AWS Control Tower melakukan pemeriksaan awal untuk memvalidasi kunci KMS Anda. Kuncinya harus memenuhi persyaratan ini:

- Diaktifkan
- Simetris
- Bukan kunci Multi-wilayah

- Memiliki izin yang benar ditambahkan ke kebijakan
- Kuncinya ada di akun manajemen

Anda mungkin melihat spanduk kesalahan jika kunci tidak memenuhi persyaratan ini. Dalam hal ini, pilih kunci lain atau buat kunci. Pastikan untuk mengedit kebijakan izin kunci, seperti yang dijelaskan di bagian berikutnya.

Memperbarui kebijakan kunci KMS

Sebelum Anda dapat memperbarui kebijakan kunci KMS, Anda harus membuat kunci KMS. Untuk informasi selengkapnya, lihat Membuat kebijakan kunci di Panduan Developer AWS Key Management Service .

Untuk menggunakan kunci KMS dengan AWS Control Tower, Anda harus memperbarui kebijakan kunci KMS default dengan menambahkan izin minimum yang diperlukan untuk AWS Config dan. AWS CloudTrail Sebagai praktik terbaik, kami sarankan Anda menyertakan izin minimum yang diperlukan dalam kebijakan apa pun. Saat memperbarui kebijakan kunci KMS, Anda dapat menambahkan izin sebagai grup dalam satu pernyataan JSON atau baris demi baris.

Prosedur ini menjelaskan cara memperbarui kebijakan kunci KMS default di AWS KMS konsol dengan menambahkan pernyataan kebijakan yang memungkinkan AWS Config dan digunakan CloudTrail AWS KMS untuk enkripsi. Pernyataan kebijakan mengharuskan Anda menyertakan informasi berikut:

- **`YOUR-MANAGEMENT-ACCOUNT-ID`**— ID akun manajemen tempat AWS Control Tower akan disiapkan.
- **`YOUR-HOME-REGION`**— Wilayah rumah yang akan Anda pilih saat menyiapkan AWS Control Tower.
- **`YOUR-KMS-KEY-ID`**— ID kunci KMS yang akan digunakan dengan kebijakan.
- **`PARTITION`**— partisi Wil AWS ayah tempat Anda mengatur Menara Kontrol AWS, seperti`aws`,`aws-us-gov`,`aws-cn`, atau`aws-eusc`.

Untuk memperbarui kebijakan kunci KMS

1. Buka AWS KMS konsol di https://console.aws.amazon.com/kms
2. Dari panel navigasi, pilih Kunci yang dikelola pelanggan.
3. Dalam tabel, pilih kunci yang ingin Anda edit.

4. Di tab Kebijakan kunci, pastikan Anda dapat melihat kebijakan utama. Jika Anda tidak dapat melihat kebijakan utama, pilih Ber alih ke tampilan kebijakan.
5. Pilih Edit, dan perbarui kebijakan kunci KMS default dengan menambahkan pernyataan kebijakan berikut untuk AWS Config dan CloudTrail.

   AWS Config pernyataan kebijakan

```
{
    "Sid": "Allow Config to use KMS for encryption",
    "Effect": "Allow",
    "Principal": {
        "Service": "config.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": "arn:PARTITION:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID"
}
```

   CloudTrail pernyataan kebijakan

```
{
    "Sid": "Allow CloudTrail to use KMS for encryption",
    "Effect": "Allow",
    "Principal": {
        "Service": "cloudtrail.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
    ],
    "Resource": "arn:PARTITION:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID",
    "Condition": {
        "StringEquals": {
            "aws:SourceArn": "arn:PARTITION:cloudtrail:YOUR-HOME-REGION:YOUR-
MANAGEMENT-ACCOUNT-ID:trail/aws-controltower-BaselineCloudTrail"
        },
        "StringLike": {
```

```
            "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:PARTITION:cloudtrail:*:YOUR-MANAGEMENT-ACCOUNT-ID:trail/*"
        }
    }
}
```

6. Pilih Simpan perubahan.

Contoh kebijakan kunci KMS

Contoh kebijakan berikut menunjukkan seperti apa kebijakan kunci KMS Anda setelah Anda menambahkan pernyataan kebijakan yang memberikan AWS Config dan izin minimum CloudTrail yang diperlukan. Kebijakan contoh tidak menyertakan kebijakan kunci KMS default Anda.

```
{
    "Version": "2012-10-17",
    "Id": "CustomKMSPolicy",
    "Statement": [
        {
        ... YOUR-EXISTING-POLICIES ...
        },
        {
            "Sid": "Allow Config to use KMS for encryption",
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:PARTITION:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID"
        },
        {
            "Sid": "Allow CloudTrail to use KMS for encryption",
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
```

```
            ],
            "Resource": "arn:PARTITION:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": "arn:PARTITION:cloudtrail:YOUR-HOME-REGION:YOUR-
MANAGEMENT-ACCOUNT-ID:trail/aws-controltower-BaselineCloudTrail"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:PARTITION:cloudtrail:*:YOUR-MANAGEMENT-ACCOUNT-ID:trail/*"
                }
            }
        }
    ]
}
```

Untuk melihat contoh kebijakan lainnya, lihat halaman berikut:

- Memberikan izin enkripsi di Panduan AWS CloudTrail Pengguna.
- Izin yang Diperlukan untuk Kunci KMS Saat Menggunakan Service-Linked RolesS3 Bucket Delivery) di Panduan Peng AWS Config embang.

> **Melindungi dari penyerang**
>
> Dengan menambahkan kondisi tertentu ke kebijakan Anda, Anda dapat membantu mencegah jenis serangan tertentu, yang dikenal sebagai serangan wakil yang membing ungkan, yang terjadi jika entitas memaksa entitas yang lebih istimewa untuk melakukan tindakan, seperti dengan peniruan lintas layanan. Untuk informasi umum tentang kondisi kebijakan, lihat jugaMenentukan kondisi dalam kebijakan.

AWS Key Management Service (AWS KMS) memungkinkan Anda membuat kunci KMS multi-wilayah dan kunci asimetris; namun, AWS Control Tower tidak mendukung kunci Multi-wilayah atau kunci asimetris. AWS Control Tower melakukan pra-pemeriksaan kunci yang ada. Anda mungkin melihat pesan galat jika memilih kunci Multi-wilayah atau kunci asimetris. Dalam hal ini, buat kunci lain untuk digunakan dengan sumber daya AWS Control Tower.

Untuk informasi selengkap AWS KMS nya, lihat Panduan Peng AWS KMS embang.

Perhatikan bahwa data pelanggan di AWS Control Tower dienkripsi saat diam, secara default, menggunakan SSE-S3.

Secara opsional mengkonfigurasi pendaftaran otomatis untuk akun

Saat Anda mengaktifkan fitur ini selama penyiapan, atau yang lebih baru, akun yang dipindahkan antara dua OU terdaftar, atau dipindahkan ke lingkungan Menara Kontrol AWS Anda untuk pertama kalinya, tidak lagi menunjukkan status penyimpangan warisan. Akun secara otomatis mewarisi garis dasar dan kontrol yang diaktifkan pada OU baru. Kontrol dan garis dasar dari OU sebelumnya dihapus.

Untuk memilih pendaftaran otomatis kapan saja setelah penyiapan, navigasikan ke halaman Peng aturan zona pendaratan dan pilih Per barui zona pendaratan, atau panggil AWS Control Tower `UpdateLandingZone` API.

Anda dapat memindahkan akun antar OU melalui AWS Organizations API, atau melalui konsol AWS Control Tower. Jika Anda memindahkan akun di luar OU yang terdaftar, AWS Control Tower menghapus semua garis dasar dan kontrol yang digunakan, secara otomatis. Ini pada dasarnya membatalkan pendaftaran akun dari AWS Control Tower.

> **Note**
>
> Jika Anda memilih untuk mengaktifkan kemampuan pendaftaran otomatis setelah penyiapan awal zona pendaratan, AWS Control Tower tidak akan secara surut menyelesaikan penyimpangan warisan yang disebabkan oleh pemindahan akun antar OU sebelum kemampuan pendaftaran otomatis diaktifkan. Resolusi penyimpangan otomatis mulai berlaku untuk akun yang dipindahkan setelah Anda mengaktifkan pengaturan ini.

Secara opsional mengkonfigurasi dan membuat akun anggota yang disesuaikan

Saat mengikuti alur kerja Buat akun untuk menambahkan akun anggota, Anda dapat secara opsional menentukan cetak biru yang telah ditentukan sebelumnya untuk digunakan untuk menyediakan akun anggota yang disesuaikan dari konsol AWS Control Tower. Anda dapat menyesuaikan akun nanti jika Anda tidak memiliki cetak biru yang tersedia. Lihat Sesuaikan akun dengan Kustomisasi Pabrik Akun (AFC).

Langkah 3. Tinjau dan atur zona pendaratan

Bagian selanjutnya dalam penyiapan menunjukkan izin yang diperlukan AWS Control Tower untuk zona pendaratan Anda. Pilih kotak centang untuk memperluas setiap topik. Anda akan diminta untuk menyetujui izin ini, yang dapat memengaruhi beberapa akun, dan untuk menyetujui Ket entuan Layanan secara keseluruhan.

Untuk menyelesaikan

1. Di konsol, tinjau izin Layanan, dan ketika Anda siap, pilih Saya mengerti izin yang akan digunakan AWS Control Tower untuk mengelola AWS sumber daya dan menegakkan aturan atas nama saya.
2. Untuk menyelesaikan pilihan Anda dan menginisialisasi peluncuran, pilih A tur zona pendaratan.

Rangkaian langkah ini memulai proses pengaturan zona pendaratan Anda, yang dapat memakan waktu sekitar tiga puluh menit untuk menyelesaikannya. Selama penyiapan, AWS Control Tower membuat level Root Anda, OU Keamanan, dan akun bersama. Sumber AWS daya lain dibuat, dimodifikasi, atau dihapus.

⚠ Konfirmasikan langganan SNS

Alamat email yang Anda berikan untuk akun audit akan menerima AWS Notifikasi — Email Konfirmasi Lang ganan dari setiap Wil AWS ayah yang didukung oleh AWS Control Tower. Untuk menerima email kepatuhan di akun audit Anda, Anda harus memilih tautan Kon firmasi langganan dalam setiap email dari setiap Wil AWS ayah yang didukung oleh AWS Control Tower.

Memulai AWS Control Tower menggunakan API

Prosedur memulai ini ditujukan untuk administrator AWS Control Tower. Prosedur ini memerlukan beberapa prasyarat dan mencakup dua langkah utama.

Dalam prosedur ini, Anda akan menggunakan API dari AWS Control Tower dan AWS layanan lainnya untuk mengonfigurasi dan meluncurkan landing zone. API ini memungkinkan Anda membuat lingkungan AWS Control Tower secara terprogram, baik melalui CloudFormation konsol, atau melalui. AWS CLI

Sebelum meluncurkan landing zone AWS Control Tower, lakukan tugas prasyarat berikut:

- Tentukan Wilayah rumah yang paling tepat. Untuk informasi selengkapnya, lihat Kiat administratif untuk pengaturan landing zone.
- Tinjau Prasyarat: Pemeriksaan pra-peluncuran otomatis untuk akun manajemen Anda untuk mempelajari tentang pemeriksaan pra-peluncuran otomatis yang memastikan akun manajemen Anda siap untuk perubahan yang menetapkan landing zone Anda.

Topik

- Harapan untuk konfigurasi landing zone dengan API
- Langkah 1: Konfigurasikan landing zone
- Langkah 2: Luncurkan landing zone Anda menggunakan AWS Control Tower API
- Identifikasi landing zone
- Perbarui landing zone
- Setel ulang landing zone untuk mengatasi drift
- Melihat detail file manifes zona pendaratan Anda
- Melihat status operasi zona pendaratan Anda
- Contoh: Menyiapkan zona pendaratan AWS Control Tower hanya dengan API
- Skema zona pendaratan
- Luncurkan landing zone menggunakan CloudFormation

Harapan untuk konfigurasi landing zone dengan API

Proses pengaturan zona landing AWS Control Tower Anda memiliki beberapa langkah. Aspek tertentu dari zona landing zone AWS Control Tower Anda dapat dikonfigurasi. Pilihan lain tidak dapat diubah setelah pengaturan.

Item kunci untuk dikonfigurasi selama penyiapan

- Anda dapat memilih nama Foundational OU Anda selama pengaturan, dan Anda juga dapat mengubah nama OU setelah Anda mengatur landing zone Anda. Secara default, Foundational OU diberi nama Security dan Sandbox. Untuk informasi selengkapnya, lihat Pedoman untuk mengatur lingkungan yang dirancang dengan baik.

- Selama penyiapan, Anda dapat memilih nama yang disesuaikan untuk akun bersama yang dibuat AWS Control Tower, yang disebut arsip log dan audit secara default, tetapi Anda tidak dapat mengubah nama ini setelah penyiapan. (Ini adalah pilihan satu kali.)
- Selama penyiapan dengan API, Anda harus menentukan AWS akun yang ada untuk AWS Control Tower untuk digunakan sebagai akun audit dan arsip log. Untuk menentukan AWS akun yang ada, jika akun tersebut memiliki AWS Config sumber daya yang ada, Anda harus menghapus atau memodifikasi AWS Config sumber daya yang ada sebelum dapat mendaftarkan akun ke AWS Control Tower. (Ini adalah pilihan satu kali.)
- Jika Anda menyiapkan untuk pertama kalinya, atau jika Anda meningkatkan ke landing zone versi 3.0, Anda dapat memilih apakah akan mengizinkan AWS Control Tower menyiapkan AWS CloudTrail jejak tingkat organisasi untuk organisasi Anda, atau Anda dapat memilih keluar dari jalur yang dikelola oleh AWS Control Tower dan mengelola jalur Anda sendiri. CloudTrail Anda dapat memilih atau memilih keluar dari jalur tingkat organisasi yang dikelola oleh AWS Control Tower kapan pun Anda memperbarui landing zone.
- Anda dapat secara opsional menetapkan kebijakan retensi khusus untuk bucket log Amazon S3 dan bucket akses log, saat menyiapkan atau memperbarui landing zone.

Pilihan konfigurasi yang tidak dapat dibatalkan

- Anda tidak dapat mengubah Wilayah asal setelah menyiapkan landing zone.
- Jika Anda menyediakan akun dengan VPC, CIDR VPC tidak dapat diubah setelah dibuat.

Bagian selanjutnya memberikan prasyarat pengaturan dan langkah-langkah secara rinci, dengan penjelasan dan peringatan. Untuk contoh kode tambahan, lihatContoh: Menyiapkan zona pendaratan AWS Control Tower hanya dengan API.

Langkah 1: Konfigurasikan landing zone

Proses pengaturan zona landing AWS Control Tower Anda memiliki beberapa langkah. Aspek tertentu dari zona landing zone AWS Control Tower Anda dapat dikonfigurasi, tetapi pilihan lain tidak dapat diubah setelah penyiapan. Untuk mempelajari lebih lanjut tentang pertimbangan penting ini sebelum meluncurkan landing zone Anda, tinjau Ekspektasi untuk konfigurasi landing zone.

Sebelum menggunakan AWS Control Tower landing zone API, Anda harus terlebih dahulu memanggil API dari AWS layanan lain untuk mengonfigurasi landing zone Anda sebelum diluncurkan. Prosesnya mencakup tiga langkah utama:

1. menciptakan AWS organisasi Organizations baru,
2. menyiapkan akun integrasi layanan Anda,
3. dan membuat peran IAM atau pengguna Pusat Identitas IAM dengan izin yang diperlukan untuk memanggil API landing zone.

Langkah 1. Buat organisasi yang akan berisi landing zone Anda:

Hubungi AWS Organizations `CreateOrganization` API dan aktifkan semua fitur untuk membuat Foundational OU. AWS Control Tower juga merekomendasikan pembuatan OU Keamanan yang ditunjuk. Keamanan OU ini harus berisi semua akun integrasi layanan Anda. Ini akan menjadi akun arsip log dan akun audit untuk versi Zona Pendaratan sebelumnya.

```
aws organizations create-organization --feature-set ALL
```

AWS Control Tower dapat menyiapkan satu atau lebih OU Tambahan. Kami menyarankan Anda menyediakan setidaknya satu OU Tambahan di landing zone Anda, selain Security OU. Jika OU Tambahan ini ditujukan untuk proyek pengembangan, sebaiknya beri nama Sandbox OU, seperti yang diberikan dalam strategi multi-akun AWS untuk landing zone AWS Control Tower Anda.

Langkah 2. Penyediaan akun integrasi layanan jika diperlukan:

Untuk mengatur landing zone Anda, AWS Control Tower memungkinkan pelanggan mengonfigurasi integrasi layanan AWS. Masing-masing integrasi layanan ini mungkin memerlukan satu atau lebih akun pusat integrasi layanan. Jika Anda menggunakan landing zone API untuk menyiapkan AWS Control Tower untuk pertama kalinya, Anda harus menyediakan akun integrasi pusat untuk setiap integrasi layanan AWS yang diaktifkan. Anda dapat menggunakan akun AWS yang ada atau menyediakan akun ini melalui konsol AWS Control Tower atau AWS Organizations API. Pastikan akun integrasi layanan ini berada di OU Keamanan yang ditunjuk yang berada di tingkat root di organisasi Anda.

1. Hubungi AWS Organizations `CreateAccount` API untuk membuat akun arsip Log dan akun Audit di OU Keamanan.

```
aws organizations create-account --email mylog@example.com --account-name "Logging
 Account"
aws organizations create-account --email mysecurity@example.com --account-name
 "Security Account"
```

(Opsional) Periksa status `CreateAccount` operasi menggunakan AWS Organizations `DescribeAccount` API.

2. Pindahkan akun integrasi layanan yang disediakan ke dalam OU Keamanan yang ditunjuk

```
aws organizations move-account \
    --account-id 0123456789012 \
    --source-parent-id r-examplerootid111 \
    --destination-parent-id ou-examplerootid111-security
```

Langkah 3. Buat peran layanan yang diperlukan

Buat peran layanan IAM berikut di jalur `/service-role/` IAM yang memungkinkan AWS Control Tower menjalankan panggilan API yang diperlukan untuk menyiapkan landing zone Anda:

- `AWSControlTowerAdmin`
- `AWSControlTowerCloudTrailRole`
- `AWSControlTowerStackSetRole`
- `AWSControlTowerConfigAggregatorRoleForOrganizations`(tidak diperlukan untuk landing zone versi 4.0 dan yang lebih baru)

Untuk informasi selengkapnya tentang peran ini dan kebijakannya, lihatMenggunakan kebijakan berbasis identitas (kebijakan IAM) untuk AWS Control Tower.

Untuk membuat peran IAM:

Buat peran IAM dengan izin yang diperlukan untuk memanggil semua API landing zone. Atau, Anda dapat membuat pengguna Pusat Identitas IAM dan menetapkan izin yang diperlukan.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "backup:UpdateGlobalSettings",
                "controltower:CreateLandingZone",
                "controltower:UpdateLandingZone",
```

```
                "controltower:ResetLandingZone",
                "controltower:DeleteLandingZone",
                "controltower:GetLandingZoneOperation",
                "controltower:GetLandingZone",
                "controltower:ListLandingZones",
                "controltower:ListLandingZoneOperations",
                "controltower:ListTagsForResource",
                "controltower:TagResource",
                "controltower:UntagResource",
                "servicecatalog:*",
                "organizations:*",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:EnableAWSServiceAccess",
                "organizations:DeregisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "sso:*",
                "sso-directory:*",
                "logs:*",
                "cloudformation:*",
                "kms:*",
                "iam:GetRole",
                "iam:CreateRole",
                "iam:GetSAMLProvider",
                "iam:CreateSAMLProvider",
                "iam:CreateServiceLinkedRole",
                "iam:ListRolePolicies",
                "iam:PutRolePolicy",
                "iam:ListAttachedRolePolicies",
                "iam:AttachRolePolicy",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

> **Note**
>
> Saat memutakhirkan ke landing zone versi 4.0 dengan integrasi AWS Config diaktifkan, pelanggan harus `organizations:ListDelegatedAdministrators` memiliki izin.

Langkah 2: Luncurkan landing zone Anda menggunakan AWS Control Tower API

Anda dapat menggunakan AWS Control Tower API untuk meluncurkan landing zone Anda. Bagian ini menjelaskan cara membuat file manifes landing zone yang diperlukan dan menggunakannya dengan operasi `CreateLandingZone` API.

Membuat file manifes

File manifes adalah dokumen JSON yang menentukan konfigurasi landing zone Anda. Dengan landing zone versi 4.0, banyak komponen sekarang opsional, memungkinkan penerapan yang lebih fleksibel.

Struktur Manifes

Di bawah ini adalah struktur lengkap file manifes dengan semua konfigurasi yang tersedia:

```
{
    "accessManagement": {
        "enabled": true    // Required - Controls IAM Identity Center integration
    },
    "backup": {
        "enabled": true,   // Required - Controls AWS Backup integration
        "configurations": {
            "backupAdmin": {
                "accountId": "111122223333"    // Backup administrator account
            },
            "centralBackup": {
                "accountId": "111122224444"    // Central backup account
            },
            "kmsKeyArn": "arn:aws:kms:region:account-id:key/key-id"
        }
    },
    "centralizedLogging": {
```

```
        "accountId": "111122225555",    // Log archive account
        "enabled": true,                // Required - Controls centralized logging
        "configurations": {
            "accessLoggingBucket": {
                "retentionDays": 365    // Minimum value: 1
            },
            "loggingBucket": {
                "retentionDays": 365    // Minimum value: 1
            },
            "kmsKeyArn": "arn:aws:kms:region:account-id:key/key-id"
        }
    },
    "config": {
        "accountId": "111122226666",    // Config aggregator account
        "enabled": true,                // Required - Controls AWS Config integration
        "configurations": {
            "accessLoggingBucket": {
                "retentionDays": 365    // Minimum value: 1
            },
            "loggingBucket": {
                "retentionDays": 365    // Minimum value: 1
            },
            "kmsKeyArn": "arn:aws:kms:region:account-id:key/key-id"
        }
    },
    "governedRegions": [              // Optional - List of regions to govern
        "us-east-1",
        "us-west-2"
    ],
    "securityRoles": {
        "enabled": true,              // Required - Controls security roles creation
        "accountId": ""111122226666"    // Security/Audit account
    }
}
```

Catatan Penting

- Semua `enabled` bendera diperlukan dalam manifes.
- Jika Anda menonaktifkan integrasi AWS Config (`"config.enabled": false`), Anda juga harus menonaktifkan integrasi berikut:
  - Peran Keamanan (`"securityRoles.enabled": false`)

  - Manajemen Akses (`"accessManagement.enabled": false`)
  - Cadangan (`"backup.enabled": false`)
- ID akun harus berupa 12 digit ID AWS akun yang valid.
- ARN kunci KMS harus ARN AWS KMS kunci yang valid.
- Hari retensi harus minimal 1.

Menggunakan CreateLandingZone API

Untuk membuat landing zone menggunakan API:

```
aws controltower create-landing-zone --landing-zone-version 4.0 --manifest file://
manifest.json
```

API akan mengembalikan ID operasi landing zone yang dapat Anda gunakan untuk melacak kemajuan pembuatan landing zone Anda. Contoh respons:

```
{
    "arn": "arn:aws:controltower:us-west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H",
    "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

Anda dapat memantau status operasi menggunakan `GetLandingZoneOperation` API yang mengembalikan status`SUCCEEDED`,`FAILED`, atau`IN_PROGRESS`:

```
aws controltower get-landing-zone-operation --operation-identifier "55XXXXXX-eXXX-4XXX-
aXXX-44XXXXXXXXXX"
```

Apa yang Diubah di landing zone versi 4.0

Perubahan penting pada struktur dan persyaratan manifes:

- Struktur Organisasi
  - `organizationStructure`definisi telah dihapus dari manifes
  - Pelanggan sekarang dapat menentukan struktur organisasi mereka sendiri

  - Satu-satunya persyaratan: Akun integrasi layanan harus berada di OU yang sama langsung di bawah root
- Bendera yang Diaktifkan
  - Semua konfigurasi integrasi layanan memiliki `enabled` bendera yang sekarang menjadi bidang wajib.
  - Pelanggan harus selalu memberikan nilai boolean. Tidak ada nilai default yang disediakan.
  - Pelanggan perlu secara eksplisit enable/disable setiap konfigurasi integrasi layanan dalam manifes:
    - `accessManagement`
    - `backup`
    - `centralizedLogging`
    - `config`
    - `securityRoles`
- Peran Keamanan
  - Integrasi Peran Keamanan sekarang opsional
  - `enabled`Bendera baru diperkenalkan untuk mengelola `securityRoles` penyebaran
  - Saat dinonaktifkan, fitur keamanan terkait tidak akan diterapkan
- AWS Integrasi Config
  - Bagian integrasi layanan AWS Config baru ditambahkan ke manifes seperti pada `config` bidang berikut:
    - `enabled`: Bendera boolean yang diperlukan untuk mengelola penerapan integrasi AWS Config
    - `accountId`: ID akun AWS untuk agregator AWS Config
    - konfigurasi:
      - `accessLoggingBucket.retentionDays`: Periode retensi untuk log akses
      - `loggingBucket.retentionDays`: Periode retensi untuk log AWS Config
      - `kmsKeyArn`: Kunci KMS untuk enkripsi

Identifikasi landing zone

Panggilan `ListLandingZones` dapat membantu Anda menentukan apakah akun Anda sudah diatur dengan AWS Control Tower. API ini mengembalikan satu pengenal landing zone (ARN) di seluruh

wilayah komersial mana pun, terlepas dari wilayah asal landing zone. ARN zona pendaratan unik secara regional.

```
aws controltower list-landing-zones --region us-east-1
```

Untuk wilayah keikutsertaan, `ListLandingZones` API hanya menampilkan pengenal landing zone jika Anda memanggil API di wilayah yang sama dengan wilayah asal API. Misalnya, jika landing zone Anda diatur di af-south-1 dan Anda `ListLandingZones` memanggil af-south-1, API mengembalikan pengenal landing zone. Jika landing zone Anda diatur di af-south-1 dan Anda **`ListLandingZones`** memanggil ap-east-1, API tidak mengembalikan pengenal landing zone.

Output:

```
{
   "landingZones" [
        "arn": "arn:aws:controltower:us-
west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
   ]
}
```

Perbarui landing zone

Ketika versi landing zone baru tersedia, atau untuk membuat pembaruan lain pada konfigurasi landing zone Anda, Anda dapat memanggil `UpdateLandingZone` API dan mereferensikan file manifes landing zone yang diperbarui. API ini mengembalikan sebuah`OperationIdentifier`, yang kemudian dapat Anda gunakan saat memanggil `GetLandingZoneOperation` API untuk memeriksa status operasi pembaruan.

Untuk memperbarui landing zone

1. Hubungi AWS Control Tower `UpdateLandingZone` API dan lihat versi landing zone yang diperbarui atau file manifes landing zone Anda yang diperbarui.

   ```
   aws controltower update-landing-zone --landing-zone-version 3.3 --landing-zone-
   identifier "arn:aws:controltower:us-west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
    --manifest file://LandingZoneManifest.json
   ```

Contoh LandingZoneManifest.json file, dengan Wilayah dan logging terpusat:

```
{
   "governedRegions": ["us-west-2","us-west-1"],
   "organizationStructure": {
       "security": {
           "name": "Security"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   },
   "centralizedLogging": {
        "accountId": "LOG ARCHIVE ACCOUNT ID",
        "configurations": {
            "loggingBucket": {
                "retentionDays":2555
            },
            "accessLoggingBucket": {
                "retentionDays": 2555
            },
            "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX"
        },
        "enabled": true
   },
   "securityRoles": {
        "accountId": "SECURITY ACCOUNT ID"
   },
   "accessManagement": {
        "enabled": true
   }
}
```

Output:

```
{
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

> **Opsional Re-register OU untuk memperbarui akun**
>
> Untuk AWS Control Tower OU terdaftar dengan kurang dari 1000 akun, Anda dapat menggunakan konsol AWS Control Tower mengakses halaman OU di dasbor dan memilih Re-registerOU untuk memperbarui akun di OU tersebut.

Setel ulang landing zone untuk mengatasi drift

Saat Anda membuat landing zone, landing zone dan semua unit organisasi (OU), akun, dan sumber daya sesuai dengan aturan tata kelola yang diberlakukan oleh kontrol yang Anda pilih. Saat Anda dan anggota organisasi Anda menggunakan landing zone, perubahan status kepatuhan ini dapat terjadi. Perubahan ini disebut drift.

Untuk mengidentifikasi apakah landing zone Anda dalam drift, Anda dapat memanggil `GetLandingZone` API. API ini mengembalikan status drift zona pendaratan `DRIFTED` atau`IN_SYNC`.

Untuk mengatasi drift di dalam landing zone, Anda dapat menggunakan `ResetLandingZone` API untuk mengatur ulang landing zone kembali ke konfigurasi aslinya. Misalnya, AWS Control Tower mengaktifkan IAM Identity Center secara default untuk membantu Anda mengelola Akun AWS--tetapi jika Anda mengonfigurasi parameter landing zone asli Anda dengan IAM Identity Center dinonaktifkan, panggilan `ResetLandingZone` mempertahankan konfigurasi IAM Identity Center yang dinonaktifkan.

Anda dapat menggunakan `ResetLandingZone` API hanya jika landing zone Anda menggunakan versi 3.1 atau yang lebih baru. Anda dapat memanggil `GetLandingZone` API untuk memeriksa versi landing zone Anda saat ini. Jika landing zone Anda menggunakan versi lebih awal dari 3.1, `ResetLandingZone` API tidak tersedia. Dalam hal ini, setidaknya Perbarui landing zone ke versi 3.1. Proses pembaruan menyelesaikan drift sendiri, jadi Anda tidak perlu mengatur ulang secara terpisah. Menyetel ulang landing zone Anda tidak memutakhirkannya ke versi terbaru yang tersedia.

1. Panggil `GetLandingZone` API. Jika API mengembalikan status drift`DRIFTED`, landing zone Anda berada dalam drift.
2. Panggil `ResetLandingZone` API untuk mengatur ulang landing zone Anda ke konfigurasi aslinya.

```
aws controltower reset-landing-zone --landing-zone-identifier
 "arn:aws:controltower:us-west-2:123456789123:landingzone/1A2B3C4D5E6F7G8H"
```

Output:

```
{
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

> **Note**
>
> Menyetel ulang landing zone tidak memperbarui versi landing zone. Tinjau Perbarui landing zone untuk detail tentang memperbarui versi landing zone.

Melihat detail file manifes zona pendaratan Anda

File manifes zona pendaratan AWS Control Tower adalah file teks yang menjelaskan sumber daya AWS Control Tower Anda. Bagian berikut menunjukkan definisi rinci entri dalam file manifes zona pendaratan.

Untuk melihat contoh skema zona pendaratan lengkap, lihat Skema zona pendaratan.

GovernedRegions — Wilayah yang akan ditempatkan di bawah pemerintahan

- Jenis: Daftar string
- Wajib: Tidak
- Contoh:

```
"governedRegions": ["us-west-2","us-west-1"]
```

OrganizationStructure — Pilih nama OU keamanan dan kotak pasir yang akan dibuat di organisasi Anda

- Jenis: Objek
- Wajib: Ya
- Properti:
- Contoh:
  - `security`- objek dengan satu properti yang diperlukan`name`,, yang mengambil `String`
  - `sandbox`- objek dengan satu properti yang diperlukan`name`,, yang mengambil `String`

```
"organizationStructure": {
       "security": {
           "name": "CORE"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   }
```

> **Note**
>
> Bid `organizationStructure` ang tidak ada di zona pendaratan versi 4.0 dan yang lebih baru.

CentralizedLogging — Konfigurasi untuk AWS CloudTrail

- Jenis: Ob jek
- Diperlukan: Tidak (versi 4.0 dan yang lebih baru). Ya (versi 3.3 dan sebelumnya).
- Properti:
  - accountID - `String` a mewakili AWS akun tempat sumber daya logging harus digunakan
  - konfigurasi - `Object` dengan tiga properti
    - `loggingBucket`- objek dengan satu properti,`retentionDays`, yang mengambil `Number`
    - `accessLoggingBucket`- objek dengan satu properti,`retentionDays`, yang mengambil `Number`
    - `kmsKeyArn`- opsional `String`
  - diaktifkan - a `Boolean` (diperlukan dalam versi 4.0 dan yang lebih baru, opsional di versi 3.3 dan sebelumnya)
- Contoh:

```
"centralizedLogging": {
       "accountId": "222222222222",
       "configurations": {
           "loggingBucket": {
               "retentionDays": 60
           },
```

```
            "accessLoggingBucket": {
                "retentionDays": 60
            },
            "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX"
        },
        "enabled": true
   }
```

> **Note**
>
> Di zona pendaratan versi 4.0 dan yang lebih `accountId` baru, hanya `enabled` diperlukan bila disetel ke`true`. Bidang `enabled` wajib diisi.

SecurityRoles — Pilih tempat penyebaran sumber daya pusat untuk pemantauan keamanan dalam organisasi Anda

- Jenis: Ob jek
- Diperlukan: Tidak (versi 4.0 dan yang lebih baru). Ya (versi 3.3 dan sebelumnya).
- Properti:
  - Account Id - `String` yang mewakili AWS akun di mana sumber daya pemantauan keamanan pusat harus dikerahkan. Diper `enabled` lukan kapan`true`.
  - diaktifkan - a `Boolean` (diperlukan dalam versi 4.0 dan yang lebih baru)
- Contoh:

```
"securityRoles": {
        "accountId": "333333333333",
        "enabled": true
   }
```

> **Note**
>
> Di zona pendaratan versi 4.0 dan yang lebih baru, `securityRoles` menyertakan properti `enabled` Boolean yang diperlukan. Ini hanya `accountId` diperlukan ketika dis `enabled` etel ke`true`.

AccessManagement — Pilih apakah akan mengaktifkan manajemen akses

- Jenis: Ob jek
- Wajib: Tidak
- Properti: diaktifkan - Boolean
- Contoh:

```
"accessManagement": {
        "enabled": true
   }
```

backup — Konfigurasi untuk AWS Backup dengan AWS Control Tower

- Jenis: Ob jek
- Wajib: Tidak
- Properti:
  - konfigurasi - `Object` dengan tiga properti
    - `centralBackup`- objek dengan satu properti,`accountId`, yang mengambil `String`
    - `backupAdmin`- objek dengan satu properti,`accountId`, yang mengambil `String`
    - `kmsKeyArn`- opsional `String`
  - diaktifkan - a `Boolean`
- Contoh:

```
"backup": {
    "configurations": {
        "centralBackup": {
            "accountId": "CENTRAL BACKUP ACCOUNT ID"
        },
        "backupAdmin": {
            "accountId": "BACKUP MANAGER ACCOUNT ID"
        },
        "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/e84XXXXX-6bXX-49XX-9eXX-
ecfXXXXXXXXX"
    },
    "enabled": true
}
```

konfigurasi — Konfigurasi untuk AWS Config dengan AWS Control Tower

- Jenis: Ob jek
- Wajib: Tidak
- Properti:
  - Account Id - `String` yang mewakili AWS akun di mana AWS Config sumber daya harus dikerahkan. Diper `enabled` lukan kapan`true`.
  - konfigurasi - opsional `Object` dengan tiga properti
    - `loggingBucket`- objek dengan satu properti,`retentionDays`, yang mengambil `Number`
    - `accessLoggingBucket`- objek dengan satu properti,`retentionDays`, yang mengambil `Number`
    - `kmsKeyArn`- opsional `String`
  - diaktifkan - diperlukan `Boolean`
- Contoh:

```
"config": {
    "accountId": "444444444444",
    "configurations": {
        "loggingBucket": {
            "retentionDays": 60
        },
        "accessLoggingBucket": {
            "retentionDays": 60
        },
        "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/e84XXXXX-6bXX-49XX-9eXX-
ecfXXXXXXXXX"
    },
    "enabled": true
}
```

> **Note**
>
> Bid `config` ang ini hanya tersedia di zona pendaratan versi 4.0 dan yang lebih baru.

Melihat status operasi zona pendaratan Anda

`ListLandingZoneOperations`API memungkinkan Anda melihat status operasi AWS Control Tower yang melakukan tindakan di zona pendaratan Anda.

Untuk informasi selengkapnya tentang operasi API ini, lihat ListLandingZoneOperations.

ListLandingZoneOperations

Contoh input dan output untuk **`ListLandingZoneOperations`**.

Contoh ini menunjukkan cara memanggil API tanpa parameter.

```
aws controltower --region us-east-1 list-landing-zone-operations

{
    "landingZoneOperations": [
        {
            "operationIdentifier": "873fe98d-1ecc-4154-b593-86e4a95ebfXX",
            "operationType": "CREATE",
            "status": "FAILED"
        },
        {
            "operationIdentifier": "0016d43d-a307-4ad8-a2a2-b427b8eb1cXX",
            "operationType": "DELETE",
            "status": "SUCCEEDED"
        },
        {
            "operationIdentifier": "002b8b5a-6bb7-4c40-89cd-5822a73d13XX",
            "operationType": "CREATE",
            "status": "SUCCEEDED"
        },
        {
            "operationIdentifier": "008886a0-f7a2-4df3-90e8-6e9f936507XX",
            "operationType": "CREATE",
            "status": "FAILED"
        }
    ]
}
```

Contoh ini menunjukkan cara memanggil API dan menentukan jumlah maksimum hasil.

```
aws controltower --region us-east-1 list-landing-zone-operations --max-results 1
```

```
{
    "landingZoneOperations": [
        {
            "operationIdentifier": "873fe98d-1ecc-4154-b593-86e4a95ebfXX",
            "operationType": "CREATE",
            "status": "FAILED"
        }
    ],
    "nextToken": "AAMAATFMzwP0QysYY8npWgstfcHGQBj-
XCC18ISyd9mkQmzLR7ZFMket4F0aWv8tUTtnsTWOnfblUp_Q9U-
nX9_6lEsLHs0RlhceDKskHr0_3fm8KdPTa6ofxMt5SPw8WF7-Jsvw2rJVvhj4DHDipo-y1HVK_eZ__Z3-
OzInm403cIHxhbjGPgqCX6FeKr8lwgTDKOejkLYZ9w7J5aqPAKLfVP8KKNda5g0VfMj1wdl4J2nwnHI-
UuCTIZ5nUEgXgUHaFq6Ma1pLDfGefZQJn5HmDhhgd5yvqzSRH1BtrHpdV_N1EVP8u3JJr3eWQHe9jNB02lihD4Mdcbm3SJg
VXRwTUIBInrit4HslNtPE8-IC1gxCjGoYPGtuWBPumK-pUPE="
}
```

Contoh ini menunjukkan cara memanggil API dan mendapatkan hasil berpaginasi dengan`nextToken`.

```
aws controltower --region us-east-1 list-landing-zone-operations --next-token
 AAMAATFMzwP0QysYY8npWgstfcHGQBj-XCC18ISyd9mkQmzLR7ZFMket4F0aWv8tUTtnsTWOnfblUp_Q9U-
nX9_6lEsLHs0RlhceDKskHr0_3fm8KdPTa6ofxMt5SPw8WF7-Jsvw2rJVvhj4DHDipo-y1HVK_eZ__Z3-
OzInm403cIHxhbjGPgqCX6FeKr8lwgTDKOejkLYZ9w7J5aqPAKLfVP8KKNda5g0VfMj1wdl4J2nwnHI-
UuCTIZ5nUEgXgUHaFq6Ma1pLDfGefZQJn5HmDhhgd5yvqzSRH1BtrHpdV_N1EVP8u3JJr3eWQHe9jNB02lihD4Mdcbm3SJg
VXRwTUIBInrit4HslNtPE8-IC1gxCjGoYPGtuWBPumK-pUPE=

{
    "landingZoneOperations": [
        {
            "operationIdentifier": "0016d43d-a307-4ad8-a2a2-b427b8eb1cXX",
            "operationType": "DELETE",
            "status": "SUCCEEDED"
        },
        {
            "operationIdentifier": "002b8b5a-6bb7-4c40-89cd-5822a73d13XX",
            "operationType": "CREATE",
            "status": "SUCCEEDED"
        },
        {
            "operationIdentifier": "008886a0-f7a2-4df3-90e8-6e9f936507XX",
            "operationType": "CREATE",
            "status": "FAILED"
```

```
        }
    ]
}
```

Contoh ini menunjukkan cara memanggil API dengan filter.

```
aws controltower --region us-east-1 list-landing-zone-operations --filter '{"types":
["CREATE"],"statuses":["FAILED"]}'

{
    "landingZoneOperations": [
        {
            "operationIdentifier": "873fe98d-1ecc-4154-b593-86e4a95ebfXX",
            "operationType": "CREATE",
            "status": "FAILED"
        },
        {
            "operationIdentifier": "008886a0-f7a2-4df3-90e8-6e9f936507XX",
            "operationType": "CREATE",
            "status": "FAILED"
        }
    ]
}
```

Contoh: Menyiapkan zona pendaratan AWS Control Tower hanya dengan API

Panduan contoh ini adalah dokumen pendamping. Untuk penjelasan, peringatan, dan informasi selengkapnya, lihat Memulai dengan AWS Control Tower menggunakan API.

Prasyarat

Sebelum membuat zona pendaratan AWS Control Tower, Anda harus membuat organisasi, dua akun bersama, dan beberapa peran IAM. Tutorial panduan ini mencakup langkah-langkah ini, dengan contoh perintah dan output CLI.

Langkah 1. Buat organisasi dan dua akun yang diperlukan.

```
aws organizations create-organization --feature-set ALL
aws organizations create-account --email example+log@example.com --account-name "Log
 archive account"
```

```
aws organizations create-account --email example+aud@example.com --account-name "Audit
 account"
```

Langkah 2. Buat peran IAM yang diperlukan.

AWSControlTowerAdmin

```
cat <<EOF >controltower_trust.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "controltower.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF
aws iam create-role --role-name AWSControlTowerAdmin --path /service-role/ --assume-
role-policy-document file://controltower_trust.json
cat <<EOF >ct_admin_role_policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*"
        }
    ]
}
EOF
aws iam put-role-policy --role-name AWSControlTowerAdmin --policy-name
 AWSControlTowerAdminPolicy --policy-document file://ct_admin_role_policy.json
aws iam attach-role-policy --role-name AWSControlTowerAdmin --policy-arn
 arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy
```

AWSControlTowerCloudTrailRole

```
cat <<EOF >cloudtrail_trust.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
EOF
aws iam create-role --role-name AWSControlTowerCloudTrailRole --path /service-role/ --
assume-role-policy-document file://cloudtrail_trust.json
cat <<EOF >cloudtrail_role_policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "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:*",
            "Effect": "Allow"
        }
    ]
}
EOF
aws iam put-role-policy --role-name AWSControlTowerCloudTrailRole --
policy-name AWSControlTowerCloudTrailRolePolicy --policy-document file://
cloudtrail_role_policy.json
```

AWSControlTowerStackSetRole

```
cat <<EOF >cloudformation_trust.json
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudformation.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
EOF
aws iam create-role --role-name AWSControlTowerStackSetRole --path /service-role/ --
assume-role-policy-document file://cloudformation_trust.json
cat <<EOF >stackset_role_policy.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution"
            ],
            "Effect": "Allow"
        }
    ]
}
EOF
aws iam put-role-policy --role-name AWSControlTowerStackSetRole --policy-name
 AWSControlTowerStackSetRolePolicy --policy-document file://stackset_role_policy.json
```

AWSControlTowerConfigAggregatorRoleForOrganizations

```
cat <<EOF >config_trust.json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "config.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
```

```
        }
    ]
}
EOF
aws iam create-role --role-name AWSControlTowerConfigAggregatorRoleForOrganizations --
path /service-role/ --assume-role-policy-document file://config_trust.json
aws iam attach-role-policy --role-name
 AWSControlTowerConfigAggregatorRoleForOrganizations --policy-arn
 arn:aws:iam::aws:policy/service-role/AWSConfigRoleForOrganizations
```

Langkah 3. Dapatkan ID akun dan buat file manifes zona pendaratan.

Dua perintah pertama dalam contoh berikut menyimpan ID akun untuk akun yang Anda buat di Langkah 1 ke dalam variabel. Variabel-variabel ini kemudian membantu menghasilkan file manifes zona pendaratan.

```
sec_account_id=$(aws organizations list-accounts | jq -r '.Accounts[] | select(.Name ==
 "Audit account") | .Id')
log_account_id=$(aws organizations list-accounts | jq -r '.Accounts[] | select(.Name ==
 "Log archive account") | .Id')

cat <<EOF >landing_zone_manifest.json
{
   "governedRegions": ["us-west-1", "us-west-2"],
   "organizationStructure": {
       "security": {
           "name": "Security"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   },
   "centralizedLogging": {
        "accountId": "$log_account_id",
        "configurations": {
            "loggingBucket": {
                "retentionDays": 60
            },
            "accessLoggingBucket": {
                "retentionDays": 60
            }
        },
        "enabled": true
```

```
   },
   "securityRoles": {
        "accountId": "$sec_account_id"
   },
   "accessManagement": {
        "enabled": true
   }
}
EOF
```

Langkah 4. Buat zona pendaratan dengan versi terbaru.

Anda harus mengatur zona pendaratan dengan file manifes dan versi terbaru. Contoh ini menunjukkan versi 3.3.

```
aws --region us-west-1 controltower create-landing-zone --manifest file://
landing_zone_manifest.json --landing-zone-version 3.3
```

Output akan berisi arn dan operationIdentifier, seperti yang ditunjukkan pada contoh berikut.

```
{
    "arn": "arn:aws:controltower:us-west-1:0123456789012:landingzone/4B3H0ULNUOL2AXXX",
    "operationIdentifier": "16bb47f7-b7a2-4d90-bc71-7df4ca1201xx"
}
```

Langkah 5. (Opsional) Lacak status operasi pembuatan zona pendaratan Anda, dengan menyiapkan loop.

Untuk melacak status, gunakan Oper ationIdentifier dari output `create-landing-zone` perintah sebelumnya.

```
aws --region us-west-1 controltower get-landing-zone-operation --operation-identifier
 16bb47f7-b7a2-4d90-bc71-7df4ca1201xx
```

Output status sampel:

```
{
    "operationDetails": {
        "operationType": "CREATE",
        "startTime": "2024-02-28T21:49:31Z",
        "status": "IN_PROGRESS"
```

```
    }
}
```

Anda dapat menggunakan contoh skrip berikut untuk membantu Anda mengatur loop, yang melaporkan status operasi berulang kali, seperti file log. Maka Anda tidak perlu terus memasukkan perintah.

```
while true; do echo "$(date) $(aws --region us-west-1 controltower get-landing-
zone-operation --operation-identifier 16bb47f7-b7a2-4d90-bc71-7df4ca1201xx | jq -
r .operationDetails.status)"; sleep 15; done
```

Untuk menampilkan informasi terperinci tentang zona pendaratan Anda

Langkah 1. Temukan ARN dari zona pendaratan

```
aws --region us-west-1 controltower list-landing-zones
```

Output akan mencakup pengenal zona pendaratan, seperti yang ditunjukkan pada contoh output berikut.

```
{
    "landingZones": [
        {
            "arn": "arn:aws:controltower:us-
west-1:123456789012:landingzone/4B3H0ULNUOL2AXXX"
        }
    ]
}
```

Langkah 2. Dapatkan informasinya

```
aws --region us-west-1 controltower get-landing-zone --landing-zone-identifier
 arn:aws:controltower:us-west-1:123456789012:landingzone/4B3H0ULNUOL2AXXX
```

Berikut adalah contoh dari jenis output yang mungkin Anda lihat:

```
{
    "landingZone": {
        "arn": "arn:aws:controltower:us-
west-1:123456789012:landingzone/4B3H0ULNUOL2AXXX",
```

```
        "driftStatus": {
            "status": "IN_SYNC"
        },
        "latestAvailableVersion": "3.3",
        "manifest": {
            "accessManagement": {
                "enabled": true
            },
            "securityRoles": {
                "accountId": "9750XXXX4444"
            },
            "governedRegions": [
                "us-west-1",
                "us-west-2"
            ],
            "organizationStructure": {
                "sandbox": {
                    "name": "Sandbox"
                },
                "security": {
                    "name": "Security"
                }
            },
            "centralizedLogging": {
                "accountId": "012345678901",
                "configurations": {
                    "loggingBucket": {
                        "retentionDays": 60
                    },
                    "accessLoggingBucket": {
                        "retentionDays": 60
                    }
                },
                "enabled": true
            }
        },
        "status": "ACTIVE",
        "version": "3.3"
    }
}
```


Langkah 6. (Opsional) Panggil **`ListLandingZoneOperations`** API untuk melihat status operasi apa pun yang mengubah zona pendaratan Anda.

Untuk melacak status operasi zona pendaratan apa pun, Anda dapat memanggil ListLandingZoneOperations API.

Skema zona pendaratan

Landing zone adalah AWS sumber daya, yang dibuat melalui skema. Setiap versi landing zone AWS Control Tower memiliki skema unik.

Skema untuk zona pendaratan AWS Control Tower, versi 3.1 dan yang lebih baru, diterbitkan di bagian referensi ini, untuk membantu Anda memilih versi yang kompatibel.

> **Note**
>
> Masalah yang diketahui mengenai pencatatan akses yang tidak perlu ada di landing zone versi 3.0. Masalah ini diatasi di landing zone versi 3.1. Untuk informasi selengkapnya tentang perubahan, lihatZona pendaratan Menara Kontrol AWS versi 3.1.

Skema zona pendaratan 4.0

```
{
    "type": "object",
    "required": [],
    "properties": {
        "accessManagement": {
            "$ref": "#/definitions/AccessManagement"
        },
        "backup": {
            "$ref": "#/definitions/Backup"
        },
        "centralizedLogging": {
            "$ref": "#/definitions/CentralizedLogging"
        },
        "governedRegions": {
            "type": "array",
            "items": {
                "type": "string",
                "maxLength": 24,
                "minLength": 1,
                "pattern": "^[a-z]{2}-[a-z\\-]*-[0-9]{1}$",
                "additionalProperties": false
            },
```

```
            "additionalProperties": false
        },
        "securityRoles": {
            "$ref": "#/definitions/SecurityRoles"
        },
        "config": {
            "$ref": "#/definitions/Config"
        }
    },
    "additionalProperties": false,
    "definitions": {
        "AccessManagement": {
            "type": "object",
            "required": [
                "enabled"
            ],
            "properties": {
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "Backup": {
            "type": "object",
            "required": [
                "enabled"
            ],
            "properties": {
                "configurations": {
                    "$ref": "#/definitions/BackupConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false,
            "if": {
                "properties": {
                    "enabled": {
                        "const": true
                    }
```

```
                }
            },
            "then": {
                "required": [
                    "configurations"
                ]
            }
        },
        "BackupAdminConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "BackupConfigurations": {
            "type": "object",
            "required": [
                "backupAdmin",
                "centralBackup",
                "kmsKeyArn"
            ],
            "properties": {
                "backupAdmin": {
                    "$ref": "#/definitions/BackupAdminConfigurations"
                },
                "centralBackup": {
                    "$ref": "#/definitions/CentralBackupConfigurations"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                }
```

```
            },
            "additionalProperties": false
        },
        "CentralBackupConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "CentralizedLogging": {
            "type": "object",
            "required": [
                "enabled"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                },
                "configurations": {
                    "$ref": "#/definitions/LoggingConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false,
            "if": {
                "properties": {
                    "enabled": {
```

```
                    "const": true
                }
            }
        },
        "then": {
            "required": [
                "accountId"
            ]
        }
    },
    "LoggingConfigurations": {
        "type": "object",
        "properties": {
            "accessLoggingBucket": {
                "$ref": "#/definitions/S3BucketConfiguration"
            },
            "kmsKeyArn": {
                "type": "string",
                "maxLength": 2048,
                "minLength": 1,
                "additionalProperties": false
            },
            "loggingBucket": {
                "$ref": "#/definitions/S3BucketConfiguration"
            }
        },
        "additionalProperties": false
    },
    "S3BucketConfiguration": {
        "type": "object",
        "properties": {
            "retentionDays": {
                "type": "number",
                "minimum": 1,
                "additionalProperties": false
            }
        },
        "additionalProperties": false
    },
    "SecurityRoles": {
        "type": "object",
        "required": [
            "enabled"
        ],
```

```
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false,
            "if": {
                "properties": {
                    "enabled": {
                        "const": true
                    }
                }
            },
            "then": {
                "required": [
                    "accountId"
                ]
            }
        },
        "Config": {
            "type": "object",
            "required": [
                "enabled"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                },
                "configurations": {
                    "$ref": "#/definitions/ConfigConfiguration"
                },
                "enabled": {
```

```
                    "type": "boolean",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false,
            "if": {
                "properties": {
                    "enabled": {
                        "const": true
                    }
                }
            },
            "then": {
                "required": [
                    "accountId"
                ]
            }
        },
        "ConfigConfiguration": {
            "type": "object",
            "required": [],
            "properties": {
                "loggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                },
                "accessLoggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                }
            }
        }
    }
}
```

Skema zona pendaratan 3.3

```
{
    "type": "object",
```

```
    "required": [
        "centralizedLogging",
        "organizationStructure",
        "securityRoles"
    ],
    "properties": {
        "accessManagement": {
            "$ref": "#/definitions/AccessManagement"
        },
        "backup": {
            "$ref": "#/definitions/Backup"
        },
        "centralizedLogging": {
            "$ref": "#/definitions/CentralizedLogging"
        },
        "governedRegions": {
            "type": "array",
            "items": {
                "type": "string",
                "maxLength": 24,
                "minLength": 1,
                "pattern": "^[a-z]{2}-[a-z\\-]*-[0-9]{1}$",
                "additionalProperties": false
            },
            "additionalProperties": false
        },
        "organizationStructure": {
            "$ref": "#/definitions/OrganizationStructure"
        },
        "securityRoles": {
            "$ref": "#/definitions/SecurityRoles"
        }
    },
    "additionalProperties": false,
    "definitions": {
        "AccessManagement": {
            "type": "object",
            "required": [
                "enabled"
            ],
            "properties": {
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
```

```
                    "default": true
                }
            },
            "additionalProperties": false
        },
        "Backup": {
            "type": "object",
            "properties": {
                "configurations": {
                    "$ref": "#/definitions/BackupConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": false
                }
            },
            "additionalProperties": false,
            "if": {
                "properties": {
                    "enabled": {
                        "const": true
                    }
                }
            },
            "then": {
                "required": [
                    "configurations"
                ]
            }
        },
        "BackupAdminConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
```

```
            },
            "additionalProperties": false
        },
        "BackupConfigurations": {
            "type": "object",
            "required": [
                "backupAdmin",
                "centralBackup",
                "kmsKeyArn"
            ],
            "properties": {
                "backupAdmin": {
                    "$ref": "#/definitions/BackupAdminConfigurations"
                },
                "centralBackup": {
                    "$ref": "#/definitions/CentralBackupConfigurations"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "CentralBackupConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "CentralizedLogging": {
            "type": "object",
```

```
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                },
                "configurations": {
                    "$ref": "#/definitions/LoggingConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": true
                }
            },
            "additionalProperties": false
        },
        "LoggingConfigurations": {
            "type": "object",
            "properties": {
                "accessLoggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                },
                "loggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                }
            },
            "additionalProperties": false
        },
        "OrganizationalUnit": {
            "type": "object",
            "required": [
                "name"
```

```
            ],
            "properties": {
                "name": {
                    "type": "string",
                    "maxLength": 120,
                    "minLength": 1,
                    "pattern": "^[\\s\\S]*$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "OrganizationStructure": {
            "type": "object",
            "required": [
                "security"
            ],
            "properties": {
                "sandbox": {
                    "$ref": "#/definitions/OrganizationalUnit"
                },
                "security": {
                    "$ref": "#/definitions/OrganizationalUnit"
                }
            },
            "additionalProperties": false
        },
        "S3BucketConfiguration": {
            "type": "object",
            "properties": {
                "retentionDays": {
                    "type": "number",
                    "minimum": 1,
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "SecurityRoles": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
```

```
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        }
    }
}
```

Skema zona pendaratan 3.2

```
{
    "type": "object",
    "required": [
        "centralizedLogging",
        "organizationStructure",
        "securityRoles"
    ],
    "properties": {
        "accessManagement": {
            "$ref": "#/definitions/AccessManagement"
        },
        "backup": {
            "$ref": "#/definitions/Backup"
        },
        "centralizedLogging": {
            "$ref": "#/definitions/CentralizedLogging"
        },
        "governedRegions": {
            "type": "array",
            "items": {
                "type": "string",
                "maxLength": 24,
                "minLength": 1,
                "pattern": "^[a-z]{2}-[a-z\\-]*-[0-9]{1}$",
                "additionalProperties": false
            },
            "additionalProperties": false
        },
```

```
        "organizationStructure": {
            "$ref": "#/definitions/OrganizationStructure"
        },
        "securityRoles": {
            "$ref": "#/definitions/SecurityRoles"
        }
    },
    "additionalProperties": false,
    "definitions": {
        "AccessManagement": {
            "type": "object",
            "required": [
                "enabled"
            ],
            "properties": {
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": true
                }
            },
            "additionalProperties": false
        },
        "Backup": {
            "type": "object",
            "properties": {
                "configurations": {
                    "$ref": "#/definitions/BackupConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": false
                }
            },
            "additionalProperties": false,
            "if": {
                "properties": {
                    "enabled": {
                        "const": true
                    }
                }
            },
            "then": {
```

```
                "required": [
                    "configurations"
                ]
            }
        },
        "BackupAdminConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "BackupConfigurations": {
            "type": "object",
            "required": [
                "backupAdmin",
                "centralBackup",
                "kmsKeyArn"
            ],
            "properties": {
                "backupAdmin": {
                    "$ref": "#/definitions/BackupAdminConfigurations"
                },
                "centralBackup": {
                    "$ref": "#/definitions/CentralBackupConfigurations"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
```

```
        "CentralBackupConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "CentralizedLogging": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                },
                "configurations": {
                    "$ref": "#/definitions/LoggingConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": true
                }
            },
            "additionalProperties": false
        },
        "LoggingConfigurations": {
            "type": "object",
            "properties": {
                "accessLoggingBucket": {
```

```
                    "$ref": "#/definitions/S3BucketConfiguration"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                },
                "loggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                }
            },
            "additionalProperties": false
        },
        "OrganizationalUnit": {
            "type": "object",
            "required": [
                "name"
            ],
            "properties": {
                "name": {
                    "type": "string",
                    "maxLength": 120,
                    "minLength": 1,
                    "pattern": "^[\\s\\S]*$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "OrganizationStructure": {
            "type": "object",
            "required": [
                "security"
            ],
            "properties": {
                "sandbox": {
                    "$ref": "#/definitions/OrganizationalUnit"
                },
                "security": {
                    "$ref": "#/definitions/OrganizationalUnit"
                }
            },
            "additionalProperties": false
```

```
        },
        "S3BucketConfiguration": {
            "type": "object",
            "properties": {
                "retentionDays": {
                    "type": "number",
                    "minimum": 1,
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "SecurityRoles": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        }
    }
}
```

Skema zona pendaratan 3.1

```
{
    "type": "object",
    "required": [
        "centralizedLogging",
        "organizationStructure",
        "securityRoles"
    ],
    "properties": {
        "accessManagement": {
            "$ref": "#/definitions/AccessManagement"
```

```
        },
        "backup": {
            "$ref": "#/definitions/Backup"
        },
        "centralizedLogging": {
            "$ref": "#/definitions/CentralizedLogging"
        },
        "governedRegions": {
            "type": "array",
            "items": {
                "type": "string",
                "maxLength": 24,
                "minLength": 1,
                "pattern": "^[a-z]{2}-[a-z\\-]*-[0-9]{1}$",
                "additionalProperties": false
            },
            "additionalProperties": false
        },
        "organizationStructure": {
            "$ref": "#/definitions/OrganizationStructure"
        },
        "securityRoles": {
            "$ref": "#/definitions/SecurityRoles"
        }
    },
    "additionalProperties": false,
    "definitions": {
        "AccessManagement": {
            "type": "object",
            "required": [
                "enabled"
            ],
            "properties": {
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": true
                }
            },
            "additionalProperties": false
        },
        "Backup": {
            "type": "object",
            "properties": {
```

```
                "configurations": {
                    "$ref": "#/definitions/BackupConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": false
                }
            },
            "additionalProperties": false,
            "if": {
                "properties": {
                    "enabled": {
                        "const": true
                    }
                }
            },
            "then": {
                "required": [
                    "configurations"
                ]
            }
        },
        "BackupAdminConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "BackupConfigurations": {
            "type": "object",
            "required": [
                "backupAdmin",
                "centralBackup",
```

```
                "kmsKeyArn"
            ],
            "properties": {
                "backupAdmin": {
                    "$ref": "#/definitions/BackupAdminConfigurations"
                },
                "centralBackup": {
                    "$ref": "#/definitions/CentralBackupConfigurations"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "CentralBackupConfigurations": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                }
            },
            "additionalProperties": false
        },
        "CentralizedLogging": {
            "type": "object",
            "required": [
                "accountId"
            ],
            "properties": {
                "accountId": {
                    "type": "string",
                    "maxLength": 12,
                    "minLength": 12,
```

```
                    "pattern": "^\\d{12}$",
                    "additionalProperties": false
                },
                "configurations": {
                    "$ref": "#/definitions/LoggingConfigurations"
                },
                "enabled": {
                    "type": "boolean",
                    "additionalProperties": false,
                    "default": true
                }
            },
            "additionalProperties": false
        },
        "LoggingConfigurations": {
            "type": "object",
            "properties": {
                "accessLoggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                },
                "kmsKeyArn": {
                    "type": "string",
                    "maxLength": 2048,
                    "minLength": 1,
                    "additionalProperties": false
                },
                "loggingBucket": {
                    "$ref": "#/definitions/S3BucketConfiguration"
                }
            },
            "additionalProperties": false
        },
        "OrganizationalUnit": {
            "type": "object",
            "required": [
                "name"
            ],
            "properties": {
                "name": {
                    "type": "string",
                    "maxLength": 120,
                    "minLength": 1,
                    "pattern": "^[\\s\\S]*$",
                    "additionalProperties": false
```

```
            }
        },
        "additionalProperties": false
    },
    "OrganizationStructure": {
        "type": "object",
        "required": [
            "security"
        ],
        "properties": {
            "sandbox": {
                "$ref": "#/definitions/OrganizationalUnit"
            },
            "security": {
                "$ref": "#/definitions/OrganizationalUnit"
            }
        },
        "additionalProperties": false
    },
    "S3BucketConfiguration": {
        "type": "object",
        "properties": {
            "retentionDays": {
                "type": "number",
                "minimum": 1,
                "additionalProperties": false
            }
        },
        "additionalProperties": false
    },
    "SecurityRoles": {
        "type": "object",
        "required": [
            "accountId"
        ],
        "properties": {
            "accountId": {
                "type": "string",
                "maxLength": 12,
                "minLength": 12,
                "pattern": "^\\d{12}$",
                "additionalProperties": false
            }
        },
```

```
            "additionalProperties": false
        }
    }
}
```

Luncurkan landing zone menggunakan CloudFormation

Anda dapat mengonfigurasi dan meluncurkan landing zone dengan CloudFormation baik melalui CloudFormation konsol, atau melalui AWS CLI. Bagian ini memberikan instruksi dan contoh untuk meluncurkan landing zone menggunakan API CloudFormation.

Topik

- Prasyarat untuk meluncurkan landing zone menggunakan CloudFormation
- Buat landing zone baru menggunakan CloudFormation
- Mengelola landing zone yang ada menggunakan CloudFormation

Prasyarat untuk meluncurkan landing zone menggunakan CloudFormation

1. Dari AWS CLI, gunakan AWS Organizations `CreateOrganization` API untuk membuat organisasi dan mengaktifkan semua fitur.

   Untuk instruksi yang lebih rinci, tinjauLangkah 1: Konfigurasikan landing zone.
2. Dari CloudFormation konsol atau menggunakan AWS CLI, gunakan CloudFormation templat yang membuat sumber daya berikut di akun manajemen:
   - Akun Log Archive (kadang-kadang disebut akun “Logging”)
   - Akun audit (kadang-kadang disebut akun “Keamanan”)
   - Peran AWSControlTowerAdminAWSControlTowerCloudTrailRole, AWSControlTowerConfigAggregatorRoleForOrganizations,, dan AWSControlTowerStackSetRolelayanan.

     Untuk informasi tentang cara AWS Control Tower menggunakan peran ini untuk melakukan panggilan API landing zone, lihat Langkah 1: Mengonfigurasi landing zone Anda.

```
Parameters:
  LoggingAccountEmail:
    Type: String
    Description: The email Id for centralized logging account
  LoggingAccountName:
```

```
    Type: String
    Description: Name for centralized logging account
  SecurityAccountEmail:
    Type: String
    Description: The email Id for security roles account
  SecurityAccountName:
    Type: String
    Description: Name for security roles account
Resources:
  MyOrganization:
    Type: 'AWS::Organizations::Organization'
    Properties:
      FeatureSet: ALL
  LoggingAccount:
    Type: 'AWS::Organizations::Account'
    Properties:
      AccountName: !Ref LoggingAccountName
      Email: !Ref LoggingAccountEmail
  SecurityAccount:
    Type: 'AWS::Organizations::Account'
    Properties:
      AccountName: !Ref SecurityAccountName
      Email: !Ref SecurityAccountEmail
  AWSControlTowerAdmin:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerAdmin
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: controltower.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
      ManagedPolicyArns:
        - !Sub >-
          arn:${AWS::Partition}:iam::aws:policy/service-role/
AWSControlTowerServiceRolePolicy
  AWSControlTowerAdminPolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyName: AWSControlTowerAdminPolicy
      PolicyDocument:
```

```
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Action: 'ec2:DescribeAvailabilityZones'
            Resource: '*'
      Roles:
        - !Ref AWSControlTowerAdmin
  AWSControlTowerCloudTrailRole:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerCloudTrailRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: cloudtrail.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
  AWSControlTowerCloudTrailRolePolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyName: AWSControlTowerCloudTrailRolePolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Action:
              - 'logs:CreateLogStream'
              - 'logs:PutLogEvents'
            Resource: !Sub >-
              arn:${AWS::Partition}:logs:*:*:log-group:aws-controltower/
CloudTrailLogs:*
            Effect: Allow
      Roles:
        - !Ref AWSControlTowerCloudTrailRole
  AWSControlTowerConfigAggregatorRoleForOrganizations:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerConfigAggregatorRoleForOrganizations
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
```

```
              Service: config.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
      ManagedPolicyArns:
        - !Sub arn:${AWS::Partition}:iam::aws:policy/service-role/
AWSConfigRoleForOrganizations
  AWSControlTowerStackSetRole:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSControlTowerStackSetRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: cloudformation.amazonaws.com
            Action: 'sts:AssumeRole'
      Path: '/service-role/'
  AWSControlTowerStackSetRolePolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyName: AWSControlTowerStackSetRolePolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Action: 'sts:AssumeRole'
            Resource: !Sub 'arn:${AWS::Partition}:iam::*:role/
AWSControlTowerExecution'
            Effect: Allow
      Roles:
        - !Ref AWSControlTowerStackSetRole

Outputs:
  LogAccountId:
    Value:
      Fn::GetAtt: LoggingAccount.AccountId
    Export:
      Name: LogAccountId
  SecurityAccountId:
    Value:
      Fn::GetAtt: SecurityAccount.AccountId
    Export:
      Name: SecurityAccountId
```

Buat landing zone baru menggunakan CloudFormation

Dari CloudFormation konsol atau menggunakan AWS CLI, gunakan CloudFormation template berikut untuk membuat landing zone.

```
Parameters:
  Version:
    Type: String
    Description: The version number of Landing Zone
  GovernedRegions:
    Type: CommaDelimitedList
    Description: List of governed regions
  SecurityOuName:
    Type: String
    Description: The security Organizational Unit name
  SandboxOuName:
    Type: String
    Description: The sandbox Organizational Unit name
  CentralizedLoggingAccountId:
    Type: String
    Description: The AWS account ID for centralized logging
  SecurityAccountId:
    Type: String
    Description: The AWS account ID for security roles
  LoggingBucketRetentionPeriod:
    Type: Number
    Description: Retention period for centralized logging bucket
  AccessLoggingBucketRetentionPeriod:
    Type: Number
    Description: Retention period for access logging bucket
  KMSKey:
    Type: String
    Description: KMS key ARN used by CloudTrail and Config service to encrypt data in
 logging bucket
Resources:
  MyLandingZone:
    Type: 'AWS::ControlTower::LandingZone'
    Properties:
      Version:
        Ref: Version
      Tags:
        - Key: "keyname1"
          Value: "value1"
```

```
        - Key: "keyname2"
          Value: "value2"
      Manifest:
        governedRegions:
          Ref: GovernedRegions
        organizationStructure:
          security:
            name:
              Ref: SecurityOuName
          sandbox:
            name:
              Ref: SandboxOuName
        centralizedLogging:
          accountId:
            Ref: CentralizedLoggingAccountId
          configurations:
            loggingBucket:
              retentionDays:
                Ref: LoggingBucketRetentionPeriod
            accessLoggingBucket:
              retentionDays:
                Ref: AccessLoggingBucketRetentionPeriod
            kmsKeyArn:
              Ref: KMSKey
          enabled: true
        securityRoles:
          accountId:
            Ref: SecurityAccountId
        accessManagement:
          enabled: true
```

Mengelola landing zone yang ada menggunakan CloudFormation

Anda dapat menggunakan CloudFormation untuk mengelola landing zone yang telah diluncurkan dengan mengimpor landing zone di CloudFormation tumpukan baru atau yang sudah ada. Tinjau Membawa sumber daya yang ada ke dalam CloudFormation manajemen untuk detail dan instruksi.

Untuk mendeteksi dan menyelesaikan drift dalam landing zone, Anda dapat menggunakan konsol AWS Control Tower, the AWS CLI, atau `ResetLandingZone`API.

Langkah selanjutnya

Sekarang zona pendaratan Anda diatur, itu siap digunakan.

Untuk mempelajari selengkapnya tentang cara menggunakan AWS Control Tower, lihat topik berikut:

- Untuk praktik administrasi yang direkomendasikan, lihat Praktik Terbaik.
- Anda dapat mengatur pengguna dan grup Pusat Identitas IAM dengan peran dan izin tertentu. Untuk rekomendasi, lihatRekomendasi untuk menyiapkan grup, peran, dan kebijakan.
- Untuk mulai mendaftarkan organisasi dan akun dari penerapan Anda AWS Organizations , lihat Mengatur organisasi dan akun yang ada.
- Pengguna akhir Anda dapat menyediakan AWS akun mereka sendiri di zona pendaratan menggunakan Account Factory. Untuk informasi selengkapnya, lihat Izin untuk mengonfigurasi dan menyediakan akun.
- Untuk memastikanValidasi Kepatuhan untuk AWS Control Tower, administrator cloud pusat Anda dapat meninjau arsip log di akun Arsip Log, dan auditor pihak ketiga yang ditunjuk dapat meninjau informasi audit di akun Audit (bersama), yang merupakan anggota OU Keamanan.
- Untuk mempelajari selengkapnya tentang kemampuan AWS Control Tower, lihat Informasi terkait.
- Dari waktu ke waktu, Anda mungkin perlu memperbarui zona pendaratan Anda untuk mendapatkan pembaruan backend terbaru, kontrol terbaru, dan untuk menjaga zona pendaratan Anda tetap mutakhir. Untuk informasi selengkapnya, lihat Manajemen pembaruan konfigurasi di AWS Control Tower.
- Jika Anda mengalami masalah saat menggunakan AWS Control Tower, lihatPemecahan Masalah.

> **Important**
>
> Jika Anda belum mengaktifkan MFA untuk pengguna root akun Anda, lakukan sekarang. Untuk informasi selengkapnya tentang praktik terbaik untuk pengguna root, lihat Praktik terbaik untuk melindungi pengguna root akun Anda.

Batasan dan kuota di AWS Control Tower

Bab ini mencakup batasan dan kuota AWS layanan yang harus Anda ingat saat menggunakan AWS Control Tower. Jika Anda tidak dapat mengatur zona pendaratan karena masalah kuota layanan, hubungi AWS Dukungan.

Untuk informasi selengkapnya tentang batasan yang khusus untuk kontrol, lihatBatasan kontrol.

> **Panduan Referensi Kontrol**
>
> Informasi terperinci tentang kontrol AWS Control Tower telah dipindahkan ke Panduan Referensi Kontrol Menara Kontrol AWS.

Keterbatasan yang diketahui di AWS Control Tower

Bagian ini menjelaskan batasan yang diketahui dan kasus penggunaan yang tidak didukung di AWS Control Tower.

- AWS Control Tower memiliki batasan konkur ensi secara keseluruhan. Secara umum, satu operasi pada satu waktu diizinkan. Dua pengecualian untuk batasan ini diperbolehkan:
  - Kontrol opsional dapat diaktifkan dan dinonaktifkan secara bersamaan, melalui proses asinkron. Hingga seratus (100) operasi terkait kontrol pada satu waktu dapat berlangsung, secara total, tidak peduli apakah mereka dipanggil dari konsol atau dari API.
  - Akun dapat disediakan, diperbarui, dan didaftarkan secara bersamaan di Account Factory, melalui proses asinkron, dengan hingga lima (5) operasi terkait akun yang sedang berlangsung secara bersamaan. Akun yang tidak dikelola harus dilakukan satu akun pada satu waktu.
    - Dengan pendaftaran otomatis diaktifkan, hanya operasi akun pemindahan tunggal yang dapat dilakukan pada OU tujuan dan operasi terkait akun tambahan pada OU yang sama akan dianggap bertentangan hingga operasi akun pemindahan selesai.
  - Account Factory for Terraform (AFT) memiliki parameter konkurensi tambahan yang dikonfigurasi selama penerapan. AWS telah menguji AFT dengan nilai default berikut:
    - `concurrent_account_factory_actions`: 5 (penyediaan akun)
    - `maximum_concurrent_customizations`: 5 (pipa kustomisasi)

    Meningkatkan batas ini di luar default yang diuji dapat mengurangi stabilitas.

- Alamat email akun bersama di OU Keamanan dapat diubah, tetapi Anda harus memperbarui zona pendaratan untuk melihat perubahan ini di konsol AWS Control Tower.
- Batas sepuluh (10) SCP per OU berlaku untuk OU di zona pendaratan AWS Control Tower Anda.
- AWS Control Tower mendukung hingga 10.000 akun di organisasi zona pendaratan Anda, dibagi di antara semua OU Anda.
- OU yang ada dengan lebih dari 1000 akun bersarang langsung tidak dapat didaftarkan atau didaftarkan ulang di AWS Control Tower. Untuk informasi selengkapnya tentang batasan pendaftaran OU, lihatKeterbatasan berdasarkan yang mendasarinya AWS layanan.
- Kustomisasi untuk AWS Control Tower (CfCT) tidak tersedia dalam hal ini Wilayah AWS, karena beberapa dependensi tidak tersedia:
  - Eropa (Zurich), eu-central-2
  - Eropa (Spanyol), eu-selatan-2
  - Kanada Barat (Calgary) ca-west-1
  - Asia Pasifik (Melbourne), ap-Southeast-4
  - Asia Pasifik (Malaysia), ap-Southeast-5
  - Asia Pasifik (Thailand), ap-southeast-7
  - Meksiko (Tengah), mx-central-1
  - Asia Pasifik (Selandia Baru), ap-southeast-6
  - Asia Pasifik (Taipei), ap-east-2
  - AWS Awan Berdaulat Eropa (Jerman), eusc-de-east-1

  Anda dapat menerapkan dan mengelola sumber daya di Wilayah ini dengan cFCT, jika Anda menerapkan cFCT ke Wilayah rumah Menara Kontrol AWS Anda, tetapi Anda tidak dapat membangun cFCT di Wilayah ini.
- AWS Control Tower Account Factory for Terraform (AFT) tidak tersedia di bawah ini Wilayah AWS, karena beberapa dependensi tidak tersedia:
  - Eropa (Zurich), eu-central-2
  - Eropa (Spanyol), eu-selatan-2
  - Kanada Barat (Calgary), ca-west-1
  - Asia Pasifik (Melbourne), ap-Southeast-4
  - Asia Pasifik (Malaysia), ap-Southeast-5
  - Asia Pasifik (Thailand), ap-southeast-7

  - Meksiko (Tengah), mx-central-1
  - Asia Pasifik (Selandia Baru), ap-southeast-6
  - Asia Pasifik (Taipei), ap-east-2
  - AWS Awan Berdaulat Eropa (Jerman), eusc-de-east-1
- AWS Control Tower Account Factory for Terraform (AFT) tidak dapat digunakan oleh pelanggan AFT baru di Wilayah berikut, karena tidak AWS CodeConnections tersedia untuk terhubung ke sistem kontrol versi pihak ketiga (VCS):
  - Asia Pasifik (Hong Kong), Afrika (Cape Town), Timur Tengah (Bahrain), Eropa (Zurich), Asia Pasifik (Jakarta), Asia Pasifik (Hyderabad), Asia Pasifik (Osaka), Asia Pasifik (Melbourne), Israel (Tel Aviv), Eropa (Spanyol), Timur Tengah (UEA), Asia Pasifik (Thailand), Meksiko (Tengah)
- Wilayah berikut tidak mendukung AWS Service Catalog.
  - Kanada Barat (Calgary), ca-west-1
  - Asia Pasifik (Malaysia), ap-Southeast-5
  - Asia Pasifik (Thailand), ap-southeast-7
  - Meksiko (Tengah), mx-central-1
  - Asia Pasifik (Selandia Baru), ap-southeast-6
  - Asia Pasifik (Taipei), ap-east-2
  - AWS Awan Berdaulat Eropa (Jerman), eusc-de-east-1

> **Note**
>
> Wilayah yang tidak mendukung Katalog Layanan tidak mendukung Kustomisasi Pabrik Akun untuk AWS Control Tower (AFC).

  Untuk informasi selengkapnya tentang fungsionalitas AWS Control Tower di Wilayah yang tidak mendukung AWS Service Catalog, lihatAWS Control Tower tersedia di AWS Kanada Barat (Calgary).
- Saat memanggil API kontrol untuk mengaktifkan atau menonaktifkan kontrol, batas `EnableControl` dan `DisableControl` pembaruan di AWS Control Tower adalah seratus (100) operasi bersamaan. Sepuluh operasi (10) dapat berlangsung secara bersamaan, dengan operasi yang tersisa mengantri. Anda mungkin perlu menyesuaikan kode Anda untuk menunggu penyelesaian.

- Saat Anda menyediakan akun melalui Kustomisasi Pabrik Akun (AFC), dengan cetak biru yang berbasis di Terraform, Anda dapat menerapkan cetak biru tersebut hanya ke satu. Wilayah AWS Secara default, AWS Control Tower diterapkan ke Wilayah asal.

Meminta peningkatan kuota

Konsol Kuota Layanan menyediakan informasi tentang kuota AWS Control Tower. Anda dapat menggunakan konsol Service Quotas untuk melihat kuota layanan default atau mengajukan penambahan kuota untuk kuota yang dapat disesuaikan.

> **Note**
>
> Akun dan organisasi yang baru dibuat mungkin mengalami kuota di bawah default 10 akun.

Kuota berikut dapat dilihat melalui konsol Kuota Layanan

- Kuota operasi akun bersamaan: Jumlah maksimum operasi akun bersamaan yang dapat dilakukan secara bersamaan. Default: 5, Maksimum: 10, dapat disesuaikan
- Jumlah akun dalam satu OU: Jumlah maksimum akun terkelola AWS Control Tower yang dapat hadir dalam satu OU. Jika Anda menambahkan akun di luar batas ini, proses pendaftaran OU di AWS Control Tower tidak dapat dilakukan. Untuk mempelajari lebih lanjut tentang jumlah akun per OU, tinjau Keterbatasan berdasarkan yang mendasarinya AWS layanan dalam dokumentasi AWS Control Tower. Default: 1000, tidak dapat disesuaikan.
- Operasi bersamaan untuk unit organisasi (OU): Jumlah maksimum OU-related operasi bersamaan yang dapat dilakukan pada waktu yang sama. Default: 1, tidak dapat disesuaikan.

Misalnya, Anda dapat meminta peningkatan kuota dari lima hingga sepuluh operasi terkait akun bersamaan. Beberapa karakteristik kinerja AWS Control Tower dapat berubah setelah peningkatan kuota. Misalnya, mungkin perlu waktu lebih lama untuk memperbarui OU ketika Anda memiliki lebih banyak akun di dalamnya. Atau, mungkin perlu waktu lebih lama untuk menyelesaikan tindakan pada OU dengan lima SCP daripada dengan tiga SCP.

> **Note**
>
> Permintaan kenaikan kuota layanan mungkin memerlukan waktu hingga dua hari sebelum berlaku. Pastikan untuk meminta kenaikan kuota dari Wilayah rumah AWS Control Tower Anda.

Sebagai alternatif, Anda dapat menghubungi AWS Dukungan untuk meminta peningkatan kuota untuk beberapa sumber daya di AWS Control Tower. Atau Anda dapat melihat video berikut, dan mempelajari cara mengotomatiskan kenaikan kuota layanan tertentu.

Video: Otomatisasi permintaan kenaikan kuota layanan, dalam layanan yang terkait dengan AWS Control Tower

Video ini (7:24) menjelaskan cara mengotomatiskan peningkatan kuota layanan untuk AWS layanan terintegrasi terkait, berdasarkan penerapan di AWS Control Tower. Ini juga menunjukkan cara mengotomatiskan pendaftaran akun baru ke dukungan AWS Enterprise untuk organisasi Anda. Untuk tampilan yang lebih baik, pilih ikon di sudut kanan bawah video untuk memperbesarnya ke layar penuh. Keterangan tersedia.

Panduan Video Peningkatan Kuota di Menara Kontrol AWS.

Saat menyediakan akun baru di lingkungan ini, Anda dapat menggunakan peristiwa siklus hidup untuk memicu permintaan otomatis untuk peningkatan kuota layanan yang ditentukan Wilayah AWS.

Informasi lebih lanjut AWS tentang kuota tersedia di Refer AWS ensi Umum.

Batasan kontrol

AWS Control Tower membantu Anda menjaga lingkungan multi-akun yang aman AWS melalui kontrol, yang diterapkan dalam berbagai bentuk, seperti kebijakan kontrol layanan (SCP), AWS Config aturan, dan CloudFormation kait.

> **Panduan Referensi Kontrol**
>
> Informasi terperinci tentang kontrol AWS Control Tower telah dipindahkan ke Panduan Referensi Kontrol Menara Kontrol AWS.

Jika Anda memodifikasi sumber daya AWS Control Tower, seperti SCP, atau menghapus AWS Config sumber daya apa pun, seperti perekam atau agregator Config, AWS Control Tower tidak dapat lagi menjamin bahwa kontrol berfungsi seperti yang dirancang. Oleh karena itu, keamanan lingkungan multi-akun Anda mungkin terganggu. Model keamanan tanggung jawab AWS bersama berlaku untuk setiap perubahan yang mungkin Anda buat.

> **Note**
>
> AWS Control Tower membantu menjaga integritas lingkungan Anda dengan mengatur ulang SCP dari kontrol preventif ke konfigurasi standarnya saat Anda memperbarui zona pendaratan. Perubahan yang mungkin telah Anda buat pada SCP diganti dengan versi standar kontrol, berdasarkan desain.

Batasan menurut Wilayah

Beberapa kontrol di AWS Control Tower tidak beroperasi di Wilayah AWS mana AWS Control Tower tersedia, karena Wilayah tersebut tidak mendukung fungsionalitas dasar yang diperlukan. Akibatnya, ketika Anda menerapkan kontrol itu, kontrol tersebut mungkin tidak beroperasi di semua Wilayah yang Anda atur dengan AWS Control Tower. Batasan ini memengaruhi kontrol detektif tertentu, kontrol proaktif tertentu, dan kontrol tertentu di Security Hub CSPM Service-managed Standard: AWS Control Tower. Untuk informasi selengkapnya tentang ketersediaan Regional, lihat kontrol Hub Keamanan. Lihat juga dokumentasi daftar layanan Regional dan dokumentasi referensi kontrol Security Hub CSPM.

Perilaku kontrol juga terbatas dalam kasus tata kelola campuran. Untuk informasi selengkapnya, lihat Hindari tata kelola campuran saat mengonfigurasi Wilayah.

Untuk informasi selengkapnya tentang cara AWS Control Tower mengelola batasan Wilayah dan kontrol, lihatPertimbangan untuk mengaktifkan AWS Wilayah opt-in.

> **Note**
>
> Untuk informasi terbaru tentang kontrol dan dukungan Wilayah, kami sarankan Anda memanggil operasi `GetControl` dan `ListControls` API.

Temukan kontrol dan Wilayah yang tersedia

Anda dapat melihat Wilayah yang tersedia untuk setiap kontrol di konsol AWS Control Tower. Anda dapat melihat Wilayah yang tersedia secara terprogram dengan `ListControls` API `GetControl` dan dari Katalog AWS Kontrol.

Untuk informasi tentang AWS Security Hub CSPM kontrol dari Service-Managed Standar: Menara Kontrol AWS yang tidak didukung di wilayah tertentu Wilayah AWS, lihat “Wilayah Tidak Didukung” di standar CSP M Hub Keamanan.

Keterbatasan berdasarkan yang mendasarinya AWS layanan

Halaman ini menjelaskan batasan yang mungkin Anda temui karena keterbatasan dalam AWS layanan lain, dan cara AWS Control Tower bekerja dengan layanan tersebut.

Pedoman umum

Sebagai aturan umum, kami berharap bahwa jumlah akun yang didukung saat mendaftarkan OU berkurang saat Anda meningkatkan jumlah Wilayah yang diatur, dan jumlah kontrol yang diaktifkan, untuk OU tersebut. Pedoman umum ini mengasumsikan bahwa Anda memiliki 15 kontrol opsional yang diaktifkan. Jika Anda memiliki lebih banyak atau lebih sedikit kontrol yang diaktifkan pada OU Anda, batas akun per OU akan berbeda saat mendaftar.

- Dengan 15 Wilayah yang diatur, OU hingga 1000 akun didukung.
- Dengan 16 hingga 21 Wilayah yang diatur, ukuran OU maksimum yang didukung berada di kisaran 600-1000 akun.
- Dengan 22 Wilayah yang diatur, OU hingga 680 akun didukung.
- Dengan 23 atau lebih Wilayah yang diatur, ukuran OU maksimum yang didukung kurang dari 680 akun.

Jika terjadi kesalahan

Jika pendaftaran gagal, Anda dapat mencoba Re-register ke OU. Juga, Anda dapat membuat OU lebih kecil dengan menggunakan OU bersarang atau dengan memindahkan akun ke OU lain.

> **Note**
>
> Kontrol wajib yang selalu diberlakukan AWS Control Tower tidak dihitung dalam jumlah kontrol yang telah Anda aktifkan pada OU, untuk tujuan pendaftaran.

CloudFormation batasan set tumpukan

Jika Anda berencana untuk mendaftarkan sejumlah besar akun di beberapa akun Wilayah AWS, Anda mungkin menemukan batasan yang dibuat CloudFormation oleh kumpulan tumpukan pada ukuran keseluruhan organisasi. Anda dapat memperkirakan batasannya dengan rumus ini:

Jumlah akun terkelola dalam organisasi x Jumlah Wilayah yang diatur <= 150.000

Keterbatasan ini menjadi jelas selama proses pendaftaran OU. Misalnya, jika 15 Wilayah diatur, dan 15 kontrol opsional diaktifkan, batas untuk mendaftarkan OU adalah 1000 akun. Namun, jika Anda perlu mendaftarkan OU dengan lebih dari 1000 akun, atau jika Anda mengaktifkan sejumlah besar kontrol opsional, Anda harus mengurangi jumlah Wilayah yang diatur di bawah 15. Pengurangan ini disebabkan oleh batasan set tumpukan.

AWS Config keterbatasan

Jika Anda berencana untuk mendaftarkan OU dengan sejumlah besar akun, Anda mungkin menemukan batasan dengan jumlah maksimum akun yang AWS Config memungkinkan untuk dibuat atau dihapus setiap minggu, di semua agregator. Akun terdaftar tidak dihitung dalam batas ini: Anda dapat mendaftarkan hingga 1000 akun baru ke AWS Control Tower setiap minggu.

First-time batasan untuk akun dan Wilayah opt-in

Jika Anda berencana untuk mendaftarkan OU dengan sejumlah besar akun di beberapa Wilayah pilihan untuk pertama kalinya, Anda mungkin mengalami keterbatasan karena kuota Manajemen Akun, yang dapat menyebabkan latensi yang berkepanjangan. Kesalahan dapat terjadi selama pendaftaran OU karena latensi.

Perbedaan regional untuk fungsionalitas AWS Control Tower

Ada perbedaan tertentu dalam perilaku Menara Kontrol AWS di seluruh Wilayah AWS, karena AWS Control Tower mengatur perilaku AWS layanan lain. Contoh:

- AWS Service Catalog tidak tersedia di semua Wilayah AWS tempat AWS Control Tower tersedia, yang mengubah perilaku Account Factory di Wilayah tersebut.
- Di Wilayah tertentu, Kustomisasi Pabrik Akun (AFC) tidak tersedia karena Katalog Layanan tidak tersedia untuk mendukung fungsionalitas dasar untuk cetak biru.
- Kontrol tertentu tidak tersedia sama sekali Wilayah AWS karena kurangnya fungsionalitas yang mendasarinya.
- AFT dan CFCT tidak tersedia sama sekali Wilayah AWS karena kurangnya fungsionalitas yang mendasarinya.

Untuk membuat penentuan perilaku terbaik untuk lingkungan Menara Kontrol AWS Anda, pastikan Wilayah asal Anda. Kemudian, evaluasi item berikut. Untuk detail selengkapnya, lihat Batasan dan kuota di AWS Control Tower.

- Apakah AWS Service Catalog tersedia di Wilayah rumah yang Anda inginkan?
- Apakah kontrol tersedia yang Anda butuhkan? Lihat Batasan kontrol.
- Apakah IAM Identity Center tersedia di Wilayah rumah yang Anda inginkan?

Wilayah yang Dapat Digunakan untuk kontrol

AWS Control Tower tidak dapat mengaktifkan kontrol tertentu saat Anda menyebarkannya di Wilayah tertentu, karena kurangnya dependensi yang mendasarinya. Anda dapat menemukan informasi terbaru tentang Wilayah yang dapat diterapkan untuk kontrol apa pun dengan memanggil API `ListControls` and`GetControl`. Anda juga dapat melihat Wilayah yang dapat digunakan di konsol AWS Control Tower.

Saat Anda mengaktifkan kontrol pada OU yang diatur oleh AWS Control Tower, area efektif kontrol adalah persimpangan Wilayah yang diatur Menara Kontrol AWS Anda dengan Wilayah kontrol yang dapat diterapkan.

Misalnya, kontrol dapat diaktifkan pada OU yang beroperasi di Wilayah X, Y dan Z yang diatur. Tetapi setelah diaktifkan, kontrol yang sama hanya digunakan pada Wilayah X dan Z, karena kontrol itu sendiri tidak mendukung Wilayah Y.

Penting untuk memantau hubungan antara kontrol yang Anda terapkan dan Wilayah tempat Anda mengoperasikan beban kerja di AWS Control Tower, sehingga Anda tidak mengalami celah dalam perlindungan sumber AWS daya Anda.

Cara memeriksa Wilayah yang dilindungi

- Di konsol AWS Control Tower, Anda dapat melihat kontrol dan Wilayah yang diaktifkan di bagian Kontrol yang diaktifkan.
- Jika Anda memanggil `GetEnabledControl` API, parameter targetRegions hanya akan menampilkan Regions tempat Anda dapat menerapkan kontrol secara efektif, bukan Regions yang tidak dapat digunakan.

Panduan Referensi Kontrol Menara Kontrol AWS

Informasi terperinci tentang kontrol di AWS Control Tower telah dipindahkan ke Panduan Referensi Kontrol Menara Kontrol AWS.

Praktik terbaik untuk administrator AWS Control Tower

Topik ini ditujukan terutama untuk administrator akun manajemen.

Administrator akun manajemen bertanggung jawab untuk menjelaskan beberapa tugas yang dikendalikan AWS Control Tower mencegah administrator akun anggota mereka melakukannya. Topik ini menjelaskan beberapa praktik dan prosedur terbaik untuk mentransfer pengetahuan ini, dan memberikan tips lain untuk menyiapkan dan memelihara lingkungan AWS Control Tower Anda secara efisien.

Menjelaskan akses ke pengguna

Konsol AWS Control Tower hanya tersedia untuk pengguna dengan izin administrator akun manajemen. Hanya pengguna ini yang dapat melakukan pekerjaan administratif di dalam landing zone Anda. Sesuai dengan praktik terbaik, ini berarti bahwa sebagian besar pengguna dan administrator akun anggota Anda tidak akan pernah melihat konsol AWS Control Tower. Sebagai anggota grup administrator akun manajemen, Anda bertanggung jawab untuk menjelaskan informasi berikut kepada pengguna dan administrator akun anggota Anda, sebagaimana mestinya.

- Jelaskan AWS sumber daya mana yang dapat diakses pengguna dan administrator di dalam landing zone.
- Buat daftar kontrol pencegahan yang berlaku untuk setiap unit organisasi (OU) sehingga administrator lain dapat merencanakan dan melaksanakan AWS beban kerja mereka sesuai dengan itu.

Menjelaskan akses sumber daya

Beberapa administrator dan pengguna lain mungkin memerlukan penjelasan tentang sumber AWS daya yang dapat mereka akses di dalam landing zone Anda. Akses ini dapat mencakup akses terprogram dan akses berbasis konsol. Secara umum, akses baca dan akses tulis untuk AWS sumber daya diperbolehkan. Untuk melakukan pekerjaan di dalam AWS, pengguna Anda memerlukan beberapa tingkat akses ke layanan spesifik yang mereka butuhkan untuk melakukan pekerjaan mereka.

Beberapa pengguna, seperti AWS pengembang Anda, mungkin perlu mengetahui tentang sumber daya yang dapat mereka akses, sehingga mereka dapat membuat solusi teknik. Pengguna lain,

seperti pengguna akhir aplikasi yang berjalan pada AWS layanan, tidak perlu tahu tentang AWS sumber daya dalam landing zone Anda.

AWS menawarkan alat untuk mengidentifikasi ruang lingkup akses AWS sumber daya pengguna. Setelah Anda mengidentifikasi ruang lingkup akses pengguna, Anda dapat berbagi informasi tersebut dengan pengguna, sesuai dengan kebijakan manajemen informasi organisasi Anda. Untuk informasi selengkapnya tentang alat ini, lihat tautan yang mengikuti.

- AWS Access Advisor — Alat penasihat akses AWS Identity and Access Management (IAM) memungkinkan Anda menentukan izin yang dimiliki pengembang Anda dengan menganalisis stempel waktu terakhir ketika entitas IAM, seperti pengguna, peran, atau grup, disebut layanan. AWS Anda dapat mengaudit akses layanan dan menghapus izin yang tidak perlu, dan Anda dapat mengotomatiskan proses jika diperlukan. Untuk informasi lebih lanjut, lihat posting blog AWS Keamanan kami.
- Simulator kebijakan IAM — Dengan simulator kebijakan IAM, Anda dapat menguji dan memecahkan masalah IAM-based dan kebijakan berbasis sumber daya. Untuk informasi selengkapnya, lihat Menguji Kebijakan IAM dengan IAM Policy Simulator.
- AWS CloudTrail log — Anda dapat meninjau AWS CloudTrail log untuk melihat tindakan yang diambil oleh pengguna, peran, atau Layanan AWS. Untuk informasi selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

  Tindakan yang dilakukan oleh administrator landing zone AWS Control Tower dapat dilihat di akun manajemen landing zone. Tindakan yang dilakukan oleh administrator akun anggota dan pengguna dapat dilihat di akun arsip log bersama.

  Anda dapat melihat tabel ringkasan peristiwa AWS Control Tower di halaman Aktivitas.

Menjelaskan kontrol preventif

Kontrol preventif memastikan bahwa akun organisasi Anda tetap mematuhi kebijakan perusahaan Anda. Status kontrol preventif ditegakkan atau tidak diaktifkan. Kontrol preventif mencegah pelanggaran kebijakan dengan menggunakan kebijakan kontrol layanan (SCP), kebijakan pengendalian sumber daya (RCP), atau kebijakan deklaratif. Sebagai perbandingan, kontrol detektif memberi tahu Anda tentang berbagai peristiwa atau keadaan yang ada, melalui aturan yang ditentukan AWS Config .

Beberapa pengguna Anda, seperti AWS pengembang, mungkin perlu mengetahui tentang kontrol pencegahan yang berlaku untuk akun dan OU apa pun yang mereka gunakan, sehingga mereka

dapat membuat solusi teknik. Prosedur berikut menawarkan beberapa panduan tentang cara memberikan informasi ini untuk pengguna yang tepat, sesuai dengan kebijakan manajemen informasi organisasi Anda.

> **Note**
>
> Prosedur ini mengasumsikan Anda telah membuat setidaknya satu anak OU dalam landing zone Anda, serta setidaknya satu AWS IAM Identity Center pengguna.

Contoh: Untuk menunjukkan kontrol preventif bagi pengguna yang perlu tahu

1. Masuk ke konsol AWS Control Tower di https://console.aws.amazon.com/controltower/.
2. Dari navigasi kiri, pilih Organisasi.
3. Dari tabel, pilih nama salah satu OU yang pengguna Anda butuhkan informasi tentang kontrol yang berlaku.
4. Perhatikan nama OU dan kontrol yang berlaku untuk OU ini.
5. Ulangi dua langkah sebelumnya untuk setiap OU tentang informasi yang dibutuhkan pengguna Anda.

Untuk informasi terperinci tentang kontrol dan fungsinya, lihat Tentang kontrol di AWS Control Tower.

Rencanakan landing zone AWS Control Tower

Saat Anda melalui proses penyiapan, AWS Control Tower meluncurkan sumber daya utama yang terkait dengan akun Anda, yang disebut landing zone, yang berfungsi sebagai rumah bagi organisasi Anda dan akun mereka.

> **Note**
>
> Anda dapat memiliki satu landing zone per organisasi.

Untuk informasi tentang beberapa praktik terbaik yang harus diikuti saat Anda merencanakan dan mengatur landing zone, lihatAWS strategi multi-akun untuk landing zone AWS Control Tower.

Cara Mengatur AWS Control Tower

Anda dapat menyiapkan zona landing zone AWS Control Tower di organisasi yang sudah ada, atau Anda dapat memulai dengan membuat organisasi baru yang berisi zona landing zone AWS Control Tower Anda.

- Luncurkan AWS Control Tower di Organisasi yang Ada: Bagian ini diperuntukkan bagi pelanggan yang sudah AWS Organizations siap untuk dibawa ke tata kelola oleh AWS Control Tower.
- Luncurkan AWS Control Tower di Organisasi Baru: Bagian ini untuk pelanggan tanpa ada AWS Organizations, OU, dan akun.

> **Note**
>
> Jika Anda sudah memiliki AWS Organizations landing zone, Anda dapat memperluas tata kelola AWS Control Tower dari landing zone yang ada ke beberapa atau semua OU dan akun yang ada dalam suatu organisasi. Lihat Mengatur organisasi dan akun yang ada.

Bandingkan fungsionalitas

Berikut adalah perbandingan singkat perbedaan antara menambahkan AWS Control Tower ke organisasi yang ada atau memperluas tata kelola AWS Control Tower ke OU dan akun. Selain itu, beberapa pertimbangan khusus berlaku jika Anda pindah ke AWS Control Tower dari solusi AWS Landing Zone.

Tentang Menambahkan ke Organisasi yang Ada: Menambahkan AWS Control Tower ke organisasi yang ada adalah sesuatu yang dapat Anda capai di dalam AWS konsol. Dalam hal ini, Anda sudah memiliki organisasi yang telah Anda buat di AWS Organizations layanan, organisasi tersebut saat ini tidak terdaftar di AWS Control Tower, dan Anda ingin menambahkan landing zone sesudahnya.

Saat Anda menambahkan landing zone ke organisasi yang ada, AWS Control Tower menyiapkan struktur paralel, pada AWS Organizations level tersebut. Itu tidak mengubah OU dan akun dalam organisasi Anda yang ada.

Tentang Memperluas Tata Kelola: Memperluas tata kelola berlaku untuk OU dan akun tertentu dalam satu organisasi yang sudah terdaftar di AWS Control Tower, yang berarti bahwa landing zone sudah ada untuk organisasi tersebut. Memperluas tata kelola berarti kontrol AWS Control Tower diperpanjang sehingga batasannya berlaku untuk OU dan akun tertentu dalam organisasi terdaftar

tersebut. Dalam hal ini, Anda tidak meluncurkan landing zone baru, Anda hanya memperluas landing zone saat ini untuk organisasi Anda.

> **Important**
>
> Pertimbangan khusus: Jika saat ini Anda menggunakan solusi AWS Landing Zone (ALZ) untuk AWS Organizations, tanyakan kepada arsitek AWS solusi Anda sebelum Anda mencoba mengaktifkan AWS Control Tower di organisasi Anda. AWS Control Tower tidak dapat melakukan pra-pemeriksaan yang menentukan apakah AWS Control Tower dapat mengganggu penerapan landing zone Anda saat ini. Untuk informasi selengkapnya, lihat Panduan: Pindah dari ALZ ke AWS Control Tower. Juga, untuk informasi tentang memindahkan akun dari satu landing zone ke yang lain, lihat Jika akun tidak memenuhi prasyarat

Luncurkan AWS Control Tower di Organisasi yang Ada

Dengan menyiapkan zona landing zone AWS Control Tower di organisasi yang sudah ada, Anda dapat segera mulai bekerja, secara paralel dengan AWS Organizations lingkungan yang ada. OU Anda yang lain yang AWS Organizations dibuat di dalamnya tidak berubah, karena tidak terdaftar di AWS Control Tower. Anda dapat terus menggunakan OU dan akun tersebut persis seperti apa adanya.

AWS Control Tower berkonsolidasi dengan menggunakan akun manajemen dari organisasi Anda yang ada sebagai akun pengelolaannya. Tidak diperlukan akun manajemen baru. Anda dapat meluncurkan landing zone AWS Control Tower dari akun manajemen yang ada.

> **Note**
>
> Untuk menyiapkan AWS Control Tower di organisasi yang ada, batas layanan Anda harus memungkinkan pembuatan setidaknya dua akun tambahan.

Efek penambahan AWS Control Tower ke organisasi Anda yang ada

AWS Control Tower membuat dua akun di organisasi Anda: akun audit dan akun logging. Akun ini menyimpan catatan tindakan yang diambil oleh tim Anda, di akun pengguna akhir individu mereka. Akun arsip Audit dan Log muncul di OU Keamanan dalam landing zone AWS Control Tower Anda.

Saat Anda mengatur landing zone, akun yang ditambahkan AWS Control Tower menjadi bagian dari akun yang sudah ada AWS Organizations, dan karenanya akun tersebut menjadi bagian dari penagihan untuk organisasi Anda yang ada.

Ringkasan kemampuan

Mengaktifkan AWS Control Tower pada AWS Organizations organisasi yang ada menyediakan beberapa peningkatan besar bagi organisasi.

- Ini memungkinkan penagihan terpadu di seluruh grup organisasi Anda, karena akun yang ditambahkan oleh AWS Control Tower akan menjadi bagian dari organisasi Anda yang ada.
- Ini memberi Anda kemampuan untuk mengelola semua akun dari satu akun manajemen di OU Anda.
- Ini menyederhanakan cara Anda menerapkan dan menegakkan kontrol yang mencakup keamanan dan kepatuhan untuk akun yang ada dan yang baru.

> **Important**
>
> Meluncurkan landing zone AWS Control Tower di AWS Organizations organisasi yang ada tidak memungkinkan Anda memperluas tata kelola AWS Control Tower dari organisasi tersebut ke OU lain atau akun yang tidak terdaftar di AWS Control Tower.

Untuk meluncurkan AWS Control Tower di organisasi Anda yang ada, ikuti proses yang diuraikan. Memulai dengan AWS Control Tower

Untuk informasi selengkapnya tentang cara AWS Control Tower berinteraksi dengan AWS Organizations organisasi yang ada, lihatMengatur organisasi dan akun dengan AWS Control Tower.

Luncurkan AWS Control Tower di Organisasi Baru

Jika Anda baru mengenal AWS Control Tower dan belum pernah bekerja sama AWS Organizations, tempat terbaik untuk memulai adalah dengan Pengaturan dokumen kami.

AWS Control Tower menyiapkan organisasi untuk Anda secara otomatis ketika Anda belum mengaturnya.

AWS strategi multi-akun untuk landing zone AWS Control Tower

Pelanggan AWS Control Tower sering mencari panduan tentang cara mengatur AWS lingkungan mereka dan memperhitungkan hasil terbaik.AWS telah membuat serangkaian rekomendasi terpadu, yang disebut strategi multi-akun, untuk membantu Anda memanfaatkan AWS sumber daya sebaik-baiknya, termasuk zona landing zone AWS Control Tower Anda.

Pada dasarnya, AWS Control Tower bertindak sebagai lapisan orkestrasi yang berfungsi dengan AWS layanan lain, yang membantu Anda menerapkan rekomendasi AWS multi-akun untuk akun dan. AWS AWS Organizations Setelah landing zone Anda disiapkan, AWS Control Tower terus membantu Anda mempertahankan kebijakan perusahaan dan praktik keamanan di beberapa akun dan beban kerja.

Sebagian besar zona pendaratan berkembang seiring waktu. Karena jumlah unit organisasi (OU) dan akun di zona landing zone AWS Control Tower Anda meningkat, Anda dapat memperluas penerapan AWS Control Tower dengan cara yang membantu mengatur beban kerja Anda secara efektif. Bab ini memberikan panduan preskriptif tentang cara merencanakan dan menyiapkan landing zone AWS Control Tower Anda, selaras dengan strategi AWS multi-akun, dan memperpanjangnya dari waktu ke waktu.

Untuk diskusi umum tentang praktik terbaik untuk unit organisasi, lihat Praktik Terbaik untuk Unit Organisasi dengan AWS Organizations.

AWS strategi multi-akun: Panduan praktik terbaik

AWS praktik terbaik untuk lingkungan yang dirancang dengan baik merekomendasikan agar Anda memisahkan sumber daya dan beban kerja Anda menjadi beberapa akun. AWS Anda dapat menganggap AWS akun sebagai wadah sumber daya yang terisolasi: mereka menawarkan kategorisasi beban kerja, serta pengurangan radius ledakan ketika terjadi kesalahan.

Definisi AWS akun

AWS Akun bertindak sebagai wadah sumber daya dan batas isolasi sumber daya.

> **Note**
>
> AWS Akun tidak sama dengan akun pengguna, yang diatur melalui Federasi atau AWS Identity and Access Management (IAM).

Lebih lanjut tentang AWS akun

AWS Akun menyediakan kemampuan untuk mengisolasi sumber daya dan menahan ancaman keamanan untuk beban AWS kerja Anda. Akun juga menyediakan mekanisme untuk penagihan dan tata kelola lingkungan beban kerja.

AWS Akun adalah mekanisme implementasi utama untuk menyediakan wadah sumber daya untuk beban kerja Anda. Jika lingkungan Anda dirancang dengan baik, Anda dapat mengelola beberapa AWS akun secara efektif, dan dengan demikian, mengelola beberapa beban kerja dan lingkungan.

AWS Control Tower menyiapkan lingkungan yang dirancang dengan baik. Ini bergantung pada AWS akun, bersama dengan AWS Organizations, yang membantu mengatur perubahan pada lingkungan Anda yang dapat meluas di beberapa akun.

Definisi lingkungan yang dirancang dengan baik

> AWS mendefinisikan lingkungan yang dirancang dengan baik sebagai lingkungan yang dimulai dengan landing zone.

AWS Control Tower menawarkan landing zone yang diatur secara otomatis. Ini memberlakukan kontrol untuk memastikan kepatuhan terhadap pedoman perusahaan Anda, di beberapa akun di lingkungan Anda.

Definisi dari landing zone

> Landing zone adalah lingkungan cloud yang menawarkan titik awal yang direkomendasikan, termasuk akun default, struktur akun, tata letak jaringan dan keamanan, dan sebagainya. Dari landing zone, Anda dapat menerapkan beban kerja yang memanfaatkan solusi dan aplikasi Anda.

Pedoman untuk mengatur lingkungan yang dirancang dengan baik

Tiga komponen kunci dari lingkungan yang dirancang dengan baik, dijelaskan dalam bagian berikut, adalah:

- Beberapa AWS akun
- Beberapa unit organisasi (OU)
- Struktur yang terencana dengan baik

Gunakan beberapa akun AWS

Satu akun tidak cukup untuk mengatur lingkungan yang dirancang dengan baik. Dengan menggunakan beberapa akun, Anda dapat mendukung tujuan keamanan dan proses bisnis Anda dengan sebaik-baiknya. Berikut adalah beberapa manfaat menggunakan pendekatan multi-akun:

- Kontrol keamanan — Aplikasi memiliki profil keamanan yang berbeda, sehingga memerlukan kebijakan dan mekanisme kontrol yang berbeda. Misalnya, jauh lebih mudah untuk berbicara dengan auditor dan menunjuk ke satu akun yang menampung beban kerja industri kartu pembayaran (PCI).
- Isolasi — Akun adalah unit perlindungan keamanan. Potensi risiko dan ancaman keamanan dapat terkandung dalam akun tanpa mempengaruhi orang lain. Oleh karena itu, kebutuhan keamanan mungkin mengharuskan Anda untuk mengisolasi akun satu sama lain. Misalnya, Anda mungkin memiliki tim dengan profil keamanan yang berbeda.
- Banyak tim — Tim memiliki tanggung jawab dan kebutuhan sumber daya yang berbeda. Dengan menyiapkan beberapa akun, tim tidak dapat mengganggu satu sama lain, karena mereka mungkin saat menggunakan akun yang sama.
- Isolasi Data — Mengisolasi penyimpanan data ke akun membantu membatasi jumlah orang yang memiliki akses ke data dan dapat mengelola penyimpanan data. Isolasi ini membantu mencegah paparan data yang sangat pribadi secara tidak sah. Misalnya, isolasi data membantu mendukung kepatuhan terhadap Peraturan Perlindungan Data Umum (GDPR).
- Proses bisnis — Unit bisnis atau produk sering memiliki tujuan dan proses yang sama sekali berbeda. Akun individu dapat dibuat untuk melayani kebutuhan khusus bisnis.
- Penagihan — Akun adalah satu-satunya cara untuk memisahkan item pada tingkat penagihan, termasuk hal-hal seperti biaya transfer dan sebagainya. Strategi multi-akun membantu membuat item yang dapat ditagih terpisah di seluruh unit bisnis, tim fungsional, atau pengguna individu.
- Alokasi kuota — AWS kuota diatur berdasarkan per akun. Memisahkan beban kerja ke dalam akun yang berbeda memberi setiap akun (seperti proyek) kuota individual yang terdefinisi dengan baik.

Gunakan beberapa unit organisasi

AWS Control Tower dan kerangka kerja orkestrasi akun lainnya dapat membuat perubahan yang melintasi batas akun. Oleh karena itu, praktik AWS terbaik mengatasi perubahan lintas akun, yang berpotensi dapat merusak lingkungan atau merusak keamanannya. Dalam beberapa kasus, perubahan dapat mempengaruhi lingkungan secara keseluruhan, di luar kebijakan. Oleh karena itu, kami menyarankan Anda untuk menyiapkan setidaknya dua akun wajib, Produksi dan Pementasan.

Selain itu, AWS akun sering dikelompokkan ke dalam unit organisasi (OU), untuk tujuan tata kelola dan kontrol. OU dirancang untuk menangani penegakan kebijakan di beberapa akun.

Rekomendasi kami adalah, setidaknya, Anda membuat lingkungan pra-produksi (atau Pementasan) yang berbeda dari lingkungan Produksi Anda—dengan kontrol dan kebijakan yang berbeda. Lingkungan Produksi dan Pementasan dapat dibuat dan diatur sebagai OU terpisah, dan ditagih sebagai akun terpisah. Selain itu, Anda mungkin ingin menyiapkan Sandbox OU untuk pengujian kode.

Gunakan struktur yang terencana dengan baik untuk OU di landing zone Anda

AWS Control Tower menyiapkan beberapa OU untuk Anda secara otomatis. Saat beban kerja dan persyaratan Anda bertambah seiring waktu, Anda dapat memperluas konfigurasi landing zone asli agar sesuai dengan kebutuhan Anda.

> **Note**
>
> Nama-nama yang diberikan dalam contoh mengikuti konvensi AWS penamaan yang disarankan untuk menyiapkan lingkungan multi-akun AWS . Anda dapat mengganti nama OU setelah menyiapkan landing zone, dengan memilih Edit pada halaman detail OU.

Rekomendasi

Setelah AWS Control Tower menyiapkan OU pertama yang diperlukan untuk Anda — Security OU — kami sarankan untuk membuat beberapa OU tambahan di landing zone Anda.

Kami menyarankan Anda mengizinkan AWS Control Tower untuk membuat setidaknya satu OU tambahan, yang disebut Sandbox OU. OU ini untuk lingkungan pengembangan perangkat lunak Anda. AWS Control Tower dapat mengatur Sandbox OU untuk Anda selama pembuatan landing zone, jika Anda memilihnya.

Dua rekomendasi OU lain yang dapat Anda atur sendiri: Infrastruktur OU, untuk memuat layanan bersama dan akun jaringan Anda, dan OU untuk memuat beban kerja produksi Anda, yang disebut Workloads OU. Anda dapat menambahkan OU tambahan di landing zone melalui konsol AWS Control Tower di halaman Unit Organisasi.

OU yang direkomendasikan selain yang diatur secara otomatis

- Infrastruktur OU - Berisi layanan bersama dan akun jaringan Anda.

> **Note**
>
> AWS Control Tower tidak menyiapkan Infrastruktur OU untuk Anda.

- Sandbox OU — Sebuah pengembangan perangkat lunak OU. Misalnya, mungkin memiliki batas pengeluaran tetap, atau mungkin tidak terhubung ke jaringan produksi.

> **Note**
>
> AWS Control Tower merekomendasikan agar Anda menyiapkan Sandbox OU, tetapi ini opsional. Ini dapat diatur secara otomatis sebagai bagian dari konfigurasi landing zone Anda.

- Workloads OU - Berisi akun yang menjalankan beban kerja Anda.

> **Note**
>
> AWS Control Tower tidak menyiapkan Workloads OU untuk Anda.

Untuk informasi selengkapnya, lihat Cara AWS Control Tower menetapkan lingkungan multi-akun Anda.

Sejajarkan struktur OU Anda dengan AWS strategi multi-akun

AWS Control Tower mendukung hierarki OU bersarang, yang berarti Anda dapat membuat struktur OU hierarkis yang memenuhi persyaratan organisasi Anda. Anda dapat membangun lingkungan AWS Control Tower agar sesuai dengan panduan strategi AWS multi-akun.

Untuk informasi selengkapnya tentang cara kerja AWS Control Tower dengan struktur OU bersarang, lihatOU bersarang di Menara Kontrol AWS.

Untuk OU dan akun yang direkomendasikan di luar akun AWS Control Tower yang disiapkan secara default, lihat OU dan akun yang direkomendasikan di AWS white paper.

Tentang Root

Root bukan OU. Ini adalah wadah untuk akun manajemen, dan untuk semua OU dan akun di organisasi Anda. Secara konseptual, Root berisi semua OU. Itu tidak bisa dihapus. Anda tidak dapat

mengatur akun terdaftar di tingkat Root dalam AWS Control Tower. Sebagai gantinya, atur akun terdaftar dalam OU Anda. Untuk diagram yang bermanfaat, lihat AWS Organizations dokumentasi.

Kiat administratif untuk pengaturan landing zone

Berikut adalah beberapa tips untuk mengatur dan mengonfigurasi landing zone Anda.

- AWS Wilayah tempat Anda melakukan pekerjaan paling banyak harus menjadi wilayah asal Anda.
- Siapkan landing zone Anda dan gunakan akun Account Factory Anda dari dalam Wilayah asal Anda.
- Jika Anda berinvestasi di beberapa AWS Wilayah, pastikan sumber daya cloud Anda berada di Wilayah tempat Anda akan melakukan sebagian besar pekerjaan administrasi cloud dan menjalankan beban kerja Anda.
- Dengan menyimpan beban kerja dan log Anda di AWS Wilayah yang sama, Anda mengurangi biaya yang terkait dengan pemindahan dan pengambilan informasi log di seluruh wilayah.
- Audit dan bucket Amazon S3 lainnya dibuat di AWS Wilayah yang sama tempat Anda meluncurkan AWS Control Tower. Kami menyarankan Anda untuk tidak memindahkan ember ini.
- Anda dapat membuat ember log Anda sendiri di akun Arsip Log, tetapi tidak disarankan. Pastikan untuk meninggalkan bucket yang dibuat oleh AWS Control Tower.
- Log akses Amazon S3 Anda harus berada di AWS Wilayah yang sama dengan bucket sumber.
- Saat diluncurkan, titik akhir AWS Security Token Service (STS) harus diaktifkan di akun manajemen, untuk semua Wilayah yang didukung oleh AWS Control Tower. Jika tidak, peluncuran mungkin gagal di tengah proses konfigurasi.
- AWS Control Tower mendukung penandaan hanya untuk kontrol yang diaktifkan. Untuk informasi selengkapnya, lihat API penandaan kontrol Menara Kontrol AWS.
- Sebaiknya aktifkan autentikasi multi-faktor (MFA) untuk setiap akun yang dikelola AWS Control Tower.
- Atau, Anda dapat menggunakan fitur AWS Root Access Management, yang memungkinkan tindakan root dilakukan pada akun anggota, dan menghilangkan kebutuhan untuk mengaktifkan MFA untuk setiap akun. Untuk informasi selengkapnya, lihat Mengelola akses root secara terpusat untuk pelanggan yang menggunakan AWS Organizations.

Pertimbangan tentang VPC

- VPC yang dibuat oleh AWS Control Tower terbatas Wilayah AWS pada tempat AWS Control Tower tersedia. Beberapa pelanggan yang beban kerjanya berjalan di Wilayah yang tidak didukung mungkin ingin menonaktifkan VPC yang dibuat dengan akun Account Factory Anda. Mereka mungkin lebih suka membuat VPC baru menggunakan portofolio Service Catalog, atau membuat VPC kustom yang hanya berjalan di Wilayah yang diperlukan.
- VPC yang dibuat oleh AWS Control Tower tidak sama dengan VPC default yang dibuat untuk semua. Akun AWS Di Wilayah di mana AWS Control Tower didukung, AWS Control Tower menghapus VPC default saat membuat AWS Control Tower VPC.
- Jika Anda menghapus VPC default Anda di AWS Wilayah rumah Anda, yang terbaik adalah menghapusnya di semua Wilayah lain AWS .

Panduan migrasi Landing Zone v4.0

AWS Control Tower Landing Zone 4.0 memperkenalkan perombakan besar-besaran pada arsitektur landing zone, menawarkan pengalaman kontrol khusus yang fleksibel dan integrasi layanan opsional sepenuhnya. Penyempurnaan utama mencakup kemampuan untuk mengaktifkan secara selektif, AWS Config AWS, dan AWS Backup integrasi CloudTrail SecurityRoles, dengan sumber daya khusus untuk dan AWS Config CloudTrail AWS untuk isolasi yang lebih baik.

Rilis ini menghapus persyaratan struktur organisasi wajib, memungkinkan pelanggan untuk menentukan sendiri, sambil memperkenalkan yang baru `ConfigBaseline` untuk dukungan kontrol detektif tanpa memerlukan yang komprehensif`AWSControlTowerBaseline`. Agregator Config tertaut layanan menggantikan metode agregasi sebelumnya, menyederhanakan pengumpulan data kepatuhan.

Selain itu, bidang manifes menjadi opsional, memungkinkan penyebaran landing zone minimalis yang hanya berfokus pada AWS Organizations integrasi dan pemberdayaan kontrol. Perubahan ini memberikan opsi penyesuaian yang lebih besar sambil mempertahankan kemampuan tata kelola yang kuat, memungkinkan pelanggan untuk menyesuaikan AWS Control Tower dengan kebutuhan spesifik mereka secara lebih efektif.

Topik

- Perubahan kunci
- Pembaruan AWS Config
- Perbandingan fitur dengan dan tanpa AWS Config integrasi

Perubahan kunci

> **Note**
>
> - Definisi “terdaftar” dan “terdaftar” telah bergeser dengan versi baru AWS Control Tower ini. Jika Anda account/OU mengaktifkan sumber daya AWS Control Tower (misalnya kontrol atau baseline), sumber daya AWS Control Tower akan dianggap sebagai sumber daya yang diatur. Definisi tidak akan lagi didorong oleh kehadiran `AWSControlTowerBaseline` baseline.
> - Service-Linked Peran dipertahankan di semua versi landing zone dan tidak lagi dihapus ketika OU menjadi “tidak terdaftar”
> - Service-Linked Peran hanya dapat dihapus secara manual oleh pelanggan setelah penonaktifan landing zone

> **Upgrade dari versi 3.3 atau versi sebelumnya ke versi 4.0**
>
> Jangan menonaktifkan integrasi layanan (AWS Config, SecurityRoles) sebagai bagian dari peningkatan versi. Di landing zone versi 3.3 dan sebelumnya, AWS Config dan SecurityRoles selalu diaktifkan secara implisit. Versi 4.0 menampilkan integrasi ini sebagai opsi yang dapat dikonfigurasi untuk pertama kalinya. Setelah berhasil meningkatkan ke versi 4.0, Anda dapat menonaktifkan integrasi layanan sesuai keinginan.

- Pre-requisite untuk Landing Zone 4.0: Saat memutakhirkan ke versi 4.0 melalui API, pastikan peran `AWSControlTowerCloudTrailRole` layanan menggunakan kebijakan terkelola baru, `AWSControlTowerCloudTrailRolePolicy` bukan kebijakan sebaris yang ada. Lepaskan kebijakan inline saat ini dan lampirkan kebijakan terkelola baru seperti yang dijelaskan dalam dokumentasi.
- Manifes Opsional: Bidang manifes di API landing zone sekarang opsional. Pelanggan dapat membuat Zona Pendaratan tanpa integrasi layanan apa pun. Tidak ada dampak bagi pelanggan yang sudah ada yang sudah menggunakan bidang manifes.
- Struktur Organisasi Opsional: AWS Control Tower tidak lagi memberlakukan atau mengelola pembuatan OU Keamanan sehingga pelanggan dapat menentukan dan mengelola struktur organisasi mereka sendiri. Namun, AWS Control Tower akan mewajibkan semua akun yang dikonfigurasi untuk setiap integrasi layanan AWS berada di bawah OU induk yang sama. Tidak

ada dampak bagi pelanggan yang telah menyiapkan AWS Control Tower dan memiliki Security OU. AWS Control Tower secara otomatis menyebarkan sumber daya dan kontrol yang diperlukan untuk mengelola akun integrasi layanan di OU Keamanan. Misalnya, ketika integrasi AWS Config diaktifkan, perekaman AWS Config diaktifkan di semua akun integrasi layanan. AWS Control Tower Baseline dan AWS Config Baseline tidak berlaku untuk OU Keamanan dan akun integrasi layanan. Untuk mengubah integrasi layanan, perbarui pengaturan landing zone.

> **Note**
>
> - Pengaturan struktur organisasi untuk AWS Control Tower landing zone 4.0 telah berubah dari versi landing zone sebelumnya. AWS Control Tower tidak akan lagi membuat OU Keamanan yang ditunjuk. OU dengan akun integrasi layanan akan menjadi OU Keamanan yang ditunjuk.
> - Jika akun anggota pindah ke OU di mana akun untuk setiap integrasi berada, kontrol yang diaktifkan pada OU tersebut akan dialihkan terlepas dari apakah pendaftaran otomatis diaktifkan atau dimatikan.

Status dasar untuk OU Keamanan: Baseline AWS Control Tower dan AWS Config Baseline tidak dapat diterapkan ke OU Keamanan. Keamanan OU menampilkan status dasar “Tidak Berlaku” untuk baseline ini. Status ini diharapkan. Ini BackupBaseline dapat diterapkan ke OU Keamanan.

AWS Control Tower mengelola akun integrasi layanan melalui landing zone, bukan melalui OU-level baseline. Jika akun integrasi layanan menampilkan status dasar “Tidak Diaktifkan” dan integrasi layanan terkait dinonaktifkan, AWS Control Tower tidak lagi mengelola akun tersebut.

Akun di OU Keamanan yang tidak ditetapkan sebagai akun integrasi layanan tidak menerima sumber daya dasar. Untuk mengatur akun ini, pindahkan ke OU yang dikelola dan perluas tata kelola.

Set izin IAM Identity Center untuk akun integrasi layanan: AWS Control Tower menyediakan set izin IAM Identity Center untuk akun Logging dan akun. SecurityRoles AWS Control Tower tidak menyediakan set izin untuk akun Config atau akun Backup. Untuk mengakses akun Config atau Backup melalui IAM Identity Center, buat set izin secara manual menggunakan resource IAM Identity Center yang digunakan AWS Control Tower.

- Pemberitahuan Drift: AWS Control Tower akan berhenti mengirimkan notifikasi drift ke topik SNS untuk semua pelanggan di landing zone 4.0 dan yang lebih baru, dan akan mulai mengirim

notifikasi drift ke akun EventBridge manajemen. Untuk menerima pemberitahuan ini, buat EventBridge aturan di akun manajemen. Kemudian konfigurasikan target, seperti topik SNS atau fungsi Lambda. Untuk informasi selengkapnya tentang notifikasi drift dan contoh EventBridge peristiwa, lihat Jenis penyimpangan tata kelola.

- Integrasi Layanan Opsional: Anda sekarang memiliki kemampuan untuk enable/disable semua integrasi AWS Control Tower termasuk CloudTrail, AWS Config AWS SecurityRoles, dan. AWS Backup Integrasi ini juga sekarang memiliki `enabled` flag yang diperlukan di API. Garis dasar yang mungkin berlaku untuk landing zone atau akun bersama Anda sekarang memiliki ketergantungan satu sama lain. Dependensi spesifik Integrasi adalah:
  - Pemberdayaan:
    - `CentralSecurityRolesBaseline`→ `CentralConfigBaseline` perlu diaktifkan
    - `IdentityCenterBaseline`→ `CentralSecurityRolesBaseline` perlu diaktifkan
    - `BackupCentralVaultBaseline`→ `CentralSecurityRolesBaseline` perlu diaktifkan
    - `BackupAdminBaseline`→ `CentralSecurityRolesBaseline` perlu diaktifkan
    - `LogArchiveBaseline`→ independen (tidak ada dependensi)
    - `CentralConfigBaseline`→ independen (tidak ada dependensi)
  - Cacat:
    - `CentralConfigBaseline`hanya dapat dinonaktifkan jika`CentralSecurityRolesBaseline`,`IdentityCenterBaseline`, `BackupAdminBaseline` dan `BackupCentralVaultBaseline` baseline dinonaktifkan terlebih dahulu.
    - `CentralSecurityRolesBaseline`hanya dapat dinonaktifkan jika`IdentityCenterBaseline`, `BackupAdminBaseline` dan `BackupCentralVaultBaseline` baseline dinonaktifkan terlebih dahulu.
    - `IdentityCenterBaseline`dapat dinonaktifkan secara mandiri.
    - `BackupAdminBaseline`dan `BackupCentralVaultBaseline` baseline dapat dinonaktifkan secara independen
    - `LogArchiveBaseline`dapat dinonaktifkan secara mandiri

> ⚠ Lingkup AWS Config pemberdayaan integrasi layanan
>
> Mengaktifkan integrasi AWS Config layanan di tingkat landing zone akan menyebarkan sumber daya perekaman Config ke akun integrasi layanan saja. Untuk menyebarkan

AWS Config sumber daya (Config Recorder, Delivery Channel) ke akun anggota, aktifkan baseline pada setiap AWS Config OU yang dikelola secara individual.
Mengaktifkan integrasi Config di level landing zone merupakan prasyarat untuk mengaktifkan baseline Config pada OU. Pengaturan tingkat zona pendaratan saja tidak menerapkan sumber daya Config ke akun anggota.
Untuk informasi selengkapnya, lihat Pembaruan AWS Config.

⚠ CentralizedLogging perubahan perilaku di versi 4.0

Di landing zone versi 3.3 dan sebelumnya, CentralizedLogging menonaktifkan Organisasi menjadi nonaktif dan mempertahankan semua sumber CloudTrail daya yang digunakan. Di versi 4.0, menonaktifkan CentralizedLogging menghapus semua sumber daya terkait dari akun logging. Sumber daya ini mencakup Config Recorder, Delivery Channel, dan instance CloudTrail-related stack. Setelah penonaktifan, AWS Control Tower tidak lagi mengelola akun logging.
Untuk memulihkan pengelolaan akun logging, aktifkan kembali CentralizedLogging atau pindahkan akun ke OU terkelola dan perpanjang tata kelola.

Pembaruan AWS Config

- Sumber daya khusus untuk AWS Config dan AWS CloudTrail: AWS Config dan AWS CloudTrail sekarang menggunakan bucket S3 dan topik SNS khusus yang terpisah alih-alih sumber daya bersama. Pelanggan memiliki fleksibilitas terbatas untuk menggunakan akun tunggal atau terpisah untuk beberapa integrasi.
  - Saat memutakhirkan ke AWS Control Tower landing zone versi 4.0, data yang ada dan bucket S3 tidak dipindahkan. CloudTrail Integrasi AWS terus menggunakan bucket S3 yang ada dengan awalan`aws-controltower-logs`. Data AWS Config baru setelah operasi pembaruan akan disimpan dalam bucket S3 baru dengan awalan yang dibuat AWS Control `aws-controltower-config` Tower di akun yang ditunjuk untuk. CentralConfigBaseline

    ℹ Note

    Mengaktifkan CloudTrail integrasi AWS di landing zone 4.0 untuk pertama kalinya akan membuat bucket S3 baru setiap kali dengan awalan `aws-controltower-cloudtrail`

  - Perubahan Lokasi Data: Pelanggan yang sudah ada yang meningkatkan dari sumber daya yang dibagikan sebelumnya ke sumber daya khusus akan memiliki AWS Config dan CloudTrail data AWS dalam bucket S3 yang berbeda. Alur kerja dan alat pelanggan yang sudah mapan mungkin memerlukan pembaruan untuk mengakses data dari lokasi bucket baru.
  - AWS CloudTrail akan terus berada di bucket yang sama, tetapi AWS Config data akan berada di bucket S3 baru yang dibuat oleh AWS Control Tower.
  - Pelanggan dapat mengatur replikasi cross-bucket jika mereka ingin memusatkan log yang berbeda ke satu ember. Silakan lihat dokumentasi S3 untuk informasi lebih lanjut.
  - Jika Anda telah mendaftarkan akun dengan Saluran Pengiriman AWS Config yang sudah ada sebelumnya yang tidak dibuat oleh AWS Control Tower di Wilayah yang diatur oleh AWS Control Tower, perbarui nama bucket S3 Saluran Pengiriman ke bucket S3 baru dengan awalan `aws-controltower-config-logs-` di akun integrasi AWS Config agar konsisten dengan konfigurasi AWS Control Tower di landing zone 4.0. Lihat detail selengkapnya di Daftarkan akun yang sudah ada AWS Config sumber daya.
- AWS Config integrasi pada landing zone versi 4.0: Saat bermigrasi ke landing zone 4.0 dengan AWS Config integrasi diaktifkan, pelanggan akan melihat perubahan berikut -
  1. Akun Audit yang ada terdaftar sebagai admin yang didelegasikan untuk AWS Config.
  2. Service-Linked Config Aggregator disebarkan ke akun Audit (akun agregator AWS Config pusat untuk pelanggan baru dan akun Audit untuk pelanggan yang sudah ada). Agregator baru dapat mengumpulkan data dari AWS Config Perekam mana pun di organisasi, termasuk akun yang dikelola Non-Control Tower.
  3. Agregator yang ada akan dihapus - Agregator organisasi di akun manajemen (`aws-controltower-ConfigAggregatorForOrganizations`) dan agregator akun di akun Audit (`aws-controltower-GuardRailsComplianceAggregator`) akan dihapus.
  4. Karena Configuration Aggregator terhubung dengan layanan, kontrol yang terkait dengan agregator yang dihapus akan dihapus secara otomatis.
     a. Larang Perubahan pada Tag yang Dibuat oleh AWS Control Tower untuk Sumber Daya AWS Config
     b. Larang Penghapusan Otorisasi Agregasi AWS Config yang Dibuat oleh AWS Control Tower
- **`ConfigBaseline`**Garis dasar baru: Sekarang ada yang terpisah `ConfigBaseline` di tingkat OU untuk dukungan kontrol detektif tanpa memerlukan yang komprehensif. `AWSControlTowerBaseline` Lihat daftar tipe dasar di tingkat OU untuk informasi lebih lanjut. Untuk pelanggan lama yang menggunakan landing zone default, semua integrasi layanan

sekarang opsional, dengan peringatan persyaratan ketergantungan yang diuraikan dalam. Perubahan kunci

- Service-Linked Config Aggregator: Menggantikan agregator organisasi dan akun di akun agregator pusat. AWS Config
  - Saat memutakhirkan ke landing zone 4.0 dengan AWS Config integrasi diaktifkan, pelanggan harus memiliki izin `organizations:ListDelegatedAdministrators`

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
           "backup:UpdateGlobalSettings",
           "controltower:CreateLandingZone",
           "controltower:UpdateLandingZone",
           "controltower:ResetLandingZone",
           "controltower:DeleteLandingZone",
           "controltower:GetLandingZoneOperation",
           "controltower:GetLandingZone",
           "controltower:ListLandingZones",
           "controltower:ListLandingZoneOperations",
           "controltower:ListTagsForResource",
           "controltower:TagResource",
           "controltower:UntagResource",
            "servicecatalog:*",
            "organizations:*",
            "organizations:RegisterDelegatedAdministrator",
            "organizations:EnableAWSServiceAccess",
            "organizations:DeregisterDelegatedAdministrator",
            "organizations:ListDelegatedAdministrators",
            "sso:*",
            "sso-directory:*",
            "logs:*",
            "cloudformation:*",
            "kms:*",
            "iam:GetRole",
            "iam:CreateRole",
            "iam:GetSAMLProvider",
            "iam:CreateSAMLProvider",
            "iam:CreateServiceLinkedRole",
```

```
            "iam:ListRolePolicies",
            "iam:PutRolePolicy",
            "iam:ListAttachedRolePolicies",
            "iam:AttachRolePolicy",
            "iam:DeleteRole",
            "iam:DeleteRolePolicy",
            "iam:DetachRolePolicy"
         ],
         "Resource": "*"
      }
   ]
}
```

Important

Setelah Anda meng-upgrade ke landing zone versi 4.0 dan mengaktifkan AWS Config integrasi, Anda harus menyelesaikan proses enablement. Perbarui atau aktifkan `ConfigBaseline` pada semua OU tempat Anda ingin menyebarkan AWS Config sumber daya. Sampai Anda menyelesaikan proses ini, AWS Config Aggregator Anda tidak akan menerima data dari perekam. Setiap akun terus merekam dan menyimpan data. Setelah Anda selesai memperbarui`ConfigBaseline`, data yang direkam secara otomatis mengisi kembali ke agregator.

Kami menyarankan Anda mendaftarkan ulang OU Anda atau mengaktifkan `ConfigBaseline` sesegera mungkin setelah mengaktifkan integrasi. AWS Config Pembaruan landing zone menghapus izin AWS Config pengiriman dari kebijakan bucket S3 sebelumnya, tetapi saluran pengiriman dialihkan ke bucket baru hanya setelah Anda menyelesaikan pendaftaran ulang. Sampai saat itu, snapshot konfigurasi dan riwayat konfigurasi tidak dikirim ke S3.

Jika pendaftaran ulang tertunda, beberapa data ini mungkin tidak dikirim ke S3 setelah pendaftaran ulang selesai. Anda dapat mengambil semua data yang direkam dalam periode retensi yang dikonfigurasi menggunakan `config:GetResourceConfigHistory` API.

Perbandingan fitur dengan dan tanpa AWS Config integrasi

Dengan Landing Zone 4.0, Anda dapat menonaktifkan AWS Config integrasi. Tabel berikut merangkum fitur AWS Control Tower yang tersedia dengan dan tanpa AWS Config integrasi yang diaktifkan di landing zone.

Fitur	AWS Config Integrasi Diaktifkan	AWS Config Integrasi Dinonaktifkan
Kontrol preventif	✓	✓
Kontrol proaktif	✓	✓
Kontrol Region Deny diterapkan ke OU	✓	✓
Kontrol Region Deny diterapkan pada landing zone	✓	
Kontrol detektif	✓	
Account Factory	✓	Lihat alternatif
Account Factory untuk Terraform (AFT)	✓	
Kustomisasi Account Factory (AFC)	✓	
Integrasi AWS Service Catalog dengan Account Factory	✓	
Kustomisasi untuk AWS Control Tower (CFCT)	✓	
Garis dasar diterapkan pada OU	✓	
CloudTrail Integrasi dan baseline AWS	✓	✓
Integrasi AWS Backup dan baseline	✓	
Integrasi dan baseline AWS IAM Identity Center	✓	
Integrasi AWS SNS untuk notifikasi drift	✓	

Fitur	AWS Config Integrasi Diaktifkan	AWS Config Integrasi Dinonaktifkan
EventBridge Integrasi Amazon untuk notifikasi drift	✓	✓
Daftar OU	✓	Lihat alternatif

Alternatif

Account Factory

Jika AWS Config integrasi dinonaktifkan, Anda dapat mengaktifkan pendaftaran otomatis dan menggunakannya AWS Organizations untuk membuat dan memindahkan akun. Akun akan mewarisi kontrol yang diterapkan ke OU induk.

Daftar OU

Jika AWS Config integrasi Anda dinonaktifkan, Anda dapat menggunakan AWS Organizations untuk membuat OU. Kemudian, aktifkan kontrol melalui halaman Control Catalog di konsol AWS Control Tower, setel ulang kontrol di halaman Organisasi, atau gunakan AWS Control Tower API.

Rekomendasi untuk menyiapkan grup, peran, dan kebijakan

Saat Anda mengatur landing zone, ada baiknya Anda memutuskan sebelumnya pengguna mana yang akan memerlukan akses ke akun tertentu dan mengapa. Misalnya, akun keamanan harus dapat diakses hanya oleh tim keamanan, akun manajemen harus dapat diakses hanya oleh tim administrator cloud, dan sebagainya.

Untuk informasi lebih lanjut tentang topik ini, lihatManajemen identitas dan akses di AWS Control Tower.

Pembatasan yang disarankan

Anda dapat membatasi ruang lingkup akses administratif ke organisasi Anda dengan menyiapkan peran atau kebijakan IAM yang memungkinkan administrator mengelola tindakan AWS Control Tower saja. Pendekatan yang disarankan adalah dengan menggunakan kebijakan `arn:aws:iam::aws:policy/service-role/AWSControlTowerServiceRolePolicy` IAM.

Dengan `AWSControlTowerServiceRolePolicy` peran diaktifkan, administrator hanya dapat mengelola AWS Control Tower. Pastikan untuk menyertakan akses yang tepat AWS Organizations untuk mengelola kontrol pencegahan Anda, dan SCP, dan akses ke AWS Config, untuk mengelola kontrol detektif, di setiap akun.

Saat menyiapkan akun audit bersama di landing zone, sebaiknya tetapkan `AWSSecurityAuditors` grup tersebut ke auditor pihak ketiga mana pun di akun Anda. Grup ini memberikan izin read-only kepada anggotanya. Akun tidak boleh memiliki izin menulis tentang lingkungan yang diaudit, karena dapat melanggar kepatuhan terhadap persyaratan Pemisahan Tugas untuk auditor.

Anda dapat menerapkan ketentuan dalam kebijakan kepercayaan peran Anda, untuk membatasi akun dan sumber daya yang berinteraksi dengan peran tertentu di AWS Control Tower. Kami sangat menyarankan Anda membatasi akses ke `AWSControlTowerAdmin` peran, karena memungkinkan izin akses yang luas. untuk informasi selengkapnya, lihat Ketentuan opsional untuk hubungan kepercayaan peran Anda.

Panduan untuk membuat dan memodifikasi sumber daya AWS Control Tower

Kami merekomendasikan praktik terbaik berikut saat Anda membuat dan memodifikasi sumber daya di AWS Control Tower. Panduan ini mungkin berubah saat layanan diperbarui. Ingatlah bahwa model tanggung jawab bersama berlaku untuk lingkungan AWS Control Tower Anda.

Bimbingan Umum

- Jangan mengubah atau menghapus sumber daya apa pun yang dibuat oleh AWS Control Tower, termasuk sumber daya di akun manajemen, di akun bersama, dan di akun anggota. Jika Anda memodifikasi sumber daya ini, Anda mungkin diminta untuk memperbarui landing zone atau mendaftarkan ulang OU, dan modifikasi dapat mengakibatkan pelaporan kepatuhan yang tidak akurat.

  Secara khusus:

  - Simpan AWS Config perekam aktif. Jika Anda menghapus perekam Config, kontrol detektif tidak dapat mendeteksi dan melaporkan penyimpangan. Non-compliant sumber daya dapat dilaporkan sebagai Compliant karena informasi yang tidak mencukupi.
  - Jangan mengubah atau menghapus peran AWS Identity and Access Management (IAM) yang dibuat dalam akun bersama di unit organisasi Keamanan (OU). Modifikasi peran ini dapat memerlukan pembaruan ke landing zone Anda.

  - Jangan hapus `AWSControlTowerExecution` peran dari akun anggota Anda, bahkan di akun yang tidak terdaftar. Jika ya, Anda tidak akan dapat mendaftarkan akun ini dengan AWS Control Tower, atau mendaftarkan OU induk langsung mereka.
- Jangan melarang penggunaan apapun Wilayah AWS melalui SCP atau AWS Security Token Service ()AWS STS. Melakukannya akan menyebabkan AWS Control Tower memasuki status tidak terdefinisi. Jika Anda melarang Wilayah dengan AWS STS, fungsionalitas Anda akan gagal di Wilayah tersebut, karena otentikasi tidak akan tersedia di Wilayah tersebut. Sebagai gantinya, andalkan kemampuan penolakan Wilayah AWS Control Tower, seperti yang ditunjukkan dalam kontrol, Tolak akses AWS berdasarkan permintaan Wilayah AWS, yang berfungsi pada tingkat landing zone, atau kontrol Wilayah menolak kontrol yang diterapkan pada OU, yang bekerja di tingkat OU untuk membatasi akses ke Wilayah.
- AWS Organizations `FullAWSAccess`SCP harus diterapkan dan tidak boleh digabungkan dengan SCP lainnya. Perubahan pada SCP ini tidak dilaporkan sebagai drift; namun, beberapa perubahan dapat memengaruhi fungsionalitas AWS Control Tower dengan cara yang tidak dapat diprediksi, jika akses ke sumber daya tertentu ditolak. Misalnya, jika SCP terlepas, atau dimodifikasi, akun mungkin kehilangan akses ke AWS Config perekam atau membuat celah dalam CloudTrail pencatatan.
- Jangan gunakan AWS Organizations `DisableAWSServiceAccess` API untuk mematikan akses layanan AWS Control Tower ke organisasi tempat Anda menyiapkan landing zone. Jika Anda melakukannya, fitur deteksi drift AWS Control Tower tertentu mungkin tidak berfungsi dengan baik tanpa dukungan pesan dari AWS Organizations. Fitur deteksi drift ini membantu menjamin AWS Control Tower dapat melaporkan status kepatuhan unit organisasi, akun, dan kontrol di organisasi Anda secara akurat. Untuk informasi selengkapnya, lihat API_DisableAWSServiceAccessdi Referensi AWS Organizations API.
- Secara umum, AWS Control Tower melakukan satu tindakan pada satu waktu, yang harus diselesaikan sebelum tindakan lain dapat dimulai. Misalnya, jika Anda mencoba menyediakan akun saat proses mengaktifkan kontrol sudah beroperasi, penyediaan akun akan gagal.

  Pengecualian:

  - AWS Control Tower memungkinkan tindakan bersamaan untuk menerapkan kontrol opsional. Untuk informasi selengkapnya, lihat Penerapan bersamaan untuk kontrol opsional.
  - AWS Control Tower memungkinkan hingga sepuluh tindakan membuat, memperbarui, atau mendaftarkan akun secara bersamaan, dengan Account Factory.

> **Note**
>
> Untuk informasi selengkapnya tentang sumber daya yang dibuat oleh AWS Control Tower, lihatApa saja akun bersama?.

Kiat tentang akun dan OU

- Kami menyarankan agar Anda menyimpan setiap OU yang terdaftar hingga maksimum 1000 akun, sehingga Anda dapat memperbarui akun tersebut dengan kemampuan Re-register OU setiap kali pembaruan akun diperlukan, seperti saat Anda mengonfigurasi Wilayah baru untuk tata kelola.
- Untuk mengurangi waktu yang diperlukan saat mendaftarkan OU, kami sarankan Anda menyimpan jumlah akun per OU menjadi sekitar 680, meskipun batasnya adalah 1000 akun per OU. Sebagai aturan umum, waktu yang diperlukan untuk mendaftarkan OU meningkat sesuai dengan jumlah Wilayah di mana OU Anda beroperasi, dikalikan dengan jumlah akun di OU.
- Sebagai perkiraan, OU dengan 680 akun mungkin memerlukan hingga 2 jam untuk mendaftar dan mengaktifkan kontrol, dan hingga 1 jam untuk mendaftar ulang. Juga, OU yang memiliki banyak kontrol membutuhkan waktu lebih lama untuk mendaftar daripada OU dengan sedikit kontrol.
- Satu kekhawatiran tentang mengizinkan jangka waktu yang lebih lama untuk mendaftarkan OU adalah bahwa proses ini memblokir tindakan lain. Beberapa pelanggan merasa nyaman membiarkan waktu yang lebih lama untuk mendaftar atau mendaftar ulang OU, karena mereka lebih suka mengizinkan lebih banyak akun di setiap OU.

Kapan harus masuk sebagai pengguna root

Tugas administratif tertentu mengharuskan Anda masuk sebagai pengguna root. Anda dapat masuk sebagai pengguna root ke Akun AWS yang dibuat oleh pabrik akun di AWS Control Tower.

Anda harus masuk sebagai pengguna root untuk melakukan tindakan berikut:

- Ubah pengaturan akun tertentu, termasuk nama akun, kata sandi pengguna root, atau alamat email. Untuk informasi selengkapnya, lihat Memperbarui dan memindahkan akun dengan AWS Control Tower.
- Untuk menutup sebuah Akun AWS.

- Untuk informasi selengkapnya tentang tindakan yang memerlukan kredenal login pengguna root, lihat Tugas yang memerlukan kredenal pengguna root di Panduan Referensi.AWS Account Management

> **Note**
>
> Untuk mengubah atau mengaktifkan paket AWS Support Anda, Anda harus masuk sebagai pengguna root atau menjadi pengguna dengan izin IAM yang sesuai. .

Untuk masuk sebagai pengguna root

1. Buka halaman AWS masuk.

   Jika Anda tidak memiliki alamat email yang Anda perlukan akses, Anda bisa mendapatkannya dari AWS Control Tower. Akun AWS Buka konsol untuk akun manajemen, pilih Akun, dan cari alamat emailnya.
2. Masukkan alamat email yang Akun AWS Anda perlukan akses, lalu pilih Berikutnya.
3. Pilih Lupa kata sandi? agar instruksi pengaturan ulang kata sandi dikirim ke alamat email pengguna root.
4. Buka pesan email reset kata sandi dari kotak pesan pengguna root, lalu ikuti petunjuk untuk mengatur ulang kata sandi Anda.
5. Buka halaman AWS login, lalu masuk dengan kata sandi setel ulang.

Atau, Anda dapat menggunakan fitur AWS Root Access Management, yang memungkinkan tindakan root dilakukan pada akun anggota, tanpa perlu masuk sebagai Root. Untuk informasi selengkapnya, lihat Mengelola akses root secara terpusat untuk pelanggan yang menggunakan AWS Organizations.

AWS Organizations bimbingan

AWS Control Tower terkait erat dengan AWS Organizations. Berikut adalah beberapa panduan khusus tentang bagaimana mereka bekerja sama terbaik untuk melindungi AWS lingkungan Anda.

- Anda dapat menemukan panduan tentang praktik terbaik untuk melindungi keamanan akun manajemen AWS Control Tower dan akun anggota Anda dalam AWS Organizations dokumentasi.
  - Praktik terbaik untuk akun manajemen

  - Praktik terbaik untuk akun anggota
- Jangan mengubah atau melepaskan kebijakan kontrol layanan (SCP) yang dibuat AWS Control Tower untuk OU terdaftar. Memodifikasi atau melepaskan SCP ini dapat menyebabkan kontrol memasuki status yang tidak diketahui. Jika itu terjadi, Anda harus mengatur ulang landing zone atau mendaftarkan ulang OU Anda di AWS Control Tower. Sebagai gantinya, gunakan AWS Organizations untuk membuat SCP baru dan melampirkannya ke OU.
- Memindahkan akun individu, yang sudah terdaftar, ke AWS Control Tower, dari luar OU terdaftar, menyebabkan penyimpangan yang harus diselesaikan. Lihat Jenis penyimpangan tata kelola.
- Jika Anda menggunakannya AWS Organizations untuk membuat, mengundang, atau memindahkan akun dalam organisasi yang terdaftar di AWS Control Tower, akun tersebut tidak terdaftar oleh AWS Control Tower dan perubahan tersebut tidak dicatat. Jika Anda memerlukan akses ke akun ini melalui SSO, lihat Akses Akun Anggota.
- Jika Anda menggunakannya AWS Organizations untuk memindahkan OU ke organisasi yang dibuat oleh AWS Control Tower, OU eksternal tidak terdaftar oleh AWS Control Tower.
- AWS Control Tower menangani pemfilteran izin secara berbeda dari yang AWS Organizations dilakukan. Jika akun Anda disediakan dengan pabrik akun AWS Control Tower, pengguna akhir dapat melihat nama dan orang tua dari semua OU di konsol AWS Control Tower, meskipun mereka tidak memiliki izin untuk mengambil nama dan orang tua tersebut secara langsung. AWS Organizations
- AWS Control Tower tidak mendukung izin campuran pada organisasi, seperti izin untuk melihat induk OU tetapi tidak untuk melihat nama OU. Untuk alasan ini, administrator AWS Control Tower diharapkan memiliki izin penuh.
- AWS Organizations `FullAWSAccess`SCP harus diterapkan dan tidak boleh digabungkan dengan SCP lainnya. Perubahan pada SCP ini tidak dilaporkan sebagai drift; namun, beberapa perubahan dapat memengaruhi fungsionalitas AWS Control Tower dengan cara yang tidak dapat diprediksi, jika akses ke sumber daya tertentu ditolak. Misalnya, jika SCP terlepas, atau dimodifikasi, akun mungkin kehilangan akses ke AWS Config perekam atau membuat celah dalam CloudTrail pencatatan.
- Jangan gunakan AWS Organizations `DisableAWSServiceAccess` API untuk mematikan akses layanan AWS Control Tower ke organisasi tempat Anda menyiapkan landing zone. Jika Anda melakukannya, fitur deteksi drift AWS Control Tower tertentu mungkin tidak berfungsi dengan baik tanpa dukungan pesan dari AWS Organizations. Fitur deteksi drift ini membantu menjamin AWS Control Tower dapat melaporkan status kepatuhan unit organisasi, akun, dan kontrol di organisasi Anda secara akurat. Untuk informasi selengkapnya, lihat API_DisableAWSServiceAccessdi Referensi AWS Organizations API.

Panduan Pusat Identitas IAM

AWS Control Tower merekomendasikan agar Anda menggunakan AWS Identity and Access Management (IAM) untuk mengatur akses ke Anda Akun AWS. Namun, Anda memiliki opsi untuk memilih apakah AWS Control Tower menyiapkan IAM Identity Center untuk Anda, apakah Anda menyiapkan Pusat Identitas IAM untuk diri sendiri, dengan cara yang paling efektif memenuhi persyaratan bisnis Anda, atau memilih metode lain untuk akses akun.

> **Note**
>
> SSO adalah singkatan yang digunakan dalam industri teknologi untuk menunjukkan single sign-on. Secara umum, SSO adalah sesi dan layanan otentikasi pengguna. Ini memungkinkan seseorang untuk menggunakan satu set kredensi login untuk akses ke banyak aplikasi. Ketika mengacu pada kemampuan single-sign on AWS, kami mengacu pada AWS layanan yang disebut AWS Identity and Access Management, dan disingkat IAM atau IAM Identity Center.

Secara default, AWS Control Tower menyiapkan Pusat AWS Identitas IAM untuk landing zone Anda, selaras dengan panduan praktik terbaik yang ditentukan dalam Mengatur AWS lingkungan Anda menggunakan beberapa akun. Sebagian besar pelanggan memilih default. Metode akses alternatif kadang-kadang diperlukan, untuk kepatuhan peraturan di industri atau negara tertentu, atau di Wilayah AWS mana Pusat AWS Identitas IAM tidak tersedia.

Memilih opsi

Dari konsol, Anda dapat memilih untuk mengelola sendiri Pusat Identitas IAM selama proses penyiapan landing zone, daripada mengizinkan AWS Control Tower mengaturnya untuk Anda. Kapan saja nanti, Anda dapat memilih untuk mengubah pilihan ini, dengan memodifikasi pengaturan landing zone dan memperbarui landing zone Anda di halaman Pengaturan landing zone.

Untuk menghentikan AWS Pusat Identitas IAM di AWS Control Tower, atau untuk mulai menggunakan AWS Pusat Identitas IAM

1. Arahkan ke halaman Pengaturan landing zone
2. Pilih tab Konfigurasi
3. Kemudian pilih tombol radio yang sesuai, untuk mengubah pilihan Anda untuk AWS IAM Identity Center.

Setelah Anda memilih untuk mengelola sendiri Pusat Identitas AWS IAM sebagai IDP Anda, AWS Control Tower hanya membuat peran dan kebijakan yang diperlukan untuk mengelola AWS Control Tower, seperti dan. `AWSControlTowerAdmin` `AWSControlTowerAdminPolicy` Untuk zona pendaratan yang dikelola sendiri, AWS Control Tower tidak lagi membuat peran dan pengelompokan IAM untuk penggunaan khusus pelanggan — tidak selama proses pengaturan landing zone, maupun selama penyediaan akun dengan Account Factory.

> **Note**
>
> Jika Anda menghapus Pusat AWS Identitas IAM dari zona landing AWS Control Tower Anda, pengguna, grup, dan set izin yang dibuat AWS Control Tower tidak akan dihapus. Kami menyarankan Anda menghapus sumber daya ini.

Pelanggan Account Factory dengan penyedia identitas alternatif (IdPs) seperti Azure AD, Ping, atau Okta, dapat mengikuti proses AWS IAM Identity Center untuk terhubung ke penyedia identitas eksternal dan melakukan onboard IDP mereka. Anda dapat kembali membuat AWS Control Tower menghasilkan pengelompokan dan peran Anda kapan saja, dengan memodifikasi pengaturan landing zone.

- Untuk informasi spesifik tentang cara AWS Control Tower bekerja dengan IAM Identity Center berdasarkan sumber identitas Anda, lihat Pertimbangan untuk AWS IAM Identity Center pelanggan di bagian Pre-launch pemeriksaan di halaman Memulai Panduan Pengguna ini.
- Untuk informasi tambahan tentang bagaimana perilaku AWS Control Tower berinteraksi dengan IAM Identity Center dan berbagai sumber identitas, lihat Pertimbangan untuk Mengubah Sumber Identitas Anda di Panduan Pengguna Pusat Identitas IAM.
- Lihat Bekerja dengan AWS Pusat Identitas IAM dan AWS Control Tower untuk informasi selengkapnya tentang bekerja dengan AWS Control Tower dan IAM Identity Center.

Panduan Account Factory

> **Note**
>
> Penyediaan, pembaruan, dan penyesuaian akun tunggal harus menargetkan unit organisasi (OU) dengan AWSControlTowerBaseline diaktifkan. Jika OU tidak mengaktifkan, Anda dapat mengaktifkan pendaftaran otomatis akun atau penggunaan ResetEnabledBaseline dan ResetEnabledControl API pada EnabledBaselines dan EnabledControls pada

OU tersebut untuk mendaftarkan akun. AWSControlTowerBaseline Untuk detailnya AWSControlTowerBaseline, lihat:Jenis dasar yang berlaku di tingkat OU.

Anda dapat mengalami masalah saat menggunakan Account Factory untuk menyediakan akun baru di AWS Control Tower. Untuk informasi tentang cara memecahkan masalah ini, lihat bagian Penyediaan Akun Baru Gagal di Pemecahan Masalah Panduan Pengguna AWS Control Tower.

Kami menyarankan Anda membuat pengguna federasi atau peran IAM, bukan pengguna IAM. Pengguna federasi dan peran IAM memberi Anda kredensi sementara. Pengguna IAM memiliki kredensi jangka panjang yang sulit dikelola. Untuk informasi selengkapnya, lihat identitas IAM (pengguna, grup pengguna, dan peran) di Panduan Pengguna IAM.

Jika Anda diautentikasi sebagai pengguna IAM atau pengguna Pusat Identitas IAM saat menyediakan akun baru di Account Factory atau saat menggunakan fitur akun Daftar AWS Control Tower, verifikasi bahwa pengguna Anda memiliki akses ke portofolio Anda. AWS Service Catalog Jika tidak, Anda mungkin menerima pesan galat dari Service Catalog. Untuk informasi selengkapnya, lihat Kesalahan portofolio AWS Control Tower Account Factory di bagian Pemecahan Masalah pada Panduan Pengguna AWS Control Tower.

> **Note**
>
> Dengan pendaftaran otomatis dinonaktifkan: Hingga lima akun dapat disediakan secara bersamaan.
> Dengan pendaftaran otomatis diaktifkan: Hingga 5 akun dapat disediakan secara bersamaan, tetapi setiap operasi pemindahan akun aktif untuk tujuan OU memblokir semua penyediaan pada OU yang sama hingga selesai.

Panduan untuk berlangganan Topik SNS

Berlangganan topik SNS untuk mendapatkan informasi tentang lingkungan AWS Control Tower Anda.

> **Note**
>
> AWS Control Tower akan berhenti mengirimkan notifikasi drift ke topik SNS untuk semua pelanggan di LZ4.0 +.

- Topik `aws-controltower-AllConfigNotifications` SNS menerima semua acara yang diterbitkan oleh AWS Config, termasuk pemberitahuan kepatuhan dan pemberitahuan CloudWatch acara Amazon. Misalnya, topik ini memberi tahu Anda jika pelanggaran kontrol telah terjadi. Ini juga memberikan informasi tentang jenis acara lainnya. (Pelajari lebih lanjut AWS Configtentang apa yang mereka terbitkan saat topik ini dikonfigurasi.)
- Peristiwa Data dari `aws-controltower-BaselineCloudTrail` jejak diatur untuk dipublikasikan ke topik `aws-controltower-AllConfigNotifications` SNS juga.
- Untuk menerima pemberitahuan kepatuhan terperinci, kami sarankan Anda berlangganan topik `aws-controltower-AllConfigNotifications` SNS. Topik ini menggabungkan pemberitahuan kepatuhan dari semua akun anak.
- Untuk menerima pemberitahuan drift dan pemberitahuan lainnya serta pemberitahuan kepatuhan, tetapi lebih sedikit pemberitahuan secara keseluruhan, kami sarankan Anda berlangganan topik `aws-controltower-AggregateSecurityNotifications` SNS.
- Untuk menerima pemberitahuan tentang kesalahan AWS Control Tower Account Factory for Terraform (AFT), Anda dapat berlangganan topik SNS yang disebut aft_failure_notifications, yang ditampilkan di repositori AFT. Contoh:

```
resource "aws_sns_topic" "aft_failure_notifications" {
    name = "aft-failure-notifications"
    kms_master_key_id = "alias/aws/sns"
}
```

- Semua topik SNS dienkripsi saat istirahat dengan enkripsi disk. untuk informasi selengkapnya, lihat Enkripsi data.

Untuk informasi selengkapnya tentang topik dan kepatuhan SNS, lihat Pencegahan dan pemberitahuan.

Panduan untuk kunci KMS

AWS Control Tower bekerja dengan AWS Key Management Service (AWS KMS). Secara opsional, jika Anda ingin mengenkripsi dan mendekripsi sumber daya AWS Control Tower Anda dengan kunci enkripsi yang Anda kelola, Anda dapat membuat dan mengonfigurasi. AWS KMS keys Anda dapat menambahkan atau mengubah kunci KMS setiap kali Anda memperbarui landing zone Anda. Sebagai praktik terbaik, kami sarankan menggunakan kunci KMS Anda sendiri dan mengubahnya dari waktu ke waktu.

AWS KMS memungkinkan Anda membuat kunci KMS Multi-wilayah dan tombol asimetris. Namun, AWS Control Tower tidak mendukung kunci Multi-region atau kunci asimetris. AWS Control Tower melakukan pra-pemeriksaan kunci yang ada. Anda mungkin melihat pesan galat jika memilih tombol Multi-region atau tombol asimetris. Dalam hal ini, buat kunci lain untuk digunakan dengan sumber daya AWS Control Tower.

Untuk pelanggan yang mengoperasikan klaster AWS CloudHSM: Buat toko kunci khusus yang terkait dengan klaster CloudHSM Anda. Kemudian Anda dapat membuat kunci KMS, yang berada di toko kunci kustom CloudHSM yang Anda buat. Anda dapat menambahkan kunci KMS ini ke AWS Control Tower.

Anda harus membuat pembaruan khusus pada kebijakan izin kunci KMS agar berfungsi dengan AWS Control Tower. Untuk detailnya, lihat bagian yang disebutMemperbarui kebijakan kunci KMS.

Praktik terbaik untuk pembaruan landing zone

Bagian ini memberikan beberapa pertimbangan dan praktik terbaik yang perlu diingat saat Anda mempertimbangkan peningkatan versi landing zone Anda di AWS Control Tower. Perubahan dari seri versi landing zone 2.0 menjadi seri versi landing zone 3.0 sangat penting. Saat Anda meningkatkan landing zone, AWS Control Tower secara otomatis memindahkan Anda ke versi terbaru yang tersedia.

> **Note**
>
> Ini adalah praktik terbaik untuk memperbarui ke versi terbaru dari landing zone.

Ringkasan praktik terbaik yang dijelaskan di bagian ini

- Praktik terbaik: Untuk alasan keamanan dan audit, kami sangat menyarankan Anda mengaktifkan pencatatan di seluruh papan, untuk semua akun, dan mengirim informasi pencatatan ke lokasi terpusat. Di AWS Control Tower, lokasi terpusat ini adalah akun arsip Log, yang menyediakan bucket logging Amazon S3.
- Praktik terbaik: Jika Anda memilih keluar dari CloudTrail jejak tingkat organisasi di AWS Control Tower, siapkan dan kelola jalur Anda sendiri.
- Praktik terbaik: Saat mengoperasikan lingkungan AWS Control Tower, siapkan lingkungan pengujian.

Manfaat untuk berpindah dari versi landing zone 2.x ke versi landing zone 3.x

- Catat AWS Config sumber daya hanya di Wilayah asal, yang menciptakan penghematan biaya saat Anda mengelola sumber daya global
- Enkripsi AWS CloudTrail jejak Anda dengan kunci KMS Anda sendiri
- Sesuaikan jangka waktu penyimpanan log Anda
- Kontrol wajib yang ditingkatkan
- Peningkatan jumlah kontrol yang tersedia
- Terintegrasi dengan AWS Security Hub CSPM
- Pembaruan runtime Python

Peringatan untuk pindah dari versi landing zone 2.x ke versi landing zone 3.x

- Dengan landing zone 3.0 dan versi lebih baru, AWS Control Tower tidak lagi mendukung AWS CloudTrail jalur tingkat akun yang mengelola. AWS
- Anda memiliki opsi untuk memilih jejak tingkat organisasi yang dikelola oleh AWS Control Tower, atau memilih keluar darinya dan mengelola jalur Anda sendiri CloudTrail .
- Beberapa potensi ada untuk biaya ganda, terutama jika beberapa akun dalam OU tidak terdaftar di AWS Control Tower dan memiliki jejak tingkat akun sendiri yang ingin Anda pertahankan.

Pertimbangan tentang memilih jalur tingkat organisasi CloudTrail

- Saat Anda meningkatkan ke 3.0 atau versi lebih baru, AWS Control Tower menghapus jejak tingkat akun yang awalnya dibuat, setelah 24 jam. [Pengecualian]
- Tidak ada data dari jalur ini yang hilang. Log Anda yang ada dipertahankan bahkan ketika jejak dihapus.
- AWS Control Tower membuat jalur baru di bucket Amazon S3 yang sama untuk jalur, untuk membedakan jejak tingkat akun dari jalur tingkat organisasi.
  - Jalur log jejak akun adalah dari formulir ini: `/orgId/AWSLogs/...`
  - Jalur log jejak organisasi adalah dari formulir ini: `/orgId/AWSLogs/orgId/...`
- CloudTrail Jalur tambahan yang telah Anda gunakan, jalur yang tidak digunakan oleh AWS Control Tower, tidak disentuh.
- Semua akun disertakan dalam jejak tingkat organisasi—termasuk akun yang tidak terdaftar di AWS Control Tower—jika akun yang tidak terdaftar merupakan bagian dari OU terdaftar.

- CloudWatch Alarm Amazon di akun tertaut tidak dipicu.
- Jika Anda memilih keluar dari jejak tingkat organisasi, AWS Control Tower masih membuat jejak, tetapi menetapkan statusnya ke Off.
- Sebagai praktik terbaik, jika Anda memilih keluar dari jejak tingkat organisasi di AWS Control Tower, Anda harus menyiapkan dan mengelola jalur Anda sendiri CloudTrail ,

Manfaat jalur tingkat organisasi

- Jejak organisasi bekerja di semua akun di OU.
- Item yang dicatat distandarisasi dan tidak dapat dimodifikasi oleh pengguna akun.

Pertimbangkan lingkungan pengujian

Saat Anda memutakhirkan landing zone, AWS Control Tower hanya membuat perubahan pada akun bersama dan Foundational OU. Itu tidak membuat perubahan pada akun beban kerja atau OU Anda. Namun, sebagai praktik terbaik, saat mengoperasikan lingkungan AWS Control Tower, kami menyarankan Anda menyiapkan lingkungan pengujian. Dalam lingkungan pengujian yang terisolasi, Anda dapat menguji upgrade landing zone AWS Control Tower, serta perubahan apa pun yang mungkin Anda lakukan pada kebijakan kontrol layanan (SCP), dan Anda dapat menguji kontrol yang ingin Anda terapkan pada lingkungan. Rekomendasi ini sangat membantu jika Anda beroperasi di industri yang diatur.

Daftar periksa untuk kesalahan umum saat memperbarui

Berikut adalah daftar singkat tugas yang dapat Anda lakukan untuk menghindari kesalahan umum saat memperbarui landing zone AWS Control Tower Anda dari versi 2.x ke versi 3.x.

Daftar periksa pembaruan dasar

- Periksa landing zone Anda:

  — Buka layanan AWS Control Tower, tinjau halaman Unit Organisasi dan Akun, lalu konfirmasikan bahwa status akun Anda disetel ke Terdaftar dan Terdaftar.

  — Jika berlaku, verifikasi dan konfirmasikan bahwa proses terakhir dari pipeline kustomisasi Anda berhasil.

  — Periksa bucket logging terpusat Amazon S3 di akun Audit, karena setiap perubahan yang sebelumnya dibuat pada kebijakan bucket akan ditimpa.

- Validasi bahwa SCP apa pun yang tidak dimiliki AWS Control Tower tidak akan membatasi `AWSControlTowerExecution` peran untuk melakukan tindakan di akun anggota, atau tindakan di akun manajemen, untuk peran administratif yang melakukan pembaruan.

AI-based layanan dan AWS Control Tower

Anda dapat membuat kebijakan kontrol layanan (SCP) yang memungkinkan Anda memilih untuk tidak menyimpan data Anda oleh AI-based layanan. AWS Kebijakan SCP ini menentukan bahwa AI-based layanan, seperti Amazon Rekognition CodeWhisperer atau Amazon, tidak dapat menyimpan dan menggunakan data AI-based AWS Anda untuk meningkatkan layanan lainnya.

Kebijakan SCP opt-out AI ini dapat berlaku untuk seluruh organisasi Anda, ke OU, atau ke akun tertentu. Kebijakan tersebut berlaku secara global. Anda dapat menemukan informasi lebih lanjut tentang kebijakan ini di kebijakan opt-out layanan AI, dalam dokumentasi. AWS Organizations

Untuk daftar AWS layanan yang menggunakan AI, bersama dengan contoh kebijakan, lihat sintaks kebijakan opt-out layanan AI dan contoh, di Panduan Pengguna.AWS Organizations

Manajemen pembaruan konfigurasi di AWS Control Tower

Merupakan tanggung jawab anggota tim administrator cloud pusat Anda untuk memperbarui landing zone Anda. Memperbarui landing zone Anda memastikan AWS Control Tower ditambal dan diperbarui. Selain itu, untuk melindungi landing zone Anda dari potensi masalah kepatuhan, anggota tim administrator cloud pusat harus menyelesaikan masalah drift segera setelah terdeteksi dan dilaporkan.

> **Note**
>
> Konsol AWS Control Tower menunjukkan kapan landing zone Anda perlu diperbarui. Jika Anda tidak melihat opsi untuk memperbarui, landing zone Anda sudah up to date.

Tabel berikut berisi daftar rilis pembaruan landing zone AWS Control Tower, dengan tautan ke deskripsi setiap rilis.

Versi	Tanggal rilis	Deskripsi
4.0	11-17-2025	Zona pendaratan versi 4.0
3.3	12-12-2023	Zona pendaratan versi 3.3
3.2	6-09-2023	Zona pendaratan versi 3.2
3.1	2-09-2023	Zona pendaratan versi 3.1
3.0	7-26-2022	Zona pendaratan versi 3.0
2.9	4-22-2022	Zona pendaratan versi 2.9
2.8	2-10-2022	Zona pendaratan versi 2.8
2.7	4-8-2021	Zona pendaratan versi 2.7
2.6	12-29-2020	Zona pendaratan versi 2.6
2.5	11-18-2020	Zona pendaratan versi 2.5

Versi	Tanggal rilis	Deskripsi
2.4	Tidak ada	Tidak ada
2.3	3-5-2020	Zona pendaratan versi 2.3
2.2	11-13-19	Zona pendaratan versi 2.2
2.1	6-24-19	Zona pendaratan versi 2.1

Setiap kali Anda memperbarui landing zone Anda, Anda memiliki kesempatan untuk mengubah pengaturan landing zone Anda.

Manfaat memperbarui

- Anda dapat mengubah Wilayah yang diatur
- Anda dapat mengubah kebijakan penyimpanan log
- Anda dapat menambahkan atau menghapus kontrol penolakan Wilayah
- Anda dapat menerapkan kunci enkripsi AWS KMS
- Anda dapat mengaktifkan atau menonaktifkan jejak tingkat organisasi CloudTrail Anda.
- Anda dapat mengatasi drift landing zone

Saat memperbarui landing zone, Anda akan menerima fitur terbaru untuk AWS Control Tower, secara otomatis. Lihat versi landing zone Anda saat ini di halaman pengaturan zona pendaratan.

Jika pembaruan gagal, AWS Control Tower tidak memutar kembali ke versi landing zone sebelumnya. Anda mungkin menemukan landing zone Anda dalam keadaan tak tentu. Jika demikian, hubungi AWS dukungan. Untuk informasi selengkapnya tentang pemecahan masalah kegagalan untuk memperbarui, lihat. Tidak Dapat Memperbarui Zona Pendaratan

Anda memiliki kesempatan untuk menghapus pemetaan Pusat AWS Identitas yang tidak terpakai (sebelumnya disebut AWS SSO) saat Anda memperbarui landing zone Anda. Untuk informasi selengkapnya, lihat Catatan Bidang: Hapus Pemetaan Pusat Identitas IAM yang Tidak Digunakan Secara Otomatis Selama Peningkatan AWS Control Tower.

Prasyarat untuk Update dan Reset - matikan Requester Pays

Sebelum memperbarui atau mengatur ulang landing zone, pastikan bucket logging Amazon S3 untuk akun Arsip Log tidak mengaktifkan fitur Requester Pays. Anda harus mematikan fitur tersebut sebelum memulai proses Update atau Reset. Saat AWS Control Tower menyiapkan bucket logging Anda, fitur ini tidak diaktifkan. Oleh karena itu, hanya pelanggan yang kemudian mengaktifkan fitur Requester Pays yang harus mematikannya. Untuk informasi selengkapnya, lihat kebijakan bucket Amazon S3 untuk CloudTrail dan Menggunakan bucket Requester Pays.

Tentang pembaruan landing zone

Pembaruan diperlukan untuk memperbaiki penyimpangan tata kelola, atau untuk pindah ke AWS Control Tower versi baru. Untuk melakukan pembaruan lengkap AWS Control Tower, Anda harus memperbarui landing zone terlebih dahulu dan kemudian memperbarui akun yang terdaftar satu per satu. Anda mungkin perlu melakukan tiga jenis pembaruan pada waktu yang berbeda.

- Pembaruan landing zone: Paling sering jenis pembaruan ini dilakukan dengan memilih Perbarui pada halaman pengaturan zona pendaratan. Anda mungkin perlu melakukan pembaruan landing zone untuk menyelesaikan jenis drift tertentu, dan Anda dapat memilih Reset bila diperlukan.
- Pembaruan satu atau beberapa akun individual: Anda harus memperbarui akun jika informasi terkait berubah, atau jika jenis penyimpangan tertentu telah terjadi. Jika akun memerlukan pembaruan, status akun akan menampilkan Pembaruan yang tersedia di halaman Akun.

  Untuk memperbarui satu akun, navigasikan ke halaman detail akun dan pilih Perbarui akun. Akun juga dapat diperbarui dengan proses manual, dengan memilih Re-register OU, atau dengan pendekatan skrip otomatis, yang dijelaskan di bagian selanjutnya dari halaman ini.
- Pembaruan lengkap: Pembaruan lengkap mencakup pembaruan landing zone Anda, diikuti dengan pembaruan semua akun terdaftar di OU terdaftar Anda. Pembaruan lengkap diperlukan dengan rilis baru AWS Control Tower seperti 3.0, 3.2, dan seterusnya. Untuk membuat proses pembaruan penuh lebih mudah, untuk OU dengan 1000 atau lebih sedikit akun, Anda dapat memilih Re-register OU untuk memperbarui semua akun dalam OU itu, dan ulangi perintah Re-registerOU untuk setiap OU.

Untuk informasi selengkapnya tentang pembaruan landing zone, lihat Praktik terbaik untuk pembaruan landing zone.

> **Note**
>
> Setelah menyelesaikan pembaruan landing zone, Anda tidak dapat membatalkan pembaruan atau downgrade ke versi sebelumnya.

Perbarui landing zone Anda

Cara termudah untuk memperbarui landing zone AWS Control Tower adalah melalui halaman pengaturan zona pendaratan, yang dapat Anda jangkau dengan memilih pengaturan zona pendaratan di navigasi kiri dasbor AWS Control Tower.

Halaman pengaturan zona pendaratan menunjukkan versi landing zone saat ini, dan mencantumkan versi terbaru yang mungkin tersedia. Anda dapat memilih tombol Perbarui jika Anda perlu memperbarui versi Anda.

> **Note**
>
> Atau, Anda dapat memperbarui landing zone Anda secara manual. Pembaruan membutuhkan waktu yang kira-kira sama, apakah Anda menggunakan tombol Perbarui atau proses manual. Untuk melakukan pembaruan manual pada landing zone Anda saja, lihat langkah 1 dan 2 yang mengikuti.

Prosedur pembaruan standar

Prosedur berikut memandu Anda melalui langkah-langkah pembaruan lengkap untuk AWS Control Tower dari konsol. Untuk memperbarui akun individual, lihatPerbarui akun di konsol.

Untuk memperbarui landing zone Anda, dengan sejumlah akun per OU

1. Buka browser web, dan navigasikan ke konsol AWS Control Tower di https://console.aws.amazon.com/controltower/home/update.
2. Tinjau informasi di wizard dan pilih Perbarui. Ini memperbarui backend landing zone serta akun bersama Anda. Proses ini bisa memakan waktu sedikit lebih dari setengah jam.
3. Perbarui akun anggota Anda (prosedur ini harus diikuti untuk OU yang berisi lebih dari 1000 akun).
4. Dari panel navigasi kiri, pilih Organisasi.

5. Untuk memperbarui setiap akun, ikuti langkah-langkah yang diberikanPerbarui akun di konsol.

> **Opsional Re-register OU untuk memperbarui akun**
>
> Untuk AWS Control Tower OU terdaftar dengan kurang dari 1000 akun, Anda dapat membuka halaman OU di dasbor dan memilih Re-registerOU untuk memperbarui akun di OU tersebut.

Pilih versi landing zone

Jika Anda menjalankan AWS Control Tower landing zone versi 3.1 dan yang lebih baru, Anda dapat memilih untuk tetap menggunakan versi saat ini, atau Anda dapat meningkatkan ke versi yang lebih baru, saat Anda melakukan operasi Pembaruan atau Reset pada konfigurasi landing zone Anda. Operasi Reset adalah cara terbaik untuk memperbaiki drift, dalam banyak situasi.

Anda dapat memilih versi landing zone di konsol AWS Control Tower, atau melalui AWS Control Tower API.

> **Note**
>
> Jika Anda memilih untuk menerapkan versi landing zone yang melompati versi perantara, misalnya jika Anda berpindah dari 3.1 ke 3.3, AWS Control Tower secara otomatis menerapkan versi perantara sebagai bagian dari operasi pembaruan.
> Dalam percakapan, pindah ke versi yang lebih baru sering disebut sebagai peningkatan, bukan hanya pembaruan. Kedua konsep ini berbeda, karena Anda dapat memperbarui pengaturan landing zone tanpa memutakhirkan ke versi baru, misalnya, dengan mengubah Wilayah yang Anda atur. Di konsol, tombol Perbarui melakukan pembaruan di tempat atau operasi pemutakhiran, berdasarkan versi landing zone Anda saat ini dan yang Anda pilih untuk diterapkan.

Pilih versi landing zone Anda — prosedur konsol

1. Dari konsol AWS Control Tower, navigasikan ke halaman pengaturan zona pendaratan. Dalam tabel zona pendaratan yang tersedia, pilih versi baru. Ingat bahwa Anda dapat memilih versi 3.1 atau yang lebih baru. Versi sebelumnya 3.1 tidak kompatibel dengan fitur ini.

2. Ketika Anda memilih versi dari tabel, Anda dapat melihat tindakan yang tersedia. Pembaruan tersedia jika versi Anda saat ini lebih awal dari versi yang dipilih. Reset tersedia jika versi Anda saat ini adalah 3.1 atau yang lebih baru.
3. Setelah Anda memilih versi, pilih tombol Perbarui atau tombol Reset, di area kanan atas layar.
4. Anda akan melihat tampilan konfirmasi yang menunjukkan versi landing zone yang telah Anda pilih untuk penerapan. Untuk melanjutkan, pilih Berikutnya di kanan bawah. Operasi pembaruan Anda mungkin memakan waktu beberapa menit atau lebih.
5. Setelah landing zone diperbarui, Anda mungkin perlu memperbarui OU terdaftar Anda. Untuk memperbarui OU, Anda harus mendaftar ulang dengan menggunakan proses Re-register OU. Re-registering OU menerapkan baseline yang diperbarui ke semua akun di OU tersebut.

Pembaruan akun, versi landing zone, dan baseline

Zona pendaratan AWS Control Tower adalah AWS sumber daya yang sesuai dengan serangkaian konfigurasi dasar. Tidak ada pemetaan satu-ke-satu versi baseline dan landing zone. Anda dapat melihat tabel yang menunjukkanKompatibilitas baseline OU dan versi landing zone.

Ketika Anda melompat ke versi dasar, Anda harus memperbarui akun setelah pembaruan landing zone Anda. Misalnya, saat memutakhirkan dari 3.1 ke 3.2, Anda tidak perlu memperbarui akun Anda, karena versi landing zone ini memiliki baseline yang sama.

Sebaliknya, jika Anda memutakhirkan dari 3.1 ke 3.3, Anda harus memperbarui akun, karena versi dasarnya adalah 4.0, yang mencakup 3,2 hingga 3,3.

Untuk informasi selengkapnya tentang hubungan antara versi landing zone dan baseline, lihat. Kompatibilitas baseline OU dan versi landing zone

AWS CloudTrail Pertahankan jalur selama pembaruan landing zone

Anda dapat memilih untuk mempertahankan AWS CloudTrail jejak tingkat akun saat memutakhirkan versi landing zone AWS Control Tower.

Prasyarat

- Versi landing zone Anda kurang dari 3.0.
- Operasi Buat atau Perbarui terbaru Anda berhasil.

Untuk mempertahankan jejak tingkat akun dan ikut serta dalam jalur tingkat organisasi CloudTrail

1. Hubungi AWS Support dengan permintaan untuk mengizinkan daftar akun Anda.
2. Tim dukungan mengonfirmasi kapan akun target diizinkan terdaftar.
3. Setelah konfirmasi, perbarui landing zone Anda ke versi 3.1 atau lebih tinggi, dan pilih AWS CloudTrail konfigurasi - Diaktifkan.

Untuk mempertahankan jejak tingkat akun dan memilih keluar dari CloudTrail jalur yang dikelola oleh AWS Control Tower

1. Hubungi AWS Support dengan permintaan untuk mengizinkan daftar akun Anda.
2. Tim dukungan mengonfirmasi kapan akun target diizinkan terdaftar.
3. Setelah konfirmasi, perbarui landing zone Anda ke versi 3.1 atau lebih tinggi dan pilih AWS CloudTrail konfigurasi - Tidak Diaktifkan.

> **Important**
>
> Setelah CloudTrail jejak tingkat akun dipertahankan, kami tidak dapat menghapus jejak atau menghapus akun Anda dari daftar izin.

Cara membuat permintaan dukungan untuk mempertahankan jejak tingkat akun Anda

Jika Anda perlu mempertahankan jejak tingkat akun selama pembaruan Zona Pendaratan, Anda harus menghubungi AWS Support untuk menambahkan akun Anda ke daftar izin AWS Control Tower. Ikuti langkah-langkah berikut untuk mengirimkan tiket dukungan:

1. Masuk ke Konsol AWS Manajemen.
2. Arahkan ke AWS Support Center.
3. Pilih Buat kasus.
4. Untuk tipe Kasus, pilih Dukungan teknis.
5. Untuk Layanan, pilih AWS Control Tower.
6. Untuk Kategori, pilih Panduan Umum.
7. Di baris Subjek, sertakan frasa berikut:

```
Allow retention of account-level trails during Landing Zone update
```

8. Di bidang Deskripsi, berikan detail berikut:
   - Nomor akun AWS Manajemen Anda
   - Wilayah beranda yang dipilih untuk lingkungan AWS Control Tower
9. Lengkapi kolom lain yang diperlukan dalam formulir kasus dukungan.
10. Pilih Kirim untuk membuat kasus dukungan.

Setelah Anda mengirimkan tiket, AWS Support meninjau permintaan Anda dan menambahkan akun Anda ke daftar izin, jika sesuai. Anda akan menerima instruksi dan konfirmasi lebih lanjut melalui saluran komunikasi kasus dukungan.

> **Note**
>
> Untuk menghapus jejak tingkat akun setelah diizinkan, gunakan akun manajemen untuk menghapus kumpulan CloudFormation tumpukan atau instance tumpukan tertentu. Semua sumber daya dalam tumpukan dihapus.

Selesaikan drift dengan Reset dan Re-register

Drift sering terjadi saat Anda dan anggota organisasi Anda menggunakan landing zone.

Deteksi drift otomatis di AWS Control Tower. Pemindaian otomatis SCP Anda membantu Anda mengidentifikasi sumber daya yang memerlukan perubahan atau pembaruan konfigurasi yang harus dilakukan untuk mengatasi penyimpangan.

Untuk memperbaiki banyak jenis drift, pilih Reset pada halaman pengaturan zona pendaratan di konsol. Selain itu, Anda dapat menyelesaikan beberapa jenis drift dengan memilih Re-registerOU di konsol. Untuk kontrol, Anda dapat menyelesaikan drift secara terprogram dengan memanggil API. ResetEnabledControl Untuk informasi selengkapnya tentang jenis drift dan cara mengatasinya, lihat Jenis penyimpangan tata kelola danMendeteksi dan mengatasi penyimpangan di AWS Control Tower.

Satu kasus khusus resolusi drift terjadi untuk penyimpangan peran. Jika peran yang diperlukan tidak tersedia, konsol akan menampilkan halaman peringatan dan beberapa petunjuk tentang cara mengembalikan peran. Landing zone Anda tidak tersedia sampai drift peran diselesaikan. Reset drift ini tidak sama dengan reset full landing zone. Untuk informasi selengkapnya, lihat Jangan menghapus peran yang diperlukan di bagian yang dipanggilJenis drift untuk segera diselesaikan.

⚠ Saat Anda mengambil tindakan untuk menyelesaikan drift pada versi landing zone, perilakunya bergantung pada versi Anda saat ini.

- Jika Anda menggunakan landing zone versi 3.1 atau lebih tinggi, Anda dapat memilih Perbarui untuk mengubah konfigurasi landing zone tanpa memutakhirkan versi, atau memilih Reset untuk menerapkan kembali konfigurasi yang disimpan ke sumber daya zona pendaratan drifted Anda. Drift diselesaikan sebagai bagian dari proses pembaruan.
- Jika Anda menggunakan versi landing zone lebih awal dari 3.1, Anda tidak dapat memilih Reset. Anda harus memilih Perbarui dan tingkatkan landing zone Anda ke setidaknya versi 3.1.

Menyediakan dan memperbarui akun menggunakan otomatisasi

Note

Penyediaan, pembaruan, dan penyesuaian akun tunggal harus menargetkan unit organisasi (OU) dengan AWSControlTowerBaseline diaktifkan. Jika OU tidak mengaktifkan, Anda dapat mengaktifkan pendaftaran otomatis akun atau penggunaan ResetEnabledBaseline dan ResetEnabledControl API pada EnabledBaselines dan EnabledControls pada OU tersebut untuk mendaftarkan akun. AWSControlTowerBaseline Untuk detailnya AWSControlTowerBaseline, lihat:Jenis dasar yang berlaku di tingkat OU.

Anda dapat menyediakan atau memperbarui akun individual di AWS Control Tower dengan beberapa metode:

- Anda dapat menyediakan dan menyesuaikan akun dengan AWS Control Tower Account Factory for Terraform (AFT). Untuk informasi selengkapnya, lihat Ikhtisar Pabrik Akun Menara Kontrol AWS untuk Terraform (AFT).
- Anda dapat memperbarui akun dengan Kustomisasi untuk AWS Control Tower (CFCT). Untuk informasi selengkapnya, lihat Kustomisasi untuk ikhtisar AWS Control Tower (CFCT).
- Otomatisasi skrip: Jika Anda lebih suka menggunakan pendekatan API, Anda dapat memperbarui akun menggunakan kerangka kerja API Service Catalog dan memperbarui akun dalam proses batch. AWS CLI Anda akan memanggil `UpdateProvisionedProduct`API Service Catalog untuk setiap akun. Anda dapat menulis skrip untuk memperbarui akun, satu per satu, dengan API

ini. Informasi lebih lanjut tentang pendekatan ini, saat menambahkan Wilayah untuk tata kelola, tersedia di posting blog, Mengaktifkan pagar pembatas di Wilayah baru. AWS

Anda dapat memperbarui sebanyak lima (5) akun sekaligus. Anda harus menunggu setidaknya satu pembaruan akun agar berhasil sebelum memulai pembaruan akun berikutnya. Karena itu, prosesnya mungkin memakan waktu lama jika Anda memiliki banyak akun, tetapi tidak rumit. Untuk informasi lebih lanjut tentang pendekatan ini, lihatMengotomatiskan Penyediaan Akun di AWS Control Tower menurut Service Catalog API.

Panduan video

Panduan VideoIni dirancang untuk penyediaan akun otomatis dengan skrip, tetapi langkah-langkahnya juga berlaku untuk pembaruan akun. Gunakan `UpdateProvisionedProduct` API alih-alih `ProvisionProduct` API.

Langkah selanjutnya dari otomatisasi dengan skrip adalah memeriksa status Sukses dari peristiwa `UpdateLandingZone` siklus hidup AWS Control Tower. Gunakan sebagai pemicu untuk mulai memperbarui akun individual seperti yang dijelaskan dalam video. Peristiwa siklus hidup menandai penyelesaian urutan aktivitas, sehingga terjadinya peristiwa ini berarti pembaruan landing zone selesai. Pembaruan landing zone harus lengkap sebelum pembaruan akun dimulai. Untuk informasi selengkapnya tentang bekerja dengan peristiwa siklus hidup, lihat Peristiwa Siklus Hidup.

Lihat juga:

- Gunakan AWS CloudShell untuk bekerja dengan AWS Control Tower.
- Otomatisasi tugas di AWS Control Tower.

Otomatisasi tugas di AWS Control Tower

Banyak pelanggan lebih suka mengotomatiskan tugas di AWS Control Tower, seperti penyediaan akun, penugasan kontrol, dan audit. Anda dapat mengatur tindakan otomatis ini dengan panggilan ke:

- AWS Service Catalog API
- AWS Organizations API
- API Menara Kontrol AWS
- AWS CLI
- Acara Siklus Hidup

Informasi dan tautan tambahanHalaman ini berisi tautan ke banyak posting blog teknis yang sangat baik yang dapat membantu Anda mengotomatiskan tugas di AWS Control Tower. Bagian berikut menyediakan tautan ke area dalam Panduan Pengguna Menara Kontrol AWS ini yang dapat membantu Anda mengotomatiskan tugas.

Mengotomatiskan tugas kontrol

Anda dapat mengotomatiskan tugas yang terkait dengan penerapan dan penghapusan kontrol (juga dikenal sebagai pagar pem batas) melalui AWS Control Tower API. Untuk detailnya, lihat Referensi API Menara Kontrol AWS.

Untuk informasi selengkapnya tentang cara melakukan operasi kontrol dengan AWS Control Tower API, lihat posting blog AWS Control Tower merilis API, kontrol yang telah ditentukan sebelumnya ke unit organisasi Anda.

Mengotomatiskan tugas zona pendaratan

API zona pendaratan AWS Control Tower membantu Anda mengotomatiskan tugas tertentu yang terkait dengan zona pendaratan Anda. Untuk detailnya, lihat Referensi API Menara Kontrol AWS.

Mengotomatiskan pendaftaran OU

API dasar AWS Control Tower membantu Anda mengotomatiskan tugas-tugas tertentu, seperti mendaftarkan OU. Untuk detailnya, lihat Referensi API Menara Kontrol AWS.

Penutupan akun otomatis

Anda dapat mengotomatiskan penutupan akun anggota AWS Control Tower dengan AWS Organizations API. Untuk informasi selengkapnya, lihat Menutup akun anggota AWS Control Tower melalui AWS Organizations.

Penyediaan dan pembaruan akun otomatis

Kustomisasi Pabrik Akun AWS Control Tower (AFC) membantu Anda membuat akun dari konsol AWS Control Tower, dengan CloudFormation templat khusus yang kami sebut sebagai cetak biru. Proses ini otomatis dalam arti bahwa Anda dapat membuat akun baru dan memperbarui akun berulang kali, setelah menyiapkan cetak biru tunggal, tanpa memelihara pipeline.

AWS Control Tower Account Factory for Terraform (AFT) mengikuti GitOps model untuk mengotomatiskan proses penyediaan akun dan pembaruan akun di AWS Control Tower. Untuk informasi selengkapnya, lihat Menyediakan akun dengan AWS Control Tower Account Factory untuk Terraform (AFT).

Kustomisasi untuk AWS Control Tower (CfCT) membantu Anda menyesuaikan zona pendaratan AWS Control Tower dan tetap selaras dengan praktik AWS terbaik. Kustomisasi diimplementasikan dengan AWS CloudFormation template, kebijakan kontrol layanan (SCP), dan kebijakan kontrol sumber daya (RCP). Untuk informasi selengkapnya, lihat Kustomisasi untuk ikhtisar AWS Control Tower (CFCT).

Untuk informasi selengkapnya dan video tentang penyediaan akun otomatis, lihat Panduan: Penyediaan akun otomatis di Menara Kontrol AWS dan Penyediaan Otomatis dengan peran IAM.

Lihat juga Memper barui akun dengan skrip.

Audit akun secara terprogram

Untuk informasi selengkapnya tentang mengaudit akun secara terprogram, lihat Peran terprogram dan hubungan kepercayaan untuk akun audit AWS Control Tower.

Mengotomatiskan tugas lain

Untuk informasi tentang cara meningkatkan kuota layanan AWS Control Tower tertentu dengan metode permintaan otomatis, lihat video ini: Otom atisasi Peningkatan Batas Layanan.

Untuk blog teknis yang mencakup kasus penggunaan otomatisasi dan integrasi, lihat Otomatisasi dan integrasi.

Dua sampel open source tersedia GitHub untuk membantu Anda dengan tugas-tugas otomatisasi tertentu yang terkait dengan keamanan.

- Sampel yang disebut aws-control-tower-org-setup-sample menunjukkan cara mengotomatiskan pengaturan akun Audit sebagai administrator yang didelegasikan untuk layanan terkait keamanan.
- Sampel yang disebut aws-control-tower-account-setup-using-step-functions menunjukkan cara mengotomatiskan praktik terbaik keamanan menggunakan Fungsi Langkah, saat menyediakan dan mengonfigurasi akun baru. Contoh ini termasuk menambahkan prinsipal ke AWS Service Catalog portofolio bersama organisasi dan mengaitkan grup Pusat Identitas AWS IAM di seluruh organisasi ke akun baru secara otomatis. Ini juga menggambarkan cara menghapus VPC default di setiap Wilayah.

Arsit AWS ektur Referensi Keamanan mencakup contoh kode untuk mengotomatisasi tugas yang terkait dengan AWS Control Tower. Untuk informasi selengkapnya, lihat halaman Panduan AWS Preskriptif dan GitHub repositori https://github.com/aws-samples/aws-security-reference-architecture-examples/tree/main/aws_sra_examples terkait.

Untuk informasi tentang menggunakan AWS Control Tower dengan AWS CloudShell, AWS layanan yang memfasilitasi bekerja di AWS CLI, lihat AWS CloudShell dan AWS CLI.

Karena AWS Control Tower adalah lapisan orkestrasi untuk AWS Organizations, banyak AWS layanan lain tersedia melalui API dan AWS CLI. Untuk informasi selengkapnya, lihat AWS Layanan terkait.

Anda dapat memperpanjang otomatisasi dengan menggunakan peristiwa siklus hidup yang dipancarkan AWS Control Tower. Peristiwa ini dapat dipantau melalui EventBridge aturan Amazon, yang kemudian dapat memicu otomatisasi khusus, seperti memanggil AWS Lambda fungsi untuk menerapkan tag, mengonfigurasi sumber daya, atau memberi tahu tim ketika akun tertentu atau peristiwa terkait kontrol terjadi di zona pendaratan Anda.

Untuk informasi selengkapnya tentang peristiwa siklus hidup, lihat Peristiwa siklus hidup di AWS Control Tower.

Gunakan AWS CloudShell untuk bekerja dengan AWS Control Tower

AWS CloudShell adalah AWS layanan yang memfasilitasi bekerja di AWS CLI — ini adalah shell pra-otentikasi berbasis browser yang dapat Anda luncurkan langsung dari. Konsol Manajemen AWS Tidak perlu mengunduh atau menginstal alat baris perintah. Anda dapat menjalankan AWS

CLI perintah untuk AWS Control Tower dan AWS layanan lainnya dari shell pilihan Anda (Bash, PowerShell atau Z shell).

Saat Anda meluncurkan AWS CloudShell dari Konsol Manajemen AWS, AWS kredenSIAL yang Anda gunakan untuk masuk ke konsol tersedia di sesi shell baru. Anda dapat melewatkan memasukkan kredentif konfigurasi Anda saat berinteraksi dengan AWS Control Tower dan AWS layanan lainnya, dan Anda akan menggunakan AWS CLI versi 2, yang sudah diinstal sebelumnya di lingkungan komputasi shell.Anda telah diautentikasi sebelumnya dengan. AWS CloudShell

Dapatkan izin IAM untuk AWS CloudShell

AWS Identity and Access Management menyediakan sumber daya manajemen akses yang memungkinkan administrator memberikan izin kepada pengguna IAM dan pengguna Pusat Identitas IAM untuk akses ke. AWS CloudShell

Cara tercepat bagi administrator untuk memberikan akses kepada pengguna adalah melalui kebijakan terkel AWS ola. Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. Kebijakan terkel AWS ola berikut untuk CloudShell dapat dilampirkan ke identitas IAM:

- `AWSCloudShellFullAccess`: Memberikan izin untuk digunakan AWS CloudShell dengan akses penuh ke semua fitur.

Jika Anda ingin membatasi ruang lingkup tindakan yang dapat dilakukan pengguna IAM atau pengguna Pusat Identitas IAM AWS CloudShell, Anda dapat membuat kebijakan kustom yang menggunakan kebijakan terkel `AWSCloudShellFullAccess` ola sebagai templat. Untuk informasi selengkapnya tentang membatasi tindakan yang tersedia bagi pengguna CloudShell, lihat M engelola AWS CloudShell akses dan penggunaan dengan kebijakan IAM di Panduan AWS CloudShell Pengguna.

> **Note**
>
> Identitas IAM Anda juga memerlukan kebijakan yang memberikan izin untuk melakukan panggilan ke AWS Control Tower. Untuk informasi selengkapnya, lihat Izin yang diperlukan untuk menggunakan AWS Control Tower konsol.

Luncurkan AWS CloudShell

Dari Konsol Manajemen AWS, Anda dapat meluncurkan CloudShell dengan memilih opsi berikut yang tersedia di bilah navigasi:

- Pilih CloudShell ikon.
- Mulai ketik “cloudshell” di kotak Pencarian dan kemudian pilih CloudShell opsi.

Sekarang setelah Anda mulai CloudShell, Anda dapat memasukkan AWS CLI perintah apa pun yang Anda butuhkan untuk bekerja dengan AWS Control Tower. Misalnya, Anda dapat memeriksa AWS Config status Anda.

Berinteraksi dengan AWS Control Tower lewat AWS CloudShell

Setelah Anda meluncurkan AWS CloudShell dari Konsol Manajemen AWS, Anda dapat segera mulai berinteraksi dengan AWS Control Tower dari antarmuka baris perintah. AWS CLI perintah bekerja dengan cara standar di CloudShell.

> **Note**
>
> Saat menggunakan AWS CLI in AWS CloudShell, Anda tidak perlu mengunduh atau menginstal sumber daya tambahan apa pun. Anda sudah diautentikasi di dalam shell, jadi Anda tidak perlu mengonfigurasi kredenSIAL sebelum melakukan panggilan.

Gunakan AWS CloudShell untuk membantu mengatur AWS Control Tower

Sebelum melakukan prosedur ini, kecuali dinyatakan lain, Anda harus masuk ke Wilayah Konsol Manajemen AWS di rumah untuk zona pendaratan Anda, dan Anda harus masuk sebagai pengguna Pusat Identitas IAM atau pengguna IAM dengan izin administratif untuk akun manajemen yang berisi zona pendaratan Anda.

1. Berikut cara Anda dapat menggunakan perintah AWS Config CLI AWS CloudShell untuk menentukan status perekam konfigurasi dan saluran pengiriman sebelum Anda mulai mengonfigurasi zona AWS Control Tower pendaratan Anda.

   Contoh: Periksa AWS Config status Anda

Lihat perintah:

- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-recorders`
- Respon normal adalah sesuatu seperti `"name": "default"`

2. Jika Anda memiliki AWS Config perekam atau saluran pengiriman yang perlu Anda hapus sebelum mengatur zona AWS Control Tower pendaratan, berikut adalah beberapa perintah yang dapat Anda masukkan:

   Contoh: Kelola sumber daya yang sudah ada sebelumnya AWS Config

   Hapus perintah:

   - `aws configservice stop-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`
   - `aws configservice delete-delivery-channel --delivery-channel-name NAME-FROM-DESCRIBE-OUTPUT`
   - `aws configservice delete-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`

   > **Important**
   >
   > Jangan hapus AWS Control Tower sumber daya untuk AWS Config. Hilangnya sumber daya ini dapat AWS Control Tower menyebabkan memasuki keadaan yang tidak konsisten.

   Untuk informasi lebih lanjut, lihat AWS Config dokumentasi

   - Mengelola Perekam Konfigurasi (AWS CLI)
   - Mengelola Saluran Pengiriman

3. Contoh ini menunjukkan perintah AWS CLI yang akan Anda masukkan AWS CloudShell untuk mengaktifkan atau menonaktifkan akses te AWS Organizations percaya. Untuk AWS Control Tower Anda tidak perlu mengaktifkan atau menonaktifkan akses tepercaya untuk AWS

Organizations, itu hanya sebuah contoh. Namun, Anda mungkin perlu mengaktifkan atau menonaktifkan akses tepercaya untuk AWS layanan lain jika Anda mengotomatiskan atau menyesuaikan tindakan di. AWS Control Tower

Contoh: Mengaktifkan atau menonaktifkan akses layanan tepercaya

- `aws organizations enable-aws-service-access`
- `aws organizations disable-aws-service-access`

Contoh: Buat bucket Amazon S3 dengan AWS CloudShell

Dalam contoh berikut, Anda dapat menggunakan AWS CloudShell untuk membuat bucket Amazon S3 dan kemudian menggunakan PutObject metode untuk menambahkan file kode sebagai objek dalam bucket itu.

1. Untuk membuat bucket di Wil AWS ayah tertentu, masukkan perintah berikut di CloudShell baris perintah:

   ```
   aws s3api create-bucket --bucket insert-unique-bucket-name-here --region us-east-1
   ```

   Jika panggilan berhasil, baris perintah menampilkan respons dari layanan yang mirip dengan output berikut:

   ```
   {
       "Location": "/insert-unique-bucket-name-here"
   }
   ```

   > **Note**
   >
   > Jika Anda tidak mematuhi aturan untuk penamaan bucket (hanya menggunakan huruf kecil, misalnya), kesalahan berikut ditampilkan: Terjadi kesalahan (InvalidBucketName) saat memanggil CreateBucket operasi: Bucket yang ditentukan tidak valid.

2. Untuk mengunggah file dan menambahkannya sebagai objek ke bucket yang baru saja dibuat, panggil PutObject metode:

   ```
   aws s3api put-object --bucket insert-unique-bucket-name-here --key add_prog --body
    add_prog.py
   ```

Jika objek berhasil diunggah ke bucket Amazon S3, baris perintah menampilkan respons dari layanan yang mirip dengan output berikut:

```
{
            "ETag": "\"ab123c1:w:wad4a567d8bfd9a1234ebeea56\""}
```

Ini `ETag` adalah hash dari objek yang telah disimpan. Ini dapat digunakan untuk memeriksa integritas objek yang diunggah ke Amazon S3.

Buat AWS Control Tower sumber daya dengan AWS CloudFormation

AWS Control Tower terintegrasi dengan AWS CloudFormation, layanan yang membantu Anda memodelkan dan mengatur AWS sumber daya Anda sehingga Anda dapat menghabiskan lebih sedikit waktu untuk membuat dan mengelola sumber daya dan infrastruktur Anda. Anda membuat template yang menjelaskan semua AWS sumber daya yang Anda inginkan, seperti `AWS::ControlTower::EnabledControl` untuk kontrol. CloudFormation menyediakan dan mengkonfigurasi sumber daya tersebut untuk Anda.

Saat Anda menggunakan CloudFormation, Anda dapat menggunakan kembali template Anda untuk mengatur AWS Control Tower sumber daya Anda secara konsisten dan berulang kali. Jelaskan sumber daya Anda sekali, lalu sediakan sumber daya yang sama berulang-ulang di beberapa Akun AWS dan Wilayah.

AWS Control Tower and CloudFormation templat

Untuk menyediakan dan mengonfigurasi sumber daya untuk AWS Control Tower dan layanan terkait, Anda harus memahami CloudFormation template. Templat adalah file teks dengan format JSON atau YAML. Template ini menjelaskan sumber daya yang ingin Anda sediakan di tumpukan CloudFormation Anda. Jika Anda tidak terbiasa dengan JSON atau YAML, Anda dapat menggunakan AWS Infrastructure Composer untuk membantu Anda memulai dengan CloudFormation template. Untuk informasi selengkapnya, lihat Apa itu AWS Infrastructure Composer? dalam Panduan Pengguna Komposer Infrastruktur AWS.

AWS Control Tower mendukung pembuatan `AWS::ControlTower::EnabledControl` (sumber daya kontrol), `AWS::ControlTower::LandingZone` (zona pendaratan), dan

`AWS::ControlTower::EnabledBaseline` (garis dasar) di. CloudFormation Untuk informasi selengkapnya, termasuk contoh template JSON dan YAML untuk jenis sumber daya ini, lihat AWS Control Tower di Panduan AWS CloudFormation Pengguna.

> **Note**
>
> Batas `EnableControl` dan `DisableControl` pembaruan AWS Control Tower adalah 100 operasi bersamaan.

Untuk melihat beberapa AWS Control Tower contoh untuk CLI dan konsol, lihat Meng aktifkan kontrol dengan CloudFormation.

Pelajari lebih lanjut tentang CloudFormation

Untuk mempelajari selengkap CloudFormation nya, lihat sumber daya berikut:

- AWS CloudFormation
- AWS CloudFormation Panduan Pengguna
- Referensi CloudFormation API
- AWS CloudFormation Panduan Pengguna Antarmuka Baris Perintah

Menyesuaikan zona pendaratan AWS Control Tower

Aspek tertentu dari zona pendaratan AWS Control Tower dapat dikonfigurasi di konsol, seperti pemilihan Wilayah dan kontrol opsional. Perubahan lain dapat dilakukan di luar konsol, dengan otomatisasi.

Misalnya, Anda dapat membuat penyesuaian zona pendaratan yang lebih luas dengan kemampuan Ku stomisasi untuk AWS Control Tower, kerangka GitOps-style penyesuaian yang berfungsi dengan AWS CloudFormation template dan peristiwa siklus hidup AWS Control Tower.

Kustomisasi dari konsol AWS Control Tower

Untuk membuat penyesuaian ini ke zona pendaratan Anda, ikuti langkah-langkah yang diberikan oleh konsol AWS Control Tower.

Pilih nama yang disesuaikan selama penyiapan

- Anda dapat memilih nama OU tingkat atas Anda selama penyiapan. Anda dapat mengganti nama OU Anda kapan saja menggunakan AWS Organizations konsol, tetapi membuat perubahan pada OU Anda AWS Organizations dapat menyebabkan penyimpangan yang dapat diperbaiki.
- Anda dapat memilih nama akun Audit dan Arsip Log bersama, tetapi Anda tidak dapat mengubah nama setelah penyiapan. (Ini adalah pilihan satu kali.)

> **Kiat**
>
> Ingatlah bahwa mengganti nama OU AWS Organizations tidak memperbarui produk yang disediakan terkait di Account Factory. Untuk memperbarui produk yang disediakan secara otomatis (dan menghindari penyimpangan), Anda harus melakukan operasi OU melalui AWS Control Tower, termasuk membuat, menghapus, atau mendaftarkan ulang OU.

Pilih AWS Wilayah

- Anda dapat menyesuaikan zona pendaratan dengan memilih Wil AWS ayah tertentu untuk tata kelola. Ikuti langkah-langkah di konsol AWS Control Tower.
- Anda dapat memilih dan membatalkan pilihan Wil AWS ayah untuk tata kelola saat memperbarui zona pendaratan.

- Anda dapat mengatur kontrol Penolakan Wilayah ke Di aktifkan atau Tidak diaktifkan, dan mengontrol akses pengguna ke sebagian besar AWS layanan di Wilayah yang tidak diatur AWS .

Untuk informasi tentang Wilayah AWS di mana cFCT memiliki batasan penerapan, lihatBatasan kontrol.

Sesuaikan dengan menambahkan kontrol opsional

- Kontrol yang sangat disarankan dan elektif bersifat opsional, yang berarti Anda dapat menyesuaikan tingkat penegakan untuk zona pendaratan Anda dengan memilih mana yang akan diaktifkan. Kontrol opsional tidak diaktifkan secara default.
- Kontrol residensi Data opsional memungkinkan Anda menyesuaikan Wilayah tempat Anda menyimpan dan mengizinkan akses ke data Anda.
- Kontrol opsional yang merupakan bagian dari standar CSPM Security Hub terintegrasi memungkinkan Anda memindai lingkungan AWS Control Tower untuk memeriksa risiko keamanan.
- Kontrol proaktif opsional memungkinkan Anda memeriksa CloudFormation sumber daya sebelum disediakan, untuk memastikan sumber daya baru sesuai dengan tujuan kontrol lingkungan Anda.

Sesuaikan Anda AWS CloudTrail jalan setapak

- Saat memperbarui zona pendaratan ke versi 3.0 atau yang lebih baru, Anda dapat memilih untuk memilih atau memilih keluar dari CloudTrail jalur tingkat organisasi yang dikelola oleh AWS Control Tower. Anda dapat mengubah pilihan ini setiap kali memperbarui zona pendaratan Anda. AWS Control Tower membuat jejak tingkat organisasi di akun manajemen Anda, dan jejak tersebut memasuki status aktif atau tidak aktif, berdasarkan pilihan Anda. Zona pendaratan 3.0 tidak mendukung CloudTrail jalur tingkat akun; namun, jika Anda memerlukannya, Anda dapat mengonfigurasi dan mengelola jalur Anda sendiri. Anda mungkin dikenakan biaya tambahan untuk jalur duplikat.

Buat akun anggota yang disesuaikan di konsol

- Anda dapat membuat akun anggota AWS Control Tower yang disesuaikan, dan Anda dapat memperbarui akun anggota yang ada untuk menambahkan penyesuaian, dari konsol AWS Control Tower. Untuk informasi selengkapnya, lihat Sesuaikan akun dengan Kustomisasi Pabrik Akun (AFC).

Mengotomatiskan penyesuaian di luar konsol AWS Control Tower

Beberapa penyesuaian tidak tersedia melalui konsol AWS Control Tower, tetapi dapat diimplementasikan dengan cara lain. Contoh:

- Anda dapat menyesuaikan akun selama penyediaan, dalam GitOps-style alur kerja, dengan Ac count Factory for Terraform (AFT).

  AFT digunakan dengan modul Terraform, tersedia di repositori AFT.
- Anda dapat menyesuaikan zona pendaratan AWS Control Tower dengan Ku stomisasi untuk AWS Control Tower (cFCT), paket fungsionalitas yang dibangun berdasarkan AWS CloudFormation template dan kebijakan kontrol layanan (SCP). Anda dapat menerapkan templat dan kebijakan khusus ke akun individu dan unit organisasi (OU) dalam organisasi Anda.

  Kode sumber untuk CfCT tersedia di GitHub reposit ori.
- Anda dapat menyesuaikan zona pendaratan AWS Control Tower dengan Landing Zone Accelerator (LZA) aktif. AWS Solusi LZA dirancang agar selaras dengan praktik AWS terbaik dan sesuai dengan berbagai kerangka kerja kepatuhan global. Sebaiknya gunakan AWS Control Tower sebagai zona pendaratan dasar, dan kemudian meningkatkan kemampuan zona pendaratan dengan LZA, sesuai kebutuhan. Untuk informasi selengkapnya, lihat Menara Kontrol AWS dan akselerator zona pendaratan.

Menara Kontrol AWS dan akselerator zona pendaratan

Bagian ini menjelaskan manfaat bekerja dengan AWS Control Tower dan solusi L anding Zone Accelerator (LZA) bersama-sama.

Anda dapat menyesuaikan zona pendaratan AWS Control Tower dengan Landing Zone Accelerator (LZA) aktif. AWS

LZA adalah solusi yang menerapkan serangkaian kemampuan dasar yang dirancang agar selaras dengan praktik AWS terbaik, dan dengan beberapa kerangka kerja kepatuhan global, untuk membantu Anda mengelola dan mengatur lingkungan multi-akun. LZA dibangun menggunakan AWS Cloud Development Kit (CDK).

LZA secara otomatis menyiapkan lingkungan cloud yang cocok untuk hosting beban kerja yang aman. Solusi ini dapat diterapkan di semua Wilayah AWS, untuk membantu Anda menjaga

konsistensi operasi dan tata kelola. Solusi LZA dirancang agar selaras dengan praktik AWS terbaik, dan sesuai dengan berbagai kerangka kerja kepatuhan global.

Sebaiknya gunakan AWS Control Tower sebagai zona pendaratan dasar, dan kemudian meningkatkan kemampuan zona pendaratan Anda dengan LZA, sesuai kebutuhan. Kombinasi LZA dan AWS Control Tower menyediakan solusi komprehensif tanpa kode yang membantu Anda mengelola dan mengatur lingkungan multi-akun—solusi ini dibuat untuk mendukung beban kerja yang sangat diatur dan persyaratan kepatuhan yang kompleks. Bersama-sama, AWS Control Tower dan Landing Zone Accelerator membantu Anda menetapkan kesiapan platform, termasuk keamanan, kepatuhan, dan kemampuan operasional.

Kode sumber untuk LZA tersedia di GitHub reposit ori.

Untuk informasi selengkapnya tentang cara menggabungkan LZA dan AWS Control Tower, lihat panduan implement asi LZA.

Manfaat Kustomisasi untuk AWS Control Tower (cFCT)

Paket fungsionalitas yang kami sebut sebagai Ku stomisasi untuk Menara Kontrol AWS (CfCT) membantu Anda membuat penyesuaian yang lebih luas untuk zona pendaratan daripada yang dapat Anda buat di konsol AWS Control Tower. Ini menawarkan GitOps-style proses otomatis. Anda dapat membentuk kembali zona pendaratan Anda untuk memenuhi kebutuhan bisnis Anda.

Proses penyesuaian infrastruktur sebagai kode ini mengintegrasikan AWS CloudFormation template dengan kebijakan kontrol AWS layanan (SCP), kebijakan kontrol sumber daya (RCP), dan peristiwa siklus hidup AWS Control Tower, sehingga penerapan sumber daya Anda tetap disinkronkan dengan zona pendaratan Anda. Misalnya, saat Anda membuat akun baru dengan Account Factory, sumber daya yang dilampirkan ke akun dan OU dapat digunakan secara otomatis.

> **Note**
>
> Tidak seperti Account Factory dan AFT, CfCT tidak secara khusus dimaksudkan untuk membuat akun baru, tetapi untuk menyesuaikan akun dan OU di zona pendaratan Anda dengan menyebarkan sumber daya yang Anda tentukan.

> **Note**
>
> Unit organisasi target (OU) yang dikonfigurasi di CfCT harus AWSControlTowerBaseline diaktifkan di AWS Control Tower. Untuk detailnya AWSControlTowerBaseline, lihat:Jenis dasar yang berlaku di tingkat OU.

Manfaat

- Perluas lingkungan yang disesuaikan dan aman — Anda dapat memperluas AWS lingkungan AWS Control Tower multi-akun Anda dengan lebih cepat, dan menggabungkan praktik AWS terbaik ke dalam alur kerja penyesuaian yang dapat diulang.
- Buat contoh kebutuhan Anda — Anda dapat menyesuaikan zona pendaratan AWS Control Tower untuk kebutuhan bisnis Anda, dengan AWS CloudFormation templat dan kebijakan kontrol layanan yang mengekspresikan niat kebijakan Anda.
- Otomatisasi lebih lanjut dengan peristiwa siklus hidup AWS Control Tower — Peristiwa siklus hidup memungkinkan Anda menerapkan sumber daya berdasarkan penyelesaian rangkaian acara sebelumnya. Anda dapat mengandalkan peristiwa siklus hidup untuk membantu Anda menyebarkan sumber daya ke akun dan OU, secara otomatis.
- Perluas arsitektur jaringan Anda — Anda dapat menerapkan arsitektur jaringan khusus yang meningkatkan dan melindungi konektivitas Anda, seperti gateway transit.

Contoh CfCT tambahan

- Contoh kasus penggunaan jaringan dengan Ku stomisasi untuk Menara Kontrol AWS (CfCT) diberikan di posting blog AWS Arsitektur, Menye barkan DNS yang konsisten dengan Katalog Layanan dan penyesuaian AWS Control Tower.
- Contoh spesifik yang terkait dengan CfCT dan Amazon GuardDuty tersedia GitHub di `aws-samples` repositori.
- Contoh kode tambahan mengenai CfCT tersedia sebagai bagian dari Arsitektur Referensi AWS Keamanan, di `aws-samples` repositori. Banyak dari contoh ini berisi `manifest.yaml` file sampel dalam direktori bernama`customizations_for_aws_control_tower`.

Untuk informasi selengkapnya tentang Ar AWS sitektur Referensi Keamanan, lihat halaman Panduan AWS Preskriptif.

Kustomisasi untuk ikhtisar AWS Control Tower (CFCT)

Kustomisasi untuk AWS Control Tower (CFCT) membantu Anda menyesuaikan landing zone AWS Control Tower dan tetap selaras dengan praktik terbaik. AWS Kustomisasi diimplementasikan dengan AWS CloudFormation template, kebijakan kontrol layanan (SCP), dan kebijakan kontrol sumber daya (RCP).

Kemampuan CFCT ini terintegrasi dengan peristiwa siklus hidup AWS Control Tower, sehingga penerapan sumber daya Anda tetap disinkronkan dengan landing zone Anda. Misalnya, ketika akun baru dibuat melalui pabrik akun, semua sumber daya yang dilampirkan ke akun dikerahkan secara otomatis. Anda dapat menerapkan templat dan kebijakan khusus ke akun individual dan unit organisasi (OU) dalam organisasi Anda.

> **Note**
>
> Unit organisasi target (OU) yang dikonfigurasi dalam CFCT harus AWSControlTowerBaseline diaktifkan di AWS Control Tower. Untuk detailnya AWSControlTowerBaseline, lihat:Jenis dasar yang berlaku di tingkat OU.

Video berikut menjelaskan praktik terbaik untuk menerapkan pipeline CFCT yang dapat diskalakan dan penyesuaian CFCT umum.

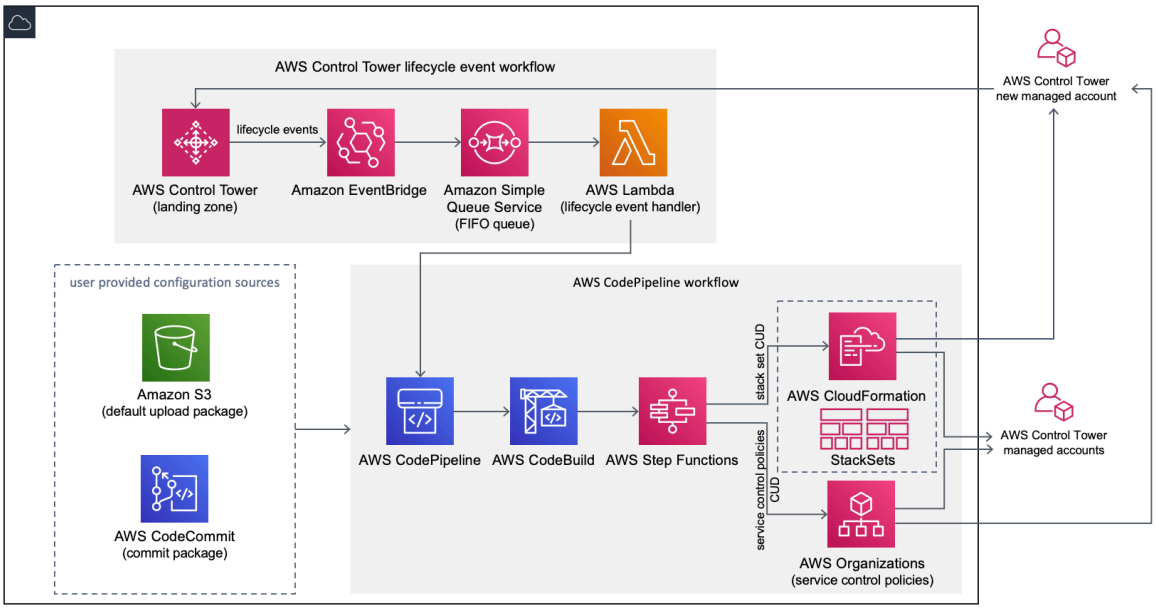
Bagian berikut memberikan pertimbangan arsitektur dan langkah-langkah konfigurasi untuk menerapkan Kustomisasi untuk AWS Control Tower (CFCT). Ini mencakup tautan ke AWS CloudFormationtemplate yang meluncurkan, mengonfigurasi, dan menjalankan AWS layanan yang diperlukan, selaras dengan praktik AWS terbaik untuk keamanan dan ketersediaan.

Topik ini ditujukan untuk arsitek dan pengembang infrastruktur TI yang memiliki pengalaman praktis dalam arsitektur di AWS Cloud.

Untuk informasi tentang pembaruan terbaru dan perubahan pada Kustomisasi untuk AWS Control Tower (CFCT), lihat CHANGELOG.md file di repositori. GitHub

Gambaran umum arsitektur

Menerapkan CFCT membangun lingkungan berikut di AWS Cloud, dengan bucket Amazon S3 sebagai sumber konfigurasi.



Gambar 1: Kustomisasi untuk arsitektur AWS Control Tower

CFCT menyertakan AWS CloudFormation template yang Anda terapkan di akun manajemen AWS Control Tower Anda. Template meluncurkan semua komponen yang diperlukan untuk membangun alur kerja, sehingga Anda dapat menyesuaikan landing zone AWS Control Tower Anda.

> **Catatan**
>
> CFCT harus diterapkan di Wilayah home AWS Control Tower dan di akun manajemen AWS Control Tower, karena di situlah zona landing zone AWS Control Tower Anda digunakan. Untuk informasi tentang menyiapkan zona landing zone AWS Control Tower, lihatMemulai.

Saat Anda menerapkan CFCT, ia mengemas dan mengunggah sumber daya khusus ke sumber pipeline kode, melalui Amazon Simple Storage Service (Amazon S3). Proses upload secara otomatis memanggil mesin status kebijakan kontrol layanan (SCP), mesin status kebijakan kontrol sumber daya (RCP), dan mesin status untuk menerapkan SCP dan RCP di tingkat OU, atau untuk menerapkan instance tumpukan di tingkat OU atau akun. AWS CloudFormation StackSets

> **Catatan**
>
> Secara default, CfCT membuat bucket Amazon S3 untuk menyimpan sumber pipeline. Jika Anda memiliki AWS CodeCommit repositori yang ada, Anda dapat mengubah lokasi ke

repositori. CodeCommit Untuk informasi selengkapnya, lihat Mengatur Amazon S3 sebagai sumber konfigurasi.

CFCT menyebarkan dua alur kerja:

- AWS CodePipelinealur kerja
- dan alur kerja peristiwa siklus hidup AWS Control Tower.

AWS CodePipeline Alur kerja

AWS CodePipeline Alur kerja mengonfigurasi AWS CodePipeline, AWS CodeBuildmemproyeksikan, dan AWS Step Functionsmengatur pengelolaan, SCP AWS CloudFormation StackSets, dan RCP di organisasi Anda.

Saat Anda mengunggah paket konfigurasi, CFCT memanggil pipeline kode untuk menjalankan empat tahap.

- Build Stage — memvalidasi konten paket konfigurasi menggunakan AWS CodeBuild.
- SCP Stage — memanggil mesin status kebijakan kontrol layanan, yang memanggil AWS Organizations API untuk membuat SCP.
- Tahap RCP — memanggil mesin status kebijakan kontrol sumber daya, yang memanggil AWS Organizations API untuk membuat RCP.
- CloudFormation Tahap - memanggil mesin status set tumpukan untuk menyebarkan sumber daya yang ditentukan dalam daftar akun atau OU, yang telah Anda berikan dalam file manifes.

Pada setiap tahap, pipeline kode memanggil fungsi stack set, SCP, dan RCP step, yang menyebarkan set tumpukan khusus, SCP, dan RCP ke akun individual yang ditargetkan, atau ke seluruh unit organisasi.

> **Catatan**
>
> Untuk informasi rinci tentang menyesuaikan paket konfigurasi, lihat. Panduan kustomisasi CfCT

Alur kerja peristiwa siklus hidup AWS Control Tower

Saat akun baru dibuat di AWS Control Tower, peristiwa siklus hidup dapat memanggil alur kerja. AWS CodePipeline Anda dapat menyesuaikan paket konfigurasi melalui alur kerja ini, yang terdiri dari aturan EventBridge peristiwa Amazon, antrian Amazon Simple Queue Service (Amazon SQS) first-in first-out (FIFO), dan fungsi. AWS Lambda

Saat aturan EventBridge peristiwa Amazon mendeteksi peristiwa siklus hidup yang cocok, aturan tersebut meneruskan peristiwa tersebut ke antrean Amazon SQS FIFO, memanggil AWS Lambda fungsi, dan memanggil pipeline kode untuk melakukan penerapan hilir kumpulan tumpukan, SCP, dan RCP.

Biaya

Biaya untuk menjalankan CFCT tergantung pada jumlah AWS CodePipeline proses, durasi AWS CodeBuild berjalan, jumlah dan durasi AWS Lambda fungsi, dan jumlah EventBridge acara Amazon yang diterbitkan. Misalnya, jika Anda menjalankan 100 build dalam satu bulan menggunakan build.general1.small di mana setiap build berjalan selama lima menit, maka perkiraan biaya untuk menjalankan CFCT adalah $3,00 per bulan. Untuk detail selengkapnya, Anda dapat meninjau halaman web harga untuk setiap AWS layanan yang Anda jalankan.

Bucket AWS CodeCommit Git-based dan sumber daya repositori Amazon Simple Storage Service (Amazon S3) disimpan setelah Anda menghapus template, untuk melindungi informasi konfigurasi Anda. Bergantung pada opsi yang Anda pilih, Anda dikenakan biaya berdasarkan jumlah data yang disimpan di bucket Amazon S3 dan jumlah permintaan Git (tidak berlaku untuk sumber daya Amazon S3). Lihat Amazon S3 dan AWS CodeCommitharga untuk detailnya.

Layanan komponen

AWS Layanan berikut adalah komponen Ku stomisasi untuk AWS Control Tower (CfCT).

AWS CodeCommit

Jika Anda memiliki AWS CodeCommit repositori yang ada, Anda dapat mengonfigurasinya sebagai sumber untuk pipeline Anda, sebagai alternatif untuk Amazon S3.

Berdasarkan masukan Anda ke CloudFormation template, cFCT dapat membuat AWS CodeCommit repositori dengan konfigurasi sampel yang sama seperti yang dijelaskan di bagian Amazon Simple Storage Service.

Untuk mengkloning AWS CodeCommit repositori cFCT ke komputer lokal Anda, Anda harus membuat kredenSIAL yang memberi Anda akses sementara ke repositori, seperti yang dijelaskan

dalam Panduan AWS CodeCommit Pengguna. Untuk informasi tentang kompatibilitas versi, lihat Menyiapkan untuk AWS CodeCommit.

> **Note**
>
> Jika Anda belum menggunakannya CodeCommit, satu-satunya pilihan Anda adalah mengatur bucket Amazon S3 sebagai lokasi penyimpanan untuk paket konfigurasi Anda. CodeCommit tidak tersedia jika Anda menerapkan CfCT untuk pertama kalinya.

AWS CodePipeline

AWS CodePipeline memvalidasi, menguji, dan mengimplementasikan perubahan berdasarkan pembaruan paket konfigurasi, yang akan Anda buat baik di bucket Amazon S3 default atau AWS CodeCommit repositori. Untuk informasi selengkapnya tentang kontrol sumber konfigurasi, lihat Menggunakan Amazon S3 sebagai Sumber Konfigurasi. Pipeline mencakup tahapan untuk memvalidasi dan mengelola file konfigurasi dan templat, akun inti, kebijakan kontrol AWS Organizations layanan, dan AWS CloudFormation StackSets. Untuk informasi lebih lanjut tentang tahapan pipa, lihat Panduan kustomisasi CfCT

AWS Key Management Service

CfCT membuat kunci `CustomControlTowerKMSKey` enkripsi AWS Key Management Service (AWS KMS). Kunci ini digunakan untuk mengenkripsi objek di bucket konfigurasi Amazon S3, antrian Amazon SQS, dan parameter sensitif di Penyimpanan Parameter Manajer AWS Sistem. Secara default, hanya peran yang disediakan oleh CfCT yang memiliki izin untuk melakukan operasi enkripsi atau dekripsi dengan kunci ini. Untuk akses ke file konfigurasi, antrian FIFO, atau `SecureString` nilai Penyimpanan Parameter, administrator harus ditambahkan ke `CustomControlTowerKMSKey` kebijakan. Rotasi tombol otomatis diaktifkan secara default.

AWS Lambda

CfCT menggunakan AWS Lambda fungsi untuk memanggil komponen instalasi selama instalasi awal dan penyebaran AWS CloudFormation StackSets AWS Organizations SCP selama peristiwa siklus hidup AWS Control Tower.

Layanan Notifikasi Sederhana Amazon

CfCT dapat menerbitkan pemberitahuan, seperti persetujuan pipeline untuk topik Amazon Simple Notification Service (Amazon SNS) selama alur kerja. Amazon SNS diluncurkan hanya jika Anda memilih untuk menerima pemberitahuan persetujuan pipeline.

Amazon Simple Storage Service

Saat Anda menerapkan cFCT, cFct membuat bucket Amazon Simple Storage Service (Amazon S3) dengan nama unik:

Contoh: Nama bucket Amazon S3

`custom-control-tower-configuration-`*`accountID`*`-`*`region`*

Bucket berisi file konfigurasi sampel yang disebut `_custom-control-tower-configuration.zip`

Perhatikan garis bawah terdepan dalam nama file.

File zip ini menyediakan manifes sampel dan template sampel terkait yang menjelaskan struktur folder yang diperlukan. Contoh-contoh ini membantu Anda mengembangkan paket konfigurasi untuk menyesuaikan zona pendaratan AWS Control Tower Anda. Manifes sampel mengidentifikasi konfigurasi yang diperlukan untuk kumpulan tumpukan dan kebijakan kontrol layanan (SCP) yang Anda perlukan, saat Anda menerapkan penyesuaian.

Anda dapat menggunakan paket konfigurasi sampel ini sebagai model, untuk mengembangkan dan mengunggah paket kustom Anda, yang memicu pipeline konfigurasi cFCT secara otomatis.

Untuk informasi tentang menyesuaikan file konfigurasi, lihatPanduan kustomisasi CfCT.

Amazon Simple Queue Service

CfCT menggunakan antrian FIFO Amazon Simple Queue Service (Amazon SQS) untuk menangkap peristiwa siklus hidup dari Amazon. EventBridge Ini memicu AWS Lambda fungsi, yang memanggil AWS CodePipeline untuk menyebarkan AWS CloudFormation StackSets atau SCP. Untuk informasi lebih lanjut tentang SCP, lihat AWS Organizations.

AWS Step Functions

CfCT membuat Fungsi Langkah untuk mengatur penerapan kustomisasi. Fungsi Langkah ini menerjemahkan file konfigurasi untuk menerapkan penyesuaian sesuai kebutuhan di seluruh lingkungan.

AWS Penyimpanan Parameter Systems Manager

AWS Systems Manager Parameter Store menyimpan parameter konfigurasi cFCT. Parameter ini memungkinkan Anda untuk mengintegrasikan template konfigurasi terkait. Misalnya, Anda dapat mengonfigurasi setiap akun untuk mencatat AWS CloudTrail data ke bucket Amazon S3 terpusat. Selain itu, System Manager Parameter Store menyediakan lokasi terpusat di mana administrator dapat melihat input dan parameter cFCT.

Pertimbangan deployment

Pastikan untuk meluncurkan Kustomisasi untuk AWS Control Tower (CFCT) di akun dan Wilayah yang sama tempat landing zone AWS Control Tower Anda digunakan; artinya, Anda harus menerapkannya di akun manajemen AWS Control Tower di Wilayah AWS Control Tower home Anda. Secara default, CFCT membuat dan menjalankan paket konfigurasi landing zone dengan menyiapkan pipeline konfigurasi di akun dan Region tersebut.

Bersiaplah untuk penyebaran

Anda memiliki beberapa opsi saat menyiapkan CloudFormation template untuk penerapan awal. Anda dapat memilih sumber konfigurasi, dan Anda dapat mengizinkan persetujuan manual penerapan pipeline. Dua bagian berikutnya menjelaskan lebih lanjut tentang opsi ini.

Pilih sumber konfigurasi Anda

Secara default, template membuat bucket Amazon Simple Storage Service (Amazon S3) Simple Storage S3) untuk menyimpan paket konfigurasi sampel sebagai `.zip` file yang dipanggil. `_custom-control-tower-configuration.zip` Bucket Amazon S3 dikontrol versi, dan Anda dapat memperbarui paket konfigurasi sesuai kebutuhan. Untuk informasi tentang memperbarui paket konfigurasi, lihat Menggunakan Amazon S3 sebagai Sumber Konfigurasi.

> **Ingatlah untuk menghapus garis bawah**
>
> Nama file paket konfigurasi sampel dimulai dengan garis bawah (_) sehingga tidak dimulai secara AWS CodePipeline otomatis. Setelah Anda selesai menyesuaikan paket konfigurasi, pastikan untuk mengunggah `custom-control-tower-configuration.zip` tanpa garis bawah (_) untuk memulai penerapan di. AWS CodePipeline

Jika Anda memiliki repositori AWS CodeCommit Git yang sudah ada, Anda dapat mengubah lokasi penyimpanan paket konfigurasi dari bucket Amazon S3 ke repositori Git. AWS CodeCommit Untuk melakukannya, pilih `CodeCommit` opsi di CloudFormation parameter.

> **Untuk zip, atau tidak ke zip?**
>
> Saat Anda menggunakan bucket S3 default, pastikan paket konfigurasi tersedia sebagai `.zip` file. Jika Anda menggunakan AWS CodeCommit repositori, pastikan untuk menempatkan paket konfigurasi di repositori tanpa zip file. Untuk informasi tentang membuat dan menyimpan paket konfigurasi AWS CodeCommit, lihatPanduan kustomisasi CfCT.

Anda dapat menggunakan paket konfigurasi sampel untuk membuat sumber konfigurasi kustom Anda sendiri. Saat Anda siap untuk menerapkan konfigurasi kustom Anda, unggah paket konfigurasi secara manual, baik ke bucket Amazon S3 atau ke repositori. AWS CodeCommit Pipeline dimulai secara otomatis saat Anda mengunggah file konfigurasi.

Pilih parameter persetujuan konfigurasi pipeline

AWS CloudFormation Template menyediakan opsi untuk menyetujui penerapan perubahan konfigurasi secara manual. Secara default, persetujuan manual tidak diaktifkan. Untuk informasi lebih lanjut, lihat Langkah 1. Luncurkan tumpukan.

Saat persetujuan manual diaktifkan, pipeline konfigurasi memvalidasi penyesuaian yang dibuat pada manifes dan templat file AWS Control Tower, lalu menghentikan proses hingga persetujuan manual diberikan. Setelah disetujui, penerapan dilanjutkan untuk menjalankan tahapan pipeline yang tersisa, sesuai kebutuhan, untuk mengimplementasikan fungsionalitas Kustomisasi untuk AWS Control Tower (CFCT).

Anda dapat menggunakan parameter persetujuan manual agar penyesuaian konfigurasi AWS Control Tower tidak berjalan, dengan menolak upaya pertama untuk dijalankan melalui pipeline.

Parameter ini juga memungkinkan Anda untuk memvalidasi penyesuaian untuk perubahan konfigurasi AWS Control Tower secara manual, sebagai kontrol akhir sebelum implementasi.

Untuk memperbarui Kustomisasi untuk AWS Control Tower

Jika sebelumnya Anda telah menerapkan CFCT, Anda harus memperbarui CloudFormation tumpukan untuk mendapatkan versi terbaru dari kerangka kerja CFCT. Untuk detailnya, lihat Perbarui Tumpukan.

Template dan kode sumber

Kustomisasi untuk AWS Control Tower (CFCT) diterapkan di akun manajemen Anda setelah Anda meluncurkan template. AWS CloudFormation Anda dapat mengunduh template dari GitHub dan kemudian meluncurkannya dari AWS CloudFormation.

customizations-for-aws-control-tower.template menerapkan yang berikut ini:

- Sebuah AWS CodeBuild proyek
- Sebuah AWS CodePipeline proyek
- EventBridge Aturan Amazon
- AWS Lambda fungsi
- Antrean Amazon Simple Queue Service
- Bucket Amazon Simple Storage Service dengan paket konfigurasi sampel
- AWS Step Functions

> **Note**
>
> Anda dapat menyesuaikan template berdasarkan kebutuhan spesifik Anda.

Repositori kode sumber

Anda dapat mengunjungi GitHubrepositori kami untuk mengunduh template dan skrip untuk CFCT, dan untuk berbagi kustomisasi landing zone Anda dengan orang lain.

Otomatisasi deployment

Sebelum Anda meluncurkan penerapan otomatis, tinjau pertimbangannya. Ikuti step-by-step petunjuk di bagian ini untuk mengonfigurasi dan menerapkan solusi ke akun manajemen AWS Control Tower Anda.

Waktu untuk menyebarkan: Sekitar 15 menit

Prasyarat

CFCT harus diterapkan di akun manajemen AWS Control Tower Anda, dan di Wilayah AWS Control Tower home Anda. Jika Anda tidak memiliki landing zone yang diatur, lihatMemulai.

Langkah-langkah penyebaran

Prosedur untuk menerapkan CFCT terdiri dari dua langkah utama. Untuk petunjuk terperinci, ikuti tautan untuk setiap langkah.

Langkah 1. Luncurkan tumpukan

- Luncurkan CloudFormation template ke akun manajemen Anda.
- Tinjau parameter template, dan sesuaikan jika perlu.

Langkah 2. Buat paket kustom

- Buat paket konfigurasi kustom.

> **Important**
>
> Untuk mengunduh AWS CloudFormation templat yang benar dan meluncurkan CFCT, ikuti GitHub tautan yang diberikan di bagian ini. Jangan ikuti tautan lama ke bucket S3 yang ditentukan sebelumnya.

Langkah 1. Luncurkan tumpukan

CloudFormation Template di bagian ini menerapkan Kustomisasi untuk AWS Control Tower (CFCT) di akun Anda.

> **Catatan**
>
> Anda bertanggung jawab atas biaya AWS layanan yang digunakan saat Anda menjalankan CFCT. Untuk detail selengkapnya, lihat Biaya.

1. Untuk meluncurkan Kustomisasi AWS Control Tower, unduh templat dari GitHub lalu luncurkan. AWS CloudFormation
2. Template diluncurkan di Wilayah AS Timur (Virginia N.) secara default. Untuk meluncurkan CFCT di AWS Wilayah lain, gunakan pemilih Wilayah di bilah navigasi konsol.

   > **Note**
   >
   > CFCT harus diluncurkan di Wilayah dan akun yang sama tempat Anda menerapkan landing zone AWS Control Tower, yang merupakan Wilayah asal Anda.

3. Pada halaman Buat tumpukan, verifikasi bahwa URL templat yang benar ditampilkan di kotak teks URL dan pilih Berikutnya.
4. Pada halaman Tentukan detail tumpukan, tetapkan nama ke tumpukan CFCT Anda.
5. Di bawah Parameter, tinjau parameter berikut dan modifikasi dalam templat, jika perlu.

Konfigurasi Pipa		
Parameter	Default	Deskripsi
Tahap Persetujuan Pipa	No	Pilih apakah akan mengubah konfigurasi pipeline dari tahap persetujuan otomatis default ke tahap persetujuan manual. Untuk informasi selengkapnya, lihat the section called “Panduan kustomisasi CfCT”.
Alamat Email Persetujuan Pipa	<Optional Input>	Alamat email untuk pemberitahuan persetujuan. Untuk menggunakan

Konfigurasi Pipa		
Parameter	Default	Deskripsi
		parameter ini, Anda harus mengatur parameter Pipeline Approval Stage ke`Yes`.
CodePipelineSumber AWS	`Amazon S3`	Sumber AWS CodePipeline untuk membantu Anda memilih tempat menyimpan dan mengonfigurasi penyesuaian CFCT.
CodeCommit Pengaturan AWS		
Parameter	Default	Deskripsi
CodeCommitRepositori yang Ada?	`No`	Pilih apakah akan menggunakan repositori CodeCommit Git yang ada. Jika Anda memilih`Yes`, Anda harus mengatur parameter CodePipeline Sumber ke`AWS CodeCommit` .
CodeCommit Nama Repositori	`custom-control-tower-configuration`	Jika Anda memberikan nama repositori Git yang ada, Anda harus mengatur Repositori yang Ada? CodeCommit parameter ke `Yes` dan masukkan nama yang tepat dari repositori itu.

CodeCommit Pengaturan AWS		
Parameter	Default	Deskripsi
CodeCommit Nama Cabang	`main`	Cabang Git tempat paket kustomisasi disimpan. Untuk menggunakan parameter ini, Anda harus mengatur parameter CodePipeline Sumber ke`AWS CodeCommit` .
CloudFormation StackSets Konfigurasi		
Parameter	Default	Deskripsi
Jenis Konkurensi Wilayah	`PARALLEL`	Pilih jenis StackSets operasi penyebaran konkurensi di Wilayah. Pengaturan ini berlaku untuk membuat, memperbarui, dan menghapus alur kerja. Nilai lain yang diizinkan adalah`SEQUENTIAL` .
Persentase Konkuren Maks	`100`	Persentase maksimum akun untuk melakukan operasi ini pada satu waktu. Nilai maksimum yang diizinkan adalah 100. Untuk informasi selengkapnya, lihat opsi operasi Stack Set.

CloudFormation StackSets Konfigurasi		
Parameter	Default	Deskripsi
Persentase Toleransi Kegagalan	`10`	Persentase akun, per Wilayah, yang operasi tumpukan ini dapat gagal sebelum AWS CloudFormation menghentikan operasi di Wilayah tersebut. Nilai minimum yang diizinkan adalah 0 dan nilai maksimum yang diizinkan adalah 100. Untuk informasi selengkapnya, lihat opsi operasi Stack Set.

6. Pilih Berikutnya.
7. Pada halaman Konfigurasikan opsi tumpukan, pilih Berikutnya.
8. Pada halaman Ulasan, tinjau dan konfirmasikan pengaturan. Pastikan untuk mencentang kotak yang mengakui bahwa template akan membuat sumber daya AWS Identity and Access Management (IAM).
9. Pilih Membuat tumpukan untuk menerapkannya.

   Anda dapat melihat status tumpukan di CloudFormation konsol di kolom Status. Anda akan melihat status CREATE_COMPLETE dalam waktu sekitar 15 menit.

Langkah 2. Buat paket kustom

Dengan tumpukan yang diluncurkan, Anda dapat menambahkan penyesuaian ke zona landing zone AWS Control Tower dan kebijakan kontrol layanan (SCPs) dengan menyesuaikan paket konfigurasi yang disertakan. Untuk petunjuk rinci tentang membuat paket kustom, lihatPanduan kustomisasi CfCT.

> **Catatan**
>
> Pipeline tidak berjalan tanpa mengunggah paket konfigurasi khusus.

Perbarui tumpukan

Jika sebelumnya Anda menerapkan Kustomisasi untuk AWS Control Tower (CFCT), ikuti prosedur untuk memperbarui AWS CloudFormation tumpukan untuk versi terbaru kerangka kerja CFCT.

> **Important**
>
> Sebelum Anda dapat menyelesaikan prosedur berikut, Anda harus mengunggah template terbaru dari GitHub ke bucket Amazon Simple Storage Service (Amazon S3). Untuk petunjuk tentang cara memulai Amazon S3, lihat Memulai Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

1. Masuk ke konsol AWS CloudFormation tersebut.
2. Pilih Penyesuaian yang ada untuk CloudFormation tumpukan AWS Control Tower (CFCT), lalu pilih Perbarui.
3. Di bawah Prasyarat - Siapkan templat, pilih Ganti templat saat ini.
4. Di bawah Tentukan template, lakukan hal berikut:
   a. Untuk sumber Template, pilih Ganti template saat ini.
   b. Untuk URL Amazon S3, masukkan URL templat untuk templat yang sebelumnya Anda unggah ke Amazon GitHub S3, lalu pilih Berikutnya.
   c. Verifikasi bahwa URL template sudah benar. Kemudian pilih Next dan Next lagi.
5. Di bawah Parameter, tinjau parameter untuk templat dan modifikasi sesuai kebutuhan. Lihat Langkah 1. Luncurkan tumpukan untuk detail tentang parameter.
6. Pilih Berikutnya.
7. Pada halaman Konfigurasikan opsi tumpukan, pilih Berikutnya.
8. Pada halaman Ulasan, tinjau dan konfirmasikan pengaturan. Pastikan untuk mencentang kotak yang mengakui bahwa template mungkin membuat sumber daya AWS Identity and Access Management (IAM).
9. Pilih Lihat set perubahan dan verifikasi perubahan.
10. Pilih Perbarui tumpukan untuk menyebarkan tumpukan.

    Anda dapat melihat status tumpukan di AWS CloudFormation konsol di kolom Status. Anda akan melihat status UPDATE_COMPLETE dalam waktu sekitar 15 menit.

Hapus set tumpukan

Anda dapat menghapus kumpulan tumpukan jika Anda telah mengaktifkan penghapusan kumpulan tumpukan dalam file manifes. Secara default, parameter `enable_stack_set_deletion` diatur ke `false`. Dalam konfigurasi ini, tidak ada tindakan yang diambil untuk menghapus kumpulan tumpukan terkait saat sumber daya dihapus dari file manifes CFCT.

Jika Anda mengubah nilai `enable_stack_set_deletion` ke `true` dalam file manifes, CFCT menghapus kumpulan tumpukan dan semua sumber dayanya saat Anda menghapus sumber daya terkait dari file manifes.

Kemampuan ini didukung di v2 dari file manifes.

> **Important**
>
> Saat Anda awalnya menetapkan nilai `enable_stack_set_deletion` to`true`, saat berikutnya Anda memanggil CFCT, SEMUA sumber daya yang dimulai dengan awalan, yang memiliki tag kunci terkait`CustomControlTower-`, dan yang tidak dideklarasikan dalam file manifes`Key:AWS_Solutions, Value: CustomControlTowerStackSet`, akan dipentaskan untuk dihapus.

Berikut adalah contoh cara mengatur parameter ini dalam `manifest.yaml` file:

```
version: 2021-03-15
region: us-east-1
enable_stack_set_deletion: true   #New opt-in functionality


resources:
  - name: demo_resource_1
    resource_file: s3://demo_bucket/resource.template
    deployment_targets:
      accounts:
        - 012345678912
    deploy_method: stack_set
    ...
    regions:
    - us-east-1
    - us-west-2
```

```
  - name: demo_resource_2
    resource_file: s3://demo_bucket/resource.template
    deployment_targets:
      accounts:
        - 012345678912
    deploy_method: stack_set
    ...
    regions:
    - us-east-1
    - eu-north-1
```

Siapkan Amazon S3 sebagai sumber konfigurasi

Saat Anda menyiapkan Kustomisasi untuk AWS Control Tower, ia menyimpan file konfigurasi awal, yang disebut `_custom-control-tower-configuration.zip` file dalam bucket Amazon Simple Storage Service (Amazon S3), dinamai. `custom-control-tower-configuration-`*`account-ID`*`-`*`region`*

> **Catatan**
>
> Jika Anda memilih untuk mengunduh dan memodifikasi file ini, ingatlah untuk zip perubahan, simpan sebagai file baru bernama`custom-control-tower-configuration.zip`, lalu unggah kembali ke bucket Amazon S3 yang sama.
> Bucket Amazon S3 adalah sumber default dari pipeline. Saat pengaturan default sudah ada, mengunggah file zip konfigurasi tanpa awalan garis bawah dalam nama file ke bucket S3 akan memulai pipeline secara otomatis.

File zip dilindungi oleh Server-Side Encryption (SSE) dengan AWS Key Management Service (AWS KMS), dan penolakan penggunaan kunci KMS. Untuk akses ke file zip, Anda harus memperbarui Kebijakan Kunci KMS untuk menentukan peran yang harus diberikan akses. Peran tersebut dapat berupa peran administrator, pengguna, atau keduanya. Ikuti prosedur ini:

1. Navigasikan ke konsol AWS Key Management Service tersebut.
2. Di Customer Managed Keys, pilih CustomControlTowerKMSKey.
3. Pilih tab Kebijakan kunci. Kemudian, pilih Edit.

4. Di halaman kebijakan kunci Edit, temukan bagian Izinkan Penggunaan kunci dalam kode, dan tambahkan salah satu izin berikut:
   - Untuk menambahkan peran administrasi:

     `arn:aws:iam::<account-ID>:role/<administrator-role>`
   - Untuk menambahkan pengguna::

     `arn:aws:iam::<account-ID>:user/<username>`
5. Pilih Simpan Perubahan.
6. Arahkan ke konsol Amazon S3, temukan bucket S3 yang berisi file zip konfigurasi, dan pilih unduh.
7. Buat perubahan konfigurasi yang diperlukan pada file manifes dan file template. Untuk informasi tentang menyesuaikan file manifes dan template, lihatthe section called “Panduan kustomisasi CfCT”.
8. Unggah perubahan Anda:
   a. Zip file konfigurasi yang dimodifikasi, dan beri nama file:`custom-control-tower-configuration.zip`.
   b. Unggah file ke Amazon S3 menggunakan SSE dengan master-key:. AWS KMS `CustomControlTowerKMSKey`

Siapkan GitHub sebagai sumber konfigurasi

Bagian ini memberi tahu Anda cara menerapkan Kustomisasi untuk AWS Control Tower (CfCT) GitHub sebagai sumber. Prosesnya memiliki tiga langkah utama:

- Siapkan GitHub repositori
- Buat koneksi GitHub kode
- Terapkan tum CloudFormation pukan

Siapkan GitHub repositori

Buat repositori dalam GitHub akun Anda, nama default yang digunakan dalam template adalah`custom-control-tower-configuration`. Pertimbangkan untuk membuat repositori target pribadi. Anda akan menentukan penyesuaian Anda dalam `yaml` file yang dipanggil `manifest.yaml` di folder pener apan repositori cFCT.

Panduan peny esuaian cFCT memberikan panduan terperinci tentang membuat `manifest.yaml` untuk mengonfigurasi penyesuaian Anda.

Buat GitHub koneksi

Dari instance Developer Tools --Connections untuk Github, lakukan langkah-langkah berikut:

1. Pilih Buat koneksi dan pilih GitHub sebagai penyedia
2. Pilih Buat koneksi GitHub Aplikasi, dan di bidang Nama koneksi, masukkan GitHub CfCT, atau nama apa pun yang Anda pilih
3. Pilih Hubungkan ke GitHub lalu pilih Instal aplikasi baru
4. Pilih GitHub Pengguna atau Organisasi untuk repositori Anda
5. Di bawah Akses repositori, pilih Hanya pilih repositori, lalu pilih repositori yang Anda buat sebelumnya, dan S impan pekerjaan Anda.
6. Perhatikan Kode Connections ARN - Anda akan membutuhkannya saat menerapkan CloudFormation tumpukan.

Menyebarkan CloudFormation tumpukan

- Unduh `custom-control-tower-initiation.template` file dari repositori.
- Buat CloudFormation tumpukan baru, menggunakan `custom-control-tower-initiation.template` file.
- Di bawah AWS CodePipeline Sumber, pilih GitHub (melalui Koneksi Kode).
- Di bawah GitHub Setup, tentukan bidang ini:
  - Untuk ARN dari Kode Koneksi, berikan Kode Koneksi ARN
  - untuk GitHub Pengguna atau Organisasi, berikan nama GitHub pengguna atau organisasi tempat Anda membuat repositori
  - Untuk Nama GitHub Repositori, masukkan nama repositori (default ke`custom-control-tower-configuration`)
  - Untuk Nama GitHub Cab ang, masukkan nama cabang (default ke`main`)

Pengumpulan metrik operasional

Kustomisasi untuk AWS Control Tower (CFCT) mencakup opsi untuk mengirim metrik operasional anonim ke. AWS AWS menggunakan data ini untuk memahami bagaimana pelanggan menggunakan CFCT, serta layanan dan produk terkait lainnya. Ketika pengumpulan data diaktifkan, informasi berikut dikirim ke AWS:

- ID Solusi: Pengidentifikasi AWS solusi
- Unique ID (UUID): Pengidentifikasi unik yang dibuat secara acak untuk setiap penerapan
- Stempel waktu: Stempel waktu pengumpulan data
- Jumlah Eksekusi Mesin Status: Secara bertahap menghitung berapa kali mesin status ini berjalan
- Manifest Version: Versi manifes yang digunakan dalam konfigurasi

> **Note**
>
> AWS memiliki data yang dikumpulkannya. Pengumpulan data tunduk pada Kebijakan AWS Privasi.

Untuk memilih keluar dari pengiriman metrik operasional anonim ke AWS, selesaikan salah satu tugas berikut:

- Perbarui bagian pemetaan AWS CloudFormation template sebagai berikut:

  dari

  ```
  AnonymousData:
       SendAnonymousData:
          Data: Yes
  ```

  untuk

  ```
  AnonymousData:
       SendAnonymousData:
          Data: No
  ```

- Setelah CFCT digunakan, cari kunci parameter **`/org/primary/metrics_flag`** SSM di konsol Parameter Store, dan perbarui nilainya ke. **`No`**

Panduan kustomisasi CfCT

Panduan Kustomisasi untuk Menara Kontrol AWS (CfCT) ditujukan untuk administrator, DevOps profesional, vendor perangkat lunak independen, arsitek infrastruktur TI, dan integrator sistem yang ingin menyesuaikan dan memperluas lingkungan Menara Kontrol AWS mereka untuk perusahaan dan pelanggan mereka. Ini memberikan informasi tentang menyesuaikan dan memperluas lingkungan AWS Control Tower dengan paket kustomisasi cFCT.

> **Note**
>
> Untuk menerapkan dan mengkonfigurasi (CfCT), Anda harus menerapkan dan memproses paket konfigurasi melalui AWS CodePipeline. Bagian berikut menjelaskan proses secara rinci.

Ikhtisar pipa kode

Paket konfigurasi memerlukan Amazon Simple Storage Service (Amazon S3) dan AWS CodePipeline. Paket konfigurasi berisi item ini:

- Sebuah file manifes
- Satu set templat yang menyertainya
- File JSON lainnya untuk menjelaskan dan mengimplementasikan penyesuaian lingkungan AWS Control Tower Anda

Secara default, paket `_custom-control-tower-configuration.zip` konfigurasi dimuat dalam bucket Amazon S3 dengan konvensi penamaan berikut:

`custom-control-tower-configuration-`*`accountID`*`-`*`region`*.

> **Note**
>
> Secara default, cFCT membuat bucket Amazon S3 untuk menyimpan sumber pipeline. Sebagian besar pelanggan tetap menggunakan default ini. Jika Anda memiliki AWS CodeCommit repositori yang ada, Anda dapat mengubah lokasi sumber ke AWS CodeCommit repositori Anda. Untuk informasi selengkapnya, lihat Meng edit pipeline CodePipeline di Panduan AWS CodePipeline Pengguna.

File manifes adalah file teks yang menjelaskan AWS sumber daya yang dapat Anda gunakan untuk menyesuaikan zona pendaratan Anda. CodePipeline melakukan tugas-tugas ini:

- mengekstrak file manifes, set templat yang menyertainya, dan file JSON lainnya
- melakukan validasi manifes dan template
- memanggil bagian dalam file manifes cfCT untuk menjalankan tahapan pipeline tertentu.

Saat Anda memperbarui paket konfigurasi dengan menyesuaikan file manifes dan menghapus garis bawah (_) dari nama file paket konfigurasi, paket akan dimulai secara otomatis. AWS CodePipeline

> **Ingat garis bawah**
>
> Nama file paket konfigurasi sampel dimulai dengan garis bawah (_) sehingga tidak AWS CodePipeline dipicu secara otomatis. Setelah Anda menyelesaikan penyesuaian paket konfigurasi, unggah file `custom-control-tower-configuration.zip` tanpa garis bawah (_) untuk memicu penerapan di AWS CodePipeline.

AWS CodePipeline tahapan

Pipeline cFCT memerlukan beberapa AWS CodePipeline tahap untuk mengimplementasikan dan memperbarui lingkungan AWS Control Tower Anda.

1. Tahap sumber

   Tahap sumber adalah tahap awal. Paket konfigurasi khusus Anda memulai tahap pipeline ini. Sumber untuk AWS CodePipeline dapat berupa bucket Amazon S3 atau AWS CodeCommit repositori, di mana paket konfigurasi dapat dihosting.
2. Bangun panggung

   Tahap build mengharuskan AWS CodeBuild untuk memvalidasi isi paket konfigurasi. Pemeriksaan ini termasuk pengujian sintaks `manifest.yaml` file dan skema, bersama dengan semua CloudFormation templat yang disertakan dalam paket atau dihosting dari jarak jauh, menggunakan CloudFormation `validate-template` dancfn_nag. Jika file manifes dan CloudFormation templat lulus tes, pipeline berlanjut ke tahap berikutnya. Jika pengujian gagal, Anda dapat meninjau CodeBuild log untuk mengidentifikasi masalah dan mengedit file sumber konfigurasi sesuai kebutuhan.
3. Tahap persetujuan manual (opsional)

Tahap persetujuan manual adalah opsional. Jika Anda mengaktifkan tahap ini, ini memberikan kontrol tambahan atas pipeline konfigurasi. Ini menjeda pipa selama penerapan, sampai persetujuan diberikan. Anda dapat memilih persetujuan manual dengan mengedit parameter Pipeline Approval Stage ke Ya saat Anda meluncurkan tumpukan.

4. Tahap Kebijakan Pengendalian Layanan

   Tahap Kebijakan Kontrol Layanan memanggil mesin status kebijakan kontrol layanan (SCP) untuk memanggil AWS Organizations API yang membuat SCP.

5. Tahap Kebijakan Pengendalian Sumber Daya

   Tahap Kebijakan Kontrol Sumber Daya memanggil mesin status kebijakan kontrol sumber daya (RCP) untuk memanggil AWS Organizations API yang membuat RCP.

6. CloudFormation tahap sumber daya

   T CloudFormation ahap sumber daya memanggil mesin status set tumpukan untuk menyebarkan sumber daya yang ditentukan dalam daftar akun atau unit organisasi (OU), yang Anda berikan dalam file manifes. Mesin status membuat CloudFormation sumber daya sesuai urutan yang ditentukan dalam file manifes. Untuk menentukan ketergantungan sumber daya, atur urutan sumber daya yang ditentukan dalam file manifes. Urutan sumber daya dalam file manifes adalah satu-satunya cara untuk menentukan ketergantungan.

Tentukan konfigurasi khusus

Anda akan menentukan konfigurasi Menara Kontrol AWS kustom Anda dengan file manifes cFct, kumpulan templat yang menyertainya, dan file JSON lainnya. Anda akan mengemas file-file ini ke dalam struktur folder dan menempatkannya di bucket Amazon S3 sebagai `.zip` file, seperti yang ditunjukkan dalam contoh kode berikut.

Struktur folder konfigurasi kustom

```
- manifest.yaml
- policies/                                                [optional]
   - service control policies files (*.json)
- templates/                                               [optional]
   - template files for AWS CloudFormation Resources (*.template)
```

Contoh sebelumnya menggambarkan struktur folder konfigurasi kustom. Struktur folder tetap sama apakah Anda memilih Amazon S3 atau AWS CodeCommit repositori sebagai lokasi penyimpanan sumber Anda. Jika Anda memilih Amazon S3 sebagai penyimpanan sumber, kompres semua folder dan file ke dalam `custom-control-tower-configuration.zip` file, dan unggah hanya `.zip` file tersebut ke bucket Amazon S3 yang ditunjuk.

> **Note**
>
> Jika Anda menggunakan AWS CodeCommit, letakkan file di repositori tanpa zip file.

File manifes cfCT

File CFCT adalah `manifest.yaml` file teks yang menjelaskan AWS sumber daya Anda. Contoh berikut menunjukkan struktur file manifes cfCT.

```
---
region: String
version: 2021-03-15

resources:
  #set of CloudFormation resources, SCP policies, or RCP policies
...
```

Seperti yang ditunjukkan pada contoh kode sebelumnya, dua baris pertama dari file manifes menentukan nilai wilayah dan kata kunci versi. Berikut adalah definisi dari kata kunci tersebut.

region — String teks untuk Wilayah default Menara Kontrol AWS. Nilai ini harus berupa nama Wil AWS ayah yang valid (sepertius-east-1,eu-west-1, atauap-southeast-1). Wilayah rumah AWS Control Tower adalah default saat Anda membuat sumber daya AWS Control Tower kustom (seperti CloudFormation StackSets), kecuali jika Wilayah yang lebih spesifik sumber daya ditentukan.

```
region:your-home-region
```

version — Nomor versi skema manifes. Versi terbaru yang didukung adalah 2021-03-15.

```
version: 2021-03-15
```

> **Note**
>
> Kami sangat menyarankan Anda menggunakan versi terbaru. Untuk memperbarui properti manifes dalam versi terbaru, lihatPeningkatan versi untuk manifes cFCT.

Kata kunci berikutnya yang ditampilkan dalam contoh sebelumnya adalah kata kunci resource. Bagian sumber daya dari file manifes sangat terstruktur. Ini berisi daftar rinci AWS sumber daya, yang akan digunakan secara otomatis oleh pipa CfCT. Deskripsi sumber daya dan parameter yang tersedia diberikan di bagian berikutnya.

Bagian sumber daya dari file manifes cfCT

Topik ini menjelaskan bagian sumber daya dari file manifes cFct, di mana Anda akan menentukan sumber daya yang diperlukan untuk penyesuaian Anda. Bagian dari file manifes cfCT ini dimulai pada sumber daya kata kunci dan berlanjut ke akhir file.

Bagian sumber daya dari file manifes menentukan CloudFormation StackSets, atau AWS Organizations SCP dan RCP, yang digunakan CfCT secara otomatis melalui pipa kode. Anda dapat mencantumkan OU, akun, dan Wilayah untuk menerapkan instans tumpukan.

Instans tumpukan digunakan di tingkat akun, bukan tingkat OU. SCP dan RCP dikerahkan di tingkat OU. Untuk informasi selengkapnya, lihat Membuat penyesuaian Anda sendiri.

Template contoh berikut menjelaskan kemungkinan entri yang tersedia untuk bagian sumber daya dari file manifes.

```
resources: # List of resources
  - name: [String]
    resource_file: [String] [Local File Path, S3 URI, S3 URL]
    deployment_targets: # account and/or organizational unit names
      accounts: # array of strings, [0-9]{12}
        - 012345678912
        - AccountName1
      organizational_units: #array of strings
        - OuName1
        - OuName2
    deploy_method: scp | stack_set | rcp
    parameters: # List of parameters [SSM, Alfred, Values]
      - parameter_key: [String]
        parameter_value: [String]
```

```
    export_outputs: # list of ssm parameters to store output values
      - name: /org/member/test-ssm/app-id
        value: $[output_ApplicationId]
    regions: #list of strings
    - [String]
```

Sisa topik ini memberikan definisi terperinci untuk kata kunci yang ditunjukkan dalam contoh kode sebelumnya.

name — Nama yang terkait dengan CloudFormation StackSets.
String yang Anda berikan memberikan nama yang lebih ramah pengguna untuk kumpulan tumpukan.

- Tipe: String
- Wajib: Ya
- Nilai yang Valid: a-z, A-Z, 0-9, dan tanda hubung (-). Nama harus dimulai dengan karakter abjad.

deskripsi — Deskripsi untuk sumber daya.

- Tipe: String
- Wajib: Tidak

resource_file — File ini dapat ditentukan sebagai lokasi relatif ke file manifes, URI Amazon S3 atau URL yang menunjuk ke CloudFormation template atau kebijakan kontrol AWS Organizations layanan di JSON untuk membuat CloudFormation sumber daya, SCP, atau RCP.

- Tipe: String
- Wajib: Ya

1. Contoh berikut menunjukkan`resource_file`, diberikan sebagai lokasi relatif ke file sumber daya di dalam paket konfigurasi.

   ```
   resources:
     - name: SecurityRoles
       resource_file: templates/custom-security.template
   ```

2. Contoh berikut menunjukkan file sumber daya yang diberikan sebagai URI Amazon S3

   ```
   resources:
   ```

```
  - name: SecurityRoles
    resource_file: s3://amzn-s3-demo-bucket/[key-name]
```

3. Contoh berikut menunjukkan file sumber daya yang diberikan sebagai URL HTTPS Amazon S3

```
resources:
  - name: SecurityRoles
    resource_file: https://bucket-name.s3.Region.amazonaws.com/key-name
```

> **Note**
>
> Jika Anda memberikan URL Amazon S3, verifikasi bahwa kebijakan bucket mengizinkan akses baca untuk akun manajemen AWS Control Tower tempat Anda menerapkan CfCT. Jika Anda memberikan URL HTTPS Amazon S3, verifikasi bahwa jalur tersebut menggunakan notasi titik. Misalnya, `S3.us-west-1`. CfCT tidak mendukung titik akhir yang berisi tanda hubung antara S3 dan Wilayah, seperti. `S3-us-west-2`

4. Contoh berikut menunjukkan kebijakan bucket Amazon S3 dan ARN tempat sumber daya disimpan.

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
        "Effect": "Allow",
        "Principal": {"AWS": "arn:aws:iam::AccountId:root"},
        "Action": "s3:GetObject",
        "Resource": "arn:aws:s3:::my-bucket/*”
       }
   ]
}
```

Anda akan mengganti *AccountId* variabel yang ditunjukkan dalam contoh dengan ID AWS akun untuk akun manajemen yang menerapkan CfCT. Untuk contoh selengkapnya, lihat contoh kebijakan Bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

parameter — Menentukan nama dan nilai untuk CloudFormation parameter.

- Jenis MapList:
- Wajib: Tidak

Bagian parameter berisi pasangan key/value parameter. Template semu berikut menguraikan bagian parameter.

```
parameters:
  - parameter_key: [String]
    parameter_value: [String]
```

- parameter_key — Kunci yang terkait dengan parameter.
  - Tipe: String
  - Diperlukan: Ya (di bawah properti parameter)
  - Nilai yang Valid: a-z, A-Z, dan 0-9
- parameter_value — Nilai input yang terkait dengan parameter.
  - Tipe: String
  - Diperlukan: Ya (di bawah properti parameter)

deploy_method — Metode penerapan untuk menyebarkan sumber daya ke dalam akun. Saat ini, deploy_method mendukung penerapan sumber daya menggunakan `stack_set` opsi untuk penyebaran sumber daya melalui CloudFormation StackSets, `scp` opsi jika Anda menerapkan SCP, atau `rcp` opsi jika Anda menerapkan RCP.

- Tipe: String
- Nilai yang Valid: `stack_set` | `scp` | `rcp`
- Wajib: Ya

deployment_target — Daftar akun atau Unit Organisasi (OU), di mana CfCT akan menyebarkan CloudFormation sumber daya, ditentukan sebagai akun atau organizational_units.

> **Note**
>
> Jika Anda ingin menerapkan SCP atau RCP, targetnya harus OU, bukan akun.

- Jenis: Daftar string `account name` atau `account number` untuk menunjukkan bahwa sumber daya ini akan digunakan ke daftar akun yang diberikan, atau `0U names` untuk menunjukkan bahwa sumber daya ini akan digunakan ke daftar OU yang diberikan.
- Diperlukan: Setidaknya satu akun atau organizational_units
  - akun:

    Jenis: Daftar string `account name` atau `account number` untuk menunjukkan bahwa sumber daya ini akan digunakan ke daftar akun yang diberikan.
  - unit_organisasi:

    Jenis: Daftar string `0U names` untuk menunjukkan bahwa sumber daya ini akan digunakan ke daftar OU tertentu. Jika Anda menyediakan OU yang tidak berisi akun dan properti account tidak ditambahkan, CfCt hanya membuat kumpulan tumpukan.

    > **Note**
    >
    > ID akun manajemen organisasi bukanlah nilai yang diizinkan. CfCT tidak mendukung penerapan instans tumpukan ke akun manajemen organisasi, secara default. Jika Anda memiliki kasus penggunaan khusus, lihat Root OU.

export_output — Daftar name/value pasangan yang menunjukkan kunci parameter SSM. Kunci parameter SSM ini memungkinkan Anda untuk menyimpan output template ke dalam penyimpanan parameter SSM. Output dimaksudkan untuk referensi oleh sumber daya lain, yang didefinisikan sebelumnya dalam file manifes.

```
export_outputs: # List of SSM parameters
  - name: [String]
    value: [String]
```

- Jenis: Daftar pasangan kunci nama dan nilai. Nama berisi `name` string kunci penyimpanan parameter SSM, dan nilai berisi `value` string parameter.
- Nilai Valid: Setiap string atau `$[output_`*`CfnOutput-Logical-ID`*`]` variabel yang *`CfnOutput-Logical-ID`* sesuai dengan variabel keluaran template. Untuk informasi selengkapnya tentang bagian Output dalam CloudFormation template, lihat Output di Panduan CloudFormation Pengguna.
- Wajib: Tidak

Misalnya, cuplikan kode berikut menyimpan variabel VPCID keluaran template ke dalam kunci parameter SSM yang diberi nama. /org/member/audit/vpc_id

```
export_outputs: # List of SSM parameters
  - name: /org/member/audit/VPC-ID
    value: $[output_VPCID]
```

> **Note**
>
> Nama kunci export_output mungkin berisi nilai selain. output Misalnya, jika namanya / org/environment-name, nil ainya mungkinproduction.

wilayah — Daftar Wilayah di mana CfCT akan menerapkan instans CloudFormation tumpukan.

- Jenis: Setiap daftar nama AWS Wilayah komersial, untuk menunjukkan bahwa sumber daya ini akan digunakan ke daftar Wilayah yang diberikan. Jika kata kunci ini tidak ada di file manifes, sumber daya digunakan di Wilayah beranda saja.
- Wajib: Tidak

Root OU

CfCT mendukung Root sebagai nilai untuk unit organisasi (OU) di bawah organizational_units dalam versi manifes V2 (2021-03-15).

- Jika Anda memilih metode penerapan scp ataurcp, saat menambahkan Root di bawahorganizational_units, AWS Control Tower menerapkan kebijakan ke semua OU di bawah Root. Jika Anda memilih metode penerapanstack_set, saat Anda menambahkan Root di bawahorganizational_units, cFCT menerapkan kumpulan tumpukan di semua akun di bawah Root yang terdaftar di AWS Control Tower, kecuali untuk akun manajemen.
- Sesuai praktik terbaik AWS Control Tower, akun manajemen dimaksudkan hanya untuk mengelola akun anggota dan untuk tujuan penagihan. Jangan menjalankan beban kerja produksi di akun manajemen AWS Control Tower.

  Sesuai dengan panduan praktik terbaik, penyebaran AWS Control Tower menempatkan akun manajemen di bawah Root OU, sehingga memiliki akses penuh dan tidak menjalankan sumber daya tambahan. Untuk alasan ini, AWSControlTowerExecution peran tidak digunakan ke akun manajemen.

- Kami menyarankan Anda mengikuti praktik terbaik ini untuk akun manajemen. Jika Anda memiliki kasus penggunaan tertentu yang mengharuskan Anda menerapkan kumpulan tumpukan di akun manajemen, sertakan akun sebagai target penerapan dan tentukan akun manajemen. Jika tidak, jangan sertakan akun sebagai target penerapan. Anda harus membuat sumber daya yang hilang, termasuk peran IAM yang diperlukan, di akun manajemen.

Untuk menerapkan set tumpukan di akun manajemen, sertakan `accounts` sebagai target penerapan dan tentukan akun manajemen. Jika tidak, jangan sertakan akun sebagai target penerapan.

```
---
region: your-home-region
version: 2021-03-15

resources:

  …truncated…

    deployment_targets:
      organizational_units:
        - Root
```

> **Note**
>
> Fitur Root OU hanya didukung dalam versi V2 dari file manifes (2021-03-15). Jika Anda menambahkan Root sebagai OU di bawah`organizational_units`, jangan tambahkan OU lainnya.

OU bersarang

CfCT mendukung daftar satu atau lebih OU bersarang di bawah `organizational_units` kata kunci dalam versi manifes V2 (2021-03-15).

Diperlukan jalur lengkap (tidak termasuk Root) untuk OU bersarang, menggunakan titik dua sebagai pemisah antara OU. Untuk metode pener `scp` apan atau`rcp`, AWS Control Tower menerapkan SCP atau RCP ke OU terakhir di jalur OU bersarang. Untuk metode penerapan`stack_set`, AWS Control Tower menyebarkan kumpulan tumpukan ke semua akun di bawah OU terakhir di jalur OU bersarang.

Misalnya, pertimbangkan jalurnya`OUName1:OUName2:OUName3`. OU terakhir di jalan adalah`OUName3`. CfCT menyebarkan SCP atau RCP ke `OUName3` dan menumpuk set ke semua akun langsung di bawah, saja. `OUName3`

```
---
region: your-home-region
version: 2021-03-15

resources:

  …truncated…

    deployment_targets:
      organizational_units:
        - OuName1:OUName2:OUName3
```

> **Note**
>
> Fitur OU bersarang hanya didukung dalam versi V2 dari file manifes (2021-03-15).

Buat kustomisasi Anda sendiri

Untuk membuat penyesuaian sendiri, Anda dapat memodifikasi `manifest.yaml` file CfCT dengan menambahkan atau memperbarui kebijakan kontrol layanan (SCP), kebijakan kontrol sumber daya (RCP), dan sumber daya. CloudFormation Untuk sumber daya yang harus digunakan, Anda dapat menambahkan atau menghapus akun dan OU. Anda dapat menambahkan atau memodifikasi template di folder paket, membuat folder Anda sendiri, dan mereferensikan template atau folder dalam `manifest.yaml` file.

Bagian ini menjelaskan dua bagian utama membangun kustomisasi Anda sendiri:

- cara mengatur paket konfigurasi Anda sendiri untuk kebijakan kontrol layanan
- cara mengatur paket konfigurasi Anda sendiri untuk set AWS CloudFormation tumpukan

Siapkan paket konfigurasi untuk SCP atau RCP

Bagian ini menjelaskan cara membuat paket konfigurasi untuk kebijakan kontrol layanan (SCP) atau kebijakan kontrol sumber daya (RCP). Dua bagian utama dari proses ini adalah (1) menyiapkan file manifes cfCT, dan (2) menyiapkan struktur folder Anda.

Langkah 1: Edit file manifest.yaml

Gunakan `manifest.yaml` file sampel sebagai titik awal Anda. Masukkan semua konfigurasi yang diperlukan. Tambahkan `resource_file` dan `deployment_targets` detailnya.

Cuplikan berikut menunjukkan file manifes default.

```
---
region: us-east-1
version: 2021-03-15

resources: []
```

Nilai untuk ditambahkan `region` secara otomatis selama penerapan. Itu harus sesuai dengan Wilayah tempat Anda menggunakan CfCT. Wilayah ini harus sama dengan wilayah Menara Kontrol AWS.

Untuk menambahkan SCP atau RCP khusus di `example-configuration` folder dalam paket zip yang disimpan di bucket Amazon S3, buka `example-manifest.yaml` file dan mulailah mengedit.

```
---
region: your-home-region
version: 2021-03-15

resources:
  - name: test-preventive-controls
    description: To prevent from deleting or disabling resources in member accounts
    resource_file: policies/preventive-controls.json
    deploy_method: scp | rcp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - OUName1
        - OUName2

…truncated…
```

Cuplikan berikut menunjukkan contoh file manifes yang disesuaikan. Anda dapat menambahkan lebih dari satu kebijakan dalam satu perubahan.

```
---
region: us-east-1
version: 2021-03-15

resources:
  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp | rcp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - OUName1
        - OUName2
```

Langkah 2: Buat struktur folder

Anda dapat melewati langkah ini jika Anda menggunakan URL Amazon S3 untuk file sumber daya dan menggunakan parameter dengan key/value pasangan.

Anda harus menyertakan kebijakan SCP atau kebijakan RCP dalam format JSON untuk mendukung manifes, karena file manifes mereferensikan file JSON. Pastikan jalur file cocok dengan informasi jalur yang disediakan dalam file manifes.

- File JSON kebijakan berisi SCP atau RCP yang akan digunakan ke OU.

Cuplikan berikut menunjukkan struktur folder untuk file manifes sampel.

```
- manifest.yaml
- policies/
   - block-s3-public.json
```

Cuplikan berikut adalah contoh file `block-s3-public.json` kebijakan.

JSON

```
{
```

```
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"GuardPutAccountPublicAccessBlock",
         "Effect":"Deny",
         "Action":"s3:PutAccountPublicAccessBlock",
         "Resource":"arn:aws:s3:::*"
      }
   ]
}
```

Menyiapkan paket konfigurasi untuk CloudFormation StackSets

Bagian ini menjelaskan cara mengatur paket konfigurasi untuk CloudFormation StackSets. Dua bagian utama dari proses ini adalah: (1) menyiapkan file manifes, dan (2) memperbarui struktur folder.

Langkah 1: Edit file manifes yang ada

Tambahkan CloudFormation StackSets informasi baru ke file manifes yang sebelumnya Anda edit.

Hanya untuk ditinjau, cuplikan berikut berisi file manifes khusus yang sama yang ditampilkan sebelumnya untuk menyiapkan paket konfigurasi untuk SCP atau RCP. Sekarang Anda dapat mengedit file ini lebih lanjut, untuk memasukkan detail tentang sumber daya Anda.

```
---
region: us-east-1
version: 2021-03-15

resources:

  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp | rcp
    #Apply to the following OU(s)
    deployment_targets:
    organizational_units: #array of strings
    - OUName1
    - OUName2
```

Cuplikan berikut menunjukkan file manifes sampel yang diedit yang berisi `resources` detail. Urutan `resources` menentukan urutan eksekusi untuk membuat `resources` dependensi. Anda dapat mengedit contoh file manifes berikut sesuai dengan kebutuhan bisnis Anda.

```
---
region: your-home-region
version: 2021-03-15

…truncated…

resources:
  - name: stackset-1
    resource_file: templates/create-ssm-parameter-keys-1.template
    parameters:
      - parameter_key: parameter-1
        parameter_value: value-1
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - account number or account name
        - 123456789123
      organizational_units: #array of strings, ou ids, ou-xxxx
        - OuName1
        - OUName2
    export_outputs:
      - name: /org/member/test-ssm/app-id
        value: $[output_ApplicationId]
    regions:
      - region-name

  - name: stackset-2
    resource_file: s3://bucket-name/key-name
    parameters:
      - parameter_key: parameter-1
        parameter_value: value-1
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - account number or account name
        - 123456789123
      organizational_units: #array of strings
        - OuName1
        - OUName2
```

```
regions:
  - region-name
```

Contoh berikut menunjukkan bahwa Anda dapat menambahkan lebih dari satu CloudFormation sumber daya dalam file manifes.

```
---
region: us-east-1
version: 2021-03-15

resources:
  - name: block-s3-public-access
    description: To S3 buckets to have public access
    resource_file: policies/block-s3-public.json
    deploy_method: scp | rcp
    #Apply to the following OU(s)
    deployment_targets:
      organizational_units: #array of strings
        - Custom
        - Sandbox

  - name: transit-network
    resource_file: templates/transit-gateway.template
    parameter_file: parameters/transit-gateway.json
    deploy_method: stack_set
    deployment_targets:
      accounts: # array of strings, [0-9]{12}
        - Prod
        - 123456789123 #Network
      organizational_units: #array of strings
        - Custom
    export_outputs:
      - name: /org/network/transit-gateway-id
        value: $[output_TransitGatewayID]
    regions:
      - us-east-1
```

Langkah 2: Perbarui struktur folder

Saat memperbarui struktur folder, Anda dapat menyertakan semua file CloudFormation template pendukung dan file kebijakan SCP atau RCP yang ada dalam file manifes. Verifikasi bahwa jalur file cocok dengan apa yang disediakan dalam file manifes.

- File template berisi AWS sumber daya yang akan digunakan di OU dan akun.
- File kebijakan berisi parameter input yang digunakan dalam file template.

Contoh berikut menunjukkan struktur folder untuk file manifes sampel yang dibuat pada Langkah 1.

```
- manifest.yaml
- policies/
   - block-s3-public.json
- templates/
   - transit-gateway.template
```

Pembantu 'Alfred' dan CloudFormation berkas parameter

CfCT memberi Anda mekanisme yang dikenal sebagai helper Alfred untuk mendapatkan nilai kunci Penyimpanan Parameter SSM yang didefinisikan dalam template. CloudFormation Menggunakan helper Alfred, Anda dapat menggunakan nilai yang disimpan di SSM Parameter Store dan tanpa memperbarui CloudFormation template. Untuk informasi selengkapnya, lihat Apa itu CloudFormation template? dalam Panduan CloudFormation Pengguna.

> **Important**
>
> Pemb antu Alfred memiliki dua keterbatasan. Parameter hanya tersedia di wilayah asal akun manajemen AWS Control Tower. Sebagai praktik terbaik, pertimbangkan untuk bekerja dengan nilai yang tidak berubah dari instance stack ke instance stack. Ketika pembantu 'Alfred' mereproduksi kembali parameter, ia memilih instance tumpukan acak dari kumpulan tumpukan yang mengekspor variabel.

Contoh

Misalkan Anda memiliki dua set CloudFormation tumpukan. Stack set 1 memiliki satu instance stack dan disebarkan ke satu akun di satu Wilayah. Ini membuat Amazon VPC dan subnet di zona ketersediaan, dan `VPC ID` dan `subnet ID` harus diteruskan ke stack set 2 sebagai nilai parameter. Sebelum `VPC ID` dan `subnet ID` dapat diteruskan ke set tumpukan 2, `VPC ID` dan `subnet ID` harus disimpan dalam set tumpukan 1 menggunakan`AWS:::SSM::Parameter`. Untuk informasi selengkapnya, lihat `AWS:::SSM::Parameter` di CloudFormation Panduan Pengguna.

CloudFormation set tumpukan 1:

Dalam cuplikan berikut, helper Alfred dapat mendapatkan nilai untuk `VPC ID` dan `subnet ID` dari penyimpanan parameter dan meneruskannya sebagai input ke mesin StackSet status.

```
VpcIdParameter:
    Type: AWS::SSM::Parameter
    Properties:
      Name: '/stack_1/vpc/id'
      Description: Contains the VPC id
      Type: String
      Value: !Ref MyVpc

SubnetIdParameter:
    Type: AWS::SSM::Parameter
    Properties:
      Name: '/stack_1/subnet/id'
      Description: Contains the subnet id
      Type: String
      Value: !Ref MySubnet
```

CloudFormation set tumpukan 2:

Cuplikan menunjukkan parameter yang ditentukan dalam `manifest.yaml` file CloudFormation stack 2.

```
parameters:
      - parameter_key: VpcId
        parameter_value: $[alfred_ssm_/stack_1/vpc/id]
      - parameter_key: SubnetId
        parameter_value: $[alfred_ssm_/stack_1/subnet/id]
```

CloudFormation set tumpukan 2.1:

Cuplikan menunjukkan bahwa Anda dapat mencant `alfred_ssm` umkan properti untuk mendukung parameter jenis CommaDelimitedList. Untuk informasi selengkapnya, lihat `Parameters` di CloudFormation Panduan Pengguna.

```
parameters:
      - parameter_key: VpcId # Type: String
        parameter_value: $[alfred_ssm_/stack_1/vpc/id']
      - parameter_key: SubnetId # Type: String
        parameter_value: $[ alfred_ssm_/stack_1/subnet/id']
      - parameter_key: AvailablityZones # Type: CommaDelimitedList
```

```
        parameter_value:
  - "$[alfred_ssm_/availability_zone_1]"
  - "$[alfred_ssm_/availability_zone_2]"
```

Skema JSON untuk paket kustomisasi

Skema JSON untuk paket kustomisasi untuk CfCT terletak di repositori kode sumber pada GitHub. Anda dapat menggunakan skema dengan banyak alat pengembangan favorit Anda, dan Anda mungkin merasa berguna untuk mengurangi kesalahan saat Anda membuat `manifest.yaml` file cfct Anda sendiri.

Peningkatan versi untuk manifes cFCT

Untuk informasi tentang versi terbaru Ku stomisasi untuk AWS Control Tower (CfCT), lihat `CHANGELOG.md file` di repositori. GitHub

Warning

Versi 2.2.0 dari Ku stomisasi untuk AWS Control Tower (cFCT) memperkenalkan skema manifes cFCT (versi 2021-03-15) untuk menyelaraskan dengan API layanan terkait. AWS Skema manifes memungkinkan satu file manifest.yaml untuk mengelola sumber daya yang didukung (CloudFormation template, SCP, dan RCP) melalui alur kerja yang dipisahkan. DevOps

Kami sangat menyarankan Anda memperbarui skema manifes cFCT dari versi 2020-01-01 ke versi 2021- 03-15 atau yang lebih baru.

CfCT terus mendukung versi 2021-03-15 dan 2020-01- 01 dari file tersebut. `manifest.yaml` Tidak diperlukan perubahan pada konfigurasi yang ada. Namun, versi 2020-01-01 berada di Ak hir Dukungan. Kami tidak lagi menyediakan pembaruan atau menambahkan penyempurnaan ke versi 2020-01-01. Fitur Root OU dan OU bersarang tidak didukung di versi 2020- 01-01.

Properti yang tidak digunakan lagi dalam manifes cfCT versi 2021-03-15:

```
organization_policies
policy_file
apply_to_accounts_in_ou
```

```
cloudformation_resources
template_file
deploy_to_account
deploy_to_ou
ssm_parameters
```

Langkah-langkah peningkatan CfCT wajib

Saat Anda memutakhirkan ke skema manifes cFCT versi 2021-03-15, berikut adalah perubahan yang harus Anda lakukan untuk memperbarui file Anda. Bagian selanjutnya menguraikan perubahan wajib dan direkomendasikan untuk transisi.

Kebijakan organisasi

1. Pindahkan SCP atau RCP di bawah organization_policies di bawah sumber daya properti baru.
2. Ubah properti policy_file ke properti baru resource_file.
3. Ubah apply_to_accounts_in_ou ke properti deployment_target baru. Daftar OU harus didefinisikan di bawah sub-properti organiz ational_units. Sub-properti akun tidak didukung untuk kebijakan organisasi.
4. Tambahkan properti baru deploy_method dengan nilai scp atau rcp.

CloudFormation sumber daya

1. Pindahkan CloudFormation sumber daya di bawah cloudformation_resources di bawah sumber daya properti baru.
2. Ubah properti template_file ke properti baru resource_file.
3. Ubah deploy_to_ou ke properti baru deployment_target. Daftar OU harus didefinisikan di bawah sub-properti organiz ational_units.
4. Ubah deploy_to_accounts ke properti deployment_target baru. Daftar akun harus ditentukan di bawah akun sub-properti.
5. Ubah properti ssm_parameters ke properti baru export_output.

Langkah-langkah peningkatan cFCT yang sangat direkomendasikan

CloudFormation parameter

1. Ubah properti parameter_file ke parameter properti baru.

2. Hapus jalur file dalam nilai properti parameter_file.
3. Salin kunci parameter dan nilai parameter dari file JSON parameter yang ada ke format baru untuk properti parameter. Ini akan membantu Anda mengelolanya di file manifes.

> **Note**
>
> Properti parameter_file didukung dalam manifes cfCT versi 2021-03-15.

Jaringan di Menara Kontrol AWS

AWS Control Tower menyediakan dukungan dasar untuk jaringan melalui VPC.

Jika konfigurasi atau kemampuan default AWS Control Tower VPC tidak memenuhi kebutuhan Anda, Anda dapat menggunakan AWS layanan lain untuk mengonfigurasi VPC Anda. Untuk informasi selengkapnya tentang cara bekerja dengan VPC dan AWS Control Tower, lihat Mem bangun Infrastruktur Multi-VPC AWS Jaringan yang Dapat Diskalakan dan Aman.

AWS Control Tower mendukung protokol IPv4 dan IPv6, melalui alamat IP dual-stack. Untuk informasi selengkapnya, lihat titik akhir dan kuota Katalog AWS Kontrol serta titik akhir dan kuota AWS Control Tower.

Topik terkait

- Untuk informasi tentang cara kerja AWS Control Tower saat Anda mendaftarkan akun yang memiliki VPC yang sudah ada, lihatDaftarkan akun yang ada dengan VPC.
- Dengan Account Factory, Anda dapat menyediakan akun yang menyertakan AWS Control Tower VPC, atau Anda dapat menyediakan akun tanpa VPC. Untuk informasi tentang cara menghapus AWS Control Tower VPC atau mengonfigurasi akun AWS Control Tower tanpa VPC, lihat. Panduan: Konfigurasikan Menara Kontrol AWS Tanpa VPC
- Untuk informasi tentang cara mengubah pengaturan akun untuk VPC, lihat dokumentasi Pabrik Akun tentang memperbarui akun.
- Untuk informasi selengkapnya tentang bekerja dengan jaringan dan VPC di AWS Control Tower, lihat bagian tentang Jaringan di halaman informasi terkait Panduan Pengguna ini.

VPC dan AWS Wilayah di AWS Control Tower

Sebagai bagian standar pembuatan akun, AWS buat VPC AWS default di setiap Wilayah, bahkan Wilayah yang tidak Anda atur dengan AWS Control Tower. VPC default ini tidak sama dengan VPC yang dibuat AWS Control Tower untuk akun yang disediakan, tetapi VPC AWS default di Wilayah yang tidak diatur mungkin dapat diakses oleh pengguna IAM.

Adminstrator dapat mengaktifkan kontrol Penolakan Wilayah, sehingga pengguna akhir Anda tidak memiliki izin untuk terhubung ke VPC di Wilayah yang didukung oleh AWS Control Tower tetapi di luar Wilayah yang diatur. Untuk mengonfigurasi kontrol penolakan wilayah, buka halaman pengaturan zona pendaratan dan pilih Ubah pengaturan.

Kontrol penolakan Wilayah memblokir panggilan API ke sebagian besar layanan yang tidak diatur Wilayah AWS. Untuk informasi selengkapnya, lihat Men AWS olak akses berdasarkan permintaan Wilayah AWS. .

> **Note**
>
> Kontrol Penolakan Wilayah mungkin tidak mencegah pengguna IAM terhubung ke VPC AWS default di Wilayah di mana AWS Control Tower tidak didukung.

Secara opsional, Anda dapat menghapus VPC AWS default di Wilayah yang tidak diatur. Untuk mencantumkan VPC default di Wilayah, Anda dapat menggunakan perintah CLI yang mirip dengan contoh ini:

```
aws ec2 --region us-west-1 describe-vpcs --filter Name=isDefault,Values=true
```

Ikhtisar AWS Control Tower dan VPC

Berikut adalah beberapa fakta penting tentang AWS Control Tower VPC:

- VPC yang dibuat oleh AWS Control Tower saat Anda menyediakan akun di Account Factory tidak sama dengan AWS VPC default.
- AWS Control Tower secara otomatis menghapus VPC default di Wilayah yang diatur yang dipilih (AWS Wilayah yang diatur oleh AWS Control Tower di landing zone Anda) untuk akun yang Anda buat dari konsol AWS Control Tower. AWS Control Tower tidak menghapus VPC default di akun yang ada, yang menyertakan akun yang Anda berikan dalam file `CreateLandingZone` manifes atau memilih dari AWS Organisasi Anda selama penyiapan Control Tower.
- Setiap akun AWS Control Tower diizinkan satu VPC yang dibuat oleh AWS Control Tower. Akun dapat memiliki AWS VPC tambahan dalam batas akun.
- Setiap AWS Control Tower VPC memiliki tiga Availability Zone di semua Wilayah kecuali Wilayah AS Barat (California Utara)`us-west-1`, dan dua Availability Zone di. `us-west-1` Secara default, setiap Availability Zone diberi satu subnet publik dan dua subnet pribadi. Oleh karena itu, di Wilayah kecuali US West (California N.) setiap AWS Control Tower VPC berisi sembilan subnet secara default, dibagi menjadi tiga Availability Zone. Di AS Barat (California Utara), enam subnet dibagi menjadi dua Availability Zone.
- Setiap subnet di AWS Control Tower VPC Anda diberi rentang unik, dengan ukuran yang sama.

- Jumlah subnet dalam VPC dapat dikonfigurasi. Untuk informasi selengkapnya tentang cara mengubah konfigurasi subnet VPC Anda, lihat topik Account Factory.
- Karena alamat IP tidak tumpang tindih, enam atau sembilan subnet dalam AWS Control Tower VPC Anda dapat berkomunikasi satu sama lain dengan cara yang tidak terbatas.

Saat bekerja dengan VPC, AWS Control Tower tidak membuat perbedaan di tingkat Wilayah. Setiap subnet dialokasikan dari rentang CIDR yang tepat yang Anda tentukan. Subnet VPC dapat ada di Wilayah mana pun.

Catatan

> **Kelola biaya VPC**
>
> Jika Anda menyetel konfigurasi VPC Account Factory sehingga subnet publik diaktifkan saat menyediakan akun baru, Account Factory akan mengonfigurasi VPC untuk membuat NAT Gateway. Anda akan ditagih untuk penggunaan Anda oleh Amazon VPC.

> **VPC dan pengaturan kontrol**
>
> Jika Anda menyediakan akun Account Factory dengan pengaturan akses internet VPC diaktifkan, setelan Account Factory akan mengganti kontrol Larang akses internet untuk instans Amazon VPC yang dikelola oleh pelanggan. Untuk menghindari mengaktifkan akses internet untuk akun yang baru disediakan, Anda harus mengubah pengaturan di Account Factory. Untuk informasi selengkapnya, lihat Panduan: Mengonfigurasi AWS Control Tower Tanpa VPC.

CIDR dan Peering untuk VPC dan AWS Control Tower

Bagian ini ditujukan terutama untuk administrator jaringan. Administrator jaringan perusahaan Anda biasanya adalah orang yang memilih rentang CIDR keseluruhan untuk organisasi AWS Control Tower Anda. Administrator jaringan kemudian mengalokasikan subnet dari dalam rentang tersebut untuk tujuan tertentu.

Saat Anda memilih rentang CIDR untuk VPC Anda, AWS Control Tower memvalidasi rentang alamat IP sesuai dengan spesifikasi RFC 1918. Account Factory memungkinkan blok CIDR hingga `/16` dalam rentang:

- `10.0.0.0/8`
- `172.16.0.0/12`
- `192.168.0.0/16`
- `100.64.0.0/10`(hanya jika penyedia internet Anda mengizinkan penggunaan rentang ini)

`/16`Pembatas memungkinkan hingga 65.536 alamat IP yang berbeda.

Anda dapat menetapkan alamat IP yang valid dari rentang berikut:

- `10.0.x.x to 10.255.x.x`
- `172.16.x.x - 172.31.x.x`
- `192.168.0.0 - 192.168.255.255`(tidak ada IP di luar `192.168` jangkauan)

Jika rentang yang Anda tentukan berada di luar ini, AWS Control Tower memberikan pesan kesalahan.

Rentang CIDR default adalah`172.31.0.0/16`.

Saat AWS Control Tower membuat VPC menggunakan rentang CIDR yang Anda pilih, AWS Control Tower menetapkan rentang CIDR yang sama ke setiap VPC untuk setiap akun yang Anda buat dalam unit organisasi (OU). Karena tumpang tindih default alamat IP, implementasi ini pada awalnya tidak mengizinkan pengintipan di antara VPC AWS Control Tower Anda di OU.

Subnet

Dalam setiap VPC, AWS Control Tower membagi rentang CIDR yang Anda tentukan secara merata menjadi sembilan subnet (kecuali di AS Barat (California Utara), di mana itu adalah enam subnet). Tak satu pun dari subnet dalam VPC tumpang tindih. Oleh karena itu, mereka semua dapat berkomunikasi satu sama lain, di dalam VPC.

Singkatnya, secara default, komunikasi subnet dalam VPC tidak dibatasi. Praktik terbaik untuk mengendalikan komunikasi di antara subnet VPC Anda, jika diperlukan, adalah mengatur daftar kontrol akses dengan aturan yang menentukan arus lalu lintas yang diizinkan. Gunakan grup keamanan untuk mengontrol lalu lintas di antara instans tertentu. Untuk informasi selengkapnya tentang menyiapkan grup keamanan dan firewall di AWS Control Tower, lihat Panduan: Mengatur Grup Keamanan di AWS Control Tower Dengan Firewall Manager AWS.

Mengintip

AWS Control Tower tidak membatasi VPC-to-VPC peering untuk komunikasi di beberapa VPC. Namun, secara default, semua AWS Control Tower VPC memiliki rentang CIDR default yang sama. Untuk mendukung peering, Anda dapat memodifikasi rentang CIDR di pengaturan Account Factory sehingga alamat IP tidak tumpang tindih.

Jika Anda mengubah rentang CIDR di pengaturan Account Factory, semua akun baru yang kemudian dibuat oleh AWS Control Tower (menggunakan Account Factory) ditetapkan rentang CIDR baru. Akun lama tidak diperbarui. Misalnya, Anda dapat membuat akun, lalu mengubah rentang CIDR dan membuat akun baru, dan VPC yang dialokasikan ke kedua akun tersebut dapat diintip. Peering dimungkinkan karena rentang alamat IP mereka tidak identik.

Akses Menara Kontrol AWS menggunakan titik akhir antarmuka (AWS PrivateLink)

Anda dapat menggunakannya AWS PrivateLink untuk membuat koneksi pribadi antara VPC dan AWS Control Tower. Anda dapat mengakses AWS Control Tower seolah-olah berada di VPC Anda, tanpa menggunakan gateway internet, perangkat NAT, koneksi VPN, atau Direct Connect koneksi. Instans di VPC Anda tidak memerlukan alamat IP publik untuk mengakses AWS Control Tower.

Anda membuat koneksi pribadi ini dengan membuat titik akhir antarmuka, didukung oleh AWS PrivateLink. Kami membuat antarmuka jaringan endpoint di setiap subnet yang Anda aktifkan untuk titik akhir antarmuka. Ini adalah antarmuka jaringan yang dikelola permintaan yang berfungsi sebagai titik masuk untuk lalu lintas yang ditujukan untuk Menara Kontrol AWS.

Untuk informasi selengkapnya, lihat Ak AWS PrivateLink ses Layanan AWS melalui dalam AWS PrivateLink Panduan.

Pertimbangan untuk Menara Kontrol AWS

Sebelum Anda menyiapkan titik akhir antarmuka untuk AWS Control Tower, tinjau Per timbangan dalam AWS PrivateLink Panduan.

AWS Control Tower mendukung panggilan ke semua tindakan API-nya melalui titik akhir antarmuka.

Membuat titik akhir antarmuka untuk AWS Control Tower

Anda dapat membuat titik akhir antarmuka untuk AWS Control Tower menggunakan konsol Amazon VPC atau AWS Command Line Interface (AWS CLI). Untuk informasi selengkapnya, lihat Membuat titik akhir antarmuka di AWS PrivateLink Panduan.

Buat titik akhir antarmuka untuk AWS Control Tower menggunakan nama layanan berikut:

```
com.amazonaws.region.controltower
com.amazonaws.region.controltower-fips
```

Jika Anda mengaktifkan DNS pribadi untuk titik akhir antarmuka, Anda dapat membuat permintaan API ke AWS Control Tower menggunakan nama DNS Regional defaultnya. Misalnya, `controltower.us-east-1.amazonaws.com`.

Membuat kebijakan titik akhir untuk titik akhir antarmuka Anda

Kebijakan titik akhir adalah sumber daya IAM yang dapat Anda lampirkan ke titik akhir antarmuka. Kebijakan titik akhir default memungkinkan akses penuh ke AWS Control Tower melalui titik akhir antarmuka. Untuk mengontrol akses yang diizinkan ke AWS Control Tower dari VPC Anda, lampirkan kebijakan titik akhir khusus ke titik akhir antarmuka.

kebijakan titik akhir mencantumkan informasi berikut:

- Prinsipal yang dapat melakukan tindakan (Akun AWS, pengguna IAM, dan peran IAM).
- Tindakan yang dapat dilakukan.
- Sumber daya untuk melakukan tindakan.

Untuk informasi selengkapnya, lihat Mengontrol akses ke layanan menggunakan kebijakan titik akhir di Panduan AWS PrivateLink .

Contoh: Kebijakan titik akhir VPC untuk tindakan AWS Control Tower

Berikut ini adalah contoh kebijakan titik akhir khusus. Saat Anda melampirkan kebijakan ini ke titik akhir antarmuka, kebijakan ini akan memberikan akses ke tindakan AWS Control Tower yang terdaftar untuk semua prinsipal di semua sumber daya.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "controltower:ListEnabledControls",
            "controltower:ListLandingZones"
```

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

> **Note**
>
> Untuk daftar lengkap operasi AWS Control Tower API, lihat Referensi API Menara Kontrol AWS.

Peran dan izin yang diperlukan

AWS Control Tower menggunakan peran IAM untuk membantu mengelola akses ke sumber daya.

Untuk informasi umum tentang peran, lihat Grup pengguna, peran, dan set izin.

Tentang izin

- Untuk informasi tentang grup IAM dan izinnya di AWS Control Tower, lihat grup Pusat Identitas IAM untuk AWS Control Tower.
- Untuk informasi tentang izin yang diperlukan untuk menyediakan akun, lihat Izin yang diperlukan untuk akun.
- Untuk informasi tentang izin konsol yang diperlukan untuk AWS Control Tower, lihat Izin yang diperlukan untuk menggunakan konsol AWS Control Tower.

Tentang peran

- Untuk informasi tentang cara membuat peran, termasuk izin yang dirancang untuk akses terprogram, lihat Membuat peran dan menetapkan izin, serta peran terprogram dan hubungan kepercayaan untuk akun audit AWS Control Tower.
- Untuk informasi tentang peran lain yang digunakan AWS Control Tower untuk mengelola akun Anda, lihat Menggunakan kebijakan berbasis identitas (kebijakan IAM) untuk AWS Control Tower, dan kebijakan Terkelola untuk AWS Control Tower.
- Untuk informasi tentang AWS Control Tower dan AWS Config peran, lihat AWS Control Tower ConfigRecorderRole.
- Untuk informasi tentang peran yang digunakan AWS Control Tower untuk mengumpulkan AWS Config informasi akun Anda, lihat Cara AWS Control Tower menggabungkan AWS Config aturan di OU dan akun yang tidak dikelola.
- Untuk informasi tentang cara melindungi sumber daya saat menetapkan peran dan izin, lihat Ketentuan opsional untuk hubungan kepercayaan peran Anda, Mengkonfigurasi AWS KMS kunci secara opsional, dan Mencegah peniruan identitas lintas layanan.
- Untuk informasi spesifik tentang penyediaan akun otomatis di AWS Control Tower dengan peran IAM, lihat Penyediaan Akun Otomatis dengan Peran IAM.
- Untuk melihat kebijakan yang melindungi topik AWS Config SNS, lihat Kebijakan topik AWS Config SNS.

Cara AWS Control Tower bekerja dengan peran untuk membuat dan mengelola akun

Secara umum, peran adalah bagian dari identitas dan manajemen akses (IAM) di AWS. Untuk informasi umum tentang IAM dan peran dalam AWS, lihat topik peran IAM di Panduan Pengguna AWS IAM.

Peran dan pembuatan akun

AWS Control Tower membuat akun pelanggan dengan memanggil `CreateAccount` API AWS Organizations. Saat AWS Organizations membuat akun ini, akun ini akan menciptakan peran dalam akun tersebut, yang diberi nama AWS Control Tower dengan meneruskan parameter ke API. Nama perannya adalah`AWSControlTowerExecution`.

AWS Control Tower mengambil alih `AWSControlTowerExecution` peran untuk semua akun yang dibuat oleh Account Factory. Dengan menggunakan peran ini, AWS Control Tower memberi dasar pada akun dan menerapkan kontrol wajib (dan lainnya yang diaktifkan), yang menghasilkan pembuatan peran lain. Peran ini pada gilirannya digunakan oleh layanan lain, seperti AWS Config.

> **Note**
>
> Untuk mendasarkan akun berarti menyiapkan sumber dayanya, yang mencakup template Account Factory, kadang-kadang disebut sebagai cetak biru, dan kontrol. Proses baselining juga mengatur pencatatan terpusat dan peran audit keamanan pada akun, sebagai bagian dari penerapan templat. Garis dasar AWS Control Tower terdapat dalam peran yang Anda terapkan pada setiap akun yang terdaftar.

Untuk informasi selengkapnya tentang akun dan sumber daya, lihatTentang Akun AWS di AWS Control Tower.

AWSControlTowerExecution Peran tersebut, dijelaskan

`AWSControlTowerExecution`Peran harus ada di semua akun yang terdaftar. Ini memungkinkan AWS Control Tower untuk mengelola akun individual Anda dan melaporkan informasi tentangnya ke akun Audit dan Arsip Log Anda.

`AWSControlTowerExecution`Peran tersebut dapat ditambahkan ke akun dengan beberapa cara, sebagai berikut:

- Untuk akun di Security OU (terkadang disebut akun inti), AWS Control Tower menciptakan peran pada saat penyiapan AWS Control Tower awal.
- Untuk akun Account Factory yang dibuat melalui konsol AWS Control Tower, AWS Control Tower membuat peran ini pada saat pembuatan akun.
- Untuk pendaftaran satu akun, kami meminta pelanggan untuk membuat peran secara manual dan kemudian mendaftarkan akun di AWS Control Tower.
- Saat memperluas tata kelola ke OU, AWS Control Tower menggunakan StackSet-AWSControlTowerExecutionRoleuntuk membuat peran di semua akun di OU tersebut.

> **Note**
>
> Saat Anda membatalkan pendaftaran akun, AWS Control Tower menghapus `AWSControlTowerExecution` peran tersebut, tidak peduli apakah itu dibuat secara manual atau oleh AWS Control Tower itu sendiri.

Tujuan `AWSControlTowerExecution` peran:

- `AWSControlTowerExecution`memungkinkan Anda membuat dan mendaftarkan akun, secara otomatis, dengan skrip dan fungsi Lambda.
- `AWSControlTowerExecution`membantu Anda mengonfigurasi pencatatan organisasi Anda, sehingga semua log untuk setiap akun dikirim ke akun logging.
- `AWSControlTowerExecution`memungkinkan Anda mendaftarkan akun individual di AWS Control Tower. Pertama, Anda harus menambahkan `AWSControlTowerExecution` peran ke akun itu. Untuk langkah-langkah tentang cara menambahkan peran, lihatMenambahkan peran IAM yang diperlukan secara manual ke yang sudah ada Akun AWS dan mendaftarkannya.

Bagaimana `AWSControlTowerExecution` peran bekerja dengan OU:

`AWSControlTowerExecution`Peran ini memastikan bahwa kontrol AWS Control Tower yang Anda pilih berlaku secara otomatis ke setiap akun individual, di setiap OU, di organisasi Anda, serta setiap akun baru yang Anda buat di AWS Control Tower. Hasilnya:

- Anda dapat memberikan laporan kepatuhan dan keamanan dengan lebih mudah, berdasarkan fitur audit dan pencatatan yang diwujudkan oleh kontrol AWS Control Tower.

- Tim keamanan dan kepatuhan Anda dapat memverifikasi bahwa semua persyaratan terpenuhi, dan tidak ada penyimpangan organisasi yang terjadi.

Untuk informasi selengkapnya tentang drift, lihat Mendeteksi dan menyelesaikan drift di AWS Control Tower.

Untuk meringkas, `AWSControlTowerExecution` peran dan kebijakan terkait memberi Anda kontrol keamanan dan kepatuhan yang fleksibel di seluruh organisasi Anda. Oleh karena itu, pelanggaran keamanan atau protokol lebih kecil kemungkinannya terjadi.

Kondisi opsional untuk hubungan kepercayaan peran Anda

Untuk menambahkan lapisan keamanan tambahan ke lingkungan AWS Control Tower, Anda dapat menerapkan ketentuan dalam kebijakan kepercayaan peran Anda, untuk membatasi akun dan sumber daya yang berinteraksi dengan peran tertentu di AWS Control Tower. Misalnya, Anda dapat membatasi akses ke `AWSControlTowerAdmin` peran lebih lanjut, karena memungkinkan izin akses yang luas.

Untuk membantu mencegah pelaku ancaman mendapatkan akses ke sumber daya Anda, edit kebijakan kepercayaan AWS Control Tower Anda secara manual untuk menambahkan setidaknya satu `aws:SourceArn` atau `aws:SourceAccount` bersyarat pada pernyataan kebijakan. Sebagai praktik terbaik keamanan tambahan, Anda dapat menambahkan `aws:SourceArn` kondisi, karena lebih spesifik daripada`aws:SourceAccount`, membatasi akses ke akun tertentu dan sumber daya tertentu.

Jika Anda tidak mengetahui ARN lengkap sumber daya, atau jika Anda menentukan beberapa sumber daya, Anda dapat menggunakan `aws:SourceArn` kondisi dengan wildcard (*) untuk bagian ARN yang tidak diketahui. Misalnya, `arn:aws:controltower:*:123456789012:*` berfungsi jika Anda tidak ingin menentukan Wilayah.

Contoh berikut menunjukkan penggunaan kondisi `aws:SourceArn` IAM dengan kebijakan kepercayaan peran IAM Anda. Tambahkan kondisi dalam hubungan kepercayaan Anda untuk AWSControlTowerAdminperan tersebut, karena prinsipal layanan AWS Control Tower berinteraksi dengannya.

Seperti yang ditunjukkan pada contoh, sumber ARN adalah format:
`arn:aws:controltower:${HOME_REGION}:${CUSTOMER_AWSACCOUNT_id}:*`

Ganti string `${HOME_REGION}` dan `${CUSTOMER_AWSACCOUNT_id}` dengan wilayah rumah Anda sendiri dan ID akun dari akun panggilan.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:controltower:us-west-2:012345678901:*"
        }
      }
    }
  ]
}
```

Dalam contoh, Sumber ARN ditunjuk sebagai satu-satunya `arn:aws:controltower:us-west-2:012345678901:*` ARN yang diizinkan untuk melakukan tindakan. `sts:AssumeRole` Dengan kata lain, hanya pengguna yang dapat masuk ke ID akun`012345678901`, di `us-west-2` Wilayah, yang diizinkan untuk melakukan tindakan yang memerlukan peran dan hubungan kepercayaan khusus ini untuk layanan AWS Control Tower, yang ditetapkan sebagai`controltower.amazonaws.com`.

Contoh berikutnya menunjukkan `aws:SourceAccount` dan `aws:SourceArn` kondisi yang diterapkan pada kebijakan kepercayaan peran.

JSON

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

```
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "012345678901"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:controltower:us-west-2:012345678901:*"
        }
      }
    }
  ]
}
```

Contoh menggambarkan pernyataan `aws:SourceArn` kondisi, dengan pernyataan `aws:SourceAccount` kondisi tambahan. Untuk informasi selengkapnya, lihat Mencegah peniruan lintas layanan.

Untuk informasi umum tentang kebijakan izin di AWS Control Tower, lihatKelola akses ke sumber daya.

Rekomendasi:

Kami menyarankan Anda menambahkan kondisi ke peran yang dibuat AWS Control Tower, karena peran tersebut secara langsung diasumsikan oleh layanan AWS lainnya. Untuk informasi selengkapnya, lihat contoh untuk AWSControlTowerAdmin, yang ditunjukkan sebelumnya di bagian ini. Untuk peran AWS Config perekam, kami sarankan menambahkan `aws:SourceArn` kondisi, menentukan ARN perekam Config sebagai ARN sumber yang diizinkan.

Untuk peran seperti AWSControlTowerExecutionatau peran terprogram lainnya yang dapat diasumsikan oleh akun AWS Control Tower Audit di semua akun terkelola, kami sarankan Anda menambahkan `aws:PrincipalOrgID` kondisi ke kebijakan kepercayaan untuk peran ini, yang memvalidasi bahwa prinsipal yang mengakses sumber daya milik akun di organisasi yang benar.

AWS Jangan tambahkan pernyataan `aws:SourceArn` kondisi, karena tidak akan berfungsi seperti yang diharapkan.

> **Note**
>
> Dalam kasus drift, ada kemungkinan bahwa peran AWS Control Tower dapat diatur ulang dalam keadaan tertentu. Disarankan agar Anda memeriksa kembali peran secara berkala, jika Anda telah menyesuaikannya.

Bagaimana AWS Control Tower digabungkan AWS Config aturan di OU dan akun yang tidak dikelola

- Akun manajemen AWS Control Tower membuat agregator tingkat organisasi, yang membantu mendeteksi AWS Config aturan eksternal, sehingga AWS Control Tower tidak perlu mendapatkan akses ke akun yang tidak dikelola. Konsol AWS Control Tower menunjukkan kepada Anda berapa banyak AWS Config aturan yang dibuat secara eksternal yang Anda miliki untuk akun tertentu. Anda dapat melihat detail tentang aturan eksternal tersebut di tab Kepatuhan Aturan Konfigurasi Eksternal di halaman Detail Akun.
- Untuk membuat agregator, AWS Control Tower menambahkan peran dengan izin yang diperlukan untuk mendeskripsikan organisasi dan membuat daftar akun di bawahnya. `AWSControlTowerConfigAggregatorRoleForOrganizations`Peran tersebut membutuhkan kebijakan yang `AWSConfigRoleForOrganizations` dikelola dan hubungan kepercayaan dengan`config.amazonaws.com`.

> **Note**
>
> Pelanggan yang menggunakan landing zone versi 4.0 tidak memerlukan peran ini karena AWS Control Tower telah bermigrasi dari agregator konfigurasi tingkat organisasi yang ada ke agregator konfigurasi terkait layanan

> **Note**
>
> Saat Anda mengaktifkan akses tepercaya pada organisasi yang berisi landing zone Anda, AWS Control Tower dapat membuat peran, mengelola sumber daya, dan membaca data

untuk semua akun di organisasi. Melalui akses tepercaya, akun atau OU apa pun di organisasi tersedia untuk AWS Control Tower, baik terdaftar maupun terdaftar, atau tidak terdaftar dan tidak terdaftar.

Berikut adalah kebijakan IAM (artefak JSON) yang melekat pada peran:

JSON

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

Inilah hubungan `AWSControlTowerConfigAggregatorRoleForOrganizations` kepercayaannya:

```
{
    "Version": "2012-10-17",
      "Statement": [
      {
        "Effect": "Allow",
        "Principal": {
        "Service": "config.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
      }
    ]
  }
}
```

Untuk menerapkan fungsionalitas ini di akun manajemen, izin berikut ditambahkan dalam kebijakan terkelolaAWSControlTowerServiceRolePolicy, yang digunakan oleh AWSControlTowerAdmin peran saat membuat agregator: AWS Config

JSON

```
{
  "Version":"2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "config:PutConfigurationAggregator",
          "config:DeleteConfigurationAggregator",
          "iam:PassRole"
          ],
        "Resource": [
          "arn:aws:iam::123456789012:role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations",
          "arn:aws:config:us-east-1:123456789012:config-aggregator/"
          ]
        },
      {
        "Effect": "Allow",
        "Action": "organizations:EnableAWSServiceAccess",
        "Resource": "*"
      }
    ]
}
```

Sumber daya baru dibuat: AWSControlTowerConfigAggregatorRoleForOrganizations dan aws-controltower-ConfigAggregatorForOrganizations

Ketika Anda siap, Anda dapat mendaftarkan akun satu per satu, atau mendaftarkannya sebagai grup dengan mendaftarkan OU. Ketika Anda telah mendaftarkan akun, jika Anda membuat aturan AWS Config, AWS Control Tower mendeteksi aturan baru. Agregator menunjukkan jumlah aturan eksternal dan menyediakan tautan ke AWS Config konsol tempat Anda dapat melihat detail setiap aturan eksternal untuk akun Anda. Gunakan informasi di AWS Config konsol dan konsol AWS Control Tower untuk menentukan apakah Anda mengaktifkan kontrol yang sesuai untuk akun tersebut.

Peran terprogram dan hubungan kepercayaan untuk akun audit AWS Control Tower

Anda dapat masuk ke akun audit dan berperan untuk meninjau akun lain secara terprogram. Akun audit tidak memungkinkan Anda untuk masuk ke akun lain secara manual.

Akun audit memberi Anda akses terprogram ke akun lain, melalui beberapa peran yang diberikan hanya untuk fungsi AWS Lambda. Untuk tujuan keamanan, peran ini memiliki hubungan kepercayaan dengan peran lain, yang berarti bahwa kondisi di mana peran dapat digunakan didefinisikan secara ketat.

Tumpukan AWS Control Tower `StackSet-AWSControlTowerBP-BASELINE-ROLES` membuat peran IAM lintas akun khusus program ini di setiap akun terkelola, termasuk akun agregator Config (sebelumnya akun audit). Akun agregator Config mengasumsikan peran eksekusi ini untuk mengakses akun lain secara terprogram:

- aws-menara pengendali- AdministratorExecutionRole
- aws-menara pengendali- ReadOnlyExecutionRole

Tumpukan AWS Control Tower `StackSet-AWSControlTowerSecurityResources` membuat peran IAM lintas akun khusus program ini di akun audit:

- aws-menara pengendali- AuditAdministratorRole
- aws-menara pengendali- AuditReadOnlyRole

`ReadOnlyExecutionRole:`Perhatikan bahwa peran ini memungkinkan akun audit membaca objek di bucket Amazon S3 di seluruh organisasi (berbeda dengan `SecurityAudit` kebijakan, yang hanya mengizinkan akses metadata).

aws-controltower-: AdministratorExecutionRole

- Memiliki izin administrator
- Tidak dapat diasumsikan dari konsol
- Dapat diasumsikan hanya dengan peran dalam akun audit - `aws-controltower-AuditAdministratorRole`

Artefak berikut menunjukkan hubungan kepercayaan untuk`aws-controltower-AdministratorExecutionRole`. Nomor placeholder `012345678901` akan diganti dengan `Audit_acct_ID` nomor untuk akun audit Anda.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/aws-controltower-AuditAdministratorRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

aws-controltower-: AuditAdministratorRole

- Dapat diasumsikan oleh layanan AWS Lambda saja
- Memiliki izin untuk melakukan operasi baca (Dapatkan) dan tulis (Put) pada objek Amazon S3 dengan nama yang dimulai dengan log string

Kebijakan terlampir:

1. AWSLambdaExecute— kebijakan AWS terkelola

2. AssumeRole-aws-controltower-AuditAdministratorRole— kebijakan inline — Dibuat oleh AWS Control Tower, artefak mengikuti.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
 {
 "Action": [
   "sts:AssumeRole"
   ],
 "Resource": [
```

```
    "arn:aws:iam::*:role/aws-controltower-AdministratorExecutionRole"
    ],
  "Effect": "Allow"
  }
    ]
}
```

Artefak berikut menunjukkan hubungan kepercayaan untuk`aws-controltower-AuditAdministratorRole`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

aws-controltower-: ReadOnlyExecutionRole

- Tidak dapat diasumsikan dari konsol
- Dapat diasumsikan hanya dengan peran lain dalam akun audit - `AuditReadOnlyRole`

Artefak berikut menunjukkan hubungan kepercayaan untuk`aws-controltower-ReadOnlyExecutionRole`. Nomor placeholder `012345678901` akan diganti dengan `Audit_acct_ID` nomor untuk akun audit Anda.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/aws-controltower-AuditReadOnlyRole "
      },
```

```
      "Action": "sts:AssumeRole"
    }
  ]
}
```

aws-controltower-: AuditReadOnlyRole

- Dapat diasumsikan oleh layanan AWS Lambda saja
- Memiliki izin untuk melakukan operasi baca (Dapatkan) dan tulis (Put) pada objek Amazon S3 dengan nama yang dimulai dengan log string

Kebijakan terlampir:

1. AWSLambdaExecute— kebijakan AWS terkelola

2. AssumeRole-aws-controltower-AuditReadOnlyRole— kebijakan inline — Dibuat oleh AWS Control Tower, artefak mengikuti.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
 {
 "Action": [
  "sts:AssumeRole"
 ],
 "Resource": [
  "arn:aws:iam::*:role/aws-controltower-ReadOnlyExecutionRole"
 ],
 "Effect": "Allow"
   }
  ]
}
```

Artefak berikut menunjukkan hubungan kepercayaan untuk`aws-controltower-AuditReadOnlyRole`:

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "lambda.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Penyediaan Akun Otomatis Dengan Peran IAM

Untuk mengonfigurasi akun Account Factory dengan cara yang lebih otomatis, Anda dapat membuat fungsi Lambda di akun manajemen AWS Control Tower, yang mengambil AWSControlTowerExecutionperan dalam akun anggota. Kemudian, dengan menggunakan peran tersebut, akun manajemen melakukan langkah-langkah konfigurasi yang diinginkan di setiap akun anggota.

Jika Anda menyediakan akun menggunakan fungsi Lambda, identitas yang akan melakukan pekerjaan ini harus memiliki kebijakan izin IAM berikut, sebagai tambahan. `AWSServiceCatalogEndUserFullAccess`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSControlTowerAccountFactoryAccess",
            "Effect": "Allow",
            "Action": [
                "sso:GetProfile",
                "sso:CreateProfile",
                "sso:UpdateProfile",
                "sso:AssociateProfile",
                "sso:CreateApplicationInstance",
                "sso:GetSSOStatus",
                "sso:GetTrust",
                "sso:CreateTrust",
                "sso:UpdateTrust",
                "sso:GetApplicationInstance",
                "sso:ListDirectoryAssociations",
```

```
                "sso:ListPermissionSets",
                "sso:GetPermissionSet",
                "sso:ListProfileAssociations",
                "sso-directory:ListMembersInGroup",
                "sso-directory:AddMemberToGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchUsers",
                "sso-directory:CreateUser",
                "sso-directory:DescribeGroups",
                "sso-directory:DescribeDirectory",
                "sso-directory:GetUserPoolInfo",
                "controltower:CreateManagedAccount",
                "controltower:DescribeManagedAccount",
                "controltower:DeregisterManagedAccount",
                "s3:GetObject",
                "organizations:describeOrganization",
                "sso:DescribeRegisteredRegions"
            ],
            "Resource": "*"
        }
    ]
}
```

Sumber daya di AWS Control Tower

- Untuk informasi umum tentang kepemilikan sumber daya di AWS Control Tower, lihatIkhtisar pengelolaan izin akses ke sumber daya AWS Control Tower.
- Untuk informasi tentang sumber daya yang dibuat AWS Control Tower di akun bersama, lihatAkun integrasi layanan.
- Untuk informasi tentang sumber daya yang dibuat AWS Control Tower saat menyediakan akun melalui Account Factory, lihatPertimbangan Sumber Daya untuk Pabrik Akun.
- Untuk melihat detail tentang jenis AWS sumber daya yang ditentukan oleh AWS Control Tower, untuk digunakan dengan AWS Control Tower API, lihat referensi jenis sumber daya AWS Control Tower di Panduan AWS CloudFormation Pengguna.

Bagaimana AWS Wilayah Bekerja Dengan AWS Control Tower

AWS Control Tower didukung di Wil AWS ayah berikut:

- Timur AS (N. Virginia)
- AS Timur (Ohio)
- AS Barat (Oregon)
- Kanada (Pusat)
- Asia Pasifik (Sydney)
- Asia Pasifik (Singapura)
- Eropa (Frankfurt)
- Eropa (Irlandia)
- Europe (London)
- Eropa (Stockholm)
- Asia Pasifik (Mumbai)
- Asia Pasifik (Seoul)
- Asia Pasifik (Tokyo)
- Eropa (Paris)
- Amerika Selatan (São Paulo)
- AS Barat (California Utara)
- Asia Pasifik (Hong Kong)
- Asia Pasifik (Jakarta)
- Asia Pasifik (Osaka)
- Europe (Milan)
- Africa (Cape Town)
- Timur Tengah (Bahrain)
- Israel (Tel Aviv)
- Timur Tengah (UAE)
- Eropa (Spanyol)

- Asia Pasifik (Hyderabad)
- Europe (Zurich)
- Asia Pacific (Melbourne)
- Kanada Barat (Calgary)
- Malaysia (Kuala Lumpur)
- Asia Pasifik (Thailand)
- Meksiko (Tengah)
- Asia Pasifik (Taipei)

Tentang Daerah rumah Anda

Saat Anda membuat zona pendaratan, Wilayah yang Anda gunakan untuk akses ke konsol AWS Manajemen menjadi Wil AWS ayah rumah Anda untuk Menara Kontrol AWS. Selama proses pembuatan, beberapa sumber daya disediakan di Wilayah rumah. Sumber daya lain, seperti OU dan AWS akun, bersifat global.

Setelah Anda memilih Wilayah beranda, Anda tidak dapat mengubahnya.

Kontrol dan Wilayah

Saat ini, semua kontrol pencegahan bekerja secara global. Kontrol detektif dan proaktif, bagaimanapun, hanya berfungsi di Wilayah di mana AWS Control Tower didukung. Untuk informasi selengkapnya tentang perilaku kontrol saat Anda mengaktifkan AWS Control Tower di Wilayah baru, lihatKonfigurasikan Wilayah Menara Kontrol AWS Anda.

Konfigurasikan Wilayah Menara Kontrol AWS Anda

Bagian ini menjelaskan perilaku yang dapat Anda harapkan saat memperluas zona pendaratan AWS Control Tower ke Wil AWS ayah baru, atau menghapus Wilayah dari konfigurasi zona pendaratan Anda. Umumnya, tindakan ini dilakukan melalui fungsi Pem baruan konsol AWS Control Tower.

> **Note**
>
> Sebaiknya hindari memperluas zona pendaratan AWS Control Tower ke Wil AWS ayah di mana Anda tidak memerlukan beban kerja untuk dijalankan. Memilih keluar dari Wilayah tidak mencegah Anda menerapkan sumber daya di Wilayah tersebut, tetapi sumber daya tersebut akan tetap berada di luar tata kelola AWS Control Tower.

Selama konfigurasi Wilayah baru, AWS Control Tower memperbarui zona pendaratan, yang berarti zona pen daratan dasar Anda —

- untuk beroperasi secara aktif di semua Wilayah yang baru dipilih, dan
- untuk berhenti mengatur sumber daya di Daerah yang tidak dipilih.

Akun individu dalam unit organisasi (OU) Anda yang dikelola oleh AWS Control Tower tidak diperbarui sebagai bagian dari proses pembaruan zona pendaratan ini. Oleh karena itu, Anda harus memperbarui akun Anda dengan mendaftarkan ulang OU Anda.

Saat mengonfigurasi Wilayah Menara Kontrol AWS Anda, perhatikan rekomendasi dan batasan berikut:

- Pilih Wilayah tempat Anda berencana untuk meng-host AWS sumber daya atau beban kerja.
- Memilih keluar dari Wilayah tidak mencegah Anda menerapkan sumber daya di Wilayah tersebut, tetapi sumber daya tersebut akan tetap berada di luar tata kelola AWS Control Tower.

Saat mengonfigurasi zona pendaratan untuk Wilayah baru, kontrol detektif AWS Control Tower mematuhi aturan berikut:

- Apa yang ada tetap sama. Perilaku kontrol, detektif maupun preventif, tidak berubah untuk akun yang ada, di OU yang ada, di Wilayah yang ada.
- Anda tidak dapat menerapkan kontrol detektif baru ke OU yang ada yang berisi akun yang tidak diperbarui. Setelah mengonfigurasi zona pendaratan AWS Control Tower ke Wilayah baru (dengan memperbarui zona pendaratan), Anda harus memperbarui akun yang ada di OU yang ada sebelum Anda dapat mengaktifkan kontrol detektif baru pada OU dan akun tersebut.
- Kontrol detektif Anda yang ada mulai bekerja di Wilayah yang baru dikonfigurasi segera setelah Anda memperbarui akun. Saat Anda memperbarui zona pendaratan AWS Control Tower untuk mengonfigurasi Wilayah baru dan kemudian memperbarui akun, kontrol detektif yang sudah diaktifkan pada OU akan mulai bekerja pada akun tersebut di Wilayah yang baru dikonfigurasi.

Konfigurasikan Wilayah Menara Kontrol AWS

1. Masuk ke konsol AWS Control Tower di https://console.aws.amazon.com/controltower
2. Di menu navigasi panel kiri, pilih Pengaturan zona pendaratan.

3. Pada halaman pengaturan zona pendaratan, di bagian Detail, pilih tombol Ubah pengaturan di kanan atas. Anda diarahkan ke alur kerja zona pendaratan pembaruan.
4. Di bawah Wilayah yang diatur Tambahan, cari Wilayah yang ingin Anda atur (atau berhenti mengatur).
5. Pilih kotak centang untuk setiap Wilayah tambahan yang akan diatur. Hapus centang kotak untuk setiap Wilayah tempat Anda menghapus tata kelola.

> **Note**
>
> Jika Anda memilih untuk tidak mengatur Wilayah, Anda masih dapat menerapkan sumber daya di Wilayah tersebut, tetapi sumber daya tersebut akan tetap berada di luar tata kelola AWS Control Tower.

6. Selesaikan sisa alur kerja, lalu pilih Per barui zona pendaratan.
7. Ketika pengaturan zona pendaratan selesai, Re-register OU akan memperbarui akun di Wilayah baru Anda. Untuk informasi selengkapnya, lihat Kapan harus memperbarui AWS Control Tower OU dan akun.

Metode alternatif penyediaan atau memperbarui akun individual setelah mengonfigurasi Wilayah baru adalah dengan menggunakan kerangka API Katalog Layanan dan AWS CLI untuk memperbarui akun dalam proses batch. Untuk informasi selengkapnya, lihat Menyediakan dan memperbarui akun menggunakan otomatisasi.

Hindari tata kelola campuran saat mengonfigurasi Wilayah

Penting untuk memperbarui semua akun di OU setelah Anda memperluas tata kelola AWS Control Tower ke yang baru Wilayah AWS, dan setelah Anda menghapus tata kelola AWS Control Tower dari Wilayah.

Tata kelola campuran adalah situasi yang tidak diinginkan yang dapat terjadi jika kontrol yang mengatur OU tidak sepenuhnya cocok dengan kontrol yang mengatur setiap akun dalam OU. Tata kelola campuran terjadi di OU jika akun tidak diperbarui setelah AWS Control Tower memperluas tata kelola ke tata kelola baru Wilayah AWS, atau menghapus tata kelola.

Dalam situasi ini, akun tertentu dalam OU mungkin memiliki kontrol yang berbeda yang diterapkan di Wilayah yang berbeda, jika dibandingkan dengan akun lain di OU, atau bila dibandingkan dengan postur tata kelola zona pendaratan secara keseluruhan.

Dalam OU dengan tata kelola campuran, jika Anda menyediakan akun baru, akun baru tersebut menerima postur tata kelola Wilayah dan OU yang sama (diperbarui) sebagai zona pendaratan. Namun, akun yang ada yang belum diperbarui tidak menerima postur tata kelola Wilayah yang diperbarui.

Secara umum, tata kelola campuran dapat menciptakan indikator status yang kontradiktif atau tidak akurat di konsol AWS Control Tower. Misalnya, selama tata kelola campuran, Wilayah pilihan ditampilkan dengan status Tidak diatur, di OU terdaftar, untuk akun yang belum diperbarui.

> **Note**
>
> AWS Control Tower tidak mengizinkan kontrol diaktifkan selama keadaan tata kelola campuran.

Perilaku kontrol selama tata kelola campuran

- Selama tata kelola campuran, AWS Control Tower tidak dapat secara konsisten menerapkan kontrol yang didasarkan pada AWS Config aturan (yaitu, kontrol detektif) di Wilayah yang OU sudah ditampilkan sebagai Diatur, karena beberapa akun di OU belum diperbarui. Anda mungkin menerima pesan `FAILED_TO_ENABLE` kesalahan.
- Selama tata kelola campuran, jika Anda memperluas tata kelola zona pendaratan ke Wilayah opt-in sementara akun apa pun di OU belum diperbarui, operasi `EnableControl` API pada OU gagal untuk kontrol detektif dan proaktif. Anda akan menerima pesan `FAILED_TO_ENABLE` kesalahan, karena akun anggota yang tidak diperbarui dalam OU belum dipilih ke Wilayah tersebut.
- Selama tata kelola campuran, kontrol yang merupakan bagian dari Service-managed Standar CSPM Hub Keamanan: Menara Kontrol AWS tidak dapat melaporkan kepatuhan secara akurat di Wilayah di mana terdapat ketidakcocokan antara konfigurasi zona pendaratan dan akun yang tidak diperbarui.
- Tata kelola campuran tidak mengubah perilaku SCP-based kontrol (kontrol preventif), yang berlaku secara seragam untuk setiap akun di OU, di setiap Wilayah yang diatur.

> **Note**
>
> Tata kelola campuran tidak sama dengan drift, dan tidak dilaporkan sebagai drift.

Untuk memperbaiki tata kelola campuran

- Pelanggan sekarang dapat memperbaiki tata kelola campuran dengan mengatur ulang kontrol regional. Setiap kontrol non-global bersifat regional (kontrol detektif dan proaktif). Anda akan diberitahu bahwa OU Anda berada dalam tata kelola campuran melalui spanduk peringatan.

Pertimbangan untuk mengaktifkan AWS Wilayah opt-in

Meskipun sebagian besar aktif Wilayah AWS secara default untuk Anda Akun AWS, Wilayah tertentu diaktifkan hanya ketika Anda memilihnya secara manual. Dokumen ini mengacu pada Wilayah tersebut sebagai Wilayah pilihan. Sebaliknya, Wilayah yang aktif secara default, segera setelah Anda Akun AWS dibuat, disebut sebagai Wilayah komersial, Wilayah default , atau hanya, Wil ayah.

Istilah opt-in memiliki dasar historis. Semua Wilayah AWS yang diperkenalkan setelah 20 Maret 2019 digunakan sebagai Wilayah opt-in. Di Wilayah pilihan, akun Anda tidak diaktifkan di Wilayah tersebut—dan identitas Anda tidak direplikasi ke Wilayah tersebut—kecuali jika Anda memilih untuk memilih untuk menggunakan Wilayah tersebut. Semua data yang dikelola melalui layanan IAM dianggap sebagai data identitas, termasuk pengguna, grup, peran, kebijakan, penyedia identitas, data terkait mereka (misalnya, sertifikat X.509 penandatanganan atau kredentif spesifik konteks), dan pengaturan tingkat akun lainnya, seperti kebijakan kata sandi dan alias akun.

Anda dapat mengaktifkan Wilayah opt-in secara otomatis selama pengaturan zona pendaratan, dengan memilihnya. Zona pendaratan Anda menjadi aktif di semua Wilayah yang dipilih.

Jika Anda memilih untuk memilih Wilayah pilihan sebagai Wilayah rumah AWS Control Tower, aktifkan terlebih dahulu dengan mengikuti langkah-langkah di Mengaktifkan Wilayah, saat masuk ke Konsol AWS Manajemen. Untuk membawa Arsip Log dan akun Audit Anda sendiri yang ada dari Wilayah opt-in, aktifkan Wilayah tersebut secara manual terlebih dahulu.

Wil AWS ayah opt-in mencakup beberapa Wilayah di mana AWS Control Tower tersedia:

- Wilayah Asia Pasifik (Hong Kong), ap-east-1
- Wilayah Asia Pasifik (Jakarta), ap-southeast-3
- Wilayah Eropa (Milan), eu-selatan-1
- Wilayah Afrika (Cape Town), af-south-1
- Wilayah Timur Tengah (Bahrain), me-south-1

- Israel (Tel Aviv), sentral-1
- Wilayah Timur Tengah (UEA), me-central-1
- Wilayah Eropa (Spanyol), eu-south-2
- Wilayah Asia Pasifik (Hyderabad), ap-south-2
- Wilayah Eropa (Zurich), eu-central-2
- Wilayah Asia Pasifik (Melbourne), ap-Southeast-4
- Kanada Wilayah Barat (Calgary), ca-west-1
- Asia Pasifik (Thailand), ap-southeast-7
- Meksiko (Tengah), mx-central-1
- Asia Pasifik (Taipei), ap-east-2
- Asia Pasifik (Selandia Baru), ap-southeast-6

AWS Control Tower memiliki beberapa kontrol yang bekerja secara berbeda di Wilayah opt-in dibandingkan di Wilayah default (Wilayah komersial lainnya). Untuk informasi selengkapnya, lihat Batasan kontrol. Berikut adalah beberapa pertimbangan yang perlu diingat saat Anda menerapkan beban kerja ke Wilayah opt-in.

> **Mengatur atau mengaktifkan?**
>
> Ingatlah bahwa mengatur Wilayah adalah tindakan yang dapat Anda pilih dari konsol AWS Control Tower, sehingga kontrol dapat diterapkan di Wilayah. Mengaktifkan atau menonaktifkan Wilayah pilihan adalah tindakan berbeda yang dapat Anda pilih di AWS konsol, yang membuka Wilayah ke akun Anda, sehingga Anda dapat menyebarkan sumber daya dan beban kerja di Wilayah.

Pertimbangan perilaku

- Jika Anda memilih untuk mengatur Wilayah pilihan, kami sarankan Anda tidak menonaktifkan (memilih keluar dari) Wilayah pilihan yang diatur Anda, karena hal itu dapat menyebabkan kegagalan beban kerja Anda. AWS Control Tower tidak mengizinkan penonaktifan Wilayah yang diatur dari dalam konsol AWS Control Tower, tetapi pastikan Anda tidak menonaktifkan Wilayah yang diatur dari sumber di luar AWS Control Tower, seperti konsol Pen AWS agihan atau AWS SDK.

- Saat AWS Control Tower memperluas tata kelola ke Wilayah pilihan, AWS akan mengaktifkan (opts-in) ke Wilayah di semua akun anggota. Saat Anda menghapus Wilayah dari tata kelola, AWS Control Tower tidak menonaktifkan (memilih keluar dari) Wilayah di akun anggota.
- Selama penghentian Wilayah, AWS Control Tower melewatkan penghapusan sumber daya dari Wilayah pilihan jika Wilayah tersebut dinonaktifkan secara manual untuk akun dari sumber di luar AWS Control Tower, seperti konsol Penagihan atau SDK. AWS AWS Sebaiknya hapus sumber daya dari Wilayah yang telah dinonaktifkan, atau Anda mungkin menerima biaya penagihan tak terduga untuk sumber daya tersebut.
- Jika zona pendaratan Anda dinonaktifkan, AWS Control Tower membersihkan sumber daya di semua Wilayah yang diatur, termasuk Wilayah pilihan. Namun, AWS Control Tower tidak menonaktifkan Wilayah opt-in. Anda dapat menonaktifkan Wilayah opt-in sebagai langkah tambahan setelah penonaktifan.
- Jika Wilayah asal Anda adalah Wilayah pilihan, dan jika Anda bermaksud mendaftarkan akun yang ada sebagai akun Arsip Log dan Audit, Anda harus mengaktifkan Wilayah pilihan secara manual sebelum Anda dapat memilihnya sebagai Wilayah asal untuk zona pendaratan Anda. Lihat Mengaktifkan Wilayah.
- Jika AWS Control Tower diatur dengan Wilayah opt-in sebagai Wilayah asal Anda, dan jika Anda mengunjungi layanan Menara Kontrol AWS dari AWS konsol di Wilayah lain, konsol tidak mengarahkan Anda secara otomatis ke Wilayah asal.
- API yang mendasarinya memiliki batas kapasitas, yang dapat meningkatkan latensi dari beberapa menit menjadi beberapa jam, tergantung pada jumlah Wilayah, akun, dan beban layanan. Sebagai praktik terbaik, ikut serta hanya untuk mereka di Wilayah AWS mana Anda akan menjalankan beban kerja, dan ikut serta dalam satu Wilayah pada satu waktu.

Batasan penting untuk tata kelola dan akun

- Jika 16 atau lebih Wilayah komersial di mana AWS Control Tower tersedia diatur, termasuk Wilayah opt-in, batas atas jumlah akun per unit organisasi (OU), dikurangi, saat mendaftarkan OU. Untuk informasi selengkapnya, lihat Bat asan berdasarkan AWS layanan yang mendasarinya.

Konfigurasikan kontrol Penolakan Wilayah

AWS Control Tower menawarkan dua kontrol Penolakan Wilayah. Satu kontrol,`AWS-GR_REGION_DENY`, ketika diaktifkan, berlaku untuk seluruh zona pendaratan. Kontrol lain`CT.MULTISERVICE.PV.1`, ketika diaktifkan, dapat diterapkan ke OU tertentu yang Anda

tentukan. Untuk informasi selengkapnya, lihat Menolak akses AWS berdasarkan kontrol yang diminta Wilayah AWS dan Penolakan Wilayah yang diterapkan ke OU.

Pertimbangan tentang Wilayah menolak kontrol untuk zona pendaratan

Kontrol Wilayah menolak, `AWS-GR_REGION_DENY` adalah unik, karena berlaku untuk zona pendaratan secara keseluruhan, bukan untuk OU tertentu. Untuk mengonfigurasi kontrol penolakan wilayah, buka halaman pengaturan zona pendaratan dan pilih Ubah pengaturan.

- Pengaturan ini dapat diubah di lain waktu.
- Saat diaktifkan, kontrol ini berlaku untuk semua OU dengan di `AWSControlTowerBaseline` aktifkan.
- Kontrol ini tidak dapat dikonfigurasi untuk OU individual.

> **Note**
>
> Sebelum mengaktifkan kontrol Penolakan wilayah, pastikan Anda tidak memiliki sumber daya yang ada di Wilayah ini, karena Anda tidak akan memiliki akses ke sumber daya setelah menerapkan kontrol. Saat kontrol diaktifkan, Anda tidak akan dapat menyebarkan sumber daya di Wilayah yang ditolak.

Ketika Anda mengaktifkan kontrol, itu berlaku untuk semua OU tingkat atas dengan di `AWSControlTowerBaseline` aktifkan, dan diwarisi oleh OU yang lebih rendah dalam hierarki organisasi. Saat Anda menghapus kontrol, kontrol akan dihapus pada semua OU yang diterapkan sebelumnya, semua Wilayah yang tidak diatur di AWS Control Tower tetap dalam status Tidak diatur, dan Anda dapat menerapkan sumber daya di Wilayah di luar ketersediaan AWS Control Tower.

> **Pengecualian**
>
> Anda tidak dapat menolak akses ke Wilayah rumah Anda. AWS Layanan global tertentu, seperti IAM dan AWS Organizations, dikecualikan dari kontrol menolak Wilayah. Untuk mempelajari selengkapnya, lihat Men AWS olak akses berdasarkan permintaan Wilayah AWS.

- Nama kontrol penuh: Tolak akses AWS berdasarkan Wilayah yang diminta AWS untuk zona pendaratan
- Deskripsi kontrol: Melarang akses ke operasi yang tidak terdaftar di layanan global dan regional di luar Wilayah yang ditentukan untuk zona pendaratan.
- Ini adalah kontrol elektif dengan bimbingan pencegahan.

Untuk melihat template SCP kontrol penolakan wilayah, lihat Menolak akses AWS berdasarkan yang diminta Wilayah AWS dalam referensi Kontrol Menara Kontrol AWS. AWS Control Tower SCP mirip dengan SCP untuk AWS Organizations, tetapi tidak identik.

Anda dapat menentukan titik akhir layanan Regi onal di halaman Layanan regional.

Pertimbangan untuk OU-level Wilayah menolak kontrol

Pertimbangan utama tentang kontrol Pen OU-level olakan Wilayah adalah untuk menentukan bagaimana kontrol tersebut akan berinteraksi dengan kontrol penolakan wilayah zona pendaratan, jika keduanya diaktifkan. Untuk informasi selengkapnya, lihat Kontrol penolakan wilayah yang diterapkan ke OU.

Anda juga mungkin ingin meninjau Konfigurasi kontrol penolakan wilayah.

Tentang Akun AWS di AWS Control Tower

An Akun AWS adalah wadah untuk semua sumber daya milik Anda. Sumber daya ini termasuk identitas AWS Identity and Access Management (IAM) yang diterima oleh akun, yang menentukan siapa yang memiliki akses ke akun itu. Identitas IAM dapat mencakup pengguna, grup, peran, dan banyak lagi. Untuk informasi selengkapnya tentang bekerja dengan IAM, pengguna, peran, dan kebijakan di AWS Control Tower, lihat Manajemen identitas dan akses di AWS Control Tower.

Sumber daya dan waktu pembuatan akun

Saat AWS Control Tower membuat atau mendaftarkan akun, AWS Control Tower akan menerapkan konfigurasi sumber daya minimum yang diperlukan untuk akun tersebut. Misalnya, mungkin termasuk sumber daya dalam bentuk template Account Factory dan sumber daya lain di landing zone Anda, seperti peran IAM, AWS CloudTrail jalur, produk yang disediakan Service Catalog, dan pengguna IAM Identity Center. AWS Control Tower juga menyebarkan sumber daya, seperti yang dipersyaratkan oleh konfigurasi kontrol, untuk unit organisasi (OU) di mana akun baru ditakdirkan untuk menjadi akun anggota.

AWS Control Tower mengatur penerapan sumber daya ini atas nama Anda. Mungkin diperlukan beberapa menit per sumber daya untuk menyelesaikan penerapan, jadi pertimbangkan total waktu sebelum Anda membuat atau mendaftarkan akun. Untuk informasi selengkapnya tentang mengelola sumber daya di akun Anda, lihatPanduan untuk membuat dan memodifikasi sumber daya AWS Control Tower.

Apa yang terjadi ketika AWS Control Tower membuat akun

Akun baru di AWS Control Tower dibuat dan kemudian disediakan oleh interaksi antara AWS Control Tower, AWS Organizations, dan. AWS Service Catalog Anda dapat membuat akun dan mendaftarkan akun yang ada dari konsol AWS Control Tower. Untuk langkah-langkah mendetail untuk mendaftarkan yang sudah ada Akun AWS menggunakan konsol AWS Control Tower, lihatMendaftarkan akun yang sudah ada dari konsol AWS Control Tower.

Di balik layar pembuatan akun

1. Anda memulai permintaan, misalnya, dari halaman AWS Control Tower Account Factory, atau langsung dari AWS Service Catalog konsol, atau dengan memanggil Service Catalog `ProvisionProduct` API.

2. AWS Service Catalog memanggil AWS Control Tower.
3. AWS Control Tower memulai alur kerja, yang sebagai langkah pertama memanggil AWS Organizations `CreateAccount` API.
4. Setelah AWS Organizations membuat akun, AWS Control Tower menyelesaikan proses penyediaan dengan menerapkan cetak biru dan kontrol.
5. Service Catalog terus melakukan polling AWS Control Tower untuk memeriksa penyelesaian proses penyediaan.
6. Ketika alur kerja di AWS Control Tower selesai, Service Catalog menyelesaikan status akun dan memberi tahu Anda (pemohon) hasilnya.

Pertimbangan untuk membawa akun keamanan atau pencatatan yang ada

Sebelum menerima akun Akun AWS keamanan (nama default: Config aggregator) atau logging (nama default CloudTrail : administrator), AWS Control Tower memeriksa akun untuk sumber daya yang bertentangan dengan persyaratan AWS Control Tower. Misalnya, Anda mungkin memiliki bucket logging dengan nama yang sama dengan AWS Control Tower. Selain itu, AWS Control Tower memvalidasi bahwa akun dapat menyediakan sumber daya; misalnya, dengan memastikan bahwa AWS Security Token Service (AWS STS) diaktifkan, bahwa akun tidak ditangguhkan, dan AWS Control Tower memiliki izin untuk menyediakan sumber daya di dalam akun.

AWS Control Tower tidak menghapus sumber daya apa pun yang ada di akun pencatatan dan keamanan yang Anda berikan. Namun, jika Anda memilih untuk mengaktifkannya, kontrol penolakan Wilayah AWS Control Tower mencegah akses ke sumber daya di Wilayah yang ditolak.

> **Keamanan untuk akun Anda**
>
> Anda dapat menemukan panduan tentang praktik terbaik untuk melindungi keamanan akun manajemen AWS Control Tower dan akun anggota Anda dalam AWS Organizations dokumentasi.
>
> - Praktik terbaik untuk akun manajemen
> - Praktik terbaik untuk akun anggota

Akun integrasi layanan

AWS Control Tower menggunakan tiga fitur khusus Akun AWS: akun manajemen, akun agregator Config, dan akun administrator. CloudTrail AWS Control Tower mengacu pada akun agregator Config dan akun CloudTrail administrator sebagai akun integrasi layanan.

> **Nama akun lama**
>
> Dalam versi landing zone lebih awal dari 4.0, akun ini disebut akun bersama (atau terkadang akun inti).

- Anda dapat memilih nama yang disesuaikan untuk akun integrasi layanan saat menyiapkan landing zone. Untuk informasi tentang mengubah nama akun, lihat Mengubah nama sumber daya AWS Control Tower secara eksternal.
- Anda juga dapat menentukan akun integrasi layanan AWS Control Tower Akun AWS sebagai akun integrasi layanan AWS Control Tower, selama proses penyiapan landing zone awal. Opsi ini menghilangkan kebutuhan AWS Control Tower untuk membuat akun baru. (Ini adalah pilihan satu kali.)

Untuk informasi selengkapnya tentang akun integrasi layanan dan sumber daya terkait, lihatSumber daya yang dibuat di akun integrasi layanan.

Akun manajemen

Ini Akun AWS meluncurkan AWS Control Tower. Secara default, pengguna root untuk akun ini dan pengguna IAM atau pengguna administrator IAM untuk akun ini memiliki akses penuh ke semua sumber daya dalam landing zone Anda.

> **Note**
>
> Sebagai praktik terbaik, sebaiknya masuk sebagai pengguna Pusat Identitas IAM dengan hak Administrator saat menjalankan fungsi administratif dalam konsol AWS Control Tower, alih-alih masuk sebagai pengguna root atau pengguna administrator IAM untuk akun ini.

Untuk informasi selengkapnya tentang peran dan sumber daya yang tersedia di akun manajemen, lihatSumber daya yang dibuat di akun integrasi layanan.

CloudTrail akun administrator

AWS Control Tower menyiapkan akun CloudTrail administrator saat Anda mengaktifkan integrasi logging AWS CloudTrail terpusat. Atau, Anda dapat menggunakan AWS akun yang ada sebagai akun CloudTrail administrator. Anda mungkin mengetahui akun ini dengan nama sebelumnya: akun arsip log.

Akun ini berisi bucket Amazon S3 pusat yang menyimpan file log untuk semua akun lain di landing zone Anda. Dalam versi landing zone lebih awal dari 4.0, bucket ini menyimpan keduanya AWS CloudTrail dan file AWS Config log. Di landing zone versi 4.0 dan yang lebih baru, bucket ini hanya menyimpan file AWS CloudTrail log. AWS Config menyimpan file lognya di bucket khusus di akun agregator Config.

Sebagai praktik terbaik, batasi akses ke akun ini ke tim yang bertanggung jawab atas kepatuhan dan investigasi, dan alat keamanan atau audit terkait mereka. Anda dapat menggunakan akun ini untuk audit keamanan otomatis. Anda juga dapat meng-host kustom Aturan AWS Config, seperti fungsi Lambda, untuk melakukan tindakan remediasi.

> **Kebijakan bucket Amazon S3**
>
> Untuk AWS Control Tower landing zone versi 3.3 dan yang lebih baru, akun harus memenuhi `aws:SourceOrgID` persyaratan untuk izin menulis apa pun ke bucket Audit Anda. Kondisi ini memastikan bahwa CloudTrail hanya dapat menulis log atas nama akun dalam organisasi Anda ke bucket S3 Anda; ini mencegah CloudTrail log di luar organisasi Anda menulis ke bucket AWS Control Tower S3 Anda. Untuk informasi selengkapnya, lihat Zona pendaratan Menara Kontrol AWS versi 3.3.

Untuk informasi selengkapnya tentang peran dan sumber daya yang tersedia di akun arsip log, lihat CloudTrail sumber daya akun administrator

> **Note**
>
> Log ini tidak dapat diubah. Semua log disimpan untuk tujuan audit dan investigasi kepatuhan yang terkait dengan aktivitas akun.

Akun agregator Config

AWS Control Tower menyiapkan akun agregator Config saat Anda mengaktifkan integrasi layanan. AWS Config Atau, Anda dapat menggunakan akun yang ada sebagai AWS akun agregator Config. Anda mungkin mengetahui akun ini dengan nama sebelumnya: akun audit.

Akun agregator Config harus dibatasi untuk tim keamanan dan kepatuhan dengan peran lintas akun auditor (read-only) dan administrator (akses penuh) ke semua akun di landing zone. Peran ini dimaksudkan untuk digunakan oleh tim keamanan dan kepatuhan untuk:

- Lakukan audit melalui AWS mekanisme, seperti menghosting fungsi Lambda AWS Config aturan kustom.
- Lakukan operasi keamanan otomatis, seperti tindakan remediasi.

Akun agregator Config juga menerima notifikasi melalui layanan Amazon Simple Notification Service (Amazon SNS). Anda dapat menerima tiga kategori pemberitahuan:

- Semua Peristiwa Konfigurasi — Topik ini menggabungkan semua CloudTrail dan AWS Config pemberitahuan dari semua akun di landing zone Anda.
- Pemberitahuan Keamanan Agregat — Topik ini menggabungkan semua pemberitahuan keamanan dari CloudWatch peristiwa tertentu, peristiwa perubahan status Aturan AWS Config kepatuhan, dan GuardDuty temuan.
- Pemberitahuan Drift — Topik ini menggabungkan semua peringatan drift yang ditemukan di semua akun, pengguna, OU, dan SCP di landing zone Anda. Untuk informasi lebih lanjut tentang drift, lihatMendeteksi dan mengatasi penyimpangan di AWS Control Tower.

Pemberitahuan audit yang dipicu dalam akun anggota juga dapat mengirim peringatan ke topik Amazon SNS lokal. Fungsi ini memungkinkan administrator akun untuk berlangganan pemberitahuan audit yang khusus untuk akun anggota individu. Akibatnya, administrator dapat menyelesaikan masalah yang memengaruhi akun individual, sambil tetap menggabungkan semua notifikasi akun ke akun agregator Config terpusat Anda. Untuk informasi lebih lanjut, lihat Panduan Developer Amazon Simple Notification Service.

Untuk informasi selengkapnya tentang peran dan sumber daya yang tersedia di akun agregator Config, lihat. Config sumber daya akun agregator

Untuk informasi selengkapnya tentang audit terprogram, lihat Peran terprogram dan hubungan kepercayaan untuk akun audit AWS Control Tower.

> **Important**
>
> Alamat email yang Anda berikan untuk akun agregator Config menerima email AWS Pemberitahuan - Konfirmasi Langganan dari setiap email yang Wilayah AWS didukung oleh AWS Control Tower. Untuk menerima email kepatuhan di akun agregator Config Anda, Anda harus memilih tautan Konfirmasi langganan dalam setiap email dari masing-masing yang Wilayah AWS didukung oleh AWS Control Tower.

Sumber daya yang dibuat di akun integrasi layanan

Bagian ini menunjukkan sumber daya yang dibuat AWS Control Tower di akun integrasi layanan, saat Anda menyiapkan landing zone.

Untuk informasi tentang sumber daya akun anggota, lihatPertimbangan Sumber Daya untuk Pabrik Akun.

Sumber daya akun manajemen

Saat Anda mengatur landing zone, AWS sumber daya berikut akan dibuat dalam akun manajemen Anda.

AWS service	Tipe sumber daya	Nama sumber daya
AWS Organizations	Akun	Config aggregator (audit) CloudTrail administrator (log archive)
AWS Organizations	OU	Security Sandbox
AWS Organizations	Kebijakan Kontrol Layanan	aws-guardrails-*

AWS service	Tipe sumber daya	Nama sumber daya
AWS CloudFormation	Tumpukan	AWSControlTowerBP-BASELINE-CLOUDTRAIL-MASTER AWSControlTowerBP-BASELINE-CONFIG-MASTER(di landing zone versi 2.6 dan yang lebih baru; tidak digunakan di landing zone versi 4.0 dan yang lebih baru)

AWS service	Tipe sumber daya	Nama sumber daya
AWS CloudFormation	StackSets	AWSControlTowerBP-BASELINE-CLOUDTRAIL(Tidak digunakan di landing zone versi 3.0 dan yang lebih baru) AWSControlTowerBP-BASELINE-CLOUDWATCH AWSControlTowerBP-BASELINE-CONFIG AWSControlTowerBP-BASELINE-ROLES AWSControlTowerBP-BASELINE-SERVICE-ROLES AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE(Diterapkan di landing zone versi 3.2 dan yang lebih baru) AWSControlTowerBP-SECURITY-TOPICS AWSControlTowerLoggingResources AWSControlTowerSecurityResources AWSControlTowerExecutionRole AWSControlTowerBP-CONFIG-CENTRAL-S3-

AWS service	Tipe sumber daya	Nama sumber daya
		BUCKET(Diterapkan di landing zone versi 4.0 dan yang lebih baru)
AWS Service Catalog	Produk	AWS Control Tower Account Factory
AWS Config	Agregator	aws-controltower-ConfigAggregatorForOrganizations(Tidak digunakan di landing zone versi 4.0 dan yang lebih baru)
AWS CloudTrail	Jejak	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch Log	aws-controltower/CloudTrail Logs
AWS Identity and Access Management	Peran	AWSControlTowerAdmin AWSControlTowerStackSetRole AWSControlTowerCloudTrailRolePolicy
AWS Identity and Access Management	Kebijakan	AWSControlTowerServiceRolePolicy AWSControlTowerAdminPolicy AWSControlTowerCloudTrailRolePolicy AWSControlTowerStackSetRolePolicy

AWS service	Tipe sumber daya	Nama sumber daya
AWS IAM Identity Center	Grup direktori	AWSAccountFactory AWSAuditAccountAdmins AWSControlTowerAdmins AWSLogArchiveAdmins AWSLogArchiveViewers AWSSecurityAuditors AWSSecurityAuditPowerUsers AWSServiceCatalogAdmins
AWS IAM Identity Center	Set Izin	AWSAdministratorAccess AWSPowerUserAccess AWSServiceCatalogAdminFullAccess AWSServiceCatalogEndUserAccess AWSReadOnlyAccess AWSOrganizationsFullAccess

Note

CloudFormation StackSet `BP_BASELINE_CLOUDTRAIL`Ini tidak digunakan di landing zone versi 3.0 atau yang lebih baru. Namun, itu terus ada di versi sebelumnya dari landing zone, sampai Anda memperbarui landing zone Anda.

Per Juni 2025, AWS Control Tower menerapkan kontrol detektif sebagai AWS Config aturan terkait layanan secara langsung di akun terdaftar, bukan melalui. CloudFormation StackSets Instance StackSets `AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-`

READ-PROHIBITED AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED dan tumpukan terkaitnya tidak lagi digunakan. Untuk informasi selengkapnya, lihat Dukungan untuk kontrol detektif yang diterapkan sebagai aturan AWS Config terkait layanan.

CloudTrail sumber daya akun administrator

Saat Anda mengatur landing zone, AWS sumber daya berikut akan dibuat di dalam akun CloudTrail administrator Anda.

AWS service	Tipe sumber daya	Nama Sumber Daya
AWS CloudFormation	Tumpukan	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH- StackSet-AWSControlTowerBP-BASELINE-CONFIG- StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL- StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES- StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In landing zone version 3.2 and later) StackSet-AWSControlTowerBP-BASELINE-ROLES-

AWS service	Tipe sumber daya	Nama Sumber Daya
		StackSet-AWSContro lTowerLoggingResources-
AWS Config	Aturan AWS Config	AWSControlTower_AW S-GR_AUDIT_BUCKET_ PUBLIC_READ_PROHIBITED AWSControlTower_AW S-GR_AUDIT_BUCKET_ PUBLIC_WRITE_PROHI BITED
AWS CloudTrail	Jalan setapak	aws-controltower-BaselineCl oudTrail
Amazon CloudWatch	CloudWatch Aturan Acara	aws-controltower-ConfigComp lianceChangeEventRule
Amazon CloudWatch	CloudWatch Log	/aws/lambda/aws-controltowe r-NotificationForwarder

AWS service	Tipe sumber daya	Nama Sumber Daya
AWS Identity and Access Management	Peran	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole AWSControlTowerExecution AWSServiceRoleForAWSControlTower
AWS Identity and Access Management	Kebijakan	AWSControlTowerServiceRolePolicy
Layanan Notifikasi Sederhana Amazon	Topik	aws-controltower-SecurityNotifications
AWS Lambda	Aplikasi	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*
AWS Lambda	Fungsi	aws-controltower-NotificationForwarder
Amazon Simple Storage Service	Kategori	aws-controltower-logs-* aws-controltower-s3-access-logs-*

Config sumber daya akun agregator

Saat menyiapkan landing zone, AWS sumber daya berikut akan dibuat dalam akun agregator Config Anda.

AWS service	Tipe sumber daya	Nama sumber daya
AWS CloudFormation	Tumpukan	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH- StackSet-AWSControlTowerBP-BASELINE-CONFIG- StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL- StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES- StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In landing zone version 3.2 and later) StackSet-AWSControlTowerBP-SECURITY-TOPICS- StackSet-AWSControlTowerBP-BASELINE-ROLES- StackSet-AWSControlTowerSecurityResources-*

AWS service	Tipe sumber daya	Nama sumber daya
		StackSet-AWSControlTowerBP-CONFIG-CENTRAL-S3-BUCKET-(Diterapkan di landing zone versi 4.0 dan yang lebih baru)
AWS Config	Agregator	aws-controltower-GuardrailsComplianceAggregator(Tidak digunakan di landing zone versi 4.0 dan yang lebih baru)
AWS Config	Agregator	aws-controltower-ConfigAggregatorForOrganizations(Diterapkan di landing zone versi 4.0 dan yang lebih baru)
AWS Config	Aturan AWS Config	AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIBITED
AWS CloudTrail	Jejak	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch Aturan Acara	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch Log	/aws/lambda/aws-controltower-NotificationForwarder

AWS service	Tipe sumber daya	Nama sumber daya
AWS Identity and Access Management	Peran	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole aws-controltower-AuditAdministratorRole aws-controltower-AuditReadOnlyRole AWSControlTowerExecution AWSServiceRoleForAWSControlTower
AWS Identity and Access Management	Kebijakan	AWSControlTowerServiceRolePolicy
Layanan Notifikasi Sederhana Amazon	Topik	aws-controltower-AggregateSecurityNotifications aws-controltower-AllConfigNotifications aws-controltower-SecurityNotifications

AWS service	Tipe sumber daya	Nama sumber daya
AWS Lambda	Fungsi	aws-controltower-NotificationForwarder
Amazon Simple Storage Service	Kategori	aws-controltower-config-logs-*(Diterapkan di landing zone versi 4.0 dan yang lebih baru) aws-controltower-config-access-logs-*(Diterapkan di landing zone versi 4.0 dan yang lebih baru)

Tentang akun anggota

Akun anggota adalah akun tempat pengguna Anda melakukan AWS beban kerja mereka. Akun anggota AWS Control Tower dapat dibuat dan disesuaikan dengan berbagai metode, termasuk metode otomatis. Dalam beberapa kasus, Anda dapat membawa yang ada Akun AWS ke AWS Control Tower. Saat akun anggota dibuat atau didaftarkan, akun tersebut harus ada di dalam unit organisasi (OU) yang dibuat di konsol AWS Control Tower, atau terdaftar di AWS Control Tower. Untuk informasi lebih lanjut, lihat topik terkait ini:

- Metode penyediaan
- Menyediakan dan mengelola akun dengan Account Factory
- Otomatisasi tugas di AWS Control Tower
- Memindahkan dan mendaftarkan akun dengan pendaftaran otomatis
- Menyediakan akun dengan AWS Control Tower Account Factory untuk Terraform (AFT)
- AWS Organizations Terminology and Concepts dalam AWS Organizations User Guide

> **Akun dan kontrol**
>
> Akun anggota dapat didaftarkan di AWS Control Tower, atau akun tersebut dapat dibuka. Kontrol berlaku berbeda untuk akun terdaftar dan tidak terdaftar, dan kontrol mungkin berlaku untuk akun di OU bersarang berdasarkan warisan.

Untuk informasi tentang sumber daya akun anggota yang dialokasikan AWS Control Tower, lihat. Pertimbangan Sumber Daya untuk Pabrik Akun

Berinteraksi dengan akun AWS Control Tower dari AWS Service Catalog

Bagian ini menjelaskan cara menangani akun AWS Control Tower Anda dengan kemampuan AWS Service Catalog.

Topik

- Menyediakan akun di konsol Service Catalog, dengan Account Factory
- Mengotomatiskan Penyediaan Akun di AWS Control Tower menurut Service Catalog API
- Memperbarui produk yang disediakan di Service Catalog
- Membatalkan pendaftaran akun di Service Catalog

Menyediakan akun di konsol Service Catalog, dengan Account Factory

Prosedur berikut menjelaskan cara membuat dan menyediakan akun sebagai pengguna di IAM Identity Center melalui AWS Service Catalog. Prosedur ini juga disebut sebagai penyediaan akun lanjutan, atau penyediaan akun manual. Secara opsional, Anda mungkin dapat menyediakan akun AWS Control Tower secara terprogram, AWS dengan CLI, dengan Service Catalog API, atau dengan AWS Control Tower Account Factory for Terraform (AFT). Anda mungkin dapat menyediakan akun yang disesuaikan di konsol jika sebelumnya Anda telah menyiapkan cetak biru khusus. Untuk informasi selengkapnya tentang kustomisasi, lihatSesuaikan akun dengan Kustomisasi Pabrik Akun (AFC).

> **Note**
>
> Jika Anda telah menonaktifkan Pusat Identitas IAM di pengaturan landing zone, parameter pengguna SSO (`SSOUserEmail`,`SSOUserFirstName`, dan`SSOUserLastName`) tidak digunakan selama penyediaan akun. Jika diinginkan, Anda dapat memberikan nilai placeholder untuk parameter yang diperlukan ini dan memodifikasinya nanti dengan mengikuti instruksi di. Memperbarui produk yang disediakan di Service Catalog

Untuk menyediakan akun secara individual di Account Factory, sebagai pengguna

1. Masuk dari URL portal pengguna Anda.
2. Dari aplikasi Anda, pilih AWS Akun.
3. Dari daftar akun, pilih ID akun untuk akun manajemen Anda. ID ini mungkin juga memiliki label, misalnya, (Manajemen).
4. Dari AWSServiceCatalogEndUserAccess, pilih Konsol manajemen. Ini membuka Konsol Manajemen AWS untuk pengguna ini di akun ini.
5. Pastikan Anda telah memilih yang benar Wilayah AWS untuk menyediakan akun, yang seharusnya merupakan Wilayah AWS Control Tower Anda.
6. Cari dan pilih Service Catalog untuk membuka konsol Service Catalog.
7. Di panel navigasi, pilih Produk.
8. Pilih AWS Control Tower Account Factory, lalu pilih tombol Luncurkan produk. Pilihan ini memulai wizard untuk menyediakan akun baru.
9. Isi informasinya, dan ingatlah hal-hal berikut:
   - SSOUserEmailDapat berupa alamat email baru, atau alamat email yang terkait dengan pengguna Pusat Identitas IAM yang ada. Apapun yang Anda pilih, pengguna ini akan memiliki akses administratif ke akun yang Anda sediakan.
   - AccountEmailHarus berupa alamat email yang belum dikaitkan dengan file Akun AWS. Jika Anda menggunakan alamat email baru SSOUserEmail, Anda dapat menggunakan alamat email tersebut di sini.
10. Jangan tentukan TagOptionsdan jangan aktifkan Pemberitahuan, jika tidak, akun dapat gagal disediakan. Setelah selesai, pilih Luncurkan produk.
11. Tinjau pengaturan akun Anda, lalu pilih Luncurkan. Jangan membuat rencana sumber daya, jika tidak, akun akan gagal disediakan.
12. Akun Anda sekarang sedang disediakan. Ini bisa memakan waktu beberapa menit untuk menyelesaikannya. Anda dapat me-refresh halaman untuk memperbarui informasi status yang ditampilkan.

> **Note**
>
> Hingga lima akun dapat disediakan sekaligus.

Mengotomatiskan Penyediaan Akun di AWS Control Tower menurut Service Catalog API

AWS Control Tower terintegrasi dengan beberapa AWS layanan lain, seperti AWS Service Catalog. Anda dapat menggunakan API untuk membuat dan menyediakan akun anggota Anda di AWS Control Tower, atau untuk mendaftarkan akun anggota yang ada.

> **Note**
>
> Jika Anda telah menonaktifkan Pusat Identitas IAM di pengaturan landing zone, parameter pengguna SSO (`SSOUserEmail`,`SSOUserFirstName`, dan`SSOUserLastName`) tidak digunakan selama penyediaan akun. Jika diinginkan, Anda dapat memberikan nilai placeholder untuk parameter yang diperlukan ini dan memodifikasinya nanti dengan mengikuti instruksi di. Memperbarui produk yang disediakan di Service Catalog

Video menunjukkan kepada Anda cara menyediakan akun secara otomatis, secara batch, dengan memanggil AWS Service Catalog API. Untuk penyediaan, Anda akan memanggil `ProvisionProduct`API dari antarmuka baris AWS perintah (CLI), dan Anda akan menentukan file JSON yang berisi parameter untuk setiap akun yang ingin Anda atur. Video menggambarkan menginstal dan menggunakan lingkungan pengembangan AWS Cloud9 untuk melakukan pekerjaan ini. Perintah CLI akan sama jika Anda menggunakan Cloudshell AWS alih-alih Cloud9. AWS

> **Note**
>
> Anda juga dapat menyesuaikan pendekatan ini untuk mengotomatiskan pembaruan akun, dengan memanggil `UpdateProvisionedProduct`API AWS Service Catalog untuk setiap akun. Anda dapat menulis skrip untuk memperbarui akun, satu per satu.

Sebagai metode otomatisasi yang sama sekali berbeda, jika Anda terbiasa dengan Terraform, Anda dapat menyediakan akun dengan AWS Control Tower Account Factory for Terraform (AFT).

Contoh peran administrasi otomatisasi

Berikut adalah contoh templat yang dapat Anda gunakan untuk membantu mengonfigurasi peran administrasi otomatisasi Anda di akun manajemen. Anda akan mengonfigurasi peran ini di akun manajemen Anda sehingga dapat melakukan otomatisasi dengan akses Administrator di akun target.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure the SampleAutoAdminRole

Resources:
  AdministrationRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: SampleAutoAdminRole
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service: cloudformation.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
      Policies:
        - PolicyName: AssumeSampleAutoAdminRole
          PolicyDocument:
            Version: 2012-10-17
            Statement:
              - Effect: Allow
                Action:
                  - sts:AssumeRole
                Resource:
                  - "arn:aws:iam::*:role/SampleAutomationExecutionRole"
```

Contoh peran eksekusi otomatisasi

Berikut adalah contoh template yang dapat Anda gunakan untuk membantu Anda mengatur peran eksekusi otomatisasi Anda. Anda akan mengonfigurasi peran ini di akun target.

```
AWSTemplateFormatVersion: "2010-09-09"
Description: "Create automation execution role for creating Sample Additional Role."

Parameters:
  AdminAccountId:
    Type: "String"
    Description: "Account ID for the administrator account (typically management,
 security or shared services)."
  AdminRoleName:
    Type: "String"
```

```
    Description: "Role name for automation administrator access."
    Default: "SampleAutomationAdministrationRole"
  ExecutionRoleName:
    Type: "String"
    Description: "Role name for automation execution."
    Default: "SampleAutomationExecutionRole"
  SessionDurationInSecs:
    Type: "Number"
    Description: "Maximum session duration in seconds."
    Default: 14400

Resources:
  # This needs to run after AdminRoleName exists.
  ExecutionRole:
    Type: "AWS::IAM::Role"
    Properties:
      RoleName: !Ref ExecutionRoleName
      MaxSessionDuration: !Ref SessionDurationInSecs
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: "Allow"
            Principal:
              AWS:
                - !Sub "arn:aws:iam::${AdminAccountId}:role/${AdminRoleName}"
            Action:
              - "sts:AssumeRole"
      Path: "/"
      ManagedPolicyArns:
        - "arn:aws:iam::aws:policy/AdministratorAccess"
```

Setelah mengonfigurasi peran ini, Anda memanggil AWS Service Catalog API untuk melakukan tugas otomatis. Perintah CLI diberikan dalam video.

Contoh masukan penyediaan untuk Service Catalog API

Berikut adalah contoh masukan yang dapat Anda berikan ke Service Catalog `ProvisionProduct` API jika Anda menggunakan API untuk menyediakan akun AWS Control Tower baru atau mendaftarkan akun anggota yang ada:

> **Note**
>
> Untuk mendaftarkan akun anggota yang ada menggunakan `ProvisionProduct` API, peran `AWSControlTowerExecution` IAM harus ada di akun target sebelum Anda memanggil API. Anda dapat menggunakan parameter input yang sama yang ditunjukkan dalam contoh berikut untuk penyediaan akun baru dan pendaftaran akun yang sudah ada.

```
{
  pathId: "lpv2-7n2o3nudljh4e",
  productId: "prod-y422ydgjge2rs",
  provisionedProductName: "Example product 1",
  provisioningArtifactId: "pa-2mmz36cfpj2p4",
  provisioningParameters: [
    {
      key: "AccountEmail",
      value: "abc@amazon.com"
    },
    {
      key: "AccountName",
      value: "ABC"
    },
    {
      key: "ManagedOrganizationalUnit",
      value: "Custom (ou-xfe5-a8hb8ml8)"
    },
    {
      key: "SSOUserEmail",
      value: "abc@amazon.com"
    },
    {
      key: "SSOUserFirstName",
      value: "John"
    },
    {
      key: "SSOUserLastName",
      value: "Smith"
    }
  ],
  provisionToken: "c3c795a1-9824-4fb2-a4c2-4b1841be4068"
}
```

Untuk informasi selengkapnya, lihat referensi API untuk Service Catalog.

> **Note**
>
> Perhatikan bahwa format string input untuk nilai `ManagedOrganizationalUnit` telah berubah dari `OU_NAME` ke`OU_NAME (OU_ID)`. Video berikut tidak menyebutkan perubahan ini.

Panduan Video

Video ini (6:58) menjelaskan cara mengotomatiskan penerapan akun di AWS Control Tower. Untuk tampilan yang lebih baik, pilih ikon di sudut kanan bawah video untuk memperbesarnya ke layar penuh. Captioning tersedia.

Panduan Video Penyediaan Akun Otomatis di AWS Control Tower.

Memperbarui produk yang disediakan di Service Catalog

Prosedur berikut memandu Anda melalui cara memperbarui akun Anda di Account Factory atau memindahkannya ke OU baru, dengan memperbarui produk yang disediakan akun di Service Catalog.

> **Note**
>
> Jika Anda telah menonaktifkan Pusat Identitas IAM di pengaturan landing zone, parameter pengguna SSO (`SSOUserEmail`,`SSOUserFirstName`, dan`SSOUserLastName`) tidak digunakan selama penyediaan akun. Jika diinginkan, Anda dapat memberikan nilai placeholder untuk parameter yang diperlukan ini dan memodifikasinya nanti dengan mengikuti instruksi di bagian ini.

Untuk memperbarui akun Account Factory atau mengubah OU melalui Service Catalog

1. Masuk ke AWS Management Console, dan buka AWS Service Catalog konsol di https://console.aws.amazon.com/servicecatalog/.

> **Note**
>
> Anda harus masuk sebagai pengguna dengan izin untuk menyediakan produk baru di Service Catalog (misalnya, pengguna IAM Identity Center di `AWSAccountFactory` atau `AWSServiceCatalogAdmins` grup).

2. Di panel navigasi, pilih Provisioning, lalu pilih Provisioned products.
3. Untuk setiap akun anggota yang terdaftar, lakukan langkah-langkah berikut untuk memperbarui semua akun anggota:

   a. Pilih akun anggota. Anda diarahkan ke halaman detail produk yang disediakan untuk akun tersebut.

   b. Pada halaman Detail produk yang disediakan, pilih tab Acara.

   c. Catat parameter berikut:

      - SSOUserEmail(Tersedia dalam detail produk yang disediakan)
      - AccountEmail(Tersedia dalam detail produk yang disediakan)
      - SSOUserFirstName(Tersedia di Pusat Identitas IAM)
      - SSOUSerLastName(Tersedia di Pusat Identitas IAM)
      - AccountName(Tersedia di Pusat Identitas IAM)

   d. Dari Tindakan, pilih Perbarui.

   e. Pilih tombol di sebelah Versi produk yang ingin Anda perbarui, dan pilih Berikutnya.

   f. Berikan nilai parameter yang disebutkan sebelumnya.

      - Jika Anda ingin menyimpan OU yang ada, untuk ManagedOrganizationalUnit, pilih OU yang sudah ada di akun tersebut.
      - Jika Anda ingin memigrasikan akun ke OU baru, untuk ManagedOrganizationalUnit, pilih OU baru untuk akun tersebut.

      Administrator cloud pusat dapat menemukan informasi ini di konsol AWS Control Tower, di halaman Organisasi.

   g. Pilih Berikutnya.

   h. Tinjau perubahan Anda, lalu pilih Perbarui. Proses ini dapat memakan waktu beberapa menit per akun.

Membatalkan pendaftaran akun di Service Catalog

Membatalkan pendaftaran akun dapat dilakukan di konsol Service Catalog oleh pengguna IAM Identity Center di `AWSAccountFactory` grup, dengan menghentikan Produk yang Disediakan. Untuk informasi selengkapnya tentang pengguna atau grup Pusat Identitas IAM, lihat Mengelola pengguna dan mengakses melalui AWS IAM Identity Center. Prosedur berikut menjelaskan cara membuka pendaftaran akun anggota di Service Catalog.

Untuk membatalkan pendaftaran akun yang terdaftar melalui Service Catalog

1. Buka konsol Service Catalog di browser web Anda dihttps://console.aws.amazon.com/servicecatalog.
2. Di panel navigasi kiri, pilih Daftar produk yang disediakan.
3. Dari daftar akun yang disediakan, pilih nama akun yang Anda inginkan AWS Control Tower tidak lagi dikelola.
4. Pada halaman Detail produk yang disediakan, dari menu Tindakan, pilih Hentikan.
5. Dari kotak dialog yang muncul, pilih Hentikan.

> **Important**
>
> Kata terminate khusus untuk Service Catalog. Ketika Anda mengakhiri akun di Service Catalog Account Factory, akun tersebut tidak ditutup. Tindakan ini menghapus akun dari OU dan landing zone Anda.

6. Ketika akun telah dibuka, statusnya berubah menjadi Tidak Diaktifkan.
7. Jika Anda tidak lagi membutuhkan akun, tutuplah. Untuk informasi selengkapnya tentang menutup AWS akun, lihat Menutup akun di Panduan AWS Billing Pengguna

> **Note**
>
> Tunggu status akun ditampilkan Tidak Diaktifkan.

Menyediakan dan mengelola akun di AWS Control Tower

Bab ini meliputi:

- ikhtisar dan prosedur untuk menyediakan dan mengelola akun anggota baru di AWS Control Tower.
- ikhtisar dan prosedur untuk mendaftarkan AWS akun yang ada ke AWS Control Tower.

Untuk informasi umum tentang akun di AWS Control Tower, lihatTentang Akun AWS di AWS Control Tower. Untuk informasi tentang mendaftarkan beberapa akun ke AWS Control Tower, lihat. Mendaftarkan unit organisasi yang ada dengan AWS Control Tower

> **Note**
>
> Penyediaan akun tunggal, pembaruan, dan penyesuaian harus menargetkan unit organisasi (OU) dengan AWSControlTowerBaseline diaktifkan. Jika OU tidak mengaktifkan, Anda dapat mengaktifkan pendaftaran otomatis akun atau menggunakan ResetEnabledControl API EnabledControls pada ResetEnabledBaseline EnabledBaselines dan di OU tersebut untuk mendaftarkan akun. AWSControlTowerBaseline Untuk detailnya AWSControlTowerBaseline, lihat:Jenis dasar yang berlaku di tingkat OU.

> **Note**
>
> Anda dapat melakukan hingga lima (5) operasi terkait akun secara bersamaan, termasuk penyediaan, memperbarui, dan mendaftar.

Izin diperlukan untuk penyediaan akun

Dengan izin grup pengguna yang sesuai, penyedia dapat menentukan garis dasar standar dan konfigurasi jaringan untuk setiap akun di organisasi mereka.

Saat membuat akun dari konsol AWS Control Tower dengan Account Factory, Anda harus masuk ke akun dengan pengguna IAM yang mengaktifkan `AWSServiceCatalogEndUserFullAccess` kebijakan, bersama dengan izin untuk menggunakan konsol AWS Control Tower, dan Anda tidak dapat masuk sebagai pengguna Root.

> **Note**
>
> Saat menyediakan akun, pemohon akun selalu harus memiliki izin `CreateAccount` dan. `DescribeCreateAccountStatus` Kumpulan izin ini adalah bagian dari peran Admin, dan diberikan secara otomatis ketika pemohon mengambil peran Admin. Jika Anda mendelegasikan izin untuk menyediakan akun, Anda mungkin perlu menambahkan izin ini secara langsung untuk pemohon akun.

Untuk informasi umum tentang izin yang diperlukan di AWS Control Tower, lihatMenggunakan kebijakan berbasis identitas (kebijakan IAM) untuk AWS Control Tower. Untuk informasi tentang peran dan akun di AWS Control Tower, lihat Per an dan akun.

Penyediaan akun dalam AWS Control Tower

AWS Control Tower menyediakan beberapa metode untuk membuat dan memperbarui akun anggota. Beberapa metode terutama berbasis konsol, dan beberapa metode terutama otomatis.

Gambaran umum

Salah satu cara standar untuk membuat akun anggota di AWS Control Tower adalah melalui Account Factory, produk berbasis konsol yang merupakan bagian dari Katalog Layanan. Selain itu, dari konsol AWS Control Tower, Anda dapat menggunakan Buat akun sebagai metode untuk menyediakan akun baru, serta Daftarkan akun untuk mendaftarkan AWS akun yang ada ke AWS Control Tower, jika zona pendaratan Anda tidak dalam keadaan drift.

Dengan Account Factory, Anda dapat menyediakan akun dasar, mengandalkan pengaturan default AWS Control Tower. Anda juga dapat menyediakan akun khusus yang memenuhi persyaratan untuk kasus penggunaan khusus.

Kustomisasi Pabrik Akun (AFC) adalah cara menyediakan akun khusus dari konsol AWS Control Tower, dan mengotomatiskan penyesuaian dan penyebaran akun Anda. Ini memungkinkan penyediaan otomatis berbasis konsol, setelah beberapa langkah pengaturan satu kali, yang menghilangkan kebutuhan untuk menulis skrip atau mengatur pipeline. Untuk informasi selengkapnya, lihat Sesuaikan akun dengan Kustomisasi Pabrik Akun (AFC).

> **Pendaftaran otomatis**
>
> Anda juga dapat membuat Akun AWS di luar AWS Control Tower dan memindahkannya ke OU yang terdaftar di AWS Control Tower, tanpa membuat penyimpangan warisan, jika Anda memilih fitur pendaftaran akun otomatis dari Peng aturan zona pendaratan Anda. Untuk informasi selengkapnya, lihat Memindahkan dan mendaftarkan akun dengan pendaftaran otomatis.

Console-based metode:

- Melalui konsol Account Factory yang merupakan bagian dari AWS Service Catalog, untuk akun dasar atau khusus. Tinjau Menyediakan dan mengelola akun dengan Account Factory untuk detail dan instruksi.
- Melalui pendaftaran otomatis, dengan memindahkan akun ke OU dari konsol. Lihat Memindahkan dan mendaftarkan akun dengan pendaftaran otomatis
- Melalui fitur Daftar akun di AWS Control Tower, jika zona pendaratan Anda tidak dalam keadaan hanyut. Lihat Mendaftarkan akun yang sudah ada dari konsol AWS Control Tower.
- Di konsol AWS Control Tower, Anda dapat menggunakan Account Factory untuk membuat, memperbarui, atau mendaftarkan hingga lima akun secara bersamaan.

Metode otomatis:

- Kode Lambda: Dari akun manajemen zona pendaratan AWS Control Tower Anda, menggunakan kode Lambda dan peran IAM yang sesuai. Lihat Penye diaan Akun Otomatis dengan Peran IAM.
- Terraform: Dari AWS Control Tower Account Factory for Terraform (AFT), yang bergantung pada Account Factory dan GitOps model untuk memungkinkan otomatisasi penyediaan dan pembaruan akun. Lihat Menyediakan akun dengan AWS Control Tower Account Factory untuk Terraform (AFT).
- Melalui pendaftaran otomatis, dengan memindahkan akun yang ada ke OU menggunakan API. Lihat Memindahkan dan mendaftarkan akun dengan pendaftaran otomatis
- Kustomisasi Account Factory di konsol AWS Control Tower: Setelah langkah-langkah penyiapan, penyediaan akun khusus di masa mendatang tidak memerlukan konfigurasi tambahan atau pemeliharaan pipeline. Akun disediakan melalui AWS Service Catalog produk yang disebut cetak biru. Cetak biru dapat menggunakan CloudFormation templat, atau templat Terraform.

> **Note**
>
> CloudFormation cetak biru dapat menyebarkan sumber daya ke beberapa Wilayah. Cetak biru Terraform hanya dapat menyebarkan sumber daya ke satu Wilayah. Secara default, itu adalah Wilayah rumah.

Menyediakan akun di konsol AWS Control Tower

Prosedur berikut menjelaskan cara membuat dan menyediakan akun sebagai pengguna di IAM Identity Center melalui konsol AWS Control Tower. Prosedur ini juga disebut sebagai penyediaan akun manual. Secara opsional, Anda mungkin dapat menyediakan akun AWS Control Tower secara terprogram, AWS dengan CLI, dengan Service Catalog APIs, atau dengan AWS Control Tower Account Factory for Terraform (AFT), atau secara otomatis mendaftarkan akun yang ada ke OU terdaftar. Anda mungkin dapat menyediakan akun yang disesuaikan di konsol jika sebelumnya Anda telah menyiapkan cetak biru khusus. Untuk informasi selengkapnya tentang kustomisasi, lihatSesuaikan akun dengan Kustomisasi Pabrik Akun (AFC).

Untuk menyediakan akun secara individual di konsol AWS Control Tower, sebagai pengguna

1. Masuk ke AWS dan navigasikan ke konsol AWS Control Tower..
2. Dari navigasi kiri, pilih Organizations untuk melihat halaman Organisasi.
3. Dari kanan atas, pilih Buat sumber daya.
4. Di menu tarik-turun, pilih Buat akun.
5. Isi informasi di halaman, dan ingatlah hal-hal berikut:
   - Email Akun harus berupa alamat email yang belum dikaitkan dengan email Akun AWS.
   - Nama tampilan adalah nama yang ingin Anda lihat untuk akun ini.
6. Isi kolom untuk menentukan konfigurasi Access Anda, dengan alamat email IAM Identity Center dan nama pengguna.
7. Pilih OU terdaftar dari daftar dropdown, untuk menunjukkan OU di mana Anda ingin menyediakan akun.
8. Secara opsional gunakan cetak biru yang telah ditentukan sebelumnya untuk menyediakan akun Anda dengan sumber daya yang disesuaikan. Anda dapat melakukan tugas ini nanti.
9. Tinjau pilihan akun Anda, lalu pilih Buat akun, di kanan bawah.

10. Akun Anda sekarang sedang disediakan. Ini bisa memakan waktu beberapa menit untuk menyelesaikannya. Anda dapat me-refresh halaman untuk memperbarui informasi status yang ditampilkan.

> **Note**
>
> Hingga lima akun dapat disediakan sekaligus.

Melihat akun Anda

Halaman Organisasi mencantumkan semua OU dan akun di organisasi Anda, terlepas dari OU atau status pendaftaran di AWS Control Tower. Anda dapat melihat dan mendaftarkan akun anggota ke AWS Control Tower—secara individual atau berdasarkan grup OU—jika setiap akun memenuhi prasyarat untuk pendaftaran.

Untuk melihat akun tertentu

- Arahkan ke halaman Organisasi.
- Anda dapat memilih Akun hanya dari menu dropdown di kanan atas.
- Kemudian, pilih nama akun Anda dari tabel.
- Atau, Anda dapat memilih nama OU induk dari tabel, dan melihat daftar semua akun dalam OU tersebut pada halaman Detail untuk OU tersebut.

Pada halaman Organisasi dan halaman detail akun, Anda dapat melihat Status akun, yang merupakan salah satu dari berikut:

- Tidak terdaftar — Akun tersebut adalah anggota OU induk, tetapi tidak sepenuhnya dikelola oleh AWS Control Tower. Jika OU induk terdaftar, akun diatur oleh kontrol preventif yang dikonfigurasi untuk OU induk terdaftar, tetapi kontrol detektif OU tidak berlaku untuk akun ini. Jika OU induk tidak terdaftar, tidak ada kontrol yang berlaku untuk akun ini.
- Mendaf tar — Akun sedang dibawa ke tata kelola oleh AWS Control Tower. Kami menyelaraskan akun dengan konfigurasi kontrol untuk OU induk. Proses ini mungkin memerlukan beberapa menit per sumber daya akun.
- Ter daftar — Akun diatur oleh kontrol yang dikonfigurasi untuk OU induknya. Ini sepenuhnya dikelola oleh AWS Control Tower.

- Pendaftaran gagal — Akun tidak dapat didaftarkan di AWS Control Tower. Untuk informasi selengkapnya, lihat Penyebab umum kegagalan pendaftaran.
- Pembaruan tersedia — Akun memiliki pembaruan yang tersedia. Akun dalam status ini masih Ter daftar, tetapi akun harus diperbarui untuk mencerminkan perubahan terbaru yang dilakukan pada lingkungan Anda. Untuk memperbarui satu akun, navigasikan ke halaman detail akun dan pilih Per barui akun.

  Jika Anda memiliki beberapa akun dengan status ini di bawah satu OU, Anda dapat memilih Re-register OU dan memperbarui akun tersebut bersama-sama.

Tentang mendaftarkan akun yang ada

Anda dapat memperluas tata kelola AWS Control Tower ke individu, yang ada Akun AWS saat Anda men daftarkannya ke unit organisasi (OU) yang sudah diatur oleh AWS Control Tower. Akun yang memenuhi syarat ada di OU yang tidak terdaftar yang merupakan bagian dari AWS Organizations organisasi yang sama dengan OU Menara Kontrol AWS.

Ada beberapa metode untuk mendaftarkan akun ke AWS Control Tower. Informasi di halaman ini berlaku untuk semua metode pendaftaran.

> **Note**
>
> Anda tidak dapat mendaftarkan AWS akun yang ada untuk berfungsi sebagai akun audit atau arsip log kecuali selama pengaturan zona pendaratan awal.

Apa yang terjadi selama pendaftaran akun

Selama proses pendaftaran, AWS Control Tower melakukan tindakan berikut:

- Mendasari akun, yang mencakup penerapan kumpulan tumpukan ini:
  - `AWSControlTowerBP-BASELINE-CLOUDTRAIL`
  - `AWSControlTowerBP-BASELINE-CLOUDWATCH`
  - `AWSControlTowerBP-BASELINE-CONFIG`
  - `AWSControlTowerBP-BASELINE-ROLES`
  - `AWSControlTowerBP-BASELINE-SERVICE-ROLES`

- `AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLES`
- `AWSControlTowerBP-VPC-ACCOUNT-FACTORY-V1`

  Sebaiknya tinjau template dari kumpulan tumpukan ini dan memastikan bahwa templat tersebut tidak bertentangan dengan kebijakan yang ada.
- Mengidentifikasi akun melalui AWS IAM Identity Center atau AWS Organizations.
- Menempatkan akun ke OU yang telah Anda tentukan. Pastikan untuk menerapkan semua SCP yang diterapkan di OU saat ini, sehingga postur keamanan Anda tetap konsisten.
- Menerapkan kontrol wajib ke akun melalui SCP yang berlaku untuk OU yang dipilih secara keseluruhan.
- Meng AWS Config aktifkan dan mengonfigurasinya untuk merekam semua sumber daya di akun.
- Menambahkan AWS Config aturan yang menerapkan kontrol detektif AWS Control Tower ke akun.

Akun dan jejak tingkat organisasi CloudTrail

Untuk zona pendaratan versi 3.1 dan lebih tinggi, jika Anda telah memilih AWS CloudTrail integrasi opsional dalam pengaturan zona pendaratan:

- Semua akun anggota dalam OU diatur oleh AWS CloudTrail jejak untuk OU, terdaftar atau tidak.
- Saat Anda mendaftarkan akun ke AWS Control Tower, akun Anda diatur oleh AWS CloudTrail jejak untuk organisasi baru. Jika Anda memiliki penerapan CloudTrail jejak yang sudah ada, Anda mungkin melihat biaya duplikat kecuali Anda menghapus jejak yang ada untuk akun tersebut sebelum mendaftarkannya di AWS Control Tower.
- Jika Anda memindahkan akun ke OU terdaftar—misalnya melalui AWS Organizations konsol atau API—Anda mungkin ingin menghapus jejak tingkat akun yang tersisa untuk akun tersebut. Jika Anda memiliki penerapan CloudTrail jejak yang sudah ada, Anda akan dikenakan CloudTrail biaya duplikat.

Jika Anda memperbarui zona pendaratan dan memilih untuk memilih keluar dari jalur tingkat organisasi, atau jika zona pendaratan Anda lebih tua dari versi 3.0, CloudTrail jalur tingkat organisasi tidak berlaku untuk akun Anda.

Daftarkan akun yang ada dengan VPC

AWS Control Tower menangani VPC secara berbeda saat Anda menyediakan akun baru di Account Factory dibandingkan saat Anda mendaftarkan akun yang sudah ada.

- Saat Anda membuat akun baru, AWS Control Tower secara otomatis menghapus VPC AWS default dan membuat VPC baru untuk akun tersebut.
- Saat Anda mendaftarkan akun yang sudah ada, AWS Control Tower tidak membuat VPC baru untuk akun tersebut.
- Saat Anda mendaftarkan akun yang sudah ada, AWS Control Tower tidak menghapus VPC atau VPC AWS default yang ada yang terkait dengan akun tersebut.

> **Tip**
>
> Anda dapat mengubah perilaku default untuk akun baru dengan mengonfigurasi Account Factory, sehingga tidak menyiapkan VPC secara default untuk akun di organisasi Anda di bawah AWS Control Tower. Untuk informasi selengkapnya, lihat Buat Akun di AWS Control Tower Tanpa VPC.

Daftarkan akun dengan AWS Config sumber daya

Akun yang akan didaftarkan tidak harus memiliki AWS Config sumber daya yang ada. Lihat M endaftarkan akun yang memiliki AWS Config sumber daya yang ada.

Berikut adalah beberapa contoh perintah AWS Config CLI yang dapat Anda gunakan untuk menentukan status sumber AWS Config daya akun yang ada, seperti perekam konfigurasi dan saluran pengiriman.

Lihat perintah:

- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-recorders`

Respon normal adalah sesuatu seperti `"name": "default"`

Hapus perintah:

- `aws configservice stop-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-delivery-channel --delivery-channel-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`

Prasyarat untuk pendaftaran

Bagian ini menjelaskan cara mendaftarkan AWS akun yang ada ke AWS Control Tower jika Anda belum memilih fitur pendaftaran otomatis opsional di halaman Peng aturan zona landas, atau jika Anda beroperasi dengan versi zona pendaratan sebelum 3.1.

Prasyarat ini diperlukan sebelum Anda dapat mendaftarkan yang sudah ada Akun AWS di AWS Control Tower:

> **Note**
>
> Prasyarat untuk menambahkan `AWSControlTowerExecution` peran tidak diperlukan jika Anda telah mengaktifkan kemampuan pendaftaran otomatis AWS Control Tower di halaman Peng aturan zona arahan, atau jika Anda mendaftarkan akun sebagai bagian dari proses Register OU. Namun, dalam semua kasus, akun yang akan didaftarkan mungkin tidak memiliki AWS Config sumber daya yang ada. Lihat M endaftarkan akun yang memiliki AWS Config sumber daya yang ada

1. Untuk mendaftarkan yang sudah ada Akun AWS, `AWSControlTowerExecution` peran harus ada di akun yang Anda daftarkan. Anda dapat meninjau Daftarkan akun untuk detail dan instruksi.
2. Selain `AWSControlTowerExecution` peran, yang ada yang ingin Akun AWS Anda daftarkan harus memiliki izin dan hubungan kepercayaan berikut. Jika tidak, pendaftaran akan gagal.

   Izin Peran: `AdministratorAccess` (kebijakan AWS terkelola)

   Hubungan Peran Kepercayaan:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

3. Kami menyarankan agar akun tidak memiliki perekam AWS Config konfigurasi atau saluran pengiriman. Ini dapat dihapus atau dimodifikasi melalui AWS CLI sebelum Anda dapat mendaftarkan akun. Jika tidak, tin jau Daftar akun yang memiliki AWS Config sumber daya yang ada untuk petunjuk tentang cara mengubah sumber daya yang ada.
4. Akun yang ingin Anda daftarkan harus ada di AWS Organizations organisasi yang sama dengan akun manajemen AWS Control Tower. Akun yang ada hanya dapat didaftarkan ke organisasi yang sama dengan akun manajemen AWS Control Tower, di OU yang sudah terdaftar di AWS Control Tower.

Untuk memeriksa prasyarat lain untuk pendaftaran, lihat Memulai dengan AWS Control Tower.

> **Note**
>
> Saat Anda mendaftarkan akun ke AWS Control Tower, akun Anda diatur oleh AWS CloudTrail jejak organisasi AWS Control Tower. Jika Anda memiliki penerapan CloudTrail jejak yang sudah ada, Anda mungkin melihat biaya duplikat kecuali Anda menghapus jejak yang ada untuk akun tersebut sebelum mendaftarkannya di AWS Control Tower.

Tentang akses tepercaya dengan **`AWSControlTowerExecution`** peran

Sebelum Anda dapat mendaftarkan akun yang sudah ada Akun AWS ke AWS Control Tower, Anda harus memberikan izin kepada AWS Control Tower untuk mengelola, atau mengatur, akun tersebut. Secara khusus, AWS Control Tower memerlukan izin untuk membuat akses tepercaya

antara AWS CloudFormation dan AWS Organizations atas nama Anda, sehingga CloudFormation dapat menerapkan stack Anda secara otomatis ke akun di organisasi yang Anda pilih. Dengan akses tepercaya ini, `AWSControlTowerExecution` peran melakukan aktivitas yang diperlukan untuk mengelola setiap akun. Itu sebabnya Anda harus menambahkan peran ini ke setiap akun sebelum Anda mendaftarkannya.

Ketika akses tepercaya diaktifkan, CloudFormation dapat membuat, memperbarui, atau menghapus tumpukan di beberapa akun dan Wilayah AWS dengan satu operasi. AWS Control Tower bergantung pada kemampuan kepercayaan ini sehingga dapat menerapkan peran dan izin ke akun yang ada sebelum memindahkannya ke unit organisasi terdaftar, dan dengan demikian membawanya di bawah tata kelola.

Untuk mempelajari lebih lanjut tentang akses tepercaya dan AWS CloudFormation StackSets, lihat AWS CloudFormationStackSets dan AWS Organizations.

Memindahkan dan mendaftarkan akun dengan pendaftaran otomatis

Fitur pendaftaran otomatis akun tersedia untuk zona pendaratan versi 3.1 dan yang lebih tinggi.

Jika Anda mengaktifkan fitur ini secara opsional, Anda dapat menggunakan AWS Organizations API dan konsol untuk memindahkan akun ke AWS Control Tower, tanpa membuat penyimpangan warisan . Akun secara otomatis menerima sumber daya dasar dan konfigurasi kontrol dari unit organisasi tujuan (OU) di AWS Control Tower. Kemampuan opsional ini juga memungkinkan Anda untuk memindahkan akun antar OU dalam AWS Control Tower, tanpa membuat penyimpangan warisan, jika kedua OU memiliki konfigurasi dasar yang sama dan kontrol yang sama diaktifkan.

Untuk mengaktifkan pendaftaran otomatis: Anda dapat memilih pendaftaran otomatis akun di halaman Peng aturan zona landas di konsol AWS Control Tower, atau dengan memanggil Menara Kontrol AWS `CreateLandingZone` atau `UpdateLandingZone` API, dengan nilai `RemediationType` parameter disetel ke Inheritance Drift.

Untuk mendaftarkan akun: Setelah Anda mengaktifkan pendaftaran otomatis, pindahkan akun ke OU terdaftar menggunakan AWS Organizations konsol, AWS Organizations `MoveAccount` API, atau konsol AWS Control Tower. Akun secara otomatis menerima sumber daya dasar dan kontrol dari OU tersebut. Ini berlaku untuk akun yang ada dan akun yang baru dibuat (yang dibuat di root organisasi secara default).

Untuk membatalkan pendaftaran akun: P indahkan akun ke OU yang tidak terdaftar di AWS Control Tower, atau ke root organisasi. AWS Control Tower menghapus semua sumber daya dasar dan kontrol yang digunakan secara otomatis.

> **Note**
>
> Jika OU sumber dan tujuan di AWS Control Tower memiliki konfigurasi yang berbeda, akun mungkin menunjukkan penyimp Akun anggota yang dipindahkan angan.

Prasyarat: Konfigurasikan untuk pendaftaran otomatis

- Anda harus menjalankan zona pendaratan AWS Control Tower versi 3.1 atau yang lebih baru.
- Pilih kemampuan pendaftaran otomatis AWS Control Tower melalui halaman Peng aturan zona pendaratan di konsol, atau melalui API zona pendaratan AWS Control Tower, dengan menyetel nilai `RemediationTypes` parameter ke`Inheritance Drift`. Setelah Anda ikut serta, AWS Control Tower bereaksi terhadap `move account` peristiwa untuk AWS Organizations, dan segera memperbaiki penyimpangan warisan untuk akun yang dipindahkan, atas nama Anda.

Izin yang diperlukan

Peran dan izin khusus diperlukan bagi Anda untuk menggunakan AWS Organizations `CreateAccount` API dan `MoveAccount` API. Untuk informasi selengkapnya tentang penggunaan AWS Organizations dengan AWS Control Tower, lihat Menara Kontrol AWS dan AWS Organizations.

Contoh penggunaan API

Untuk informasi selengkapnya dan contoh mengenai API ini, lihat `CreateAccount` dan `MoveAccount` di Refer AWS Organizations ensi API.

Pertimbangan-pertimbangan

- Garis waktu pendaftaran: Akun yang dipindahkan ke OU yang terdaftar di AWS Control Tower terdaftar dengan model konsistensi akhirnya. Proses ini biasanya memakan waktu beberapa menit, hingga beberapa jam, tergantung pada jumlah akun yang dipindahkan.
- AWS Produk yang disediakan Katalog Layanan: Auto-enrollment tidak membuat, mengubah, atau menghentikan produk yang AWS disediakan Katalog Layanan. Jika akun sebelumnya terdaftar melalui Account Factory dan memiliki produk yang disediakan terkait, produk yang disediakan akan tetap berada di akun manajemen setelah akun tidak terdaftar. Untuk membersihkan produk yang disediakan yatim piatu, lihat Menghapus produk yang disediakan di Panduan Pengguna Katalog AWS Layanan.

Mendaftarkan akun yang sudah ada dari konsol AWS Control Tower

Ada dua cara umum untuk mendaftarkan individu Akun AWS ke AWS Control Tower.

1. Setelah memilih fitur pendaftaran otomatis di halaman Pengaturan, Anda dapat membuat bagian Akun AWS luar AWS Control Tower dan mem indahkannya langsung ke OU terdaftar. Untuk informasi selengkapnya, lihat Mem indahkan dan mendaftarkan akun secara otomatis. Opsi ini tersedia untuk zona pendaratan versi 3.1 dan yang lebih baru.
2. Anda dapat mendaftarkan akun yang sudah ada dari konsol AWS Control Tower secara manual.

Bagian berikut menjelaskan opsi kedua, yang tidak memerlukan konfigurasi sebelumnya dari lingkungan Menara Kontrol AWS Anda. Akun AWS Harus memenuhi prasyarat yang diperlukan.

Lihat akun Anda yang memenuhi syarat di konsol:

1. Arahkan ke halaman Organisasi di Menara Kontrol AWS.
2. Temukan nama akun yang ingin Anda daftarkan. Untuk menemukannya, pilih Akun hanya dari menu tarik-turun di kanan atas, lalu cari nama akun di tabel yang difilter.

Selanjutnya, ikuti langkah-langkah untuk mendaftarkan akun individu, seperti yang ditunjukkan di Langkah-langkah untuk mendaftarkan akun secara manual bagian.

Pertimbangan untuk mendaftar dari konsol

- Fitur Daftar akun yang tersedia di konsol AWS Control Tower dimaksudkan untuk mendaftarkan akun yang Akun AWS sudah ada sehingga diatur oleh AWS Control Tower. Untuk informasi selengkapnya, lihat Mend aftarkan yang sudah ada Akun AWS.
- Kemampuan akun Enroll berbasis konsol tersedia saat zona pendaratan Anda tidak dalam keadaan drift. Jika zona pendaratan Anda dalam keadaan menyimpang, Anda mungkin tidak dapat menggunakan kemampuan akun Daftar dengan sukses. Anda harus menyediakan akun baru melalui Account Factory atau metode lain, sampai penyimpangan zona pendaratan Anda diselesaikan.
- Saat mendaftarkan akun dari konsol AWS Control Tower, Anda harus masuk ke akun dengan pengguna yang mengaktifkan `AWSServiceCatalogEndUserFullAccess` kebijakan, bersama dengan izin akses Administrator untuk menggunakan konsol AWS Control Tower, dan Anda tidak dapat masuk sebagai pengguna root.

- Akun yang Anda daftarkan dapat diperbarui melalui Pabrik Akun Menara Kontrol AWS, seperti Anda akan memperbarui akun lainnya. Prosedur pembaruan diberikan di bagian yang disebutMemperbarui dan memindahkan akun dengan AWS Control Tower.

> **Note**
>
> Saat Anda mendaftarkan yang sudah ada Akun AWS, pastikan untuk memverifikasi alamat email yang ada. Jika tidak, akun baru dapat dibuat.

Langkah-langkah untuk mendaftarkan akun secara manual

Setelah izin AdministratorAccess akses (kebijakan) diterapkan di Akun AWS akun Anda yang ada, ikuti langkah-langkah berikut untuk mendaftarkan akun:

Untuk mendaftarkan akun individu di AWS Control Tower dari konsol

- Arahkan ke halaman Organisasi Menara Kontrol AWS.
- Pada halaman Organisasi, akun yang memenuhi syarat untuk di daftarkan memungkinkan Anda memilih Daftar dari menu tar ik -turun Tindakan di bagian atas. Akun ini juga menampilkan tombol Daftarkan akun saat Anda melihatnya di halaman detail akun.
- Saat memilih Daftar akun, Anda akan melihat halaman Daftar akun, di mana Anda diminta untuk menambahkan `AWSControlTowerExecution` peran ke akun. Untuk beberapa instruksi, lihatMenambahkan peran IAM yang diperlukan secara manual ke yang sudah ada Akun AWS dan mendaftarkannya.
- Selanjutnya, pilih OU terdaftar dari daftar drop-down. Jika akun sudah ada di OU terdaftar, daftar ini akan menampilkan OU.
- Pilih Daftar akun.
- Anda akan melihat pengingat modal untuk menambahkan `AWSControlTowerExecution` peran dan mengonfirmasi tindakan.
- Pilih Daftar.
- AWS Control Tower memulai proses pendaftaran, dan Anda diarahkan kembali ke halaman detail akun.

Penyebab umum kegagalan pendaftaran

- Untuk mendaftarkan akun yang sudah ada, `AWSControlTowerExecution` peran harus ada di akun yang Anda daftarkan.
- Prinsipal IAM Anda mungkin tidak memiliki izin yang diperlukan untuk menyediakan akun.
- AWS Security Token Service (AWS STS) dinonaktifkan di Wil Akun AWS ayah di rumah Anda, atau di Wilayah mana pun yang didukung oleh AWS Control Tower.
- Anda mungkin masuk sebagai pengguna atau peran IAM yang perlu ditambahkan ke Portofolio Pabrik Akun di AWS Service Catalog. Pengguna atau peran harus ditambahkan sebelum Anda memiliki akses ke Account Factory sehingga Anda dapat membuat atau mendaftarkan akun di AWS Control Tower. Jika pengguna atau peran yang sesuai tidak ditambahkan ke portofolio Pabrik Akun, Anda akan menerima kesalahan saat mencoba menambahkan akun. Untuk petunjuk tentang cara memberikan akses ke AWS Service Catalog portofolio, lihat Mem berikan akses ke pengguna.
- Anda mungkin masuk sebagai root.
- Akun yang Anda coba daftarkan mungkin memiliki AWS Config pengaturan yang tersisa. Secara khusus, akun mungkin memiliki perekam konfigurasi atau saluran pengiriman. Ini harus dihapus atau dimodifikasi AWS CLI sebelum Anda dapat mendaftarkan akun. Untuk informasi selengkapnya, lihat Daftarkan akun yang sudah ada AWS Config sumber daya dan Berinteraksi dengan AWS Control Tower lewat AWS CloudShell.
- Jika akun tersebut milik OU lain dengan akun manajemen, termasuk OU Menara Kontrol AWS lainnya, Anda harus mengakhiri akun di OU saat ini sebelum dapat bergabung dengan OU lain. Sumber daya yang ada harus dihapus di OU asli. Jika tidak, pendaftaran akan gagal.
- Penyediaan dan pendaftaran akun gagal jika SCP OU tujuan Anda tidak mengizinkan Anda membuat semua sumber daya yang diperlukan untuk akun tersebut. Misalnya, SCP di OU tujuan Anda dapat memblokir pembuatan sumber daya tanpa tag tertentu. Dalam hal ini, penyediaan akun atau pendaftaran gagal, karena AWS Control Tower tidak mendukung penandaan sumber daya. Untuk bantuan, hubungi perwakilan akun Anda, atau Dukungan.

Untuk informasi selengkapnya tentang cara AWS Control Tower bekerja dengan peran saat Anda membuat akun baru atau mendaftarkan akun yang sudah ada, lihat Per an dan akun.

> **Tip**
>
> Jika Anda tidak dapat mengonfirmasi bahwa yang Akun AWS sudah ada memenuhi prasyarat pendaftaran, Anda dapat mengatur OU Pendaftaran dan mendaftarkan akun ke OU tersebut. Setelah pendaftaran berhasil, Anda dapat memindahkan akun ke OU yang diinginkan. Jika pendaftaran gagal, tidak ada akun atau OU lain yang terpengaruh oleh kegagalan tersebut.

Jika Anda ragu bahwa akun yang ada dan konfigurasinya kompatibel dengan AWS Control Tower, Anda dapat mengikuti praktik terbaik yang disarankan di bagian berikut.

Direkomendasikan: Anda dapat mengatur pendekatan dua langkah untuk pendaftaran akun

- Pertama, gunakan paket AWS Config kesesuaian untuk mengevaluasi bagaimana akun Anda dapat dipengaruhi oleh beberapa kontrol AWS Control Tower. Untuk menentukan bagaimana pendaftaran ke AWS Control Tower dapat memengaruhi akun Anda, lihat Memper panjang tata kelola AWS Control Tower menggunakan paket AWS Config kesesuaian.
- Selanjutnya, Anda mungkin ingin mendaftarkan akun. Jika hasil kepatuhan memuaskan, jalur migrasi lebih mudah karena Anda dapat mendaftarkan akun tanpa konsekuensi yang tidak terduga.
- Setelah Anda menyelesaikan evaluasi, jika Anda memutuskan untuk mengatur zona pendaratan AWS Control Tower, Anda mungkin perlu menghapus saluran AWS Config pengiriman dan perekam konfigurasi yang dibuat untuk evaluasi Anda. Kemudian Anda akan dapat mengatur AWS Control Tower dengan sukses.

> **Note**
>
> Paket kesesuaian juga berfungsi dalam situasi di mana akun berada di OU yang terdaftar oleh AWS Control Tower, tetapi beban kerja berjalan di Wil AWS ayah yang tidak memiliki dukungan AWS Control Tower. Anda dapat menggunakan paket kesesuaian untuk mengelola sumber daya di akun yang ada di Wilayah tempat AWS Control Tower tidak digunakan.

Jika akun tidak memenuhi prasyarat

Ingatlah bahwa, sebagai prasyarat, akun yang memenuhi syarat untuk didaftarkan ke tata kelola AWS Control Tower harus menjadi bagian dari keseluruhan organisasi yang sama. Untuk memenuhi

prasyarat pendaftaran akun ini, Anda dapat mengikuti langkah-langkah persiapan berikut untuk memindahkan akun ke organisasi yang sama dengan AWS Control Tower.

Langkah persiapan untuk membawa akun ke organisasi yang sama dengan AWS Control Tower

1. Hapus akun dari organisasi yang ada. Anda harus menyediakan metode pembayaran terpisah jika Anda menggunakan pendekatan ini.
2. Undang akun untuk bergabung dengan organisasi AWS Control Tower. Untuk informasi selengkapnya, lihat Meng AWS undang akun untuk bergabung dengan organisasi Anda di Panduan AWS Organizations Pengguna.
3. Terima undangannya. Akun muncul di root organisasi. Langkah ini memindahkan akun ke organisasi yang sama dengan AWS Control Tower. dan menetapkan SCP dan penagihan konsolidasi.

> **Tip**
>
> Anda dapat mengirim undangan untuk organisasi baru sebelum akun keluar dari organisasi lama. Undangan akan menunggu ketika akun secara resmi keluar dari organisasi yang ada.

Langkah-langkah untuk memenuhi prasyarat yang tersisa:

1. Buat `AWSControlTowerExecution` peran yang diperlukan.
2. Hapus VPC default. (Bagian ini opsional. AWS Control Tower tidak mengubah VPC default Anda yang ada.)
3. Hapus atau ubah perekam AWS Config konfigurasi atau saluran pengiriman yang ada melalui AWS CLI atau AWS CloudShell. Untuk informasi selengkapnya, lihat Daftarkan akun dengan AWS Config sumber daya dan Daftarkan akun yang sudah ada AWS Config sumber daya

Setelah menyelesaikan langkah-langkah persiapan ini, Anda dapat mendaftarkan akun ke AWS Control Tower. Untuk informasi selengkapnya, lihat Langkah-langkah untuk mendaftarkan akun secara manual. Langkah ini membawa akun ke dalam tata kelola AWS Control Tower penuh.

Langkah-langkah opsional untuk menghentikan penyediaan akun, sehingga dapat didaftarkan dan menyimpan tumpukannya

1. Untuk mempertahankan CloudFormation tumpukan yang diterapkan, hapus instans tumpukan dari kumpulan tumpukan, dan pilih Pertahankan tumpukan untuk instance.
2. Hentikan produk yang disediakan akun di Ac AWS Service Catalog count Factory. (Langkah ini hanya menghapus produk yang disediakan dari AWS Control Tower. Itu tidak menghapus akun.)
3. Siapkan akun dengan detail penagihan yang diperlukan, seperti yang diperlukan untuk akun apa pun yang bukan milik organisasi. Kemudian hapus akun dari organisasi. (Anda melakukan ini, sehingga akun tidak dihitung terhadap total dalam AWS Organizations kuota Anda.)
4. Bersihkan akun jika sumber daya tetap ada, lalu tutup, mengikuti langkah-langkah penutupan akun diMembatalkan pendaftaran akun.
5. Jika Anda memiliki OU Dit angguhkan dengan kontrol yang ditentukan, Anda dapat memindahkan akun ke sana alih-alih melakukan Langkah 1.

Menambahkan peran IAM yang diperlukan secara manual ke yang sudah ada Akun AWS dan mendaftarkannya

Jika Anda sudah menyiapkan zona pendaratan AWS Control Tower, Anda dapat mulai mendaftarkan akun organisasi Anda ke OU yang terdaftar di AWS Control Tower. Jika Anda belum menyiapkan zona pendaratan, ikuti langkah-langkah seperti yang dijelaskan dalam Panduan Pengguna Menara Kontrol AWS di Memulai, Langkah 2. Setelah zona pendaratan siap, selesaikan langkah-langkah berikut untuk membawa akun yang ada ke dalam tata kelola oleh AWS Control Tower, secara manual.

Pastikan untuk meninjau yang Prasyarat untuk pendaftaran disebutkan sebelumnya dalam Bab ini.

Sebelum mendaftarkan akun dengan AWS Control Tower, Anda harus memberikan izin AWS Control Tower untuk mengelola akun tersebut. Untuk melakukannya, Anda akan menambahkan peran yang memiliki akses penuh ke akun, seperti yang ditunjukkan pada langkah-langkah berikut. Langkah-langkah ini harus dilakukan untuk setiap akun yang Anda daftarkan.

Untuk setiap akun:

Langkah 1: Masuk dengan akses administrator ke akun manajemen organisasi yang saat ini berisi akun yang ingin Anda daftarkan.

Misalnya, jika Anda membuat akun ini dari AWS Organizations dan menggunakan peran IAM lintas akun untuk masuk, maka Anda dapat mengikuti langkah-langkah berikut:

1. Masuk ke akun manajemen organisasi Anda.
2. Kunjungi AWS Organizations.
3. Di bawah Akun, pilih akun yang ingin Anda daftarkan dan salin ID akunnya.
4. Buka menu tarik-turun akun di bilah navigasi atas dan pilih Ber alih Per an.
5. Pada formulir Ber alih peran, isi bidang berikut:
   - Di bawah Akun, masukkan ID akun yang Anda salin.
   - Di bawah Peran, masukkan nama peran IAM yang memungkinkan akses lintas akun ke akun ini. Nama peran ini ditentukan saat akun dibuat. Jika Anda tidak menentukan nama peran saat membuat akun, masukkan nama peran default,`OrganizationAccountAccessRole`.
6. Pilih Ganti Peran.
7. Anda sekarang harus masuk ke akun Konsol Manajemen AWS sebagai anak.
8. Setelah selesai, tetaplah di akun anak untuk bagian selanjutnya dari prosedur.
9. Catat ID akun manajemen, karena Anda harus memasukkannya di langkah berikutnya.

Langkah 2: Berikan izin AWS Control Tower untuk mengelola akun.

1. Pergi ke IAM.
2. Pergi ke Peran.
3. Pilih Buat peran.
4. Saat diminta untuk memilih layanan yang digunakan untuk peran tersebut, pilih Kebijakan kepercayaan khusus.
5. Salin contoh kode yang ditampilkan di sini dan tempelkan ke Dokumen Kebijakan. Ganti string *`Management Account ID`* dengan ID akun manajemen aktual dari akun manajemen Anda. Berikut adalah kebijakan untuk ditempel:

   JSON

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

```
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

6. Saat diminta untuk melampirkan kebijakan, pilih AdministratorAccess.
7. Pilih Next:Tags.
8. Anda mungkin melihat layar opsional berjudul Tambahkan tag. Lewati layar ini untuk saat ini dengan memilih Next:Review
9. Pada layar Tinjauan, di bidang Nama peran, masukkan`AWSControlTowerExecution`.
10. Masukkan deskripsi singkat di kotak Deskripsi, seperti Mem ungkinkan akses akun penuh untuk pendaftaran.
11. Pilih Buat peran.

Langkah 3: Daftarkan akun dengan memindahkannya ke OU terdaftar, dan verifikasi pendaftaran.

Setelah menyiapkan izin yang diperlukan dengan membuat peran, ikuti langkah-langkah berikut untuk mendaftarkan akun dan memverifikasi pendaftaran.

1. Masuk lagi sebagai Admin dan buka AWS Control Tower.
2. Daftarkan akun.
   - Dari halaman Organisasi di AWS Control Tower, pilih akun Anda, lalu pilih Daftar dari menu tarik - turun Tindakan di kanan atas.
   - Ikuti langkah-langkah untuk mendaftarkan akun individu, seperti yang ditunjukkan pada Langkah-langkah untuk mendaftarkan akun secara manual halaman.
3. Verifikasi pendaftaran.
   - Dari Menara Kontrol AWS, pilih Organisasi di navigasi kiri.
   - Cari akun yang baru saja Anda daftarkan. Status awalnya akan menunjukkan status Pendaftar an.
   - Ketika status berubah menjadi Di aktifkan, pemindahan berhasil.

Untuk melanjutkan proses ini, masuk ke setiap akun di organisasi Anda yang ingin Anda daftarkan di AWS Control Tower. Ulangi langkah prasyarat dan langkah pendaftaran untuk setiap akun.

Contoh untuk menambahkan **`AWSControlTowerExecution`** peran

Template YAML berikut dapat membantu Anda dalam membuat peran yang diperlukan dalam akun, sehingga dapat didaftarkan secara terprogram.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure the AWSControlTowerExecution role to enable use of your
  account as a target account in AWS CloudFormation StackSets.
Parameters:
  AdministratorAccountId:
    Type: String
    Description: AWS Account Id of the administrator account (the account in which
      StackSets will be created).
    MaxLength: 12
    MinLength: 12
Resources:
  ExecutionRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: AWSControlTowerExecution
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              AWS:
                - !Ref AdministratorAccountId
            Action:
              - sts:AssumeRole
      Path: /
      ManagedPolicyArns:
        - !Sub arn:${AWS::Partition}:iam::aws:policy/AdministratorAccess
```

Daftarkan akun yang sudah ada AWS Config sumber daya

Topik ini menyediakan pendekatan langkah demi langkah untuk cara mendaftarkan akun yang memiliki AWS Config sumber daya yang ada. Untuk contoh cara memeriksa sumber daya yang ada, lihatDaftarkan akun dengan AWS Config sumber daya.

Contoh dari AWS Config sumber daya

Berikut adalah beberapa jenis AWS Config sumber daya yang mungkin sudah dimiliki akun Anda. Sumber daya ini mungkin perlu dimodifikasi agar Anda dapat mendaftarkan akun Anda ke AWS Control Tower.

- AWS Config perekam
- AWS Config saluran pengiriman
- AWS Config otorisasi agregasi

Batasan

- Mendaftarkan akun dengan sumber daya AWS Config yang ada tidak didukung untuk akun manajemen atau akun integrasi layanan yang dikonfigurasi di landing zone.
- Akun dapat didaftarkan hanya dengan menggunakan registrasi OU atau alur kerja pendaftaran ulang yang memungkinkan. `AWSControlTowerBaseline` Akun tidak dapat didaftarkan dengan mengaktifkan atau mengatur ulang. `ConfigBaseline`
- Akun dengan sumber daya AWS Config yang ada tidak didukung oleh. Memindahkan dan mendaftarkan akun dengan pendaftaran otomatis
- Jika sumber daya dimodifikasi dan membuat drift di akun, AWS Control Tower tidak memperbarui sumber daya.
- AWS Config sumber daya di Wilayah yang tidak diatur oleh AWS Control Tower tidak diubah.

Asumsi

- Anda telah menerapkan zona landing zone AWS Control Tower.
- Akun Anda belum terdaftar dengan AWS Control Tower.
- Akun Anda memiliki setidaknya satu AWS Config sumber daya yang sudah ada sebelumnya di setidaknya satu Wilayah yang diatur oleh AWS Control Tower.
- Akun Anda tidak dalam penyimpangan tata kelola.

> **Note**
>
> Jika Anda mencoba mendaftarkan akun yang memiliki sumber daya Config yang ada, tanpa akun ditambahkan ke daftar izin, pendaftaran akan gagal. Setelah itu, jika Anda kemudian

mencoba menambahkan akun yang sama ke daftar izin, AWS Control Tower tidak dapat memvalidasi bahwa akun tersebut disediakan dengan benar. Anda harus membatalkan penyediaan akun dari AWS Control Tower sebelum Anda dapat meminta daftar izin dan kemudian mendaftarkannya. Jika Anda hanya memindahkan akun ke AWS Control Tower OU yang berbeda, hal itu menyebabkan penyimpangan tata kelola, yang juga mencegah akun ditambahkan ke daftar izin.

Untuk blog yang menjelaskan pendekatan otomatis untuk mendaftarkan akun dengan sumber daya yang ada, lihat Mengotomatiskan pendaftaran akun dengan AWS Config sumber daya yang ada AWS Config ke AWS Control Tower.

Proses ini memiliki 5 langkah utama.

1. Tambahkan akun ke daftar izin AWS Control Tower.
2. Buat peran IAM baru di akun.
3. Memodifikasi AWS Config sumber daya yang sudah ada sebelumnya.
4. Buat AWS Config sumber daya di AWS Wilayah yang tidak ada.
5. Daftarkan akun dengan AWS Control Tower.

Sebelum Anda melanjutkan, pertimbangkan harapan berikut mengenai proses ini.

- AWS Control Tower tidak membuat AWS Config sumber daya apa pun di akun ini.
- Setelah pendaftaran, AWS Control Tower mengontrol secara otomatis melindungi AWS Config sumber daya yang Anda buat, termasuk peran IAM baru.
- Jika ada perubahan yang dilakukan pada AWS Config sumber daya setelah pendaftaran, sumber daya tersebut harus diperbarui agar selaras dengan pengaturan AWS Control Tower sebelum Anda dapat mendaftarkan ulang akun.

Langkah 1: Hubungi dukungan untuk menambahkan akun ke daftar izinkan

Sertakan frasa ini di baris subjek tiket Anda:

Daftarkan akun yang memiliki AWS Config sumber daya yang ada ke AWS Control Tower

Sertakan detail berikut di badan tiket Anda:

- Nomor akun manajemen
- Nomor akun akun anggota yang memiliki AWS Config sumber daya yang ada. Anda akan dapat membuat kasus dukungan untuk semua akun yang ingin Anda daftarkan.
- Wilayah rumah pilihan Anda untuk penyiapan AWS Control Tower

> **Note**
>
> Waktu yang diperlukan untuk menambahkan akun Anda ke daftar izin adalah 2 hari kerja.

Langkah 2: Buat peran IAM baru di akun anggota

1. Buka CloudFormation konsol untuk akun anggota.
2. Buat tumpukan baru menggunakan template berikut

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config

Resources:
  CustomerCreatedConfigRecorderRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: aws-controltower-ConfigRecorderRole-customer-created
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action:
              - sts:AssumeRole
      Path: /
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/service-role/AWS_ConfigRole
        - arn:aws:iam::aws:policy/ReadOnlyAccess
```

3. Berikan nama untuk tumpukan sebagai CustomerCreatedConfigRecorderRoleForControlTower

4. Buat tumpukan.

> **Note**
>
> SCP apa pun yang Anda buat harus mengecualikan `aws-controltower-ConfigRecorderRole*` peran. Jangan mengubah izin yang membatasi kemampuan AWS Config aturan untuk melakukan evaluasi.
> Ikuti panduan ini sehingga Anda tidak menerima `AccessDeniedException` ketika Anda memiliki SCP yang `aws-controltower-ConfigRecorderRole*` memblokir panggilan Config.

Langkah 3: Identifikasi AWS Daerah dengan sumber daya yang sudah ada sebelumnya

Untuk setiap Wilayah yang diatur (AWS Control Tower diatur) di akun, identifikasi dan catat Wilayah yang memiliki setidaknya satu jenis contoh AWS Config sumber daya yang ada yang ditampilkan sebelumnya.

Langkah 4: Identifikasi AWS Daerah tanpa AWS Config sumber daya

Untuk setiap Wilayah yang diatur (AWS Control Tower diatur) di akun, identifikasi dan catat Wilayah di mana tidak ada AWS Config sumber daya dari jenis contoh yang ditampilkan sebelumnya.

Langkah 5: Ubah sumber daya yang ada di masing-masing AWS Region

Untuk langkah ini, informasi berikut diperlukan tentang penyiapan AWS Control Tower Anda.

- `AUDIT_ACCOUNT`- ID akun integrasi layanan AWS Config (sebelumnya dikenal sebagai akun Audit)
- `CONFIG_BUCKET`- bucket AWS S3 tempat AWS Config memberikan snapshot konfigurasi dan file riwayat konfigurasi. Temukan dan konfirmasikan bahwa bucket AWS S3 ada sebelum melanjutkan ke langkah berikutnya.
  - Untuk landing zone versi 3.3 atau lebih rendah, bucket AWS S3 diberi nama`aws-controltower-logs-LOGGING_ACCOUNT-HOME_REGION`, terletak di akun Logging.
  - Untuk landing zone versi 4.0 atau lebih tinggi, bucket AWS S3 diberi nama`aws-controltower-config-logs-AUDIT_ACCOUNT-<SUFFIX_STRING>`, terletak di akun integrasi layanan AWS Config (sebelumnya dikenal sebagai akun Audit).

- `IAM_ROLE_ARN`- peran IAM ARN dibuat di Langkah 2
- `ORGANIZATION_ID`- ID organisasi untuk akun manajemen
- `MEMBER_ACCOUNT_NUMBER`- akun anggota yang sedang dimodifikasi
- `HOME_REGION`- Wilayah rumah untuk penyiapan AWS Control Tower.

Ubah setiap sumber daya yang ada dengan mengikuti instruksi yang diberikan di bagian 5a hingga 5c, yang mengikuti.

Langkah 5a. AWS Config sumber daya perekam

Hanya satu AWS Config perekam yang dapat ada per AWS Wilayah. Jika ada, ubah pengaturan seperti yang ditunjukkan. Ganti item `GLOBAL_RESOURCE_RECORDING` dengan true di Wilayah rumah Anda. Ganti item dengan false untuk Wilayah lain di mana AWS Config perekam ada.

- Nama: JANGAN UBAH
- roLearn: `IAM_ROLE_ARN`
  - RecordingGroup:
  - AllSupported: benar
  - IncludeGlobalResourceTypes: `GLOBAL_RESOURCE_RECORDING`
  - ResourceTypes: Kosong

Modifikasi ini dapat dilakukan melalui AWS CLI menggunakan perintah berikut. Ganti string `RECORDER_NAME` dengan nama AWS Config perekam yang ada.

```
aws configservice put-configuration-recorder --configuration-recorder
  name=RECORDER_NAME,roleARN=arn:aws:iam::MEMBER_ACCOUNT_NUMBER:role/
aws-controltower-ConfigRecorderRole-customer-created --recording-group
 allSupported=true,includeGlobalResourceTypes=GLOBAL_RESOURCE_RECORDING --
region CURRENT_REGION
```

Langkah 5b. Memodifikasi AWS Config sumber daya saluran pengiriman

Hanya satu saluran AWS Config pengiriman yang dapat ada per Wilayah. Jika ada yang lain, ubah pengaturan seperti yang ditunjukkan.

- Nama: JANGAN UBAH
- ConfigSnapshotDeliveryProperties: TwentyFour _Jam
- S3BucketName:*CONFIG_BUCKET*
- S3KeyPrefix: *ORGANIZATION_ID*
- SnsTopicARN: Topik SNS ARN dari akun audit, dengan format berikut:

  `arn:aws:sns:`*CURRENT_REGION*`:`*AUDIT_ACCOUNT*`:aws-controltower-AllConfigNotifications`

Modifikasi ini dapat dilakukan melalui AWS CLI menggunakan perintah berikut. Ganti string *DELIVERY_CHANNEL_NAME* dengan nama AWS Config perekam yang ada.

```
aws configservice put-delivery-channel --delivery-channel
 name=DELIVERY_CHANNEL_NAME,s3BucketName=CONFIG_BUCKET,s3KeyPrefix="ORGANIZATION_ID",configSnap
controltower-AllConfigNotifications --region CURRENT_REGION
```

Langkah 5c. Memodifikasi AWS Config sumber daya otorisasi agregasi

> **Note**
>
> Langkah ini tidak diperlukan untuk landing zone versi 4.0 atau lebih tinggi.

Beberapa otorisasi agregasi dapat ada per Wilayah. AWS Control Tower memerlukan otorisasi agregasi yang menetapkan akun audit sebagai akun resmi, dan memiliki Wilayah asal untuk AWS Control Tower sebagai Wilayah resmi. Jika tidak ada, buat yang baru dengan pengaturan berikut:

- AuthorizedAccountId: ID akun Audit
- AuthorizedAwsRegion: Wilayah beranda untuk penyiapan AWS Control Tower

Modifikasi ini dapat dilakukan melalui AWS CLI menggunakan perintah berikut:

`aws configservice put-aggregation-authorization --authorized-account-id` *AUDIT_ACCOUNT_ID* `--authorized-aws-region` *HOME_REGION* `--region` *CURRENT_REGION*

Langkah 6: Buat sumber daya yang tidak ada, di Wilayah yang diatur oleh AWS Control Tower

Merevisi CloudFormation template, sehingga di wilayah rumah Anda IncludeGlobalResourcesTypesparameter memiliki nilaiGLOBAL_RESOURCE_RECORDING, seperti yang ditunjukkan pada contoh berikut. Juga perbarui bidang yang diperlukan dalam template, seperti yang ditentukan dalam bagian ini.

Ganti item GLOBAL_RESOURCE_RECORDING dengan true di Wilayah rumah Anda. Ganti item dengan false untuk Wilayah lain di mana AWS Config perekam tidak ada.

1. Arahkan ke CloudFormation konsol akun manajemen.
2. Buat yang baru StackSet dengan nama CustomerCreatedConfigResourcesForControlTower.
3. Salin dan perbarui template berikut:

> **Note**
>
> CustomerCreatedAggregationAuthorizationSumber daya dalam template tidak diperlukan untuk landing zone versi 4.0 atau lebih tinggi.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config
Resources:
  CustomerCreatedConfigRecorder:
    Type: AWS::Config::ConfigurationRecorder
    Properties:
      Name: aws-controltower-BaselineConfigRecorder-customer-created
      RoleARN: !Sub arn:aws:iam::${AWS::AccountId}:role/aws-controltower-
ConfigRecorderRole-customer-created
      RecordingGroup:
        AllSupported: true
        IncludeGlobalResourceTypes: GLOBAL_RESOURCE_RECORDING
        ResourceTypes: []
  CustomerCreatedConfigDeliveryChannel:
    Type: AWS::Config::DeliveryChannel
    Properties:
      Name: aws-controltower-BaselineConfigDeliveryChannel-customer-created
      ConfigSnapshotDeliveryProperties:
        DeliveryFrequency: TwentyFour_Hours
```

```
      S3BucketName: CONFIG_BUCKET
      S3KeyPrefix: ORGANIZATION_ID
      SnsTopicARN: !Sub arn:aws:sns:${AWS::Region}:AUDIT_ACCOUNT:aws-controltower-
AllConfigNotifications
  CustomerCreatedAggregationAuthorization:
    Type: "AWS::Config::AggregationAuthorization"
    Properties:
      AuthorizedAccountId: AUDIT_ACCOUNT
      AuthorizedAwsRegion: HOME_REGION
```

Perbarui template dengan bidang wajib:

a. Di S3BucketNamelapangan, ganti *CONFIG_BUCKET*

b. Di S3KeyPrefixlapangan, ganti *ORGANIZATION_ID*

c. Di bidang SnsTopicARN, ganti *AUDIT_ACCOUNT*

d. Di AuthorizedAccountIdlapangan, ganti *AUDIT_ACCOUNT*

e. Di AuthorizedAwsRegionlapangan, ganti *HOME_REGION*

4. Selama penyebaran di CloudFormation konsol, tambahkan nomor akun anggota.
5. Tambahkan AWS Wilayah yang diidentifikasi pada Langkah 4.
6. Menyebarkan set tumpukan.

Langkah 7: Daftarkan OU dengan AWS Control Tower

Di dasbor AWS Control Tower, daftarkan OU.

> **Note**
>
> Alur kerja akun Mendaftar tidak akan berhasil untuk tugas ini. Anda harus memilih Register OU atau Re-registerOU.

Menyediakan dan mengelola akun dengan Account Factory

> **Note**
>
> Penyediaan akun tunggal, pembaruan, dan penyesuaian harus menargetkan unit organisasi (OU) dengan AWSControlTowerBaseline diaktifkan. Jika OU tidak mengaktifkan, Anda dapat

mengaktifkan pendaftaran otomatis akun atau menggunakan ResetEnabledControl API EnabledControls pada ResetEnabledBaseline EnabledBaselines dan di OU tersebut untuk mendaftarkan akun. AWSControlTowerBaseline Untuk detailnya AWSControlTowerBaseline, lihat:Jenis dasar yang berlaku di tingkat OU.

Bab ini mencakup ikhtisar dan prosedur untuk menyediakan akun anggota baru di zona pendaratan AWS Control Tower dengan Account Factory.

Izin untuk mengonfigurasi dan menyediakan akun

AWS Control Tower Account Factory memungkinkan administrator dan pengguna cloud AWS IAM Identity Center untuk menyediakan akun di zona pendaratan Anda. Secara default, pengguna Pusat Identitas IAM yang menyediakan akun harus berada di `AWSAccountFactory` grup atau grup manajemen.

> **Note**
>
> Berhati-hatilah saat bekerja dari akun manajemen, seperti yang Anda lakukan saat menggunakan akun apa pun yang memiliki izin di seluruh organisasi Anda.

Akun manajemen AWS Control Tower memiliki hubungan kepercayaan dengan `AWSControlTowerExecution` peran tersebut, yang memungkinkan penyiapan akun dari akun manajemen, termasuk beberapa pengaturan akun otomatis. Untuk informasi selengkapnya tentang `AWSControlTowerExecution` peran, lihat Peran dan akun.

> **Note**
>
> Untuk mendaftarkan akun yang sudah ada Akun AWS ke AWS Control Tower, `AWSControlTowerExecution` peran tersebut harus diaktifkan. Untuk informasi selengkapnya tentang cara mendaftarkan akun yang sudah ada, lihatTentang mendaftarkan akun yang ada.

Untuk informasi selengkapnya tentang izin, lihat Izin diperlukan untuk penyediaan akun.

Pertimbangan untuk mengelola akun di Account Factory

Anda dapat memperbarui, membatalkan pendaftaran, dan menutup akun yang Anda buat dan sediakan melalui Account Factory. Anda dapat mendaur ulang akun dengan memperbarui parameter pengguna di akun yang ingin Anda gunakan kembali. Anda juga dapat mengubah unit organisasi (OU) akun.

> **Note**
>
> Saat memperbarui produk yang disediakan yang terkait dengan akun yang dijual Account Factory, jika Anda menentukan alamat email pengguna baru AWS IAM Identity Center, AWS Control Tower akan membuat pengguna baru di Pusat Identitas IAM. Akun yang dibuat sebelumnya tidak dihapus. Untuk informasi tentang menghapus alamat email pengguna IAM Identity Center sebelumnya dari Pusat Identitas IAM, lihat Menon aktifkan Pengguna.

Memperbarui dan memindahkan akun dengan AWS Control Tower

Cara termudah untuk memperbarui akun terdaftar adalah melalui konsol AWS Control Tower. Pembaruan akun individu berguna untuk menyelesaikan penyimpangan, seperti Akun anggota yang dipindahkan. Pembaruan akun juga diperlukan sebagai bagian dari pembaruan zona pendaratan penuh.

Perbarui akun di konsol

Untuk memperbarui akun di konsol AWS Control Tower

1. Saat masuk ke AWS Control Tower, navigasikan ke halaman Organisasi.
2. Dalam daftar OU dan akun, pilih nama akun yang ingin Anda perbarui. Akun yang tersedia untuk diperbarui menampilkan status Pem baruan tersedia.
3. Selanjutnya Anda akan melihat halaman detail akun untuk akun yang Anda pilih.
4. Di kanan atas, pilih Per barui akun.

Jika Anda memindahkan akun dari satu unit organisasi (OU) ke unit organisasi lainnya, ingatlah bahwa kontrol yang diterapkan oleh OU baru mungkin berbeda dari kontrol di OU sebelumnya. Pastikan kontrol di OU baru memenuhi persyaratan kebijakan Anda untuk akun tersebut.

Akun AWS Control Tower dimodifikasi secara berbeda, tergantung pada apakah Anda telah memilih untuk mendaftar akun secara otomatis atau tidak. Untuk informasi selengkapnya tentang pendaftaran otomatis, lihatSecara opsional mengkonfigurasi pendaftaran otomatis untuk akun.

Kontrol perilaku saat akun dipindahkan
OU, dengan pendaftaran otomatis diaktifkan

Saat Anda memindahkan akun ke OU baru, AWS Control Tower menerapkan garis dasar dan kontrol OU yang diaktifkan ke akun tersebut. Kontrol dan garis dasar dari OU sebelumnya dihapus. Jika Anda memindahkan akun di luar OU yang terdaftar, AWS Control Tower menghapus semua garis dasar dan kontrol yang digunakan.

Kontrol perilaku saat akun dipindahkan
OU, tanpa pendaftaran otomatis

Saat Anda memindahkan akun antar OU, kontrol untuk OU tujuan diterapkan ke akun. Namun, kontrol yang diterapkan ke akun dari OU sebelumnya tidak dihapus. Perilaku kontrol yang tepat khusus untuk implementasi kontrol yang aktif pada OU sebelumnya dan OU tujuan.

- Untuk kontrol yang diimplementasikan dengan AWS Config aturan: Kontrol dari OU sebelumnya tidak dihapus. Kontrol ini harus dihapus secara manual.
- Untuk kontrol yang diimplementasikan dengan SCP: SCP-based Kontrol dari OU sebelumnya adalah
  dihapus. SCP-based Kontrol untuk OU tujuan mulai berlaku pada akun ini.
- Untuk kontrol yang diimplementasikan dengan CloudFormation kait: Per ilaku ini tergantung pada status kontrol di OU baru.
  - Jika OU tujuan tidak memiliki kontrol berbasis kait yang aktif: Yang lama kontrol tetap aktif untuk akun yang dipindahkan, kecuali jika Anda menghapusnya secara manual.
  - Jika OU tujuan memiliki kontrol kait aktif: Kontrol lama adalah dihapus dan kontrol di OU tujuan diterapkan ke akun.

Mengubah alamat email akun yang terdaftar

Untuk mengubah alamat email akun AWS Control Tower yang terdaftar, ikuti prosedur di bagian ini.

> **Mengubah alamat email akun manajemen**
>
> Untuk mengubah alamat email akun AWS manajemen, masuk sebagai pengguna root dengan izin administrator.

Mengubah alamat email dengan menggunakan AWS Organizations

1. Untuk petunjuk tentang memperbarui alamat email pengguna root, lihat Memperbarui alamat email pengguna root untuk akun anggota di Panduan Referensi Manajemen AWS Akun.
2. Setelah memperbarui alamat email, perbarui akun di AWS Control Tower. Pembaruan ini mengaitkan alamat email baru dengan akun di AWS Control Tower. Jika memperbarui akun melalui produk yang disediakan Katalog Layanan, tentukan alamat email lama sebagai nilai `AccountEmail` parameter.

Ubah alamat email dengan menggunakan kredensional pengguna root

1. Pulihkan kata sandi pengguna root untuk akun tersebut. Untuk petunjuk tentang memulihkan kata sandi yang hilang, lihat Bagaimana cara memulihkan kata AWS sandi yang hilang atau terlupakan?
2. Masuk ke akun dengan kata sandi pengguna root.
3. Ubah alamat email seperti yang Anda lakukan untuk yang lain Akun AWS, dan tunggu perubahan berlaku AWS Organizations. Anda mungkin mengalami penundaan saat perubahan alamat email selesai diperbarui.
4. Setelah memperbarui alamat email, perbarui akun di AWS Control Tower. Pembaruan ini mengaitkan alamat email baru dengan akun di AWS Control Tower. Jika memperbarui akun melalui produk yang disediakan Katalog Layanan, tentukan alamat email lama sebagai nilai `AccountEmail` parameter.

Mengubah nama akun yang terdaftar

Ikuti prosedur di bagian ini untuk mengubah nama akun AWS Control Tower yang terdaftar.

> **Note**
>
> Untuk mengubah nama akun AWS administrator, Anda harus memiliki izin admin dan masuk sebagai pengguna root akun.

Untuk mengubah nama akun yang dibuat oleh AWS Control Tower, dengan menggunakan AWS Organizations konsol atau API

- Ikuti petunjuk yang tersedia di Panduan Referensi Manajemen AWS Akun.

Metode alternatif untuk mengubah nama akun yang dibuat oleh AWS Control Tower

1. Pulihkan kata sandi root untuk akun. Anda dapat mengikuti langkah-langkah yang diuraikan dalam artikel ini, Bagaimana cara memulihkan AWS kata sandi yang hilang atau terlupakan?
2. Masuk ke akun dengan kata sandi root.
3. Di AWS Billing konsol, navigasikan ke halaman Pengaturan akun.
4. Ubah nama di Peng aturan akun, seperti yang Anda lakukan untuk yang lain Akun AWS.
5. AWS Control Tower memperbarui dirinya secara otomatis untuk mencerminkan perubahan nama. Pembaruan ini tidak akan tercermin dalam produk yang disediakan di AWS Service Catalog.

Konfigurasikan Pabrik Akun dengan pengaturan Amazon Virtual Private Cloud

Account Factory memungkinkan Anda membuat garis dasar dan opsi konfigurasi yang telah disetujui sebelumnya untuk akun di organisasi Anda. Anda dapat mengonfigurasi dan menyediakan akun baru melalui AWS Service Catalog.

Pada halaman Account Factory, Anda dapat melihat daftar unit organisasi (OU) dan status daftar izin mereka. Secara default, semua OU ada di daftar izinkan, yang berarti bahwa akun dapat disediakan di bawahnya. Anda dapat menonaktifkan OU tertentu untuk penyediaan akun. AWS Service Catalog

Anda dapat melihat opsi konfigurasi Amazon VPC yang tersedia untuk pengguna akhir Anda saat mereka menyediakan akun baru.

Untuk mengkonfigurasi pengaturan Amazon VPC di Account Factory

1. Sebagai administrator cloud pusat, masuk ke konsol AWS Control Tower dengan izin administrator di akun manajemen.
2. Dari sisi kiri dasbor, pilih Ac count Factory untuk menavigasi ke halaman konfigurasi jaringan Account Factory. Di sana Anda dapat melihat pengaturan jaringan default yang ditampilkan. Untuk mengedit, pilih Edit dan lihat versi pengaturan konfigurasi jaringan Account Factory yang dapat diedit.
3. Anda dapat memodifikasi setiap bidang pengaturan default sesuai kebutuhan. Pilih opsi konfigurasi VPC yang ingin Anda buat untuk semua akun Pabrik Akun baru yang dapat dibuat pengguna akhir Anda, dan masukkan pengaturan Anda ke dalam bidang.

- Pilih dinon aktifkan atau diaktifkan untuk membuat subnet publik di Amazon VPC. Secara default, subnet yang dapat diakses internet tidak diizinkan.

  > **Note**
  >
  > Jika Anda menyetel konfigurasi VPC pabrik akun sehingga subnet publik di aktifkan saat menyediakan akun baru, pabrik akun mengonfigurasi Amazon VPC untuk membuat NAT Gateway. https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html Anda akan ditagih untuk penggunaan Anda oleh Amazon VPC. Lihat Harga VPC untuk informasi selengkapnya.

- Pilih jumlah maksimum subnet pribadi di Amazon VPC dari daftar. Secara default, 1 dipilih. Jumlah maksimum subnet pribadi yang diizinkan adalah 2 per zona ketersediaan.
- Masukkan rentang alamat IP untuk membuat VPC akun Anda. Nilai harus dalam bentuk blok routing antar-domain (CIDR) tanpa kelas (misalnya, defaultnya adalah). `172.31.0.0/16` Blok CIDR ini menyediakan rentang keseluruhan alamat IP subnet untuk VPC yang dibuat Account Factory untuk akun Anda. Dalam VPC Anda, subnet ditetapkan secara otomatis dari rentang yang Anda tentukan, dan ukurannya sama. Secara default, subnet dalam VPC Anda tidak tumpang tindih. Namun, rentang alamat IP subnet di VPC dari semua akun yang disediakan dapat tumpang tindih.
- Pilih wilayah atau semua wilayah untuk membuat VPC saat akun disediakan. Secara default semua wilayah yang tersedia dipilih.
- Dari daftar, pilih jumlah Zona Ketersediaan untuk mengkonfigurasi subnet di setiap VPC. Nomor default dan yang disarankan adalah 3.

- Pilih Simpan.

Anda dapat mengatur opsi konfigurasi ini untuk membuat akun baru yang tidak menyertakan VPC. Lihat pandu annya.

Membatalkan pendaftaran akun

Jika Anda membuat akun di Account Factory atau men daftarkan akun Akun AWS, dan Anda tidak lagi ingin akun tersebut dikelola oleh AWS Control Tower di zona pendaratan, Anda dapat membatalkan pendaftaran akun dari konsol AWS Control Tower.

Saat Anda membatalkan pendaftaran akun AWS Control Tower, semua sumber daya yang disediakan oleh AWS Control Tower dihapus, termasuk kontrol dan cetak biru apa pun. Akun dipindahkan dari OU Menara Kontrol AWS mana pun dan masuk ke area Root. Akun tidak lagi menjadi bagian dari OU terdaftar, dan tidak lagi tunduk pada AWS Control Tower SCP. Anda dapat menutup akun melalui AWS Organizations.

Untuk membatalkan pendaftaran akun terdaftar dari konsol AWS Control Tower

1. Buka konsol AWS Control Tower di browser web Anda di https://console.aws.amazon.com/controltower
2. Di panel navigasi kiri, pilih Organisasi.
3. Di halaman Organisasi, perluas OU yang berisi akun, dengan memilih tombol + di dekat OU.
4. Pilih akun dan kemudian pilih Batalkan kel ola.

> **Note**
>
> Tunggu status akun ditampilkan Tidak terdaftar.

Jika Anda tidak lagi membutuhkan akun, tutuplah. Untuk informasi selengkapnya tentang menutup AWS akun, lihat Menutup akun di Panduan AWS Billing Pengguna

> **Batalkan pendaftaran akun saat pendaftaran otomatis aktif**
>
> Jika kemampuan pendaftaran otomatis aktif di halaman Pengaturan, Anda juga dapat membatalkan pendaftaran akun dengan mem indahkannya ke OU yang tidak terdaftar di

AWS Control Tower. Semua sumber daya AWS Control Tower dihapus. Ketahuilah bahwa Anda tidak membatalkan pendaftaran akun secara tidak sengaja dengan cara ini. Namun, Anda dapat mendaftarkan ulang akun dengan mengembalikannya ke OU.

Saat Anda membatalkan pendaftaran akun khusus, AWS Control Tower menghapus sumber daya yang telah digunakan zona pendaratan, serta sumber daya lain yang dibuat AWS Control Tower di dalam akun. AWS Control Tower juga menghapus AWSControlTowerExecution peran, bahkan jika itu ditambahkan secara manual. Menghapus peran ini sejalan dengan prinsip hak istimewa terkecil, karena peran eksekusi layanan tidak boleh tetap berada di akun yang tidak dikelola.

Setelah Anda membatalkan pendaftaran akun, Anda dapat menutup akun melalui AWS Organizations.

Note

Akun yang tidak terdaftar tidak ditutup atau dihapus. Ketika akun telah dibatalkan pendaftaran, pengguna Pusat Identitas IAM yang Anda pilih saat membuat akun di Account Factory masih memiliki akses administratif ke akun tersebut. Jika Anda tidak ingin pengguna ini memiliki akses administratif, Anda harus mengubah pengaturan ini di Pusat Identitas IAM dengan memperbarui akun di Pabrik Akun dan mengubah alamat email pengguna Pusat Identitas IAM untuk akun tersebut. Untuk informasi selengkapnya, lihat Memperbarui dan memindahkan akun dengan AWS Control Tower.

Panduan video

Video ini (3:25) menjelaskan cara menghapus akun dari AWS Control Tower, mendapatkan akses root ke akun, dan akhirnya menutup. Akun AWS Anda juga dapat menutup akun dengan AWS Organizations API. Untuk tampilan yang lebih baik, pilih ikon di sudut kanan bawah video untuk memperbesarnya ke layar penuh. Keterangan tersedia.

Panduan Video Menutup Akun di Menara Kontrol AWS.

Tutup akun yang dibuat di Account Factory

Akun yang dibuat di Account Factory adalah Akun AWS. Untuk informasi tentang penutupan Akun AWS, lihat Menutup AWS akun di Panduan Referensi Manajemen Akun .

> **Note**
>
> Menutup akun Akun AWS tidak sama dengan membatalkan pendaftaran akun dari AWS Control Tower—ini adalah tindakan terpisah. Anda harus membatalkan pendaftaran akun sebelum menutupnya.

Menutup akun anggota AWS Control Tower melalui AWS Organizations

Anda dapat menutup akun anggota AWS Control Tower dari akun manajemen organisasi Anda tanpa perlu masuk ke setiap akun anggota secara individual dengan kredenSIAL root, melalui AWS Organizations. Namun, Anda tidak dapat menutup akun manajemen Anda dengan cara ini.

Saat Anda memang AWS Organizations CloseAccount gil API, atau menutup akun di AWS Organizations konsol, akun anggota diisolasi selama 90 hari, Akun AWS seperti halnya. Akun menunjukkan status Dit angguhkan di Menara Kontrol AWS dan AWS Organizations. Jika Anda mencoba bekerja dengan akun selama 90 hari tersebut, AWS Control Tower memberikan pesan kesalahan.

> **Note**
>
> Jika OU telah menangguhkan akun, EnabledControl operasi akan gagal untuk kontrol regional pada target.

Sebelum 90 hari berakhir, Anda dapat memulihkan akun anggota, seperti yang dapat Anda lakukan dengan apa pun Akun AWS. Setelah waktu 90 hari itu, catatan akun dihapus.

Kami menyarankan, sebagai praktik terbaik, untuk membatalkan pendaftaran akun anggota sebelum Anda menutup akun tersebut. Jika Anda menutup akun anggota tanpa terlebih dahulu menghapus pengelolaannya, AWS Control Tower akan menampilkan status akun tersebut sebagai Dit angguhkan, tetapi juga sebagai Terdaftar. Akibatnya, jika Anda mencoba ke Re-register OU akun selama waktu 90 hari tersebut, AWS Control Tower akan menghasilkan pesan kesalahan. Akun yang ditangguhkan pada dasarnya memblokir tindakan pendaftaran ulang dengan kegagalan pra-pemeriksaan. Jika Anda menghapus akun dari OU, Anda dapat Re-register menggunakan OU, tetapi AWS dapat menghasilkan kesalahan terkait metode pembayaran yang hilang untuk akun tersebut. Untuk mengatasi kendala ini, buat OU lain, dan pindahkan akun ke OU tersebut sebelum

Anda mencoba mendaftar ulang. Kami merekomendasikan menamai OU ini sebagai OU yang Ditangguhkan.

> **Note**
>
> Jika Anda tidak membatalkan pendaftaran akun sebelum menutupnya, Anda harus menghapus produk yang disediakan akun AWS Service Catalog setelah 90 hari tersebut selesai.

Untuk informasi selengkapnya, lihat AWS Organizations dokumentasi tentang CloseAccount API.

Pertimbangan Sumber Daya untuk Pabrik Akun

Saat akun disediakan dengan Account Factory, AWS sumber daya berikut dibuat di dalam akun.

AWS layanan	Tipe sumber daya	Nama sumber daya
AWS CloudFormation	Tumpukan	StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL-*(Tidak digunakan di zona pendaratan versi 3.0 dan yang lebih baru) StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-* StackSet-AWSControlTowerBP-BASELINE-CONFIG-* StackSet-AWSControlTowerBP-BASELINE-ROLES-* StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES-*

AWS layanan	Tipe sumber daya	Nama sumber daya
AWS CloudTrail	Jejak	aws-controltower-BaselineCloudTrail
AWS Config	Saluran pengiriman	aws-controltower-BaselineConfigDeliveryChannel
AWS Config	Perekam	aws-controltower-BaselineConfigRecorder
Amazon CloudWatch	CloudWatch Log	/aws/lambda/aws-controltower-NotificationForwarder
AWS Identity and Access Management	Peran	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole(Tidak digunakan di zona pendaratan versi 3.0 dan yang lebih baru) aws-controltower-ConfigRecorderRole(Tidak digunakan di zona pendaratan versi 2.8 dan yang lebih baru) aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole AWSControlTowerExecution
AWS Identity and Access Management	Kebijakan	AWSControlTowerServiceRolePolicy
Layanan Notifikasi Sederhana Amazon	Topik	aws-controltower-SecurityNotifications

AWS layanan	Tipe sumber daya	Nama sumber daya
AWS Lambda	Aplikasi	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*
AWS Lambda	Fungsi	aws-controltower-NotificationForwarder
Amazon EventBridge	Aturan	AWSControlTowerManagedRule
Amazon EventBridge	Aturan	aws-controltower-ConfigComplianceChangeEventRule

Sesuaikan akun dengan Kustomisasi Pabrik Akun (AFC)

> **Note**
>
> Penyediaan akun tunggal, pembaruan, dan penyesuaian harus menargetkan unit organisasi (OU) dengan AWSControlTowerBaseline diaktifkan. Jika OU tidak mengaktifkan, Anda dapat mengaktifkan pendaftaran otomatis akun atau menggunakan ResetEnabledControl API EnabledControls pada ResetEnabledBaseline EnabledBaselines dan di OU tersebut untuk mendaftarkan akun. AWSControlTowerBaseline Untuk detailnya AWSControlTowerBaseline, lihat:Jenis dasar yang berlaku di tingkat OU.

AWS Control Tower memungkinkan Anda menyesuaikan yang baru dan yang sudah ada Akun AWS saat Anda menyediakan sumber daya mereka dari konsol AWS Control Tower. Setelah Anda mengatur kustomisasi Account Factory, AWS Control Tower mengotomatiskan proses ini untuk penyediaan di masa mendatang, sehingga Anda tidak perlu memelihara pipeline apa pun. Akun yang disesuaikan tersedia untuk digunakan segera setelah sumber daya disediakan.

Menyediakan akun baru dengan cetak biru

Akun kustom Anda disediakan di Pabrik Akun AWS Control Tower, melalui CloudFormation templat, atau dengan Terraform. Anda akan menentukan template yang berfungsi sebagai cetak biru akun yang disesuaikan. Cetak biru Anda menjelaskan sumber daya dan konfigurasi tertentu yang Anda

perlukan saat akun disediakan. Pre-defined cetak biru, dibangun dan dikelola oleh AWS mitra, juga tersedia. Untuk informasi selengkapnya tentang cetak biru yang dikelola mitra, lihat Perpustakaan Mem AWS Service Catalog ulai.

Menerapkan cetak biru ke akun yang ada

Anda juga dapat menerapkan cetak biru khusus ke akun yang ada, dengan mengikuti langkah-langkah Per barui akun di konsol AWS Control Tower. Lihat perinciannya di Perbarui akun di konsol.

Definisi: Akun hub Anda

Cetak biru akun Anda disimpan dalam Akun AWS, yang untuk tujuan kami disebut sebagai akun hub. Cetak biru disimpan dalam bentuk produk Katalog Layanan. Kami menyebut produk ini cetak biru, untuk membedakannya dari produk Katalog Layanan lainnya. Untuk mempelajari selengkapnya tentang cara membuat produk Katalog Layanan, lihat Membuat produk di Panduan AWS Service Catalog Administrator.

> **Note**
>
> AWS Control Tower berisi kontrol proaktif, yang memantau CloudFormation sumber daya di AWS Control Tower. Secara opsional, Anda dapat mengaktifkan kontrol ini di zona pendaratan Anda. Saat Anda menerapkan kontrol proaktif, mereka memeriksa untuk memastikan bahwa sumber daya yang akan Anda terapkan ke akun Anda sesuai dengan kebijakan dan prosedur organisasi Anda. Untuk informasi selengkapnya tentang kontrol proaktif, lihat Kontrol proaktif.

Untuk informasi selengkapnya tentang bekerja dengan AFC, lihat Men gotomatiskan kustomisasi akun menggunakan Kustomisasi Pabrik Akun di AWS Control Tower.

> **Prasyarat**
>
> Sebelum mulai membuat akun khusus dengan AWS Control Tower Account Factory, Anda harus memiliki lingkungan zona pendaratan AWS Control Tower yang digunakan, dan Anda harus memiliki unit organisasi (OU) yang terdaftar di AWS Control Tower, tempat akun yang baru dibuat akan ditempatkan.

Persiapan untuk kustomisasi

- Tentukan akun hub: Anda dapat membuat akun baru untuk berfungsi sebagai akun hub, atau Anda dapat menggunakan akun yang sudah ada Akun AWS. Kami sangat menyarankan agar Anda tidak menggunakan akun manajemen AWS Control Tower sebagai akun hub cetak biru Anda.
- Tambahkan peran yang diperlukan: Jika Anda berencana untuk mendaftar Akun AWS ke AWS Control Tower dan menyesuaikannya, Anda harus terlebih dahulu menambahkan `AWSControlTowerExecution` peran ke akun tersebut, seperti yang Anda lakukan untuk akun lain yang Anda daftarkan ke AWS Control Tower.
- Konfigurasikan cetak biru mitra (opsional): Jika Anda berencana untuk menggunakan cetak biru mitra yang memiliki persyaratan langganan pasar, Anda harus mengonfigurasinya dari akun manajemen AWS Control Tower sebelum menerapkan cetak biru mitra sebagai cetak biru kustomisasi pabrik akun.

Topik

- Siapkan untuk penyesuaian
- Buat akun yang disesuaikan dari cetak biru
- Sesuaikan akun dengan AFC saat Anda mendaftarkannya
- Menambahkan cetak biru ke akun AWS Control Tower
- Memperbarui cetak biru
- Menghapus cetak biru dari akun
- Cetak biru mitra
- Pertimbangan untuk Kustomisasi Pabrik Akun (AFC)
- Jika terjadi kesalahan cetak biru
- Menyesuaikan dokumen kebijakan Anda untuk cetak biru AFC berdasarkan CloudFormation
- Izin tambahan diperlukan untuk membuat produk Katalog Terraform-based Layanan
- Transisi ke AWS Service Catalog Jenis produk eksternal

Siapkan untuk penyesuaian

Bagian selanjutnya memberikan langkah-langkah untuk mengatur Account Factory untuk proses penyesuaian. Sebaiknya siapkan admin yang dideleg asikan untuk akun hub, sebelum memulai langkah-langkah ini.

Ringkasan

- Langkah 1. Buat peran yang diperlukan. Buat peran IAM yang memberikan izin bagi AWS Control Tower untuk memiliki akses ke akun (hub), tempat produk Katalog Layanan, juga disebut cetak biru, disimpan.
- Langkah 2. Buat AWS Service Catalog produk. Buat AWS Service Catalog produk (juga disebut “produk cetak biru”) yang Anda perlukan untuk mendasari akun kustom.
- Langkah 3. Tinjau cetak biru kustom Anda. Periksa AWS Service Catalog produk (cetak biru) yang Anda buat.
- Langkah 4. Hubungi cetak biru Anda untuk membuat akun yang disesuaikan. Masukkan informasi produk cetak biru dan informasi peran ke bidang yang tepat di Account Factory, di konsol AWS Control Tower, saat membuat akun.

Langkah 1. Buat peran yang dibutuhkan

Sebelum mulai menyesuaikan akun, Anda harus menyiapkan peran yang berisi hubungan kepercayaan antara AWS Control Tower dan akun hub Anda. Jika diasumsikan, peran tersebut memberikan akses Menara Kontrol AWS untuk mengelola sumber daya di akun hub. Peran harus diberi nama AWSControlTowerBlueprintAccess.

AWS Control Tower mengambil peran ini untuk membuat sumber daya Portofolio atas nama Anda di AWS Service Catalog, kemudian menambahkan cetak biru Anda sebagai Produk Katalog Layanan ke Portofolio ini, dan kemudian membagikan Portofolio ini, dan cetak biru Anda, dengan akun anggota Anda selama penyediaan akun.

Anda akan membuat `AWSControlTowerBlueprintAccess` peran, seperti yang dijelaskan di bagian berikut. Anda dapat mengatur peran di akun terdaftar atau tidak terdaftar.

Arahkan ke konsol IAM untuk mengatur peran yang diperlukan.

Untuk mengatur AWSControlTowerBlueprintAccess peran dalam akun AWS Control Tower yang terdaftar

1. Gabungkan atau masuk sebagai kepala sekolah di akun manajemen AWS Control Tower.
2. Dari prinsipal federasi di akun manajemen, ambil atau alihkan peran ke `AWSControlTowerExecution` peran dalam akun AWS Control Tower terdaftar yang Anda pilih untuk difungsikan sebagai akun hub cetak biru.
3. Dari `AWSControlTowerExecution` peran di akun AWS Control Tower terdaftar, buat `AWSControlTowerBlueprintAccess` peran dengan izin yang tepat dan hubungan kepercayaan.

> **Important**
>
> Untuk mematuhi panduan praktik AWS terbaik, penting bagi Anda untuk keluar dari `AWSControlTowerExecution` peran segera setelah Anda membuat `AWSControlTowerBlueprintAccess` peran.
> Untuk mencegah perubahan sumber daya yang tidak diinginkan, `AWSControlTowerExecution` peran ini dimaksudkan untuk digunakan oleh AWS Control Tower saja.

Jika akun hub cetak biru Anda tidak terdaftar di AWS Control Tower, `AWSControlTowerExecution` peran tersebut tidak akan ada di akun, dan Anda tidak perlu mengasumsikannya sebelum Anda melanjutkan pengaturan `AWSControlTowerBlueprintAccess` peran.

Cara mengatur AWSControlTowerBlueprintAccess peran dalam akun anggota yang tidak terdaftar

1. Gabungkan atau masuk sebagai kepala sekolah di akun yang ingin Anda tentukan sebagai akun hub, melalui metode pilihan Anda.
2. Saat masuk sebagai kepala sekolah di akun, buat `AWSControlTowerBlueprintAccess` peran dengan izin yang tepat dan hubungan kepercayaan.

AWSControlTowerBlueprintAccessPeran harus diatur untuk memberikan kepercayaan kepada dua kepala sekolah:

- Prinsipal (pengguna) yang menjalankan AWS Control Tower di akun manajemen AWS Control Tower.

- Peran yang disebutkan `AWSControlTowerAdmin` dalam akun manajemen AWS Control Tower.

Berikut adalah contoh kebijakan kepercayaan, mirip dengan yang perlu Anda sertakan untuk peran Anda. Kebijakan ini menunjukkan praktik terbaik pemberian akses hak istimewa terkecil. Saat membuat kebijakan sendiri, ganti istilah tersebut *`YourManagementAccountId`* dengan ID akun akun manajemen AWS Control Tower yang sebenarnya, dan ganti istilah tersebut *`YourControlTowerUserRole`* dengan pengenal peran IAM untuk akun manajemen Anda.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/service-role/
AWSControlTowerAdmin",
                    "arn:aws:iam::111122223333:role/YourControlTowerUserRole"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Kebijakan izin yang diperlukan

AWS Control Tower mengharuskan kebijakan terkelola yang diberi `AWSServiceCatalogAdminFullAccess` nama harus dilampirkan ke `AWSControlTowerBlueprintAccess` peran. Kebijakan ini memberikan izin yang AWS Service Catalog dicari kapan AWS Control Tower dapat mengelola portofolio dan sumber daya AWS Service Catalog Produk Anda. Anda dapat melampirkan kebijakan ini saat membuat peran di konsol IAM.

Izin tambahan mungkin diperlukan

- Jika Anda menyimpan cetak biru di Amazon S3, AWS Control Tower juga memerlukan kebijakan `AmazonS3ReadOnlyAccess` izin untuk `AWSControlTowerBlueprintAccess` peran tersebut.
- Jenis produk AWS Service Catalog Terraform mengharuskan Anda menambahkan beberapa izin tambahan ke kebijakan IAM kustom AFC, jika Anda tidak menggunakan kebijakan Admin default. Ini membutuhkan ini selain izin yang diperlukan untuk membuat sumber daya yang Anda tentukan di template terraform Anda.

Langkah 2. Buat AWS Service Catalog produk

Untuk membuat AWS Service Catalog produk, ikuti langkah-langkah di Membuat produk di Panduan AWS Service Catalog Administrator. Anda akan menambahkan cetak biru akun Anda sebagai template saat Anda membuat AWS Service Catalog produk.

Important

Sebagai hasil dari HashiCorp lisensi Terraform yang diperbarui, AWS Service Catalog mengubah dukungan untuk produk Terraform Open Source dan produk yang disediakan ke jenis produk baru, yang disebut Eksternal. Untuk mempelajari selengkapnya tentang bagaimana perubahan ini mempengaruhi AFC, termasuk cara memperbarui cetak biru akun Anda yang ada ke jenis produk Eksternal, tinjau Trans isi ke Jenis produk Eksternal.

Ringkasan langkah-langkah untuk membuat cetak biru

- Buat atau unduh CloudFormation template atau file konfigurasi Terraform tar.gz yang akan menjadi cetak biru akun Anda. Beberapa contoh template diberikan nanti di bagian ini.
- Masuk ke Akun AWS tempat Anda menyimpan cetak biru Account Factory Anda (kadang-kadang disebut akun hub).
- Arahkan ke AWS Service Catalog konsol. Pilih Daftar produk, lalu pilih Unggah produk baru.
- Di panel Detail produk, masukkan detail untuk produk cetak biru Anda, seperti nama dan deskripsi.

- Pilih Gunakan file template dan kemudian pilih Pilih file. Pilih atau tempel template atau file konfigurasi yang telah Anda kembangkan atau unduh untuk digunakan sebagai cetak biru Anda.
- Pilih Buat produk di bagian bawah halaman konsol.

Anda dapat mengunduh CloudFormation template dari repositori arsitektur AWS Service Catalog referensi. Salah satu contoh dari repositori itu membantu menyiapkan rencana cadangan untuk sumber daya Anda.

Berikut contoh template, untuk perusahaan fiktif bernama Best Pets. Ini membantu mengatur koneksi ke database hewan peliharaan mereka.

```
Resources:
  ConnectionStringGeneratorLambdaRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - lambda.amazonaws.com
            Action:
              - "sts:AssumeRole"
  ConnectionStringGeneratorLambda:
    Type: AWS::Lambda::Function
    Properties:
      FunctionName: !Join ['-', ['ConnectionStringGenerator', !Select [4, !Split
['-', !Select [2, !Split ['/', !Ref AWS::StackId]]]]]]
      Description: Retrieves the connection string for this account to access the Pet
 Database
      Role: !GetAtt ConnectionStringGeneratorLambdaRole.Arn
      Runtime: nodejs22.x
      Handler: index.handler
      Timeout: 5
      Code:
        ZipFile: >
           export const handler = async (event, context) => {
             const awsAccountId = context.invokedFunctionArn.split(“:”)[4]
             const connectionString= “fake connection for account ” + awsAccountId;
             const response = {
               statusCode: 200,
```

```
              body: connectionString
            };
          return response;
        };

ConnectionString:
  Type: Custom::ConnectionStringGenerator
  Properties:
    ServiceToken: !GetAtt ConnectionStringGeneratorLambda.Arn

PetDatabaseConnectionString:
  DependsOn: ConnectionString
  # For example purposes we're using SSM parameter store.
  # In your template, use secure alternatives to store
  # sensitive values such as connection strings.
  Type: AWS::SSM::Parameter
  Properties:
    Name: pet-database-connection-string
    Description: Connection information for the BestPets pet database
    Type: String
    Value: !GetAtt ConnectionString.Value
```

Langkah 3. Tinjau cetak biru kustom Anda

Anda dapat melihat cetak biru Anda di AWS Service Catalog konsol. Untuk informasi selengkapnya, lihat M engelola produk di Panduan Adminstrator Katalog Layanan.

Langkah 4. Hubungi cetak biru Anda untuk membuat akun yang disesuaikan

Saat mengikuti alur kerja Buat akun di konsol AWS Control Tower, Anda akan melihat bagian opsional tempat Anda dapat memasukkan informasi tentang cetak biru yang ingin Anda gunakan untuk menyesuaikan akun.

Prasyarat

Anda harus menyiapkan akun hub penyesuaian dan menambahkan setidaknya satu cetak biru (produk Katalog Layanan) sebelum Anda dapat memasukkan informasi tersebut ke konsol AWS Control Tower dan mulai menyediakan akun yang disesuaikan.

Buat atau perbarui akun yang disesuaikan di konsol AWS Control Tower.

1. Masukkan ID akun untuk akun yang berisi cetak biru Anda.
2. Dari akun itu, pilih produk Katalog Layanan yang ada (cetak biru yang ada).
3. Pilih versi cetak biru yang tepat (produk Katalog Layanan), jika Anda memiliki lebih dari satu versi.
4. (Opsional) Anda dapat menambahkan atau mengubah kebijakan penyediaan cetak biru pada saat proses ini. Kebijakan penyediaan cetak biru ditulis dalam JSON dan dilampirkan ke peran IAM, sehingga dapat menyediakan sumber daya yang ditentukan dalam template cetak biru. AWS Control Tower membuat peran ini di akun anggota sehingga Katalog Layanan dapat menyebarkan sumber daya menggunakan kumpulan CloudFormation tumpukan. Peran ini bernama `AWSControlTower-BlueprintExecution-bp-`*`xxxx`*. `AdministratorAccess`Kebijakan diterapkan di sini secara default.
5. Pilih Wilayah AWS atau Wilayah tempat Anda ingin menerapkan akun berdasarkan cetak biru ini.
6. Jika cetak biru berisi parameter, Anda dapat memasukkan nilai parameter ke bidang tambahan di alur kerja AWS Control Tower. Nilai tambahan mungkin termasuk: nama GitHub repositori, GitHub cabang, nama cluster Amazon ECS, dan GitHub identitas untuk pemilik repositori.
7. Anda dapat menyesuaikan akun di lain waktu dengan mengikuti proses pembaruan akun, jika akun hub atau cetak biru Anda belum siap.

Untuk detail selengkapnya, lihat Buat akun yang disesuaikan dari cetak biru.

Buat akun yang disesuaikan dari cetak biru

Setelah membuat cetak biru khusus, Anda dapat mulai membuat akun khusus di pabrik akun AWS Control Tower.

Ikuti langkah-langkah berikut untuk menerapkan cetak biru khusus saat Anda membuat yang baru AWS akun:

1. Buka Menara Kontrol AWS di Konsol Manajemen AWS.
2. Pilih Pabrik akun dan Buat akun.
3. Masukkan detail akun seperti nama akun dan alamat email.
4. Konfigurasikan detail Pusat Identitas IAM dengan alamat email dan nama pengguna.
5. Pilih OU terdaftar tempat akun Anda akan ditambahkan.

6. Perluas bagian kustomisasi pabrik akun.
7. Masukkan ID akun akun hub cetak biru yang berisi produk Katalog Layanan Anda dan pilih Validasi. Untuk informasi selengkapnya tentang akun hub cetak biru, lihatSesuaikan akun dengan Kustomisasi Pabrik Akun (AFC).
8. Pilih menu dropdown yang berisi semua cetak biru dari Daftar Produk Katalog Layanan Anda (semua cetak biru khusus dan mitra). Pilih cetak biru dan versi yang sesuai untuk diterapkan.
9. Jika cetak biru Anda berisi parameter, bidang ini ditampilkan untuk Anda isi. Nilai default sudah terisi sebelumnya.
10. Terakhir, pilih tempat Anda akan menerapkan cetak biru Anda, baik Wilayah Rumah atau Semua Wilayah yang diatur. Sumber daya global seperti Route 53 atau IAM, mungkin perlu dikerahkan ke satu Wilayah saja. Sumber daya regional, seperti instans Amazon EC2 atau bucket Amazon S3, dapat digunakan ke semua Wilayah yang diatur
11. Setelah semua bidang selesai, pilih Buat akun.

> **Note**
>
> Cetak biru yang dibuat dengan Terraform dapat diterapkan ke satu Wilayah saja, bukan beberapa Wilayah.

Anda dapat melihat kemajuan penyediaan akun Anda di halaman Organisasi. Ketika penyediaan akun Anda selesai, sumber daya yang ditentukan oleh cetak biru Anda sudah digunakan di dalamnya. Untuk melihat detail akun dan cetak biru, buka halaman detail akun.

Sesuaikan akun dengan AFC saat Anda mendaftarkannya

Untuk mendaftarkan dan menyesuaikan akun di konsol AWS Control Tower.

1. Arahkan ke konsol AWS Control Tower dan pilih Organisasi dari navigasi kiri.
2. Anda akan melihat daftar akun yang tersedia. Identifikasi akun yang ingin Anda daftarkan dengan cetak biru khusus. Kol om Negara untuk akun tersebut harus mencerminkan akun dalam status Tidak terdaftar.
3. Pilih tombol radio di sebelah kiri akun dan pilih menu tarik - turun Tindakan, di kanan atas layar. Di sini Anda akan memilih opsi Daftar.
4. Lengkapi bagian Konfigurasi Akses dengan informasi Pusat Identitas IAM akun.

5. Pilih OU terdaftar tempat akun Anda akan menjadi anggota.
6. Lengkapi bagian kustomisasi pabrik akun menggunakan langkah yang sama seperti 7-12 dari prosedur Buat akun. Untuk informasi selengkapnya, lihat Penyediaan Akun Akun Akun dengan AWS Service Catalog.

Anda dapat melihat status kemajuan akun Anda di halaman Organisasi. Ketika pendaftaran akun Anda selesai, sumber daya yang ditentukan oleh cetak biru sudah digunakan di dalamnya.

Menambahkan cetak biru ke akun AWS Control Tower

Untuk menambahkan cetak biru ke akun anggota AWS Control Tower yang ada, ikuti alur kerja Per barui akun di konsol AWS Control Tower, dan pilih cetak biru baru untuk ditambahkan ke akun. Untuk informasi selengkapnya, lihat Memper barui dan memindahkan akun Account Factory dengan AWS Control Tower atau dengan AWS Service Catalog.

> **Note**
>
> Jika Anda menambahkan cetak biru baru ke akun, cetak biru yang ada akan diganti.

> **Note**
>
> Satu cetak biru dapat digunakan per akun AWS Control Tower.

Memperbarui cetak biru

Prosedur berikut menjelaskan cara memperbarui cetak biru khusus dan cara menerapkannya.

Untuk memperbarui cetak biru kustom Anda

1. Perbarui CloudFormation template Anda atau file Terraform tar.gz (cetak biru) dengan konfigurasi baru Anda.
2. Simpan cetak biru yang diperbarui sebagai versi baru di AWS Service Catalog.

Untuk menerapkan cetak biru yang diperbarui

1. Arahkan ke halaman Organisasi di konsol AWS Control Tower.

2. Filter halaman Organisasi berdasarkan nama cetak biru dan versi.
3. Ikuti proses Perbarui akun, dan gunakan versi cetak biru terbaru di akun Anda.

Jika pembaruan cetak biru tidak berhasil

AWS Control Tower memungkinkan pembaruan cetak biru saat produk yang disediakan berada di negara bagian`AVAILABLE`. Jika produk yang disediakan dalam `TAINTED` keadaan tertentu, pembaruan akan gagal. Kami merekomendasikan solusi berikut:

1. Di AWS Service Catalog konsol, perbarui produk yang `TAINTED` disediakan secara manual untuk mengubah status menjadi`AVAILABLE`. Untuk informasi selengkapnya, lihat Memperbarui produk yang disediakan.
2. Kemudian, ikuti proses pembaruan akun dari AWS Control Tower untuk memperbaiki kesalahan penerapan cetak biru.

Kami merekomendasikan langkah manual ini karena: Ketika Anda menghapus cetak biru, itu dapat menyebabkan sumber daya di akun anggota dihapus. Menghapus sumber daya dapat memengaruhi beban kerja Anda yang ada. Untuk alasan ini, kami merekomendasikan metode ini daripada cara alternatif untuk memperbarui cetak biru—yaitu dengan menghapus dan mengganti cetak biru asli—terutama jika Anda menjalankan beban kerja produksi.

Menghapus cetak biru dari akun

Untuk menghapus cetak biru dari akun, ikuti alur kerja Per barui akun untuk menghapus cetak biru dan mengembalikan akun ke konfigurasi default Menara Kontrol AWS.

Saat Anda memasukkan al ur kerja Per barui akun di konsol, Anda akan melihat bahwa semua detail akun diisi, dan detail penyesuaian tidak diisi. Jika Anda membiarkan detail AFC ini kosong, AWS Control Tower menghapus cetak biru dari akun. Anda akan melihat pesan peringatan sebelum tindakan dimulai.

> **Note**
>
> AWS Control Tower menambahkan cetak biru ke akun hanya jika Anda memilih cetak biru selama proses Buat akun atau Per barui akun.

Cetak biru mitra

AWS Control Tower Account Factory Customization (AFC) menyediakan akses ke cetak biru kustomisasi yang telah ditentukan sebelumnya yang dibuat dan dikelola oleh Mitra. AWS Cetak biru mitra ini membantu Anda menyesuaikan akun untuk kasus penggunaan tertentu. Cetak biru setiap mitra membantu Anda membuat akun khusus, yang telah dikonfigurasi sebelumnya untuk bekerja dengan penawaran produk dari mitra tertentu.

Untuk melihat daftar lengkap cetak biru mitra AWS Control Tower, buka Pustaka Mem ulai Katalog Layanan di konsol Anda. Cari tipe sumber AWS Control Tower Blueprints.

Pertimbangan untuk Kustomisasi Pabrik Akun (AFC)

- AFC mendukung penyesuaian hanya menggunakan satu produk AWS Service Catalog cetak biru.
- Produk AWS Service Catalog cetak biru harus dibuat di akun hub, dan di Wilayah yang sama dengan Wilayah rumah zona pendaratan AWS Control Tower.
- Per `AWSControlTowerBlueprintAccess` an IAM harus dibuat dengan nama, izin, dan kebijakan kepercayaan yang tepat.
- AWS Control Tower mendukung dua opsi penerapan untuk cetak biru: hanya menerapkan ke Wilayah asal, atau menyebarkan ke semua Wilayah yang diatur oleh AWS Control Tower. Pemilihan Wilayah tidak tersedia.
- Saat Anda memperbarui cetak biru di akun anggota, ID akun hub cetak biru dan produk AWS Service Catalog cetak biru tidak dapat diubah.
- AWS Control Tower tidak mendukung penghapusan cetak biru yang ada dan menambahkan cetak biru baru dalam operasi pembaruan cetak biru tunggal. Anda dapat menghapus cetak biru dan kemudian menambahkan cetak biru baru dalam operasi terpisah.
- AWS Control Tower mengubah perilaku, berdasarkan apakah Anda membuat atau mendaftarkan akun khusus, atau akun yang tidak disesuaikan. Jika Anda tidak membuat atau mendaftarkan akun khusus dengan cetak biru, AWS Control Tower membuat produk yang disediakan Account Factory (melalui Katalog Layanan) di akun manajemen AWS Control Tower. Jika Anda menentukan penyesuaian saat membuat atau mendaftarkan akun dengan cetak biru, AWS Control Tower tidak membuat produk yang disediakan Account Factory di akun manajemen AWS Control Tower.

Jika terjadi kesalahan cetak biru

Kesalahan saat menerapkan cetak biru

Jika terjadi kesalahan selama proses penerapan cetak biru ke akun—baik akun baru atau akun yang sudah ada yang Anda daftarkan ke AWS Control Tower—prosedur pemulihannya sama. Akun akan ada, tetapi tidak disesuaikan, dan tidak terdaftar ke AWS Control Tower. Untuk melanjutkan, ikuti langkah-langkah untuk mendaftarkan akun ke AWS Control Tower, dan tambahkan cetak biru pada saat pendaftaran.

Kesalahan saat membuat **`AWSControlTowerBlueprintAccess`** peran, dan solusinya

Saat membuat `AWSControlTowerBlueprintAccess` peran dari akun AWS Control Tower, Anda harus masuk sebagai kepala sekolah menggunakan `AWSControlTowerExecution` peran tersebut. Jika Anda masuk seperti yang lain, `CreateRole` operasi dicegah oleh SCP, seperti yang ditunjukkan pada artefak berikut:

```
{
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::*:role/AWSControlTowerExecution",
                        "arn:aws:iam::*:role/stacksets-exec-*"
                    ]
                }
            },
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:DeleteRolePermissionsBoundary",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:PutRolePermissionsBoundary",
                "iam:PutRolePolicy",
                "iam:UpdateAssumeRolePolicy",
                "iam:UpdateRole",
                "iam:UpdateRoleDescription"
            ],
            "Resource": [
                "arn:aws:iam::*:role/aws-controltower-*",
                "arn:aws:iam::*:role/*AWSControlTower*",
                "arn:aws:iam::*:role/stacksets-exec-*"
            ],
            "Effect": "Deny",
            "Sid": "GRIAMROLEPOLICY"
```

```
        }
```

Solusi berikut tersedia:

- (Paling direkomendasikan) Asumsikan `AWSControlTowerExecution` peran dan buat `AWSControlTowerBlueprintAccess` peran. Jika Anda memilih solusi ini, pastikan untuk keluar dari `AWSControlTowerExecution` peran segera setelahnya, untuk mencegah perubahan sumber daya yang tidak diinginkan.
- Masuk ke akun yang tidak terdaftar di AWS Control Tower, dan karenanya tidak tunduk pada SCP ini.
- Edit sementara SCP ini untuk mengizinkan operasi.
- (Sangat tidak disarankan) Gunakan akun manajemen AWS Control Tower Anda sebagai akun hub Anda, sehingga tidak tunduk pada SCP.

Menyesuaikan dokumen kebijakan Anda untuk cetak biru AFC berdasarkan CloudFormation

Saat Anda mengaktifkan cetak biru melalui pabrik akun, AWS Control Tower mengarahkan CloudFormation untuk membuat sebuah StackSet atas nama Anda. CloudFormation memerlukan akses ke akun terkelola Anda untuk membuat CloudFormation tumpukan di StackSet. Meskipun CloudFormation sudah memiliki hak administrator di akun terkelola melalui `AWSControlTowerExecution` peran, peran ini tidak dapat diasumsikan oleh CloudFormation.

Sebagai bagian dari mengaktifkan cetak biru, AWS Control Tower membuat peran di akun anggota, yang CloudFormation dapat diasumsikan untuk menyelesaikan tugas StackSet manajemen. Cara termudah untuk mengaktifkan cetak biru khusus melalui pabrik akun adalah dengan menggunakan kebijakan al low-all, karena kebijakan tersebut kompatibel dengan template cetak biru apa pun.

Namun, praktik terbaik menyarankan Anda harus membatasi izin untuk CloudFormation akun target. Anda dapat memberikan kebijakan khusus, yang diterapkan AWS Control Tower untuk peran yang dibuat CloudFormation untuk digunakan. Misalnya, jika cetak biru Anda membuat Parameter SSM yang disebut som ething-important, Anda dapat memberikan kebijakan berikut:

JSON

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

```
    "Statement": [
        {
            "Sid": "AllowCloudFormationActionsOnStacks",
            "Effect": "Allow",
            "Action": "cloudformation:*",
            "Resource": "arn:aws:cloudformation:*:*:stack/*"
        },
        {
            "Sid": "AllowSsmParameterActions",
            "Effect": "Allow",
            "Action": [
                "ssm:PutParameter",
                 "ssm:DeleteParameter",
                 "ssm:GetParameter",
                 "ssm:GetParameters"
            ],
            "Resource": "arn:*:ssm:*:*:parameter/something-important"
        }
    ]
}
```

Per `AllowCloudFormationActionsOnStacks` nyataan ini diperlukan untuk semua kebijakan kustom AFC; CloudFormation menggunakan peran ini untuk membuat instans tumpukan, oleh karena itu diperlukan izin untuk melakukan CloudFormation tindakan pada tumpukan. `AllowSsmParameterActions`Bagian ini khusus untuk template yang diaktifkan.

Menyelesaikan masalah izin

Saat Anda mengaktifkan cetak biru dengan kebijakan terbatas, Anda mungkin menemukan bahwa tidak ada cukup izin untuk mengaktifkan cetak biru. Untuk mengatasi masalah ini, revisi dokumen kebijakan Anda dan perbarui preferensi cetak biru akun anggota untuk menggunakan kebijakan yang diperbaiki. Untuk memeriksa apakah kebijakan cukup untuk mengaktifkan cetak biru, pastikan CloudFormation izin diberikan, dan Anda dapat membuat tumpukan secara langsung menggunakan peran tersebut.

Izin tambahan diperlukan untuk membuat produk Katalog Terraform-based Layanan

Saat Anda membuat produk AWS Service Catalog Eksternal dengan file konfigurasi Terraform untuk AFC, AWS Service Catalog memerlukan izin tertentu untuk ditambahkan ke kebijakan IAM kustom

AFC Anda, selain izin yang diperlukan untuk membuat sumber daya yang ditentukan dalam template Anda. Jika Anda memilih kebijakan Admin lengkap default, Anda tidak perlu menambahkan izin tambahan ini.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "resource-groups:CreateGroup",
                "resource-groups:ListGroupResources",
                "resource-groups:DeleteGroup",
                "resource-groups:Tag"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "tag:GetResources",
                "tag:GetTagKeys",
                "tag:GetTagValues",
                "tag:TagResources",
                "tag:UntagResources"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": "s3:GetObject",
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
                }
            }
        }
    ]
}
```

Untuk informasi selengkapnya tentang membuat produk Terraform menggunakan jenis produk Eksternal di AWS Service Catalog, lihat Langkah 5: Membuat peran peluncuran di Panduan Administrator Katalog Layanan.

Transisi ke AWS Service Catalog Jenis produk eksternal

AWS Service Catalog mengubah dukungan untuk produk Terraform Open Source dan produk yang disediakan ke jenis produk baru, yang disebut Eksternal. Untuk mempelajari lebih lanjut tentang transisi ini, tinj au Memperbarui produk Terraform Open Source yang ada dan produk yang disediakan ke jenis produk Eksternal di panduan administrator. AWS Service Catalog

Perubahan ini memengaruhi akun yang sudah ada yang Anda buat atau daftarkan dengan kustomisasi pabrik akun AWS Control Tower. Untuk mengalihkan akun ini ke jenis produk Eksternal, Anda perlu membuat perubahan di kedua AWS Service Catalog dan AWS Control Tower.

Untuk transisi ke jenis produk Eksternal

1. Tingkatkan Mesin Referensi Terraform Anda yang ada untuk menyer AWS Service Catalog takan dukungan untuk jenis produk Sumber Terbuka Ek ster nal dan Terraform. Untuk petunjuk tentang memperbarui Mesin Referensi Terraform Anda, tinjau Repositori. AWS Service Catalog GitHub
2. Di AWS Service Catalog, duplikat produk Terraform Open Source (cetak biru) yang ada, dengan duplikat menggunakan jenis produk Eksternal baru. Jangan menghentikan cetak biru Terraform Open Source yang ada.
3. Di AWS Control Tower, perbarui setiap akun menggunakan cetak biru Terraform Open Source untuk menggunakan cetak biru Eksternal yang baru.
    a. Untuk memperbarui cetak biru, Anda harus terlebih dahulu menghapus cetak biru Terraform Open Source sepenuhnya. Untuk detail selengkapnya, tin jau Hapus cetak biru dari akun.
    b. Tambahkan cetak biru Eksternal baru ke akun yang sama. Untuk detail selengkapnya, tinjau Tambahkan cetak biru ke akun AWS Control Tower.
4. Setelah semua akun yang menggunakan cetak biru Terraform Open Source diperbarui ke cetak biru Eksternal, kembalilah AWS Service Catalog dan hentikan produk apa pun yang menggunakan Terraform Open Source sebagai jenis produk.
5. Ke depan, semua akun yang dibuat atau terdaftar menggunakan kustomisasi pabrik akun AWS Control Tower harus mereferensikan cetak biru menggunakan CloudFormation atau jenis produk Eksternal.

Untuk cetak biru yang dibuat menggunakan jenis produk Eksternal, AWS Control Tower hanya mendukung penyesuaian akun yang menggunakan templat Terraform dan mesin referensi Terraform. Untuk mempelajari selengkapnya, tinj au Menyiapkan untuk penyesuaian.

> **Note**
>
> AWS Control Tower tidak mendukung Terraform Open Source sebagai jenis produk saat membuat akun baru. Untuk mempelajari lebih lanjut tentang perubahan ini, tinjau Memperbarui produk Terraform Open Source yang ada dan produk yang disediakan ke jenis produk Eksternal di panduan administrator. AWS Service Catalog AWS Service Catalog akan mendukung pelanggan melalui transisi jenis produk ini, sesuai kebutuhan. Hubungi perwakilan akun Anda untuk meminta bantuan.

Menyediakan akun dengan AWS Control Tower Account Factory untuk Terraform (AFT)

AWS Control Tower Account Factory for Terraform (AFT) mengadopsi GitOps model yang mengotomatiskan proses penyediaan dan pembaruan akun di AWS Control Tower.

Dengan AFT, Anda membuat file permintaan akun Terraform, yang berisi input yang memanggil alur kerja AFT. Setelah penyediaan akun dan pembaruan selesai, alur kerja AFT berlanjut dengan menjalankan kerangka kerja penyediaan akun AFT dan langkah-langkah penyesuaian akun.

AFT tidak memengaruhi kinerja alur kerja di AWS Control Tower. Jika Anda menyediakan akun melalui AFT atau Account Factory, alur kerja backend yang sama akan terjadi.

Prasyarat

> **Note**
>
> Penyediaan akun AFT harus menargetkan unit organisasi (OU) yang AWSControlTowerBaseline diaktifkan di Menara Kontrol AWS. Untuk detailnya AWSControlTowerBaseline, lihat:Jenis dasar yang berlaku di tingkat OU.

Ketika Anda memulai dengan AFT, Anda akan membuat yang berikut:

- Di AWS Control Tower buat OU, lalu akun manajemen AFT, untuk lingkungan AFT Anda. Catat ID akun, sehingga Anda dapat memasukkannya ke dalam `main.tf` file nanti, saat Anda menerapkan AFT dengan modul Terraform. Anda dapat melihat ID akun ini di halaman detail AWS Control Tower Control. Untuk informasi selengkapnya, lihat dokumentasi Terraform.
- Satu atau lebih `git` repositori untuk lingkungan AFT Anda yang sepenuhnya digunakan. Untuk informasi selengkapnya, lihat Post-deployment langkah-langkah untuk AFT.
- Lingkungan AFT yang sepenuhnya digunakan. Untuk informasi selengkapnya, lihat Ring kasan Pabrik Akun Menara Kontrol AWS untuk Terraform (AFT) dan Menye barkan Pabrik Akun Menara Kontrol AWS untuk Terraform (AFT). Lihat juga dokumentasi Terraform.

> **Tip**
>
> Anda dapat membuat akun manajemen AFT dari konsol AWS Control Tower dengan Buat akun. Untuk informasi selengkapnya, lihat Metode penyediaan.
> Selain itu, secara opsional, Anda dapat membuat folder template akun untuk membantu menentukan akun tambahan Anda, di repositori aft-account-customizations.

Untuk akun yang terdaftar melalui Auto Enroll:

- Pembuatan akun baru melalui AFT terus bekerja secara normal.
- Impor akun yang ada memerlukan langkah-langkah tambahan:
  - Daftarkan OU untuk membuat produk yang disediakan yang diperlukan sebelum mengimpor.
  - Register OU akan memancarkan `CreateManagedAccount` dan `UpdateManagedAccount` acara, memungkinkan penyesuaian AFT.

Untuk informasi tentang Wilayah AWS di mana AFT memiliki batasan penerapan, lihat Batasan dan kuota di AWS Control Tower danBatasan kontrol.

Dokumentasi Terraform berisi ikhtisar yang baik tentang cara mengatur AWS Control Tower Account Factory untuk Terraform (AFT).

Ikhtisar Pabrik Akun Menara Kontrol AWS untuk Terraform (AFT)

Account Factory for Terraform (AFT) menyiapkan pipeline Terraform untuk membantu Anda menyediakan dan menyesuaikan akun di AWS Control Tower. AFT memberi Anda keuntungan

penyedi Terraform-based aan akun sambil memungkinkan Anda mengatur akun Anda dengan AWS Control Tower.

Dengan AFT Anda membuat file permintaan akun Terraform untuk mendapatkan input yang memicu alur kerja AFT untuk penyediaan akun. Setelah tahap penyediaan akun selesai, AFT secara otomatis menjalankan serangkaian langkah sebelum tahap penyesuaian akun dimulai. Untuk informasi selengkapnya, lihat saluran penyediaan akun AFT.

AFT mendukung HCP Terraform, Terraform Enterprise, dan Terraform Community Edition. Dengan AFT Anda dapat memulai pembuatan akun menggunakan file input dan `git push` perintah sederhana dan menyesuaikan akun baru atau yang sudah ada. Pembuatan akun mencakup semua manfaat tata kelola AWS Control Tower dan penyesuaian akun yang membantu Anda memenuhi prosedur keamanan standar dan pedoman kepatuhan organisasi Anda.

AFT mendukung pelacakan permintaan kustomisasi akun. Setiap kali Anda mengirimkan permintaan kustomisasi akun, AFT menghasilkan token pelacakan unik yang melewati mesin AWS Step Functions status penyesuaian AFT, yang mencatat token sebagai bagian dari eksekusi. Anda kemudian dapat menggunakan kueri wawasan Amazon CloudWatch Logs untuk mencari rentang stempel waktu dan mengambil token permintaan. Hasilnya, Anda dapat melihat muatan yang menyertainya token, sehingga Anda dapat melacak permintaan kustomisasi akun Anda di seluruh alur kerja AFT. Untuk informasi tentang CloudWatch Log dan Fungsi Langkah, lihat berikut ini:

- Apa itu Amazon CloudWatch Logs? dalam Panduan Pengguna Amazon CloudWatch Logs
- Apa itu AWS Step Functions? di Panduan Developer AWS Step Functions

AFT menggabungkan kemampuan AWS layanan lain sebagaiLayanan komponen, untuk membangun kerangka kerja, dengan pipeline yang menerapkan Infrastructure Terraform as Code (IAc). AFT memungkinkan Anda untuk:

- Mengirimkan permintaan penyediaan akun dan pembaruan dalam model GitOps
- Menyimpan metadata akun dan riwayat audit
- Terapkan tag tingkat akun
- Menambahkan penyesuaian ke semua akun, ke satu set akun, atau ke akun individu
- Aktifkan opsi fitur

AFT membuat akun terpisah, yang disebut akun manajemen AFT, untuk menerapkan kemampuan AFT. Sebelum Anda dapat mengatur AFT, Anda harus memiliki zona pendaratan AWS Control Tower yang ada. Akun manajemen AFT tidak sama dengan akun manajemen AWS Control Tower.

AFT menawarkan fleksibilitas

- Fleksibilitas untuk platform Anda: AFT mendukung Distribusi Terraform apa pun untuk penerapan awal dan operasi berkelanjutan: Edisi Komunitas, Cloud, dan Perusahaan.
- Fleksibilitas untuk sistem kontrol versi Anda: Dukungan AFT AWS CodeCommit, dan sumber kontrol versi alternatif melalui AWS CodeConnections.

AFT menawarkan opsi fitur

Anda dapat mengaktifkan beberapa opsi fitur, berdasarkan praktik terbaik:

- Membuat tingkat organisasi CloudTrail untuk mencatat peristiwa data
- Menghapus VPC AWS default untuk akun
- Mendaftarkan akun yang disediakan ke dalam paket Dukungan AWS Perusahaan

> **Note**
>
> Pipeline AFT tidak dimaksudkan untuk digunakan dalam penerapan sumber daya, seperti instans Amazon EC2, yang diperlukan akun Anda untuk menjalankan aplikasi Anda. Ini dimaksudkan semata-mata untuk penyediaan otomatis dan penyesuaian akun AWS Control Tower.

Panduan Video

Video ini (7:33) menjelaskan cara menerapkan akun dengan AWS Control Tower Account Factory untuk Terraform. Untuk tampilan yang lebih baik, pilih ikon di sudut kanan bawah video untuk memperbesarnya ke layar penuh. Keterangan tersedia.

Panduan Video Penyediaan Akun Otomatis di Menara Kontrol AWS.

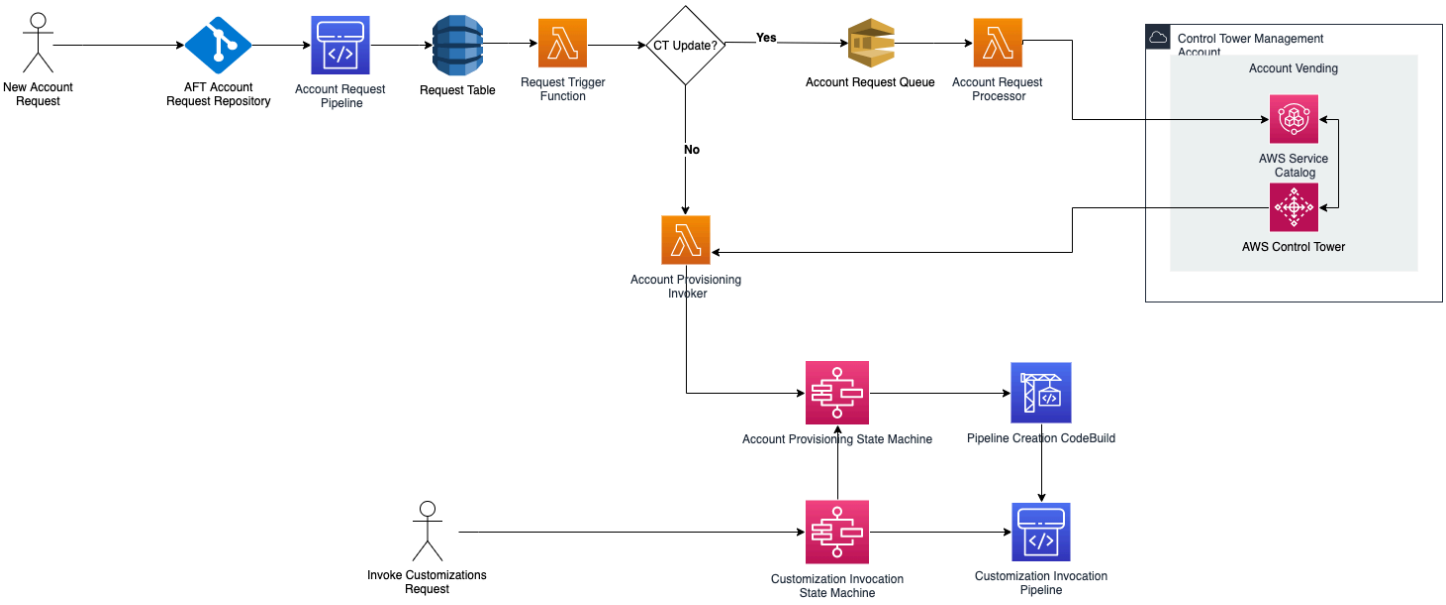
Arsitektur AFT

Urutan operasi

Anda menjalankan operasi AFT di akun manajemen AFT. Untuk alur kerja penyediaan akun lengkap, urutan tahapan dari kiri ke kanan dalam diagram adalah sebagai berikut:

1. Permintaan akun dibuat dan dikirimkan ke pipeline. Anda dapat membuat dan mengirimkan lebih dari satu permintaan akun sekaligus. Account Factory memproses permintaan dalam urutan pertama masuk-pertama keluar. Untuk informasi selengkapnya, lihat Mengirimkan beberapa permintaan akun.
2. Setiap akun disediakan. Tahap ini berjalan di akun manajemen AWS Control Tower.
3. Kustomisasi global berjalan di pipeline yang dibuat untuk setiap akun yang dijual.
4. Jika penyesuaian ditentukan dalam permintaan penyediaan akun awal, penyesuaian hanya berjalan pada akun yang ditargetkan. Jika Anda memiliki akun yang sudah disediakan, Anda harus memulai penyesuaian lebih lanjut secara manual di pipeline akun.

AWS Control Tower Account Factory untuk Terraform — alur kerja penyediaan akun



Gambar 1: Pabrik Akun Menara Kontrol AWS untuk Terraform

Biaya

Tidak ada biaya tambahan untuk AFT. Anda hanya membayar untuk sumber daya yang digunakan oleh AFT, AWS layanan yang diaktifkan oleh AFT, dan sumber daya yang Anda gunakan di lingkungan AFT Anda.

Konfigurasi AFT default mencakup alok AWS PrivateLink asi titik akhir, untuk perlindungan dan keamanan data yang ditingkatkan, dan gateway NAT yang diperlukan untuk mendukung AWS CodeBuild. Untuk detail tentang harga infrastruktur ini, lihat AWS PrivateLink harga dan harga Amazon VPC untuk NAT Gateway. Hubungi perwakilan AWS akun Anda untuk informasi lebih spesifik tentang pengelolaan biaya ini. Anda dapat mengubah pengaturan default ini untuk AFT.

Terapkan AWS Control Tower Account Factory untuk Terraform (AFT)

Bagian ini ditujukan untuk administrator lingkungan AWS Control Tower yang ingin menyiapkan Account Factory for Terraform (AFT) di lingkungan mereka yang ada. Ini menjelaskan cara menyiapkan Account Factory untuk lingkungan Terraform (AFT) dengan akun manajemen AFT khusus yang baru.

> **Note**
>
> Modul Terraform menyebarkan AFT. Modul ini tersedia di repositori AFT aktif GitHub, dan seluruh repositori AFT dianggap sebagai modul.
> Kami menyarankan Anda merujuk ke modul AFT GitHub alih-alih mengkloning repositori AFT. Dengan cara ini Anda dapat mengontrol dan menggunakan pembaruan modul saat tersedia.

Untuk detail tentang rilis terbaru fungsi AWS Control Tower Account Factory for Terraform (AFT), lihat file Rilis untuk repositori ini GitHub .

Prasyarat penyebaran

Sebelum Anda mengkonfigurasi dan meluncurkan lingkungan AFT Anda, Anda harus memiliki sumber daya berikut yang tersedia:

- Wilayah rumah untuk zona landing zone AWS Control Tower Anda. Untuk informasi selengkapnya, lihat Cara Wilayah AWS bekerja dengan AWS Control Tower.
- Sebuah landing zone AWS Control Tower. Untuk informasi selengkapnya, lihat Merencanakan landing zone AWS Control Tower Anda.

- Akun manajemen AFT, yang dapat Anda sediakan di AWS Control Tower, atau sediakan dengan cara lain dan daftarkan ke AWS Control Tower.
- Versi dan distribusi Terraform. Untuk informasi lebih lanjut, lihat versi Terraform dan AFT.
- Penyedia VCS untuk melacak dan mengelola perubahan kode dan file lainnya. Secara default, AFT menggunakan AWS CodeCommit. Untuk informasi lebih lanjut, lihat Apa itu AWS CodeCommit? dalam AWS CodeCommit User Guide.

  Jika Anda menerapkan AFT untuk pertama kalinya dan Anda tidak memiliki CodeCommit repositori yang ada, Anda harus memilih penyedia VCS eksternal, seperti atau. GitHub BitBucket Untuk informasi selengkapnya, lihat Alternatif untuk kontrol versi kode sumber di AFT.
- Lingkungan runtime tempat Anda dapat menjalankan modul Terraform yang menginstal AFT.
- Opsi fitur AFT. Untuk informasi selengkapnya, lihat Mengaktifkan opsi fitur.

Konfigurasikan dan luncurkan AWS Control Tower Account Factory untuk Terraform

Langkah-langkah berikut mengasumsikan bahwa Anda terbiasa dengan alur kerja Terraform. Anda juga dapat mempelajari lebih lanjut tentang penerapan AFT dengan mengikuti lab Pengantar AFT di situs web AWS Workshop Studio.

Langkah 1: Luncurkan landing zone AWS Control Tower

Untuk petunjuk tentang memulai AWS Control Tower, lihat Memulai AWS Control Tower. Di sinilah Anda membuat akun manajemen AWS Control Tower dan menyiapkan landing zone AWS Control Tower Anda.

> **Note**
>
> Pastikan untuk membuat peran untuk akun manajemen AWS Control Tower yang memiliki AdministratorAccesskredensil. Untuk informasi selengkapnya, lihat berikut ini:
>
> - Identitas IAM (pengguna, grup pengguna, dan peran) di AWS Identity and Access Management Panduan Pengguna
> - AdministratorAccessdalam Panduan Referensi Kebijakan AWS Terkelola

Langkah 2: Buat unit organisasi baru untuk AFT (sangat disarankan)

Kami menyarankan Anda membuat OU terpisah di zona landing zone AWS Control Tower Anda. OU ini adalah tempat Anda menyediakan akun manajemen AFT. Buat akun manajemen OU dan AFT baru dari akun manajemen AWS Control Tower Anda. Untuk informasi selengkapnya, lihat Membuat OU baru.

Langkah 3: Menyediakan akun manajemen AFT

AFT mengharuskan Anda menyediakan AWS akun yang didedikasikan untuk operasi manajemen AFT. Buat akun manajemen AFT saat Anda masuk ke akun manajemen AWS Control Tower yang terkait dengan landing zone AWS Control Tower Anda. Anda dapat menyediakan akun manajemen AFT dari konsol AWS Control Tower dengan memilih Buat akun di halaman Organisasi, atau dengan cara lain. Untuk informasi selengkapnya, lihat Menyediakan akun dengan AWS Service Catalog Account Factory.

> **Note**
>
> Jika Anda membuat OU terpisah untuk AFT, pastikan untuk memilih OU ini saat Anda membuat akun manajemen AFT.

Diperlukan waktu hingga 30 menit untuk sepenuhnya menyediakan akun manajemen AFT.

Langkah 4: Verifikasi bahwa lingkungan Terraform tersedia untuk penerapan

Langkah ini mengasumsikan bahwa Anda memiliki pengalaman dengan Terraform dan memiliki prosedur untuk menjalankan Terraform. Untuk informasi selengkapnya, lihat Command: init di situs web HashiCorp Developer.

> **Note**
>
> AFT mendukung Versi Terraform `1.6.1` atau yang lebih baru.

Langkah 5: Konfigurasi opsional

- Secara opsional mengatur konfigurasi virtual private cloud (VPC)

  Modul AFT menyertakan `aft_enable_vpc` parameter, yang menentukan apakah AWS Control Tower menyediakan sumber daya akun dalam VPC di akun manajemen AFT pusat. Secara default, parameter diatur `ketrue`. Jika Anda menyetel parameter ini`false`, AWS Control Tower

menerapkan AFT tanpa menggunakan VPC dan sumber daya jaringan pribadi, seperti NAT Gateways atau titik akhir VPC. Menonaktifkan `aft_enable_vpc` dapat membantu mengurangi biaya operasi AFT untuk beberapa pola penggunaan. Menambahkan konfigurasi VPC apa pun akan mengesampingkan parameter yang disetel ke. `aft_enable_vpc false`

> **Note**
>
> Re-enabling `aft_enable_vpc`parameter (mengalihkan nilai dari `false` ke`true`) mungkin mengharuskan Anda menjalankan `terraform apply` perintah dua kali berturut-turut.

Alih-alih menyediakan VPC baru, Anda dapat mengonfigurasi AFT untuk menggunakan VPC yang ada di akun Anda. Untuk menggunakan VPC Anda sendiri, berikan parameter konfigurasi VPC berikut:

- `aft_customer_vpc_id`- ID VPC Anda yang ada
- `aft_customer_private_subnets`- Daftar ID subnet pribadi di VPC Anda

Contoh konfigurasi:

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"

  # VPC configuration
  aft_customer_vpc_id = "vpc-0123456789abcdef0"
  aft_customer_private_subnets = ["subnet-0123456789abcdef0",
 "subnet-0123456789abcdef1"]

  # Other AFT parameters...
}
```

> **Important**
>
> Kami tidak menyarankan Anda menggunakan opsi VPC kustom jika Anda memiliki penerapan AFT yang sudah ada. Anda mungkin memiliki dependensi pada fungsi Lambda atau CodePipeline yang bergantung pada sumber daya dalam VPC yang ada.

- Konfigurasikan nama proyek Terraform secara opsional

Anda dapat menyesuaikan nama proyek Terraform yang digunakan oleh AFT dengan menyetel parameter. `terraform_project_name` Secara default, AFT menempatkan penerapan dalam proyek “default” di HCP Terraform atau Terraform Enterprise.

Contoh konfigurasi:

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"

  # Project name configuration
  terraform_project_name = "my-organization-aft"

  # Other AFT parameters...
}
```

> **Note**
>
> Parameter ini hanya berlaku untuk penerapan Terraform Enterprise atau Terraform Cloud.

- Secara opsional menerapkan tag khusus ke sumber daya AFT

Anda dapat menerapkan tag khusus ke semua sumber daya AFT dengan menggunakan `tags` parameter. Tag ini membantu organisasi sumber daya, alokasi biaya, dan kontrol akses.

Contoh konfigurasi:

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"

  # Custom tags configuration
  tags = {
    Environment = "Production"
    CostCenter = "IT-12345"
    Project = "AFT-Deployment"
    Owner = "platform-team@example.com"
  }

  # Other AFT parameters...
```

```
}
```

Tag ini diterapkan ke semua sumber daya yang dibuat oleh modul AFT. AFT secara otomatis menambahkan `managed_by = "AFT"` tag ke semua sumber daya, yang tidak dapat diganti dengan tag khusus.

> **Note**
>
> Tag khusus dapat ditambahkan kapan saja, tidak hanya selama penerapan awal.

- Secara opsional menerapkan kunci enkripsi yang AWS KMS dikelola pelanggan (CMK) ke grup CloudWatch log dan topik SNS

  Untuk mengaktifkan enkripsi KMS CMK untuk grup log dan topik SNS, atur variabel dan. `cloudwatch_log_group_enable_cmk_encryption` `sns_topic_enable_cmk_encryption`

  Jika Anda memilih pengaturan ini, AFT menggunakan CMK yang ada, alias/aft, untuk mengenkripsi CloudWatch log dan topik SNS. CMK ini dibuat ketika AFT digunakan di akun manajemen AFT, dan dapat diterapkan ke grup log dan topik SNS.

  - Jika variabel `cloudwatch_log_group_enable_cmk_encryption` disetel ke true, grup CloudWatch log untuk AFT dienkripsi menggunakan CMK. Jika variabel diatur ke false, yang merupakan nilai default, log dienkripsi menggunakan enkripsi sisi server dengan CloudWatch log default.
  - Jika variabel `sns_topic_enable_cmk_encryption` disetel ke true, notifikasi yang dikirim ke topik SNS AFT (aft-notifications dan aft-failure-notifications) dienkripsi menggunakan CMK. Jika variabel diatur ke false, yang merupakan nilai default, pesan SNS dienkripsi dengan AWS-managed kunci: /sns. alias/aws Untuk informasi selengkapnya, lihat istilah kunci SSE.
- Secara opsional mengubah jenis CodeBuild komputasi Anda

  Selama penerapan, untuk mengubah jenis komputasi yang digunakan AFT CodeBuild, setel variabel. `aft_codebuild_compute_type`

  Untuk informasi tentang jenis komputasi yang diterima, lihat Tentang jenis lingkungan sesuai permintaan. Jenis komputasi default adalah`BUILD_GENERAL1_MEDIUM`.
- Konfigurasikan OpenID Connect (OIDC) secara opsional untuk Terraform

Pelanggan yang menggunakan Terraform Enterprise atau HCP Terraform (sebelumnya Terraform Cloud) dapat menggunakan token identitas Beban Kerja Terraform (atau kredenal penyedia dinamis), yang dibangun di atas protokol OIDC, untuk menghubungkan dan mengautentikasi ruang kerja dengan aman dengan AFT.

Anda dapat mengaktifkan integrasi OIDC untuk ruang kerja AFT dengan menyetel parameter ke. `terraform_oidc_integration` `true` Secara default, parameter ini diatur kefalse. Saat mengaktifkan parameter ini, `terraform_oidc_hostname` parameter `terraform_oidc_aws_audience` and harus ditinjau dan dikonfigurasi jika default (`aws.workload.identitydanapp.terraform.io`, masing-masing) tidak cocok dengan lingkungan Anda.

Contoh konfigurasi:

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"

  # Terraform distribution must be "tfc" or "tfe" for OIDC
  terraform_distribution = "tfc"

  # Terraform OIDC Configuration
  terraform_oidc_integration  = true
  terraform_oidc_aws_audience = "aws.workload.identity"  # default
  terraform_oidc_hostname     = "app.terraform.io"       # default; set to your TFE
 hostname if applicable

  # Other AFT parameters...
}
```

> **Note**
>
> Parameter ini hanya berlaku untuk penerapan Terraform Enterprise atau HCP Terraform.

> **Note**
>
> Jika saat ini Anda memanfaatkan penyedia OIDC untuk Terraform di akun manajemen AFT, Anda harus menghapus penyedia tersebut sebelum ikut serta dalam integrasi ini. AFT akan membuat ulang penyedia itu untuk Anda saat penerapan.

Langkah 6: Hubungi Account Factory untuk modul Terraform untuk menyebarkan AFT

Panggil modul AFT dengan peran yang Anda buat untuk akun manajemen AWS Control Tower yang memiliki AdministratorAccesskredensil. AWS Control Tower menyediakan modul Terraform melalui akun manajemen AWS Control Tower, yang menetapkan semua infrastruktur yang diperlukan untuk mengatur permintaan AWS Control Tower Account Factory.

Anda dapat melihat modul AFT di repositori AFT pada. GitHub Seluruh GitHub repositori dianggap sebagai modul AFT. Lihat file README untuk informasi tentang input yang diperlukan untuk menjalankan modul AFT dan menerapkan AFT. Atau, Anda dapat melihat modul AFT di Terraform Registry.

Jika Anda memiliki saluran pipa di lingkungan Anda yang dibuat untuk mengelola Terraform, Anda dapat mengintegrasikan modul AFT ke dalam alur kerja yang ada. Jika tidak, jalankan modul AFT dari lingkungan apa pun yang diautentikasi dengan kredensi yang diperlukan.

Timeout menyebabkan penerapan gagal. Sebaiknya gunakan kredensi AWS Security Token Service (STS) untuk memastikan Anda memiliki batas waktu yang cukup untuk penerapan penuh. Batas waktu minimum untuk AWS STS kredensional adalah 60 menit. Untuk informasi selengkapnya, lihat Kredensi keamanan sementara di IAM di Panduan Pengguna.AWS Identity and Access Management

> **Note**
>
> Anda mungkin menunggu hingga 30 menit hingga AFT menyelesaikan penerapan melalui modul Terraform.

Langkah 7: Kelola file status Terraform

File status Terraform dibuat saat Anda menerapkan AFT. Artefak ini menggambarkan keadaan sumber daya yang dibuat Terraform. Jika Anda berencana untuk memperbarui versi AFT, pastikan

untuk memilih file status Terraform, atau siapkan backend Terraform menggunakan Amazon S3 dan DynamoDB. Modul AFT tidak mengelola status Terraform backend.

> **Note**
>
> Anda bertanggung jawab untuk melindungi file status Terraform. Beberapa variabel input mungkin berisi nilai sensitif, seperti `ssh` kunci pribadi atau token Terraform. Bergantung pada metode penerapan Anda, nilai-nilai ini dapat dilihat sebagai teks biasa di file status Terraform. Untuk informasi selengkapnya, lihat Data sensitif di Negara di HashiCorp situs web.

Post-deployment langkah

Setelah penyebaran infrastruktur AFT selesai, ikuti langkah-langkah tambahan ini untuk menyelesaikan proses penyiapan dan bersiap-siap untuk menyediakan akun.

Langkah 1: Lengkap AWS CodeConnections dengan penyedia VCS yang Anda inginkan

Jika Anda memilih penyedia VCS pihak ketiga, AFT menetapkan AWS CodeConnections, dan Anda mengonfirmasinya. Lihat Alternatif untuk kontrol versi kode sumber di AFT untuk mempelajari cara mengatur AFT dengan VCS pilihan Anda.

Langkah awal membangun AWS CodeStar koneksi dilakukan oleh AFT. Anda harus mengkonfirmasi koneksi.

Langkah 2: Isi setiap repositori

AFT mengharuskan Anda mengelola empat repositori:

1. Permintaan akun — Repositori ini menangani penempatan atau pembaruan permintaan akun. Contoh yang tersedia. Untuk informasi selengkapnya tentang permintaan akun AFT, lihatMenyediakan akun baru dengan AFT.
2. Kustomisasi penyediaan akun AFT — Repositori ini mengelola penyesuaian yang diterapkan ke semua akun yang dibuat oleh dan dikelola dengan AFT, sebelum memulai tahap penyesuaian global. Contoh yang tersedia. Untuk membuat kustomisasi penyediaan akun AFT, lihat. Buat mesin status penyesuaian penyediaan akun AFT Anda
3. Kustomisasi global — Repositori ini mengelola penyesuaian yang diterapkan ke semua akun yang dibuat oleh dan dikelola dengan AFT. Contoh yang tersedia. Untuk membuat kustomisasi global AFT, lihat. Terapkan kustomisasi global

4. Penyesuaian akun — Repositori ini mengelola penyesuaian yang hanya diterapkan pada akun tertentu yang dibuat oleh dan dikelola dengan AFT. Contoh yang tersedia. Untuk membuat kustomisasi akun AFT, lihat. Terapkan kustomisasi akun

AFT mengharapkan bahwa masing-masing repositori ini mengikuti struktur direktori tertentu. Template yang digunakan untuk mengisi repositori dan instruksi yang menjelaskan cara mengisi template tersedia di modul Account Factory for Terraform di repositori github AFT.

Menyediakan akun baru dengan AFT

Bagian ini mengasumsikan bahwa Anda telah menyiapkan AFT dan akun manajemen AFT Anda, dan Anda menyediakan akun tambahan.

Untuk menyediakan akun baru dengan AFT, buat file permintaan akun Terraform. File ini berisi input untuk parameter di repositori aft-account-request. Setelah membuat file permintaan akun Terraform, mulailah memproses permintaan akun Anda dengan menjalankan. `git push` Perintah ini memanggil `ct-aft-account-request` operasi di AWS CodePipeline, yang dibuat di akun manajemen AFT setelah penyediaan akun selesai. Untuk informasi selengkapnya, lihat saluran penyediaan akun AFT.

Permintaan akun Parameter file Terraform

Anda harus menyertakan parameter berikut dalam permintaan akun Anda file Terraform. Anda dapat melihat contoh permintaan akun file Terraform di. GitHub

- Nilai `module name` harus unik sesuai Akun AWS permintaan.
- Nilai `module source` adalah jalur ke permintaan akun modul Terraform yang disediakan AFT.
- Nilai `control_tower_parameters` menangkap input yang diperlukan untuk membuat akun AWS Control Tower. Nilai mencakup bidang masukan berikut:
  - `AccountEmail`
  - `AccountName`
  - `ManagedOrganizationalUnit`
  - `SSOUserEmail`
  - `SSOUserFirstName`
  - `SSOUserLastName`

> **Note**
>
> Input yang Anda berikan tidak `control_tower_parameters` dapat diubah selama penyediaan akun.
> Format yang didukung untuk menentukan `ManagedOrganizationalUnit` dalam repositori permintaan akun aft-termasuk dan. `OUName` `OUName (OU-ID)` Untuk OU bersarang (OU dalam OU), Anda harus menggunakan `OUName (OU-ID)` format. Sebagai contoh, lihat account-requ est.tf di. GitHub

- `account_tags`menangkap kunci dan nilai yang ditentukan pengguna, yang dapat menandai Akun AWS sesuai dengan kriteria bisnis. Untuk informasi selengkapnya, lihat Menandai AWS Organizations sumber daya di Panduan AWS Organizations Pengguna.
- Nilai `change_management_parameters` menangkap informasi tambahan, seperti mengapa permintaan akun dibuat dan siapa yang memulai permintaan akun. Nilai mencakup bidang masukan berikut:
  - `change_reason`
  - `change_requested_by`
- `custom_fields`menangkap metadata tambahan dengan kunci dan nilai yang digunakan sebagai parameter SSM di akun yang dijual di bawah/aft/account- request/custom -fields/. Anda dapat mereferensikan metadata ini selama penyesuaian akun untuk menerapkan kontrol yang tepat. Misalnya, akun yang tunduk pada kepatuhan terhadap peraturan mungkin menerapkan tambahan Aturan AWS Config. Metadata yang Anda kumpulkan `custom_fields` dapat memanggil pemrosesan tambahan selama penyediaan dan pembaruan akun. Jika bidang kustom dihapus dari permintaan akun, bidang kustom dihapus dari Penyimpanan Parameter SSM untuk akun yang dijual.
- (Opsional) `account_customizations_name` menangkap folder template akun di repositori aft-account-customizations. Untuk informasi selengkapnya, lihat Kustomisasi https://docs.aws.amazon.com/controltower/latest/userguide/aft-account-customization-options.html akun.

Kirim beberapa permintaan akun

AFT memproses permintaan akun satu per satu, tetapi Anda dapat mengirimkan beberapa permintaan akun ke pipeline AFT. Saat Anda mengirimkan beberapa permintaan akun ke pipeline AFT, AFT mengantri dan memproses permintaan akun dalam urutan masuk pertama, keluar pertama.

> **Note**
>
> Anda dapat membuat file Terraform permintaan akun untuk setiap akun yang Anda ingin AFT menyediakan atau mencatatkan beberapa permintaan akun dalam satu file Terraform permintaan akun.

Memperbarui akun yang sudah ada

> **Kompatibilitas Pendaftaran Otomatis**
>
> Jika organisasi Anda menggunakan Auto Entry untuk pendaftaran akun otomatis, ketahuilah bahwa AFT memiliki batasan dalam mengimpor akun ini. Akun yang terdaftar melalui Auto Entry tidak memiliki produk yang disediakan Katalog Layanan yang diperlukan oleh alur kerja impor AFT.
> Solusi: Gunakan fitur Daftar OU untuk membuat produk yang disediakan untuk akun yang terdaftar secara otomatis. Ini memungkinkan peristiwa siklus hidup yang diperlukan untuk penyesuaian AFT.

Anda dapat memperbarui akun yang disediakan AFT dengan mengedit permintaan akun yang dikirimkan sebelumnya dan menjalankannya`git push`. Perintah ini memanggil alur kerja penyediaan akun dan dapat memproses permintaan pembaruan akun. Anda dapat memperbarui input untuk`ManagedOrganizationalUnit`, yang merupakan bagian dari nilai yang diperlukan untuk`control_tower_parameters`.

`ManagedOrganizationalUnit`adalah satu-satunya parameter yang dapat diperbarui, di antara semuanya`control_tower_parameters`. Namun, parameter lain yang merupakan bagian dari permintaan akun file Terraform dapat diperbarui, seperti. `custom_fields` Untuk informasi selengkapnya, lihat Menyediakan akun baru dengan AFT.

Misalnya, untuk memperbarui nama atau alamat email akun AFT, Anda dapat menentukan spesifikasinya seperti `custom_fields` dalam file Permintaan Akun. Dengan demikian, Anda membuat parameter SSM, yang dapat Anda berikan ke sumber `aws_account_alternate_contact` daya selama penyesuaian global.

```
resource "aws_account_alternate_contact" "operations" {
```

```
  alternate_contact_type = "OPERATIONS"

  name          = "Example"
  title         = "Example"
  email_address = "someone@example.com"
  phone_number  = "+1234567890"
}
```

Anda dapat menambahkan bidang serupa untuk jenis kontak lain, seperti operasi dan keamanan. Di Kustomisasi Global, tambahkan pencarian data untuk setiap bidang kustom, untuk memastikan bahwa Anda mencari semua bidang yang Anda buat di Permintaan Akun:

```
data "aws_ssm_parameter" "billing_name" {
            name = "/aft/account-request/custom-fields/billing_name"
            }

            data "aws_ssm_parameter" "billing_title" {
            name = "/aft/account-request/custom-fields/billing_title"
            }

            data "aws_ssm_parameter" "billing_email_address" {
            name = "/aft/account-request/custom-fields/billing_email_address"
            }

            data "aws_ssm_parameter" "billing_phone_number" {
            name = "/aft/account-request/custom-fields/billing_phone_number"
            }
```

Terakhir, juga di file Kustomisasi Global, buat sumber daya kontak alternatif. Anda perlu menentukan salah satu blok ini untuk setiap jenis kontak yang Anda buat di Permintaan Akun:

```
resource "aws_account_alternate_contact" "billing" {

            alternate_contact_type = "BILLING"

            name          = data.aws_ssm_parameter.billing_name.value
            title         = data.aws_ssm_parameter.billing_title.value
            email_address = data.aws_ssm_parameter.billing_email_address.value
            phone_number  = data.aws_ssm_parameter.billing_phone_number.value
            }
```

> **Note**
>
> Input yang Anda berikan tidak `control_tower_parameters` dapat diubah selama penyediaan akun.
> Format yang didukung untuk menentukan `ManagedOrganizationalUnit` dalam repositori permintaan akun aft-termasuk dan. `OUName` `OUName (OU-ID)` Untuk OU bersarang (OU dalam OU), Anda harus menggunakan `OUName (OU-ID)` format. Sebagai contoh, lihat account-requ est.tf di. GitHub

Memperbarui akun yang tidak disediakan AFT

Anda dapat memperbarui akun AWS Control Tower yang dibuat di luar AFT dengan menentukan akun di repositori aft-account-request.

> **Note**
>
> Pastikan semua detail akun benar dan konsisten dengan organisasi AWS Control Tower dan produk yang AWS Service Catalog disediakan masing-masing.

Prasyarat untuk memperbarui yang sudah ada Akun AWS dengan AFT

- Akun AWS Harus terdaftar di AWS Control Tower.
- Akun AWS Harus menjadi bagian dari organisasi Menara Kontrol AWS.

Versi Terraform dan AFT

Account Factory for Terraform (AFT) mendukung versi Terraform atau yang lebih baru. `1.6.1` Anda harus memberikan versi Terraform sebagai parameter input untuk proses penerapan AFT, seperti yang ditunjukkan pada contoh berikut.

```
terraform_version = "1.6.1"
```

Distribusi terraform

AFT mendukung tiga distribusi Terraform:

- Edisi Komunitas Terraform
- HCP Terraform
- Perusahaan Terraform

Distribusi ini dijelaskan di bagian berikutnya. Berikan distribusi Terraform pilihan Anda sebagai parameter input selama proses bootstrap AFT. Untuk informasi selengkapnya tentang penerapan AFT dan parameter input, lihatTerapkan AWS Control Tower Account Factory untuk Terraform (AFT).

Jika Anda memilih distribusi HCP Terraform atau Terraform Enterprise, token API yang Anda tentukan `terraform_token` harus berupa token API Pengguna atau Tim. Token Organisasi tidak didukung untuk semua API yang diperlukan. Untuk alasan keamanan, Anda harus menghindari memeriksa nilai token ini ke sistem kontrol versi (VCS) Anda dengan menetapkan variabel terraform, seperti yang ditunjukkan pada contoh berikut.

```
# Sensitive variable managed in HCP Terraform:
terraform_token = var.terraform_cloud_token
```

Edisi Komunitas Terraform

Saat Anda memilih Terraform Community Edition sebagai distribusi Anda, AFT mengelola backend Terraform untuk Anda di akun manajemen AFT. AFT mengunduh versi Terraform yang Anda tentukan untuk dijalankan selama penerapan AFT dan fase pipeline AFT. `terraform-cli` Konfigurasi status Terraform yang dihasilkan disimpan dalam bucket Amazon S3, dinamai dengan bentuk berikut:

```
aft-backend-[account_id]-primary-region
```

AFT juga membuat bucket Amazon S3 yang mereplikasi konfigurasi status Terraform Anda di tempat lain Wilayah AWS, untuk tujuan pemulihan bencana, dinamai dengan formulir berikut:

```
aft-backend-[account_id]-secondary-region
```

Kami menyarankan Anda mengaktifkan otentikasi multi-faktor (MFA) untuk fungsi hapus pada bucket Amazon S3 status Terraform ini. Untuk mempelajari lebih lanjut tentang Terraform Community Edition, lihat dokumentasi Terraform.

Untuk memilih Terraform OSS sebagai distribusi Anda, berikan parameter input berikut:

```
terraform_distribution = "oss"
```

HCP Terraform

Saat Anda memilih HCP Terraform sebagai distribusi Anda, AFT membuat ruang kerja untuk komponen berikut di organisasi HCP Terraform Anda, yang memulai alur kerja. API-driven

- Permintaan akun
- Kustomisasi AFT untuk akun yang disediakan AFT
- Kustomisasi akun untuk akun yang disediakan AFT
- Kustomisasi global untuk akun yang disediakan AFT

HCP Terraform mengelola konfigurasi status Terraform yang dihasilkan.

Saat Anda memilih HCP Terraform sebagai distribusi Anda, berikan parameter input berikut:

- `terraform_distribution = "tfc"`
- `terraform_token`— Parameter ini berisi nilai token HCP Terraform. AFT menandai sebagai sensitif dan menyimpan nilai sebagai string aman di penyimpanan parameter SSM di akun manajemen AFT. Kami menyarankan Anda memutar nilai token Terraform secara berkala sesuai dengan kebijakan keamanan dan pedoman kepatuhan perusahaan Anda. Token Terraform harus berupa token API tingkat Pengguna atau Tim. Token organisasi tidak didukung.
- `terraform_org_name`— Parameter ini berisi nama organisasi HCP Terraform Anda.

> **Note**
>
> Beberapa penerapan AFT dalam satu organisasi HCP Terraform tidak didukung.

Untuk informasi tentang cara mengatur HCP Terraform, lihat dokumentasi Terraform.

Perusahaan Terraform

Saat Anda memilih Terraform Enterprise sebagai distribusi Anda, AFT membuat ruang kerja untuk komponen berikut di organisasi Terraform Enterprise Anda, dan itu memicu API-driven alur kerja untuk menjalankan Terraform yang dihasilkan.

- Permintaan akun
- Kustomisasi penyediaan akun AFT untuk akun yang disediakan oleh AFT
- Kustomisasi akun untuk akun yang disediakan oleh AFT
- Kustomisasi global untuk akun yang disediakan oleh AFT

Konfigurasi status Terraform yang dihasilkan dikelola oleh penyiapan Terraform Enterprise Anda.

Untuk memilih Terraform Enterprise sebagai distribusi Anda, berikan parameter input berikut:

- `terraform_distribution = "tfe"`
- `terraform_token`— Parameter ini berisi nilai token Terraform Enterprise Anda. AFT menandai nilainya sebagai sensitif dan menyimpannya sebagai string aman di penyimpanan parameter SSM, di akun manajemen AFT. Kami menyarankan Anda memutar nilai token Terraform secara berkala, sesuai dengan kebijakan keamanan dan pedoman kepatuhan perusahaan Anda.
- `terraform_org_name`— Parameter ini berisi nama organisasi Terraform Enterprise Anda.
- `terraform_api_endpoint`— Parameter ini berisi URL lingkungan Terraform Enterprise Anda. Nilai parameter ini harus dalam format:

```
https://{fqdn}/api/v2/
```

Lihat dokumentasi Terraform untuk mempelajari lebih lanjut tentang cara menyiapkan Terraform Enterprise.

Periksa versi AFT

Anda dapat memeriksa versi AFT yang digunakan dengan menanyakan kunci Penyimpanan Parameter AWS SSM:

```
/aft/config/aft/version
```

Jika Anda menggunakan metode registri, Anda dapat menyematkan versi.

```
module "control_tower_account_factory" {
  source  = "aws-ia/control_tower_account_factory/aws"
  version = "1.3.2"
  # insert the 6 required variables here
}
```

Anda dapat melihat informasi lebih lanjut tentang versi AFT di repositori AFT.

Perbarui versi AFT

Masuk ke akun manajemen AWS Control Tower untuk memulai pembaruan AFT ini.

Anda dapat memperbarui versi AFT yang diterapkan dengan menariknya dari cabang `main` repositori:

```
terraform get -update
```

Setelah penarikan selesai, Anda dapat menjalankan kembali paket Terraform atau menjalankan apply untuk memperbarui infrastruktur AFT dengan perubahan terbaru.

Aktifkan opsi fitur

AFT menawarkan opsi fitur berdasarkan praktik terbaik. Anda dapat ikut serta dalam fitur-fitur ini, melalui flag fitur, selama penerapan AFT. Lihat Menyediakan akun baru dengan AFT untuk informasi lebih lanjut tentang parameter konfigurasi input AFT.

Fitur-fitur ini tidak diaktifkan secara default. Anda harus secara eksplisit mengaktifkan masing-masing di lingkungan Anda.

Topik

- AWS CloudTrail peristiwa data
- AWS Paket Enterprise Support
- Hapus AWS VPC standar
- Ekspor output paket Terraform ke Amazon S3

AWS CloudTrail peristiwa data

Saat diaktifkan, opsi peristiwa AWS CloudTrail data mengonfigurasi kemampuan ini.

- Membuat Jejak Organisasi di akun manajemen AWS Control Tower, untuk CloudTrail
- Mengaktifkan pencatatan untuk peristiwa data Amazon S3 dan Lambda
- Mengenkripsi dan mengekspor semua peristiwa CloudTrail data ke bucket `aws-aft-logs-*` S3 di akun AWS Control Tower Log Archive, dengan enkripsi AWS KMS
- Mengaktifkan setelan validasi berkas Log

Untuk mengaktifkan opsi ini, setel flag fitur berikut ke True dalam konfigurasi input penerapan AFT Anda.

```
aft_feature_cloudtrail_data_events
```

Prasyarat

Sebelum Anda mengaktifkan opsi fitur ini, pastikan akses tepercaya untuk AWS CloudTrail diaktifkan di organisasi Anda.

Untuk memeriksa status akses tepercaya untuk CloudTrail :

1. Arahkan ke AWS Organizations konsol.
2. Pilih Layanan > CloudTrail.
3. Kemudian pilih Aktifkan akses tepercaya di kanan atas, jika diperlukan.

Anda mungkin menerima pesan peringatan yang menyarankan Anda untuk menggunakan AWS CloudTrail konsol, tetapi dalam kasus ini, abaikan peringatan tersebut. AFT membuat jejak sebagai bagian dari mengaktifkan opsi fitur ini, setelah Anda mengizinkan akses tepercaya. Jika akses tepercaya tidak diaktifkan, Anda akan menerima pesan kesalahan saat AFT mencoba membuat jejak untuk peristiwa data.

> **Note**
>
> Pengaturan ini berfungsi di tingkat organisasi. Mengaktifkan pengaturan ini memengaruhi semua akun AWS Organizations, baik dikelola oleh AFT atau tidak. Semua bucket di akun AWS Control Tower Log Archive pada saat mengaktifkan dikecualikan dari peristiwa data Amazon S3. Lihat Panduan AWS CloudTrail Pengguna untuk mempelajari selengkapnya CloudTrail.

AWS Paket Enterprise Support

Ketika opsi ini diaktifkan, pipeline AFT mengaktifkan paket AWS Enterprise Support untuk akun yang disediakan oleh AFT.

AWS akun secara default dilengkapi dengan paket Dukungan AWS Dasar diaktifkan. AFT menyediakan pendaftaran otomatis ke tingkat dukungan perusahaan, untuk akun yang disediakan

AFT. Proses penyediaan membuka tiket dukungan untuk akun, memintanya untuk ditambahkan ke paket Enterprise AWS Support.

Untuk mengaktifkan opsi Enterprise Support, setel flag fitur berikut ke True dalam konfigurasi input penerapan AFT Anda.

```
aft_feature_enterprise_support=false
```

Lihat Bandingkan Paket AWS Dukungan untuk mempelajari lebih lanjut tentang AWS Support Plans.

> **Note**
>
> Untuk memungkinkan fitur ini beroperasi, Anda harus mendaftarkan akun pembayar ke dalam paket Enterprise Support.

Hapus AWS VPC standar

Saat Anda mengaktifkan opsi ini, AFT menghapus semua VPC AWS default di akun manajemen AFT dan semuanya Wilayah AWS, meskipun belum menerapkan sumber daya AWS Control Tower di dalamnya. Wilayah AWS

AFT tidak menghapus VPC AWS default secara otomatis untuk akun AWS Control Tower apa pun yang disediakan AFT atau untuk AWS akun yang sudah ada yang Anda daftarkan di AWS Control Tower melalui AFT.

AWS Akun baru dibuat dengan VPC yang disiapkan di masing-masing akun Wilayah AWS, secara default. Perusahaan Anda mungkin memiliki praktik standar untuk membuat VPC, yang mengharuskan Anda menghapus VPC AWS default dan menghindari mengaktifkannya, terutama untuk akun manajemen AFT.

Untuk mengaktifkan opsi ini, setel flag fitur berikut ke True dalam konfigurasi input penerapan AFT Anda.

```
aft_feature_delete_default_vpcs_enabled
```

Berikut ini adalah contoh konfigurasi input penerapan AFT.

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"
```

```
  ct_management_account_id    = var.ct_management_account_id
  log_archive_account_id      = var.log_archive_account_id
  audit_account_id            = var.audit_account_id
  aft_management_account_id   = var.aft_management_account_id
  ct_home_region              = var.ct_home_region
  tf_backend_secondary_region = var.tf_backend_secondary_region

  vcs_provider                                = "github"
  account_request_repo_name                   = "${var.github_username}/learn-
terraform-aft-account-request"
  account_provisioning_customizations_repo_name = "${var.github_username}/learn-
terraform-aft-account-provisioning-customizations"
  global_customizations_repo_name             = "${var.github_username}/learn-
terraform-aft-global-customizations"
  account_customizations_repo_name            = "${var.github_username}/learn-
terraform-aft-account-customizations"

  # Optional Feature Flags
  aft_feature_delete_default_vpcs_enabled = true
  aft_feature_cloudtrail_data_events      = false
  aft_feature_enterprise_support          = false
}
```

Lihat VPC default dan subnet default untuk mempelajari lebih lanjut tentang VPC default.

> **Note**
>
> Penghapusan VPC default adalah upaya terbaik per. Wilayah AWS Jika titik akhir Wilayah untuk sementara tidak dapat dijangkau, AFT melewatkan Wilayah tersebut dan terus menghapus VPC default di Wilayah yang tersisa. Wilayah yang Dilewati akan dicoba ulang pada proses pipeline kustomisasi berikutnya. Untuk memeriksa apakah ada Wilayah yang dilewati, cari log fungsi `aft-delete-default-vpc` Lambda untuk pesan tersebut. `Skipping default VPC deletion in region`

Ekspor output paket Terraform ke Amazon S3

Saat Anda menerapkan AFT, AFT akan membuat bucket Amazon S3 keluaran paket terenkripsi khusus di akun manajemen AFT. AFT membuat bucket ini pada setiap penerapan AFT, terlepas dari distribusi Terraform Anda. Bucket menyimpan output JSON dari proses kustomisasi khusus paket. Untuk informasi selengkapnya tentang proses khusus rencana, lihat. Re-invoke kustomisasi

Bucket plan-output memiliki properti berikut:

- Dienkripsi dengan kunci AFT AWS KMS
- Pembuatan versi diaktifkan
- Akses publik diblokir
- Akses tulis terbatas pada peran pembuatan kustomisasi AFT

Apakah AFT mengekspor paket JSON ke bucket ini tergantung pada distribusi Terraform Anda:

- Edisi Komunitas (open source): AFT mengekspor paket JSON ke bucket secara default pada setiap proses khusus paket.
- HCP Terraform (Terraform Cloud) dan Terraform Enterprise: Anda dapat melihat hasil paket di UI run HCP Terraform. Untuk juga mengekspor paket JSON ke bucket, setel variabel berikut ke `true` dalam konfigurasi input penerapan AFT Anda.

```
aft_plan_output_export_enabled = true
```

AFT mempertahankan paket yang diekspor selama 30 hari secara default. Untuk mengubah durasi retensi, setel `aft_plan_output_retention_days` variabel dalam konfigurasi input penerapan AFT Anda.

```
aft_plan_output_retention_days = 30
```

> **Note**
>
> `aft_plan_output_export_enabled`Variabel hanya mempengaruhi distribusi HCP Terraform (Terraform Cloud) dan Terraform Enterprise. Pada distribusi Community Edition (open source), AFT mengekspor paket JSON secara default, dan variabel ini tidak berpengaruh.

Pertimbangan sumber daya untuk AWS Control Tower Account Factory untuk Terraform

Saat Anda menyiapkan landing zone menggunakan AWS Control Tower Account Factory for Terraform, beberapa jenis AWS sumber daya dibuat dalam akun Anda AWS .

Cari sumber daya

- Anda dapat menggunakan tag untuk mencari daftar sumber daya AFT terbaru. Pasangan kunci-nilai untuk pencarian Anda adalah:

```
Key: managed_by | Value: AFT
```

- Untuk layanan komponen yang tidak mendukung tag, Anda dapat menemukan sumber daya dengan pencarian `aft` di nama sumber daya.

> **Note**
>
> AFT tidak membuat sumber daya AWS Cadangan apa pun di akun manajemen.

Tabel sumber daya yang awalnya dibuat, berdasarkan akun

AWS Control Tower Account Factory untuk akun manajemen Terraform

AWS layanan	Tipe sumber daya	Nama sumber daya
AWS Identity and Access Management	Peran	AWSAFTAdmin AWSAFTExecution AWSAFTService ct-aft-* aft-* codebuild_trigger_role python-layer-builder-aft-common-*
AWS Identity and Access Management	Kebijakan	aft-*
CodeCommit	Repositori	aft-*

AWS layanan	Tipe sumber daya	Nama sumber daya
CodeBuild	Membangun Proyek	aft-* ct-aft-* python-layer-builder-aft-common-*
Kode Pipa	Jalur	*YourAccountId* -customizations-pipeline
Amazon S3	Kategori	aft-*
Amazon S3	Kategori	aft-plan-output-*
Lambda	Fungsi	aft-*
Lambda	Lapisan	aft-common-*
DynamoDB	Tabel	aft-request aft-request-audit aft-request-metadata aft-controltower-events
Step Functions	Mesin Negara	aft-account-provisioning-customizations aft-account-provisioning-framework aft-feature-options aft-invoke-customizations
VPC	VPC	aft-management-vpc

AWS layanan	Tipe sumber daya	Nama sumber daya
Amazon SNS	Topik	aft-notifications aft-failure-notifications
Amazon EventBridge	Bus peristiwa	aft-events-from-ct-management
Amazon EventBridge	Aturan acara	aft-account-provisioning-customizations-trigger aft-account-request-codepipeline-trigger aft-lambda-account-request-processor aft-controltower-event-logger
Layanan Manajemen Kunci (KMS)	Kunci yang Dikelola Pelanggan	aft-backend-*-kms-key aft
AWS Systems Manager	Menyimpan parameter	/aft/*
Amazon SQS	Antrean	aft-account-request.fifo aft-account-request-dlg.fifo
CloudWatch	Grup log	/aws/*/ct-aft-* /aws/*/aft-* /aws/codebuild/python-layer-builder-aft-common-*
AWS Backup	Vault	aft-controltower-backup-vault
AWS Backup	Rencana	aft-controltower-backup-plan

AWS layanan	Tipe sumber daya	Nama sumber daya
AWS Support Center (Opsional)	Paket Support	Enterprise

AWS akun yang disediakan melalui AWS Control Tower Account Factory untuk Terraform

AWS layanan	Tipe sumber daya	Nama sumber daya
AWS Identity and Access Management	Peran	AWSAFTExecution
AWS Support Center (Opsional)	Paket Support	Enterprise

Akun manajemen AWS Control Tower

AWS layanan	Tipe sumber daya	Nama sumber daya
AWS Identity and Access Management	Peran	AWSAFTExecution AWSAFTService aft-controltower-events-rule
AWS Systems Manager	Menyimpan parameter	/aft/*
EventBridge	Aturan acara	aft-capture-ct-events
CloudTrail (Opsional)	Jalan setapak	aws-aft-CustomizationsCloud Trail
Pusat Dukungan AWS (Opsional)	Paket Support	Enterprise

Akun arsip log AWS Control Tower

AWS layanan	Tipe sumber daya	Nama sumber daya
AWS Identity and Access Management	Peran	AWSAFTExecution AWSAFTService
Layanan Manajemen Kunci (KMS)	Kunci yang Dikelola Pelanggan	aft
Amazon S3	Kategori	aws-aft-logs-* aws-aft-s3-access-logs-*
AWS Support Center (Opsional)	Paket Support	Enterprise

Akun audit AWS Control Tower

AWS layanan	Tipe sumber daya	Nama sumber daya
AWS Identity and Access Management	Peran	AWSAFTExecution AWSAFTService
AWS Support Center (Opsional)	Paket Support	Enterprise

Peran yang diperlukan

Secara umum, peran dan kebijakan adalah bagian dari manajemen identitas dan akses (IAM) di AWS. Lihat Panduan Pengguna AWS IAM untuk informasi selengkapnya.

AFT membuat beberapa peran dan kebijakan IAM dalam manajemen AFT dan akun manajemen AWS Control Tower untuk mendukung operasi pipa AFT. Peran-peran ini dibuat berdasarkan model akses hak istimewa terendah, yang membatasi izin ke kumpulan tindakan dan sumber daya yang diperlukan minimal untuk setiap peran dan kebijakan. Peran dan kebijakan ini diberi `key:value` pasangan AWS tag, seperti `managed_by:AFT` untuk identifikasi.

Selain peran IAM ini, AFT menciptakan tiga peran penting:

- per `AWSAFTAdmin` annya
- per `AWSAFTExecution` annya
- per `AWSAFTService` annya

Peran-peran ini dijelaskan di bagian berikut.

Peran AwSaftAdmin, dijelaskan

Saat Anda menerapkan AFT, `AWSAFTAdmin` peran dibuat di akun manajemen AFT. Peran ini memungkinkan pipeline AFT untuk mengambil `AWSAFTExecution` peran dalam AWS Control Tower dan akun yang disediakan AFT, sehingga melakukan tindakan yang terkait dengan penyediaan dan penyesuaian akun.

Berikut adalah kebijakan sebaris (artefak JSON) yang dilampirkan pada `AWSAFTAdmin` peran:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": [
                "arn:aws:iam::*:role/AWSAFTExecution",
                "arn:aws:iam::*:role/AWSAFTService"
            ]
        }
    ]
}
```

Artefak JSON berikut menunjukkan hubungan kepercayaan untuk `AWSAFTAdmin` peran tersebut. Nomor placeholder `012345678901` diganti dengan nomor ID akun manajemen AFT.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Peran AWSAFTexecution, dijelaskan

Saat Anda menerapkan AFT, `AWSAFTExecution` peran dibuat di manajemen AFT dan akun manajemen AWS Control Tower. Kemudian, pipeline AFT membuat `AWSAFTExecution` peran di setiap akun yang disediakan AFT selama tahap penyediaan akun AFT.

AFT menggunakan `AWSControlTowerExecution` peran pada awalnya, untuk membuat `AWSAFTExecution` peran dalam akun tertentu. `AWSAFTExecution`Peran ini memungkinkan pipeline AFT untuk menjalankan langkah-langkah yang dilakukan selama tahap penyesuaian penyediaan dan penyediaan kerangka kerja AFT, untuk akun yang disediakan AFT dan untuk akun bersama.

> **Peran yang berbeda membantu Anda membatasi ruang lingkup**
>
> Sebagai praktik terbaik, pisahkan izin penyesuaian dari izin yang diizinkan selama penerapan sumber daya awal Anda. Ingatlah bahwa `AWSAFTService` peran dimaksudkan untuk penyediaan akun, dan `AWSAFTExecution` peran dimaksudkan untuk penyesuaian akun. Pemisahan ini membatasi ruang lingkup izin yang diizinkan selama setiap fase pipa. Perbedaan ini sangat penting jika Anda menyesuaikan akun bersama AWS Control Tower, karena akun bersama mungkin berisi informasi sensitif, seperti detail penagihan atau informasi pengguna.

Izin untuk `AWSAFTExecution` peran: AdministratorAccess — kebijakan terkelola AWS

Artefak JSON berikut menunjukkan kebijakan IAM (hubungan kepercayaan) yang dilampirkan pada peran. `AWSAFTExecution` Nomor placeholder `012345678901` diganti dengan nomor ID akun manajemen AFT.

Kebijakan kepercayaan untuk `AWSAFTExecution`

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Peran AWSAFTService, dijelaskan

`AWSAFTService`Peran menerapkan sumber daya AFT di semua akun terdaftar dan dikelola, termasuk akun bersama dan akun manajemen. Sumber daya sebelumnya dikerahkan oleh `AWSAFTExecution` peran saja.

`AWSAFTService`Peran dimaksudkan untuk digunakan oleh infrastruktur layanan untuk menyebarkan sumber daya selama tahap penyediaan, dan `AWSAFTExecution` peran dimaksudkan untuk digunakan hanya untuk menerapkan penyesuaian. Dengan mengasumsikan peran dengan cara ini, Anda dapat mempertahankan kontrol akses yang lebih terperinci selama setiap tahap.

Izin untuk `AWSAFTService` peran: AdministratorAccess — kebijakan terkelola AWS

Artefak JSON berikut menunjukkan kebijakan IAM (hubungan kepercayaan) yang dilampirkan pada peran. `AWSAFTService` Nomor placeholder `012345678901` diganti dengan nomor ID akun manajemen AFT.

Kebijakan kepercayaan untuk `AWSAFTService`

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Layanan komponen

Saat Anda menerapkan AFT, komponen ditambahkan ke AWS lingkungan Anda dari masing-masing AWS layanan ini.

- AWS Control Tower — AFT menggunakan AWS Control Tower Account Factory di akun manajemen AWS Control Tower untuk menyediakan akun.
- Amazon DynamoDB — AFT membuat tabel Amazon DynamoDB di akun manajemen AFT, yang menyimpan permintaan akun, riwayat audit pembaruan akun, metadata akun, dan peristiwa siklus hidup AWS Control Tower. AFT juga membuat pemicu DynamoDB Lambda untuk memulai proses hilir, seperti memulai alur kerja penyediaan akun AFT.
- Amazon Simple Storage Service — AFT membuat bucket Amazon Simple Storage Service (S3) di akun manajemen AFT dan akun arsip log AWS Control Tower, yang menyimpan log yang dihasilkan oleh AWS layanan yang dibutuhkan pipeline AFT. AFT juga membuat bucket S3 backend Terraform, dalam primer dan sekunder Wilayah AWS, untuk menyimpan status Terraform yang dihasilkan selama alur kerja pipa AFT.
- Layanan Pemberitahuan Sederhana Amazon — AFT membuat topik Amazon Simple Notification Service (SNS) di akun manajemen AFT, yang menyimpan pemberitahuan keberhasilan dan kegagalan setelah memproses setiap permintaan akun AFT. Anda dapat menerima pesan-pesan ini menggunakan protokol pilihan Anda.
- Layanan Antrian Sederhana Amazon — AFT membuat antrian FIFO Amazon Simple Queuing Service (Amazon SQS) di akun manajemen AFT. Antrian memungkinkan Anda mengirimkan

beberapa permintaan akun secara paralel, tetapi mengirimkan satu permintaan pada satu waktu ke AWS Control Tower Account Factory, untuk pemrosesan berurutan.

- AWS CodeBuild — AFT membuat proyek CodeBuild build AWS di akun manajemen AFT untuk menginisialisasi, mengkompilasi, menguji, dan menerapkan rencana Terraform untuk kode sumber AFT di berbagai tahap pembuatan.
- AWS CodePipeline — AFT membuat CodePipeline pipeline AWS di akun manajemen AFT untuk diintegrasikan dengan penyedia CodeStar koneksi AWS yang dipilih dan didukung untuk kode sumber AFT, dan untuk memicu pekerjaan build di AWS CodeBuild.
- AWS Lambda — AFT membuat fungsi dan lapisan AWS Lambda di akun manajemen AFT untuk melakukan langkah-langkah selama proses permintaan akun, penyediaan akun AFT, dan penyesuaian akun.
- Penyimpanan Parameter AWS Systems Manager — AFT menyiapkan Penyimpanan Parameter AWS Systems Manager di akun manajemen AFT, untuk menyimpan parameter konfigurasi yang diperlukan untuk proses pipeline AFT.
- Amazon CloudWatch — AFT membuat grup CloudWatch log Amazon di akun manajemen AFT untuk menyimpan log yang dihasilkan oleh layanan AWS yang digunakan oleh pipa AFT. Periode retensi untuk CloudWatch log diatur ke`Never Expire`.
- Amazon VPC — AFT membuat Amazon Virtual Private Cloud (VPC) untuk mengisolasi layanan dan sumber daya dalam akun manajemen AFT ke dalam lingkungan jaringan terpisah, untuk meningkatkan keamanan.
- AWS KMS — AFT menggunakan AWS Key Management Service (KMS) di akun manajemen AFT dan di akun arsip log AWS Control Tower. AFT membuat kunci untuk mengenkripsi status Terraform, data yang disimpan dalam tabel DynamoDB, dan topik SNS. Log dan artefak ini dihasilkan saat sumber daya dan layanan AWS digunakan oleh AFT. Kunci KMS yang dibuat oleh AFT mengaktifkan rotasi tahunan secara default.
- AWS Identity and Access Management (IAM) — AFT mengikuti model hak istimewa terkecil yang direkomendasikan. Ini membuat peran dan kebijakan Manajemen AWS Identitas dan Akses (IAM) di akun manajemen AFT, di akun AWS Control Tower, dan di akun yang disediakan AFT, sesuai kebutuhan, untuk melakukan tindakan yang diperlukan selama alur kerja saluran AFT.
- AWS Fungsi Langkah - AFT AWS membuat mesin status Fungsi Langkah di akun manajemen AFT. Mesin status ini mengatur dan mengotomatiskan proses dan langkah-langkah untuk kerangka kerja penyediaan akun AFT dan penyesuaian.
- Amazon EventBridge — AFT membuat bus EventBridge acara Amazon di akun manajemen AFT dan AWS Control Tower untuk menangkap dan menyimpan peristiwa siklus hidup AWS Control

Tower dalam jangka panjang di tabel DynamoDB akun manajemen AFT. AFT membuat aturan CloudWatch acara Amazon di manajemen AFT dan akun manajemen AWS Control Tower, yang memicu beberapa langkah yang diperlukan selama menjalankan alur kerja pipa AFT

- AWS CloudTrail (Opsional) — Saat fitur ini diaktifkan, AFT membuat jejak AWS CloudTrail organisasi di akun manajemen AWS Control Tower, untuk mencatat peristiwa data untuk bucket Amazon S3 dan fungsi AWS Lambda. AFT mengirimkan log ini ke bucket S3 pusat di akun arsip log AWS Control Tower.
- AWS Dukungan (Opsional) — Saat fitur ini diaktifkan, AFT mengaktifkan paket AWS Dukungan Perusahaan untuk akun yang disediakan oleh AFT. Secara default, AWS akun dibuat dengan paket Dukungan AWS Dasar diaktifkan.

Saluran penyediaan akun AFT

Setelah tahap penyediaan akun dari pipeline selesai, kerangka kerja AFT berlanjut. Secara otomatis menjalankan serangkaian langkah untuk memastikan bahwa akun yang baru disediakan memiliki detail di tempat, sebelum Kustomisasi akun tahap dimulai.

Berikut adalah langkah-langkah selanjutnya yang dijalankan oleh pipa AFT.

1. Memvalidasi input permintaan akun.
2. Mengambil informasi tentang akun yang disediakan, misalnya, ID akun.
3. Menyimpan metadata akun dalam tabel DynamoDB di akun manajemen AFT.
4. Membuat peran A wSaftExecution IAM di akun yang baru disediakan. AFT mengambil peran ini untuk melakukan tahap penyesuaian akun, karena peran ini memberikan akses ke portofolio pabrik akun.
5. Menerapkan tag akun yang Anda berikan sebagai bagian dari parameter input permintaan akun.
6. Menerapkan opsi fitur AFT yang Anda pilih pada saat penyebaran AFT.
7. Menerapkan penyesuaian penyediaan akun AFT yang Anda berikan. Bagian selanjutnya menceritakan lebih lanjut tentang cara mengatur penyesuaian ini dengan mesin status AWS Step Functions, di `git` repositori. Tahap ini kadang-kadang disebut sebagai tahap kerangka kerja penyediaan akun. Ini adalah bagian dari proses penyediaan inti, tetapi sebelumnya Anda telah menyiapkan kerangka kerja yang memberikan integrasi khusus sebagai bagian dari alur kerja penyediaan akun Anda, sebelum penyesuaian tambahan ditambahkan ke akun di tahap berikutnya.

8. Untuk setiap akun yang disediakan, itu membuat akun AWS CodePipeline manajemen AFT, yang akan dijalankan untuk melakukan Kustomisasi akun tahap (berikutnya, global).
9. Memanggil pipeline penyesuaian akun untuk setiap akun yang disediakan (dan ditargetkan).
10. Mengirim pemberitahuan sukses atau gagal ke topik SNS, dari mana Anda dapat mengambil pesan.

Menyiapkan penyesuaian kerangka kerja penyediaan akun dengan mesin status

Jika Anda menyiapkan integrasi kustom non-TerraForm sebelum Anda menyediakan akun, penyesuaian ini disertakan dalam alur kerja penyediaan akun AFT Anda. Misalnya, Anda mungkin memerlukan penyesuaian tertentu untuk memastikan bahwa semua akun yang dibuat oleh AFT sesuai dengan standar dan kebijakan organisasi Anda, seperti standar keamanan, dan standar ini dapat ditambahkan ke akun sebelum penyesuaian tambahan. Ku stomisasi kerangka penyediaan akun ini diimplementasikan pada setiap akun yang disediakan, sebelum tahap penyesuaian akun global dimulai berikutnya.

> **Note**
>
> Fitur AFT yang dijelaskan di bagian ini ditujukan untuk pengguna tingkat lanjut yang memahami fungsi AWS Step Functions. Sebagai alternatif, kami menyarankan Anda bekerja dengan pembantu global di tahap penyesuaian akun.

Kerangka penyediaan akun AFT memanggil mesin status AWS Step Functions, yang Anda tentukan, untuk mengimplementasikan penyesuaian Anda. Lihat dokumentasi AWS Step Functions untuk mempelajari selengkapnya tentang kemungkinan integrasi mesin status.

Berikut adalah beberapa integrasi umum.

- AWS Lambda berfungsi dalam bahasa pilihan Anda
- Tugas AWS ECS atau AWS Fargate, menggunakan wadah Docker
- Aktivitas AWS Step Functions menggunakan pekerja khusus, dihosting baik di AWS atau di lokasi
- Integrasi Amazon SNS atau SQS

Jika tidak ada mesin status AWS Step Functions yang ditentukan, tahap berlalu dengan no-op. Untuk membuat mesin status penyesuaian penyediaan akun AFT, ikuti instruksi di. Buat mesin status

penyesuaian penyediaan akun AFT Anda Sebelum menambahkan penyesuaian, pastikan Anda memiliki prasyarat.

Jenis integrasi ini bukan bagian dari AWS Control Tower, dan tidak dapat ditambahkan selama tahap pra-API global dari kustomisasi akun AFT. Sebagai gantinya, pipeline AFT memungkinkan Anda untuk mengatur penyesuaian ini sebagai bagian dari proses penyediaan, dan mereka dijalankan dalam alur kerja penyediaan. Anda harus menerapkan penyesuaian ini dengan membuat mesin status Anda sebelumnya, sebelum memulai tahap penyediaan akun AFT, seperti yang dijelaskan di bagian berikut.

Prasyarat untuk membuat mesin negara

- AFT yang dikerahkan sepenuhnya. Lihat Terapkan AWS Control Tower Account Factory untuk Terraform (AFT) untuk informasi selengkapnya tentang penerapan AFT.
- Siapkan `git` repositori di lingkungan Anda untuk penyesuaian penyediaan akun AFT. Untuk informasi selengkapnya, lihat Post-deployment langkah.

Buat mesin status penyesuaian penyediaan akun AFT Anda

Langkah 1: Ubah definisi mesin negara

Ubah contoh definisi mesin `customizations.asl.json` status. Contoh ini tersedia di `git` repositori yang Anda atur untuk menyimpan kustomisasi penyediaan akun AFT, dalam langkah-langkah pasca-penerapan Anda. Lihat Panduan Pengembang AWS Step Functions untuk mempelajari selengkapnya tentang definisi mesin status.

Langkah 2: Sertakan konfigurasi Terraform yang sesuai

Sertakan file Terraform dengan `.tf` ekstensi di `git` repositori yang sama dengan definisi mesin status untuk integrasi kustom Anda. Misalnya, jika Anda memilih untuk memanggil fungsi Lambda dalam definisi tugas mesin negara Anda, Anda akan menyertakan `lambda.tf` file dalam direktori yang sama. Pastikan Anda menyertakan peran dan izin IAM yang diperlukan untuk konfigurasi kustom Anda.

Saat Anda memberikan input yang sesuai, pipeline AFT secara otomatis memanggil mesin status Anda dan menerapkan penyesuaian Anda sebagai bagian dari tahap kerangka kerja penyediaan akun AFT.

Untuk memulai kembali kerangka kerja penyediaan akun AFT dan penyesuaian

AFT menjalankan kerangka kerja penyediaan akun dan langkah-langkah penyesuaian untuk setiap akun yang dijual melalui pipa AFT. Untuk memulai kembali penyesuaian penyediaan akun, Anda dapat menggunakan salah satu dari dua metode berikut:

1. Buat perubahan apa pun pada akun yang ada di repo permintaan akun.
2. Menyediakan akun baru dengan AFT.

Kustomisasi akun

AFT dapat menerapkan konfigurasi standar atau khusus di akun yang disediakan. Di akun manajemen AFT, AFT menyediakan satu pipeline untuk setiap akun. Dengan pipeline ini, Anda dapat menerapkan penyesuaian di semua akun, dalam satu set akun, atau di akun individual. Anda dapat menjalankan skrip Python, skrip bash, dan konfigurasi Terraform, atau Anda dapat berinteraksi dengan AWS CLI sebagai bagian dari tahap penyesuaian akun Anda.

Gambaran umum

Setelah kustomisasi Anda ditentukan dalam `git` repositori pilihan Anda, baik tempat Anda menyimpan penyesuaian global atau tempat Anda menyimpan penyesuaian akun, tahap penyesuaian akun diselesaikan secara otomatis oleh pipeline AFT. Untuk menyesuaikan akun secara surut, lihatRe-invoke kustomisasi.

Kustomisasi global (opsional)

Anda dapat memilih untuk menerapkan penyesuaian tertentu ke semua akun yang disediakan oleh AFT. Misalnya, jika Anda perlu membuat peran IAM tertentu, atau menerapkan kontrol kustom di setiap akun, tahap penyesuaian global dalam pipeline AFT memungkinkan Anda melakukannya, secara otomatis.

Kustomisasi akun (opsional)

Untuk menyesuaikan akun individual, atau satu set akun, secara berbeda dari akun yang disediakan AFT lainnya, Anda dapat memanfaatkan bagian penyesuaian akun dari pipeline AFT untuk menerapkan konfigurasi khusus akun. Misalnya, hanya akun tertentu yang mungkin memerlukan akses ke gateway internet.

Prasyarat kustomisasi

Sebelum Anda mulai menyesuaikan akun, pastikan prasyarat ini sudah ada.

- AFT yang sepenuhnya dikerahkan. Untuk informasi tentang cara menerapkan, lihatKonfigurasikan dan luncurkan AWS Control Tower Account Factory untuk Terraform.
- Pre-populated `git`repositori untuk kustomisasi global dan kustomisasi akun di lingkungan Anda. Lihat Mengisi setiap repositori Post-deployment langkah untuk informasi selengkapnya.

Terapkan kustomisasi global

Untuk menerapkan penyesuaian global, Anda harus mendorong struktur folder tertentu ke repositori pilihan Anda.

- Jika konfigurasi kustom Anda dalam bentuk program atau skrip Python, letakkan api_helpers/pythondi bawah folder di repositori Anda.
- Jika konfigurasi kustom Anda dalam bentuk skrip Bash, letakkan di bawah folder api_helpers di repositori Anda.
- Jika konfigurasi khusus Anda dalam bentuk Terraform, letakkan di bawah folder terraform di repositori Anda.
- Lihat file README kustomisasi global untuk detail selengkapnya tentang membuat konfigurasi kustom.

> **Note**
>
> Kustomisasi global diterapkan secara otomatis, setelah tahap kerangka kerja penyediaan akun AFT di pipeline AFT.

Terapkan kustomisasi akun

Anda dapat menerapkan penyesuaian akun dengan mendorong struktur folder tertentu ke repositori pilihan Anda. Kustomisasi akun diterapkan secara otomatis di pipeline AFT dan setelah tahap penyesuaian global. Anda juga dapat membuat beberapa folder yang berisi penyesuaian akun yang berbeda di repositori penyesuaian akun Anda. Untuk setiap kustomisasi akun yang Anda butuhkan, gunakan langkah-langkah berikut.

Untuk menerapkan kustomisasi akun

1. Langkah 1: Buat folder untuk kustomisasi akun

   Di repositori pilihan Anda, salin `ACCOUNT_TEMPLATE` folder yang disediakan AFT ke folder baru. Nama folder baru Anda harus sesuai dengan `account_customizations_name` yang Anda berikan dalam permintaan akun Anda.

2. Tambahkan konfigurasi ke folder kustomisasi akun spesifik Anda

   Anda dapat menambahkan konfigurasi ke folder penyesuaian akun Anda berdasarkan format konfigurasi Anda.

   - Jika konfigurasi kustom Anda dalam bentuk program atau skrip Python, letakkan di bawah folderapi_helpers/python/yang ada ***`[account_customizations_name]`***di repositori Anda.
   - Jika konfigurasi kustom Anda dalam bentuk skrip Bash, letakkan di bawah folder ***`[account_customizations_name]`***/api_helpers yang ada di repositori Anda.
   - Jika konfigurasi khusus Anda dalam bentuk Terraform, letakkan di bawah folder ***`[account_customizations_name]`***/terraform yang ada di repositori Anda.

   Untuk informasi selengkapnya tentang membuat konfigurasi kustom, lihat file README penyesuaian akun.

3. Lihat **`account_customizations_name`** parameter spesifik dalam file permintaan akun

   File permintaan akun AFT menyertakan parameter input`account_customizations_name`. Masukkan nama kustomisasi akun Anda sebagai nilai untuk parameter ini.

> **Note**
>
> Anda dapat mengirimkan beberapa permintaan akun untuk akun di lingkungan Anda. Bila Anda ingin menerapkan kustomisasi akun yang berbeda atau serupa, tentukan kustomisasi akun menggunakan parameter `account_customizations_name` input dalam permintaan akun Anda. Untuk informasi selengkapnya, lihat Mengirimkan beberapa permintaan akun.

Re-invoke kustomisasi

AFT menyediakan cara untuk memanggil kembali penyesuaian di pipeline AFT. Metode ini berguna ketika Anda telah menambahkan langkah penyesuaian baru, atau ketika Anda membuat perubahan pada kustomisasi yang ada. Saat Anda memanggil ulang, AFT memulai pipeline penyesuaian untuk membuat perubahan pada akun yang disediakan AFT. Pemanggilan ulang berbasis sumber peristiwa memungkinkan Anda menerapkan penyesuaian ke akun individual, ke semua akun, ke akun sesuai dengan OU mereka, atau ke akun yang dipilih sesuai dengan tag.

Ikuti tiga langkah ini untuk memanggil kembali penyesuaian untuk akun. AFT-provisioned

Langkah 1: Dorong perubahan ke repositori kustomisasi **`git`** global atau akun

Anda dapat memperbarui penyesuaian global dan akun sesuai kebutuhan dan mendorong perubahan kembali ke repositori Anda`git`. Pada titik ini, tidak ada yang terjadi, Pipa penyesuaian harus dipanggil oleh sumber acara, seperti yang dijelaskan dalam dua langkah berikutnya.

Langkah 2: Mulai AWS Step Function untuk menjalankan kembali kustomisasi

AFT menyediakan AWS Step Function yang disebut `aft-invoke-customizations` di akun manajemen AFT. Tujuan dari fungsi itu adalah untuk memanggil kembali pipeline kustomisasi untuk AFT-provisioned akun.

Berikut adalah contoh skema acara (format JSON) yang dapat Anda buat untuk meneruskan input ke `aft-invoke-customizations` AWS Step Function.

```
{
  "include": [
    {
      "type": "all"
    },
    {
      "type": "ous",
      "target_value": [ "ou1","ou2"]
    },
    {
      "type": "tags",
      "target_value": [ {"key1": "value1"}, {"key2": "value2"}]
    },
    {
      "type": "accounts",
```

```
      "target_value": [ "acc1_ID","acc2_ID"]
    }
  ],

  "exclude": [
    {
      "type": "ous",
      "target_value": [ "ou1","ou2"]
    },
    {
      "type": "tags",
      "target_value": [ {"key1": "value1"}, {"key2": "value2"}]
    },
    {
      "type": "accounts",
      "target_value": [ "acc1_ID","acc2_ID"]
    }
  ]
}
```

Contoh skema acara menunjukkan bahwa Anda dapat memilih akun untuk disertakan atau dikecualikan dari proses pemanggilan ulang. Anda dapat memfilter berdasarkan unit organisasi (OU), tag akun, dan ID akun. Jika Anda tidak menerapkan filter apa pun dan menyertakan pernyataan`"type":"all"`, penyesuaian untuk semua AFT-provisioned akun akan dipanggil kembali.

Anda dapat menyertakan `bypass_steps` parameter dalam input Step Functions untuk melewati fase penyediaan tertentu selama pemanggilan ulang.

Nilai **`bypass_steps`**	Perilaku
`["provisioning_bootstrap"]`	Melewati penyediaan akun dan fase bootstrap; hanya menjalankan akun dan saluran kustomisasi global.
`[]`(kosong)	Menjalankan aliran penuh termasuk penyediaan (default).

Contoh berikut menunjukkan input Step Functions yang memanggil kembali kustomisasi untuk akun tertentu sambil melewati langkah-langkah penyediaan dan bootstrap.

```
{
```

```
  "include": [
    {
      "type": "accounts",
      "target_value": ["123456789012"]
    }
  ],
  "bypass_steps": ["provisioning_bootstrap"]
}
```

> **Note**
>
> Jika versi AWS Control Tower Account Factory for Terraform (AFT) Anda adalah 1.6.5 atau yang lebih baru, Anda dapat menargetkan OU bersarang dengan sintaks). `OU Name (ou-id-1234` Untuk informasi lebih lanjut, lihat topik berikut di GitHub.

Untuk melihat pratinjau perubahan yang akan dilakukan AFT ke akun tanpa menerapkannya, gunakan proses khusus rencana. Untuk memulainya, sertakan `plan_only` parameter yang diatur ke `true` dalam input Step Functions. Saat Anda menyetel`"plan_only": true`, AFT berjalan `terraform plan` untuk penyesuaian global dan akun Anda, bukan. `terraform apply` Anda kemudian dapat meninjau perubahan yang akan diterima akun sebelum Anda menerapkannya. Plan-only menjalankan pekerjaan di semua distribusi Terraform yang didukung, termasuk Edisi Komunitas, HCP Terraform (Terraform Cloud), dan Terraform Enterprise.

Contoh berikut menunjukkan input Step Functions yang menjalankan plan-only run untuk akun tertentu dengan menyetel `plan_only` ke `true` dan menentukan ID akun di blok. `include`

```
{
  "include": [
    {
      "type": "accounts",
      "target_value": ["123456789012"]
    }
  ],
  "plan_only": true
}
```

Dalam contoh sebelumnya, ganti nilai berikut dengan informasi Anda sendiri:

- `123456789012`— Ganti nilai ini dengan ID akun AWS yang ingin Anda targetkan untuk menjalankan rencana saja.

Setelah Anda meninjau output paket, jalankan kembali pipeline kustomisasi tanpa `plan_only` parameter (berjalan normal) untuk menerapkan perubahan ke akun Anda.

> **Note**
>
> Pada distribusi Edisi Komunitas (open source), AFT mengekspor output JSON setiap paket ke bucket Amazon S3 keluaran rencana terenkripsi di akun manajemen AFT. Ekspor ini terjadi pada setiap proses khusus rencana. Pada distribusi HCP Terraform (Terraform Cloud) dan Terraform Enterprise, Anda dapat melihat hasil paket di UI run HCP Terraform. Anda juga dapat secara opsional mengekspor output JSON setiap paket ke bucket. Untuk informasi selengkapnya, lihat Ekspor output paket Terraform ke Amazon S3.

Setelah Anda mengisi parameter acara, Step Functions berjalan dan memanggil penyesuaian yang sesuai. AFT dapat memanggil maksimal 5 penyesuaian sekaligus. Step Functions menunggu dan mengulang sampai semua akun yang cocok dengan kriteria acara selesai.

Langkah 3: Pantau output AWS Step Function dan saksikan AWS CodePipeline berjalan

- Output Step Function yang dihasilkan berisi ID akun yang cocok dengan sumber peristiwa masukan Fungsi Langkah.
- Arahkan ke AWS CodePipeline di bawah Alat Pengembang dan lihat pipeline penyesuaian yang sesuai untuk ID akun.

Pemecahan masalah dengan penelusuran permintaan kustomisasi akun AFT

Alur kerja kustomisasi akun yang didasarkan pada log AWS Lambda emit yang berisi akun target dan ID permintaan kustomisasi. AFT memungkinkan Anda melacak dan memecahkan masalah permintaan kustomisasi dengan Amazon CloudWatch Logs dengan menyediakan kueri Wawasan CloudWatch Log yang dapat Anda gunakan untuk memfilter CloudWatch Log yang terkait dengan permintaan penyesuaian berdasarkan akun target atau ID permintaan kustomisasi. Untuk informasi selengkapnya, lihat Menganalisis data log dengan CloudWatch Log Amazon di Panduan Pengguna CloudWatch Log Amazon.

Untuk menggunakan Wawasan CloudWatch Log untuk AFT

1. Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
2. Dari panel navigasi, pilih Log, lalu pilih Wawasan log.
3. Pilih Kueri.
4. Di bawah Contoh kueri, pilih Account Factory untuk Terraform, lalu pilih salah satu kueri berikut:

   - Log Kustomisasi berdasarkan ID Akun

     > **Note**
     >
     > Pastikan untuk mengganti *"YOUR-ACCOUNT-ID"* dengan ID akun target Anda.

     ```
     fields @timestamp, log_message.account_id as target_account_id,
      log_message.customization_request_id as customization_request_id,
      log_message.detail as detail, @logStream
     | sort @timestamp desc
     | filter log_message.account_id == "YOUR-ACCOUNT-ID" and @message like /
     customization_request_id/
     ```

   - Log Kustomisasi dengan ID Permintaan Kustomisasi

     > **Note**
     >
     > Pastikan untuk mengganti *"YOUR-CUSTOMIZATION-REQUEST-ID"* dengan ID permintaan kustomisasi Anda. Anda dapat menemukan ID permintaan kustomisasi Anda di output mesin AWS Step Functions status kerangka kerja penyediaan akun AFT. Untuk informasi selengkapnya tentang kerangka kerja penyediaan akun AFT, lihat pipeline penyediaan akun AFT

     ```
     fields @timestamp, log_message.account_id as target_account_id,
      log_message.customization_request_id as customization_request_id,
      log_message.detail as detail, @logStream
     | sort @timestamp desc
     | filter log_message.customization_request_id == "YOUR-CUSTOMIZATION-REQUEST-ID"
     ```

5. Setelah Anda memilih kueri, pastikan untuk memilih interval waktu, lalu pilih Jalankan kueri.

Pemicu kustomisasi

Pemicu kustomisasi Account Factory for Terraform (AFT) mengotomatiskan eksekusi ulang akun dan penyesuaian global saat akun berpindah antar unit organisasi (OU). Seiring perkembangan organisasi Anda, akun sering bertransisi antar OU untuk mencerminkan perubahan dalam kepemilikan tim, persyaratan kepatuhan, atau klasifikasi beban kerja. Tanpa pemicu penyesuaian, setiap langkah memerlukan intervensi manual untuk menerapkan kembali penyesuaian yang selaras dengan konteks organisasi baru akun.

Dengan mengaktifkan pemicu kustomisasi, AFT mendeteksi perubahan OU dan secara otomatis memanggil pipeline kustomisasi Anda untuk akun yang terpengaruh. Ini memastikan bahwa akun selalu menjalankan penyesuaian yang sesuai dengan penempatan OU mereka saat ini, mengurangi overhead operasional dan meminimalkan risiko penyimpangan konfigurasi. Misalnya, ketika akun berpindah dari OU Pengembangan ke OU Produksi, pemicu penyesuaian dapat secara otomatis menerapkan kontrol keamanan khusus produksi dan kebijakan kepatuhan tanpa intervensi manual.

> **Important**
>
> Akun yang diperbarui melalui fitur Auto Enroll di AWS Control Tower landing zone tidak memancarkan peristiwa siklus `UpdateManagedAccount` hidup. Pemicu kustomisasi tidak menyala untuk operasi tersebut. Jika Anda mengandalkan Auto Enroll untuk membawa akun di bawah manajemen AWS Control Tower, Anda harus memanggil ulang penyesuaian secara manual untuk akun tersebut.

Cara kerja pemicu kustomisasi

Saat pemicu penyesuaian diaktifkan dan AFT memproses peristiwa penyediaan akun, pemicu akan mengevaluasi apakah OU akun telah berubah dan mengambil tindakan yang tepat.

1. AFT mendeteksi perubahan OU dengan membandingkan OU akun saat ini dengan OU yang direkam sebelumnya.
2. Jika OU berubah, AFT memperkaya eksekusi dengan konteks pemicu, termasuk sumber dan tujuan OU.
3. AFT memanggil pipeline kustomisasi, melewati langkah-langkah penyediaan dan bootstrap yang telah selesai. Untuk detail tentang konfigurasi bypass, lihatthe section called “Re-invoke kustomisasi”.

4. AFT mencatat entri audit dengan sumber pemicu dan akun target.

Jika fitur dinonaktifkan atau jika OU tidak berubah, penyediaan standar berlanjut tanpa memicu eksekusi ulang kustomisasi.

Mengkonfigurasi pemicu kustomisasi

Untuk mengaktifkan pemicu penyesuaian, setel `aft_customization_triggers` variabel dalam modul penerapan AFT Anda:

```
module "aft" {
  source = "github.com/aws-ia/terraform-aws-control_tower_account_factory"

  aft_customization_triggers = ["account_move"]

  # ... other variables
}
```

Satu-satunya nilai yang valid adalah `"account_move"`. Untuk menonaktifkan pemicu kustomisasi, atur variabel ke daftar kosong (`[]`). Fitur ini dinonaktifkan secara default.

Untuk mengecualikan akun tertentu dari pemrosesan pemicu otomatis, setel `account_skip_customization_triggers` atribut ke `"true"` akun target dalam file Terraform permintaan akun. Ketika atribut ini disetel, AFT melewatkan pemanggilan kustomisasi untuk akun itu bahkan ketika mendeteksi perubahan OU. Ini berguna untuk akun yang menjalani migrasi terencana di mana penyesuaian ulang otomatis tidak diinginkan.

Jalur acara yang didukung

`account_move`Pemicu menyala saat AFT menerima peristiwa siklus hidup `UpdateManagedAccount` AWS Control Tower. Acara ini dipancarkan ketika:

- OU akun diubah melalui file permintaan akun AFT (pembaruan `ManagedOrganizationalUnit` parameter Terraform).
- Akun diperbarui melalui konsol AWS Control Tower.
- Akun dipindahkan menggunakan operasi Register OU atau Account Factory (konsol atau Service Catalog API).

> **Important**
>
> Akun yang diperbarui melalui fitur Auto Enroll di AWS Control Tower landing zone tidak memancarkan peristiwa siklus `UpdateManagedAccount` hidup. Pemicu penyesuaian tidak menyala untuk operasi tersebut.

Untuk informasi selengkapnya tentang peristiwa siklus hidup AWS Control Tower, lihat peristiwa Siklus Hidup di Panduan Pengguna AWS Control Tower.

Pemantauan dan keterlacakan

Setiap eksekusi kustomisasi (apakah dipicu oleh perubahan OU, pemanggilan manual, atau permintaan akun) menulis catatan audit ke tabel DynamoDB. Anda dapat menggunakan catatan ini untuk memahami mengapa kustomisasi dijalankan, akun mana yang terpengaruh, dan bagaimana eksekusi terkait dengan aktivitas pipeline lainnya.

Bidang	Deskripsi
`execution_id`	ID eksekusi Step Functions
`timestamp`	Ketika catatan dibuat
`target_accounts`	Daftar ID akun target
`bypass_steps`	Langkah-langkah penyediaan yang dilewati
`customization_triggers`	Konteks pemicu (sumber dan tujuan OU)
`trigger_source`	Mengapa eksekusi berjalan:`account_move` ,`manual`, atau `account_request`
`customization_request_id`	Menautkan eksekusi penyediaan dan penyesuaian untuk korelasi ujung ke ujung

`customization_request_id`Ini memungkinkan Anda untuk mengkorelasikan peristiwa pemicu dengan eksekusi pipa hilir di kedua mesin status Step Functions. Anda dapat menggunakan

pengenal ini untuk melacak satu perpindahan akun dari deteksi awal hingga penyelesaian penyesuaian.

Example Kueri catatan audit berdasarkan sumber pemicu

```
aws dynamodb scan \
  --table-name aft-customizations-audit \
  --filter-expression "trigger_source = :ts" \
  --expression-attribute-values '{":ts": {"S": "account_move"}}'
```

Alternatif untuk kontrol versi kode sumber di AFT

AFT digunakan AWS CodeCommit untuk sistem kontrol versi kode sumber (VCS), dan memungkinkan lainnya AWS CodeConnectionsyang memenuhi persyaratan bisnis Anda atau arsitektur yang ada.

Jika Anda menerapkan AFT untuk pertama kalinya dan Anda tidak memiliki CodeCommit repositori yang ada, Anda harus menentukan penyedia VCS eksternal, sebagai bagian dari prasyarat penerapan AFT.

AFT mendukung alternatif kontrol kode sumber berikut:

- GitHub
- GitHub Server Perusahaan
- BitBucket
- GitLab
- GitLab Self-managed
- Azure DevOps

> **Note**
>
> Jika Anda menentukan AWS CodeCommit sebagai VCS Anda, tidak ada langkah tambahan yang diperlukan. AFT membuat `git` repositori yang diperlukan di lingkungan Anda, dengan nama default. Namun, Anda dapat mengganti nama repositori default untuk CodeCommit, sesuai kebutuhan, untuk mematuhi standar organisasi Anda.

Siapkan sistem kontrol versi kode sumber alternatif (VCS khusus) dengan AFT

Untuk menyiapkan sistem kontrol versi kode sumber alternatif untuk penerapan AFT Anda, ikuti langkah-langkah berikut.

Langkah 1: Buat **`git`** repositori dalam sistem kontrol versi pihak ketiga (VCS) yang didukung.

Jika Anda tidak menggunakan AWS CodeCommit, Anda harus membuat `git` repositori di lingkungan penyedia VCS pihak ketiga Anda AFT-supported untuk item berikut.

- Permintaan akun AFT. Kode sampel tersedia. Untuk informasi selengkapnya tentang permintaan akun AFT, lihatMenyediakan akun baru dengan AFT.
- Kustomisasi penyediaan akun AFT. Kode sampel tersedia. Untuk informasi selengkapnya tentang penyesuaian penyediaan akun AFT, lihat. Buat mesin status penyesuaian penyediaan akun AFT Anda
- Kustomisasi global AFT. Kode sampel tersedia. Untuk informasi selengkapnya tentang kustomisasi global AFT, lihat. Kustomisasi akun
- Kustomisasi akun AFT. Kode sampel tersedia. Untuk informasi selengkapnya tentang penyesuaian akun AFT, lihat. Kustomisasi akun

Langkah 2: Tentukan parameter konfigurasi VCS yang diperlukan untuk penerapan AFT

Parameter input berikut diperlukan untuk mengonfigurasi penyedia VCS Anda sebagai bagian dari penerapan AFT.

- vcs_provider: Jika Anda tidak menggunakan AWS CodeCommit, tentukan penyedia VCS sebagai`"bitbucket"`,,,, `"github"` `"githubenterprise"`, atau `"gitlab"` `"gitlabselfmanaged"` `"azuredevops"`, berdasarkan kasus penggunaan Anda.
- github_enterprise_url: Hanya untuk pelanggan GitHub Enterprise, tentukan URL-nya. GitHub
- account_request_repo_name: Untuk pengguna, nilai ini diatur ke. AWS CodeCommit `aft-account-request` Di lingkungan penyedia VCS pihak ketiga AFT-supported, perbarui nilai input ini dengan nama repositori Anda yang sebenarnya. Untuk BitBucket, Github, GitHub Enterprise,, GitLab GitLab Self-managed, dan Azure DevOps, nama repositori harus memiliki format. `[Org]/[Repo]`
- account_customizations_repo_name: Untuk pengguna, nilai ini diatur ke. AWS CodeCommit `aft-account-customizations` Di lingkungan penyedia VCS pihak ketiga AFT-supported, perbarui

nilai input ini dengan nama repositori Anda. Untuk BitBucket, Github, GitHub Enterprise,, GitLab GitLab Self-managed, dan Azure DevOps, nama repositori harus memiliki format. `[Org]/[Repo]`

- account_provisioning_customizations_repo_name: Untuk pengguna, nilai ini diatur ke. AWS CodeCommit `aft-account-provisioning-customizations` Di lingkungan penyedia VCS pihak ketiga AFT-supported, perbarui nilai input ini dengan nama repositori Anda. Untuk BitBucket, Github, GitHub Enterprise,, GitLab GitLab Self-managed, dan Azure DevOps, nama repositori harus memiliki format. `[Org]/[Repo]`
- global_customizations_repo_name: Untuk pengguna, nilai ini diatur ke. AWS CodeCommit `aft-global-customizations` Di lingkungan penyedia VCS pihak ketiga AFT-supported, perbarui nilai input ini dengan nama repositori Anda. Untuk BitBucket, Github, GitHub Enterprise,, GitLab GitLab Self-managed, dan Azure DevOps, nama repositori harus memiliki format. `[Org]/[Repo]`
- account_request_repo_branch: Cabang secara default, tetapi nilainya dapat diganti`main`.

Secara default, sumber AFT dari `main` cabang setiap `git` repositori. Anda dapat mengganti nilai nama cabang dengan parameter input tambahan. Untuk informasi lebih lanjut tentang parameter input, lihat file README di modul AFT Terraform.

> **Untuk yang ada AWS CodeCommit pelanggan**
>
> Jika Anda membuat CodeCommit repositori dengan nama baru untuk AFT, Anda dapat memperbarui nama repositori dengan memperbarui nilai untuk parameter input ini.

Langkah 3: Selesaikan AWS CodeCommit koneksi untuk penyedia VCS pihak ketiga

Saat penerapan Anda berjalan, AFT membuat AWS CodeCommit repositori yang diperlukan, atau membuat AWS CodeCommit koneksi untuk penyedia VCS pihak ketiga yang Anda pilih. Dalam kasus yang terakhir, Anda harus masuk secara manual ke konsol akun manajemen AFT untuk menyelesaikan CodeCommit koneksi yang tertunda. Lihat AWS CodeCommit dokumentasi untuk instruksi lebih lanjut tentang menyelesaikan CodeCommit koneksi.

Pindahkan AFT dari AWS CodeCommit ke penyedia VCS lain

Bagian ini memberikan gambaran umum tentang cara memindahkan AWS Control Tower Account Factory for Terraform (AFT) dari AWS CodeCommit sebagai sistem kontrol versi (VCS) ke penyedia VCS lain.

Langkah 1. Siapkan repositori baru di VCS pilihan Anda.

Langkah 2. Tambahkan repositori ini sebagai remote baru. `git`

Langkah 3. J `git push` alankan ke penyedia VCS baru.

> **Note**
>
> Struktur repositori yang Anda buat harus sama seperti di AWS CodeCommit. Mengubah struktur menghambat kemampuan AFT untuk mengeksekusi kode yang diinginkan.
>
> Struktur repositori:
>
> - permintaan akun aft-
> - kustomisasi akun aft-
> - aft-global-kustomisasi
> - kustomisasi penyediaan akun aft-

Langkah 4. Di akun manajemen AWS Control Tower Anda, perbarui modul Terraform (bootstrap) untuk menunjuk ke penyedia VCS Anda, seperti yang ditunjukkan pada contoh berikut:

Contoh: GitLab dengan Terraform OSS

— Lakukan `terraform plan` untuk melihat pratinjau perubahan, lalu`terraform apply`.

Langkah 5. Selesaikan langkah-langkah untuk menyelesaikan pengaturan CodeConnection (sebelumnya dikenal sebagai CodeStar):

1. Masuk ke akun manajemen AFT Anda
2. Cari dan selesaikan proses pen AWS CodeConnections undaan untuk penyedia VCS baru, seperti yang dijelaskan dalam Memperbarui koneksi yang tertun da, atau di AWS konsol, [`https://us-east-1.console.aws.amazon.com/codesuite/settings/connections`].
3. Referensi: Post-deployment langkah

> **Note**
>
> Pipeline akun mempertahankan sumber sebelumnya sampai `aft-invoke-customizations` Fungsi Langkah dipanggil. Pemanggilan ini dapat dilakukan sebagai bagian dari peningkatan atau sebagai bagian dari pemanggilan penyesuaian berikutnya.

Untuk informasi selengkapnya, lihat blog ini: Cara memigrasikan AWS CodeCommit repositori Anda ke penyedia Git lain.

Perlindungan data

Model tanggung jawab AWS bersama berlaku untuk perlindungan data di AFT. Untuk tujuan perlindungan data, kami merekomendasikan praktik terbaik berikut untuk keamanan.

- Ikuti panduan Perlindungan Data yang disediakan oleh AWS Control Tower. Lihat perinciannya di Perlindungan Data di AWS Control Tower.
- Pertahankan konfigurasi status Terraform yang dihasilkan pada saat penyebaran AFT. Lihat perinciannya di Terapkan AWS Control Tower Account Factory untuk Terraform (AFT).
- Putar kredentif sensitif secara berkala seperti yang diarahkan oleh kebijakan keamanan organisasi Anda. Contoh rahasia adalah token Terraform, `git` token, dan sebagainya.

Enkripsi saat diam

AFT membuat bucket Amazon S3, topik Amazon SNS, antrian Amazon SQS, dan database Amazon DynamoDB yang dienkripsi saat diam dengan AWS kunci Layanan Manajemen Kunci. Kunci KMS yang dibuat oleh AFT mengaktifkan rotasi tahunan secara default. Jika Anda memilih distribusi HCP Terraform atau Terraform Enterprise dari Terraform, AFT menyertakan SecureString parameter Manajer AWS Sistem untuk menyimpan nilai token Terraform yang sensitif.

AFT menggunakan AWS layanan yang dijelaskan dalam Layanan komponen yang, secara default, dienkripsi saat diam. Untuk detailnya, lihat AWS dokumentasi untuk setiap AWS layanan komponen AFT, dan pelajari tentang praktik perlindungan data yang diikuti oleh setiap layanan.

Enkripsi dalam transit

AFT bergantung pada AWS layanan yang dijelaskan dalam Layanan komponen yang menggunakan enkripsi dalam transit, secara default. Untuk detailnya, lihat AWS dokumentasi untuk setiap AWS layanan komponen AFT, dan pelajari tentang praktik perlindungan data yang diikuti oleh setiap layanan.

Untuk distribusi HCP Terraform atau Terraform Enterprise, AFT memanggil API titik akhir HTTPS untuk akses ke organisasi Terraform Anda. Jika Anda memilih penyedia VCS pihak ketiga yang didukung oleh AWS CodeStar koneksi, AFT memanggil API titik akhir HTTPS untuk akses ke organisasi penyedia VCS Anda.

Hapus akun dari AFT

Topik ini menjelaskan cara menghapus akun dari AFT, sehingga pipeline AFT berhenti menerapkan dan memperbarui akun.

Important

Menghapus akun dari pipa AFT tidak dapat diubah dan dapat mengakibatkan hilangnya status.

Anda dapat menghapus akun dari AFT ketika Anda ingin menutup akun untuk aplikasi pensiun, mengisolasi akun yang disusupi, atau memindahkan akun dari satu organisasi ke organisasi lain.

Note

Menghapus akun dari AFT berbeda dengan menghapus akun AWS Control Tower atau Akun AWS. Saat Anda menghapus akun dari AFT, AWS Control Tower masih mengelola akun tersebut. Untuk menghapus akun AWS Control Tower atau Akun AWS, lihat berikut ini:

- Hapus kelola akun di Panduan Pengguna AWS Control Tower.
- Menutup akun di Panduan AWS Billing Pengguna.

Untuk menghapus akun dari pipa AFT

Prosedur berikut menjelaskan cara menghapus akun dari AFT.

1. Hapus akun dari **`git`** repositori yang menyimpan permintaan akun

   Di `git` repositori tempat Anda menyimpan permintaan akun, hapus permintaan akun untuk akun yang ingin Anda hapus dari AFT.

   Saat Anda menghapus permintaan akun dari repositori permintaan akun, AFT menghapus pipeline penyesuaian dan metadata akun. Untuk informasi lebih lanjut, lihat catatan rilis 1.8.0 untuk AFT di. GitHub
2. Hapus ruang kerja Terraform (Hanya untuk pelanggan HCP Terraform dan Terraform Enterprise)

   Hapus ruang kerja kustomisasi global dan kustomisasi akun untuk akun yang ingin Anda hapus dari AFT.

3. Hapus status Terraform dari backend Amazon S3

   Di akun manajemen AFT, hapus semua folder yang relevan di dalam bucket Amazon S3 untuk akun yang ingin Anda hapus dari AFT.

   > **Tip**
   >
   > Dalam contoh berikut, ganti *012345678901* dengan nomor ID akun manajemen AFT.

   Contoh: Terraform OSS

   Saat Anda memilih Terraform OSS, Anda menemukan 3 folder untuk setiap akun di bucket Amazon `aft-backend-`*012345678901*`-primary-region` S3 `aft-backend-`*012345678901*`-secondary-region` dan Amazon. Folder ini terkait dengan status kustomisasi akun, status pipeline penyesuaian, dan status penyesuaian global

   Contoh: HCP Terraform atau Terraform Enterprise

   Saat Anda memilih HCP Terraform atau Terraform Enterprise, Anda menemukan folder untuk setiap akun di bucket Amazon S3 dan Amazon`aft-backend-`*012345678901*`-primary-region`. `aft-backend-`*012345678901*`-secondary-region` Folder ini terkait dengan status pipeline kustomisasi.

Metrik operasional

Secara default, Account Factory for Terraform (AFT) mengirimkan metrik operasional anonim ke. AWS Kami menggunakan data ini untuk memahami bagaimana pelanggan menggunakan AFT sehingga kami dapat meningkatkan kualitas dan fitur solusi. Anda dapat memilih keluar dari pengumpulan data dengan mengubah parameter selama penerapan AFT. Saat pengumpulan diaktifkan, data berikut dikirim ke AWS:

- Solusi: Pengidentifikasi khusus AFT
- Versi: Versi AFT
- Universally Unique Identifier (UUID): Pengidentifikasi unik yang dibuat secara acak untuk setiap penerapan AFT
- Stempel waktu: Stempel waktu pengumpulan data

- Data: Konfigurasi AFT dan tindakan yang diambil oleh pelanggan

AWS memiliki data yang dikumpulkan. Pengumpulan data tunduk pada Kebijakan AWS Privasi.

> **Note**
>
> Versi AFT sebelum 1.6.0 tidak melaporkan metrik penggunaan ke. AWS

Untuk memilih keluar dari metrik pelaporan:

- Tetapkan nilai input `aft_metrics_reporting` ke `false` dalam file konfigurasi input Terraform Anda, seperti yang ditunjukkan pada contoh berikut, dan gunakan kembali AFT. Nilai ini diatur ke secara `true` default, jika Anda tidak mengaturnya secara eksplisit.

Jika Anda menyalin contoh, ingatlah untuk mengganti ID aktual dan nilai Region Anda dengan `x` item yang diberikan dalam string.

```
module "control_tower_account_factory" {
source = "aws-ia/control_tower_account_factory/aws"

# Required Vars
ct_management_account_id    = "xxxxxxxxxxx"
log_archive_account_id      = "xxxxxxxxxxx"
audit_account_id            = "xxxxxxxxxxx"
aft_management_account_id   = "xxxxxxxxxxx"
ct_home_region              = "xx-xxxx-x"
tf_backend_secondary_region = "xx-xxxx-x"

# Optional Vars
aft_metrics_reporting = false    # to opt out, set this value to false
}
```

Panduan pemecahan masalah Account Factory untuk Terraform (AFT)

Bagian ini dapat membantu Anda memecahkan masalah umum yang mungkin Anda temui saat menggunakan Account Factory for Terraform (AFT).

Topik

- Masalah umum
- Masalah yang berkaitan dengan akun provisioning/registration
- Masalah yang terkait dengan pemanggilan penyesuaian
- Masalah yang terkait dengan alur kerja penyesuaian akun

Masalah umum

- Kuota AWS sumber daya terlampaui

  Jika grup log menunjukkan bahwa Anda melebihi kuota AWS sumber daya, hubungi AWS Dukungan. Account Factory menggunakan Layanan AWS dengan kuota sumber daya yang mencakup AWS CodeBuild AWS Organizations,, dan AWS Systems Manager. Untuk informasi selengkapnya, lihat berikut ini:

  - Apa itu AWS CodeBuild? dalam Panduan CodeBuild Pengguna.
  - Apa itu AWS Organizations? dalam Panduan Pengguna Organisasi.
  - Apa itu AWS Systems Manager? dalam Panduan Pengguna Manajer Sistem.
- Versi Account Factory yang sudah ketinggalan zaman

  Jika Anda mengalami masalah dan yakin masalahnya adalah bug, pastikan Anda memiliki Account Factory versi terbaru. Untuk informasi selengkapnya, lihat Memperbarui versi Account Factory.
- Perubahan lokal dilakukan pada kode sumber Account Factory

  Account Factory adalah proyek open source. AWS Control Tower mendukung kode inti Account Factory. Jika Anda membuat perubahan lokal pada kode inti Account Factory, AWS Control Tower hanya mendukung penerapan Account Factory Anda berdasarkan upaya terbaik.
- Izin peran Pabrik Akun Tidak Mencukupi

  Account Factory membuat peran dan kebijakan IAM untuk mengelola penerapan dan penyesuaian akun yang dijual. Jika Anda mengubah peran atau kebijakan ini, pipeline Account Factory mungkin tidak dapat melakukan tindakan tertentu. Untuk informasi selengkapnya, lihat Per an yang diperlukan.
- Repositori akun tidak diisi dengan benar

  Pastikan Anda mengikuti langkah-langkah pasca-penerapan sebelum menyediakan akun.
- Tidak mendeteksi penyimpangan setelah mengubah OU secara manual

> **Note**
>
> AWS Control Tower mendeteksi penyimpangan secara otomatis. Untuk informasi tentang menyelesaikan penyimpangan, lihat Men deteksi dan menyelesaikan penyimpangan di AWS Control Tower.

Penyimpangan tidak terdeteksi saat unit organisasi (OU) diubah secara manual. Hal ini disebabkan oleh sifat Account Factory yang digerakkan oleh peristiwa. Saat permintaan akun dikirimkan, sumber daya yang dikelola Terraform adalah item Amazon DynamoDB, bukan akun langsung. Setelah item diubah, permintaan dimasukkan ke dalam antrian, di mana AWS Control Tower memprosesnya melalui Katalog Layanan (layanan yang mengelola detail akun). Jika Anda mengubah OU secara manual, penyimpangan tidak terdeteksi karena permintaan akun belum berubah.

Masalah yang berkaitan dengan akun provisioning/registration

- Permintaan akun (email address/name) sudah ada

  Masalah ini biasanya mengakibatkan kegagalan produk Katalog Layanan selama penyediaan atau sebagai`ConditionalCheckFailedException`.

  Anda dapat menemukan informasi lebih lanjut tentang masalah ini dengan melakukan salah satu hal berikut:

  - Tinjau grup log Terraform atau CloudWatch Logs Anda.
  - Tinjau kegagalan yang dipancarkan ke topik `aft-failure-notifications` Amazon SNS.
- Permintaan akun yang salah

  Pastikan permintaan akun Anda mengikuti skema yang diharapkan. Sebagai contoh, lihat terraform -aws-control_tower_account_factory on. GitHub
- Melebi AWS hi kuota sumber daya Organisasi

  Pastikan permintaan akun Anda tidak melebihi kuota AWS Organizations sumber daya. Untuk informasi selengkapnya, lihat Kuota untuk AWS Organisasi.

Masalah yang terkait dengan pemanggilan penyesuaian

- Akun target tidak terpasang ke Account Factory

  Pastikan semua akun yang disertakan dalam permintaan kustomisasi telah di-onboarding ke Account Factory. Untuk informasi selengkapnya, lihat Memperbarui akun yang sudah ada.

- Akun yang menargetkan permintaan kustomisasi ada di tabel DynamoDB**`aft-request-metadata`**, tetapi tidak di repositori permintaan akun

  Format permintaan pemanggilan kustomisasi Anda untuk mengecualikan akun yang melanggar dengan melakukan salah satu hal berikut:

  - Di tabel DynamoDB`aft-request-metadata`, hapus entri yang merujuk akun yang tidak lagi ada di repositori permintaan akun Anda.
  - Tidak menggunakan “semua” sebagai target.
  - Tidak menargetkan OU milik akun tersebut.
  - Tidak menargetkan akun secara langsung.

- Menggunakan token yang salah untuk HCP Terraform

  Pastikan Anda mengatur token yang benar. HCP Terraform hanya mendukung token berbasis tim, bukan token berbasis organisasi.

- Gagal membuat akun sebelum pipeline penyesuaian akun dibuat; tidak dapat menyesuaikan akun

  Buat perubahan pada spesifikasi akun di repositori permintaan akun. Saat Anda membuat perubahan, seperti mengubah nilai tag untuk akun, Account Factory mengikuti jalur yang mencoba membuat pipeline, meskipun pipeline tidak ada.

Masalah yang terkait dengan alur kerja penyesuaian akun

Jika Anda mengalami masalah terkait alur kerja penyesuaian akun, pastikan versi AFT Anda adalah 1.8.0 atau lebih tinggi, dan bahwa Anda menghapus semua instance metadata terkait akun dari tabel permintaan DynamoDB Anda.

Untuk informasi tentang AFT versi 1.8.0, lihat R ilis 1.8.0 pada. GitHub

Untuk informasi tentang cara memeriksa dan memperbarui versi AFT Anda, lihat berikut ini:

- Periksa versi AFT
- Perbarui versi AFT

Anda juga dapat melacak dan memecahkan masalah permintaan penyesuaian dengan menggunakan kueri Amazon CloudWatch Logs Insights untuk memfilter log yang berisi akun target dan ID permintaan kustomisasi. Untuk informasi selengkapnya, lihat Pemec ahan masalah dengan pelacakan permintaan kustomisasi akun AFT.

Mendeteksi dan mengatasi penyimpangan di AWS Control Tower

Mengidentifikasi dan menyelesaikan drift adalah tugas operasi reguler untuk administrator akun manajemen AWS Control Tower. Menyelesaikan drift membantu memastikan kepatuhan Anda terhadap persyaratan tata kelola.

Saat Anda membuat landing zone, landing zone dan semua unit organisasi (OU), akun, dan sumber daya sesuai dengan aturan tata kelola yang diberlakukan oleh kontrol yang Anda pilih. Saat Anda dan anggota organisasi Anda menggunakan landing zone, perubahan status kepatuhan ini dapat terjadi. Beberapa perubahan mungkin tidak disengaja, dan beberapa mungkin dibuat dengan sengaja untuk menanggapi peristiwa operasional yang sensitif terhadap waktu.

Deteksi drift membantu Anda dalam mengidentifikasi sumber daya yang memerlukan perubahan atau pembaruan konfigurasi untuk menyelesaikan penyimpangan.

Mendeteksi drift

AWS Control Tower mendeteksi drift secara otomatis. Untuk mendeteksi drift, `AWSControlTowerAdmin` peran tersebut memerlukan akses terus-menerus ke akun manajemen Anda sehingga AWS Control Tower dapat melakukan panggilan API hanya-baca. AWS Organizations Panggilan API ini muncul sebagai AWS CloudTrail peristiwa.

Drift untuk akun anggota muncul di notifikasi Amazon Simple Notification Service (Amazon SNS) yang digabungkan dalam akun audit. Pemberitahuan di setiap akun anggota mengirim peringatan ke topik Amazon SNS lokal, dan ke fungsi Lambda.

> **Note**
>
> Ketika kemampuan pendaftaran otomatis untuk akun diaktifkan di Pengaturan, pemberitahuan SNS ini tidak tersedia.

Untuk kontrol yang merupakan bagian dari AWS Security Hub CSPM Service-Managed Standar: AWS Control Tower, drift ditampilkan di halaman detail Akun dan Akun di konsol AWS Control Tower, serta melalui notifikasi Amazon SNS.

Administrator akun anggota dapat (dan sebagai praktik terbaik, mereka harus) berlangganan pemberitahuan drift SNS untuk akun tertentu. Misalnya, topik `aws-controltower-AggregateSecurityNotifications` SNS menyediakan notifikasi drift. Konsol AWS Control Tower menunjukkan kepada administrator akun manajemen kapan drift telah terjadi. Untuk informasi selengkapnya tentang topik SNS untuk deteksi dan notifikasi drift, lihat Pencegahan dan pemberitahuan drift.

De-duplikasi pemberitahuan drift

Jika jenis drift yang sama terjadi pada kumpulan sumber daya yang sama beberapa kali, AWS Control Tower mengirimkan notifikasi SNS hanya untuk instance awal drift. Jika AWS Control Tower mendeteksi bahwa instance drift ini telah diperbaiki, AWS akan mengirimkan pemberitahuan lain hanya jika drift terjadi kembali untuk sumber daya yang identik tersebut.

Contoh: SCP drift ditangani dengan cara berikut

- Jika Anda memodifikasi SCP terkelola yang sama beberapa kali, Anda menerima pemberitahuan untuk pertama kalinya Anda memodifikasinya.
- Jika Anda memodifikasi SCP terkelola, lalu memulihkan drift, lalu memodifikasinya lagi, Anda akan menerima dua notifikasi.

Jenis penyimpangan akun

- Akun dipindahkan antara OU (lihat Pergeseran warisan pada baseline yang diaktifkandanPergeseran warisan pada kontrol yang diaktifkan)
- Akun dihapus dari organisasi

> **Note**
>
> Ketika Anda memindahkan akun dari satu OU ke yang lain, kontrol dari OU sebelumnya tidak dihapus. Jika Anda mengaktifkan kontrol berbasis kait baru di OU tujuan, yang lama Kontrol berbasis kait dihapus dari akun, dan kontrol baru menggantikannya. Kontrol yang diterapkan dengan SCP dan AWS Config aturan selalu harus dihapus secara manual saat akun mengubah OU.

Contoh penyimpangan kebijakan

- SCP diperbarui
- SCP terlepas dari OU

Untuk informasi selengkapnya, lihat Tipe of Governance Drift.

Melihat drift

Anda dapat melihat status drift untuk akun dan OU Anda melalui konsol atau API, dan mengidentifikasi kapan konfigurasi akun dan OU dialihkan, atau tidak sinkron. Status drift juga dikomunikasikan dengan pesan SNS. Untuk informasi selengkapnya tentang menerima pesan SNS ini, lihat Panduan tentang berlangganan Topik SNS.

Untuk melihat status OU dan akun drift di konsol, buka halaman Organisasi, lalu pilih OU atau akun yang ingin Anda periksa.

Untuk melihat status drift untuk OU dan akun secara terprogram, panggil `ListEnabledBaselines`API untuk melihat status untuk garis dasar yang diaktifkan. Untuk melihat status akun individual secara terprogram dengan `ListEnabledBaselines` API, gunakan tanda. `includeChildren` Anda dapat memfilter berdasarkan status ini, dan hanya melihat akun dan OU yang membutuhkan perhatian Anda.

> **Note**
>
> AWS Control Tower menghasilkan peristiwa siklus hidup saat setiap operasi remediasi drift selesai.

Menyelesaikan drift

Meskipun deteksi otomatis, langkah-langkah untuk menyelesaikan drift harus dilakukan secara manual melalui konsol, atau dengan API. (Kecuali dalam kasus tertentu ketika pendaftaran otomatis diaktifkan untuk akun yang dipindahkan.)

Misalnya, Anda dapat menyelesaikan penyimpangan kebijakan untuk kontrol secara terprogram, dengan memanggil API. `ResetEnabledControl`

Untuk mengatasi penyimpangan dasar konfigurasi untuk OU, Anda dapat memilih Re-register OU di konsol. Jika penyimpangan disebabkan oleh satu akun, Anda dapat memilih Perbarui akun di konsol. Untuk mengatasi penyimpangan dasar dengan API, Anda dapat memanggil `ResetEnabledBaseline`API di OU.

Ringkasan

- Banyak jenis drift dapat diselesaikan melalui halaman pengaturan zona pendaratan. Anda dapat memilih tombol Reset di bagian Versi untuk mengatasi jenis penyimpangan ini.
- Jika OU Anda memiliki kurang dari 1000 akun, Anda dapat menyelesaikan penyimpangan di akun yang disediakan Account Factory, atau drift SCP, dengan memilih Re-registerOU di halaman Organisasi atau halaman detail OU.
- Anda mungkin dapat mengatasi penyimpangan akun, sepertiAkun anggota yang dipindahkan, dengan memperbarui akun individual. Untuk informasi selengkapnya, lihat Perbarui akun di konsol.
- Untuk kontrol, banyak jenis drift dapat diselesaikan dengan memanggil `ResetEnabledControl`API.
- Pergeseran dasar pada OU dan akun dapat diselesaikan dengan memanggil `ResetEnabledBaseline`API, atau dengan memilih akun Re-register OU atau Perbarui di konsol AWS Control Tower.
- Untuk mengatasi penyimpangan warisan yang terjadi saat akun dipindahkan antar OU, Anda dapat mengaktifkan fitur pendaftaran otomatis. Saat pendaftaran otomatis diaktifkan, AWS Control Tower secara otomatis memulihkan penyimpangan warisan dengan menerapkan sumber daya dasar dan konfigurasi kontrol dari OU tujuan ke akun yang dipindahkan. Anda dapat mengaktifkan pendaftaran otomatis di halaman Pengaturan landing zone di konsol, atau dengan memanggil **`UpdateLandingZone`**API dengan **`RemediationType`** parameter yang disetel ke Inheritance Drift. Untuk informasi selengkapnya, lihat Memindahkan dan mendaftarkan akun dengan pendaftaran otomatis.

⚠ Saat Anda mengambil tindakan untuk menyelesaikan drift pada versi landing zone, perilakunya bergantung pada versi Anda saat ini.

- Jika Anda menggunakan landing zone versi 3.1 atau lebih tinggi, Anda dapat memilih Perbarui untuk mengubah konfigurasi landing zone tanpa memutakhirkan versi, atau memilih Reset untuk menerapkan kembali konfigurasi yang disimpan ke sumber daya zona pendaratan drifted Anda. Drift diselesaikan sebagai bagian dari proses pembaruan.

- Jika Anda menggunakan versi landing zone lebih awal dari 3.1, Anda tidak dapat memilih Reset. Anda harus memilih Perbarui dan tingkatkan landing zone Anda ke setidaknya versi 3.1.

Pertimbangan tentang drift dan pemindaian kebijakan

AWS Control Tower memindai SCP, RCP, dan kebijakan Deklaratif terkelola Anda setiap hari untuk memverifikasi bahwa kontrol yang sesuai diterapkan dengan benar dan belum hanyut. Untuk mengambil sumber daya ini dan menjalankan pemeriksaannya, AWS Control Tower memanggil AWS Organizations atas nama Anda, menggunakan peran di akun manajemen Anda.

Jika pemindaian AWS Control Tower menemukan drift, Anda akan menerima pemberitahuan. AWS Control Tower hanya mengirimkan satu notifikasi per masalah drift, jadi jika landing zone Anda sudah dalam keadaan drift, Anda tidak akan menerima notifikasi tambahan kecuali item drift baru ditemukan.

AWS Organizations membatasi seberapa sering masing-masing API-nya dapat dipanggil. Batas ini dinyatakan dalam transaksi per detik (TPS), dan dikenal sebagai batas TPS, laju pembatasan, atau tingkat permintaan API. Saat AWS Control Tower mengaudit SCP, RCP, dan kebijakan Deklaratif Anda dengan menelepon AWS Organizations, panggilan API yang dibuat AWS Control Tower dihitung terhadap batas TPS Anda, karena AWS Control Tower menggunakan akun manajemen untuk melakukan panggilan.

Dalam situasi yang jarang terjadi, batas ini dapat dicapai ketika Anda memanggil API yang sama berulang kali, baik melalui solusi pihak ketiga atau skrip khusus yang Anda tulis. Misalnya, jika Anda dan AWS Control Tower memanggil AWS Organizations API yang sama pada saat yang sama (dalam 1 detik), dan batas TPS tercapai, panggilan berikutnya akan dibatasi. Artinya, panggilan ini mengembalikan kesalahan seperti`Rate exceeded`.

Jika tingkat permintaan API terlampaui

- Jika AWS Control Tower mencapai batas dan dibatasi, kami menjeda eksekusi audit dan melanjutkannya di lain waktu.
- Jika beban kerja Anda mencapai batas dan dibatasi, hasilnya dapat berkisar dari sedikit latensi hingga kesalahan fatal dalam beban kerja, tergantung pada bagaimana beban kerja dikonfigurasi. Kasus tepi ini adalah sesuatu yang harus diperhatikan.

Pemindaian SCP harian terdiri dari

1. Mengambil OU Anda yang baru saja aktif.
2. Untuk setiap OU yang terdaftar, ambil semua SCP yang dikelola oleh AWS Control Tower yang dilampirkan ke OU. SCP terkelola memiliki pengidentifikasi yang dimulai dengan. `aws-guardrails`
3. Untuk setiap kontrol preventif yang diaktifkan pada OU, memverifikasi bahwa pernyataan kebijakan kontrol hadir dalam SCP yang dikelola OU.

OU mungkin memiliki satu atau lebih SCP terkelola.

Jenis drift untuk segera diselesaikan

Sebagian besar jenis drift dapat diselesaikan oleh administrator. Beberapa jenis drift harus segera diselesaikan, termasuk penghapusan unit organisasi yang diperlukan oleh zona landing zone AWS Control Tower. Berikut adalah beberapa contoh penyimpangan utama yang mungkin ingin Anda hindari:

- Jangan hapus OU Keamanan: Unit organisasi yang awalnya bernama Security selama penyiapan landing zone oleh AWS Control Tower tidak boleh dihapus. Jika Anda menghapusnya, Anda akan melihat pesan kesalahan yang menginstruksikan Anda untuk segera mengatur ulang landing zone. Anda tidak akan dapat mengambil tindakan lain di AWS Control Tower hingga reset selesai.
- Jangan hapus peran yang diperlukan: AWS Control Tower memeriksa peran AWS Identity and Access Management (IAM) tertentu saat Anda masuk ke konsol untuk penyimpangan peran IAM. Jika peran ini hilang atau tidak dapat diakses, Anda akan melihat halaman kesalahan yang menginstruksikan Anda untuk mengatur ulang landing zone Anda. Peran ini adalah `AWSControlTowerAdmin` `AWSControlTowerCloudTrailRoleAWSControlTowerStackSetRole`.

  Untuk informasi lebih lanjut tentang peran ini, lihatIzin Diperlukan untuk menggunakan konsol AWS Control Tower.
- Jangan hapus semua OU Tambahan: Setidaknya satu OU Tambahan diperlukan agar AWS Control Tower dapat beroperasi, tetapi tidak harus berupa Sandbox OU.
- Jangan hapus akun bersama: Jika Anda menghapus akun bersama dari Foundational OU dengan AWS Organizations konsol atau API, seperti menghapus akun logging dari OU Keamanan.

Memindahkan akun ini menciptakan jenis drift Move Account yang harus diperbaiki. Untuk memulihkan jenis drift ini, Anda harus memperbarui landing zone.

> **Note**
>
> Sebagai praktik terbaik, jangan pindahkan akun bersama ini dari Foundational OU.

Perubahan sumber daya yang dapat diperbaiki

Berikut adalah daftar perubahan pada sumber daya AWS Control Tower yang diizinkan, meskipun mereka menciptakan penyimpangan yang dapat diselesaikan. Hasil operasi yang diizinkan ini dapat dilihat di konsol AWS Control Tower, meskipun penyegaran mungkin diperlukan.

Untuk informasi selengkapnya tentang cara mengatasi penyimpangan yang dihasilkan, lihat Mengelola Sumber Daya Di Luar AWS Control Tower.

Perubahan diizinkan di luar konsol AWS Control Tower

- Ubah nama OU yang terdaftar.
- Ubah nama Security OU.
- Ubah nama akun anggota di OU non-dasar.
- Hapus OU Non-Foundational.
- Hapus akun terdaftar dari OU non-dasar.
- Ubah alamat email akun bersama di Security OU.
- Ubah alamat email akun anggota di OU terdaftar.

> **Note**
>
> Memindahkan akun antara OU dianggap drift, dan itu harus diselesaikan.

Drift dan penyediaan akun baru

Jika landing zone Anda dalam keadaan drift, fitur akun Daftar di AWS Control Tower tidak akan berfungsi. Dalam hal ini, Anda harus menyediakan akun baru melalui AWS Service Catalog. Untuk petunjuk, lihat Menyediakan akun di konsol Service Catalog, dengan Account Factory.

Khususnya, jika Anda telah membuat perubahan tertentu pada akun Anda melalui Service Catalog, seperti mengubah nama portofolio Anda, fitur akun Daftar tidak akan berfungsi.

Jenis penyimpangan tata kelola

Pergeseran tata kelola, juga disebut penyimpangan organisasi terjadi ketika OU, SCP, dan akun anggota diubah atau diperbarui. Jenis drift tata kelola yang dapat dideteksi di AWS Control Tower adalah sebagai berikut:

- Pergeseran akun dan tata kelola OU
- Zona pendaratan melayang
- Kontrol drift untuk kontrol non-SCP
- Penyimpangan warisan untuk garis dasar dan kontrol

Bagian selanjutnya memberikan detail tentang jenis drift yang dilaporkan AWS Control Tower, dan cara mengatasinya.

> **Note**
>
> AWS Control Tower akan berhenti mengirim notifikasi drift ke topik SNS untuk pelanggan LZ4.0 + dan akan mulai mengirim notifikasi drift ke EventBridge akun manajemen. Untuk melihat contoh peristiwa dan panduan tentang cara menerima pemberitahuan drift melalui, EventBridge silakan lihat bagian di bawah ini tentang EventBridge pembuatan.

Pergeseran akun dan tata kelola OU

- Akun anggota yang dipindahkan
- Akun anggota yang dihapus
- Pembaruan yang tidak direncanakan ke SCP terkelola
- SCP terlepas dari OU terkelola

Zona pendaratan melayang

Jenis drift lainnya adalah landing zone drift, yang dapat ditemukan melalui akun manajemen. Pergeseran zona pendaratan terdiri dari penyimpangan peran IAM, atau jenis penyimpangan organisasi apa pun yang secara khusus memengaruhi OU Foundational dan akun bersama.

- Dihapus Foundational OU
- Akses tepercaya dinonaktifkan

Kasus khusus drift landing zone adalah role drift, yang terdeteksi ketika peran yang diperlukan tidak tersedia. Jika jenis penyimpangan ini terjadi, konsol menampilkan halaman peringatan dan beberapa instruksi tentang cara mengembalikan peran. Landing zone Anda tidak tersedia sampai drift peran diselesaikan. Untuk informasi selengkapnya tentang pergeseran peran, lihat Jangan menghapus peran yang diperlukan di bagian yang dipanggilJenis drift untuk segera diselesaikan.

Kontrol drift untuk kontrol non-SCP

AWS Control Tower melaporkan penyimpangan kontrol terkait kontrol yang diterapkan dengan kebijakan kontrol sumber daya (RCP), kebijakan deklaratif, dan kontrol yang merupakan bagian dari AWS Security Hub CSPM Service-managed Standar: AWS Control Tower.

- Security Hub CSPM kontrol drift
- Pengendalian kebijakan drift

Penyimpangan warisan untuk garis dasar dan kontrol

- Drift baseline yang diaktifkan

  Ketika konfigurasi dasar pada akun anggota berbeda dari yang diterapkan pada OU induk, AWS Control Tower melaporkan penyimpangan warisan untuk garis dasar yang diaktifkan (konfigurasi sumber daya) pada OU dan akun tersebut. Untuk informasi selengkapnya tentang garis dasar, lihat Jenis garis dasar.

  - Pergeseran warisan pada baseline yang diaktifkan
- Drift kontrol yang diaktifkan

  Jika konfigurasi kontrol yang diaktifkan pada akun anggota berbeda dari yang diterapkan pada OU induk, AWS Control Tower melaporkan penyimpangan warisan untuk kontrol yang diaktifkan pada OU dan akun tersebut.

- Pergeseran warisan pada kontrol yang diaktifkan

> **Drift yang tidak dilaporkan**
>
> - AWS Control Tower tidak mencari penyimpangan terkait layanan lain yang bekerja dengan akun manajemen, termasuk, Amazon AWS CloudTrail CloudWatch, IAM Identity Center, CloudFormation AWS Config, dan sebagainya.
> - AWS Control Tower tidak mendeteksi penyimpangan sumber daya atau jenis drift lain yang mungkin terjadi jika Anda memodifikasi sumber daya yang terdapat dalam baseline.

Akun anggota yang dipindahkan

> **Note**
>
> Untuk pelanggan di LZ 4.0+, AWS Control Tower tidak akan mengirimkan notifikasi drift akun pemindahan untuk akun Account Factory tanpanya. AWSControlTowerBaseline

Jenis penyimpangan ini terjadi pada akun daripada OU. Jenis drift ini dapat terjadi ketika akun anggota AWS Control Tower, akun audit, atau akun arsip log dipindahkan dari AWS Control Tower OU terdaftar ke OU lainnya. Dalam banyak kasus, Anda dapat menghindari jenis penyimpangan ini jika Anda mengaktifkan fitur pendaftaran otomatis untuk akun, di halaman Pengaturan. Untuk detail selengkapnya, lihat Memindahkan dan mendaftarkan akun dengan pendaftaran otomatis.

Berikut ini adalah contoh notifikasi drift saat jenis drift ini terdeteksi.

```
{
  "Message" : "AWS Control Tower has detected that your member account 'account-
email@amazon.com (012345678909)' has been moved from organizational unit 'Sandbox
 (ou-0123-eEXAMPLE)' to 'Security (ou-3210-1EXAMPLE)'. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
move-account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ACCOUNT_MOVED_BETWEEN_OUS",
```

```
  "RemediationStep" : "Re-register this organizational unit (OU), or if the OU has more
 than 1000 accounts, you must update the provisioned product in Account Factory.",
  "AccountId" : "012345678909",
  "SourceId" : "012345678909",
  "DestinationId" : "ou-3210-1EXAMPLE"
}
```

Resolusi

Ketika jenis drift ini terjadi untuk akun yang disediakan Account Factory di OU dengan hingga 1000 akun, Anda dapat menyelesaikannya dengan:

- Menavigasi ke halaman Organisasi di konsol AWS Control Tower, memilih akun, dan memilih Perbarui akun di kanan atas (opsi tercepat untuk akun individual).
- Menavigasi ke halaman Organisasi di konsol AWS Control Tower, lalu memilih Re-registerOU yang berisi akun (opsi tercepat untuk beberapa akun). Untuk informasi selengkapnya, lihat Mendaftarkan unit organisasi yang ada dengan AWS Control Tower.
- Memperbarui produk yang disediakan di Account Factory. Untuk informasi selengkapnya, lihat Memperbarui dan memindahkan akun dengan AWS Control Tower.

> **Note**
>
> Jika Anda memiliki beberapa akun individual untuk diperbarui, lihat juga metode ini untuk membuat pembaruan dengan skrip:Menyediakan dan memperbarui akun menggunakan otomatisasi.

- Ketika jenis penyimpangan ini terjadi di OU dengan lebih dari 1000 akun, resolusi drift mungkin tergantung pada jenis akun mana yang telah dipindahkan, seperti yang dijelaskan dalam paragraf berikutnya. Untuk informasi selengkapnya, lihat Perbarui landing zone Anda.
  - Jika akun yang disediakan Account Factory dipindahkan - Di OU dengan kurang dari 1000 akun, Anda dapat menyelesaikan penyimpangan akun dengan memperbarui produk yang disediakan di Account Factory, dengan mendaftarkan ulang OU, atau dengan memperbarui landing zone Anda.

    Dalam OU dengan lebih dari 1000 akun, Anda harus menyelesaikan penyimpangan dengan membuat pembaruan ke setiap akun yang dipindahkan, baik melalui konsol AWS Control Tower

atau produk yang disediakan, karena Re-register OU tidak akan melakukan pembaruan. Untuk informasi selengkapnya, lihat Memperbarui dan memindahkan akun dengan AWS Control Tower.

- Jika akun bersama dipindahkan — Anda dapat mengatasi penyimpangan dari memindahkan akun audit atau arsip log dengan memperbarui landing zone Anda. Untuk informasi selengkapnya, lihat Perbarui landing zone Anda.

> ⚠ Nama bidang yang tidak digunakan lagi
>
> Nama bidang `MasterAccountID` telah diubah `ManagementAccountID` untuk mematuhi AWS pedoman. Nama lama sudah usang. Sejak 2022, skrip yang berisi nama bidang usang tidak lagi berfungsi.

Akun anggota yang dihapus

Jenis drift ini dapat terjadi ketika akun anggota dihapus dari unit organisasi AWS Control Tower yang terdaftar. Contoh berikut menunjukkan pemberitahuan drift ketika jenis drift terdeteksi.

```
{
  "Message" : "AWS Control Tower has detected that the member account 012345678909 has
 been removed from organization o-123EXAMPLE. For more information, including steps
 to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/remove-
account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ACCOUNT_REMOVED_FROM_ORGANIZATION",
  "RemediationStep" : "Add account to Organization and update Account Factory
 provisioned product",
  "AccountId" : "012345678909"
}
```

Resolusi

- Ketika jenis drift ini terjadi di akun anggota, Anda dapat menyelesaikan drift dengan memperbarui akun di konsol AWS Control Tower, atau di Account Factory. Misalnya, Anda dapat menambahkan akun ke OU terdaftar lain dari panduan pembaruan Account Factory. Untuk informasi selengkapnya, lihat Memperbarui dan memindahkan akun dengan AWS Control Tower.

- Jika akun bersama dihapus dari Foundational OU, Anda harus menyelesaikan drift dengan mengatur ulang landing zone Anda. Sampai penyimpangan ini teratasi, Anda tidak akan dapat menggunakan konsol AWS Control Tower.
- Untuk informasi selengkapnya tentang menyelesaikan penyimpangan untuk akun dan OU, lihat. Jika Anda mengelola sumber daya di luar AWS Control Tower

> **Note**
>
> Di Service Catalog, produk yang disediakan Account Factory yang mewakili akun tidak diperbarui untuk menghapus akun. Sebagai gantinya, produk yang disediakan ditampilkan sebagai `TAINTED` dan dalam status kesalahan. Untuk membersihkan, buka Service Catalog, pilih produk yang disediakan, lalu pilih Terminate.

Pembaruan yang tidak direncanakan ke SCP terkelola

Jenis drift ini dapat terjadi ketika SCP untuk kontrol diperbarui di AWS Organizations konsol atau secara terprogram menggunakan AWS CLI atau salah satu AWS SDK. Berikut ini adalah contoh notifikasi drift saat jenis drift ini terdeteksi.

```
{
  "Message" : "AWS Control Tower has detected that the managed service control policy
 'aws-guardrails-012345 (p-tEXAMPLE)', attached to the registered organizational unit
 'Security (ou-0123-1EXAMPLE)', has been modified. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
update-scp'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_UPDATED",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
  "PolicyId" : "p-tEXAMPLE"
}
```

Resolusi

Ketika jenis penyimpangan ini terjadi di OU dengan hingga 1000 akun, Anda dapat menyelesaikannya dengan:

- Menavigasi ke halaman Organisasi di konsol AWS Control Tower untuk mendaftarkan ulang OU (opsi tercepat). Untuk informasi selengkapnya, lihat Mendaftarkan unit organisasi yang ada dengan AWS Control Tower.
- Memperbarui landing zone Anda (opsi lebih lambat). Untuk informasi selengkapnya, lihat Perbarui landing zone Anda.

Ketika jenis drift ini terjadi di OU dengan lebih dari 1000 akun, selesaikan dengan memperbarui landing zone Anda. Untuk informasi selengkapnya, lihat Perbarui landing zone Anda.

SCP terlepas dari OU terkelola

Jenis drift ini dapat terjadi ketika SCP untuk kontrol telah terlepas dari OU yang dikelola oleh AWS Control Tower. Kejadian ini sangat umum terjadi saat Anda bekerja dari luar konsol AWS Control Tower. Berikut ini adalah contoh notifikasi drift saat jenis drift ini terdeteksi.

```
{
  "Message" : "AWS Control Tower has detected that the managed service control
 policy 'aws-guardrails-012345 (p-tEXAMPLE)' has been detached from the registered
 organizational unit 'Sandbox (ou-0123-1EXAMPLE)'. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
scp-detached'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_DETACHED_FROM_OU",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
  "PolicyId" : "p-tEXAMPLE"
}
```

Resolusi

Ketika jenis penyimpangan ini terjadi di OU dengan hingga 1000 akun, Anda dapat menyelesaikannya dengan:

- Menavigasi ke OU di konsol AWS Control Tower untuk mendaftarkan ulang OU (opsi tercepat). Untuk informasi selengkapnya, lihat Mendaftarkan unit organisasi yang ada dengan AWS Control Tower.

- Memperbarui landing zone Anda (opsi lebih lambat). Jika drift memengaruhi kontrol wajib, proses pembaruan membuat kebijakan kontrol layanan baru (SCP) dan menempelkannya ke OU untuk menyelesaikan penyimpangan. Untuk informasi selengkapnya tentang cara memperbarui landing zone Anda, lihatPerbarui landing zone Anda.

Ketika jenis drift ini terjadi di OU dengan lebih dari 1000 akun, selesaikan dengan memperbarui landing zone Anda. Jika drift memengaruhi kontrol wajib, proses pembaruan membuat kebijakan kontrol layanan baru (SCP) dan menempelkannya ke OU untuk menyelesaikan penyimpangan. Untuk informasi selengkapnya tentang cara memperbarui landing zone Anda, lihatPerbarui landing zone Anda.

Dihapus Foundational OU

Jenis drift ini hanya berlaku untuk AWS Control Tower Foundational OU, seperti Security OU. Hal ini dapat terjadi jika Foundational OU dihapus di luar konsol AWS Control Tower. Foundational OU tidak dapat dipindahkan tanpa membuat jenis drift ini, karena memindahkan OU sama dengan menghapusnya dan kemudian menambahkannya di tempat lain. Saat Anda menyelesaikan drift dengan memperbarui landing zone, AWS Control Tower menggantikan Foundational OU di lokasi aslinya. Contoh berikut menunjukkan pemberitahuan drift yang mungkin Anda terima saat jenis drift ini terdeteksi.

```
{
  "Message" : "AWS Control Tower has detected that the registered organizational unit
 'Security (ou-0123-1EXAMPLE)' has been deleted. For more information, including steps
 to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/delete-
ou'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "ORGANIZATIONAL_UNIT_DELETED",
  "RemediationStep" : "Delete organizational unit in Control Tower",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE"
}
```

Resolusi

Karena penyimpangan ini terjadi hanya untuk Foundational OU, resolusinya adalah memperbarui landing zone. Ketika jenis OU lainnya dihapus, AWS Control Tower diperbarui secara otomatis.

Untuk informasi selengkapnya tentang menyelesaikan penyimpangan untuk akun dan OU, lihat. Jika Anda mengelola sumber daya di luar AWS Control Tower

Security Hub CSPM kontrol drift

Jenis drift ini terjadi ketika kontrol yang merupakan bagian dari AWS Security Hub CSPM Service-Managed Standar: AWS Control Tower melaporkan keadaan drift. AWS Security Hub CSPM Layanan itu sendiri tidak melaporkan keadaan drift untuk kontrol ini. Sebagai gantinya, layanan mengirimkan temuannya ke AWS Control Tower.

Drift kontrol CSPM Security Hub juga dapat dideteksi jika AWS Control Tower belum menerima pembaruan status dari Security Hub CSPM lebih dari 24 jam. Jika temuan tersebut tidak diterima seperti yang diharapkan, AWS Control Tower memverifikasi bahwa kontrol dalam drift. Contoh berikut menunjukkan pemberitahuan drift yang mungkin Anda terima saat jenis drift ini terdeteksi.

```
{
"Message" : "AWS Control Tower has detected that an AWS Security Hub control
 was removed in your account example-account@amazon.com <mailto:example-
account@amazon.com>. The artifact deployed on the target OU and accounts does not match
 the expected template and configuration for the control. This mismatch indicates that
 configuration changes were made outside of AWS Control Tower. For more information,
 view Security Hub standard",
"MasterAccountId" : "123456789XXX",
"ManagementAccountId" : "123456789XXX",
"OrganizationId" : "o-123EXAMPLE",
"DriftType" : "SECURITY_HUB_CONTROL_DISABLED",
"RemediationStep" : "To remediate the issue, Re-register the OU, or remove the control
 and enable it again. If the problem persists, contact AWS support.",
"AccountId" : "7876543219XXX",
"ControlId" : "SH.XXXXXXX.1",
"ControlName" : "EBS snapshots should not be publicly restorable",
"ApiControlIdentifier" : "arn:aws:controltower:us-east-1::control/PYBETSAGNUZB",
"EnabledControlIdentifier": "arn:aws:controltower:us-
east-1::enabledcontrol/<UNIQUE_ID>".
"Region" : "us-east-1"
}
```

Resolusi

Untuk OU dengan kurang dari 1000 akun, resolusi yang disarankan adalah memanggil ResetEnabledControlAPI untuk kontrol drifted. Di konsol, Anda dapat memilih Re-registeruntuk OU,

yang mengatur ulang kontrol ke keadaan semula. Atau, untuk setiap OU, Anda dapat menghapus dan mengaktifkan kembali kontrol melalui konsol atau AWS Control Tower API, yang juga mengatur ulang kontrol.

Untuk informasi selengkapnya tentang menyelesaikan penyimpangan untuk akun dan OU, lihat. Jika Anda mengelola sumber daya di luar AWS Control Tower

Pengendalian kebijakan drift

Jenis drift ini terjadi ketika kontrol yang diterapkan dengan kebijakan kontrol sumber daya (RCP) atau kebijakan deklaratif melaporkan keadaan drift. Ini mengembalikan status`CONTROL_INEFFECTIVE`, yang dapat Anda lihat di konsol AWS Control Tower dan dalam pesan drift. Pesan drift untuk jenis drift ini juga mencakup `EnabledControlIdentifier` untuk kontrol yang terpengaruh.

Jenis drift ini tidak dilaporkan untuk SCP-based kontrol.

Contoh berikut menunjukkan pemberitahuan drift yang mungkin Anda terima saat jenis drift ini terdeteksi.

```
{
    "Message": "AWS Control Tower detects that a policy it owns was updated
 unexpectedly. This mismatch indicates that configuration changes were made outside of
 AWS Control Tower.",
    "MasterAccountId": "123456789XXX",
    "ManagementAccountId": "123456789XXX",
    "OrganizationId": "o-123EXAMPLE",
    "DriftType": "CONTROL_INEFFECTIVE",
    "RemediationStep": "To remediate the issue, Reset the DRIFTED enabled control if
 permitted or Re-register the OU. If the problem persists, contact AWS support.",
    "TargetIdentifier": "arn:aws:::organizations/o-123456/ou-1234-4567",
    "ControlId": "CT.XXXXXXX.PV.1",
    "ControlName": "EBS snapshots should not be publicly restorable",
    "ApiControlIdentifier": "arn:aws:controlcatalog:::control/<UNIQUE_ID>",
    "EnabledControlIdentifier": "arn:aws:controltower:us-
east-1::enabledcontrol/<UNIQUE_ID>"
}
```

Resolusi

Resolusi termudah untuk penyimpangan kebijakan kontrol pada kontrol RCP, kontrol kebijakan deklaratif, dan kontrol CSPM Security Hub yang diaktifkan di AWS Control Tower adalah dengan memanggil API. `ResetEnabledControl`

Untuk OU dengan kurang dari 1000 akun, resolusi lain dari konsol atau API adalah Re-registerke OU, yang mengatur ulang kontrol ke status semula.

Untuk setiap individu OU, Anda dapat menghapus dan mengaktifkan kembali kontrol melalui konsol atau AWS Control Tower API, yang juga mengatur ulang kontrol.

Untuk informasi selengkapnya tentang menyelesaikan penyimpangan untuk akun dan OU, lihat. Jika Anda mengelola sumber daya di luar AWS Control Tower

Akses tepercaya dinonaktifkan

Jenis drift ini berlaku untuk zona pendaratan AWS Control Tower. Ini terjadi ketika Anda menonaktifkan akses tepercaya ke AWS Control Tower AWS Organizations setelah Anda menyiapkan zona landing zone AWS Control Tower.

Ketika akses tepercaya dinonaktifkan, AWS Control Tower tidak lagi menerima peristiwa perubahan dari AWS Organizations. AWS Control Tower mengandalkan peristiwa perubahan ini agar tetap disinkronkan. AWS Organizations Akibatnya, AWS Control Tower mungkin melewatkan perubahan organisasi dalam akun dan OU. Itulah mengapa penting untuk mendaftarkan ulang setiap OU, setiap kali Anda memperbarui landing zone Anda.

Contoh: pemberitahuan drift

Berikut ini adalah contoh notifikasi drift yang Anda terima saat jenis drift ini terjadi.

```
{
  "Message" : "AWS Control Tower has detected that trusted access has been disabled in
 AWS Organizations. For more information, including steps to resolve this issue, see
 https://docs.aws.amazon.com/controltower/latest/userguide/drift.html#drift-trusted-
access-disabled",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "TRUSTED_ACCESS_DISABLED",
  "RemediationStep" : "Reset Control Tower landing zone."
}
```

Resolusi

AWS Control Tower memberi tahu Anda saat jenis drift ini terjadi di konsol AWS Control Tower. Resolusinya adalah mengatur ulang landing zone AWS Control Tower Anda. Untuk informasi selengkapnya, lihat Menyelesaikan penyimpangan.

Pergeseran warisan pada baseline yang diaktifkan

Jenis drift ini dapat terjadi pada AWS Control Tower OU dan akun.

Resolusi

AWS Control Tower memberi tahu Anda saat jenis drift ini terjadi. Untuk hampir semua kasus penyimpangan warisan, Anda akan menerima pemberitahuan drift untuk drift akun anggota yang dipindahkan. Itu karena jenis drift ini biasanya terjadi ketika akun telah dipindahkan, atau akun gagal pendaftaran.

Lihat dan selesaikan penyimpangan di konsol

Di konsol AWS Control Tower, Anda dapat melihat status drift yang diwariskan ini di kolom status Baseline di halaman Organizations. Resolusi dari konsol adalah untuk OU Re-registerAnda atau Perbarui akun Anda.

Lihat dan selesaikan drift secara terprogram

Untuk melihat status drift secara terprogram, Anda dapat memanggil `ListEnabledBaselines`API untuk melihat status garis dasar yang diaktifkan di OU Anda. Untuk melihat status akun individual secara terprogram dengan `ListEnabledBaselines` API, gunakan tanda. `includeChildren`

Anda dapat menyelesaikan jenis drift ini secara terprogram, dengan memanggil API. `ResetEnabledBaseline`

Mencegah penyimpangan warisan dengan pendaftaran otomatis

Untuk mencegah penyimpangan ini pada perpindahan akun future, aktifkan pendaftaran otomatis. Saat pendaftaran otomatis aktif, AWS Control Tower menerapkan garis dasar OU tujuan dan konfigurasi kontrol ke akun yang dipindahkan saat Anda memperbarui akun untuk memindahkannya ke OU yang berbeda. Untuk informasi lebih lanjut, lihatMemindahkan dan mendaftarkan akun dengan pendaftaran otomatis. Auto-enrollment tidak menyelesaikan penyimpangan dasar yang sudah ada dari langkah sebelumnya. Untuk mengatasi penyimpangan yang ada, gunakan salah satu metode resolusi yang dijelaskan sebelumnya di bagian ini. Anda dapat mendaftarkan ulang OU, memperbarui akun, atau memanggil `ResetEnabledBaseline` API.

Pergeseran warisan pada kontrol yang diaktifkan

Jenis drift ini dapat terjadi pada AWS Control Tower OU dan akun.

Resolusi

AWS Control Tower memberi tahu Anda saat jenis drift ini terjadi. Untuk hampir semua kasus penyimpangan warisan, Anda menerima pemberitahuan drift untuk drift akun anggota yang dipindahkan. Jenis penyimpangan ini biasanya terjadi ketika Anda memindahkan akun di antara OU saat pendaftaran otomatis dimatikan. Dalam hal ini, AWS Control Tower menerapkan kontrol OU tujuan ke akun, tetapi tidak secara otomatis menghapus kontrol akun yang diwarisi dari OU sebelumnya. Akibatnya, kontrol Detektif dan kontrol Proaktif dari OU sebelumnya dapat tetap berada di akun dalam keadaan hanyut. Kontrol preventif tidak tunduk pada jenis penyimpangan warisan ini.

> **Note**
>
> Anda tidak dapat memulihkan penyimpangan warisan ini dengan memperbarui akun, dengan mendaftarkan ulang OU, atau dengan memanggil API. `ResetEnabledControl` Tindakan tersebut hanya menyelesaikan penyimpangan konfigurasi. Mereka tidak menghapus kontrol yang masih diwarisi akun yang dipindahkan dari OU sebelumnya. Untuk menghapus kontrol sisa, Anda harus menonaktifkannya dengan `DisableControl` API, seperti yang dijelaskan di bagian ini.

Lihat drift di konsol

Di konsol AWS Control Tower, Anda dapat melihat kontrol yang diaktifkan yang memiliki status Drifted. Informasi ini hanya muncul di halaman Detail akun untuk akun yang terpengaruh. Konsol tidak menampilkan `EnabledControlIdentifier` (ARN dari kontrol yang diaktifkan) yang Anda perlukan untuk menonaktifkan kontrol hanyut. Untuk mendapatkan`EnabledControlIdentifier`, gunakan AWS Control Tower API, seperti yang dijelaskan di bagian ini.

Lihat dan selesaikan drift dengan menggunakan AWS CLI

Untuk menemukan kontrol drifted pada akun yang terpengaruh, daftarkan kontrol yang diaktifkan untuk akun tersebut. Tetapkan pengenal target ke akun, dan sertakan `--include-children` tanda sehingga kontrol yang diwariskan dikembalikan:

```
aws controltower list-enabled-controls --target-identifier <account ARN> --include-children
```

Dalam output, temukan kontrol yang diaktifkan yang tipe `inheritance` driftnya menunjukkan `DRIFTED` status. Perhatikan `arn` nilai kontrol yang diaktifkan. Nilai ini adalah `EnabledControlIdentifier` yang Anda gunakan untuk menonaktifkan kontrol. Contoh:

```
{
    "arn": "arn:aws:controltower:<Region>:<management account
 ID>:enabledcontrol/<enabled control ID>",
    "controlIdentifier": "arn:aws:controlcatalog:::control/<control ID>",
    "targetIdentifier": "arn:aws:organizations::<management account
 ID>:account/<organization ID>/<member account ID>",
    "driftStatusSummary": {
        "driftStatus": "DRIFTED",
        "types": {
            "inheritance": { "status": "DRIFTED" },
            "resource": { "status": "IN_SYNC" }
        }
    }
}
```

Untuk menghapus kontrol hanyut, nonaktifkan dengan meneruskan `EnabledControlIdentifier` ke perintah: `disable-control`

```
aws controltower disable-control --enabled-control-
identifier <EnabledControlIdentifier>
```

Untuk informasi selengkapnya, lihat ListEnabledControlsdan DisableControldi Referensi AWS Control Tower API.

Mencegah penyimpangan warisan dengan pendaftaran otomatis

Untuk mencegah penyimpangan ini pada perpindahan akun future, aktifkan pendaftaran otomatis. Untuk informasi selengkapnya, lihat Memindahkan dan mendaftarkan akun dengan pendaftaran otomatis. Saat pendaftaran otomatis aktif, AWS Control Tower menerapkan dasar OU tujuan dan konfigurasi kontrol ke akun yang dipindahkan dan menghapus kontrol OU sebelumnya. Namun, pendaftaran otomatis tidak menghapus kontrol yang sudah tersisa dari langkah yang terjadi sebelum Anda menyalakannya. Untuk menghapus kontrol tersebut, gunakan `DisableControl` API.

EventBridge penciptaan

> **Note**
>
> EventBridge diaktifkan hanya untuk pelanggan LZ4.0 +.

Contoh EventBridge format untuk AWS Control Tower

```
{
   "version": "0",
   "id": "cd4d811e-ab12-322b-8255-872ce65b1bc8",
   "detail-type": "Drift Detected",
   "source": "aws.controltower",
   "account": "111122223333",
   "time": "2018-03-22T00:38:11Z",
   "region": "us-east-1",
   "resources": [],
   "detail": {
       "message" : "AWS Control Tower has detected that your member account 'account-
email@amazon.com (012345678909)' has been moved from organizational unit 'Sandbox
 (ou-0123-eEXAMPLE)' to 'Security (ou-3210-1EXAMPLE)'. For more information, including
 steps to resolve this issue, see 'https://docs.aws.amazon.com/console/controltower/
move-account'",
       "managementAccountId" : "012345678912",
       "organizationId" : "o-123EXAMPLE",
       "driftType" : "ACCOUNT_MOVED_BETWEEN_OUS",
       "remediationStep" : "Re-register this organizational unit (OU), or if the OU has
 more than 1000 accounts, you must update the provisioned product in Account Factory.",

       "accountId" : "012345678909",
       "sourceId" : "012345678909",
       "destinationId" : "ou-3210-1EXAMPLE"
   }
}
```

Panduan untuk membuat EventBridge aturan untuk menerima pemberitahuan drift:

Untuk membuat EventBridge aturan untuk notifikasi drift

1. Buka EventBridge Konsol Amazon:
2. Di panel navigasi, pilih Aturan.
3. Pilih Buat aturan.
4. Masukkan nama dan deskripsi aturan.
5. Untuk Tipe aturan, pilih Aturan dengan pola peristiwa.
6. Tentukan Sumber Acara:
   - Untuk “Sumber acara”, pilih AWS layanan sebagai sumber acara.
   - Untuk "nama AWS layanan”, pilih AWS Control Tower.
   - Untuk “Jenis acara”, pilih Drift Detected
7. Pilih Target:
   - Untuk jenis Target, pilih AWS layanan, dan untuk Pilih target, pilih target seperti topik pemberitahuan drift atau fungsi Lambda. Target terpicu saat peristiwa diterima yang sesuai dengan pola peristiwa yang ditentukan dalam aturan.
   - Bergantung pada target yang Anda pilih, berikan detail konfigurasi yang diperlukan, seperti nama fungsi Lambda atau ARN topik pemberitahuan drift.
8. Tinjau dan Buat Aturan:
   - Tinjau detail aturan Anda dan buat perubahan yang diperlukan.
   - Setelah Anda puas, klik Buat aturan untuk menyimpan EventBridge aturan baru.

Setelah membuat aturan, aturan akan mulai memantau peristiwa AWS Control Tower yang ditentukan dan memicu tindakan target yang dipilih saat peristiwa drift terjadi.

Jika Anda mengelola sumber daya di luar AWS Control Tower

AWS Control Tower menyiapkan akun, unit organisasi, dan sumber daya lain atas nama Anda, tetapi Anda adalah pemilik sumber daya ini. Anda dapat mengubah sumber daya ini di dalam AWS Control Tower atau di luarnya. Tempat paling umum untuk mengubah sumber daya di luar AWS Control Tower adalah AWS Organizations konsol. Topik ini menjelaskan cara merekonsiliasi perubahan pada sumber daya AWS Control Tower saat Anda membuat perubahan di luar AWS Control Tower.

Mengganti nama, menghapus, dan memindahkan sumber daya di luar konsol AWS Control Tower menyebabkan konsol menjadi tidak sinkron. Banyak perubahan dapat direkonsiliasi secara otomatis. Perubahan tertentu memerlukan pengaturan ulang ke zona pendaratan Anda, untuk memperbarui informasi yang ditampilkan di konsol AWS Control Tower.

Secara umum, perubahan yang Anda buat di luar konsol AWS Control Tower ke sumber daya AWS Control Tower membuat status penyimpangan yang dapat diselesaikan di zona pendaratan Anda. Untuk informasi lebih lanjut tentang perubahan ini, lihatPerubahan sumber daya yang dapat diperbaiki.

Tugas yang memerlukan pengaturan ulang zona pendaratan

- Menghapus OU Keamanan (Kasus khusus, tidak boleh dilakukan dengan enteng.)
- Menghapus akun bersama dari OU Keamanan (Tidak disarankan.)
- Memperbarui, melampirkan, atau melepaskan SCP yang terkait dengan OU Keamanan.

Perubahan yang diperbarui secara otomatis oleh AWS Control Tower

- Mengubah alamat email akun yang terdaftar
- Mengganti nama akun terdaftar
- Membuat unit organisasi tingkat atas (OU) baru
- Mengganti nama OU terdaftar
- Menghapus OU terdaftar (Kecuali OU Keamanan, yang memerlukan pembaruan.)
- Menghapus akun terdaftar (Kecuali akun bersama di OU Keamanan.)

> **Note**
>
> AWS Service Catalog menangani perubahan secara berbeda dari AWS Control Tower. AWS Service Catalog dapat menciptakan perubahan dalam postur tata kelola ketika mendamaikan perubahan Anda. Untuk informasi selengkapnya tentang memperbarui produk yang disediakan, lihat Memper barui Produk yang Disediakan dalam dokumentasi AWS Service Catalog .

Mengacu pada sumber daya di luar AWS Control Tower

Saat Anda membuat OU dan akun baru di luar AWS Control Tower, akun tersebut tidak diatur oleh AWS Control Tower, meskipun akun tersebut mungkin ditampilkan.

Membuat OU

Unit Organisasi (OU) yang dibuat di luar AWS Control Tower disebut sebagai Tidak Ter daftar. Mereka ditampilkan di halaman Organisasi, tetapi tidak diatur oleh kontrol Menara Kontrol AWS.

Membuat akun

Akun yang dibuat di luar AWS Control Tower disebut sebagai Tidak Ter daftar. Akun terdaftar dan tidak terdaftar milik OU yang terdaftar di AWS Control Tower ditampilkan di halaman Organisasi. Akun yang bukan milik OU terdaftar dapat diundang dengan menggunakan AWS Organizations konsol. Undangan untuk bergabung ini tidak mendaftarkan akun di AWS Control Tower atau memperluas tata kelola AWS Control Tower ke akun. Untuk memperluas tata kelola dengan men daftarkan akun, buka halaman Organisasi atau halaman detail akun di AWS Control Tower dan pilih Daftarkan akun.

Mengubah nama sumber daya AWS Control Tower secara eksternal

Anda dapat mengubah nama unit organisasi (OU) dan akun di luar konsol AWS Control Tower, dan konsol diperbarui secara otomatis untuk mencerminkan perubahan tersebut.

Mengganti nama OU

Di AWS Organizations, Anda dapat mengubah nama OU dengan menggunakan AWS Organizations API atau konsol. Saat Anda mengubah nama OU di luar AWS Control Tower, konsol AWS Control Tower secara otomatis mencerminkan perubahan nama. Namun, jika Anda menyediakan akun menggunakan AWS Service Catalog, Anda juga harus mengatur ulang zona pendaratan untuk memastikan AWS Control Tower tetap konsisten dengan AWS Organizations. Alur kerja Reset memastikan konsistensi di seluruh layanan untuk OU Dasar dan Tambahan. Anda dapat mengatasi jenis penyimpangan ini dari halaman pengaturan zona pendaratan. Lihat bagian yang disebut “Menyelesaikan Drift” diMendeteksi dan mengatasi penyimpangan di AWS Control Tower.

AWS Control Tower menampilkan nama-nama OU di halaman Organisasi di dasbor AWS Control Tower. Anda dapat melihat kapan operasi reset zona pendaratan Anda telah berhasil.

Mengganti nama akun yang terdaftar

Setiap AWS akun memiliki nama tampilan yang dapat diubah oleh pengguna root akun di AWS Manajemen Penagihan dan Biaya konsol. Saat Anda mengganti nama akun yang terdaftar di AWS Control Tower, perubahan nama secara otomatis tercermin di AWS Control Tower. Untuk informasi selengkapnya tentang mengubah nama akun, lihat M engelola AWS akun di Panduan Pengguna AWS Penagihan.

Menghapus OU Keamanan

Jenis penyimpangan ini adalah kasus khusus. Jika Anda menghapus OU Keamanan, Anda akan melihat halaman pesan kesalahan, meminta Anda untuk mengatur ulang zona pendaratan Anda. Anda harus mengatur ulang zona pendaratan sebelum dapat mengambil tindakan lain di AWS Control Tower.

- Anda tidak akan dapat melakukan tindakan apa pun di konsol AWS Control Tower dan Anda tidak akan dapat membuat akun baru AWS Service Catalog sampai reset selesai.
- Anda tidak akan dapat melihat halaman pengaturan zona pendaratan untuk melihat tombol Reset di sana.

Dalam situasi ini, proses reset zona pendaratan membuat OU Keamanan baru dan memindahkan dua akun bersama ke OU Keamanan baru. AWS Control Tower menandai akun Log Archive dan Audit sebagai hanyut. Proses yang sama menyelesaikan penyimpangan dalam akun ini.

Jika Anda menentukan bahwa Anda harus menghapus OU Keamanan, inilah yang perlu Anda ketahui:

Sebelum Anda dapat menghapus OU Keamanan, Anda harus memastikan bahwa itu tidak berisi akun. Secara khusus, Anda harus menghapus Arsip Log dan akun Audit dari OU. Kami menyarankan Anda memindahkan akun ini ke OU lain.

> **Note**
>
> Tindakan menghapus OU Keamanan Anda tidak akan dilakukan tanpa pertimbangan. Tindakan tersebut dapat menimbulkan masalah kepatuhan jika pencatatan ditangguhkan sementara, dan karena beberapa kontrol mungkin tidak diberlakukan.

Untuk informasi umum tentang drift, lihat “Menyelesaikan Drift” diMendeteksi dan mengatasi penyimpangan di AWS Control Tower.

Menghapus akun dari OU Keamanan

Kami tidak menyarankan Anda menghapus akun bersama apa pun dari organisasi Anda atau memindahkannya dari OU Keamanan. Jika Anda telah menghapus akun bersama secara tidak sengaja, Anda dapat mengikuti langkah-langkah perbaikan di bagian ini untuk memulihkan akun.

- Dari dalam konsol AWS Control Tower: Untuk memulai proses remediasi, ikuti langkah-langkah remediasi semi-manual. Pastikan pengguna atau peran yang Anda gunakan untuk mengakses konsol AWS Control Tower memiliki izin untuk berjalan`organizations:InviteAccountToOrganization`. Jika Anda tidak memiliki izin tersebut, ikuti langkah-langkah remediasi manual, yang menggunakan konsol AWS Control Tower dan AWS Organizations konsol.
- Mulai dari AWS Organizations konsol: Proses remediasi ini adalah prosedur yang sedikit lebih lama dan sepenuhnya manual. Saat mengikuti langkah-langkah remediasi manual, Anda akan beralih antara AWS Organizations konsol dan konsol AWS Control Tower. Saat bekerja AWS Organizations, Anda memerlukan pengguna atau peran dengan kebijakan terkel `AWSOrganizationsFullAccess` ola atau yang setara. Saat bekerja di konsol AWS Control Tower, Anda memerlukan pengguna atau peran dengan kebijakan terkel `AWSControlTowerServiceRolePolicy` ola atau yang setara, dan izin untuk menjalankan semua tindakan AWS Control Tower (menara kontrol: *).
- Jika langkah remediasi tidak memulihkan akun, hubungi AWS Dukungan.

Hasil menghapus akun bersama melalui AWS Organizations:

- Akun tidak lagi dilindungi oleh kontrol wajib AWS Control Tower dengan kebijakan kontrol layanan (SCP). Hasil: Sumber daya yang dibuat oleh AWS Control Tower di akun dapat dimodifikasi atau dihapus.
- Akun tersebut tidak lagi berada di bawah akun AWS Organizations manajemen. Hasil: Administrator akun AWS Organizations manajemen tidak lagi memiliki visibilitas ke dalam pengeluaran akun.
- Akun tidak lagi dijamin akan dipantau oleh AWS Config. Hasil: Administrator akun AWS Organizations manajemen mungkin tidak dapat mendeteksi perubahan sumber daya.
- Akun tidak lagi ada di organisasi. Hasil: Pembaruan dan pengaturan ulang AWS Control Tower akan gagal.

Untuk memulihkan akun bersama menggunakan konsol AWS Control Tower (prosedur semi-manual)

1. Masuk ke konsol AWS Control Tower di https://console.aws.amazon.com/controltower. Anda harus masuk sebagai pengguna IAM, pengguna di Pusat Identitas IAM, atau peran dengan izin untuk menjalankan. `organizations:InviteAccountToOrganization` Jika Anda tidak memiliki izin tersebut, gunakan prosedur remediasi manual yang dijelaskan nanti dalam topik ini.
2. Pada halaman terdeteksi penyimpangan zona pendaratan, pilih Re-Invite untuk memperbaiki penghapusan akun bersama dengan mengundang kembali akun bersama ke dalam organisasi. Email yang dibuat secara otomatis dikirim ke alamat email untuk akun.
3. Terima undangan untuk membawa akun bersama kembali ke organisasi. Lakukan salah satu tindakan berikut:

   - Masuk ke akun bersama yang telah dihapus, lalu buka https://console.aws.amazon.com/organizations/home #/undang
   - Jika Anda memiliki akses ke pesan email yang dikirim saat Anda mengundang kembali akun, masuk ke akun yang dihapus, lalu klik tautan dalam pesan untuk menavigasi langsung ke undangan akun.
   - Jika akun bersama yang dihapus tidak ada di organisasi lain, masuk ke akun, buka AWS Organizations konsol dan navigasikan ke Und angan.
4. Masuk ke akun manajemen lagi, atau muat ulang konsol AWS Control Tower jika sudah terbuka. Anda akan melihat halaman drift zona pendaratan. Pilih Reset untuk memperbaiki zona pendaratan.
5. Tunggu proses reset selesai.

Jika remediasi berhasil, akun bersama muncul dalam keadaan normal dan kepatuhan.

Jika langkah perbaikan tidak memulihkan akun, hubungi AWS Dukungan.

Untuk memulihkan akun bersama menggunakan AWS Control Tower dan AWS Organizations konsol (Remediasi manual)

1. Masuk ke AWS Organizations konsol dihttps://console.aws.amazon.com/organizations/. Anda harus masuk sebagai pengguna IAM, pengguna di Pusat Identitas IAM, atau peran dengan kebijakan terkel `AWSOrganizationsFullAccess` ola atau yang setara.
2. Undang akun bersama kembali ke organisasi. Untuk informasi tentang persyaratan, prasyarat, dan prosedur untuk mengundang akun AWS Organizations, lihat Mengundang AWS akun ke organisasi Anda di Panduan AWS Organizations Pengguna.

3. Masuk ke akun bersama yang telah dihapus, lalu buka https://console.aws.amazon.com/organizations/home #/undang untuk menerima undangan.
4. Masuk ke akun manajemen lagi.
5. Masuk ke konsol AWS Control Tower sebagai pengguna atau peran dengan kebijakan terkel `AWSControlTowerServiceRolePolicy` ola atau yang setara, dan izin untuk menjalankan semua tindakan AWS Control Tower (menara kontrol: *).
6. Anda akan melihat halaman drift zona pendaratan dengan opsi untuk mengatur ulang zona pendaratan. Pilih Reset untuk memperbaiki zona pendaratan.
7. Tunggu proses reset selesai.

Jika remediasi berhasil, akun bersama muncul dalam keadaan normal dan kepatuhan.

Jika langkah perbaikan tidak memulihkan akun, hubungi AWS Dukungan.

Perubahan eksternal yang diperbarui secara otomatis

Perubahan yang Anda buat pada alamat email akun diperbarui oleh AWS Control Tower secara otomatis, tetapi Account Factory tidak memperbaruinya secara otomatis.

Mengubah alamat email akun yang diatur

AWS Control Tower mengambil dan menampilkan alamat email sesuai kebutuhan pengalaman konsol. Oleh karena itu, alamat email akun bersama dan alamat email lainnya diperbarui dan ditampilkan secara konsisten di AWS Control Tower setelah Anda mengubahnya.

> **Note**
>
> Di AWS Service Catalog, Account Factory menampilkan parameter yang ditentukan di konsol saat Anda membuat produk yang disediakan. Namun, alamat email akun asli tidak diperbarui secara otomatis ketika alamat email akun berubah. Itu karena akun secara konseptual terkandung dalam produk yang disediakan; itu tidak sama dengan produk yang disediakan. Untuk memperbarui nilai ini, Anda harus memperbarui produk yang disediakan, yang dapat menyebabkan perubahan postur tata kelola.

Menerapkan AWS Config aturan eksternal

AWS Control Tower menampilkan status kepatuhan dari semua AWS Config aturan yang digunakan ke unit organisasi yang terdaftar di AWS Control Tower, termasuk aturan yang diaktifkan di luar konsol AWS Control Tower.

Menghapus sumber daya AWS Control Tower di luar AWS Control Tower

Anda dapat menghapus OU dan akun di AWS Control Tower dan Anda tidak perlu mengambil tindakan lebih lanjut untuk melihat pembaruan. Account Factory diperbarui secara otomatis saat Anda menghapus OU, tetapi tidak saat Anda menghapus akun.

Menghapus OU terdaftar (kecuali OU Keamanan)

Di dalamnya AWS Organizations, Anda dapat menghapus unit organisasi kosong (OU) dengan menggunakan API atau konsol. OU yang berisi akun tidak dapat dihapus.

AWS Control Tower menerima pemberitahuan AWS Organizations saat OU dihapus. Ini memperbarui daftar OU di Pabrik Akun, sehingga daftar OU terdaftar tetap konsisten.

> **Note**
>
> Di AWS Service Catalog, Pabrik Akun diperbarui untuk menghapus OU yang dihapus dari daftar OU yang tersedia tempat Anda dapat menyediakan akun.

Menghapus akun terdaftar dari OU

Saat Anda menghapus akun terdaftar, AWS Control Tower menerima pemberitahuan dan membuat pembaruan, sehingga informasi tetap konsisten.

> **Note**
>
> Di AWS Service Catalog, produk yang disediakan Account Factory yang mewakili akun yang diatur tidak diperbarui untuk menghapus akun. Sebagai gantinya, produk yang disediakan ditampilkan sebagai `TAINTED` dan dalam status kesalahan. Untuk membersihkan, buka AWS Service Catalog, pilih produk yang disediakan, lalu pilih Hentikan.

Mengatur organisasi dan akun dengan AWS Control Tower

Semua unit organisasi (OU) dan akun yang Anda buat di AWS Control Tower diatur secara otomatis oleh AWS Control Tower. Selain itu, jika Anda memiliki OU dan akun yang sudah dibuat di luar AWS Control Tower, Anda dapat membawanya ke tata kelola AWS Control Tower.

Untuk AWS akun AWS Organizations dan akun yang ada, sebagian besar pelanggan lebih suka mendaftarkan grup akun dengan mendaftarkan seluruh unit organisasi (OU) yang berisi akun. Anda juga dapat mendaftarkan akun secara individual. Untuk informasi selengkapnya tentang mendaftarkan akun individual, lihatTentang mendaftarkan akun yang ada.

Terminologi

- Ketika Anda membawa organisasi yang sudah ada ke AWS Control Tower, itu disebut mendaftar kan organisasi, atau memperluas tata kelola ke organisasi.
- Saat Anda membawa AWS akun ke AWS Control Tower, itu disebut men daftarkan akun.

Lihat OU dan akun Anda

Di halaman Organisasi Menara Kontrol AWS, Anda dapat melihat semua OU di Anda AWS Organizations, termasuk OU yang terdaftar di AWS Control Tower dan yang tidak terdaftar. Anda dapat melihat OU bersarang sebagai bagian dari hierarki. Cara mudah untuk melihat unit organisasi Anda di halaman Organisasi adalah dengan memilih Unit organisasi hanya dari dropdown di kanan atas.

Halaman Organisasi mencantumkan semua akun di organisasi Anda, terlepas dari OU atau status pendaftaran di AWS Control Tower. Cara mudah untuk melihat akun Anda di halaman Organisasi adalah dengan memilih Akun hanya dari dropdown di kanan atas. Anda dapat melihat, memperbarui, dan mendaftarkan akun secara individual dalam OU, jika akun memenuhi prasyarat untuk pendaftaran.

Jika Anda tidak memilih pemfilteran apa pun, halaman Organisasi menampilkan akun dan OU Anda dalam hierarki. Ini adalah lokasi pusat untuk memantau dan mengambil tindakan pada semua sumber daya AWS Control Tower Anda. Untuk informasi selengkapnya tentang halaman Organisasi, Anda dapat melihat panduan video.

> **Note**
>
> Saat Anda mengaktifkan akses tepercaya pada organisasi yang berisi zona pendaratan Anda, AWS Control Tower dapat membuat peran, mengelola sumber daya, dan membaca data untuk semua akun di organisasi. Melalui akses tepercaya, akun atau OU apa pun di organisasi tersedia untuk AWS Control Tower, baik terdaftar dan terdaftar, atau tidak terdaftar dan tidak terdaftar.

Panduan video

Video ini (4:01) menjelaskan cara bekerja dengan halaman Organisasi di AWS Control Tower. Untuk tampilan yang lebih baik, pilih ikon di sudut kanan bawah video untuk memperbesarnya ke layar penuh. Keterangan tersedia.

Panduan Video Bekerja dengan Halaman Organisasi di Menara Kontrol AWS.

Topik

- Mendaftarkan unit organisasi yang ada dengan AWS Control Tower
- Tentang mendaftarkan akun yang ada
- Transfer akun ke organisasi yang berbeda

Memperluas tata kelola ke organisasi yang sudah ada

Anda dapat menambahkan tata kelola AWS Control Tower ke organisasi yang sudah ada dengan menyiapkan zona pendaratan (LZ) seperti yang diuraikan dalam Panduan Pengguna Menara Kontrol AWS di Memulai, Langkah 2.

Inilah yang diharapkan saat menyiapkan zona pendaratan AWS Control Tower di organisasi yang sudah ada.

- Anda dapat memiliki satu zona pendaratan per AWS Organizations organisasi.
- AWS Control Tower menggunakan akun manajemen dari AWS Organizations organisasi Anda yang ada sebagai akun manajemennya. Tidak diperlukan akun manajemen baru.
- AWS Control Tower menyiapkan dua akun baru di OU terdaftar: akun audit dan akun logging.

- Batas layanan organisasi Anda harus memungkinkan pembuatan dua akun tambahan ini.
- Setelah Anda meluncurkan zona pendaratan atau mendaftarkan OU, kontrol AWS Control Tower berlaku secara otomatis ke semua akun terdaftar di OU tersebut.
- Anda dapat M endaf AWS tarkan akun tambahan yang ada ke OU yang diatur oleh AWS Control Tower, sehingga kontrol berlaku untuk akun tersebut.
- Anda dapat menambahkan lebih banyak OU di AWS Control Tower dan Anda dapat Mendaftarkan OU yang sudah ada.

Untuk memeriksa prasyarat lain untuk pendaftaran dan pendaftaran, lihat Memulai dengan AWS Control Tower.

Berikut detail selengkapnya tentang bagaimana kontrol AWS Control Tower tidak berlaku untuk OU Anda di organisasi AWS yang tidak memiliki zona pendaratan AWS Control Tower yang diatur:

- Akun baru yang dibuat di luar AWS Control Tower Account Factory tidak terikat oleh kontrol OU terdaftar.
- Akun baru yang dibuat di OU yang tidak terdaftar di AWS Control Tower tidak terikat oleh kontrol, kecuali jika Anda secara khusus men daftar kan akun tersebut ke AWS Control Tower. Lihat Tentang mendaftarkan akun yang ada untuk informasi selengkapnya tentang mendaftarkan akun.
- Organisasi tambahan yang ada, akun yang ada, dan OU baru atau akun apa pun yang Anda buat di luar AWS Control Tower, tidak terikat oleh kontrol Menara Kontrol AWS, kecuali Anda mendaftarkan OU secara terpisah atau mendaftarkan akun tersebut.

Untuk informasi selengkapnya tentang cara menerapkan AWS Control Tower ke OU dan akun yang ada, lihatMendaftarkan unit organisasi yang ada dengan AWS Control Tower.

Untuk gambaran umum tentang proses menyiapkan zona pendaratan AWS Control Tower di organisasi Anda yang sudah ada, lihat video di bagian berikutnya.

> **Note**
>
> Selama pengaturan, AWS Control Tower melakukan pemeriksaan awal untuk menghindari masalah umum. Namun, jika saat ini Anda menggunakan solusi Zona Pen AWS daratan untuk AWS Organizations, tanyakan kepada arsitek AWS solusi Anda sebelum mencoba mengaktifkan AWS Control Tower di organisasi Anda untuk menentukan apakah AWS Control Tower dapat mengganggu penerapan zona pendaratan Anda saat ini. Juga, lihat

Jika akun tidak memenuhi prasyarat informasi tentang memindahkan akun dari satu zona pendaratan ke zona pendaratan lainnya.

Video: Aktifkan Zona Pendaratan yang ada AWS Organizations

Video ini (7:48), menjelaskan cara mengatur dan mengaktifkan zona pendaratan Menara Kontrol AWS di AWS Organizations struktur yang ada. Untuk tampilan yang lebih baik, pilih ikon di sudut kanan bawah video untuk memperbesarnya ke layar penuh. Keterangan tersedia.

Aktifkan AWS Control Tower untuk organisasi yang sudah ada

Pertimbangan untuk Pusat Identitas IAM dan organisasi yang ada

- Jika AWS IAM Identity Center (Pusat Identitas IAM) sudah disiapkan, Wilayah rumah AWS Control Tower harus sama dengan Wilayah Pusat Identitas IAM.
- AWS Control Tower tidak menghapus konfigurasi yang ada.
- Jika Pusat Identitas IAM sudah diaktifkan, dan jika Anda menggunakan Direktori Pusat Identitas IAM, AWS Control Tower menambahkan sumber daya seperti kumpulan izin, grup, dan sebagainya, dan melanjutkan seperti biasa.
- Jika direktori lain (eksternal, AD, Managed AD) diatur, AWS Control Tower tidak mengubah konfigurasi yang ada. Untuk detail selengkapnya, lihat Pertimbangan untuk AWS IAM Identity Center Pelanggan (Pusat Identitas IAM).

Akses ke yang lain AWS layanan

Setelah Anda membawa organisasi Anda ke tata kelola AWS Control Tower, Anda masih memiliki akses ke AWS layanan apa pun yang tersedia melalui AWS Organizations, melalui AWS Organizations konsol dan API. Lihat informasi yang lebih lengkap di Layanan AWS terkait.

OU bersarang di Menara Kontrol AWS

Bab ini mencantumkan harapan dan pertimbangan yang ingin Anda ketahui saat bekerja dengan OU bersarang di AWS Control Tower. Dalam kebanyakan hal, bekerja dengan OU bersarang sama dengan bekerja dengan struktur OU datar. Register dan Re-register fitur berfungsi dengan OU bersarang, kecuali untuk perilaku yang diubah yang dicatat dalam Bab ini.

Panduan Video

Video ini (4:46) menjelaskan cara mengelola penerapan OU bersarang di AWS Control Tower. Untuk tampilan yang lebih baik, pilih ikon di sudut kanan bawah video untuk memperbesarnya ke layar penuh. Keterangan tersedia.

Panduan Video Mengelola OU Bersarang di Menara Kontrol AWS.

Untuk panduan mengenai praktik terbaik untuk OU bersarang dan zona pendaratan Anda, lihat posting blog Mengatur zona pendaratan Menara Kontrol AWS Anda dengan OU bersarang.

Perluas dari struktur OU datar ke struktur OU bersarang

Jika Anda membuat zona pendaratan AWS Control Tower dengan struktur OU datar, Anda dapat memperluasnya ke struktur OU bersarang.

Proses ini memiliki empat langkah utama:

1. Buat struktur OU bersarang yang Anda inginkan di AWS Control Tower.
2. Buka AWS Organizations konsol dan gunakan fitur pemindahan massal mereka untuk memindahkan akun dari OU sumber (datar) ke OU tujuan (bersarang). Begini caranya:
   a. Pergi ke OU tempat Anda ingin memindahkan akun.
   b. Pilih semua akun di OU.
   c. Pilih Pindahkan.

   > **Note**
   >
   > Langkah ini harus dilakukan di dalam AWS Organizations konsol karena AWS Control Tower tidak memiliki fitur Move.

3. Buka OU bersarang di Menara Kontrol AWS dan Daftar atau Re-register itu. Semua akun di OU bersarang akan didaftarkan.
   - Jika Anda membuat OU di AWS Control Tower, Re-register OU.
   - Jika Anda membuat OU di AWS Organizations, Daf tarkan OU untuk pertama kalinya.
4. Setelah akun Anda dipindahkan dan terdaftar, hapus OU tingkat atas yang kosong, baik dari AWS Organizations konsol atau dari konsol AWS Control Tower.

Pra-pemeriksaan pendaftaran OU bersarang

Untuk mendukung keberhasilan pendaftaran OU bersarang Anda dan akun anggotanya, AWS Control Tower melakukan serangkaian pemeriksaan awal. Pemeriksaan awal yang sama ini dilakukan saat mendaftarkan OU tingkat atas atau OU bersarang. Untuk informasi selengkapnya, lihat Penyebab umum kegagalan selama pendaftaran atau pendaftaran ulang.

- Jika semua pra-pemeriksaan lulus, AWS Control Tower mulai mendaftarkan OU Anda, secara otomatis.
- Jika ada pra-pemeriksaan yang gagal, AWS Control Tower menghentikan proses pendaftaran dan memberi Anda daftar item yang harus diperbaiki sebelum Anda dapat mendaftarkan OU Anda.

OU dan peran bersarang

AWS Control Tower menerapkan `AWSControlTowerExecution` peran ke akun di bawah OU target, dan ke akun di semua OU yang bersarang di bawah OU target, bahkan ketika niat Anda adalah mendaftarkan OU target saja. Peran ini memberi setiap pengguna akun manajemen izin Administrator pada akun apa pun yang memiliki `AWSControlTowerExecution` peran tersebut. Peran dapat digunakan untuk melakukan tindakan yang biasanya tidak diizinkan oleh kontrol AWS Control Tower.

Anda dapat menghapus peran ini dari akun yang tidak terdaftar yang tidak Anda rencanakan untuk didaftarkan. Jika Anda menghapus peran ini, Anda tidak dapat mendaftarkan akun dengan AWS Control Tower, atau mendaftarkan OU induk langsung, kecuali Anda mengembalikan peran tersebut ke akun. Untuk menghapus `AWSControlTowerExecution` peran dari akun, Anda harus masuk di bawah `AWSControlTowerExecution` peran tersebut, karena tidak ada kepala sekolah IAM lain yang diizinkan untuk menghapus peran yang dikelola oleh AWS Control Tower.

Untuk informasi tentang cara membatasi akses peran, lihat Kondisi opsional untuk hubungan kepercayaan peran Anda.

Apa yang terjadi selama pendaftaran dan pendaftaran ulang OU dan akun bersarang

Saat Anda mendaftarkan atau mendaftarkan ulang OU bersarang, AWS Control Tower mendaftarkan semua akun OU target yang tidak terdaftar, dan memperbarui semua akun terdaftar. Inilah yang diharapkan.

AWS Control Tower melakukan tugas-tugas berikut

- Menambahkan `AWSControlTowerExecution` peran ke semua akun yang tidak terdaftar di bawah OU ini, dan ke semua akun yang tidak terdaftar di OU bersarangnya.
- Mendaftarkan akun anggota yang tidak terdaftar.
- Re-enrolls akun anggota terdaftar.
- Membuat login Pusat Identitas IAM untuk akun anggota yang baru terdaftar.
- Memperbarui akun anggota terdaftar yang ada untuk mencerminkan perubahan zona pendaratan Anda.
- Memperbarui kontrol yang dikonfigurasi untuk OU ini dan akun anggotanya.

Pertimbangan untuk pendaftaran OU bersarang

- Anda tidak dapat mendaftarkan OU di bawah OU inti (OU Keamanan).
- OU bersarang harus didaftarkan secara terpisah.
- Anda tidak dapat mendaftarkan OU kecuali OU induknya terdaftar.
- Anda tidak dapat mendaftarkan OU kecuali semua OU yang lebih tinggi di pohon telah berhasil didaftarkan pada suatu waktu (beberapa mungkin telah dihapus).
- Anda dapat mendaftarkan OU yang berada di bawah OU yang lebih tinggi yang melayang, tetapi penyimpangan tidak diperbaiki oleh tindakan itu.

Batasan OU bersarang

- OU dapat bersarang maksimal 5 level jauh di bawah akar.
- OU bersarang di bawah OU target harus didaftarkan atau didaftarkan ulang secara terpisah.
- Jika OU target berada di Level 2 atau di bawah dalam hierarki, yaitu, jika itu bukan OU tingkat atas, kontrol preventif yang diaktifkan pada OU yang lebih tinggi diberlakukan pada OU ini dan semua OU di bawahnya, secara otomatis.
- Kegagalan registrasi OU tidak menyebar ke atas pohon hierarki. Anda dapat melihat detail tentang status OU bersarang di halaman detail OU induk.
- Kegagalan registrasi OU tidak menyebar ke bawah pohon hierarki.
- AWS Control Tower tidak mengubah pengaturan VPC Anda untuk akun baru atau yang sudah ada.

OU bersarang dan kepatuhan

Dari konsol AWS Control Tower, Anda dapat melihat OU dan akun yang tidak sesuai di halaman Organisasi, sehingga Anda dapat memahami kepatuhan dalam skala yang lebih besar.

Pertimbangan tentang kepatuhan untuk OU dan akun bersarang

- Kepatuhan OU tidak ditentukan berdasarkan kepatuhan OU yang bersarang di bawahnya.
- Status kepatuhan kontrol dihitung pada semua OU tempat kontrol diaktifkan, termasuk OU bersarang. Lihat status kepatuhan AWS Control Tower untuk OU dan akun.
- OU ditampilkan sebagai tidak sesuai hanya jika memiliki akun yang tidak sesuai, terlepas dari di mana OU berada dalam hierarki OU.
- Jika OU bersarang tidak sesuai, OU induknya tidak secara otomatis dianggap tidak sesuai.
- Pada halaman detail OU atau detail akun, Anda dapat melihat daftar sumber daya yang tidak sesuai yang mungkin menyebabkan OU atau akun Anda menampilkan status tidak sesuai.

OU bersarang dan drift

Dalam situasi tertentu, drift dapat mencegah pendaftaran OU bersarang.

Harapan untuk U drift dan bersarang

- Anda dapat mengaktifkan kontrol pada OU dengan orang tua yang hanyut, tetapi tidak pada OU yang hanyut secara langsung.
- Anda diizinkan untuk mengaktifkan kontrol detektif di bawah OU yang hanyut, selama itu bukan OU yang melayang tingkat atas.
- Kontrol wajib diaktifkan hanya pada OU tingkat atas. Kontrol wajib dilewati saat Anda mendaftarkan OU bersarang.
- Satu kontrol wajib melindungi AWS Config sumber daya; oleh karena itu, kontrol itu harus dalam keadaan tidak hanyut untuk mendaftarkan OU bersarang. Jika hanyut, AWS Control Tower memblokir pendaftaran OU bersarang.
- Jika OU tingkat atas sedang menyimpang, kontrol yang melindungi AWS Config sumber daya mungkin hanyut. Dalam situasi ini, AWS Control Tower memblokir tindakan apa pun yang memerlukan pembuatan atau pembaruan sumber AWS Config daya, termasuk penerapan kontrol detektif.

OU dan kontrol bersarang

Saat Anda mengaktifkan kontrol pada OU terdaftar, kontrol preventif dan detektif memiliki perilaku yang berbeda. Untuk OU bersarang, kontrol proaktif berperilaku mirip dengan kontrol detektif.

Kontrol preventif

- Kontrol preventif diberlakukan pada OU bersarang.
- Kontrol preventif wajib diberlakukan pada semua akun di bawah OU dan OU bersarangnya.
- Kontrol preventif memengaruhi semua akun dan OU yang bersarang di bawah OU target, bahkan jika akun dan OU tersebut tidak terdaftar.

Kontrol detektif dan proaktif

- OU bersarang tidak mewarisi kontrol detektif atau proaktif secara otomatis; ini harus diaktifkan secara terpisah.
- Kontrol detektif dan proaktif hanya digunakan untuk akun terdaftar di Wilayah operasi zona pendaratan Anda.

Status kontrol dan warisan yang diaktifkan

Anda dapat melihat kontrol yang diwariskan untuk setiap OU, pada halaman detail OU.

> **Tip**
>
> Anda dapat menggunakan warisan kontrol untuk membantu tetap berada dalam kuota SCP OU. Misalnya, Anda dapat mengaktifkan kontrol di OU tingkat atas hierarki OU, alih-alih mengaktifkan langsung untuk OU bersarang.

Status warisan

- Status War isan menunjukkan bahwa kontrol diaktifkan oleh warisan saja, dan belum diterapkan langsung ke OU.
- Status Di aktifkan berarti kontrol diterapkan pada OU ini, terlepas dari statusnya pada OU lain.
- Status Gagal berarti kontrol tidak diterapkan pada OU ini, terlepas dari statusnya pada OU lain.

> **Note**
>
> Status War isan menunjukkan bahwa kontrol diterapkan ke OU yang lebih tinggi di pohon, dan diterapkan pada OU ini, tetapi tidak ditambahkan langsung ke OU ini.

> **Jika zona pendaratan Anda bukan versi saat ini**
>
> Setiap baris dalam tabel kontrol yang diaktifkan mewakili satu kontrol yang diaktifkan pada satu OU individual.

OU bersarang dan akarnya

Root bukan OU, dan tidak dapat didaftarkan atau didaftarkan ulang. Anda juga tidak dapat membuat akun langsung di root. Akar tidak boleh tidak sesuai atau memiliki status siklus hidup, seperti terdaftar atau dalam drift.

Namun, root adalah wadah tingkat atas untuk semua akun dan OU. Dalam konteks OU bersarang, itu adalah simpul di mana semua OU lainnya bersarang.

Mendaftarkan unit organisasi yang ada dengan AWS Control Tower

Cara efisien untuk membawa beberapa AWS akun yang sudah ada ke AWS Control Tower adalah dengan memperluas tata kelola oleh AWS Control Tower ke seluruh unit organisasi (OU).

Untuk mengaktifkan tata kelola AWS Control Tower atas OU yang sudah ada yang dibuat dengan AWS Organizations, dan akunnya, daftarkan OU ke zona pendaratan AWS Control Tower Anda. Anda dapat mendaftarkan OU yang berisi hingga 1000 akun. Jika OU berisi lebih dari 1000 akun, Anda tidak dapat mendaftarkannya di AWS Control Tower.

Saat Anda mendaftarkan OU, akun anggotanya terdaftar ke zona pendaratan AWS Control Tower. Mereka diatur oleh kontrol yang berlaku untuk OU mereka.

Dimulai dengan Landing Zone versi 4.0, Anda dapat langsung mengaktifkan kontrol pada OU. Kontrol detektif memerlukan perekaman AWS Config yang dapat diaktifkan dengan mendaftarkan OU atau mengaktifkan perekaman AWS Config pada OU. Daftar OU akan mengaktifkan`AWSControlTowerBaseline`. Aktifkan perekaman AWS Config akan

diaktifkan`ConfigBaseline`. Untuk informasi selengkapnya, lihat Jenis baseline dan Panduan Referensi Kontrol Menara Kontrol AWS

> **Note**
>
> Jika Anda belum memiliki zona pendaratan AWS Control Tower, mulailah dengan menyiapkan zona pendaratan, baik di organisasi baru yang dibuat oleh AWS Control Tower, atau di AWS Organizations organisasi yang sudah ada. Untuk detail selengkapnya tentang cara mengatur zona pendaratan, lihatMemulai dengan AWS Control Tower.

Apa yang terjadi pada akun saya ketika saya mendaftarkan OU saya?

AWS Control Tower memerlukan izin untuk membuat akses tepercaya antara AWS CloudFormation dan AWS Organizations atas nama Anda, sehingga AWS CloudFormation dapat menerapkan stack Anda ke akun di organisasi Anda secara otomatis.

- `AWSControlTowerExecution`Peran ditambahkan ke semua akun dengan status Tidak terdaftar.
- Kontrol wajib diaktifkan secara default ke OU Anda dan semua akunnya saat Anda mendaftarkan OU Anda.

Pendaftaran sebagian akun setelah OU terdaftar

Dimungkinkan untuk mendaftarkan OU dengan sukses, namun akun tertentu mungkin tetap tidak terdaftar. Jika demikian, akun ini tidak memenuhi beberapa prasyarat untuk pendaftaran. Jika pendaftaran akun sebagai bagian dari proses Register OU tidak berhasil, status akun di halaman akun menunjukkan Pendaftaran gagal. Anda juga dapat melihat informasi akun di halaman OU Anda seperti 4 dari 5, di bidang akun.

Misalnya, jika Anda melihat 4 dari 5, itu berarti bahwa OU Anda memiliki total 5 akun, dan 4 di antaranya berhasil terdaftar, tetapi satu akun gagal mendaftar selama proses Daftar OU. Anda dapat memilih Re-Register OU untuk memasukkan akun ke pendaftaran, setelah Anda memastikan akun memenuhi prasyarat pendaftaran.

Prasyarat pengguna IAM untuk mendaftarkan OU

Identi AWS Identity and Access Management tas (IAM) Anda (pengguna atau peran) atau identitas pengguna Pusat Identitas IAM harus disertakan pada portofolio Pabrik Akun yang sesuai saat Anda melakukan operasi Daftar OU, meskipun Anda sudah memiliki `Admin` izin. Jika tidak, pembuatan

produk yang disediakan akan gagal selama pendaftaran. Kegagalan terjadi karena AWS Control Tower bergantung pada kredensional pengguna IAM atau identitas pengguna IAM Identity Center saat mendaftarkan OU.

Portofolio yang relevan adalah portofolio yang dibuat oleh AWS Control Tower, yang disebut AWS Control Tower Account Factory Portfolio. Arahkan ke sana dengan memilih Katalog Layanan > Pabrik Akun > Portofolio Pabrik Akun AWS Control Tower. Kemudian pilih tab yang disebut Grup, peran, dan pengguna untuk melihat identitas Pusat Identitas IAM atau IAM Anda. Untuk informasi selengkapnya tentang cara memberikan akses, lihat dokument asi untuk AWS Service Catalog.

Daftarkan OU yang ada

Di konsol AWS Control Tower, pada halaman Organisasi, Anda dapat melihat semua OU dan akun organisasi Anda dalam hierarki, termasuk OU yang terdaftar di AWS Control Tower, dan yang tidak terdaftar.

Secara umum, OU yang tidak terdaftar dibuat di AWS Organizations, dan mereka tidak diatur oleh zona pendaratan lainnya. Anda dapat mendaftarkan OU yang ada yang berisi hingga 1000 akun. Jika OU berisi lebih dari 1000 akun, Anda tidak dapat mendaftarkannya di AWS Control Tower.

Untuk mendaftarkan OU yang ada dari konsol

1. Masuk ke konsol AWS Control Tower di https://console.aws.amazon.com/controltower.
2. Di menu navigasi panel kiri, pilih Organisasi.
3. Pada halaman Organisasi, pilih tombol radio di sebelah OU yang ingin Anda daftarkan, lalu pilih Daftar unit organisasi dari menu tar ik -turun Tindakan di kanan atas, atau sebagai alternatif, pilih nama OU sehingga Anda dapat melihat halaman detail OU untuk OU tersebut.
4. Pada halaman detail OU, di kanan atas Anda dapat memilih Daftar OU dari menu tarik-turun T indakan.

Proses pendaftaran membutuhkan minimal 10 menit untuk memperpanjang tata kelola ke OU, dan hingga 2 menit tambahan untuk setiap akun tambahan.

Untuk mendaftarkan OU yang ada dengan API

Untuk mendaftarkan OU yang ada dengan AWS Control Tower API, Anda dapat memanggil `EnableBaseline` API dengan `AWSControlTowerBaseline` di `baselineIdentifier` lapangan. Untuk informasi selengkapnya, lihat Mendaftarkan OU AWS Control Tower dengan API saja.

Hasil pendaftaran OU yang ada

Setelah Anda mendaftarkan OU yang ada, `AWSControlTowerExecution` peran tersebut memungkinkan AWS Control Tower memperluas tata kelola ke akun individualnya. Pagar pembatas diberlakukan, dan informasi tentang aktivitas akun dilaporkan ke akun audit dan pencatatan Anda.

Hasil lainnya termasuk yang berikut:

- `AWSControlTowerExecution`memungkinkan audit oleh akun audit AWS Control Tower.
- `AWSControlTowerExecution`membantu Anda mengonfigurasi logging organisasi Anda, sehingga semua log untuk setiap akun dikirim ke akun logging.
- `AWSControlTowerExecution`memastikan bahwa kontrol Menara Kontrol AWS yang Anda pilih berlaku secara otomatis ke setiap akun individu di OU Anda, serta ke setiap akun baru yang Anda buat di AWS Control Tower.

Untuk OU terdaftar, Anda dapat memberikan laporan kepatuhan dan keamanan berdasarkan fitur audit dan pencatatan yang diwujudkan oleh kontrol AWS Control Tower. Tim keamanan dan kepatuhan Anda dapat memverifikasi bahwa semua persyaratan terpenuhi, dan bahwa tidak ada penyimpangan organisasi yang terjadi. Untuk informasi lebih lanjut tentang drift, lihat[Mendeteksi dan mengatasi penyimpangan di AWS Control Tower](#).

> **Note**
>
> Satu situasi yang tidak biasa dapat terjadi ketika AWS Control Tower menampilkan OU dan akunnya. Jika Anda telah membuat akun di OU terdaftar dan kemudian Anda memindahkan akun terdaftar itu ke OU lain yang tidak terdaftar, terutama jika Anda menggunakannya AWS Organizations untuk memindahkan akun, Anda dapat melihat hasil akun “1 dari 0” di halaman detail OU Anda. Selanjutnya, Anda mungkin telah membuat akun lain yang tidak terdaftar di OU yang tidak terdaftar itu. Jika ada akun yang tidak terdaftar, konsol dapat membaca “1 dari 1" untuk OU. Tampaknya akun tunggal (yang baru dibuat) terdaftar, tetapi sebenarnya tidak. Anda harus mendaftarkan akun baru.

Buat OU baru

Berikut cara membuat OU atau OU bersarang di AWS Control Tower.

Cara membuat OU baru di AWS Control Tower

1. Arahkan ke halaman Organisasi.
2. Pilih Buat unit organisasi dari menu tar ik- turun Buat sumber daya di kanan atas.
3. Tentukan nama di bidang nama OU.
4. Di drop down Parent OU, Anda dapat melihat hierarki OU terdaftar. Pilih OU induk untuk OU baru yang Anda buat.
5. Pilih Tambahkan.

> **Tip**
>
> Untuk menambahkan OU bersarang dalam langkah yang lebih sedikit, pilih nama OU induk yang ditampilkan dalam tabel di halaman Organisasi, lihat halaman OU untuk OU induk tersebut, lalu pilih Tambahkan OU dari menu tarik- turun Tindakan di kanan atas. OU baru dibuat sebagai OU bersarang di bawah OU yang Anda pilih, secara otomatis.

> **Note**
>
> Jika zona pendaratan Anda tidak diperbarui, Anda akan melihat daftar datar alih-alih hierarki di menu dropdown. Bahkan jika zona pendaratan Anda menyertakan OU bersarang, Anda tidak akan melihat OU L5 di dropdown, karena Anda tidak dapat membuat OU baru di bawah OU L5. Untuk informasi selengkapnya tentang OU bersarang di AWS Control Tower, lihatOU bersarang di Menara Kontrol AWS.

Menghapus OU

AWS Control Tower mendukung tindakan konsol terpisah untuk membatalkan pendaftaran OU dan menghapus OU.

Menghapus OU adalah final. Itu tidak bisa dibatalkan.

Pertimbangan-pertimbangan

- OU harus kosong dari akun agar operasi H apus dan Deregister berhasil.

- Semua kontrol opsional harus dihapus dari OU.
- Anda harus membatalkan pendaftaran OU sebelum menghapusnya.
- Anda dapat menghapus OU dari AWS Control Tower dengan membatalkan pendaftaran, tanpa menghapusnya.

Untuk menghapus OU dari AWS Control Tower

1. Masuk ke konsol AWS Control Tower di https://console.aws.amazon.com/controltower.
2. Arahkan ke halaman Organisasi.
3. Pilih nama OU untuk melihat halaman detail OU, dan pastikan bahwa semua akun dihapus dari OU.
4. Juga pada halaman detail OU, pastikan bahwa semua kontrol opsional dihapus dari OU.
5. Kembali ke halaman Organisasi dan pilih tombol radio di sebelah OU.
6. Pilih Deregister unit organisasi dari menu tarik- turun Tindakan di kanan atas.
7. Berhenti di sini jika Anda tidak ingin menghapus OU sepenuhnya, hanya untuk membatalkan pendaftaran dari AWS Control Tower. Untuk menghapus OU sepenuhnya, lanjutkan ke langkah berikutnya.
8. Untuk melanjutkan, pilih H apus dari menu tar ik -turun Tindakan di kanan atas.

Anda harus menunggu hingga proses deregistrasi selesai sebelum Anda dapat membatalkan pendaftaran OU lain.

> **Note**
>
> Untuk menghapus akun yang dikelola oleh AWS Control Tower, Anda dapat menavigasi ke Ac count factory dari panel navigasi kiri di konsol AWS Control Tower. Untuk menghapus akun di OU yang tidak dikelola oleh AWS Control Tower, buka AWS Organizations konsol.

Untuk membatalkan pendaftaran OU secara terprogram, panggil API. `DisableBaseline`

Penyebab umum kegagalan selama pendaftaran atau pendaftaran ulang

Secara umum, saat Anda mendaftarkan atau mendaftarkan ulang OU, semua akun dalam OU tersebut terdaftar di AWS Control Tower. Namun, ada kemungkinan bahwa beberapa akun mungkin

gagal mendaftar, bahkan jika OU secara keseluruhan berhasil terdaftar. Dalam kasus ini, Anda harus menyelesaikan kegagalan pra-pemeriksaan yang terkait dengan akun dan kemudian mencoba mendaftarkan ulang akun atau OU tersebut.

Jika pendaftaran (atau pendaftaran ulang) OU atau akun anggotanya gagal, AWS Control Tower mengembalikan pesan kesalahan untuk akun anggota yang terpengaruh. Anda dapat melihat pesan kesalahan pada halaman detail OU, di mana tabel menggabungkan pra-pemeriksaan dan pesan kesalahan akun. Jika operasi Register OU gagal, tabel menunjukkan semua pesan kesalahan untuk semua akun di bawah OU. Jika perlu, Anda juga dapat melihat pesan kesalahan di halaman detail akun untuk setiap akun.

Secara opsional, Anda dapat mengunduh file yang berisi laporan terperinci yang menunjukkan pra-pemeriksaan mana yang tidak lulus, untuk analisis offline. Anda dapat menyelesaikan unduhan dengan memilih tombol Unduh, yang muncul di kanan atas area pendaftaran.

Bagian ini mencantumkan jenis kesalahan yang mungkin Anda terima jika pra-pemeriksaan gagal, dan cara memperbaiki kesalahan.

Kesalahan Zona Pendaratan

- Zona pendaratan belum siap

  Setel ulang zona pendaratan Anda saat ini, atau perbarui ke versi terbaru.

Kesalahan OU

- Melebihi jumlah maksimum SCP

  Anda mungkin melebihi batas kebijakan kontrol layanan (SCP) per OU, atau Anda mungkin telah mencapai kuota lain. Batas 10 SCP per OU berlaku untuk semua OU di zona pendaratan AWS Control Tower Anda. Jika Anda memiliki lebih banyak SCP daripada yang diizinkan kuota, Anda harus menghapus atau menggabungkan SCP.
- SCP yang saling bertentangan

  SCP yang ada dapat diterapkan ke OU atau akun, yang mencegah AWS Control Tower mendaftarkan akun. Periksa SCP yang diterapkan untuk mengetahui kebijakan apa pun yang dapat mencegah AWS Control Tower bekerja. Pastikan untuk memeriksa SCP yang diwarisi dari OU yang lebih tinggi dalam hierarki.
- Melebihi kuota stack set

Kuota set tumpukan mungkin telah terlampaui. Jika Anda memiliki lebih banyak instans daripada yang diizinkan kuota, Anda harus menghapus beberapa instans tumpukan. Untuk informasi lebih lanjut, lihat kuota AWS CloudFormation dalam Panduan Pengguna AWS CloudFormation .

- Melebihi batas akun

  AWS Control Tower membatasi setiap OU hingga 1000 akun selama pendaftaran.

Kesalahan akun

- Pre-checks dicegah pada akun

  SCP yang ada di OU mencegah AWS Control Tower melakukan pra-pemeriksaan pada akun anggota OU Anda. Untuk mengatasi kegagalan pra-pemeriksaan ini, perbarui atau hapus SCP dari OU.

- Kesalahan alamat email

  Alamat email yang Anda tentukan untuk akun tidak sesuai dengan standar penamaan. Berikut adalah ekspresi reguler (regex) yang menentukan karakter mana yang diizinkan: `[A-Z0-9a-z._%+-]+@[A-Za-z0-9.-]+[.]+[A-Za-z]+`

- Perekam konfigurasi atau saluran pengiriman diaktifkan

  Akun mungkin memiliki perekam AWS Config konfigurasi atau saluran pengiriman yang ada. Ini harus dihapus atau dimodifikasi melalui AWS CLI di semua Wil AWS ayah di mana akun manajemen Menara Kontrol AWS telah mengatur sumber daya, sebelum Anda dapat mendaftarkan akun.

- STS dinonaktifkan

  AWS Security Token Service (AWS STS) dapat dinonaktifkan di akun. AWS Titik akhir STS harus diaktifkan di akun untuk semua Wilayah yang didukung oleh AWS Control Tower.

- Konflik Pusat Identitas IAM

  Wilayah rumah AWS Control Tower tidak sama dengan Wilayah AWS IAM Identity Center (Pusat Identitas IAM). Jika Pusat Identitas IAM sudah disiapkan, wilayah beranda AWS Control Tower harus sama dengan Wilayah Pusat Identitas IAM.

- Topik SNS yang bertentangan

Akun tersebut memiliki nama topik Amazon Simple Notification Service (Amazon SNS) yang perlu digunakan AWS Control Tower. AWS Control Tower membuat sumber daya (seperti topik SNS) dengan nama tertentu. Jika nama-nama ini sudah diambil, penyiapan AWS Control Tower gagal. Situasi ini dapat terjadi jika Anda menggunakan kembali akun yang sebelumnya terdaftar di AWS Control Tower.

- Akun yang ditangguhkan terdeteksi

  Akun ini telah ditangguhkan. Itu tidak dapat didaftarkan ke AWS Control Tower. Hapus akun dari OU ini, dan coba lagi.

- Pengguna IAM tidak dalam portofolio

  Tambahkan pengguna AWS Identity and Access Management (IAM) ke portofolio Katalog Layanan sebelum mendaftarkan OU Anda. Kesalahan ini hanya berkaitan dengan akun manajemen.

- Akun tidak memenuhi prasyarat

  Akun tidak memenuhi prasyarat untuk pendaftaran akun. Misalnya, akun mungkin kehilangan peran dan izin yang diperlukan untuk mendaftarkannya di AWS Control Tower. Instruksi untuk menambahkan peran tersedia diMenambahkan peran IAM yang diperlukan secara manual ke yang sudah ada Akun AWS dan mendaftarkannya.

Sebagai pengingat, AWS CloudTrail diaktifkan secara otomatis di semua AWS akun Anda saat Anda mendaftarkannya di AWS Control Tower. Jika CloudTrail diaktifkan pada akun sebelum pendaftaran, Anda dapat mengalami penagihan ganda kecuali Anda menonaktifkan CloudTrail sebelum memulai proses pendaftaran.

Perbarui organisasi

Cara tercepat untuk memperbarui unit organisasi (OU) atau memperbarui beberapa akun dalam OU adalah dengan melakukan salah satu tindakan berikut:

- Re-register OU jika `AWSControlTowerBaseline` diaktifkan.
- Setel ulang garis dasar yang diaktifkan atau setel ulang kontrol yang diaktifkan jika tidak `AWSControlTowerBaseline` diaktifkan.

Kapan harus memperbarui AWS Control Tower OU dan akun

Saat melakukan pembaruan landing zone, Anda harus memperbarui akun terdaftar untuk menerapkan kontrol baru ke akun tersebut.

- Anda dapat melakukan pembaruan ke semua akun di bawah OU menggunakan opsi Re-Register atau Reset.
- Jika Anda memiliki lebih dari satu OU terdaftar di landing zone Anda, daftarkan ulang atau atur ulang semua OU Anda untuk memperbarui semua akun Anda.
- Untuk memperbarui satu akun, Anda dapat memperbarui dari konsol AWS Control Tower, atau Anda dapat memilih opsi Perbarui produk yang disediakan AWS Service Catalog jika AWSControlTowerBaseline diaktifkan di akun. Lihat Perbarui akun di konsol.

Perbarui beberapa akun di OU yang sama

Ulangi langkah-langkah ini untuk setiap OU di organisasi AWS Control Tower Anda, jika Anda perlu memperbarui semua akun dan OU Anda.

Untuk memperbarui beberapa akun dalam satu OU, dengan satu tindakan

1. Masuk ke konsol AWS Control Tower di https://console.aws.amazon.com/controltower.
2. Di menu navigasi panel kiri, pilih Organisasi.
3. Pada halaman Organisasi, pilih OU untuk melihat halaman detail OU.
4. Jika AWSControlTowerBaseline diaktifkan pada OU, pilih Re-Register OU di bawah Tindakan. Jika tidak AWSControlTowerBaseline diaktifkan di OU, pilih Reset baseline AWS Config di bawah Tindakan untuk mengatur ulang baseline yang diaktifkan dan pilih kontrol yang diaktifkan dan Atur ulang kontrol di bawah bagian “Kontrol yang diaktifkan” untuk mengatur ulang kontrol yang diaktifkan.

Atau, Anda dapat memilih akun apa pun yang menunjukkan status Pembaruan yang tersedia dan kemudian memilih Perbarui akun, untuk akun sebanyak yang diperlukan.

Apa yang terjadi selama pendaftaran ulang

Saat Anda mendaftar ulang OU:

- Kolom status dasar AWS Control Tower menunjukkan apakah aplikasi **`AWSControlTowerBaseline`** diterapkan ke akun (Diaktifkan), apakah baseline belum diterapkan (Tidak diaktifkan), atau apakah penerapan baseline gagal sebelumnya (Gagal).
- Saat Anda mendaftarkan ulang OU, `AWSControlTowerExecution` peran ditambahkan ke semua akun dengan status Tidak diaktifkan atau Gagal.
- AWS Control Tower membuat login masuk tunggal (IAM Identity Center) untuk akun baru yang terdaftar.
- Akun yang diaktifkan didaftarkan ulang ke AWS Control Tower.
- Drift pada kontrol preventif apa pun yang diterapkan pada OU diperbaiki, karena SCP dikembalikan ke definisi defaultnya.
- Semua akun diperbarui untuk mencerminkan perubahan landing zone terbaru.

Untuk informasi selengkapnya, lihat Tentang mendaftarkan akun yang ada.

> **Tip**
>
> Saat Anda mendaftarkan ulang OU, atau saat memperbarui versi landing zone dan beberapa akun anggota, Anda mungkin melihat pesan kegagalan yang menyebutkan. StackSet-AWSControlTowerExecutionRole Ini StackSet di akun manajemen dapat gagal karena peran AWSControlTowerExecutionIAM sudah ada di semua akun anggota terdaftar. Pesan kesalahan ini adalah perilaku yang diharapkan, dan dapat diabaikan.

Perbarui satu akun

> **Note**
>
> Penyediaan, pembaruan, dan penyesuaian akun tunggal harus menargetkan unit organisasi (OU) dengan AWSControlTowerBaseline diaktifkan. Jika OU tidak mengaktifkan, Anda dapat mengaktifkan pendaftaran otomatis akun atau penggunaan ResetEnabledBaseline dan ResetEnabledControl API pada EnabledBaselines dan EnabledControls pada

OU tersebut untuk mendaftarkan akun. AWSControlTowerBaseline Untuk detailnya AWSControlTowerBaseline, lihat:Jenis dasar yang berlaku di tingkat OU.

Anda dapat memperbarui akun AWS Control Tower individual di konsol AWS Control Tower, atau di konsol Service Catalog.

Untuk memperbarui satu akun di konsol AWS Control Tower, lihatPerbarui akun di konsol.

Untuk memperbarui satu akun di AWS Service Catalog

1. Kunjungi AWS Service Catalog.
2. Di menu navigasi panel kiri, pilih Produk yang disediakan.
3. Pada halaman Produk yang disediakan, pilih tombol radio di sebelah produk yang disediakan yang ingin Anda perbarui.
4. Di kanan atas, pilih dropdown Actions to Update.

Untuk mempelajari lebih lanjut tentang memperbarui AWS Service Catalog, lihat Memperbarui produk yang disediakan di Service Catalog dan Memperbarui produk di Panduan Administrator Service Catalog.

Transfer akun ke organisasi yang berbeda

Anda dapat mentransfer akun anggota yang terdaftar di AWS Control Tower ke AWS Organizations organisasi lain.

Prasyarat

- Akun harus terdaftar di AWS Control Tower di organisasi sumber. Artinya, akun memiliki garis dasar, kontrol proaktif, atau kontrol detektif yang diterapkan padanya.
- Akun harus dibuat setidaknya 4 hari sebelum transfer.
- Anda harus memiliki akses ke akun manajemen organisasi sumber dan tujuan.

Langkah 1: Buka pendaftaran akun dari AWS Control Tower

Sebelum Anda mentransfer akun, Anda harus menonaktifkan semua sumber daya AWS Control Tower yang langsung diterapkan padanya. Akun dapat terus mewarisi kontrol pencegahan.

Jika Anda menggunakan Auto Enroll

Pindahkan akun ke salah satu lokasi berikut:

- Akar organisasi
- OU yang tidak terkelola
- Dengan Landing Zone 4.0 atau yang lebih baru, OU yang hanya mengaktifkan kontrol preventif

Jika Anda tidak menggunakan Auto Enroll

Metode di bawah ini juga tersedia jika Anda menggunakan Auto Enroll.

- Untuk akun dengan AWS Control Tower dan Backup baseline, pilih Unmanage dari konsol AWS Control Tower. Anda juga dapat menghentikan produk yang disediakan dengan AWS Service Catalog atau konsol. APIs
- Untuk akun dengan baseline AWS Config, nonaktifkan baseline AWS Config di OU, atau pindahkan akun ke root dan gunakan API. `DisableBaseline`

Langkah 2: Transfer akun ke organisasi tujuan

Setelah semua baseline AWS Control Tower dan kontrol yang diterapkan ke akun selain kontrol preventif dinonaktifkan, selesaikan transfer.

1. Dari akun manajemen organisasi tujuan, kirim undangan ke akun anggota.
2. Terima undangan dari akun anggota.
3. Dari akun manajemen organisasi tujuan, pindahkan akun ke OU yang diinginkan.

Untuk petunjuk tentang proses migrasi, lihat Memigrasi AWS akun ke organisasi lain di Panduan AWS Organizations Pengguna.

Langkah 3: Daftarkan akun di organisasi tujuan

Setelah akun berada di organisasi tujuan, daftarkan di AWS Control Tower.

- Jika Auto Enroll diaktifkan di zona landing zone AWS Control Tower yang mengatur organisasi tujuan, AWS Control Tower secara otomatis menerapkan baseline dan kontrol ke akun.

- Jika Anda tidak menggunakan Auto Enroll di organisasi tujuan, daftarkan akun secara manual di AWS Control Tower. Untuk informasi selengkapnya, lihat Tentang mendaftarkan akun yang ada.

Pertimbangan tambahan

Periode tunggu

Akun yang dibuat melalui AWS Organizations atau Account Factory harus berusia minimal 4 hari sebelum Anda dapat mentransfernya atau menghapusnya dari organisasi. Untuk informasi selengkapnya, lihat Menghapus akun anggota dari organisasi di Panduan AWS Organizations Pengguna.

AWS Batas agregator Config

Saat mentransfer beberapa akun, Anda mungkin mencapai batas AWS Config untuk jumlah maksimum akun yang ditambahkan atau dihapus per minggu untuk semua agregator (1.000). Untuk meminta peningkatan batas, lihat Batas layanan AWS Config. Anda juga dapat meningkatkan ke landing zone versi 4.0, yang menggunakan agregator Config terkait layanan. Untuk detail selengkapnya, lihat Pembaruan AWS Config di landing zone versi 4.0.

Akses akun anggota

Akun yang tidak terdaftar tidak memiliki peran`AWSControlTowerExecution`. Saat Anda menonaktifkan garis dasar Config atau AWS Control Tower, AWS Control Tower menghapus peran pelaksanaannya dan menambahkan. `OrganizationsAccountAccessRole` Anda dapat menggunakan peran ini untuk menerima undangan untuk organisasi tujuan.

Ketika akun terdaftar di organisasi tujuan, `AWSControlTowerExecution` peran dibuat. Peran ini menggantikan `OrganizationsAccountAccessRole` dan mempercayai akun manajemen baru.

AWS Service Catalog dan Auto Enroll

Auto Enroll tidak bertindak atas sumber daya di AWS Service Catalog. Setiap produk yang disediakan Account Factory tetap berada di akun manajemen meskipun akun yang mendasarinya tidak terdaftar. Untuk menghentikan produk yang disediakan ini di akun manajemen, lihat Menghapus produk yang disediakan di Panduan Pengguna Service Catalog.AWS Semua cetak biru Kustomisasi Account Factory (AFC) tetap ada di akun.

Layanan terintegrasi

AWS Control Tower adalah layanan yang dibangun di atas AWS layanan lain, untuk membantu Anda dalam menyiapkan lingkungan yang dirancang dengan baik. Bab ini memberikan gambaran singkat tentang layanan ini, termasuk informasi konfigurasi tentang layanan yang mendasarinya dan cara kerjanya di AWS Control Tower.

Untuk informasi lebih lanjut tentang cara mengukur lingkungan yang dirancang dengan baik, pelajari tentang Alat AWS Well-Architected . Lihat juga Panduan Lingkungan Cloud Manajemen dan Tata Kelola.

Topik

- AWS Opsi cadangan tersedia
- Menyebarkan Lingkungan dengan CloudFormation
- Memantau Acara dengan CloudTrail
- Memantau Sumber Daya dan Layanan dengan CloudWatch
- Mengatur Konfigurasi Sumber Daya dengan AWS Config
- Kelola Izin untuk Entitas dengan IAM
- AWS Key Management Service
- Jalankan Fungsi Komputasi Tanpa Server dengan Lambda
- Mengelola Akun Melalui AWS Organizations
- Simpan Objek dengan Amazon S3
- Pantau lingkungan Anda dengan Security Hub CSPM
- Rekening penyediaan melalui AWS Service Catalog
- Lacak Peringatan Melalui Layanan Pemberitahuan Sederhana Amazon
- Membangun Aplikasi Terdistribusi dengan AWS Step Functions

AWS Opsi cadangan tersedia

AWS Backup memungkinkan Anda membuat rencana cadangan untuk zona pendaratan AWS Control Tower Anda. Anda dapat memasukkan alur kerja cadangan dan pemulihan data langsung ke zona pendaratan Anda. Rencana pencadangan mencakup aturan yang telah ditentukan sebelumnya,

seperti hari retensi, frekuensi pencadangan, dan jendela waktu di mana pencadangan terjadi. Untuk informasi selengkapnya, lihat AWS Backup dan AWS Control Tower.

Menyebarkan Lingkungan dengan CloudFormation

CloudFormation memungkinkan Anda membuat dan menyediakan penerapan AWS infrastruktur secara dapat diprediksi dan berulang kali. Ini membantu Anda memanfaatkan AWS produk untuk membangun aplikasi yang sangat andal, sangat skalabel, dan hemat biaya di cloud tanpa khawatir tentang membuat dan mengonfigurasi AWS infrastruktur yang mendasarinya. CloudFormation memungkinkan Anda untuk menggunakan file template untuk membuat dan menghapus kumpulan sumber daya bersama-sama sebagai satu unit (tumpukan). Untuk informasi selengkapnya, lihat Panduan Pengguna AWS CloudFormation.

AWS Control Tower digunakan CloudFormation StackSets untuk menyebarkan dan mengelola sumber daya dasar, seperti peran dan AWS Config perekam IAM, di akun Anda. Untuk informasi selengkapnya tentang cara CloudFormation dan AWS Control Tower bekerja bersama, lihatBuat AWS Control Tower sumber daya dengan AWS CloudFormation.

Memantau Acara dengan CloudTrail

AWS Control Tower mengonfigurasi AWS CloudTrail untuk mengaktifkan pencatatan dan audit terpusat. Dengan CloudTrail, akun manajemen dapat meninjau tindakan administratif dan peristiwa siklus hidup untuk akun anggota.

CloudTrail membantu Anda memantau AWS lingkungan Anda di cloud dengan menyimpan riwayat panggilan AWS API untuk akun Anda. Misalnya, Anda dapat mengidentifikasi pengguna dan akun yang memanggil AWS API untuk layanan yang mendukung CloudTrail, alamat IP sumber dari mana panggilan dilakukan, dan waktu ketika panggilan terjadi. Anda dapat mengintegrasikan CloudTrail ke dalam aplikasi menggunakan API, mengotomatiskan pembuatan jejak untuk organisasi Anda, memeriksa status jalur Anda, dan mengontrol cara administrator mengaktifkan dan menonaktifkan CloudTrail logging. Untuk informasi selengkapnya, lihat Panduan Pengguna AWS CloudTrail.

Memantau Sumber Daya dan Layanan dengan CloudWatch

Amazon CloudWatch menyediakan solusi pemantauan yang andal, terukur, dan fleksibel yang dapat Anda mulai gunakan dalam hitungan menit. Anda tidak perlu lagi menyiapkan, mengelola, dan

menskalakan sistem dan infrastruktur pemantauan Anda sendiri. Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon .

Untuk informasi selengkapnya tentang cara CloudWatch kerja Amazon dengan AWS Control Tower, lihat Pem antauan.

Mengatur Konfigurasi Sumber Daya dengan AWS Config

AWS Config memberikan tampilan terperinci tentang sumber daya yang terkait dengan AWS akun Anda, termasuk bagaimana mereka dikonfigurasi, bagaimana mereka terkait satu sama lain, dan bagaimana konfigurasi dan hubungannya telah berubah dari waktu ke waktu. Untuk informasi selengkapnya, silakan lihat Panduan Developer AWS Config.

AWS Config sumber daya yang disediakan oleh AWS Control Tower ditandai secara otomatis dengan `aws-control-tower` dan nilainya. `managed-by-control-tower`

Untuk informasi selengkapnya tentang cara AWS Config memantau dan merekam sumber daya di AWS Control Tower, dan cara menagih Anda untuk sumber daya tersebut, lihatPantau perubahan sumber daya dengan AWS Config.

AWS Control Tower digunakan Aturan AWS Config untuk menerapkan kontrol detektif. Untuk informasi selengkapnya, lihat Tentang kontrol di AWS Control Tower.

Integrasi AWS Config di Control Tower Landing Zone 4.0

Service-Linked Agregator Konfigurasi (SLCA)

AWS Control Tower sekarang mengimplementasikan Service-Linked Config Aggregator (SLCA) sebagai bagian dari Landing Zone 4.0+. Perubahan ini merupakan peningkatan signifikan dalam cara data AWS Config dikumpulkan dan dikelola di seluruh organisasi Anda.

Perubahan Utama

Penyebaran Agregator Service-Linked Konfigurasi Baru

- Agregator Service-Linked Konfigurasi diterapkan di akun integrasi AWS Config yang Anda tentukan.
- Untuk pelanggan lama, ini akan menjadi akun audit Anda

- Untuk pelanggan baru, ini akan menjadi akun yang ditentukan di `config.accountId` bidang manifes

Administrator yang Delegasi

- Akun agregator AWS Config menjadi administrator yang didelegasikan untuk AWS Config
- AWS Control Tower secara otomatis mengonfigurasi pengaturan admin yang didelegasikan
- Ini memungkinkan pengelolaan AWS Config terpusat di seluruh organisasi Anda

Migrasi dari Agregator Legacy

Selama peningkatan ke Zona Pendaratan 4.0:

- Agregator organisasi di akun manajemen akan dihapus.
- Agregator akun di akun audit akan dihapus.
- Ini digantikan oleh Agregator Konfigurasi terkait layanan baru di akun agregator integrasi AWS Config.

Agregasi Data yang Ditingkatkan

Agregator Config yang ditautkan layanan menyediakan kemampuan yang ditingkatkan untuk agregasi data Config:

- Dapat mengumpulkan data dari perekam AWS Config apa pun di organisasi Anda
- Termasuk data dari akun yang tidak dikelola oleh Control Tower
- Menyediakan tampilan komprehensif item konfigurasi di seluruh organisasi Anda
- Mendukung kontrol perimeter data yang ditingkatkan

Pertimbangan Penting

Konfigurasi Administrator yang Delegasi

- AWS Control Tower akan menggunakan akun yang ditentukan dalam manifes Anda untuk integrasi AWS Config
- Akun ini akan secara otomatis dikonfigurasi sebagai administrator yang didelegasikan
- Tidak ada tindakan tambahan yang diperlukan dari pelanggan untuk konfigurasi ini

- Untuk pelanggan lama, akun integrasi Peran Keamanan Anda sebelumnya (akun Audit) akan dikonfigurasi sebagai akun agregator pusat AWS Config selama peningkatan Landing Zone 4.0

Lingkup Agregasi Data

- Service-Linked Config Aggregator dapat mengumpulkan data konfigurasi dari:
  - Akun terkelola Control Tower
  - Non-Control Akun yang dikelola menara
  - Akun apa pun dengan perekam konfigurasi aktif di organisasi Anda

Kontrol Akses

- Akses ke data agregat dikelola melalui kebijakan IAM
- Akun agregator pusat AWS Config memiliki akses pusat ke semua data agregat
- Akun anggota memelihara perekam AWS Config individu mereka

Praktik Terbaik

Konfigurasikan Pemilihan Akun Agregator Pusat

- Pilih akun yang didedikasikan untuk keamanan dan pemantauan kepatuhan
- Pastikan kontrol akses yang tepat ada
- Pertimbangkan untuk menggunakan akun audit atau keamanan yang ada

Pengelolaan Data

- Tinjau data konfigurasi agregat secara teratur
- Menerapkan kebijakan retensi yang sesuai
- Pantau status perekam AWS Config di seluruh akun

Dampak Migrasi

Saat memutakhirkan ke Zona Pendaratan 4.0:

Sebelum Migrasi

- Dokumentasikan aturan dan agregator AWS Config yang ada
- Tinjau pola akses data AWS Config saat ini
- Rencanakan pembaruan kebijakan IAM yang diperlukan

Selama Migrasi

- Agregator AWS Config lama akan dihapus secara otomatis
- Service-Linked Config Aggregator akan digunakan
- Administrator yang didelegasikan akan dikonfigurasi

Setelah Migrasi

- Verifikasi Service-Linked Config Aggregator berfungsi dengan benar
- Konfirmasikan agregasi data dari akun anggota
- Perbarui alat pemantauan dan pelaporan sesuai kebutuhan

Kelola Izin untuk Entitas dengan IAM

AWS Identity and Access Management (IAM) adalah AWS layanan untuk mengontrol akses ke AWS layanan lain. Dengan IAM, Anda dapat secara terpusat mengelola pengguna, kredensial keamanan —seperti kunci akses, dan izin—yang menentukan AWS sumber daya tempat pengguna dan aplikasi Anda diberikan akses.

Saat Anda mengatur zona pendaratan, sejumlah grup dapat dibuat secara AWS IAM Identity Center otomatis, jika Anda memilih IAM sebagai penyedia identitas Anda. Grup ini memiliki kumpulan izin yang merupakan kebijakan izin yang telah ditentukan sebelumnya dari IAM. Pengguna akhir Anda juga dapat menggunakan IAM untuk menentukan ruang lingkup izin bagi pengguna IAM dan entitas lain dalam akun anggota.

AWS Identity and Access Management (IAM) menyederhanakan cara Anda mengelola akses ke AWS akun dan aplikasi bisnis. Anda dapat mengontrol akses Pusat Identitas IAM dan izin pengguna di semua AWS akun Anda di AWS Control Tower.

Untuk informasi selengkapnya, lihat Panduan Pengguna AWS IAM Identity Center.

Jika Anda berbasis di Wilayah AWS yang tidak mendukung IAM, Anda dapat membawa penyedia identitas lain, untuk mengatur dan memelihara pengguna dan grup Anda sendiri secara manual.

AWS Key Management Service

AWS Key Management Service (AWS KMS) memungkinkan Anda untuk membuat dan mengontrol kunci yang melindungi data Anda. AWS Control Tower secara opsional memungkinkan Anda mengenkripsi data Anda dengan kunci AWS KMS enkripsi. Untuk informasi tentang AWS KMS, lihat Panduan Pengembang AWS KMS.

Untuk informasi tentang cara mengatur AWS KMS kunci dengan AWS Control Tower, lihat Konfigurasi AWS KMS kunci secara opsional.

Jalankan Fungsi Komputasi Tanpa Server dengan Lambda

Dengan AWS Lambda, Anda dapat menjalankan kode tanpa menyediakan atau mengelola server. Anda dapat menjalankan kode untuk berbagai jenis aplikasi atau layanan backend — tanpa perlu biaya administrasi tambahan. Saat Anda mengunggah kode Anda, Lambda dapat menjalankan dan menskalakan kode dengan ketersediaan tinggi. Anda dapat mengatur kode Anda untuk memicu dari AWS layanan lain secara otomatis, atau Anda dapat memanggilnya langsung dari aplikasi web atau seluler apa pun.

Misalnya, peran tertentu dalam akun audit AWS Control Tower dapat diasumsikan secara terprogram, sehingga Anda dapat meninjau akun lain menggunakan Lambda. Selain itu, Anda dapat menggunakan peristiwa siklus hidup AWS Control Tower untuk memicu fungsi Lambda.

Mengelola Akun Melalui AWS Organizations

AWS Organizations adalah layanan manajemen akun yang memungkinkan Anda mengkonsolidasikan beberapa AWS akun ke dalam organisasi yang Anda buat dan kelola secara terpusat. Dengan Organisasi, Anda dapat membuat akun anggota dan mengundang akun yang ada untuk bergabung dengan organisasi Anda. Anda dapat mengatur akun tersebut ke dalam grup dan melampirkan kontrol berbasis kebijakan. Untuk informasi selengkapnya, lihat Panduan Pengguna AWS Organizations.

Di AWS Control Tower, Organisasi membantu mengelola penagihan secara terpusat; mengontrol akses, kepatuhan, dan keamanan; dan berbagi sumber daya di seluruh AWS akun anggota Anda. Akun dikelompokkan ke dalam kelompok logis, yang disebut unit organisasi (OU). Untuk informasi selengkapnya tentang Organisasi, lihat Panduan AWS Organizations Pengguna .

AWS Control Tower menggunakan OU berikut:

- Root — Wadah induk untuk semua akun dan semua OU lainnya di zona pendaratan Anda.
- Keamanan — OU ini berisi akun arsip log, akun audit, dan sumber daya yang mereka miliki.
- Sandbox — OU ini dibuat saat Anda mengatur zona pendaratan Anda. Itu dan OU anak lainnya di zona pendaratan Anda berisi akun anggota Anda. Ini adalah akun yang diakses pengguna akhir Anda untuk melakukan pekerjaan pada AWS sumber daya.

> **Note**
>
> Anda dapat menambahkan OU tambahan di zona pendaratan melalui konsol AWS Control Tower di halaman Unit organisasi.

Pertimbangan-pertimbangan

OU yang dibuat melalui AWS Control Tower dapat memiliki kontrol yang diterapkan padanya. OU yang dibuat di luar AWS Control Tower tidak dapat, secara default. Namun, Anda dapat mendaftarkan OU tersebut. Setelah Anda mendaftarkan OU, Anda dapat menerapkan kontrol padanya dan akunnya. Untuk informasi tentang mendaftarkan OU, lihat M endaftarkan unit organisasi yang ada dengan AWS Control Tower.

Simpan Objek dengan Amazon S3

Amazon Simple Storage Service (Amazon S3) adalah penyimpanan untuk internet. Anda dapat menggunakan Amazon S3 untuk menyimpan dan mengambil data sebanyak apa pun kapan pun, dari mana pun di web. Anda dapat menyelesaikan tugas-tugas ini menggunakan antarmuka web yang sederhana dan intuitif dari Konsol Manajemen AWS. Untuk informasi selengkapnya, lihat Panduan Pengguna Layanan Penyimpanan Sederhana Amazon .

Saat Anda mengatur zona pendaratan, bucket Amazon S3 dibuat di akun arsip log Anda untuk berisi semua log di semua akun di zona pendaratan Anda.

Pantau lingkungan Anda dengan Security Hub CSPM

AWS Control Tower terintegrasi dengan AWS Security Hub CSPM melalui standar Security Hub CSPM yang disebut Service-Managed Standar: AWS Control Tower. Untuk informasi selengkapnya, lihat Standar Hub Keamanan.

Rekening penyediaan melalui AWS Service Catalog

AWS Service Catalog memungkinkan administrator TI untuk membuat, mengelola, dan mendistribusikan portofolio produk yang disetujui kepada pengguna akhir, yang kemudian memiliki akses ke produk yang mereka butuhkan di portal yang dipersonalisasi. Produk umum termasuk server, database, situs web, atau aplikasi yang digunakan menggunakan AWS sumber daya.

Anda dapat mengontrol pengguna yang memiliki akses ke produk tertentu, yang memungkinkan Anda menegakkan kepatuhan terhadap standar bisnis organisasi, mengelola siklus hidup produk, dan membantu pengguna menemukan dan meluncurkan produk dengan percaya diri. Untuk informasi selengkapnya, lihat Panduan Administrator Katalog Layanan .

Di AWS Control Tower, administrator cloud pusat dan pengguna akhir Anda dapat menyediakan akun khusus di zona pendaratan Anda menggunakan AWS Service Catalog produk, yang disebut cetak biru khusus. Untuk informasi selengkapnya, lihat Lang kah2. Buat AWS Service Catalog produk.

Anda dapat berinteraksi dengan akun AWS Control Tower melalui AWS Service Catalog konsol dan API. Untuk informasi selengkapnya, lihat Berinteraksi dengan akun AWS Control Tower dari AWS Service Catalog

AWS Control Tower juga dapat menggunakan API Katalog Layanan untuk lebih mengotomatiskan penyediaan dan pembaruan akun. Untuk detailnya, lihat Panduan Peng AWS Service Catalog embang.

Lacak Peringatan Melalui Layanan Pemberitahuan Sederhana Amazon

Amazon Simple Notification Service (Amazon SNS) adalah layanan web yang memungkinkan aplikasi, pengguna akhir, dan perangkat untuk mengirim dan menerima pemberitahuan secara instan dari cloud. Untuk informasi lebih lanjut, lihat Panduan Developer Amazon Simple Notification Service.

AWS Control Tower menggunakan Amazon SNS untuk mengirim peringatan terprogram ke alamat email akun manajemen dan akun audit Anda. Peringatan ini membantu Anda mencegah penyimpangan di dalam zona pendaratan Anda. Untuk informasi selengkapnya, lihat Mendeteksi dan mengatasi penyimpangan di AWS Control Tower.

Kami juga menggunakan Layanan Pemberitahuan Sederhana Amazon untuk mengirim pemberitahuan kepatuhan dari AWS Config.

> **Tip**
>
> Salah satu cara terbaik untuk menerima pemberitahuan kepatuhan kontrol AWS Control Tower (di akun audit Anda) adalah dengan berlangganan`AggregateConfigurationNotifications`. Ini adalah layanan yang membantu Anda memeriksa kepatuhan. Ini memberi Anda data nyata tentang AWS Config aturan yang keluar dari kepatuhan. AWS Config secara otomatis memelihara daftar akun di OU Anda.
>
> Anda harus berlangganan secara manual, menggunakan email atau jenis langganan apa pun yang diizinkan oleh SNS. Pernyataan `arn:aws:sns:`*`homeregion`*`:`*`account`*`:aws-controltower-AggregateSecurityNotifications` tersebut mengarah ke akun audit Anda.

Membangun Aplikasi Terdistribusi dengan AWS Step Functions

AWS Step Functions membuatnya mudah untuk mengoordinasikan komponen aplikasi terdistribusi sebagai serangkaian langkah dalam alur kerja visual. Anda dapat dengan cepat membangun dan menjalankan mesin status untuk mengeksekusi langkah-langkah aplikasi Anda secara andal dan dapat diskalakan. Untuk informasi selengkapnya, silakan lihat Panduan Developer AWS Step Functions.

Manajemen identitas dan akses di AWS Control Tower

Untuk melakukan operasi apa pun di zona pendaratan Anda, seperti menyediakan akun di Account Factory atau membuat unit organisasi (OU) baru di konsol AWS Control Tower, baik AWS Identity and Access Management (IAM) atau AWS IAM Identity Center mengharuskan Anda untuk mengotentikasi bahwa Anda adalah pengguna yang disetujui. AWS Misalnya, jika Anda menggunakan konsol AWS Control Tower, Anda mengotentikasi identitas Anda dengan memberikan kredensi Anda AWS , seperti yang disediakan oleh administrator Anda.

Setelah Anda mengotentikasi identitas Anda, IAM mengontrol akses Anda ke AWS dengan kumpulan izin tertentu pada kumpulan operasi dan sumber daya tertentu. Jika Anda adalah administrator akun, Anda dapat menggunakan IAM untuk mengontrol akses pengguna IAM lain ke sumber daya yang terkait dengan akun Anda.

Topik

- Autentikasi
- Kontrol akses
- Bekerja dengan AWS Pusat Identitas IAM dan AWS Control Tower
- Ikhtisar pengelolaan izin akses ke sumber daya AWS Control Tower
- Mencegah peniruan lintas layanan
- Menggunakan kebijakan berbasis identitas (kebijakan IAM) untuk AWS Control Tower

Autentikasi

Anda memiliki akses AWS ke salah satu jenis identitas berikut:

- AWS pengguna root akun — Saat pertama kali membuat AWS akun, Anda mulai dengan identitas yang memiliki akses lengkap ke semua AWS layanan dan sumber daya di akun. Identitas ini disebut pengguna root AWS akun. Anda memiliki akses ke identitas ini ketika Anda masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari, bahkan tugas administratif. Sebagai gantinya, p atuhi praktik terbaik menggunakan pengguna root hanya untuk membuat pengguna Pusat Identitas IAM pertama Anda (disarankan) atau pengguna IAM (bukan praktik terbaik dalam sebagian besar kasus penggunaan). Kemudian, kunci kredensial pengguna akar

dengan aman dan gunakan kredensial itu untuk melakukan beberapa tugas manajemen akun dan layanan saja. Untuk informasi selengkapnya, lihat Kapan harus masuk sebagai pengguna root.

- Pengguna IAM — Pengguna IAM adalah identitas dalam AWS akun Anda yang memiliki izin khusus dan disesuaikan. Anda dapat menggunakan kredentif pengguna IAM untuk masuk untuk mengamankan AWS halaman web seperti Konsol AWS Manajemen, Forum AWS Diskusi, atau Pusat AWS Dukungan. AWS praktik terbaik menyarankan Anda membuat pengguna Pusat Identitas IAM alih-alih pengguna IAM, karena ada lebih banyak risiko keamanan saat Anda membuat pengguna IAM yang memiliki kredenSIAL jangka panjang.

  Jika Anda harus membuat pengguna IAM untuk tujuan tertentu, selain kredentif masuk, Anda dapat membuat kunci akses untuk setiap pengguna IAM. Anda dapat menggunakan tombol ini ketika Anda memanggil AWS layanan secara terprogram, baik melalui salah satu dari beberapa SDK atau dengan menggunakan AWS Command Line Interface (CLI). Alat SDK dan CLI menggunakan access key untuk menandatangani permintaan Anda secara kriptografis. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. AWS Control Tower mendukung Signature Version 4, protokol untuk mengotentikasi permintaan API masuk. Untuk informasi selengkapnya tentang mengotentikasi permintaan, lihat Proses Penandatanganan Tanda Tangan Versi 4 di Refer AWS ensi Umum.
- IAM role – IAM role adalah identitas IAM yang dapat Anda buat di akun Anda yang memiliki izin spesifik. Peran IAM mirip dengan pengguna IAM karena merupakan AWS identitas, dan memiliki kebijakan izin yang menentukan apa yang dapat dan tidak dapat dilakukan identitas. AWS Namun, alih-alih secara unik terkait dengan satu orang, peran dimaksudkan untuk menjadi dapat diambil oleh siapa pun yang membutuhkannya. Selain itu, peran tidak memiliki kredensial jangka panjang standar seperti kata sandi atau kunci akses yang terkait dengannya. Sebagai gantinya, saat Anda mengambil peran, kredensial keamanan sementara untuk sesi peran Anda akan diberikan. Peran IAM dengan kredensial sementara berguna dalam situasi berikut:
  - Akses pengguna federasi — Alih-alih membuat pengguna IAM, Anda dapat menggunakan identitas yang ada dari Directory Service, direktori pengguna perusahaan Anda, atau penyedia identitas web. Ini dikenal sebagai pengguna federasi. AWS memberikan peran kepada pengguna federasi ketika akses diminta melalui penyedia identitas. Untuk informasi lebih lanjut tentang pengguna gabungan, lihat Pengguna Gabungan dan Peran di Panduan Pengguna IAM.
  - AWS akses layanan — Peran layanan adalah peran IAM yang diasumsikan oleh layanan untuk melakukan tindakan di akun Anda atas nama Anda. Ketika Anda mengatur beberapa lingkungan AWS layanan, Anda harus menentukan peran untuk diasumsikan oleh layanan. Peran layanan ini harus menyertakan semua izin yang diperlukan agar layanan dapat mengakses AWS sumber daya yang dibutuhkannya. Peran layanan bervariasi dari satu layanan ke layanan lainnya,

tetapi banyak yang memungkinkan Anda memilih izin selama Anda memenuhi persyaratan terdokumentasi untuk layanan tersebut. Peran layanan hanya menyediakan akses dalam akun Anda dan tidak dapat digunakan untuk memberikan akses ke layanan dalam akun lain. Anda dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Misalnya, Anda dapat membuat peran yang memungkinkan Amazon Redshift untuk mengakses bucket Amazon S3 atas nama Anda dan kemudian memuat data yang tersimpan di bucket ke dalam klaster Amazon Redshift. Untuk informasi selengkapnya, lihat Membuat Peran untuk Mendelegasikan Izin ke AWS Layanan di Panduan Pengguna IAM.

- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredenSIAL sementara untuk aplikasi yang berjalan di instans Amazon EC2 dan membuat permintaan AWS CLI atau API. AWS Ini lebih disukai daripada menyimpan kunci akses dalam instans Amazon EC2. Untuk menetapkan AWS peran ke instans Amazon EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instans yang dilampirkan ke instans. Profil instans berisi peran dan memungkinkan program yang berjalan di instans Amazon EC2 untuk mendapatkan kredenSIAL sementara. Untuk informasi selengkapnya, lihat Menggunakan IAM role untuk memberikan izin ke aplikasi yang berjalan di instans Amazon EC2 dalam Panduan pengguna IAM.

- Oten tikasi pengguna Pusat Identitas IAM ke portal pengguna Pusat Identitas IAM dikendalikan oleh direktori yang telah Anda sambungkan ke Pusat Identitas IAM. Namun, otorisasi ke AWS akun yang tersedia untuk pengguna akhir dari dalam portal pengguna ditentukan oleh dua faktor:
  - Siapa yang telah diberi akses ke AWS akun tersebut di konsol Pusat Identi AWS tas IAM. Untuk informasi selengkapnya, lihat Sign-On Akses Tunggal di Panduan AWS IAM Identity Center Pengguna.
  - Tingkat izin apa yang telah diberikan kepada pengguna akhir di konsol Pusat Identi AWS tas IAM untuk memungkinkan mereka akses yang sesuai ke akun tersebut AWS . Untuk informasi selengkapnya, lihat Kumpulan Iz in di Panduan AWS IAM Identity Center Pengguna.

Kontrol akses

Untuk membuat, memperbarui, menghapus, atau membuat daftar sumber daya AWS Control Tower, atau AWS sumber daya lain di zona pendaratan Anda, Anda memerlukan izin untuk melakukan operasi, dan Anda memerlukan izin untuk mengakses sumber daya yang sesuai. Selain itu, untuk melakukan operasi secara terprogram, Anda memerlukan kunci akses yang valid.

Bagian berikut menjelaskan cara mengelola izin untuk AWS Control Tower:

Topik

- Ikhtisar pengelolaan izin akses ke sumber daya AWS Control Tower
- Menggunakan kebijakan berbasis identitas (kebijakan IAM) untuk AWS Control Tower

Bekerja dengan AWS Pusat Identitas IAM dan AWS Control Tower

Di AWS Control Tower, IAM Identity Center memungkinkan administrator cloud pusat dan pengguna akhir untuk mengelola akses ke beberapa AWS akun dan aplikasi bisnis. Secara default, AWS Control Tower menggunakan layanan ini untuk mengatur dan mengelola akses ke akun yang dibuat melalui Account Factory, kecuali Anda telah memilih opsi untuk mengelola sendiri identitas dan kontrol akses Anda.

Untuk informasi selengkapnya tentang memilih penyedia identitas, lihatPanduan Pusat Identitas IAM.

Untuk tutorial singkat tentang cara mengatur pengguna IAM Identity Center dan izin di AWS Control Tower, Anda dapat melihat video ini (6:23). Untuk tampilan yang lebih baik, pilih ikon di sudut kanan bawah video untuk memperbesarnya ke layar penuh. Captioning tersedia.

Panduan Video Menyiapkan Pusat Identitas AWS IAM di AWS Control Tower.

Tentang menyiapkan AWS Control Tower dengan IAM Identity Center

Saat Anda pertama kali menyiapkan AWS Control Tower, hanya pengguna root dan pengguna IAM dengan izin yang benar yang dapat menambahkan pengguna IAM Identity Center. Namun, setelah pengguna akhir ditambahkan dalam AWSAccountFactorygrup, mereka dapat membuat pengguna Pusat Identitas IAM baru dari wizard Account Factory. Untuk informasi selengkapnya, lihat Menyediakan dan mengelola akun dengan Account Factory.

Jika Anda memilih default yang disarankan, AWS Control Tower menyiapkan landing zone Anda dengan direktori yang telah dikonfigurasi sebelumnya yang membantu Anda mengelola identitas pengguna dan sistem masuk tunggal, sehingga pengguna Anda memiliki akses gabungan di seluruh akun. Saat menyiapkan landing zone, direktori default ini dibuat untuk berisi grup pengguna dan set izin.

> **Note**
>
> Anda dapat mendelegasikan administrasi AWS IAM Identity Center di organisasi Anda ke akun selain akun manajemen, dengan menggunakan fitur administrator yang didelegasikan

dari Pusat Identitas IAM. Jika Anda memilih untuk menggunakan fitur ini, ketahuilah bahwa Administrator dengan akses untuk mengelola keanggotaan grup juga dapat mengelola grup yang ditetapkan ke akun manajemen. Untuk informasi lebih lanjut, lihat posting blog ini, berjudul, Memulai dengan administrasi delegasi AWS SSO

Grup pengguna, peran, dan set izin

Grup pengguna mengelola peran khusus yang ditentukan dalam akun bersama Anda. Peran menetapkan set izin yang dimiliki bersama. Semua anggota grup mewarisi set izin, atau peran, yang terkait dengan grup. Anda dapat membuat grup baru untuk pengguna akhir akun anggota Anda, sehingga Anda hanya dapat menetapkan peran yang diperlukan untuk tugas tertentu yang dilakukan grup.

Set izin yang tersedia mencakup berbagai persyaratan izin pengguna yang berbeda, seperti akses hanya-baca, akses administratif AWS Control Tower, dan akses Service Catalog. Set izin ini memungkinkan pengguna akhir Anda untuk menyediakan AWS akun mereka sendiri di landing zone Anda dengan cepat, dan sesuai dengan pedoman perusahaan Anda.

Untuk tips merencanakan alokasi pengguna, grup, dan izin Anda, lihat Rekomendasi untuk menyiapkan grup, peran, dan kebijakan

Untuk informasi selengkapnya tentang cara menggunakan layanan ini dalam konteks AWS Control Tower, lihat topik berikut di Panduan AWS IAM Identity Center Pengguna.

- Untuk menambahkan pengguna, lihat Menambahkan Pengguna.
- Untuk menambahkan pengguna ke grup, lihat Menambahkan Pengguna ke Grup.
- Untuk mengedit properti pengguna, lihat Mengedit Properti Pengguna.
- Untuk menambahkan grup, lihat Menambahkan Grup.

Warning

AWS Control Tower menyiapkan direktori Pusat Identitas IAM Anda di Wilayah asal Anda. Jika Anda mengatur landing zone di Wilayah lain dan kemudian menavigasi ke konsol Pusat Identitas IAM, Anda harus mengubah Wilayah ke wilayah asal Anda. Jangan hapus konfigurasi Pusat Identitas IAM Anda di Wilayah rumah Anda.

Hal yang perlu diketahui tentang akun IAM Identity Center dan AWS Control Tower

Berikut adalah beberapa hal baik yang perlu diketahui saat bekerja dengan akun pengguna IAM Identity Center di AWS Control Tower.

- Jika akun pengguna AWS IAM Identity Center dinonaktifkan, Anda akan mendapatkan pesan galat saat mencoba menyediakan akun baru di Account Factory. Anda dapat mengaktifkan kembali pengguna Pusat Identitas IAM Anda di konsol Pusat Identitas IAM.
- Jika Anda menentukan alamat email pengguna IAM Identity Center baru saat memperbarui produk yang disediakan yang terkait dengan akun yang dijual oleh Account Factory, AWS Control Tower akan membuat akun pengguna IAM Identity Center baru. Akun pengguna yang dibuat sebelumnya tidak dihapus. Jika Anda memilih untuk menghapus alamat email pengguna IAM Identity Center sebelumnya dari AWS IAM Identity Center, lihat Menonaktifkan Pengguna.
- AWS IAM Identity Center telah terintegrasi dengan Azure Active Directory, dan Anda dapat menghubungkan Azure Active Directory yang ada ke AWS Control Tower.
- Untuk informasi selengkapnya tentang bagaimana perilaku AWS Control Tower berinteraksi dengan AWS IAM Identity Center dan berbagai sumber identitas, lihat Pertimbangan untuk Mengubah Sumber Identitas Anda dalam dokumentasi AWS IAM Identity Center.

Grup Pusat Identitas IAM untuk AWS Control Tower

AWS Control Tower menawarkan grup yang telah dikonfigurasi sebelumnya untuk mengatur pengguna yang melakukan tugas tertentu di akun Anda. Anda dapat menambahkan pengguna dan menetapkan mereka ke grup ini secara langsung di Pusat Identitas IAM. Melakukannya mencocokkan set izin ke pengguna dalam grup dalam akun Anda. Untuk panduan terbaru dan praktik terbaik dalam mengonfigurasi grup Anda, lihat Praktik terbaik di Panduan Pengguna Pusat Identitas IAM.

Grup berikut dibuat saat Anda mengatur landing zone Anda.

AWSAccountFactory

Akun	Set izin	Deskripsi
Akun manajemen	AWSServiceCatalogEndUserAccess	Grup ini hanya digunakan di akun ini untuk menyediak

Akun	Set izin	Deskripsi
		an akun baru menggunakan Account Factory.

AWSServiceCatalogAdmins

Akun	Set izin	Deskripsi
Akun manajemen	AWSServiceCatalogAdminFullAccess	Grup ini hanya digunakan di akun ini untuk melakukan perubahan administratif pada Account Factory. Pengguna di grup ini tidak dapat menyediakan akun baru kecuali mereka juga berada di AWSAccountFactorygrup.

AWSControlTowerAdmins

Akun	Set izin	Deskripsi
Akun manajemen	AWSAdministratorAccess	Pengguna grup ini di akun ini adalah satu-satunya yang memiliki akses ke konsol AWS Control Tower.
Akun arsip log	AWSAdministratorAccess	Pengguna memiliki akses administrator di akun ini.
Akun audit	AWSAdministratorAccess	Pengguna memiliki akses administrator di akun ini.
Akun anggota	AWSOrganizationsFullAccess	Pengguna memiliki akses penuh ke Organizations di akun ini.

AWSSecurityAuditPowerUsers

Akun	Set izin	Deskripsi
Akun manajemen	AWSPowerUserAccess	Pengguna dapat melakukan tugas pengembangan aplikasi dan dapat membuat dan mengkonfigurasi sumber daya dan layanan yang mendukung pengembangan aplikasi AWS sadar.
Akun arsip log	AWSPowerUserAccess	Pengguna dapat melakukan tugas pengembangan aplikasi dan dapat membuat dan mengkonfigurasi sumber daya dan layanan yang mendukung pengembangan aplikasi AWS sadar.
Akun audit	AWSPowerUserAccess	Pengguna dapat melakukan tugas pengembangan aplikasi dan dapat membuat dan mengkonfigurasi sumber daya dan layanan yang mendukung pengembangan aplikasi AWS sadar.
Akun anggota	AWSPowerUserAccess	Pengguna dapat melakukan tugas pengembangan aplikasi dan dapat membuat dan mengkonfigurasi sumber daya dan layanan yang mendukung pengembangan aplikasi AWS sadar.

AWSSecurityAuditors

Akun	Set izin	Deskripsi
Akun manajemen	AWSReadOnlyAccess	Pengguna memiliki akses hanya-baca ke semua AWS layanan dan sumber daya di akun ini.
Akun arsip log	AWSReadOnlyAccess	Pengguna memiliki akses hanya-baca ke semua AWS layanan dan sumber daya di akun ini.
Akun audit	AWSReadOnlyAccess	Pengguna memiliki akses hanya-baca ke semua AWS layanan dan sumber daya di akun ini.
Akun anggota	AWSReadOnlyAccess	Pengguna memiliki akses hanya-baca ke semua AWS layanan dan sumber daya di akun ini.

AWSLogArchiveAdmins

Akun	Set izin	Deskripsi
Akun arsip log	AWSAdministratorAccess	Pengguna memiliki akses administrator di akun ini.

AWSLogArchiveViewers

Akun	Set izin	Deskripsi
Akun arsip log	AWSReadOnlyAccess	Pengguna memiliki akses hanya-baca ke semua AWS

Akun	Set izin	Deskripsi
		layanan dan sumber daya di akun ini.

AWSAuditAccountAdmins

Akun	Set izin	Deskripsi
Akun audit	AWSAdministratorAccess	Pengguna memiliki akses administrator di akun ini.

Ikhtisar pengelolaan izin akses ke sumber daya AWS Control Tower

Setiap AWS sumber daya dimiliki oleh Akun AWS, dan izin untuk membuat atau mendapatkan akses ke sumber daya diatur oleh kebijakan izin. Administrator akun dapat melampirkan kebijakan izin pada identitas IAM (yaitu pengguna, grup, dan peran). Beberapa layanan (seperti AWS Lambda) juga mendukung melampirkan kebijakan izin ke sumber daya.

> **Note**
>
> Administrator akun (atau administrator) adalah pengguna dengan hak administrator. Untuk informasi selengkapnya, lihat Praktik Terbaik IAM dalam Panduan Pengguna IAM.

Ketika Anda bertanggung jawab untuk memberikan izin kepada pengguna atau peran, Anda harus mengetahui dan melacak pengguna dan peran yang memerlukan izin, sumber daya yang memerlukan izin untuk setiap pengguna dan peran, dan tindakan spesifik yang harus diizinkan untuk mengoperasikan sumber daya tersebut.

Topik

- Sumber daya dan operasi AWS Control Tower
- Tentang kepemilikan sumber daya
- Kelola akses ke sumber daya

- Tentukan elemen kebijakan: Tindakan, Efek, dan Prinsip
- Menentukan kondisi dalam kebijakan

Sumber daya dan operasi AWS Control Tower

Di AWS Control Tower, sumber daya utama adalah zona pen daratan. AWS Control Tower juga mendukung jenis sumber daya tambahan, kontrol, kadang-kadang disebut sebagai pagar pem batas. Namun, untuk AWS Control Tower, Anda hanya dapat mengelola kontrol dalam konteks zona pendaratan yang ada. Kontrol dapat disebut sebagai subresource.

Sumber daya dan subsumber daya di AWS memiliki Nama Sumber Daya Amazon (ARN) unik yang terkait dengannya, seperti yang ditunjukkan pada contoh berikut.

AWS Control Tower menyediakan serangkaian operasi API untuk bekerja dengan sumber daya AWS Control Tower. Untuk daftar operasi yang tersedia, lihat AWS Control Tower Refer ensi API Menara Kontrol AWS.

Untuk informasi selengkapnya tentang CloudFormation sumber daya di AWS Control Tower, lihat Panduan AWS CloudFormation Pengguna.

Tentang kepemilikan sumber daya

Akun AWS memiliki sumber daya yang dibuat di akun, terlepas dari siapa yang membuat sumber daya. Secara khusus, pemilik sumber daya adalah AWS akun entitas utama (yaitu, pengguna Akun AWS root, pengguna Pusat Identitas IAM, pengguna IAM, atau peran IAM) yang mengotentikasi permintaan pembuatan sumber daya. Contoh berikut menggambarkan cara kerjanya:

- Jika Anda menggunakan kredentif pengguna root AWS AWS akun untuk mengatur zona pendaratan, AWS akun Anda adalah pemilik sumber daya.
- Jika Anda membuat pengguna IAM di AWS akun Anda dan memberikan izin untuk mengatur zona pendaratan kepada pengguna tersebut, pengguna dapat mengatur zona pendaratan selama akun mereka memenuhi prasyarat. Namun, AWS akun Anda, tempat pengguna berada, memiliki sumber daya zona pendaratan.
- Jika Anda membuat peran IAM di AWS akun Anda dengan izin untuk mengatur zona pendaratan, siapa pun yang dapat mengambil peran tersebut dapat mengatur zona pendaratan. AWS Akun Anda, yang menjadi milik peran tersebut, memiliki sumber daya zona pendaratan.

Kelola akses ke sumber daya

Kebijakan izin menjelaskan siapa yang memiliki akses ke suatu objek. Bagian berikut menjelaskan opsi yang tersedia untuk membuat kebijakan izin.

> **Note**
>
> Bagian ini membahas penggunaan IAM dalam konteks AWS Control Tower. Bagian ini tidak memberikan informasi yang mendetail tentang layanan IAM. Untuk dokumentasi IAM lengkap, lihat Apa yang Dimaksud dengan IAM? dalam Panduan Pengguna IAM. Untuk informasi tentang sintaksis dan deskripsi kebijakan IAM, lihat Referensi Kebijakan IAM AWS dalam Panduan Pengguna IAM.

Kebijakan yang melekat pada identitas IAM disebut sebagai kebijakan berbasis identitas (kebijakan IAM). Kebijakan yang dilampirkan pada sumber daya disebut sebagai kebijakan berbasis-sumber daya.

> **Note**
>
> AWS Control Tower hanya mendukung kebijakan berbasis identitas (kebijakan IAM).

Topik

- Tentang kebijakan berbasis identitas (kebijakan IAM)
- Buat peran dan tetapkan izin
- Resource-based kebijakan

Tentang kebijakan berbasis identitas (kebijakan IAM)

Anda dapat melampirkan kebijakan ke identitas IAM Anda. Misalnya, Anda dapat melakukan hal berikut:

- Melampirkan kebijakan izin ke pengguna atau grup di akun Anda — Untuk memberikan izin kepada pengguna untuk membuat sumber daya AWS Control Tower, seperti menyiapkan zona pendaratan, Anda dapat melampirkan kebijakan izin ke pengguna atau grup tempat pengguna tersebut berada.

- Melampirkan kebijakan izin pada peran (memberikan izin lintas akun) – Anda dapat melampirkan kebijakan izin berbasis identitas ke peran IAM untuk memberikan izin lintas akun. Misalnya, administrator untuk satu AWS akun (Akun A) dapat membuat peran yang memberikan izin lintas akun ke AWS akun lain (Akun B), atau administrator dapat membuat peran yang memberikan izin ke AWS layanan lain.

  1. Administrator Akun A membuat peran IAM dan melampirkan kebijakan izin ke peran yang memberikan izin untuk mengelola sumber daya di Akun A.
  2. Administrator Akun A melampirkan kebijakan kepercayaan ke peran tersebut. Kebijakan ini mengidentifikasi Akun B sebagai kepala sekolah yang dapat mengambil peran tersebut.
  3. Sebagai prinsipal, administrator Akun B dapat memberikan izin kepada setiap pengguna di Akun B untuk mengambil peran tersebut. Dengan mengambil peran tersebut, pengguna di Akun B dapat membuat atau mendapatkan akses ke sumber daya di Akun A.
  4. Untuk memberikan AWS layanan kemampuan (izin) untuk mengambil peran, prinsipal yang Anda tentukan dalam kebijakan kepercayaan dapat berupa AWS layanan.

Buat peran dan tetapkan izin

Peran dan izin memberi Anda akses ke sumber daya, di AWS Control Tower, dan di AWS layanan lain, termasuk akses terprogram ke sumber daya.

Untuk memberikan akses dan menambahkan izin bagi pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

  Buat rangkaian izin. Ikuti instruksi di Buat rangkaian izin dalam Panduan Pengguna AWS IAM Identity Center .

- Pengguna yang dikelola di IAM melalui penyedia identitas:

  Buat peran untuk federasi identitas. Ikuti instruksi dalam Buat peran untuk penyedia identitas pihak ketiga (federasi) dalam Panduan Pengguna IAM.

- Pengguna IAM:
  - Buat peran yang dapat diambil pengguna Anda. Ikuti instruksi dalam Buat peran untuk pengguna IAM dalam Panduan Pengguna IAM.
  - (Tidak disarankan) Lampirkan kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti petunjuk dalam Menambahkan izin ke pengguna (konsol) dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang penggunaan IAM untuk mendelegasikan izin, lihat Manajemen Akses dalam Panduan Pengguna IAM.

> **Note**
>
> Saat menyiapkan zona pendaratan AWS Control Tower, Anda memerlukan pengguna atau peran dengan kebijakan ter AdministratorAccess kelola. (arn:aws:iam: :aws:) policy/ AdministratorAccess

Untuk membuat peran untuk Layanan AWS (Konsol IAM)

1. Masuk ke Konsol Manajemen AWS dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi konsol IAM, pilih Peran, dan lalu pilih Buat peran.
3. Untuk Ti pe entitas tepercaya, pilih Layanan AWS.
4. Untuk Layanan atau kasus penggunaan, pilih layanan, lalu pilih kasus penggunaan. Kasus penggunaan ditentukan oleh layanan untuk menyertakan kebijakan kepercayaan yang diperlukan layanan.
5. Pilih Berikutnya.
6. Untuk kebijakan Iz in, opsi tergantung pada kasus penggunaan yang Anda pilih:
   - Jika layanan menentukan izin untuk peran, Anda tidak dapat memilih kebijakan izin.
   - Pilih dari kumpulan kebijakan izin terbatas.
   - Pilih dari semua kebijakan izin.
   - Pilih kebijakan tanpa izin, buat kebijakan setelah peran dibuat, lalu lampirkan kebijakan ke peran tersebut.
7. (Opsional) Tetapkan batas izin. Ini adalah fitur lanjutan yang tersedia untuk peran layanan, tetapi bukan peran tertaut layanan.
   a. Buka bagian Tetapkan batas izin, lalu pilih Gunakan batas izin untuk mengontrol izin peran maksimum.

      IAM menyertakan daftar kebijakan yang AWS dikelola dan dikelola pelanggan di akun Anda.
   b. Pilih kebijakan yang akan digunakan untuk batas izin.
8. Pilih Berikutnya.

9. Untuk nama Per an, opsi tergantung pada layanan:

   - Jika layanan mendefinisikan nama peran, Anda tidak dapat mengedit nama peran.
   - Jika layanan mendefinisikan awalan untuk nama peran, Anda dapat memasukkan akhiran opsional.
   - Jika layanan tidak menentukan nama peran, Anda dapat memberi nama peran tersebut.

   > **Important**
   >
   > Saat Anda memberi nama peran, perhatikan hal berikut:
   >
   > - Nama peran harus unik dalam nama Anda Akun AWS, dan tidak dapat dibuat unik berdasarkan kasus.
   >
   >   Misalnya, jangan membuat peran bernama keduanya **`PRODROLE`** dan**`prodrole`**. Ketika nama peran digunakan dalam kebijakan atau sebagai bagian dari ARN, nama peran tersebut peka huruf besar/kecil, namun ketika nama peran muncul kepada pelanggan di konsol, seperti selama proses masuk, nama peran tidak peka huruf besar/kecil.
   > - Anda tidak dapat mengedit nama peran setelah dibuat karena entitas lain mungkin mereferensikan peran tersebut.

10. (Opsional) Untuk Deskripsi, masukkan deskripsi untuk peran.
11. (Opsional) Untuk mengedit kasus penggunaan dan izin untuk peran, di bagian Langkah 1: Pilih entitas tepercaya atau Langkah 2: Tambahkan izin, pilih Edit.
12. (Opsional) Untuk membantu mengidentifikasi, mengatur, atau mencari peran, tambahkan tag sebagai pasangan kunci-nilai. Untuk informasi selengkapnya tentang menggunakan tag di IAM, lihat Tag untuk AWS Identity and Access Management sumber daya di Panduan Pengguna IAM.
13. Tinjau peran lalu pilih Buat peran.

Cara menggunakan editor kebijakan JSON untuk membuat kebijakan

1. Masuk ke Konsol Manajemen AWS dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Pada panel navigasi di sebelah kiri, pilih Kebijakan.

Jika ini pertama kalinya Anda memilih Kebijakan, akan muncul halaman Selamat Datang di Kebijakan Terkelola. Pilih Memulai.

3. Di bagian atas halaman, pilih Buat kebijakan.
4. Di bagian Editor kebijakan, pilih opsi JSON.
5. Masukkan atau tempel dokumen kebijakan JSON. Untuk detail bahasa kebijakan IAM, lihat Referensi kebijakan JSON IAM.
6. Selesaikan peringatan keamanan, kesalahan, atau peringatan umum yang dihasilkan selama validasi kebijakan, lalu pilih Berikutnya.

> **Note**
>
> Anda dapat beralih antara opsi editor Visual dan JSON kapan saja. Namun, jika Anda melakukan perubahan atau memilih Berikutnya di editor Visual, IAM dapat merestrukturisasi kebijakan Anda untuk mengoptimalkannya bagi editor visual. Untuk informasi selengkapnya, lihat Restrukturisasi kebijakan dalam Panduan Pengguna IAM.

7. (Opsional) Saat Anda membuat atau mengedit kebijakan di Konsol Manajemen AWS, Anda dapat membuat template kebijakan JSON atau YAML yang dapat Anda gunakan dalam CloudFormation templat.

   Untuk melakukan ini, di editor Kebijakan pilih Tind akan, lalu pilih H asilkan CloudFormation template. Untuk mempelajari selengkap CloudFormation nya, lihat referensi jenis AWS Identity and Access Management sumber daya di Panduan AWS CloudFormation Pengguna.
8. Setelah selesai menambahkan izin ke kebijakan, pilih Berikutnya.
9. Pada halaman Tinjau dan buat, masukkan Nama kebijakan dan Deskripsi (opsional) untuk kebijakan yang Anda buat. Tinjau Izin yang ditentukan dalam kebijakan ini untuk melihat izin yang diberikan oleh kebijakan Anda.
10. (Opsional) Tambahkan metadata ke kebijakan dengan melampirkan tanda sebagai pasangan nilai kunci. Untuk informasi selengkapnya tentang menggunakan tag di IAM, lihat Tag untuk AWS Identity and Access Management sumber daya di Panduan Pengguna IAM.
11. Pilih Buat kebijakan untuk menyimpan kebijakan baru Anda.

Untuk menggunakan editor visual dalam pembuatan kebijakan

1. Masuk ke Konsol Manajemen AWS dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Pada panel navigasi di sebelah kiri, pilih Kebijakan.

   Jika ini pertama kalinya Anda memilih Kebijakan, akan muncul halaman Selamat Datang di Kebijakan Terkelola. Pilih Memulai.
3. Pilih Buat kebijakan.
4. Di bagian Editor kebijakan, cari bagian Pilih layanan, lalu pilih Layanan AWS. Anda bisa menggunakan kotak pencarian di bagian atas untuk membatasi hasil pada daftar layanan. Anda bisa memilih hanya satu layanan pada blok izin editor visual. Untuk memberikan akses ke lebih dari satu layanan, tambahkan beberapa blok izin dengan memilih Tambahkan izin lainnya.
5. Di Tind akan diizinkan, pilih tindakan yang akan ditambahkan ke kebijakan. Anda bisa memilih tindakan dengan cara berikut:

   - Pilih kotak centang untuk semua tindakan.
   - Pilih Tambah tindakan untuk memasukkan nama tindakan tertentu. Anda dapat menggunakan karakter wildcard (*) untuk menentukan beberapa tindakan.
   - Pilih satu grup Tingkat akses untuk memilih semua tindakan untuk tingkat akses tersebut (misalnya, Baca, Tulis, atau Daftar).
   - Perluas setiap grup Tingkat akses untuk memilih tindakan individu.

   Secara default, kebijakan yang Anda buat mengizinkan tindakan yang Anda pilih. Sebaliknya, untuk menolak tindakan terpilih, pilih Beralih ke menolak izin. Karena IAM menolak secara default, kami merekomendasikan sebagai praktik terbaik keamanan agar Anda mengizinkan hanya tindakan dan sumber daya yang diperlukan pengguna saja. Buat pernyataan JSON untuk menolak izin hanya jika Anda ingin mengganti izin yang diizinkan secara terpisah oleh pernyataan atau kebijakan lain. Kami sarankan Anda membatasi jumlah izin penolakan seminim mungkin karena dapat meningkatkan kesulitan izin pemecahan masalah.
6. Untuk Sumber Daya, bila layanan dan tindakan yang Anda pilih di langkah sebelumnya tidak mendukung pilihan sumber daya tertentu, semua sumber daya diperbolehkan dan Anda tidak bisa mengedit bagian ini.

Jika Anda memilih satu atau lebih tindakan yang mendukungizin tingkat sumber daya, maka editor visual akan mendaftar sumber daya tersebut. Kemudian Anda bisa memperluas Sumber Daya untuk menentukan sumber daya bagi kebijakan Anda.

Anda dapat menentukan sumber daya dengan cara berikut:

- Pilih Tambahkan ARN untuk menentukan sumber daya berdasarkan Nama Sumber Daya Amazon (ARN) mereka. Anda dapat menggunakan editor ARN visual atau mendaftar ARN secara manual. Untuk informasi selengkapnya tentang sintaks ARN, lihat Nama Sumber Daya Amazon (ARN) di Panduan Pengguna IAM. Untuk informasi tentang menggunakan ARN dalam `Resource` elemen kebijakan, lihat Elemen kebijakan JSON IAM: Sumber daya di Panduan Pengguna IAM.
- Pilih Apa saja di akun ini di sebelah sumber daya untuk memberikan izin ke sumber daya apa pun dari jenis itu.
- Pilih Semua untuk memilih semua sumber daya untuk layanan.

7. (Opsional) Pilih Permintaan kondisi - opsional untuk menambahkan kondisi ke kebijakan yang Anda buat. Kondisi membatasi efek dari pernyataan kebijakan JSON. Misalnya, Anda dapat menentukan bahwa pengguna diizinkan melakukan tindakan pada sumber daya hanya ketika permintaan pengguna tersebut terjadi di rentang waktu tertentu. Anda juga dapat menggunakan kondisi yang umum digunakan untuk membatasi apakah pengguna harus diautentikasi dengan menggunakan perangkat otentikasi multi-faktor (MFA). Atau Anda bisa meminta agar permintaan yang berasal dari rentang alamat IP tertentu. Untuk daftar semua kunci konteks yang dapat Anda gunakan dalam kondisi kebijakan, lihat Tindakan, sumber daya, dan kunci kondisi untuk AWS layanan di Referensi O torisasi Layanan.

   Anda bisa memilih kondisi dengan cara berikut:

   - Gunakan kotak centang untuk memilih kondisi yang biasa dipakai.
   - Pilih Tambahkan kondisi lain untuk menentukan kondisi lain. Pilih Kunci Kondisi, Ku alifikasi, dan Operator kondisi, lalu masukkan Nilai. Untuk menambahkan lebih dari satu nilai, pilih Tam bah. Anda dapat mempertimbangkan nilai-nilai yang dihubungkan oleh `OR` operator logis. Setelah selesai, pilih Tambahkan kondisi.

   Untuk menambahkan lebih dari satu kondisi, pilih Tam bah kondisi lain lagi. Ulangi seperlunya. Setiap kondisi berlaku hanya untuk blok izin editor visual yang satu ini. Semua kondisi haruslah

benar agar blok izin dapat dianggap cocok. Dengan kata lain, pertimbangkan kondisi yang akan dihubungkan oleh AND operator logis.

Untuk informasi selengkapnya tentang elemen Kondisi, lihat Elemen kebijakan IAM JSON: Kondisi di Panduan Pengguna IAM.

8. Untuk menambahkan lebih banyak blok izin, pilih Tambahkan izin lainnya. Untuk setiap blok, ulangi langkah 2 sampai 5.

> **Note**
>
> Anda dapat beralih antara opsi editor Visual dan JSON kapan saja. Namun, jika Anda melakukan perubahan atau memilih Berikutnya di editor Visual, IAM dapat merestrukturisasi kebijakan Anda untuk mengoptimalkannya bagi editor visual. Untuk informasi selengkapnya, lihat Restrukturisasi kebijakan dalam Panduan Pengguna IAM.

9. (Opsional) Saat Anda membuat atau mengedit kebijakan di Konsol Manajemen AWS, Anda dapat membuat template kebijakan JSON atau YAML yang dapat Anda gunakan dalam CloudFormation template.

   Untuk melakukan ini, di editor Kebijakan pilih Tind akan, lalu pilih H asilkan CloudFormation template. Untuk mempelajari selengkap CloudFormation nya, lihat referensi jenis AWS Identity and Access Management sumber daya di Panduan AWS CloudFormation Pengguna.

10. Setelah selesai menambahkan izin ke kebijakan, pilih Berikutnya.
11. Pada halaman Tinjau dan buat, masukkan Nama kebijakan dan Deskripsi (opsional) untuk kebijakan yang Anda buat. Tinjau Izin yang ditentukan dalam kebijakan ini untuk memastikan bahwa Anda telah memberikan izin yang diinginkan.
12. (Opsional) Tambahkan metadata ke kebijakan dengan melampirkan tanda sebagai pasangan nilai kunci. Untuk informasi selengkapnya tentang menggunakan tag di IAM, lihat Tag untuk AWS Identity and Access Management sumber daya di Panduan Pengguna IAM.
13. Pilih Buat kebijakan untuk menyimpan kebijakan baru Anda.

Untuk memberikan akses terprogram

Pengguna memerlukan akses terprogram jika mereka ingin berinteraksi dengan AWS di luar. Konsol Manajemen AWS Cara untuk memberikan akses terprogram tergantung pada jenis pengguna yang mengakses AWS.

Untuk memberi pengguna akses programatis, pilih salah satu opsi berikut.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
IAM	(Disarankan) Gunakan kredenSIAL konsol sebagai kredenSIAL sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau AWS API.	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk AWS CLI, lihat Login untuk pengembangan AWS lokal di Panduan AWS Command Line Interface Pengguna. • Untuk AWS SDK, lihat Login untuk pengembangan AWS lokal di Panduan Refer AWS ensi SDK dan Alat.
Identitas tenaga kerja (Pengguna yang dikelola di Pusat Identitas IAM)	Gunakan kredenSIAL sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau AWS API.	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk AWS CLI, lihat Meng onfigurasi AWS CLI untuk digunakan AWS IAM Identity Center di Panduan AWS Command Line Interface Pengguna. • Untuk AWS SDK, alat, dan AWS API, lihat otentikasi Pusat Identitas IAM di Panduan Refer AWS ensi SDK dan Alat.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
IAM	Gunakan kredenSIAL sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau AWS API.	Mengikuti petunjuk dalam Menggunakan kredenSIAL sementara dengan AWS sumber daya di Panduan Pengguna IAM.
IAM	(Tidak direkomendasikan) Gunakan kredentif jangka panjang untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau AWS API.	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk itu AWS CLI, lihat Meng autentikasi menggunakan kredentif pengguna IAM di Panduan AWS Command Line Interface Pengguna. • Untuk AWS SDK dan alat, lihat Meng autentikasi menggunakan kredentif jangka panjang di Panduan Refer AWS ensi SDK dan Alat. • Untuk AWS API, lihat M engelola kunci akses untuk pengguna IAM di Panduan Pengguna IAM.

Melindungi dari penyerang

Untuk informasi selengkapnya tentang cara membantu melindungi dari penyerang saat Anda memberikan izin kepada prinsi AWS pal layanan lainnya, lihat Kondisi opsional untuk hubungan kepercayaan peran Anda. Dengan menambahkan kondisi tertentu ke kebijakan Anda, Anda dapat

membantu mencegah jenis serangan tertentu, yang dikenal sebagai serangan wakil yang membing ungkan, yang terjadi jika entitas memaksa entitas yang lebih istimewa untuk melakukan tindakan, seperti dengan peniruan lintas layanan. Untuk informasi umum tentang kondisi kebijakan, lihat jugaMenentukan kondisi dalam kebijakan.

Untuk informasi selengkapnya tentang menggunakan kebijakan berbasis identitas dengan AWS Control Tower, lihat. Menggunakan kebijakan berbasis identitas (kebijakan IAM) untuk AWS Control Tower Untuk informasi lebih lanjut tentang pengguna, grup, peran, dan izin, lihat Identitas (Pengguna, Grup, dan Peran) dalam Panduan Pengguna IAM.

Resource-based kebijakan

Layanan lain, seperti Amazon S3, juga mendukung kebijakan izin berbasis sumber daya. Misalnya, Anda dapat melampirkan kebijakan ke bucket S3 untuk mengelola izin akses ke bucket tersebut. AWS Control Tower tidak mendukung kebijakan berbasis sumber daya.

Tentukan elemen kebijakan: Tindakan, Efek, dan Prinsip

Anda dapat mengatur dan mengelola zona pendaratan melalui konsol AWS Control Tower, atau API zona pendaratan. Untuk mengatur zona pendaratan, Anda harus menjadi pengguna IAM dengan izin administratif seperti yang didefinisikan dalam kebijakan IAM.

Elemen-elemen berikut adalah yang paling mendasar yang dapat Anda identifikasi dalam kebijakan:

- Sumber daya – Dalam kebijakan, Anda menggunakan Amazon Resource Name (ARN) untuk mengidentifikasi sumber daya yang diatur kebijakan. Untuk informasi selengkapnya, lihat Sumber daya dan operasi AWS Control Tower.
- Tindakan – Anda menggunakan kata kunci tindakan untuk mengidentifikasi operasi sumber daya yang ingin Anda izinkan atau tolak. Untuk informasi tentang jenis tindakan yang tersedia untuk dilakukan, lihat Tind akan yang ditentukan oleh AWS Control Tower.
- Efek – Anda menentukan efek ketika pengguna meminta tindakan tertentu—efek ini dapat berupa pemberian izin atau penolakan. Jika Anda tidak secara eksplisit memberikan akses ke (mengizinkan) sumber daya, akses akan ditolak secara implisit. Anda juga dapat secara eksplisit menolak akses ke sumber daya, yang mungkin Anda lakukan untuk memastikan bahwa pengguna tidak dapat mengaksesnya, meskipun ada akses memberikan kebijakan yang berbeda.
- Prinsi p — Dalam kebijakan berbasis identitas (kebijakan IAM), pengguna yang dilampirkan kebijakan tersebut adalah prinsip implisit. Untuk kebijakan berbasis sumber daya, Anda menentukan pengguna, akun, layanan, atau entitas lain yang diinginkan untuk menerima izin

(berlaku hanya untuk kebijakan berbasis sumber daya). AWS Control Tower tidak mendukung kebijakan berbasis sumber daya.

Untuk mempelajari selengkapnya tentang sintaksis dan deskripsi kebijakan IAM, lihat Referensi Kebijakan IAM AWS dalam Panduan Pengguna IAM.

Menentukan kondisi dalam kebijakan

Ketika Anda memberikan izin, Anda dapat menggunakan bahasa kebijakan IAM untuk menentukan kondisi ketika kebijakan harus berlaku. Misalnya, Anda mungkin ingin kebijakan diterapkan hanya setelah tanggal tertentu. Untuk informasi selengkapnya tentang menentukan kondisi dalam bahasa kebijakan, lihat Kondisi dalam Panduan Pengguna IAM.

Untuk mengekspresikan kondisi, Anda dapat menggunakan kunci kondisi yang telah ditentukan sebelumnya. Tidak ada kunci kondisi khusus untuk AWS Control Tower. Namun, ada kunci AWS kondisi lebar yang dapat Anda gunakan sebagaimana mestinya. Untuk daftar lengkap kunci AWS-wide, lihat Kunci Ter sedia untuk Kondisi di Panduan Pengguna IAM.

Mencegah peniruan lintas layanan

Pada tahun AWS, peniruan lintas layanan dapat mengakibatkan masalah wakil yang membing ungkan. Ketika satu layanan memanggil layanan lain, peniruan lintas layanan terjadi jika satu layanan memanipulasi layanan lain untuk menggunakan izinnya untuk bertindak atas sumber daya pelanggan dengan cara yang tidak diizinkan. Untuk mencegah serangan ini, AWS menyediakan alat untuk membantu Anda melindungi data Anda, sehingga hanya layanan dengan izin sah yang dapat memperoleh akses ke sumber daya di akun Anda.

Sebaiknya gunakan `aws:SourceArn` dan `aws:SourceAccount` ketentuan dalam kebijakan Anda, untuk membatasi izin yang diberikan AWS Control Tower ke layanan lain untuk akses ke sumber daya Anda.

- Gunakan `aws:SourceArn` jika Anda ingin hanya satu sumber daya yang dikaitkan dengan akses lintas layanan.
- Gunakan `aws:SourceAccount` jika Anda ingin mengizinkan sumber daya apa pun di akun tersebut dikaitkan dengan penggunaan lintas layanan.
- Jika `aws:SourceArn` nilai tidak berisi ID akun, seperti ARN untuk bucket Amazon S3, Anda harus menggunakan kedua kondisi tersebut untuk membatasi izin.

- Jika Anda menggunakan kedua kondisi tersebut, dan jika nilainya berisi ID akun, `aws:SourceAccount` nilai dan akun dalam `aws:SourceArn` nilai harus menampilkan ID akun yang sama saat digunakan dalam pernyataan kebijakan yang sama `aws:SourceArn`

Untuk informasi selengkapnya dan contoh tambahan, lihat https://docs.aws.amazon.com/controltower/latest/userguide/conditions-for-role-trust.html.

Menggunakan kebijakan berbasis identitas (kebijakan IAM) untuk AWS Control Tower

Topik ini memberikan contoh kebijakan berbasis identitas yang menunjukkan bagaimana administrator akun dapat melampirkan kebijakan izin ke identitas IAM (yaitu pengguna, grup, dan peran) dan dengan demikian memberikan izin untuk melakukan operasi pada sumber daya AWS Control Tower.

> **Important**
>
> Kami menyarankan Anda terlebih dahulu meninjau topik pengantar yang menjelaskan konsep dasar dan opsi yang tersedia bagi Anda untuk mengelola akses ke sumber daya AWS Control Tower Anda. Untuk informasi selengkapnya, lihat Ikhtisar pengelolaan izin akses ke sumber daya AWS Control Tower.

Izin Diperlukan untuk menggunakan konsol AWS Control Tower

AWS Control Tower membuat tiga peran secara otomatis saat Anda menyiapkan zona pendaratan. Ketiga peran diperlukan untuk mengizinkan akses konsol. AWS Control Tower membagi izin menjadi tiga peran sebagai praktik terbaik untuk membatasi akses ke kumpulan tindakan dan sumber daya minimal.

Tiga peran yang diperlukan untuk akses zona pendaratan

- AWS ControlTowerAdmin peran
- AWS ControlTowerStackSetRole
- AWSControlTowerCloudTrailRole

Sebaiknya batasi akses ke kebijakan kepercayaan peran Anda untuk peran ini. Untuk informasi selengkapnya, lihat Kondisi opsional untuk hubungan kepercayaan peran Anda.

Lihat Katalog Kontrol di konsol

Untuk melihat informasi kontrol di konsol AWS Control Tower, Anda harus menambahkan `controlcatalog` izin tambahan ke kebijakan IAM Anda. Izin ini adalah sebagai berikut:

- `controlcatalog:GetControl`
- `controlcatalog:ListControls`
- `controlcatalog:ListControlMappings`
- `controlcatalog:ListCommonControls`

Berikut adalah contoh yang menunjukkan izin yang diperbarui dalam kebijakan.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "controlcatalog:GetControl",
                "controlcatalog:ListControls",
                "controlcatalog:ListControlMappings",
                "controlcatalog:ListCommonControls"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Anda harus menambahkan izin ini karena AWS Control Tower memang `controlcatalog` gil API untuk mengambil metadata kontrol tertentu, sehingga izin AWS Control Tower tidak cukup.

Untuk menemukan informasi selengkapnya tentang cara memperbarui izin Anda, lihat Membuat peran dan menetapkan izin.

Untuk menemukan informasi selengkapnya tentang tindakan `controlcatalog` IAM, lihat T indakan, sumber daya, dan kunci kondisi untuk Katalog Kontrol.

> **Note**
>
> Informasi kontrol tersedia melalui API Katalog Kontrol.

AWS ControlTowerAdmin peran

Peran ini menyediakan AWS Control Tower dengan akses ke infrastruktur penting untuk mempertahankan zona pendaratan. `AWS ControlTowerAdmin`Peran tersebut memerlukan kebijakan terkelola terlampir dan kebijakan kepercayaan peran untuk peran IAM. Kebijakan kepercayaan peran adalah kebijakan berbasis sumber daya, menentukan prinsipal mana yang dapat mengambil peran tersebut.

Berikut cuplikan contoh untuk kebijakan kepercayaan peran ini:

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "controltower.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Untuk membuat peran ini dari AWS CLI, dan memasukkannya ke dalam file yang disebut`trust.json`, berikut adalah contoh perintah CLI:

```
aws iam create-role --role-name AWSControlTowerAdmin --path /service-role/ --assume-
role-policy-document file://trust.json
```

Peran ini membutuhkan dua kebijakan IAM.

1. Kebijakan sebaris, misalnya:

   JSON

   ```
   {
       "Version":"2012-10-17",
       "Statement": [
           {
               "Effect": "Allow",
               "Action": "ec2:DescribeAvailabilityZones",
               "Resource": "*"
           }
       ]
   }
   ```

2. Kebijakan terkelola berikut, yaitu`AWS ControlTowerServiceRolePolicy`.

AWS ControlTowerServiceRolePolicy

Ini AWS ControlTowerServiceRolePolicy adalah kebijakan AWS yang dikelola yang mendefinisikan izin untuk membuat dan mengelola sumber daya AWS Control Tower, seperti AWS CloudFormation stackset dan instans tumpukan, file AWS CloudTrail log, agregator konfigurasi untuk AWS Control Tower, serta AWS Organizations akun dan unit organisasi (OU) yang diatur oleh AWS Control Tower.

Pembaruan untuk kebijakan terkelola ini dirangkum dalam tabel,Kebijakan terkelola untuk Menara Kontrol AWS.

Untuk informasi selengkapnya, lihat AWS ControlTowerServiceRolePolicy Panduan Refer AWS ensi Kebijakan Terkelola.

Kebijakan kepercayaan peran:

JSON

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

```
    "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
         ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Kebijakan sebaris adalah`AWS ControlTowerAdminPolicy`:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

AWS ControlTowerIdentityCenterManagementPolicy

Kebijakan ini memberikan izin untuk mengonfigurasi sumber daya Pusat Identitas IAM (iDC) di akun anggota yang terdaftar dengan AWS Control Tower. Saat Anda memilih Pusat Identitas IAM sebagai penyedia identitas Anda selama penyiapan (atau pembaruan) zona pendaratan di AWS Control Tower, kebijakan ini dilampirkan ke `AWS ControlTowerAdmin` peran tersebut.

Untuk melihat detail selengkapnya tentang kebijakan, termasuk versi terbaru dari dokumen kebijakan JSON, lihat AWS ControlTowerIdentityCenterManagementPolicy di Panduan Referensi AWS Kebijakan Terkelola.

AWS ControlTowerStackSetRole

CloudFormation mengambil peran ini untuk menerapkan kumpulan tumpukan di akun yang dibuat oleh AWS Control Tower. Kebijakan sebaris:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Kebijakan kepercayaan

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudformation.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWS ControlTowerCloudTrailRolePolicy

AWS Control Tower memungkinkan CloudTrail sebagai praktik terbaik dan memberikan peran ini kepada CloudTrail. CloudTrail mengambil peran ini untuk membuat dan menerbitkan CloudTrail log.

Kebijakan Terkelola: `AWS ControlTowerCloudTrailRolePolicy`

Peran ini menggunakan kebijakan AWS-managed`AWS ControlTowerCloudTrailRolePolicy`, yang memberikan izin CloudTrail yang diperlukan untuk menerbitkan log audit ke Amazon Log CloudWatch s atas nama AWS Control Tower. Kebijakan terkelola ini menggantikan kebijakan sebaris yang sebelumnya digunakan untuk peran ini, memungkinkan AWS untuk memperbarui kebijakan tanpa campur tangan pelanggan.

Untuk informasi selengkapnya, lihat AWS ControlTowerCloudTrailRolePolicy Panduan Refer AWS ensi Kebijakan Terkelola.

Pembaruan untuk kebijakan terkelola ini dirangkum dalam tabel,Kebijakan terkelola untuk Menara Kontrol AWS.

> **Note**
>
> Sebelum pengenalan kebijakan terkelola, peran ini menggunakan kebijakan sebaris dengan izin yang setara. Kebijakan sebaris telah diganti dengan kebijakan terkelola untuk mengaktifkan pembaruan tanpa batas.

Kebijakan Inline sebelumnya (untuk referensi):

JSON

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

Kebijakan kepercayaan

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWS ControlTowerBlueprintAccess persyaratan peran

AWS Control Tower mengharuskan Anda membuat `AWS ControlTowerBlueprintAccess` peran di akun hub cetak biru yang ditunjuk, dalam organisasi yang sama.

Nama peran

Nama peran harus `AWS ControlTowerBlueprintAccess`

Kebijakan kepercayaan peran

Peran harus diatur untuk mempercayai prinsip-prinsip berikut:

- Prinsipal yang menggunakan AWS Control Tower di akun manajemen.
- `AWS ControlTowerAdmin`Peran dalam akun manajemen.

Contoh berikut menunjukkan kebijakan kepercayaan hak istimewa terkecil. Saat membuat kebijakan sendiri, ganti istilah tersebut *YourManagementAccountId* dengan ID akun aktual akun manajemen AWS Control Tower Anda, dan ganti istilah tersebut *YourControlTowerUserRole* dengan pengidentifikasi peran IAM untuk akun manajemen Anda.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/service-role/
AWSControlTowerAdmin",
                    "arn:aws:iam::111122223333:role/YourControlTowerUserRole"
                ]
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

Izin peran

Anda diharuskan melampirkan kebijakan terkelola AWSServiceCatalogAdminFullAccess ke peran tersebut.

AWSServiceRoleForAWSControlTower

Peran ini memberi AWS Control Tower akses ke akun Log Archive, akun Audit, dan akun anggota, untuk operasi yang penting untuk mempertahankan zona pendaratan, seperti memberi tahu Anda tentang sumber daya yang hanyut.

`AWS ServiceRoleFor AWS ControlTower`Peran tersebut memerlukan kebijakan terkelola terlampir dan kebijakan kepercayaan peran untuk peran IAM.

Kebijakan terkelola untuk peran ini: `AWS ControlTowerAccountServiceRolePolicy`

Kebijakan kepercayaan peran:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "controltower.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWS ControlTowerAccountServiceRolePolicy

Kebijakan yang AWS dikelola ini memungkinkan AWS Control Tower untuk memanggil AWS layanan yang menyediakan konfigurasi akun otomatis dan tata kelola terpusat atas nama Anda.

Kebijakan ini berisi izin minimum bagi AWS Control Tower untuk menerapkan penerusan AWS Security Hub CSPM temuan untuk sumber daya yang dikelola oleh kontrol CSPM Hub Keamanan yang merupakan bagian dari Service-managed Standar CSPM Hub Keamanan: Menara Kontrol AWS, dan kebijakan ini mencegah perubahan yang membatasi kemampuan mengelola akun pelanggan. Ini adalah bagian dari proses deteksi AWS Security Hub CSPM penyimpangan latar belakang yang tidak langsung diprakarsai oleh pelanggan.

Kebijakan ini memberikan izin untuk membuat EventBridge aturan Amazon, khusus untuk kontrol CSPM Security Hub, di setiap akun anggota, dan aturan ini harus menentukan yang tepat. EventPattern Juga, aturan hanya dapat beroperasi pada aturan yang dikelola oleh prinsipal layanan kami.

Layanan utama: `controltower.amazonaws.com`

Untuk informasi selengkapnya, lihat AWS ControlTowerAccountServiceRolePolicy Panduan Refer AWS ensi Kebijakan Terkelola.

Pembaruan untuk kebijakan terkelola ini dirangkum dalam tabel,Kebijakan terkelola untuk Menara Kontrol AWS.

Kebijakan terkelola untuk Menara Kontrol AWS

AWS mengatasi banyak kasus penggunaan umum dengan menyediakan kebijakan IAM mandiri yang dibuat dan dikelola oleh AWS. Kebijakan terkelola memberikan izin yang diperlukan untuk kasus penggunaan umum sehingga Anda tidak perlu menyelidiki izin apa yang diperlukan. Untuk informasi selengkapnya, lihat Kebijakan Terkelola AWS dalam Panduan Pengguna IAM.

Ubah	Deskripsi	Tanggal
AWS ControlTowerServiceRolePolicy — Permbaruan ke kebijakan yang sudah ada	AWS Control Tower memindahkan `cloudformation:BatchDescribeTypeConfigurations` izin dari pernyataan hook bercakupan sumber daya ke pernyataan baru dengan`Resource: "*"`, karena CloudFormation tidak mendukung izin tingkat sumber daya untuk API ini.	Mei 19, 2026
AWS ControlTowerAccountServiceRolePolicy – Pembaruan ke kebijakan yang ada	AWS Control Tower menambahkan izin baru yang memungkinkan AWS Control Tower melakukan panggilan ke API AWS CloudFormation layanan `BatchDescribeTypeConfigurations` untuk peningkatan internal pada kait terkait layanan.	Mei 19, 2026
AWS ControlTowerAccountServiceRolePolicy –	AWS Control Tower memperbarui kebijakan yang ada untuk meningkatkan	Desember 30, 2025

Ubah	Deskripsi	Tanggal
Pembaruan ke kebijakan yang ada	presisi validasi untuk kondisi EventBridge aturan Amazon. Pembaruan memindahkan `events:detail-type` kondisi dari `StringEqu als` ke `ForAllVal ues:StringEquals` untuk kontrol pencocokan pola peristiwa yang lebih baik sambil mempertahankan izin fungsional yang sama.	
AWS ControlTowerAccoun tServiceRolePolicy – Pembaruan ke kebijakan yang ada	AWS Control Tower menambahkan kebijakan baru yang memperluas izin berikut: • AWS Config izin untuk membuat, menandai, menghapus, mengelola, dan membaca agregator konfigurasi terkait layanan • AWS Config izin untuk menjelaskan semua agregator konfigurasi • AWS Organizations izin untuk daftar administrator yang didelegasikan untuk AWS Config • AWS Organizations izin untuk mendeskripsikan organisasi • CloudFormation izin untuk mengelola kait yang ditautkan layanan	November 10, 2025

Ubah	Deskripsi	Tanggal
AWS ControlTowerServiceRolePolicy— Kebijakan terkelola yang diperbarui	AWS Control Tower memperbarui pola sumber daya Amazon CloudWatch Logs AWS ControlTowerServiceRolePolicy untuk mendukung AWS CloudTrail integrasi opsional Landing Zone 4.0. Pola berubah dari `aws-controltower/CloudTrailLogs:*` menjadi `aws-controltower/CloudTrailLogs*:*` , menambahkan karakter wildcard setelahnya a `CloudTrailLogs` untuk memungkinkan pengelolaan grup log dengan akhiran apa pun. Pembaruan ini memungkinkan AWS CloudTrail integrasi opsional Landing Zone 4.0, yang memungkinkan pelanggan mengaktifkan dan menonaktifkan AWS CloudTrail integrasi beberapa kali. Setiap kali integrasi diaktifkan, grup CloudWatch log Amazon Logs dibuat ulang dengan sufiks unik untuk menghindari konflik penamaan. Pembaruan kompatibel ke belakang dengan penerapan yang ada.	Oktober 31, 2025

Ubah	Deskripsi	Tanggal
AWS ControlTowerCloudTrailRolePolicy— Kebijakan terkelola baru	AWS Control Tower memperkenalkan kebijakan ter AWS ControlTowerCloudTrailRolePolicy kelola, yang memungkinkan CloudTrail untuk membuat aliran log dan menerbitkan peristiwa log ke grup CloudWatch log Kontrol Tower-managed Amazon Logs. Kebijakan terkelola ini menggantikan kebijakan sebaris yang sebelumny a digunakan oleh AWS ControlTowerCloudTrailRole, memungkinkan AWS untuk memperbarui kebijakan tanpa campur tangan pelanggan. Kebijakan ini dicakup untuk mencatat grup dengan nama yang cocok dengan pola`aws-controltower/CloudTrailLogs*` .	Oktober 31, 2025

Ubah	Deskripsi	Tanggal
AWS ControlTowerIdentityCenterManagementPolicy—Kebijakan baru	AWS Control Tower menambahkan kebijakan baru yang memungkinkan pelanggan mengonfigurasi sumber daya Pusat Identitas IAM di akun yang terdaftar di AWS Control Tower, dan memungkinkan AWS Control Tower untuk memperbaiki beberapa jenis penyimpangan saat mendaftar akun secara otomatis. Perubahan ini diperlukan agar pelanggan dapat mengonfigurasi Pusat Identitas IAM di AWS Control Tower, dan agar AWS Control Tower dapat memperbaiki penyimpangan pendaftaran otomatis.	Oktober 10, 2025
AWS ControlTowerServiceRolePolicy – Pembaruan ke kebijakan yang ada	AWS Control Tower menambahkan CloudFormation izin baru yang memungkinkan AWS Control Tower untuk menanyakan dan menyebarkan sumber daya kumpulan tumpukan ke akun anggota saat mendaftarkan akun secara otomatis ke AWS Control Tower.	Oktober 10, 2025

Ubah	Deskripsi	Tanggal
AWS ControlTowerServiceRolePolicy – Pembaruan ke kebijakan yang ada	AWS Control Tower menambahkan izin baru yang memungkinkan pelanggan mengaktifkan dan menonaktifkan aturan terkait layanan AWS Config . Perubahan ini diperlukan agar pelanggan dapat mengelola kontrol yang diterapkan oleh aturan Config.	5 Juni 2025
AWS ControlTowerServiceRolePolicy – Pembaruan ke kebijakan yang ada	AWS Control Tower menambahkan izin baru yang memungkinkan AWS Control Tower melakukan panggilan ke API AWS CloudFormation layanan`ActivateType` ,`DeactivateType` , dan`SetTypeConfiguration` , aktif`AWS::ControlTower types` . Perubahan ini memungkinkan pelanggan untuk menyediakan kontrol proaktif tanpa penyebaran tipe CloudFormation Hook pribadi.	Desember 10, 2024

Ubah	Deskripsi	Tanggal
AWS ControlTowerAccountServiceRolePolicy— Kebijakan baru	AWS Control Tower menambahkan peran terkait layanan baru yang memungkinkan AWS Control Tower membuat dan mengelola aturan acara, dan berdasarkan aturan tersebut, untuk mengelola deteksi penyimpangan untuk kontrol yang terkait dengan Security Hub CSPM. Perubahan ini diperlukan agar pelanggan dapat melihat sumber daya yang hanyut di konsol, ketika sumber daya tersebut terkait dengan kontrol CSPM Hub Keamanan yang merupakan bagian dari Security Hub CSPM Service-managed Standard: AWS Control Tower.	22 Mei 2023

Ubah	Deskripsi	Tanggal
AWS ControlTowerServiceRolePolicy – Pembaruan ke kebijakan yang ada	AWS Control Tower menambahkan izin baru yang memungkinkan AWS Control Tower melakukan panggilan ke`EnableRegion` ,`ListRegions` , dan `GetRegionOptStatus` API yang diterapkan oleh layanan Manajemen AWS Akun, untuk membuat opt-in Wilayah AWS tersedia untuk akun pelanggan di zona pendaratan (Akun manajemen, akun arsip log, akun audit, akun anggota OU). Perubahan ini diperlukan agar pelanggan dapat memiliki opsi untuk memperluas tata kelola Wilayah dengan AWS Control Tower ke Wilayah opt-in.	6 April 2023

Ubah	Deskripsi	Tanggal
AWS ControlTowerServiceRolePolicy – Pembaruan ke kebijakan yang ada	AWS Control Tower menambahkan izin baru yang memungkinkan AWS Control Tower mengambil `AWSControlTowerBlueprintAccess` peran dalam akun cetak biru (hub), yang merupakan akun khusus dalam organisasi, yang berisi cetak biru yang telah ditentukan sebelumnya yang disimpan dalam satu atau beberapa Produk Katalog Layanan. AWS Control Tower mengambil `AWSControlTowerBlueprintAccess` peran untuk melakukan tiga tugas: membuat Portofolio Katalog Layanan, menambahkan Produk cetak biru yang diminta, dan membagikan Portofolio ke akun anggota yang diminta pada waktu penyediaan akun. Perubahan ini diperlukan agar pelanggan dapat menyediakan akun yang disesuaikan melalui AWS Control Tower Account Factory.	28 Oktober 2022

Ubah	Deskripsi	Tanggal
AWS ControlTowerServiceRolePolicy – Pembaruan ke kebijakan yang ada	AWS Control Tower menambahkan izin baru yang memungkinkan pelanggan menyiapkan AWS CloudTrail jalur tingkat organisasi, mulai dari zona pendaratan versi 3.0. CloudTrail Fitur berbasis organisasi mengharuskan pelanggan mengaktifkan akses tepercaya untuk CloudTrail layanan, dan pengguna atau peran IAM harus memiliki izin untuk membuat jejak tingkat organisasi di akun manajemen .	Juni 20, 2022

Ubah	Deskripsi	Tanggal
AWS ControlTowerServiceRolePolicy – Pembaruan ke kebijakan yang ada	AWS Control Tower menambahkan izin baru yang memungkinkan pelanggan menggunakan enkripsi kunci KMS. Fitur KMS memungkinkan pelanggan untuk menyediakan kunci KMS mereka sendiri untuk mengenkripsi log mereka CloudTrail . Pelanggan juga dapat mengubah kunci KMS selama pembaruan atau perbaikan zona pendaratan. Saat memperbarui kunci KMS, AWS CloudFormation perlu izin untuk memanggil AWS CloudTrail `PutEventSelector` API. Perubahan pada kebijakan ini adalah mengizinkan AWS ControlTowerAdmin peran memanggil AWS CloudTrail `PutEventSelector` API.	28 Juli 2021
AWS Control Tower mulai melacak perubahan	AWS Control Tower mulai melacak perubahan untuk kebijakan yang AWS dikelolanya.	27 Mei 2021

Keamanan di AWS Control Tower

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menggambarkan ini sebagai keamanan cloud dan keamanan di cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Efektivitas keamanan kami diuji dan diverifikasi secara rutin oleh auditor pihak ketiga sebagai bagian dari program kepatuhan AWS. Untuk mempelajari tentang program kepatuhan yang berlaku untuk AWS Control Tower, lihat AWS Layanan dalam Lingkup menurut Program Kepatuhan.
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, termasuk sensitivitas data, persyaratan perusahaan, serta hukum dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan AWS Control Tower. Topik berikut menunjukkan cara mengonfigurasi AWS Control Tower untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya AWS Control Tower Anda.

Perlindungan Data di AWS Control Tower

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di AWS Control Tower. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat FAQ Privasi Data AWS . Untuk informasi tentang perlindungan data di Eropa, lihat Pusat Peraturan Umum Perlindungan Data (GDPR).

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensyal dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access

Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat Bekerja dengan CloudTrail jejak di AWS CloudTrail Panduan Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-3.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan AWS Control Tower atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

> **Note**
>
> Pencatatan aktivitas pengguna ditangani AWS CloudTrail secara otomatis di AWS Control Tower saat Anda mengatur landing zone.

Untuk informasi selengkapnya tentang perlindungan data, lihat postingan blog Model Tanggung Jawab Bersama AWS dan GDPR di Blog Keamanan AWS . AWS Control Tower menyediakan opsi

berikut yang dapat Anda gunakan untuk membantu mengamankan konten yang ada di landing zone Anda:

Topik

- Enkripsi saat Data Tidak Berpindah
- Enkripsi Saat Data Berpindah
- Batasi Akses ke Konten

Enkripsi saat Data Tidak Berpindah

AWS Control Tower menggunakan bucket Amazon S3 dan database Amazon DynamoDB yang dienkripsi saat istirahat dengan menggunakan Amazon Keys () S3-Managed untuk mendukung landing zone Anda. SSE-S3 Enkripsi ini dikonfigurasi secara default saat Anda mengatur landing zone. Secara opsional, Anda dapat mengonfigurasi landing zone untuk mengenkripsi sumber daya dengan kunci enkripsi KMS. Anda juga dapat membuat enkripsi saat istirahat untuk layanan yang Anda gunakan di landing zone Anda untuk layanan yang mendukungnya. Untuk informasi selengkapnya, lihat bagian keamanan dokumentasi online layanan tersebut.

Enkripsi Saat Data Berpindah

AWS Control Tower menggunakan Transport Layer Security (TLS) dan enkripsi sisi klien untuk enkripsi saat transit guna mendukung landing zone Anda. Selain itu, mengakses AWS Control Tower memerlukan penggunaan konsol, yang hanya dapat diakses melalui titik akhir HTTPS. Enkripsi ini dikonfigurasi secara default saat Anda mengatur landing zone.

Batasi Akses ke Konten

Sebagai praktik terbaik, Anda harus membatasi akses ke subset pengguna yang sesuai. Dengan AWS Control Tower, Anda dapat melakukan ini dengan memastikan bahwa administrator cloud pusat dan pengguna akhir Anda memiliki izin IAM yang tepat atau, dalam kasus pengguna IAM Identity Center, bahwa mereka berada dalam grup yang benar.

- Untuk informasi selengkapnya tentang peran dan kebijakan untuk entitas IAM, lihat Panduan Pengguna IAM.
- Untuk informasi selengkapnya tentang grup Pusat Identitas IAM yang dibuat saat Anda menyiapkan landing zone, lihatGrup Pusat Identitas IAM untuk AWS Control Tower.

Validasi Kepatuhan untuk AWS Control Tower

AWS Control Tower adalah layanan yang dirancang dengan baik yang dapat membantu organisasi Anda memenuhi kebutuhan kepatuhan Anda dengan kontrol dan praktik terbaik. Selain itu, auditor pihak ketiga menilai keamanan dan kepatuhan sejumlah layanan yang dapat Anda gunakan di landing zone Anda sebagai bagian dari beberapa program AWS kepatuhan. Program ini mencakup SOC, PCI, FedRAMP, HIPAA, dan lainnya.

Untuk daftar AWS layanan dalam lingkup program kepatuhan tertentu, lihat AWS Layanan dalam Lingkup berdasarkan Program Kepatuhan. Untuk informasi umum, lihat Program Kepatuhan AWS.

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifak di AWS Artifact Panduan Pengguna.

Tanggung jawab kepatuhan Anda saat menggunakan AWS Control Tower ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, serta hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar yang berfokus pada keamanan dan kepatuhan. AWS
- Arsitektur untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakannya AWS untuk membuat aplikasi. HIPAA-compliant
- AWS Sumber Daya Kepatuhan — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Config AWS Layanan ini menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub CSPM— AWS Layanan ini memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS yang membantu Anda memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik.

Ketahanan di AWS Control Tower

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan.

AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung melalui latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Availability Zones memungkinkan Anda merancang dan mengoperasikan aplikasi dan database yang secara otomatis gagal di antara Availability Zone tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur biasa yang terdiri dari satu atau beberapa pusat data.

Untuk daftar Wilayah AWS tempat AWS Control Tower tersedia, lihatBagaimana AWS Wilayah Bekerja Dengan AWS Control Tower.

Wilayah asal Anda didefinisikan sebagai AWS Wilayah tempat landing zone Anda didirikan.

Untuk informasi selengkapnya tentang AWS Wilayah dan Availability Zone, lihat Infrastruktur AWS Global.

Keamanan Infrastruktur di AWS Control Tower

AWS Control Tower dilindungi oleh prosedur keamanan jaringan AWS global yang dijelaskan dalam whitepaper Amazon Web Services: Tinjauan Proses Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk akses ke AWS layanan dan sumber daya dalam landing zone Anda melalui jaringan. Kami memerlukan Transport Layer Security (TLS) 1.2 dan merekomendasikan Transport Layer Security (TLS) 1.3 atau yang lebih baru. Klien juga harus mendukung cipher suite dengan perfect forward secrecy (PFS) seperti Ephemeral (DHE) atau Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Diffie-Hellman Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan principal IAM. Atau Anda dapat menggunakan AWS Security Token Service (AWS STS) untuk menghasilkan kredensial keamanan sementara untuk menandatangani permintaan.

Anda dapat mengatur grup keamanan untuk menyediakan keamanan infrastruktur jaringan tambahan untuk beban kerja landing zone AWS Control Tower Anda. Lihat informasi yang lebih lengkap di Panduan: Mengatur Grup Keamanan di AWS Control Tower Dengan AWS Firewall Manager.

Pencatatan dan pemantauan di AWS Control Tower

Pemantauan memungkinkan Anda untuk merencanakan dan menanggapi insiden potensial. Hasil kegiatan pemantauan disimpan dalam file log. Oleh karena itu, logging dan monitoring adalah konsep yang terkait erat, dan merupakan bagian penting dari sifat AWS Control Tower yang dirancang dengan baik.

Saat menyiapkan landing zone, salah satu akun bersama yang dibuat adalah akun arsip log. Ini didedikasikan untuk mengumpulkan semua log secara terpusat, termasuk log untuk semua akun bersama dan anggota Anda. File log disimpan dalam bucket Amazon S3. File log ini memungkinkan administrator dan auditor untuk meninjau tindakan dan peristiwa yang telah terjadi.

Sebagai praktik terbaik, Anda harus mengumpulkan data pemantauan dari semua bagian AWS pengaturan Anda ke dalam log Anda, sehingga Anda dapat lebih mudah men-debug kegagalan multi-titik jika terjadi. AWS menyediakan beberapa alat untuk memantau sumber daya dan aktivitas Anda di landing zone Anda.

Misalnya, status kontrol Anda dipantau terus-menerus. Anda dapat melihat status mereka secara sekilas di konsol AWS Control Tower, atau secara terprogram melalui AWS Control Tower API. Kesehatan dan status akun yang Anda berikan di Account Factory juga dipantau secara konstan.

Melihat tindakan yang dicatat dari halaman Aktivitas

Di konsol AWS Control Tower, halaman Aktivitas memberikan ikhtisar tindakan akun manajemen AWS Control Tower. Untuk menavigasi ke halaman AWS Control Tower Activities, pilih Aktivitas dari navigasi kiri.

Aktivitas yang ditampilkan di halaman Aktivitas adalah aktivitas yang sama yang dilaporkan dalam log AWS CloudTrail peristiwa untuk AWS Control Tower, tetapi ditampilkan dalam format tabel. Untuk mempelajari lebih lanjut tentang aktivitas tertentu, pilih aktivitas dari tabel, lalu pilih Lihat detail.

Anda dapat melihat tindakan dan peristiwa akun anggota di file arsip log.

Bagian berikut menjelaskan pemantauan dan pencatatan di AWS Control Tower dengan detail selengkapnya:

Topik

- Alat terintegrasi untuk pemantauan

- Pencatatan Tindakan Menara Kontrol AWS dengan AWS CloudTrail
- Peristiwa Siklus Hidup di Menara Kontrol AWS
- Penggunaan AWS Pemberitahuan Pengguna dengan AWS Control Tower

Tentang masuk ke AWS Control Tower

AWS Control Tower menyelesaikan pencatatan tindakan dan peristiwa secara otomatis, melalui integrasinya dengan AWS CloudTrail dan AWS Config, dan merekamnya CloudWatch. Semua tindakan dicatat, termasuk tindakan dari akun manajemen AWS Control Tower dan dari akun anggota organisasi Anda. Tindakan dan peristiwa akun manajemen dapat dilihat di halaman Aktivitas di konsol. Anda dapat melihat tindakan dan peristiwa akun anggota di file arsip log.

Organization-level jalan setapak

AWS Control Tower menyiapkan CloudTrail jejak baru saat Anda menyiapkan landing zone. Ini adalah jejak tingkat organisasi, yang berarti mencatat semua peristiwa untuk akun manajemen dan semua akun anggota dalam organisasi. Fitur ini mengandalkan akses tepercaya untuk memberikan izin akun manajemen untuk membuat jejak di setiap akun anggota.

Untuk informasi selengkapnya tentang AWS Control Tower dan jejak CloudTrail organisasi, lihat Membuat jejak untuk organisasi.

> **Note**
>
> Dalam rilis AWS Control Tower sebelum landing zone versi 3.0, AWS Control Tower membuat jejak akun anggota di setiap akun. Saat Anda memperbarui ke rilis 3.0, CloudTrail jejak Anda menjadi jejak organisasi. Untuk praktik terbaik saat berpindah antar jalur, lihat Praktik terbaik untuk mengubah jejak di CloudTrail Panduan Pengguna.

Saat Anda mendaftarkan akun ke AWS Control Tower, akun Anda diatur oleh AWS CloudTrail jejak untuk organisasi AWS Control Tower. Jika Anda memiliki penerapan CloudTrail jejak yang ada di akun tersebut, Anda mungkin melihat biaya duplikat kecuali Anda menghapus jejak yang ada untuk akun tersebut sebelum Anda mendaftarkannya di AWS Control Tower.

> **Note**
>
> Saat Anda memperbarui ke landing zone versi 3.0, AWS Control Tower menghapus jejak tingkat akun (yang telah dibuat AWS Control Tower) di akun terdaftar atas nama Anda. File log tingkat akun Anda yang ada disimpan di bucket Amazon S3 mereka.

Kebijakan bucket Amazon S3 untuk pencatatan

Di AWS Control Tower, AWS layanan memiliki akses ke sumber daya Anda hanya jika permintaan berasal dari organisasi atau unit organisasi (OU) Anda. `aws:SourceOrgID`Syarat harus dipenuhi untuk izin menulis apa pun.

Anda dapat menggunakan kunci `aws:SourceOrgID` kondisi dan menyetel nilainya ke ID organisasi di elemen kondisi kebijakan bucket Amazon S3 Anda. Kondisi ini memastikan bahwa hanya akun dalam organisasi Anda yang dapat menulis log ke bucket Amazon S3 Anda. Ini mencegah akun di luar organisasi Anda menulis log ke bucket AWS Control Tower Amazon S3 Anda.

Untuk informasi selengkapnya tentang kunci kondisi ini, lihat kunci konteks kondisi global IAM. Untuk posting blog tentang kontrol yang dapat diskalakan, lihat Menggunakan kontrol yang dapat diskalakan untuk AWS layanan yang mengakses sumber daya Anda.

Kebijakan ini tidak memengaruhi fungsionalitas beban kerja Anda yang ada.

Zona pendaratan versi 3.3 dan sebelumnya

Di landing zone versi 3.3 dan yang lebih lama, AWS Control Tower menerapkan satu bucket Amazon S3 di akun arsip log yang menyimpan AWS CloudTrail keduanya AWS Config dan log. Kebijakan bucket ditampilkan dalam contoh berikut.

```
S3AuditBucketPolicy:
    Type: AWS::S3::BucketPolicy
    Properties:
      Bucket: !Ref S3AuditBucket
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Sid: AllowSSLRequestsOnly
            Effect: Deny
            Principal: '*'
```

```
            Action: s3:*
            Resource:
             - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
             - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/*"
            Condition:
              Bool:
                aws:SecureTransport: false
          - Sid: AWSBucketPermissionsCheck
            Effect: Allow
            Principal:
              Service:
                - cloudtrail.amazonaws.com
                - config.amazonaws.com
            Action: s3:GetBucketAcl
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
          - Sid: AWSConfigBucketExistenceCheck
            Effect: Allow
            Principal:
              Service:
                - cloudtrail.amazonaws.com
                - config.amazonaws.com
            Action: s3:ListBucket
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
          - Sid: AWSBucketDeliveryForConfig
            Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action: s3:PutObject
            Resource:
              - Fn::Join:
                  - ""
                  -
                    - !Sub "arn:${AWS::Partition}:s3:::"
                    - !Ref "S3AuditBucket"
                    - !Sub "/${AWSLogsS3KeyPrefix}/AWSLogs/*/*"
            Condition:
              StringEquals:
                aws:SourceOrgID: !Ref OrganizationId
          - Sid: AWSBucketDeliveryForOrganizationTrail
            Effect: Allow
            Principal:
```

```
              Service:
                - cloudtrail.amazonaws.com
            Action: s3:PutObject
            Resource: !If [IsAccountLevelBucketPermissionRequiredForCloudTrail,
                [!Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
${AWSLogsS3KeyPrefix}/AWSLogs/${Namespace}/*", !Sub "arn:${AWS::Partition}:s3:::
${S3AuditBucket}/${AWSLogsS3KeyPrefix}/AWSLogs/${OrganizationId}/*"],
                !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
${AWSLogsS3KeyPrefix}/AWSLogs/*/*"]
            Condition:
              StringEquals:
                aws:SourceOrgID: !Ref OrganizationId
```

Zona pendaratan versi 4.0 dan yang lebih baru

Di landing zone versi 4.0 dan yang lebih baru, AWS Config dan AWS CloudTrail gunakan bucket Amazon S3 khusus yang terpisah, bukan bucket bersama. Bucket Amazon S3 untuk AWS Config log ada di akun AWS Config integrasi (sebelumnya akun Audit). Bucket Amazon S3 untuk AWS CloudTrail log ada di akun AWS CloudTrail administrator (sebelumnya akun Arsip Log). Untuk informasi selengkapnya, lihat Pembaruan AWS Config.

AWS CloudTrail kebijakan bucket (AWS CloudTrail akun administrator)

Contoh berikut menunjukkan kebijakan AWS CloudTrail bucket yang diterapkan di akun AWS CloudTrail administrator:

```
S3AuditBucketPolicy:
    Type: AWS::S3::BucketPolicy
    Properties:
      Bucket: !Ref S3AuditBucket
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Sid: AllowSSLRequestsOnly
            Effect: Deny
            Principal: '*'
            Action: s3:*
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
              - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/*"
            Condition:
              Bool:
```

```
                aws:SecureTransport: false
          - Sid: AWSBucketPermissionsCheck
            Effect: Allow
            Principal:
              Service:
                - cloudtrail.amazonaws.com
            Action: s3:GetBucketAcl
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
          - Sid: AWSConfigBucketExistenceCheck
            Effect: Allow
            Principal:
              Service:
                - cloudtrail.amazonaws.com
            Action: s3:ListBucket
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}"
          - Sid: AWSBucketDeliveryForOrganizationTrail
            Effect: Allow
            Principal:
              Service:
                - cloudtrail.amazonaws.com
            Action: s3:PutObject
            Resource: !If [IsAccountLevelBucketPermissionRequiredForCloudTrail,
                           [!Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
${AWSLogsS3KeyPrefix}/AWSLogs/${Namespace}/*", !Sub "arn:${AWS::Partition}:s3:::
${S3AuditBucket}/${AWSLogsS3KeyPrefix}/AWSLogs/${OrganizationId}/*"],
                           !Sub "arn:${AWS::Partition}:s3:::${S3AuditBucket}/
${AWSLogsS3KeyPrefix}/AWSLogs/*/*"]
            Condition:
              StringEquals:
                aws:SourceOrgID: !Ref OrganizationId
```

AWS Config kebijakan bucket (AWS Config akun integrasi)

Contoh berikut menunjukkan kebijakan AWS Config bucket yang diterapkan di akun AWS Config integrasi:

```
ConfigS3BucketPolicy:
    Type: AWS::S3::BucketPolicy
    Properties:
      Bucket: !Ref ConfigS3Bucket
      PolicyDocument:
```

```
        Version: 2012-10-17
        Statement:
          - Sid: AllowSSLRequestsOnly
            Effect: Deny
            Principal: '*'
            Action: s3:*
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigS3Bucket}"
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigS3Bucket}/*"
            Condition:
              Bool:
                aws:SecureTransport: false
          - Sid: AWSConfigBucketPermissionsCheck
            Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action: s3:GetBucketAcl
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigS3Bucket}"
          - Sid: AWSConfigBucketExistenceCheck
            Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action: s3:ListBucket
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigS3Bucket}"
          - Sid: AWSConfigBucketDelivery
            Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action: s3:PutObject
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigS3Bucket}/
${ConfigS3KeyPrefix}/AWSLogs/*/*"
            Condition:
              StringEquals:
                aws:SourceOrgID: !Ref OrganizationId
```

Alat terintegrasi untuk pemantauan

Pemantauan adalah bagian penting dalam menjaga keandalan, ketersediaan, dan kinerja AWS Control Tower dan AWS solusi Anda yang lain. AWS menyediakan alat pemantauan berikut untuk mengawasi AWS Control Tower, melaporkan ketika ada sesuatu yang salah, dan mengambil tindakan otomatis bila perlu:

- Amazon CloudWatch memantau AWS sumber daya Anda dan aplikasi yang Anda jalankan AWS secara real time. Anda dapat mengumpulkan dan melacak metrik, membuat dasbor yang disesuaikan, dan mengatur alarm yang memberi tahu Anda atau mengambil tindakan saat metrik tertentu mencapai ambang batas yang ditentukan. Misalnya, Anda dapat CloudWatch melacak penggunaan CPU atau metrik lain dari instans Amazon EC2 Anda dan secara otomatis meluncurkan instans baru bila diperlukan. Untuk informasi selengkapnya, lihat Panduan CloudWatch Pengguna Amazon.
- Amazon EventBridge memberikan aliran peristiwa sistem yang mendekati real-time yang menggambarkan perubahan AWS sumber daya. EventBridge mengaktifkan komputasi berbasis peristiwa otomatis, karena Anda dapat menulis aturan yang mengawasi peristiwa tertentu dan memicu tindakan otomatis di AWS layanan lain saat peristiwa ini terjadi. Untuk informasi selengkapnya, lihat Panduan Pengguna CloudWatch Acara Amazon.
- Amazon CloudWatch Logs memungkinkan Anda memantau, menyimpan, dan mengakses file log Anda dari instans Amazon EC2, CloudTrail, dan sumber lainnya. CloudWatch Log dapat memantau informasi dalam file log dan memberi tahu Anda ketika ambang batas tertentu terpenuhi. Anda juga dapat mengarsipkan data log dalam penyimpanan yang sangat durabel. Untuk informasi selengkapnya, lihat Panduan Pengguna Amazon CloudWatch Logs.
- AWS CloudTrailmenangkap panggilan API dan peristiwa terkait yang dibuat oleh atau atas nama AWS akun Anda dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi.

Tip: Anda dapat melihat dan CloudTrail melakukan kueri aktivitas di akun melalui Wawasan CloudWatch Log dan CloudWatch Log. Aktivitas ini mencakup peristiwa siklus hidup AWS Control Tower. CloudWatch Kemampuan log memungkinkan Anda untuk melakukan kueri yang lebih terperinci dan akurat daripada yang biasanya dapat Anda gunakan. CloudTrail

Lihat informasi yang lebih lengkap di Pencatatan Tindakan Menara Kontrol AWS dengan AWS CloudTrail.

Pencatatan Tindakan Menara Kontrol AWS dengan AWS CloudTrail

AWS Control Tower terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di AWS Control Tower. CloudTrail menangkap tindakan untuk Menara Kontrol AWS sebagai peristiwa. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon S3, termasuk acara untuk AWS Control Tower.

Jika Anda tidak membuat konfigurasi jejak, Anda masih dapat melihat kejadian terbaru dalam konsol CloudTrail di Riwayat peristiwa. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat ke AWS Control Tower, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan permintaan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, termasuk cara mengonfigurasi dan mengaktifkannya, lihat Panduan AWS CloudTrail Pengguna.

Informasi Menara Kontrol AWS di CloudTrail

CloudTrail diaktifkan pada AWS akun Anda saat Anda membuat akun. Ketika aktivitas acara yang didukung terjadi di AWS Control Tower, aktivitas tersebut dicatat dalam suatu CloudTrail acara bersama dengan peristiwa AWS layanan lainnya di ri wayat acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di AWS akun Anda. Untuk informasi selengkapnya, lihat Melihat Acara dengan Ri CloudTrail wayat Acara.

> **Note**
>
> Di rilis AWS Control Tower sebelum zona pendaratan versi 3.0, AWS Control Tower membuat jejak akun anggota. Saat Anda memperbarui ke rilis 3.0, CloudTrail jejak Anda diperbarui untuk menjadi jejak organisasi. Untuk praktik terbaik saat berpindah antar jalur, lihat Membuat jejak organisasi di Panduan CloudTrail Pengguna.

Direkomendasikan: Buat jejak

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, termasuk acara untuk AWS Control Tower, buat jejak. Jej ak CloudTrail memungkinkan pengiriman file log ke bucket Amazon

S3. Secara default, saat Anda membuat jejak di konsol tersebut, jejak diterapkan ke semua Wilayah AWS . Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan bertindak berdasarkan data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- Gambaran Umum untuk Membuat Jejak
- Bersiaplah untuk membuat jejak
- Mengelola CloudTrail biaya
- CloudTrail Layanan dan Integrasi yang Didukung
- Mengkonfigurasi Pemberitahuan Amazon SNS untuk CloudTrail
- Mener CloudTrail ima File Log dari Beberapa Wilayah dan M CloudTrail enerima File Log dari Beberapa Akun

AWS Control Tower mencatat tindakan berikut sebagai peristiwa dalam file CloudTrail log:

API Publik

- Untuk daftar lengkap API publik AWS Control Tower dan detail tentang masing-masing API, lihat Refer ensi API Menara Kontrol AWS. Panggilan ke API publik ini dicatat oleh AWS CloudTrail.

API Lainnya

- `SetupLandingZone`
- `UpdateAccountFactoryConfig`
- `ManageOrganizationalUnit`
- `CreateManagedAccount`
- `GetLandingZoneStatus`
- `GetHomeRegion`
- `ListManagedAccounts`
- `DescribeManagedAccount`
- `DescribeAccountFactoryConfig`
- `DescribeGuardrailForTarget`

- `DescribeManagedOrganizationalUnit`
- `ListEnabledGuardrails`
- `ListGuardrailViolations`
- `ListGuardrails`
- `ListGuardrailsForTarget`
- `ListManagedAccountsForGuardrail`
- `ListManagedAccountsForParent`
- `ListManagedOrganizationalUnits`
- `ListManagedOrganizationalUnitsForGuardrail`
- `GetGuardrailComplianceStatus`
- `DescribeGuardrail`
- `ListDirectoryGroups`
- `DescribeSingleSignOn`
- `DescribeCoreService`
- `GetAvailableUpdates`

Setiap entri peristiwa atau log berisi informasi tentang entitas yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut ini:

- Apakah permintaan dibuat dengan kredentif pengguna root atau AWS Identity and Access Management (IAM).
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan itu dibuat oleh AWS layanan lain.
- Apakah permintaan ditolak karena akses ditolak atau berhasil diproses.

Untuk informasi lain, lihat Elemen userIdentity CloudTrail .

Contoh: Entri File Log Menara Kontrol AWS

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili

permintaan tunggal dari sumber apa pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail peristiwa tidak muncul dalam urutan tertentu dalam file log.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan struktur entri file log khas untuk acara `SetupLandingZone` AWS Control Tower, termasuk catatan identitas pengguna yang memulai tindakan.


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:backend-test-assume-role-session",
    "arn": "arn:aws:sts::76543EXAMPLE;:assumed-role/AWSControlTowerTestAdmin/backend-
test-assume-role-session",
    "accountId": "76543EXAMPLE",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-11-20T19:36:11Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::AKIAIOSFODNN7EXAMPLE:role/AWSControlTowerTestAdmin",
        "accountId": "AIDACKCEVSQ6C2EXAMPLE",
        "userName": "AWSControlTowerTestAdmin"
      }
    }
  },
  "eventTime": "2018-11-20T19:36:15Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "SetupLandingZone",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "Coral/Netty4",
  "errorCode": "InvalidParametersException",
  "errorMessage": "Home region EU_CENTRAL_1 is unsupported",
  "requestParameters": {
    "homeRegion": "EU_CENTRAL_1",
    "logAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "sharedServiceAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
```

```
    "securityAccountEmail": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "securityNotificationEmail": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "responseElements": null,
  "requestID": "96f47b68-ed5f-4268-931c-807cd1f89a96",
  "eventID": "4ef5cf08-39e5-4fdf-9ea2-b07ced506851",
  "eventType": "AwsApiCall",
  "recipientAccountId": "76543EXAMPLE"
}
```

Pantau perubahan sumber daya dengan AWS Config

AWS Control Tower memungkinkan AWS Config pada semua akun yang terdaftar, sehingga dapat memantau kepatuhan melalui kontrol detektif, merekam perubahan sumber daya, dan mengirimkan log perubahan sumber daya ke akun terpusat. AWS Control Tower memusatkan AWS Config data ini sehingga Anda dapat meninjau perubahan konfigurasi sumber daya dari semua akun yang terdaftar di satu tempat, yang membantu Anda mengaudit lingkungan dan menunjukkan kepatuhan.

Jika versi landing zone Anda lebih awal dari 3.0: Untuk akun terdaftar Anda, AWS Config catat semua perubahan pada sumber daya, untuk semua Wilayah tempat akun beroperasi. Setiap perubahan dimodelkan sebagai item konfigurasi (CI), yang berisi informasi seperti pengidentifikasi sumber daya, Wilayah, tanggal setiap perubahan dicatat, dan apakah perubahan tersebut terkait dengan sumber daya yang diketahui atau yang baru ditemukan.

Jika versi landing zone Anda 3.0 atau yang lebih baru: AWS Control Tower membatasi perekaman untuk sumber daya global, seperti pengguna IAM, grup, peran, dan kebijakan yang dikelola pelanggan, hanya untuk Wilayah asal Anda. Salinan perubahan sumber daya global tidak disimpan di setiap Wilayah. Keterbatasan perekaman sumber daya ini sesuai dengan praktik AWS Config terbaik. Daftar lengkap sumber daya global tersedia dalam AWS Config dokumentasi.

- Untuk mempelajari selengkapnya AWS Config, lihat Cara AWS Config kerjanya.
- Untuk daftar sumber daya yang AWS Config dapat mendukung, lihat Jenis sumber daya yang didukung.
- Untuk mempelajari cara menyesuaikan pelacakan sumber daya di lingkungan AWS Control Tower, lihat posting blog berjudul Kustomisasi pelacakan AWS Config sumber daya di AWS Control Tower.

AWS Control Tower menyiapkan saluran AWS Config pengiriman di setiap akun yang terdaftar. Saluran pengiriman mengirimkan perubahan yang direkam ke akun terpusat, tempat AWS Config menyimpannya di bucket Amazon Simple Storage Service. Nama dan lokasi bucket Amazon S3 bergantung pada versi landing zone Anda:

- Untuk landing zone versi 3.3 atau yang lebih lama, log disimpan di bucket `aws-controltower-logs-*` Amazon S3 di akun arsip log.
- Untuk landing zone versi 4.0 atau yang lebih baru, log disimpan di bucket `aws-controltower-config-logs-*` Amazon S3 di akun AWS Config integrasi (sebelumnya dikenal sebagai akun Audit). Untuk informasi selengkapnya, lihat Pembaruan AWS Config.

Kelola AWS Config biaya di AWS Control Tower

Bagian ini menjelaskan cara AWS Config mencatat dan menagih Anda untuk perubahan sumber daya di akun AWS Control Tower Anda. Informasi ini dapat membantu Anda memahami cara mengelola biaya yang terkait AWS Config, saat Anda menggunakan AWS Control Tower. AWS Control Tower tidak menambahkan biaya tambahan.

> **Note**
>
> Jika versi landing zone Anda 3.0 atau yang lebih baru: AWS Control Tower membatasi AWS Config perekaman untuk sumber daya global, seperti pengguna IAM, grup, peran, dan kebijakan yang dikelola pelanggan, hanya untuk Wilayah asal Anda. Oleh karena itu, beberapa informasi di bagian ini mungkin tidak berlaku untuk landing zone Anda.

AWS Config dirancang untuk mencatat setiap perubahan ke setiap sumber daya, di setiap Wilayah tempat akun beroperasi, sebagai item konfigurasi (CI). AWS Config menagih Anda untuk setiap item konfigurasi yang dihasilkannya.

Bagaimana AWS Config beroperasi

AWS Config mencatat sumber daya di setiap Wilayah, secara terpisah. Beberapa sumber daya global, seperti peran IAM, dicatat satu kali per Wilayah. Misalnya, jika Anda membuat peran IAM baru di akun terdaftar yang beroperasi di lima Wilayah, AWS Config hasilkan lima CI, satu untuk setiap Wilayah. Sumber daya global lainnya, seperti zona yang dihosting Route 53, dicatat hanya sekali di semua Wilayah. Misalnya, jika Anda membuat zona host Route 53 baru di akun terdaftar, buat AWS Config satu CI, terlepas dari berapa banyak Wilayah yang dipilih untuk akun tersebut. Untuk daftar

yang membantu Anda membedakan jenis sumber daya ini, lihatSumber daya yang sama dicatat beberapa kali.

> **Note**
>
> Saat AWS Control Tower berfungsi AWS Config, Wilayah dapat diatur oleh AWS Control Tower, atau tidak diatur, dan AWS Config masih mencatat perubahan jika akun beroperasi di Wilayah tersebut.

AWS Config mendeteksi dua jenis hubungan dalam sumber daya

AWS Config membuat perbedaan antara hubungan langsung dan tidak langsung antara sumber daya. Jika sumber daya dikembalikan dalam panggilan API Deskripsikan sumber daya lain, sumber daya tersebut dicatat sebagai hubungan langsung. Ketika Anda mengubah sumber daya dalam hubungan langsung dengan sumber daya lain, AWS Config tidak membuat CI untuk kedua sumber daya.

Misalnya, jika Anda membuat instans Amazon EC2, dan API mengharuskan Anda membuat antarmuka jaringan, AWS Config pertimbangkan instans Amazon EC2 memiliki hubungan langsung dengan antarmuka jaringan. Akibatnya, hanya AWS Config menghasilkan satu CI.

AWS Config mencatat perubahan terpisah untuk hubungan sumber daya yang merupakan hubungan tidak langsung. Misalnya, buat AWS Config dua CI jika Anda membuat grup keamanan dan menambahkan instans Amazon EC2 terkait yang merupakan bagian dari grup keamanan.

Untuk informasi lebih lanjut tentang hubungan langsung dan tidak langsung, lihat Apa itu hubungan langsung dan tidak langsung sehubungan dengan sumber daya?

Anda dapat menemukan daftar hubungan sumber daya dalam AWS Config dokumentasi.

Lihat AWS Config data perekam pada akun terdaftar

AWS Config terintegrasi dengan CloudWatch sehingga Anda dapat melihat AWS Config CI di dasbor. Untuk informasi selengkapnya, lihat posting blog berjudul AWS Config mendukung CloudWatch metrik Amazon.

Secara terprogram, untuk melihat AWS Config data, Anda dapat bekerja dengan AWS CLI, atau Anda dapat menggunakan alat lain. AWS

Permintaan AWS Config perekam data pada sumber daya tertentu

Anda dapat menggunakan AWS CLI untuk mengambil daftar perubahan terbaru untuk sumber daya.

Perintah riwayat sumber daya:

- `aws configservice get-resource-config-history --resource-type RESOURCE-TYPE --resource-id RESOURCE-ID --region REGION`

Untuk mempelajari selengkapnya, lihat dokumentasi API untuk `get-config-history`.

Visualisasikan AWS Config Data dengan Quick

Anda dapat memvisualisasikan dan meminta sumber daya yang direkam oleh AWS Config seluruh organisasi Anda. Untuk informasi selengkapnya, lihat Dasbor Kepatuhan Sumber Daya Konfigurasi dan Memvisualisasikan AWS Config data menggunakan Amazon Athena dan Quick.

Pemecahan masalah AWS Config di AWS Control Tower

Bagian ini memberikan informasi tentang beberapa masalah yang mungkin Anda temui saat menggunakan AWS Config AWS Control Tower.

Tinggi AWS Config ongkos

Jika alur kerja Anda menyertakan proses yang sering membuat, memperbarui, atau menghapus sumber daya, atau menangani sumber daya dalam jumlah besar, alur kerja tersebut dapat menghasilkan sejumlah besar CI. Jika Anda menjalankan proses ini di akun non-produksi, pertimbangkan untuk membuka pendaftaran akun. Anda mungkin perlu menonaktifkan AWS Config perekam untuk akun itu secara manual.

> **Note**
>
> Setelah Anda membatalkan pendaftaran akun, AWS Control Tower tidak dapat menerapkan kontrol detektif atau peristiwa akun log, seperti AWS Config aktivitas, untuk sumber daya di akun tersebut.

Untuk informasi selengkapnya, lihat Membatalkan kelola akun yang terdaftar. Untuk mempelajari cara menonaktifkan AWS Config perekam, lihat Mengelola perekam konfigurasi.

Sumber daya yang sama dicatat beberapa kali

Periksa apakah sumber daya adalah sumber daya global. Untuk zona pendaratan AWS Control Tower sebelum versi 3.0, AWS Config dapat merekam sumber daya global tertentu satu kali untuk setiap Wilayah AWS Config yang beroperasi. Misalnya, jika AWS Config diaktifkan pada delapan Wilayah, setiap peran direkam delapan kali.

Sumber daya berikut dicatat satu kali untuk setiap Wilayah di mana AWS Config beroperasi:

- `AWS::IAM::Group`
- `AWS::IAM::Policy`
- `AWS::IAM::Role`
- `AWS::IAM::User`

Sumber daya global lainnya dicatat hanya sekali. Berikut adalah beberapa contoh sumber daya yang direkam satu kali:

- `AWS::Route53::HostedZone`
- `AWS::Route53::HealthCheck`
- `AWS::ECR::PublicRepository`
- `AWS::GlobalAccelerator::Listener`
- `AWS::GlobalAccelerator::EndpointGroup`
- `AWS::GlobalAccelerator::Accelerator`

AWS Config tidak merekam sumber daya

Sumber daya tertentu memiliki hubungan ketergantungan dengan sumber daya lain. Hubungan ini mungkin langsung atau tidak langsung. Anda dapat menemukan daftar hubungan tidak langsung yang tidak digunakan lagi di FAQ. AWS Config

Peristiwa Siklus Hidup di Menara Kontrol AWS

Beberapa peristiwa yang dicatat oleh AWS Control Tower adalah peristiwa siklus hidup. Tujuan peristiwa siklus hidup adalah untuk menandai penyeles aian tindakan AWS Control Tower tertentu

yang mengubah status sumber daya. Peristiwa siklus hidup berlaku untuk sumber daya yang dibuat atau dikelola AWS Control Tower, seperti zona pendaratan, garis dasar, atau kontrol, yang terkait dengan unit organisasi (OU) atau akun.

Karakteristik peristiwa siklus hidup AWS Control Tower

- Untuk setiap peristiwa siklus hidup, log peristiwa menunjukkan apakah tindakan Menara Kontrol yang berasal berhasil diselesaikan, atau gagal.
- AWS CloudTrail secara otomatis merekam setiap peristiwa siklus hidup sebagai peristiwa AWS layanan non-API. Untuk informasi selengkapnya, lihat Panduan AWS CloudTrail Pengguna.
- Setiap acara siklus hidup juga dikirimkan ke layanan Amazon EventBridge dan Amazon Ev CloudWatch ents. Catatan: Untuk menerima peristiwa siklus hidup di EventBridge, Anda harus memiliki AWS CloudTrail jejak aktif dengan pencatatan diaktifkan. Untuk informasi selengkapnya tentang acara AWS layanan yang diki AWS CloudTrail rimkan melalui, lihat acara layanan AWS yang dikirimkan melalui AWS CloudTrail di Panduan EventBridge Pengguna Amazon.

Peristiwa siklus hidup di AWS Control Tower menawarkan dua manfaat utama:

- Karena peristiwa siklus hidup mendaftarkan penyelesaian tindakan AWS Control Tower, Anda dapat membuat EventBridge aturan Amazon atau aturan Amazon Ev CloudWatch ents yang dapat memicu langkah selanjutnya dalam alur kerja otomatisasi Anda, berdasarkan status peristiwa siklus hidup.
- Log memberikan detail tambahan untuk membantu administrator dan auditor dalam meninjau jenis aktivitas tertentu di organisasi Anda.

Cara kerja peristiwa siklus hidup

AWS Control Tower bergantung pada beberapa layanan untuk mengimplementasikan tindakannya. Oleh karena itu, setiap peristiwa siklus hidup dicatat hanya setelah serangkaian tindakan selesai. Misalnya, saat Anda mengaktifkan kontrol pada OU, AWS Control Tower meluncurkan serangkaian sub-langkah yang mengimplementasikan permintaan. Hasil akhir dari seluruh rangkaian sub-langkah dicatat dalam log sebagai status peristiwa siklus hidup.

- Jika setiap sub-langkah yang mendasarinya telah berhasil diselesaikan, status peristiwa siklus hidup dicatat sebagai Berhasil.
- Jika salah satu sub-langkah yang mendasarinya tidak berhasil diselesaikan, status peristiwa siklus hidup dicatat sebagai Gag al.

Setiap peristiwa siklus hidup menyertakan stempel waktu yang dicatat yang menunjukkan kapan tindakan AWS Control Tower dimulai, dan stempel waktu lain yang menunjukkan kapan peristiwa siklus hidup selesai, menandai keberhasilan atau kegagalan.

Melihat peristiwa siklus hidup di Menara Kontrol

Anda dapat melihat peristiwa siklus hidup dari halaman Aktivitas di dasbor AWS Control Tower Anda.

- Untuk menavigasi ke halaman Aktivitas, pilih Aktiv itas dari panel navigasi kiri.
- Untuk mendapatkan detail lebih lanjut tentang acara tertentu, pilih acara dan kemudian pilih tombol Lihat detail di kanan atas.

Untuk informasi selengkapnya tentang cara mengintegrasikan peristiwa siklus hidup AWS Control Tower ke alur kerja Anda, lihat posting blog ini, Menggunakan peristiwa siklus hidup untuk melacak tindakan AWS Control Tower dan memicu alur kerja otomatis.

Perilaku yang diharapkan CreateManagedAccount dan peristiwa UpdateManagedAccount siklus hidup

Saat Anda membuat akun atau mendaftarkan akun di AWS Control Tower, kedua tindakan tersebut memanggil API internal yang sama. Jika ada kesalahan selama proses, biasanya terjadi setelah akun dibuat tetapi tidak sepenuhnya disediakan. Saat Anda mencoba lagi untuk membuat akun setelah kesalahan, atau ketika Anda mencoba memperbarui produk yang disediakan, AWS Control Tower melihat bahwa akun tersebut sudah ada.

Karena akun ada, AWS Control Tower merekam peristiwa `UpdateManagedAccount` siklus hidup alih-alih peristiwa `CreateManagedAccount` siklus hidup di akhir permintaan coba lagi. Anda mungkin mengharapkan untuk melihat `CreateManagedAccount` peristiwa lain karena kesalahan. Namun, peristiwa `UpdateManagedAccount` siklus hidup adalah perilaku yang diharapkan dan diinginkan.

Jika Anda berencana untuk membuat atau mendaftarkan akun ke AWS Control Tower menggunakan metode otomatis, program fungsi Lambda untuk mencari peristiwa UpdateManagedAccount siklus hidup serta peristiwa CreateManagedAccount siklus hidup.

Nama peristiwa siklus hidup

Setiap peristiwa siklus hidup diberi nama sehingga sesuai dengan tindakan AWS Control Tower yang berasal, yang juga direkam oleh AWS CloudTrail. Jadi, misalnya, peristiwa siklus hidup

yang berasal dari `CreateManagedAccount` CloudTrail peristiwa Menara Kontrol AWS diberi nama`CreateManagedAccount`.

Setiap nama dalam daftar berikut adalah tautan ke contoh detail yang dicatat dalam `JSON` format. Detail tambahan yang ditunjukkan dalam contoh ini diambil dari log CloudWatch peristiwa Amazon.

Meskipun `JSON` tidak mendukung komentar, beberapa komentar telah ditambahkan dalam contoh untuk tujuan penjelasan. Komentar didahului dengan "//" dan muncul di sisi kanan contoh.

Dalam contoh ini, beberapa nama akun dan nama organisasi dikaburkan. An selalu `accountId` merupakan urutan 12 angka, yang telah diganti dengan "xxxxxxxxxxxx" dalam contoh. An `organizationalUnitID` adalah string huruf dan angka yang unik. Bentuknya dipertahankan dalam contoh.

- `CreateManagedAccount`: Log mencatat apakah AWS Control Tower berhasil menyelesaikan setiap tindakan untuk membuat dan menyediakan akun baru menggunakan pabrik akun.
- `UpdateManagedAccount`: Log mencatat apakah AWS Control Tower berhasil menyelesaikan setiap tindakan untuk memperbarui produk yang disediakan yang terkait dengan akun yang sebelumnya Anda buat dengan menggunakan pabrik akun.
- `EnableGuardrail`: Log mencatat apakah AWS Control Tower berhasil menyelesaikan setiap tindakan untuk mengaktifkan kontrol pada OU.
- `DisableGuardrail`: Log mencatat apakah AWS Control Tower berhasil menyelesaikan setiap tindakan untuk menonaktifkan kontrol pada OU.
- `SetupLandingZone`: Log mencatat apakah AWS Control Tower berhasil menyelesaikan setiap tindakan untuk menyiapkan zona pendaratan.
- `UpdateLandingZone`: Log mencatat apakah AWS Control Tower berhasil menyelesaikan setiap tindakan untuk memperbarui zona pendaratan Anda yang ada.
- `RegisterOrganizationalUnit`: Log mencatat apakah AWS Control Tower berhasil menyelesaikan setiap tindakan untuk mengaktifkan fitur tata kelola pada OU.
- `DeregisterOrganizationalUnit`: Log mencatat apakah AWS Control Tower berhasil menyelesaikan setiap tindakan untuk menonaktifkan fitur tata kelola pada OU.
- `PrecheckOrganizationalUnit`: Log mencatat apakah AWS Control Tower mendeteksi sumber daya apa pun yang akan mencegah operasi Extend governance diselesaikan dengan sukses.
- `EnableBaseline`: Log mencatat apakah AWS Control Tower berhasil menyelesaikan setiap tindakan untuk mengaktifkan baseline baru pada akun anggota target di bawah OU. Operasi aktifkan dapat dimulai menggunakan `EnableBaseline` API atau konsol.

- `ResetEnabledBaseline`: Log mencatat apakah AWS Control Tower berhasil menyelesaikan setiap tindakan untuk mengatur ulang baseline yang diaktifkan yang ada pada akun anggota target di bawah OU. Operasi reset dapat dimulai menggunakan `ResetEnabledBaseline` API atau konsol.
- `UpdateEnabledBaseline`: Log mencatat apakah AWS Control Tower berhasil menyelesaikan setiap tindakan untuk memperbarui baseline yang diaktifkan yang ada pada akun anggota target di bawah OU. Operasi pembaruan dapat dimulai menggunakan `UpdateEnabledBaseline` API atau konsol.
- `DisableBaseline`: Log mencatat apakah AWS Control Tower berhasil menyelesaikan setiap tindakan untuk menonaktifkan baseline yang diaktifkan yang ada pada akun anggota target di bawah OU. Operasi penonaktifan dapat dimulai menggunakan `DisableBaseline` API atau konsol.
- `EnableControl`: Log mencatat apakah AWS Control Tower berhasil menyelesaikan setiap tindakan untuk mengaktifkan kontrol pada akun target di bawah OU. Operasi aktifkan dapat dimulai menggunakan `EnableControl` API atau konsol.
- `ResetEnabledControl`: Log mencatat apakah AWS Control Tower berhasil menyelesaikan setiap tindakan untuk mengatur ulang kontrol yang diaktifkan yang ada pada akun target di bawah OU. Operasi reset dapat dimulai menggunakan `ResetEnabledControl` API atau konsol.
- `UpdateEnabledControl`: Log mencatat apakah AWS Control Tower berhasil menyelesaikan setiap tindakan untuk memperbarui kontrol yang diaktifkan yang ada pada akun target di bawah OU. Operasi pembaruan dapat dimulai menggunakan `UpdateEnabledControl` API atau konsol.
- `DisableControl`: Log mencatat apakah AWS Control Tower berhasil menyelesaikan setiap tindakan untuk menonaktifkan kontrol yang diaktifkan yang ada pada akun target di bawah OU. Operasi penonaktifan dapat dimulai menggunakan `DisableControl` API atau konsol.

Bagian berikut menyediakan daftar peristiwa siklus hidup AWS Control Tower, dengan contoh detail yang dicatat untuk setiap jenis peristiwa siklus hidup.

`CreateManagedAccount`

Peristiwa siklus hidup ini mencatat apakah AWS Control Tower berhasil membuat dan menyediakan akun baru menggunakan pabrik akun. Acara ini sesuai dengan `CreateManagedAccount` CloudTrail acara Menara Kontrol AWS. Log peristiwa siklus hidup mencakup `accountName` dan `accountId` dari akun yang baru dibuat, `organizationalUnitName` dan dan `organizationalUnitId` OU tempat akun ditempatkan.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                    // Management account
 ID.
    "time": "2018-08-30T21:42:18Z",                               // Format: yyyy-MM-
dd'T'hh:mm:ssZ
    "region": "us-east-1",                                        // AWS Control Tower
 home region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                      // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "CreateManagedAccount",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "createManagedAccountStatus": {
                "organizationalUnit":{
                    "organizationalUnitName":"Custom",
                    "organizationalUnitId":"ou-XXXX-l3zc8b3h"

                    },
                "account":{
                    "accountName":"LifeCycle1",
                    "accountId":"XXXXXXXXXXXX"
                    },
                "state":"SUCCEEDED",
                "message":"AWS Control Tower successfully created a managed account.",
                "requestedTimestamp":"2019-11-15T11:45:18+0000",
                "completedTimestamp":"2019-11-16T12:09:32+0000"}
```

```
        }
    }
}
```

UpdateManagedAccount

Peristiwa siklus hidup ini mencatat apakah AWS Control Tower berhasil memperbarui produk yang disediakan terkait dengan akun yang dibuat sebelumnya dengan menggunakan pabrik akun. Acara ini sesuai dengan `UpdateManagedAccount` CloudTrail acara Menara Kontrol AWS. Log peristiwa siklus hidup mencakup `accountName` dan `accountId` akun terkait, `organizationalUnitName` dan dan `organizationalUnitId` OU tempat akun yang diperbarui ditempatkan.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                    // AWS Control Tower
 organization management account.
    "time": "2018-08-30T21:42:18Z",                               // Format: yyyy-MM-
dd'T'hh:mm:ssZ
    "region": "us-east-1",                                        // AWS Control Tower
 home region.
    "resources": [],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                      // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "UpdateManagedAccount",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "updateManagedAccountStatus": {
```

```
                "organizationalUnit":{
                    "organizationalUnitName":"Custom",
                    "organizationalUnitId":"ou-XXXX-l3zc8b3h"
                    },
                "account":{
                    "accountName":"LifeCycle1",
                    "accountId":"XXXXXXXXXXXX"
                    },
                "state":"SUCCEEDED",
                "message":"AWS Control Tower successfully updated a managed account.",
                "requestedTimestamp":"2019-11-15T11:45:18+0000",
                "completedTimestamp":"2019-11-16T12:09:32+0000"}
        }
    }
}
```

EnableGuardrail

Peristiwa siklus hidup ini mencatat apakah AWS Control Tower berhasil mengaktifkan kontrol pada OU yang dikelola oleh AWS Control Tower. Acara ini sesuai dengan `EnableGuardrail` CloudTrail acara Menara Kontrol AWS. Log peristiwa siklus hidup mencakup `guardrailId` dan `guardrailBehavior` kontrol, `organizationalUnitName` dan dan `organizationalUnitId` OU tempat kontrol diaktifkan.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",                                 // End-time of action.
 Format: yyyy-MM-dd'T'hh:mm:ssZ
    "region": "us-east-1",                                          // AWS Control Tower
 home region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
```

```
        "eventSource": "controltower.amazonaws.com",
        "eventName": "EnableGuardrail",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "enableGuardrailStatus": {
                "organizationalUnits": [
                    {
                      "organizationalUnitName": "Custom",
                      "organizationalUnitId": "ou-vwxy-18vy4yro"
                    }
                  ],
                  "guardrails": [
                    {
                      "guardrailId": "AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK",
                      "guardrailBehavior": "DETECTIVE"
                    }
                  ],
                  "state": "SUCCEEDED",
                  "message": "AWS Control Tower successfully enabled a guardrail on an
 organizational unit.",
                  "requestTimestamp": "2019-11-12T09:01:07+0000",
                  "completedTimestamp": "2019-11-12T09:01:54+0000"
                }
        }
    }
}
```

DisableGuardrail

Peristiwa siklus hidup ini mencatat apakah AWS Control Tower berhasil menonaktifkan kontrol pada OU yang dikelola oleh AWS Control Tower. Acara ini sesuai dengan `DisableGuardrail` CloudTrail acara Menara Kontrol AWS. Log peristiwa siklus hidup mencakup `guardrailId` dan `guardrailBehavior` kontrol, dan `organizationalUnitName` dan `organizationalUnitId` OU tempat kontrol dinonaktifkan.

```
{
    "version": "0",
```

```
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "DisableGuardrail",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "disableGuardrailStatus": {
                   "organizationalUnits": [
                    {
                      "organizationalUnitName": "Custom",
                      "organizationalUnitId": "ou-vwxy-18vy4yro"
                    }
                  ],
                  "guardrails": [
                    {
                      "guardrailId": "AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK",
                      "guardrailBehavior": "DETECTIVE"
                    }
                  ],
                  "state": "SUCCEEDED",
                  "message": "AWS Control Tower successfully disabled a guardrail on an
 organizational unit.",
                  "requestTimestamp": "2019-11-12T09:01:07+0000",
                  "completedTimestamp": "2019-11-12T09:01:54+0000"
               }
            }
        }
```

```
    }
```

SetupLandingZone

Peristiwa siklus hidup ini mencatat apakah AWS Control Tower berhasil menyiapkan zona pendaratan. Acara ini sesuai dengan `SetupLandingZone` CloudTrail acara Menara Kontrol AWS. Log peristiwa siklus hidup mencakup`rootOrganizationalId`, yang merupakan ID organisasi yang dibuat AWS Control Tower dari akun manajemen. Entri log juga mencakup `organizationalUnitName` dan `organizationalUnitId` untuk setiap OU, dan `accountName` dan `accountId` untuk setiap akun, yang dibuat saat Menara Kontrol AWS menyiapkan zona pendaratan.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",                // Request ID.
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                   // Management account
 ID.
    "time": "2018-08-30T21:42:18Z",                              // Event time from
 CloudTrail.
    "region": "us-east-1",                                       // Management account
 CloudTrail region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",                         // Management-account
 ID.
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                     // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "SetupLandingZone",
        "awsRegion": "us-east-1",                                // AWS Control Tower
 home region.
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "CloudTrail_event_ID",                        // This value is
 generated by CloudTrail.
        "readOnly": false,
```

```
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "setupLandingZoneStatus": {
                "state": "SUCCEEDED",                                // Status of entire
 lifecycle operation.
                "message": "AWS Control Tower successfully set up a new landing zone.",

                "rootOrganizationalId" : "r-1234",
                "organizationalUnits" : [                            // Use a list.
                  {
                    "organizationalUnitName": "Security",             // Security OU
 name.
                    "organizationalUnitId": "ou-adpf-302pk332"    // Security OU ID.
                  },
                  {
                    "organizationalUnitName": "Custom",           // Custom OU name.
                    "organizationalUnitId": "ou-adpf-302pk332"    // Custom OU ID.
                  },
                ],
               "accounts": [                                         // All created
 accounts are here. Use a list of "account" objects.

                  {
                    "accountName": "Audit",
                    "accountId": "XXXXXXXXXXXX"
                  },
                  {
                    "accountName": "Log archive",
                    "accountId": "XXXXXXXXXXXX"
                  }
              ],
              "requestedTimestamp": "2018-08-30T21:42:18Z",
              "completedTimestamp": "2018-08-30T21:42:18Z"
            }
        }
    }
}
```

UpdateLandingZone

Peristiwa siklus hidup ini mencatat apakah AWS Control Tower berhasil memperbarui zona pendaratan Anda yang ada. Acara ini sesuai dengan `UpdateLandingZone` CloudTrail acara Menara Kontrol AWS. Log peristiwa siklus hidup mencakup`rootOrganizationalId`, yang

merupakan ID organisasi (diperbarui) yang diatur oleh AWS Control Tower. Entri log juga mencakup `organizationalUnitName` dan `organizationalUnitId` untuk setiap OU, dan `accountName` dan `accountId` untuk setiap akun, yang dibuat sebelumnya, ketika AWS Control Tower awalnya mengatur zona pendaratan.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",                // Request ID.
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",                                   // Management account
 ID.
    "time": "2018-08-30T21:42:18Z",                              // Event time from
 CloudTrail.
    "region": "us-east-1",                                       // Management account
 CloudTrail region.
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",                         // Management account
 ID.
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",                     // Timestamp when call
 was made. Format: yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "UpdateLandingZone",
        "awsRegion": "us-east-1",                                // AWS Control Tower
 home region.
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "CloudTrail_event_ID",                        // This value is
 generated by CloudTrail.

        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "updateLandingZoneStatus": {
                "state": "SUCCEEDED",                            // Status of entire
 operation.
                "message": "AWS Control Tower successfully updated a landing zone.",
```

```
                "rootOrganizationalId" : "r-1234",
                "organizationalUnits" : [                          // Use a list.
                  {
                    "organizationalUnitName": "Security",             // Security OU
 name.
                    "organizationalUnitId": "ou-adpf-302pk332"    // Security OU ID.
                  },
                  {
                    "organizationalUnitName": "Custom",            // Custom OU name.
                    "organizationalUnitId": "ou-adpf-302pk332"     // Custom OU ID.
                  },
                ],
               "accounts": [                                        // All created
 accounts are here. Use a list of "account" objects.

                  {
                    "accountName": "Audit",
                    "accountId": "XXXXXXXXXXXX"
                  },
                  {
                    "accountName": "Log archive",
                    "accountId": "XXXXXXXXXX"
                  }
              ],
              "requestedTimestamp": "2018-08-30T21:42:18Z",
              "completedTimestamp": "2018-08-30T21:42:18Z"
            }
        }
    }
}
```

RegisterOrganizationalUnit

Peristiwa siklus hidup ini mencatat apakah AWS Control Tower berhasil mengaktifkan fitur tata kelola pada OU. Acara ini sesuai dengan `RegisterOrganizationalUnit` CloudTrail acara Menara Kontrol AWS. Log peristiwa siklus hidup mencakup `organizationalUnitName` dan OU `organizationalUnitId` yang telah dibawa oleh AWS Control Tower di bawah pemerintahannya.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
```

```
    "source": "aws.controltower",
    "account": "123456789012",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "RegisterOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "registerOrganizationalUnitStatus": {
                "state": "SUCCEEDED",

                "message": "AWS Control Tower successfully registered an organizational
 unit.",

                "organizationalUnit" :
                  {
                    "organizationalUnitName": "Test",
                    "organizationalUnitId": "ou-adpf-302pk332"
                  }
                "requestedTimestamp": "2018-08-30T21:42:18Z",
                "completedTimestamp": "2018-08-30T21:42:18Z"
            }
        }
    }
}
```

DeregisterOrganizationalUnit

Peristiwa siklus hidup ini mencatat apakah AWS Control Tower berhasil menonaktifkan fitur tata kelola pada OU. Acara ini sesuai dengan `DeregisterOrganizationalUnit` CloudTrail acara

Menara Kontrol AWS. Log peristiwa siklus hidup mencakup `organizationalUnitName` dan `organizationalUnitId` OU tempat AWS Control Tower telah menonaktifkan fitur tata kelola.

```
{
    "version": "0",
    "id": "999cccaa-eaaa-0000-1111-123456789012",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "XXXXXXXXXXXX",
    "time": "2018-08-30T21:42:18Z",
    "region": "us-east-1",
    "resources": [ ],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "XXXXXXXXXXXX",
            "invokedBy": "AWS Internal"
        },
        "eventTime": "2018-08-30T21:42:18Z",
        "eventSource": "controltower.amazonaws.com",
        "eventName": "DeregisterOrganizationalUnit",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "0000000-0000-0000-1111-123456789012",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "deregisterOrganizationalUnitStatus": {
                "state": "SUCCEEDED",
                "message": "AWS Control Tower successfully de-registered an
 organizational unit.",
                "organizationalUnit" :
                  {
                    "organizationalUnitName": "Test",                   // Foundational
 OU name.
                    "organizationalUnitId": "ou-adpf-302pk332"          // Foundational
 OU ID.
                  },
                "requestedTimestamp": "2018-08-30T21:42:18Z",
                "completedTimestamp": "2018-08-30T21:42:18Z"
            }
            }
```

```
        }
    }
```

PrecheckOrganizationalUnit

Peristiwa siklus hidup ini mencatat apakah AWS Control Tower berhasil melakukan pemeriksaan awal pada OU. Acara ini sesuai dengan `PrecheckOrganizationalUnit` CloudTrail acara Menara Kontrol AWS. Log peristiwa siklus hidup berisi bidang untuk`Id`,, dan `failedPrechecks` nilai`Name`, untuk setiap sumber daya di mana AWS Control Tower telah melakukan pemeriksaan awal selama proses pendaftaran OU.

Log peristiwa juga berisi informasi tentang akun bersarang tempat pemeriksaan awal dilakukan, termasuk bidang, `accountName``accountId`, dan`failedPrechecks`.

Jika nil `failedPrechecks` ainya kosong, itu berarti bahwa semua precheck untuk sumber daya tersebut berhasil dilewati.

- Peristiwa ini dipancarkan hanya jika ada kegagalan precheck.
- Acara ini tidak dipancarkan jika Anda mendaftarkan OU kosong.

Contoh acara:

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "XXXXXXXXXXXX",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2021-09-20T22:45:43Z",
  "eventSource": "controltower.amazonaws.com",
  "eventName": "PrecheckOrganizationalUnit",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "eventID": "b41a9d67-0da4-4dc5-a87a-25fa19dc5305",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "XXXXXXXXXXXX",
  "serviceEventDetails": {
    "precheckOrganizationalUnitStatus": {
```

```
      "organizationalUnit": {
        "organizationalUnitName": "Ou-123",
        "organizationalUnitId": "ou-abcd-123456",
        "failedPrechecks": [
            "SCP_CONFLICT"
          ]
      },
      "accounts": [
        {
          "accountName": "Child Account 1",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": [
            "FAILED_TO_ASSUME_ROLE"
          ]
        },
        {
          "accountName": "Child Account 2",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": [
            "FAILED_TO_ASSUME_ROLE"
          ]
        },
        {
          "accountName": "Management Account",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": [
            "MISSING_PERMISSIONS_AF_PRODUCT"
          ]
        },
        {
          "accountName": "Child Account 3",
          "accountId": "XXXXXXXXXXXX",
          "failedPrechecks": []
        },
        ...
      ],
      "state": "FAILED",
      "message": "AWS Control Tower failed to register an organizational unit due to
 pre-check failures. Go to the OU details page to download a list of failed pre-checks
 for the OU and accounts within.",
      "requestedTimestamp": "2021-09-20T22:44:02+0000",
      "completedTimestamp": "2021-09-20T22:45:43+0000"
    }
  },
```

```
  "eventCategory": "Management"
}
```

EnableBaseline

Peristiwa siklus hidup ini mencatat apakah AWS Control Tower berhasil mengaktifkan baseline pada akun anggota target di bawah OU. Acara ini sesuai dengan Menara Kontrol AWS `RegisterOrganizationalUnit` atau `EnableBaseline` CloudTrail peristiwa. Log peristiwa siklus hidup mencakup baseline yang diaktifkan dan versinya, tempat baseline diaktifkan, baseline yang diaktifkan pada OU induk, dan `statusSummary` menampilkan status SUCCEED atau FAILED, bersama dengan parameter tambahan dan stempel waktu operasi. `targetIdentifier` `parentIdentifier`

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "XXXXXXXXXXXX",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2025-02-10T17:14:57Z",
    "eventSource": "controltower.amazonaws.com",
    "eventName": "EnableBaseline",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "366911a2-4fa6-4e4a-ac2b-280f627e0027",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
        "enableBaselineStatus": {
            "enabledBaselineDetails": {
                "arn": "arn:aws:controltower:us-east-2:XXXXXXXXXXXX:enabledbaseline/
XXXXXXXXXXXXXXXX",
                "parentIdentifier": "arn:aws:controltower:us-
east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXX",
                "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-
ern76xmzvf/XXXXXXXXXXXX",
```

```
                "baselineIdentifier": "arn:aws:controltower:us-east-2::baseline/
XXXXXXXXXXXXXX",
                "baselineVersion": "4.0",
                "statusSummary": {
                    "lastOperationIdentifier": "37f5eb68-e5b9-4c70-ae76-4ca15f6b16de",
                    "status": "SUCCEEDED"
                },
                "parameters": [
                    {
                        "key": "IdentityCenterEnabledBaselineArn",
                        "value": {
                            "untyped": {
                                "object": "arn:aws:controltower:us-
east-2:XXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXX"                            }
                        }
                    }
                ]
            },
            "requestedTimestamp": "2025-02-10T17:07:09+0000",
            "completedTimestamp": "2025-02-10T17:14:57+0000"
        }
    },
    "eventCategory": "Management"
}
```

ResetEnabledBaseline

Peristiwa siklus hidup ini mencatat apakah AWS Control Tower berhasil mengatur ulang baseline yang diaktifkan yang ada pada akun anggota target di bawah OU. Acara ini sesuai dengan Menara Kontrol AWS `RegisterOrganizationalUnit` atau `ResetEnabledBaseline` CloudTrail peristiwa. Log peristiwa siklus hidup mencakup baseline yang diaktifkan dan versinya, tempat baseline diaktifkan, baseline yang diaktifkan pada OU induk, dan `statusSummary` menampilkan status SUCCEED atau FAILED, bersama dengan parameter tambahan dan stempel waktu operasi. `targetIdentifier` `parentIdentifier`

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "XXXXXXXXXXXX",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2025-02-10T21:17:55Z",
```

```
    "eventSource": "controltower.amazonaws.com",
    "eventName": "ResetEnabledBaseline",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "c01a32e1-13ab-4b46-8f1b-00699ef6f989",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
        "resetEnabledBaselineStatus": {
            "enabledBaselineDetails": {
                "arn": "arn:aws:controltower:us-west-2:XXXXXXXXXXXX:enabledbaseline/
XXXXXXXXXXXXXXXX",
                "parentIdentifier": "arn:aws:controltower:us-
west-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXX",
                "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/
o-0uh2kplf6d/XXXXXXXXXXXX",
                "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/
XXXXXXXXXXXXXXX",
                "baselineVersion": "1.0",
                "statusSummary": {
                    "lastOperationIdentifier": "3e364c89-89fa-42b8-9776-9f7cc47ba1fa",
                    "status": "SUCCEEDED"
                },
                "parameters": []
            },
            "requestedTimestamp": "2025-02-10T21:14:24Z",
            "completedTimestamp": "2025-02-10T21:17:54+0000"
        }
    },
    "eventCategory": "Management"
}
```


UpdateEnabledBaseline

Peristiwa siklus hidup ini mencatat apakah AWS Control Tower berhasil memperbarui baseline yang diaktifkan yang ada pada akun anggota target di bawah OU. Acara ini sesuai dengan Menara Kontrol AWS `RegisterOrganizationalUnit` atau `UpdateEnabledBaseline` CloudTrail peristiwa. Log peristiwa siklus hidup mencakup baseline yang diaktifkan dan versinya, tempat baseline diaktifkan,

baseline yang diaktifkan pada OU induk, dan `statusSummary` menampilkan status SUCCEED atau FAILED, bersama dengan parameter tambahan dan stempel waktu operasi. `targetIdentifier` `parentIdentifier`


```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "XXXXXXXXXXXX",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2025-02-10T19:45:28Z",
    "eventSource": "controltower.amazonaws.com",
    "eventName": "UpdateEnabledBaseline",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "514f2aff-1a99-4912-bda1-0d4d6662c96e",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
        "updateEnabledBaselineStatus": {
            "enabledBaselineDetails": {
                "arn": "arn:aws:controltower:us-east-2:XXXXXXXXXXXX:enabledbaseline/
XXXXXXXXXXXXXXXX",
                "parentIdentifier": "arn:aws:controltower:us-
east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXX",
                "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-
ern76xmzvf/XXXXXXXXXXXX",
                "baselineIdentifier": "arn:aws:controltower:us-east-2::baseline/
XXXXXXXXXXXXXXX",
                "baselineVersion": "4.0",
                "statusSummary": {
                    "lastOperationIdentifier": "ba3de28f-83fb-4c9a-8a8c-a4e15fac2c41",
                    "status": "SUCCEEDED"
                },
                "parameters": [
                    {
                        "key": "IdentityCenterEnabledBaselineArn",
                        "value": {
```

```
                            "untyped": {
                                "object": "arn:aws:controltower:us-
east-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXX"                          }
                        }
                    }
                ]
            },
            "requestedTimestamp": "2025-02-10T19:39:35+0000",
            "completedTimestamp": "2025-02-10T19:45:28+0000"
        }
    },
    "eventCategory": "Management"
}
```

DisableBaseline

Peristiwa siklus hidup ini mencatat apakah AWS Control Tower berhasil menonaktifkan baseline yang diaktifkan yang ada pada akun anggota target di bawah OU. Acara ini sesuai dengan `DisableBaseline` CloudTrail acara Menara Kontrol AWS. Log peristiwa siklus hidup mencakup baseline yang diaktifkan dan versinya, tempat baseline diaktifkan, baseline yang diaktifkan pada OU induk, dan `statusSummary` menampilkan status SUCCEED atau FAILED, bersama dengan parameter tambahan dan stempel waktu operasi. `targetIdentifier` `parentIdentifier`

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "XXXXXXXXXXXX",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2025-03-14T00:50:58Z",
    "eventSource": "controltower.amazonaws.com",
    "eventName": "DisableBaseline",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "704794c4-a32e-4960-8386-c7efaa5a22a1",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
```

```
    "serviceEventDetails": {
        "disableBaselineStatus": {
            "enabledBaselineDetails": {
                "arn": "arn:aws:controltower:us-west-2:XXXXXXXXXXXX:enabledbaseline/
XXXXXXXXXXXXXXXX",
                "parentIdentifier": "arn:aws:controltower:us-
west-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXX",
                "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/
o-0uh2kplf6d/XXXXXXXXXXXX",
                "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/
XXXXXXXXXXXXXXX",
                "baselineVersion": "1.0",
                "statusSummary": {
                    "lastOperationIdentifier": "7b895594-0edb-48bc-9f3d-d88c2ad618df",
                    "status": "SUCCEEDED"
                },
                "parameters": []
            },
            "baselineDetails": {
                "arn": "arn:aws:controltower:us-west-2:XXXXXXXXXXXX:enabledbaseline/
XXXXXXXXXXXXXXXX",
                "parentIdentifier": "arn:aws:controltower:us-
west-2:XXXXXXXXXXXX:enabledbaseline/XXXXXXXXXXXXXXXX",
                "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/
o-0uh2kplf6d/XXXXXXXXXXXX",
                "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/
XXXXXXXXXXXXXXX",
                "baselineVersion": "1.0",
                "statusSummary": {
                    "lastOperationIdentifier": "7b895594-0edb-48bc-9f3d-d88c2ad618df",
                    "status": "SUCCEEDED"
                },
                "parameters": []
            },
            "requestedTimestamp": "2025-03-14T00:49:13Z",
            "completedTimestamp": "2025-03-14T00:50:58+0000"
        }
    },
    "eventCategory": "Management"
}
```

EnableControl

Peristiwa siklus hidup ini mencatat apakah AWS Control Tower berhasil mengaktifkan kontrol pada akun target yang dikelola oleh AWS Control Tower. Peristiwa ini sesuai dengan `EnableControl` CloudTrail peristiwa Menara Kontrol AWS, dan dipancarkan saat kontrol diaktifkan menggunakan `EnableControl` API atau konsol. Log peristiwa siklus hidup mencakup kontrol yang diaktifkan, kontrol yang diaktifkan yang dihasilkan, kontrol yang diaktifkan pada OU induk, tempat kontrol diaktifkan, dan `state` menampilkan status BERHASIL atau GAGAL, bersama dengan `message` a dan stempel waktu operasi. `controlIdentifier` `arn` `parentIdentifier` `targetIdentifier`

> **Note**
>
> Per `EnableControl` istiwa siklus hidup sesuai dengan `EnableControl` API. AWS Control Tower juga memancarkan peristiwa `EnableGuardrail` siklus hidup lama saat kontrol diaktifkan. Jika Anda membangun otomatisasi yang bereaksi terhadap kontrol yang diaktifkan, perhitungkan kedua nama acara.


```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "XXXXXXXXXXXX",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2026-01-07T15:59:28Z",
    "eventSource": "controltower.amazonaws.com",
    "eventName": "EnableControl",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "a4f45d0d-ab6d-41c7-9f97-786d80ff23d2",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
        "enableControlStatus": {
            "arn": "arn:aws:controltower:us-
east-1:XXXXXXXXXXXX:enabledcontrol/143RH67Q683RJ20V",
```

```
            "parentIdentifier": "arn:aws:controltower:us-
east-1:XXXXXXXXXXXX:enabledcontrol/8WU3TCOLC0JPSV6T",
            "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-
GR_AUDIT_BUCKET_LOGGING_ENABLED",
            "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-
k54j7iydcs/XXXXXXXXXXXX",
            "state": "SUCCEEDED",
            "message": "AWS Control Tower successfully enabled a control on the
 target.",
            "requestedTimestamp": "2026-01-07T15:59:24+0000",
            "completedTimestamp": "2026-01-07T15:59:28+0000"
        }
    },
    "eventCategory": "Management"
}
```

ResetEnabledControl

Peristiwa siklus hidup ini mencatat apakah AWS Control Tower berhasil mengatur ulang kontrol yang diaktifkan yang ada pada akun target yang dikelola oleh AWS Control Tower. Peristiwa ini sesuai dengan `ResetEnabledControl` CloudTrail peristiwa Menara Kontrol AWS, dan dipancarkan saat kontrol yang diaktifkan diatur ulang menggunakan `ResetEnabledControl` API atau konsol. Log peristiwa siklus hidup mencakup kontrol, kontrol yang diaktifkan, kontrol yang `parentIdentifier` diaktifkan pada OU induk, tempat kontrol diatur ulang, dan `state` menampilkan status BERHASIL atau GAGAL, bersama dengan `message` a dan stempel waktu operasi. `controlIdentifier` `arn` `targetIdentifier`

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "XXXXXXXXXXXX",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2026-01-07T16:10:42Z",
    "eventSource": "controltower.amazonaws.com",
    "eventName": "ResetEnabledControl",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "c82d6f3a-4b9e-43ca-8d21-1a3f8d5b62e9",
```

```
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
        "resetEnabledControlStatus": {
            "arn": "arn:aws:controltower:us-
east-1:XXXXXXXXXXXX:enabledcontrol/143RH67Q683RJ20V",
            "parentIdentifier": "arn:aws:controltower:us-
east-1:XXXXXXXXXXXX:enabledcontrol/8WU3TCOLC0JPSV6T",
            "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-
GR_AUDIT_BUCKET_LOGGING_ENABLED",
            "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-
k54j7iydcs/XXXXXXXXXXXX",
            "state": "SUCCEEDED",
            "message": "AWS Control Tower has successfully reset the enabled control on
 the target.",
            "requestedTimestamp": "2026-01-07T16:10:36+0000",
            "completedTimestamp": "2026-01-07T16:10:42+0000"
        }
    },
    "eventCategory": "Management"
}
```

UpdateEnabledControl

Peristiwa siklus hidup ini mencatat apakah AWS Control Tower berhasil memperbarui kontrol yang diaktifkan yang ada pada akun target yang dikelola oleh AWS Control Tower. Peristiwa ini sesuai dengan `UpdateEnabledControl` CloudTrail peristiwa Menara Kontrol AWS, dan dipancarkan saat kontrol yang diaktifkan diperbarui menggunakan `UpdateEnabledControl` API atau konsol. Log peristiwa siklus hidup mencakup kontrol, kontrol yang diaktifkan, kontrol yang diaktifkan pada OU induk, tempat kontrol diperbarui, dan `state` menampilkan status BERHASIL atau GAGAL, bersama dengan `message` a dan stempel waktu operasi. `controlIdentifier` `arn` `parentIdentifier` `targetIdentifier`

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "XXXXXXXXXXXX",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2026-01-07T16:25:19Z",
```

```
    "eventSource": "controltower.amazonaws.com",
    "eventName": "UpdateEnabledControl",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "d93e7a4b-5caf-44db-9e32-2b4a9e6c73fa",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
        "updateEnabledControlStatus": {
            "arn": "arn:aws:controltower:us-
east-1:XXXXXXXXXXXX:enabledcontrol/143RH67Q683RJ20V",
            "parentIdentifier": "arn:aws:controltower:us-
east-1:XXXXXXXXXXXX:enabledcontrol/8WU3TCOLC0JPSV6T",
            "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-
GR_AUDIT_BUCKET_LOGGING_ENABLED",
            "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-
k54j7iydcs/XXXXXXXXXXXX",
            "state": "SUCCEEDED",
            "message": "AWS Control Tower successfully updated the enabled control on
 the target.",
            "requestedTimestamp": "2026-01-07T16:25:13+0000",
            "completedTimestamp": "2026-01-07T16:25:19+0000"
        }
    },
    "eventCategory": "Management"
}
```


DisableControl

Peristiwa siklus hidup ini mencatat apakah AWS Control Tower berhasil menonaktifkan kontrol yang diaktifkan yang ada pada akun target yang dikelola oleh AWS Control Tower. Peristiwa ini sesuai dengan `DisableControl` CloudTrail peristiwa Menara Kontrol AWS, dan dipancarkan saat kontrol dinonaktifkan menggunakan `DisableControl` API atau konsol. Log peristiwa siklus hidup mencakup kontrol, kontrol yang diaktifkan, kontrol yang `parentIdentifier` diaktifkan pada OU induk, tempat kontrol dinonaktifkan, dan `state` menampilkan status BERHASIL atau GAGAL, bersama dengan `message` a dan stempel waktu operasi. `controlIdentifier` `arn` `targetIdentifier`

> **Note**
>
> AWS Control Tower juga memancarkan peristiwa `DisableGuardrail` siklus hidup lama saat kontrol dinonaktifkan. Jika Anda membangun otomatisasi yang bereaksi terhadap kontrol yang dinonaktifkan, perhitungkan kedua nama acara.


```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "accountId": "XXXXXXXXXXXX",
        "invokedBy": "AWS Internal"
    },
    "eventTime": "2026-01-07T16:42:11Z",
    "eventSource": "controltower.amazonaws.com",
    "eventName": "DisableControl",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "AWS Internal",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "e04f8b5c-6dba-45ec-af43-3c5b0f7d84ab",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "XXXXXXXXXXXX",
    "serviceEventDetails": {
        "disableControlStatus": {
            "arn": "arn:aws:controltower:us-
east-1:XXXXXXXXXXXX:enabledcontrol/143RH67Q683RJ20V",
            "parentIdentifier": "arn:aws:controltower:us-
east-1:XXXXXXXXXXXX:enabledcontrol/8WU3TCOLC0JPSV6T",
            "controlIdentifier": "arn:aws:controltower:us-east-1::control/AWS-
GR_AUDIT_BUCKET_LOGGING_ENABLED",
            "targetIdentifier": "arn:aws:organizations::XXXXXXXXXXXX:account/o-
k54j7iydcs/XXXXXXXXXXXX",
            "state": "SUCCEEDED",
            "message": "AWS Control Tower successfully disabled the enabled control on
 the target.",
            "requestedTimestamp": "2026-01-07T16:42:05+0000",
            "completedTimestamp": "2026-01-07T16:42:11+0000"
        }
```

```
    },
    "eventCategory": "Management"
}
```

Penggunaan AWS Pemberitahuan Pengguna dengan AWS Control Tower

Anda dapat menggunakan Pemberitahuan AWS Pengguna untuk mengatur saluran pengiriman agar diberi tahu tentang AWS Control Tower peristiwa. Anda akan menerima notifikasi saat ada sebuah peristiwa yang cocok dengan sebuah aturan yang Anda tentukan. Anda dapat menerima pemberitahuan untuk acara melalui beberapa saluran, termasuk email, Amazon Q Developer dalam pemberitahuan obrolan aplikasi obrolan, atau pemberitahuan push Aplikasi Seluler AWS Konsol. Anda juga dapat melihat notifikasi di Pusat Notifikasi Konsol.

AWS Pemberitahuan Pengguna mendukung agregasi, yang dapat mengurangi jumlah notifikasi yang Anda terima selama acara tertentu. Pemberitahuan juga terlihat di Pusat Pemberitahuan Konsol.

Keuntungan berlangganan notifikasi melalui Pemberitahuan AWS Pengguna alih-alih EventBridge meliputi:

- Antarmuka pengguna yang lebih ramah (UI).
- Integrasi dengan AWS konsol, di bell/notifications area pada bilah navigasi global.
- Dukungan asli untuk pemberitahuan email, tidak perlu mengatur Amazon SNS.
- Terutama, dukungan untuk pemberitahuan push seluler, eksklusif untuk Pemberitahuan AWS Pengguna.

Misalnya, salah satu jenis pemberitahuan yang mungkin ingin Anda terima adalah dalam kasus temuan kritis dan tingkat keparahan CSPM Security Hub CSPM. Cuplikan kode di JSON untuk mengatur langganan notifikasi mungkin terlihat seperti ini:

```
{
  "detail": {
    "findings": {
      "Compliance": {
        "Status": ["FAILED", "WARNING", "NOT_AVAILABLE"]
      },
      "RecordState": ["ACTIVE"],
```

```
      "Severity": {
        "Label": ["CRITICAL", "HIGH"]
      },
      "Workflow": {
        "Status": ["NEW", "NOTIFIED"]
      }
    }
  }
}
```

Pemfilteran peristiwa

- Anda dapat memfilter peristiwa berdasarkan layanan dan nama menggunakan filter yang tersedia di konsol Pemberitahuan AWS Pengguna.
- Anda dapat memfilter peristiwa berdasarkan properti tertentu jika Anda membuat EventBridge filter sendiri dari kode JSON.

Contoh AWS Control Tower acara

Berikut adalah contoh acara umum untuk AWS Control Tower.

- Ini sebuah EventBridge peristiwa.
- Anda dapat berlangganan EventBridge acara (seperti ini) menggunakan Pemberitahuan AWS Pengguna.

```
{
    "version": "0",
    "id": "<id>", // alphanumeric string
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.controltower",
    "account": "<account ID>", // Management account ID.
    "time": "<date>", // Format: yyyy-MM-dd'T'hh:mm:ssZ
    "region": "<region>", // AWS Control Tower home region.
    "resources": [],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "121212121212",
            "invokedBy": "AWS Internal"
        },
```

```
        "eventTime": "2018-08-30T21:42:18Z", // Timestamp when call was made. Format:
 yyyy-MM-dd'T'hh:mm:ssZ.
        "eventSource": "controltower.amazonaws.com",
        "eventName": "<event name>", // one of the event names listed in https://
docs.aws.amazon.com/controltower/latest/userguide/lifecycle-events.html
        "awsRegion": "<region>",
        "sourceIPAddress": "AWS Internal",
        "userAgent": "AWS Internal",
        "eventID": "<id>",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            // the contents of this object vary depending on the event subtype and
 event state
        }
    }
}
```

AWS Backup dan AWS Control Tower

AWS Backup adalah layanan yang memungkinkan Anda membuat rencana untuk mencadangkan AWS sumber daya Anda secara otomatis. Untuk menyiapkan cadangan sumber daya AWS Control Tower, Anda harus mengikuti empat langkah utama:

1. Aktifkan AWS Backup untuk landing zone Anda. Anda dapat melakukannya di halaman pengaturan zona pendaratan di konsol AWS Control Tower. Saat Anda menghidupkan AWS Backup, sumber daya dibuat di beberapa akun. Untuk informasi selengkapnya, lihat Sumber daya dibuat untuk AWS Backup.
2. Opt-in ke backup AWS Control Tower di konsol. AWS Backup Untuk informasi selengkapnya, lihat Bekerja dengan layanan yang didukung di Panduan AWS Backup Pengembang.
3. Aktifkan AWS Backup pada masing-masing OU yang ingin Anda sertakan. Anda dapat melakukan tugas ini di halaman detail OU di konsol, setelah Anda mengaktifkan AWS Backup di tingkat landing zone. Saat Anda mengaktifkan AWS Backup OU, akun di OU tersebut menerima AWS Backup brankas lokal.
4. Tandai sumber daya yang dipilih untuk disertakan dalam cadangan. Tag menunjukkan frekuensi backup untuk sumber daya itu. Rencana cadangan Anda mengikuti jadwal yang ditentukan oleh tag sumber daya pada setiap sumber daya.

Untuk informasi selengkapnya, lihat Panduan AWS Backup Pengembang. Tidak ada biaya yang dikeluarkan saat Anda mengonfigurasi AWS Backup dengan AWS Control Tower. Anda akan dikenakan biaya dari AWS Backup. Untuk informasi lebih lanjut tenngenai harga, lihat harga AWS Backup.

Untuk detail selengkapnya tentang AWS Backup sumber daya yang dibuat AWS Control Tower di landing zone AWS Control Tower Anda, lihat Sumber daya dibuat untuk AWS Backup

> **Note**
>
> AWS Control Tower tidak mendukung pengaturan paket cadangan untuk sumber daya AWS Control Tower melalui AWS Backup layanan secara langsung, tanpa juga mengaktifkannya di layanan AWS Control Tower.

Prasyarat

Sebelum Anda dapat mengatur AWS Backup sumber daya AWS Control Tower, Anda harus memiliki AWS Organizations organisasi yang sudah ada. Jika Anda telah menyiapkan zona landing zone AWS Control Tower, itu berfungsi sebagai organisasi Anda yang sudah ada.

Anda harus mengalokasikan atau membuat dua AWS akun lain yang tidak terdaftar di AWS Control Tower. Akun-akun ini menjadi akun cadangan pusat dan akun administrator cadangan. Beri nama akun ini dengan nama-nama itu.

Selain itu, Anda harus memilih atau membuat kunci Multi-region AWS Key Management Service (KMS), khusus untuk Backup AWS .

Mendefinisikan prasyarat Anda

- Akun cadangan pusat —Akun cadangan pusat menyimpan brankas cadangan AWS Control Tower dan pencadangan Anda. Vault ini dibuat di semua Wilayah AWS yang diatur AWS Control Tower, dalam akun ini. Cross-account salinan disimpan dalam akun ini, jika akun dikompromikan dan memerlukan pemulihan data.
- Akun administrator cadangan —Akun administrator cadangan adalah akun administrator yang didelegasikan untuk AWS Backup layanan di AWS Control Tower. Ini menyimpan rencana laporan Backup Audit Manager (BAM). Akun ini mengumpulkan semua data pemantauan cadangan, seperti memulihkan pekerjaan dan menyalin pekerjaan. Data disimpan dalam ember Amazon S3. Untuk informasi selengkapnya, lihat Membuat rencana laporan menggunakan AWS Backup konsol di Panduan AWS Backup Pengembang.
- Persyaratan kebijakan untuk kunci Multi-wilayah AWS KMS

  AWS KMS Kunci Anda membutuhkan kebijakan utama. Pertimbangkan kebijakan utama yang serupa dengan kebijakan ini, yang membatasi akses ke prinsipal (pengguna dan peran) yang memiliki izin yang terkait dengan akun manajemen organisasi Anda:

  JSON

```
{
    "Version":"2012-10-17",
    "Id": "KMS key policy",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
```

```
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow use of the KMS key for organization",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "kms:Decrypt",
                "kms:DescribeKey",
                "kms:GenerateDataKey*",
                "kms:Encrypt",
                "kms:ReEncrypt*",
                "kms:GetKeyPolicy",
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "ORGANIZATION-ID"
                }
            }
        }
    ]
}
```

Kebijakan contoh ini memberi semua akun di organisasi Anda akses ke data cadangan terenkripsi mereka. Gunakan kunci kondisi AWS global dan tombol AWS KMS kondisi untuk memperbaiki izin, tergantung pada prinsipal mana yang memerlukan akses ke cadangan Anda.

> **Note**
>
> AWS KMS Kunci multi-wilayah Anda harus direplikasi untuk setiap Wilayah AWS yang Anda rencanakan untuk diatur dengan AWS Control Tower. Anda harus menetapkan kebijakan

kunci pada setiap kunci replika Multi-wilayah. Untuk informasi tentang cara membuat kunci replika, lihat Membuat kunci replika Multi-wilayah.

Aktifkan cadangan

Anda dapat mengaktifkan pencadangan untuk sumber daya di akun yang terdaftar di AWS Control Tower, baik selama penyiapan landing zone, atau saat Anda memperbarui landing zone.

Sebagai Prasyarat, Anda harus memberikan item berikut

- An Akun AWS untuk berfungsi sebagai akun AWS Backup Administrator
- An Akun AWS untuk berfungsi sebagai akun Cadangan AWS Backup Pusat
- AWS KMS Kunci multi-wilayah yang Anda kelola, untuk pencadangan lintas akun

Cara mengaktifkan cadangan

Proses enablement memiliki dua bagian utama: pertama, aktifkan backup untuk landing zone Anda; kemudian, aktifkan backup untuk setiap OU terdaftar yang memerlukan backup.

Bagian pertama: Siapkan backup untuk landing zone

Konsol: Anda dapat mengatur cadangan untuk landing zone di konsol AWS Control Tower, di halaman pengaturan zona pendaratan. Anda akan melihat opsi ini selama operasi penyiapan landing zone awal, dan Anda dapat mengunjunginya kembali nanti dengan pembaruan landing zone.

API: Anda dapat mengaktifkan backup dengan AWS Control Tower API, dengan memanggil `UpdateLandingZone`API, jika Anda sudah memiliki landing zone AWS Control Tower, atau `CreateLandingZone`API jika Anda menyiapkan AWS Control Tower untuk pertama kalinya. (Petunjuk: Setelah itu, panggil `EnableBaseline`API untuk membuat cadangan untuk setiap OU yang Anda butuhkan.)

Di luar konsol AWS Control Tower

Bagian dari mengaktifkan backup untuk landing zone Anda mencakup langkah di luar konsol AWS Control Tower. Anda harus menavigasi ke AWS Backup konsol untuk meninjau sumber daya Anda.

Untuk meninjau jenis sumber daya yang Anda pilih atau ikut serta dalam jenis sumber daya tambahan

1. Buka AWS Backup konsol dihttps://console.aws.amazon.com/backup.
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Pada halaman keikutsertaan Layanan, pilih Konfigurasi sumber daya.
4. Gunakan sakelar sakelar untuk mengaktifkan atau menonaktifkan layanan yang ingin Anda sertakan. AWS BackupPastikan bahwa sumber daya yang ingin Anda cadangkan dipilih, seperti RDS, EC2, DDB, dan sebagainya, apakah itu bagian dari lingkungan AWS Control Tower Anda atau bukan.

Untuk detail selengkapnya, lihat Memilih untuk mengelola layanan dengan AWS Backup.

> **Pertimbangan untuk jenis sumber daya baru**
>
> Sebelum Anda mengandalkan AWS Backup untuk mengelola perlindungan data untuk sumber daya AWS layanan apa pun, Anda harus melakukan prosedur sebelumnya dan memilih AWS Backup untuk layanan itu. Selain itu, karena AWS Backup layanan menambahkan dukungan untuk layanan tambahan dan jenis sumber dayanya di masa mendatang, Anda harus mengulangi prosedur ini dan memilih untuk setiap jenis sumber daya tambahan AWS Backup sebelum Anda dapat mencadangkan jenis sumber daya tersebut di AWS Control Tower. Menandai jenis sumber daya yang tidak didukung dapat menyebabkan cadangan Anda gagal.

Saat Anda mengaktifkan cadangan untuk landing zone, AWS Control Tower menetapkan dua akun yang Anda berikan sebagai akun Cadangan Pusat dan akun Administrator Cadangan. AWS Control Tower membuat sumber daya di akun ini dan akun lainnya.

> **Important**
>
> Untuk mengaktifkan pencadangan untuk akun AWS Control Tower Audit dan Log Archive, Anda harus menyiapkan cadangan untuk OU Keamanan, dengan memanggil API. `EnableBaseline` Kami sarankan Anda melakukan juga.

Bank rencana dan retensi yang direkomendasikan adalah sebagai berikut:

- Pencadangan per jam = retensi 2 minggu di brankas lokal, tidak ada salinan di brankas cadangan pusat
- Pencadangan harian = retensi 2 minggu di brankas lokal, retensi 1 bulan di brankas cadangan pusat
- Pencadangan mingguan = retensi 1 bulan di brankas lokal, retensi 3 bulan di brankas pusat
- Pencadangan bulanan = retensi 3 bulan di brankas lokal, retensi 3 bulan di brankas cadangan pusat

Untuk informasi tentang cara membuat paket cadangan, lihat Membuat rencana laporan menggunakan AWS Backup konsol.

Bagian selanjutnya: Aktifkan cadangan di OU

Setelah Anda mengaktifkan AWS Backup pengaturan landing zone, Anda harus mengambil langkah tambahan untuk mengaktifkan cadangan pada OU tertentu yang ingin Anda cadangkan. Jika Anda telah mengaktifkan AWS Backup landing zone, Anda akan melihat bagian di halaman detail OU di konsol, yang memungkinkan Anda memilih Aktifkan cadangan untuk OU. Jika cadangan tidak diaktifkan di tingkat landing zone, Anda tidak akan melihat bagian ini di halaman rincian OU.

Untuk mengaktifkan `BackupBaseline` pada OU, OU itu harus sudah `AWSControlTowerBaseline` diaktifkan. Akun terdaftar di setiap OU telah `AWSControlTowerBaseline` diaktifkan.

Di akun dan OU yang Anda pilih, AWS Control Tower menyiapkan sumber daya tambahan

- Brankas Cadangan lokal

  AWS Control Tower membuat brankas cadangan lokal di akun Anda, dengan empat kemungkinan jenis paket cadangan yang dilampirkan ke vault. Paket Backup yang dibuat melalui AWS Control Tower ditandai dengan awalan.

```
BackupPlanTags:
        aws-control-tower: 'managed-by-control-tower'
```

- Empat jenis paket cadangan - per jam, harian, mingguan, bulanan.

  Setiap paket dikaitkan dengan penugasan sumber daya berbasis tag. Misalnya, sumber daya apa pun yang ditandai dengan aws-control-tower-backuphourly: true dilindungi dengan paket cadangan per jam.

- Peran cadangan lokal di akun Anda

  AWS Control Tower menciptakan peran IAM, yang digunakan untuk backup. Peran tersebut membutuhkan empat izin khusus.

  ```
  "backup:UpdateGlobalSettings","organizations:RegisterDelegatedAdministrator","organizations:E
  ```

  Peran tersebut memiliki hubungan kepercayaan dengan prinsipal layanan untuk AWS Backup Peran diberi nama`aws-controltower-backup-role`, dan memiliki izin terkelola berikut yang melekat padanya:

  - AWSBackupServiceRolePolicyForBackup
  - AWSBackupServiceRolePolicyForRestores
  - AWSBackupServiceRolePolicyForS3Backup
  - AWSBackupServiceRolePolicyForS3Restore

Tag sumber daya untuk cadangan

Bagian dari proses penyiapan backup di AWS Control Tower adalah menandai sumber daya yang ingin Anda sertakan dalam paket cadangan Anda. Tag menentukan frekuensi backup. Ini adalah tag yang mungkin.

- `aws-control-tower-backuphourly : true`
- `aws-control-tower-backupdaily: true`
- `aws-control-tower-backupweekly: true`
- `aws-control-tower-backupmonthly: true`

Pertimbangan-pertimbangan

- Saat AWS Backup aktif di OU, Anda akan melihat nilai Diaktifkan di bidang Status pada halaman detail OU di konsol AWS Control Tower. Beberapa nilai lain yang mungkin dari bidang Status termasuk Tidak diaktifkan, Sedang berlangsung, dan Gagal. Jika Anda melihat status Gagal, pilih Re-register OU untuk menerapkan kembali AWS Backup konfigurasi Anda ke OU.
- Jika Anda telah AWS Backup mengaktifkan OU, akun baru yang disediakan melalui Account Factory di bawah yang akan disertakan oleh OU. AWS Backup

Matikan cadangan

Anda dapat menonaktifkan pencadangan untuk sumber daya Anda di akun yang terdaftar di AWS Control Tower, baik selama penyiapan landing zone, atau saat Anda memperbarui landing zone.

Dua langkah utama diperlukan untuk mematikan backup: pertama, matikan AWS Backup baseline pada setiap OU yang memiliki backup diaktifkan, kemudian, matikan backup untuk landing zone Anda.

Langkah pertama: Matikan cadangan di OU

Jika AWS Backup diaktifkan, Anda harus menonaktifkan AWS Backup baseline dari semua OU sebelum Anda dapat mematikan AWS Backup untuk landing zone Anda.

Jika Anda memiliki OU bersarang, nonaktifkan baseline AWS Backup pada OU anak sebelum OU induk. Meskipun baseline AWS Backup masih diaktifkan pada OU anak, AWS Control Tower tidak dapat menonaktifkannya di OU induk.

Anda dapat menonaktifkan baseline AWS Backup pada OU dengan menggunakan AWS Control Tower API atau konsol AWS Control Tower.

Untuk menonaktifkan baseline AWS Backup (API)

Pertama, temukan ARN dari baseline AWS Backup. Panggil `ListBaselines` API dan kueri baseline yang akan mendapatkan `name` ARN-nya`BackupBaseline`.

```
aws controltower list-baselines --query 'baselines[?name==`BackupBaseline`]'
```

Kemudian, dengan menggunakan ARN itu, identifikasi OU mana yang mengaktifkan baseline AWS Backup. Panggil `ListEnabledBaselines` API, memfilter pada pengenal dasar, untuk menemukan setiap `BackupBaseline` baseline yang diaktifkan dan ARN-nya untuk dinonaktifkan. `enabledBaselineIdentifier`

```
aws controltower list-enabled-baselines --filter baselineIdentifiers=BackupBaseline-ARN
```

Untuk menonaktifkan baseline AWS Backup pada OU, Anda dapat memanggil API. `DisableBaseline`

Contoh perintah:

```
aws controltower disable-baseline --enabled-baseline-identifier Enabled-baseline-ARN
```

Untuk menonaktifkan baseline AWS Backup (konsol)

1. Masuk ke konsol AWS Control Tower dan navigasikan ke halaman Organisasi.
2. Pilih OU yang status dasar AWS Backup Diaktifkan untuk membuka halaman detail OU.
3. Di bagian Integrasi pada OU ini - opsional, di bawah AWS Backup, pilih Edit.
4. Pada dialog yang muncul, pilih Nonaktifkan, lalu pilih Konfirmasi.

Saat Anda menonaktifkan AWS Backup baseline, AWS Control Tower membersihkan sumber daya berikut:

- Semua stackset yang terkait dengan AWS Backup
- Semua kontrol yang terkait dengan AWS Backup

> **Note**
>
> Vault lokal dipertahankan meskipun stackset dihapus, karena kebijakan retensi pada vault lokal disetel ke. `Retain` Ini menyimpan data Anda.

Langkah selanjutnya: Matikan AWS Backup Untuk landing zone

Setelah prasyarat terpenuhi dengan mematikan cadangan ke OU Anda, untuk mematikan cadangan dari konsol AWS Control Tower, navigasikan ke halaman pengaturan zona pendaratan. Pilih Nonaktifkan cadangan.

Saat Anda mematikan AWS Backup, AWS Control Tower mengubah sumber daya berikut:

- Menghapus semua stackset yang terkait dengan AWS Backup
- Menonaktifkan semua kontrol yang terkait dengan AWS Backup dalam Keamanan OU
- De-registers akun admin yang didelegasikan untuk AWS Backup administrasi
- Menghapus tata kelola AWS Control Tower (untuk CloudTrail AWS Config,, dan sebagainya) dari akun AWS Backup Administrator dan Central Backup
- AWS Control Tower mempertahankan AWS Backup vault dan sumber daya bucket Amazon S3 yang berisi data Anda

Setelah Anda menonaktifkan cadangan, tidak ada cadangan baru yang dibuat, tetapi cadangan yang ada tidak dihapus.

Aktifkan pencadangan pada akun yang dipindahkan

Jika Anda memindahkan akun ke AWS Control Tower OU yang telah AWS Backup diaktifkan, dan akun tersebut tidak terdaftar di AWS Control Tower, paket pencadangan Anda tidak berlaku untuk akun secara otomatis.

Konsol: AWS Backup Untuk mengaktifkan akun individual dari konsol AWS Control Tower, Anda dapat memilih Perbarui akun di halaman Detail akun, atau Anda dapat memilih Re-register OU di halaman detail OU untuk memperbarui beberapa akun secara bersamaan.

API: Dari API, jika Anda memindahkan akun ke OU yang memiliki baseline cadangan diaktifkan, Anda dapat memanggil `ResetEnabledBaseline` API pada OU itu, menentukan `EnabledBaseline` sumber daya OU sebagai target, untuk memicu pencadangan pada akun dengan warisan dari OU.

Contoh perintah:

```
aws controltower reset-enabled-baseline --enabled-baseline-identifier
 arn:aws:controltower:REGION:NAMESPACE:enabledbaseline/XOSDORW8HDB5ZNWEE --region us-
east-1
```

Contoh respons:

```
{
        "operationIdentifier": "0bbdb587-c849-4152-95c6-7afa7664ee71"
}
```

Backup drift di AWS Control Tower

Drift tidak dilaporkan untuk AWS Backup konfigurasi di AWS Control Tower. Untuk informasi selengkapnya tentang drift di AWS Control Tower, lihat Mendeteksi dan menyelesaikan drift di AWS Control Tower.

Jika Anda menghapus atau memodifikasi AWS Backup paket, paket Anda dapat memasukkan status drift. Berikut adalah beberapa modifikasi yang harus dihindari.

- Jangan pindahkan akun Administrator Cadangan dari OU Keamanan.
- Jangan pindahkan akun Central Backup dari Security OU.
- Jangan hapus akun Administrator Cadangan dari organisasi.
- Jangan hapus akun Cadangan Pusat dari organisasi.
- Jangan lepaskan, lampirkan, atau perbarui AWS Backup SCP yang diterapkan pada OU Keamanan.
- Jangan lepaskan, lampirkan, atau perbarui AWS Backup SCP yang diterapkan ke OU lainnya.
- Jangan hapus izin akun Administrator Cadangan untuk AWS Backup.
- Jangan perbarui pengaturan cadangan lintas akun Anda untuk mematikan pencadangan lintas akun. Untuk informasi selengkapnya tentang pencadangan lintas akun, lihat *UpdateGlobalSettings*di Referensi API.AWS Backup
- Jangan hapus AWS KMS kunci Anda.
- Jangan mengubah kebijakan AWS KMS kunci Anda setelah disetel.
- Jangan menonaktifkan akses tepercaya layanan untuk AWS Backup.

> **Note**
>
> Drift dilaporkan mengenai status SCP-based kontrol yang melindungi AWS Backup sumber daya di AWS Control Tower.

Sumber daya dibuat untuk AWS Backup

Tabel di halaman ini menunjukkan sumber daya yang dibuat di akun AWS Control Tower saat Anda mengaktifkan AWS Backup.

Tabel berikut menunjukkan sumber daya yang dibuat AWS Control Tower di akun AWS Control Tower Central Backup saat Anda mengaktifkan AWS Backup organisasi landing zone.

Deskripsi	Sumber daya untuk akun Cadangan Pusat
OU mana yang berisi akun?	Keamanan OU
Tindakan apa yang menciptakan sumber daya?	Zona pendaratan Buat atau Perbarui

Deskripsi	Sumber daya untuk akun Cadangan Pusat
Sumber daya apa yang dibuat?	Brankas Cadangan Pusat— `aws-controltower-central-backupvault-*`
Wilayah apa saja yang termasuk?	Semua Wilayah yang diatur
Kontrol apa yang terkait dengan sumber daya ini?	`CT.BACKUP.PV.3`

Tabel berikut menunjukkan sumber daya yang dibuat AWS Control Tower di akun AWS Control Tower Backup Administrator saat Anda mengaktifkan AWS Backup organisasi landing zone.

Deskripsi	Sumber daya untuk akun Administrator Cadangan: Ini adalah akun administrator yang didelegasikan untuk AWS Backup
OU mana yang berisi akun?	Keamanan OU
Tindakan apa yang menciptakan sumber daya?	Zona pendaratan Buat atau Perbarui
Sumber daya apa yang dibuat?	Backup Audit Manager (BAM) • `aws_controltower_copy_report` • `aws_controltower_backup_report` • `aws_controltower_restore_report` Ember Amazon S3 untuk menyimpan log BAM — `aws-controltower-backup-reports-` *`{accountId}`* `-*` Bucket logging akses Amazon S3— `aws-controltower-backup-reports-log-` *`{accountId}`* `-*`
Wilayah apa saja yang termasuk?	Wilayah Asal

Deskripsi	Sumber daya untuk akun Administrator Cadangan: Ini adalah akun administrator yang didelegasikan untuk AWS Backup
Kontrol apa yang terkait dengan sumber daya ini?	• `CT.BACKUP.PV.2` • `CT.S3.PV.1` • `CT.S3.PV.1`

Tabel berikut menunjukkan sumber daya yang dibuat AWS Control Tower di akun AWS Control Tower Audit dan di akun AWS Control Tower Log Archive saat Anda mengaktifkan AWS Backup OU Keamanan.

Deskripsi	Sumber daya untuk akun Audit dan Arsip Log
OU mana yang berisi akun?	Keamanan OU
Tindakan apa yang menciptakan sumber daya?	Mengaktifkan `BackupBaseline`

Sumber daya apa yang dibuat?	• Brankas Cadangan Lokal— `aws-controltower-local-backupvault-*`
	• Peran Backup Lokal— `aws-controltower-BackupRole`
	• Empat paket Backup lokal (per jam, mingguan, bulanan, harian)
	  • `aws-controltower-hourly-backup-plan`
	  • `aws-controltower-daily-backup-plan`
	  • `aws-controltower-weekly-backup-plan`
	  • `aws-controltower-monthly-backup-plan`
	• Peran IAM— `aws-controltower-BackupRole`

Deskripsi	Sumber daya untuk akun Audit dan Arsip Log
Wilayah apa saja yang termasuk?	Semua Wilayah yang diatur
Kontrol apa yang terkait dengan sumber daya ini?	• `CT.BACKUP.PV.3` • `CT.IAM.PV.1` • `CT.BACKUP.PV.3` • `CT.BACKUP.PV.1`

> **Note**
>
> Saat Anda menerapkan `BackupBaseline` ke OU Keamanan, semua akun anggota di OU tersebut menerima AWS Backup sumber daya, bukan hanya akun Audit dan Arsip Log.

Tabel berikut menunjukkan sumber daya yang dibuat AWS Control Tower di akun anggota AWS Control Tower OU saat Anda AWS Backup mengaktifkan OU target.

Deskripsi	Sumber daya untuk akun anggota di lain OUs
OU mana yang berisi akun?	Setiap OU selain Keamanan OU
Tindakan apa yang menciptakan sumber daya?	Mengaktifkan `BackupBaseline`

Sumber daya apa yang dibuat?	• Brankas Cadangan Lokal— `aws-controltower-local-backupvault-*`
	• Peran Backup Lokal— `aws-controltower-BackupRole`
	• Empat paket Backup lokal (per jam, mingguan, bulanan, harian)
	  • `aws-controltower-hourly-backup-plan`
	  • `aws-controltower-daily-backup-plan`

Deskripsi	Sumber daya untuk akun anggota di lain OUs
	• `aws-controltower-weekly-backup-plan` • `aws-controltower-monthly-backup-plan` • Peran IAM— `aws-controltower-BackupRole`
Wilayah apa saja yang termasuk?	Semua Wilayah yang diatur
Kontrol apa yang terkait dengan sumber daya ini?	• `CT.BACKUP.PV.3` • `CT.IAM.PV.1` • `CT.BACKUP.PV.3` • `CT.BACKUP.PV.1`

Kontrol untuk AWS Pencadangan

Saat Anda mengaktifkan AWS Backup di zona landing zone AWS Control Tower, beberapa kontrol pencegahan diaktifkan di lingkungan Anda. Kontrol ini melindungi sumber daya yang AWS Backup perlu dioperasikan dengan AWS Control Tower. Anda tidak dapat mengaktifkan kontrol AWS Backup ini jika tidak diaktifkan untuk landing zone Anda.

Untuk informasi selengkapnya, lihat Kontrol untuk AWS Backup.

Menonaktifkan landing zone AWS Control Tower

AWS Control Tower memungkinkan Anda mengatur dan mengatur AWS lingkungan multi-akun yang aman, yang dikenal sebagai zona pendaratan. Proses pembersihan semua sumber daya yang dialokasikan oleh AWS Control Tower disebut sebagai penonaktifan landing zone.

Jika Anda tidak lagi ingin menggunakan AWS Control Tower, alat penonaktifan otomatis membersihkan sumber daya yang dialokasikan oleh AWS Control Tower. Untuk memulai proses penonaktifan otomatis, navigasikan ke halaman Pengaturan Zona Landing, pilih tab dekomisi, dan pilih Decommission landing zone.

Untuk daftar tindakan yang dilakukan selama penonaktifan, lihat. Ikhtisar proses penonaktifan

> **Warning**
>
> Menghapus semua sumber daya AWS Control Tower secara manual tidak sama dengan penonaktifan. Ini tidak akan memungkinkan Anda untuk mengatur landing zone baru.

Data Anda dan data Anda yang AWS Organizations ada tidak diubah oleh proses penonaktifan, dengan cara berikut.

- AWS Control Tower tidak menghapus data Anda, hanya menghapus bagian dari landing zone yang dibuatnya.
- Setelah proses penonaktifan selesai, beberapa artefak sumber daya tetap ada, seperti bucket Amazon S3 dan grup log Amazon Logs. CloudWatch Sumber daya ini harus dihapus secara manual sebelum Anda mengatur landing zone lain, dan untuk menghindari kemungkinan biaya yang terkait dengan pemeliharaan sumber daya tertentu.
- Anda tidak dapat menggunakan penonaktifan otomatis untuk menghapus landing zone yang telah diatur sebagian. Jika proses penyiapan landing zone Anda gagal, Anda harus menyelesaikan status kegagalan dan mengaturnya sepenuhnya untuk memungkinkan penonaktifan otomatis, atau Anda harus menghapus sumber daya secara manual satu per satu.

Menonaktifkan landing zone adalah proses dengan konsekuensi yang signifikan, dan tidak dapat dibatalkan. Tindakan penonaktifan yang dilakukan oleh AWS Control Tower dan artefak yang tersisa setelah penonaktifan dijelaskan di bagian berikut.

> **Important**
>
> Kami sangat menyarankan agar Anda melakukan proses dekomisioning ini hanya jika Anda berniat untuk berhenti menggunakan landing zone Anda. Tidak mungkin untuk membuat kembali landing zone yang ada setelah Anda menonaktifkannya.

Ikhtisar proses penonaktifan

Saat Anda meminta penonaktifan landing zone Anda, AWS Control Tower melakukan tindakan berikut.

- Menonaktifkan setiap kontrol detektif diaktifkan di landing zone. AWS Control Tower menghapus CloudFormation sumber daya yang mendukung kontrol.
- Menonaktifkan setiap kontrol preventif dengan menghapus kebijakan kontrol layanan (SCP) dari. AWS Organizations Jika kebijakan kosong (yang seharusnya dilakukan setelah menghapus semua SCP yang dikelola oleh AWS Control Tower), AWS Control Tower melepaskan dan menghapus kebijakan sepenuhnya.
- Menghapus semua cetak biru yang digunakan sebagai. CloudFormation StackSets
- Menghapus semua cetak biru yang digunakan sebagai CloudFormation Tumpukan di semua Wilayah.
- Untuk setiap akun yang disediakan, AWS Control Tower melakukan tindakan berikut selama proses penonaktifan.
  - Menghapus catatan dari setiap akun akun pabrik.
  - Mencabut izin AWS Control Tower ke akun dengan menghapus peran IAM yang dibuat AWS Control Tower (kecuali kebijakan tambahan telah ditambahkan ke dalamnya) dan membuat ulang peran IAM standar. `OrganizationAccountAccessRole`
  - Menghapus catatan akun dari AWS Service Catalog.
  - Menghapus produk dan portofolio akun pabrik dari AWS Service Catalog.
- Menghapus cetak biru untuk akun bersama (Audit dan Arsip Log).
- Mencabut izin AWS Control Tower dari akun bersama dengan menghapus peran IAM yang dibuat AWS Control Tower (kecuali kebijakan tambahan telah ditambahkan ke dalamnya) dan membuat ulang peran IAM. `OrganizationAccountAccessRole`
- Menghapus catatan yang terkait dengan akun bersama.

- Menghapus catatan yang terkait dengan OU yang dibuat pelanggan.
- Menghapus catatan internal yang mengidentifikasi Wilayah asal.

> **Note**
>
> Setelah dinonaktifkan, Anda mungkin ingin menghapus cetak biru Account Factory VPC (`BP_ACCOUNT_FACTORY_VPC`) untuk membersihkan rute dan gateway NAT, jika VPC Anda tidak kosong.

Cara menonaktifkan landing zone

Untuk menonaktifkan landing zone AWS Control Tower Anda dari konsol, ikuti prosedur yang diberikan di sini.

> **Note**
>
> Kami menyarankan Anda membatalkan kelola akun terdaftar Anda sebelum dinonaktifkan.

1. Jika baseline AWS Backup diaktifkan pada OU yang terdaftar, nonaktifkan pada setiap OU yang diaktifkan sebelum Anda menonaktifkan landing zone Anda. Jika tidak, penonaktifan gagal. Untuk petunjuk, lihat the section called “Langkah pertama: Matikan cadangan di OU”.

   Jika penonaktifan gagal karena alasan ini, Anda dapat menonaktifkan baseline AWS Backup dan menjalankan penonaktifan lagi.
2. Arahkan ke halaman Pengaturan Zona Landing di konsol AWS Control Tower.
3. Pilih Donaktifkan landing zone Anda di bagian Donaktifkan landing zone Anda.
4. Dialog muncul, menjelaskan tindakan yang akan Anda lakukan, dengan proses konfirmasi yang diperlukan. Untuk mengonfirmasi maksud Anda untuk menonaktifkan, Anda harus memilih setiap kotak dan mengetik konfirmasi seperti yang diminta.

   > **Important**
   >
   > Proses dekomisioning tidak dapat dibatalkan.

5. Jika Anda mengonfirmasi maksud Anda untuk menonaktifkan landing zone, Anda akan diarahkan ke halaman beranda AWS Control Tower saat penonaktifan sedang berlangsung. Prosesnya mungkin membutuhkan waktu hingga dua jam.

   Jangan menutup akun anggota apa pun di organisasi Anda saat penonaktifan sedang berlangsung. Penonaktifan mungkin gagal.

6. Ketika penonaktifan telah berhasil, Anda harus menghapus sumber daya yang tersisa secara manual sebelum menyiapkan landing zone baru dari konsol AWS Control Tower. Sumber daya yang tersisa ini mencakup beberapa bucket Amazon S3 tertentu, organisasi, dan grup CloudWatch log Log.

   > **Note**
   >
   > Tindakan ini mungkin memiliki konsekuensi signifikan untuk aktivitas penagihan dan kepatuhan Anda. Misalnya, kegagalan untuk menghapus sumber daya ini dapat mengakibatkan biaya yang tidak terduga.

   Untuk informasi selengkapnya tentang cara menghapus sumber daya secara manual, lihatTentang menghapus sumber daya AWS Control Tower.

7. Jika Anda berniat untuk membuat landing zone baru di AWS Wilayah baru, ikuti langkah tambahan ini. Masukkan perintah berikut melalui CLI:

   ```
   aws organizations disable-aws-service-access --service-principal
    controltower.amazonaws.com
   ```

Nonaktifkan landing zone Anda dengan API

Proses membersihkan semua sumber daya zona pendaratan disebut sebagai penonaktifan landing zone.

> **Important**
>
> Kami sangat menyarankan agar Anda melakukan proses dekomisioning ini hanya jika Anda berniat untuk berhenti menggunakan landing zone Anda. Tidak mungkin untuk membuat kembali landing zone yang ada setelah Anda menonaktifkannya.

Untuk detail selengkapnya tentang penonaktifan landing zone, termasuk informasi penting tentang cara AWS Control Tower menangani data Anda dan yang ada AWS Organizations, tinjau. Menonaktifkan landing zone AWS Control Tower

Untuk menonaktifkan landing zone, panggil `DeleteLandingZone` API. API ini mengembalikan sebuah`OperationIdentifier`, yang kemudian dapat Anda gunakan saat memanggil `GetLandingZoneOperation` API untuk memeriksa status operasi penghapusan.

```
aws controltower delete-landing-zone --landing-zone-identifier
"arn:aws:controltower:us-west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H"
```

Output:

```
{
   "operationIdentifier": "55XXXXXX-e2XX-41XX-a7XX-446XXXXXXXXX"
}
```

Tugas pembersihan manual diperlukan setelah dinonaktifkan

Bagian ini mencantumkan tugas pembersihan manual yang harus Anda lakukan setelah langkah penonaktifan awal.

- Anda harus menentukan alamat email yang berbeda untuk arsip Log dan akun Audit jika Anda membuat landing zone baru setelah menonaktifkannya, atau mengikuti prosedur untuk membawa arsip Log atau akun Audit Anda sendiri yang ada.
- Grup CloudWatch log log,`aws-controltower/CloudTrailLogs`, harus dihapus secara manual sebelum Anda mengatur landing zone lain.
- Dua bucket Amazon S3 dengan nama yang dicadangkan untuk log harus dihapus, atau diganti namanya, secara manual.
- Anda harus menghapus, atau mengganti nama, unit organisasi Security dan Sandbox yang ada secara manual.

> **Note**
>
> Sebelum Anda dapat menghapus organisasi AWS Control Tower Security OU, Anda harus terlebih dahulu menghapus akun logging dan audit, tetapi bukan akun manajemen. Untuk menghapus akun ini, Anda harus Kapan harus masuk sebagai pengguna root ke akun audit dan ke akun logging dan menghapusnya satu per satu.

- Anda mungkin ingin menghapus konfigurasi AWS IAM Identity Center (IAM Identity Center) untuk AWS Control Tower secara manual, tetapi Anda dapat melanjutkan dengan konfigurasi IAM Identity Center yang ada.
- Anda mungkin ingin menghapus VPC yang dibuat oleh AWS Control Tower, dan menghapus kumpulan AWS CloudFormation tumpukan terkait.
- Sebelum Anda dapat mengatur landing zone baru di AWS Wilayah baru, Anda harus mengikuti langkah-langkah tambahan ini.
  - Masukkan perintah berikut melalui CLI:

    ```
    aws organizations disable-aws-service-access --service-principal
     controltower.amazonaws.com
    ```

  - Hapus aturan terkelola yang tersisa`AWSControlTowerManagedRule`, yang dipanggil, dari akun bersama dan anggota untuk semua Wilayah yang diatur. `AWSControlTowerManagedRule`adalah EventBridge aturan Amazon.

Sumber daya tidak dihapus selama penonaktifan

Menonaktifkan landing zone tidak sepenuhnya membalikkan proses penyiapan AWS Control Tower. Sumber daya tertentu tetap ada, yang dapat dihapus secara manual.

AWS Organizations

Untuk pelanggan tanpa AWS Organizations organisasi yang ada, AWS Control Tower menyiapkan organisasi dengan satu atau lebih unit organisasi (OU). OU Keamanan yang ditunjuk dan secara opsional dibuat Sandbox OU. Saat Anda menonaktifkan landing zone Anda, hierarki organisasi dipertahankan, sebagai berikut:

- Unit Organisasi (OU) yang Anda buat dari konsol AWS Control Tower tidak dihapus.
- Keamanan dan Sandbox OU tidak dihapus.

- Organisasi tidak dihapus dari AWS Organizations.
- Tidak ada akun di AWS Organizations (bersama, disediakan, atau manajemen) yang dipindahkan atau dihapus.

AWS IAM Identity Center (SSO)

Untuk pelanggan tanpa direktori IAM Identity Center yang ada, AWS Control Tower menyiapkan IAM Identity Center dan mengonfigurasi direktori awal. Saat Anda menonaktifkan landing zone, AWS Control Tower tidak membuat perubahan pada IAM Identity Center. Jika diperlukan, Anda dapat menghapus informasi Pusat Identitas IAM yang disimpan di akun manajemen Anda secara manual. Secara khusus, area ini tidak berubah dengan menonaktifkan:

- Pengguna yang dibuat dengan Account Factory tidak akan dihapus.
- Grup yang dibuat oleh penyiapan AWS Control Tower tidak dihapus.
- Set izin yang dibuat oleh AWS Control Tower tidak dihapus.
- Asosiasi antara AWS akun dan kumpulan izin Pusat Identitas IAM tidak dihapus.
- Direktori IAM Identity Center tidak diubah.
- Kebijakan Pusat Identitas IAM untuk AWS Control Tower ini tidak dihapus:
  - `AWSControlTowerAdminPolicy`
  - `AWSControlTowerCloudTrailRolePolicy`
  - `AWSControlTowerStackSetRolePolicy`

Peran

Selama penyiapan, AWS Control Tower membuat peran tertentu untuk Anda jika Anda menggunakan konsol, atau meminta Anda untuk membuat peran ini jika Anda menyiapkan landing zone melalui API. Saat Anda menonaktifkan landing zone, peran berikut tidak akan dihapus:

- `AWSControlTowerAdmin`
- `AWSControlTowerCloudTrailRole`
- `AWSControlTowerStackSetRole`
- `AWSControlTowerConfigAggregatorRoleForOrganizations`

> **Note**
>
> `AWSControlTowerExecution`Peran dalam akun anggota akan dihapus saat landing zone dihapus, baik AWS Control Tower membuat peran atas nama Anda atau jika Anda membuat peran secara manual. Namun, jika Anda telah melampirkan kebijakan tambahan pada peran ini, atau mengubah kebijakan yang dilampirkan pada peran ini, AWS Control Tower mungkin tidak dapat menghapus peran ini selama penghapusan Zona Pendaratan. Untuk kasus seperti itu, penghapusan Zona Pendaratan akan berhasil tetapi peran akan dipertahankan di akun anggota Anda.

Bucket Amazon S3

Selama penyiapan, AWS Control Tower membuat bucket di akun arsip log untuk AWS CloudTrail dan di akun agregator pusat konfigurasi untuk integrasi AWS Config. AWS Control Tower membuat bucket untuk logging dan untuk akses logging di masing-masing akun ini. Saat Anda menonaktifkan landing zone, sumber daya berikut tidak akan dihapus:

- Logging dan logging access S3 bucket di akun arsip log tidak dihapus.
- Bucket S3 akses logging dan logging di akun agregator pusat konfigurasi tidak dihapus.
- Isi bucket akses logging dan logging di masing-masing akun ini tidak dihapus.

Integrasi layanan Akun

AWS Control Tower mengharuskan setiap konfigurasi integrasi layanan memiliki akun pusat. Akun ini mungkin atau mungkin tidak dibuat selama penyiapan AWS Control Tower berdasarkan versi landing zone. Saat Anda menonaktifkan landing zone Anda:

- Akun integrasi layanan yang dibuat selama penyiapan AWS Control Tower tidak ditutup.
- Peran `OrganizationAccountAccessRole` IAM dibuat ulang untuk menyelaraskan dengan konfigurasi standar. AWS Organizations
- `AWSControlTowerExecution`Peran dihapus.

Akun yang Disediakan

Pelanggan AWS Control Tower dapat menggunakan akun pabrik untuk membuat AWS akun baru. Saat Anda menonaktifkan landing zone Anda:

- Akun yang disediakan yang Anda buat dengan Account Factory tidak ditutup.
- Produk yang disediakan tidak AWS Service Catalog dihapus. Jika Anda membersihkannya dengan menghentikannya, akun mereka dipindahkan ke Root OU.
- VPC yang dibuat AWS Control Tower tidak dihapus, dan AWS CloudFormation stack set (`BP_ACCOUNT_FACTORY_VPC`) terkait tidak dihapus.
- Peran `OrganizationAccountAccessRole` IAM dibuat ulang untuk menyelaraskan dengan konfigurasi standar. AWS Organizations
- `AWSControlTowerExecution`Peran dihapus.

CloudWatch Grup Log Log

- Sebuah grup CloudWatch log log,`aws-controltower/CloudTrailLogs`, dibuat sebagai bagian dari cetak biru bernama. `AWSControlTowerBP-BASELINE-CLOUDTRAIL-MASTER` Grup log ini tidak dihapus. Sebaliknya, cetak biru dihapus dan sumber daya dipertahankan.

> **Note**
>
> Pelanggan di landing zone 3.0 dan yang lebih baru tidak perlu menghapus log akun dan CloudTrail CloudTrail log peran masing-masing yang terdaftar, karena ini dibuat di akun manajemen saja, untuk jejak tingkat organisasi.
> Dimulai dengan landing zone versi 3.2, AWS Control Tower membuat EventBridge aturan Amazon, yang disebut`AWSControlTowerManagedRule`. Aturan ini dibuat di setiap akun anggota, untuk semua Wilayah yang diatur. Aturan tidak dihapus secara otomatis selama penonaktifan, jadi Anda harus menghapusnya secara manual dari akun integrasi layanan dan akun anggota untuk semua Wilayah yang diatur sebelum Anda dapat mengatur landing zone di Wilayah baru.

Prosedur untuk cara menghapus sumber daya AWS Control Tower diberikan dalamHapus sumber daya AWS Control Tower.

Hapus sumber daya AWS Control Tower

Dokumen ini memberikan petunjuk tentang cara menghapus sumber daya AWS Control Tower secara individual, sebagai bagian dari tugas pemeliharaan dan administrasi rutin. Prosedur yang

diberikan dalam pasal ini dimaksudkan hanya untuk menghilangkan sumber daya individu, atau beberapa sumber daya, bila diperlukan. Ini tidak sama dengan menonaktifkan landing zone Anda.

Dua jenis tugas mungkin mengharuskan Anda untuk menghapus sumber daya:

- Untuk menghapus sumber daya saat Anda mengelola landing zone dalam situasi biasa.
- Untuk membersihkan sumber daya yang tersisa setelah penonaktifan otomatis.

> **Warning**
>
> Menghapus sumber daya secara manual tidak akan memungkinkan Anda untuk mengatur landing zone baru. Ini tidak sama dengan penonaktifan. Jika Anda berniat untuk menonaktifkan landing zone AWS Control Tower Anda, ikuti petunjuk Menonaktifkan landing zone AWS Control Tower sebelum Anda mengambil tindakan apa pun yang dijelaskan dalam Bab ini. Petunjuk dalam Bab ini dapat membantu Anda membersihkan sumber daya yang tersisa setelah penonaktifan otomatis selesai. Bahkan jika Anda menghapus semua sumber daya landing zone Anda secara manual, itu tidak sama dengan menonaktifkan landing zone, dan Anda mungkin dikenakan biaya tak terduga.

Jika Anda perlu menghapus akun dari AWS Control Tower, lihat bagian berikut untuk menutup akun:

- Batalkan kelola akun
- Menutup akun yang dibuat di Account Factory

Apakah saya perlu menonaktifkan alih-alih menghapus?

Jika Anda tidak lagi berniat menggunakan AWS Control Tower untuk perusahaan Anda, atau jika Anda memerlukan pemindahan besar-besaran sumber daya organisasi Anda, Anda mungkin ingin menonaktifkan sumber daya yang dibuat saat pertama kali menyiapkan landing zone Anda.

- Setelah proses penonaktifan selesai, beberapa artefak sumber daya tetap ada, seperti bucket Amazon S3 dan grup log Amazon Logs. CloudWatch
- Anda harus membersihkan sumber daya yang tersisa di akun Anda secara manual sebelum menyiapkan landing zone lain, dan untuk menghindari kemungkinan biaya tak terduga. Untuk informasi selengkapnya, lihat Sumber daya tidak dihapus selama penonaktifan.

> **Warning**
>
> Kami sangat menyarankan agar Anda melakukan proses dekomisioning hanya jika Anda berniat untuk berhenti menggunakan landing zone Anda. Proses ini tidak dapat dibatalkan.

Tentang menghapus sumber daya AWS Control Tower

Prosedur individual dalam Bab ini memandu Anda melalui metode manual untuk menghapus sumber daya AWS Control Tower. Prosedur ini dapat diikuti ketika Anda perlu menghapus sumber daya tertentu dari landing zone Anda.

Sebelum melakukan prosedur ini, kecuali dinyatakan lain, Anda harus masuk ke Wilayah asal untuk landing zone Anda, dan Anda harus masuk sebagai pengguna IAM atau pengguna di IAM Identity Center dengan izin administratif untuk akun manajemen yang berisi landing zone Anda. Konsol Manajemen AWS

> **Warning**
>
> Ini adalah tindakan destruktif yang dapat memperkenalkan penyimpangan tata kelola ke penyiapan AWS Control Tower Anda. Mereka tidak bisa dibatalkan.

Topik

- Hapus SCPs
- Hapus StackSets dan Tumpukan
- Hapus Bucket Amazon S3 di Akun Arsip Log
- Menghapus Portofolio dan Produk Account Factory
- Hapus Peran dan Kebijakan AWS Control Tower
- Bantuan sumber daya AWS Control Tower

Hapus SCPs

AWS Control Tower menggunakan kebijakan kontrol layanan (SCPs) untuk kontrolnya. Prosedur ini membahas cara menghapus yang SCPs secara khusus terkait dengan AWS Control Tower.

Untuk menghapus AWS Organizations SCPs

1. Buka konsol Organizations di https://console.aws.amazon.com/organizations/.
2. Buka tab Policies, dan temukan Service Control Policies (SCPs) yang memiliki awalan aws-guardrails- dan lakukan hal berikut untuk setiap SCP:
    a. Lepaskan SCP dari OU terkait.
    b. Hapus SCP.

Hapus StackSets dan Tumpukan

AWS Control Tower menggunakan StackSets dan menumpuk untuk menerapkan Aturan AWS Config terkait dengan kontrol di landing zone Anda. Prosedur berikut berjalan melalui cara menghapus sumber daya khusus ini.

Untuk menghapus CloudFormation StackSets

1. Buka CloudFormation konsol di https://console.aws.amazon.com/cloudformation.
2. Dari menu navigasi kiri, pilih StackSets.
3. Untuk masing-masing StackSet dengan awalan AWSControlTower, lakukan hal berikut. Jika Anda memiliki banyak akun di a StackSet, ini bisa memakan waktu.
    a. Pilih yang spesifik StackSet dari tabel di dasbor. Ini membuka halaman properti untuk itu StackSet.
    b. Di bagian bawah halaman, di tabel Stacks, buat catatan AWS akun IDs untuk semua akun di tabel. Salin daftar semua akun.
    c. Dari Tindakan, pilih Hapus tumpukan dari StackSet.
    d. Pada Setel opsi penerapan, dari lokasi Deployment, pilih Menerapkan tumpukan di akun.
    e. Di bidang teks, masukkan AWS akun yang IDs Anda buat catatan di langkah 3.b, dipisahkan dengan koma. Misalnya: *123456789012*, *098765431098*, dan seterusnya.
    f. Dari Tentukan wilayah, pilih Tambahkan semua, biarkan parameter lainnya di halaman diatur ke defaultnya, dan pilih Berikutnya.
    g. Pada halaman Ulasan, tinjau pilihan Anda, lalu pilih Hapus tumpukan.
    h. Pada halaman StackSet properti, Anda dapat memulai prosedur ini lagi untuk yang lain StackSets.

4. Proses ini selesai ketika catatan dalam tabel Stacks dari halaman StackSets properti yang berbeda kosong.
5. Ketika catatan dalam tabel Stacks kosong, pilih Hapus StackSet.

Untuk menghapus CloudFormation tumpukan

1. Buka CloudFormation konsol di https://console.aws.amazon.com/cloudformation.
2. Dari dasbor Stacks, cari semua tumpukan dengan awalan AWSControl Tower.
3. Untuk setiap tumpukan dalam tabel, lakukan hal berikut:
   a. Pilih kotak centang di sebelah nama tumpukan.
   b. Dari menu Actions, pilih Delete Stack.
   c. Di kotak dialog yang terbuka, tinjau informasi untuk memastikannya akurat, dan pilih Ya, Hapus.

Hapus Bucket Amazon S3 di Akun Arsip Log

Prosedur berikut memandu Anda melalui cara masuk ke akun arsip log sebagai pengguna Pusat Identitas IAM di AWSControlTowerExecutiongrup dan kemudian menghapus bucket Amazon S3 di akun arsip log Anda.

Untuk masuk ke akun arsip log Anda dengan izin yang tepat

1. Buka konsol Organizations di https://console.aws.amazon.com/organizations/.
2. Dari tab Akun, temukan akun Arsip Log.
3. Dari panel kanan yang terbuka, buat catatan nomor akun arsip log.
4. Dari bilah navigasi, pilih nama akun Anda untuk membuka menu akun Anda.
5. Pilih Ganti Peran.
6. Pada halaman yang terbuka, berikan nomor akun untuk akun arsip log di Akun.
7. Untuk Peran, masukkan AWSControlTowerExecution.
8. Nama Tampilan diisi dengan teks.
9. Pilih Warna favorit Anda.
10. Pilih Ganti Peran.

Untuk menghapus ember Amazon S3

1. Buka konsol Amazon S3 di. https://console.aws.amazon.com/s3/
2. Cari nama bucket yang berisi aws-controltower.
3. Untuk setiap ember di tabel, lakukan hal berikut:
   a. Pilih kotak centang untuk ember di tabel.
   b. Pilih Hapus.
   c. Di kotak dialog yang terbuka, tinjau informasi untuk memastikannya akurat, masukkan nama bucket untuk mengonfirmasi, lalu pilih Konfirmasi.

Menghapus Portofolio dan Produk Account Factory

Prosedur berikut memandu Anda melalui cara masuk sebagai pengguna IAM Identity Center di AWSServiceCatalogAdminsgrup dan kemudian membersihkan portofolio dan produk Account Factory Anda.

Untuk masuk ke akun manajemen Anda dengan izin yang tepat

1. Buka URL portal pengguna Anda di *directory-id* .awsapps.com/start
2. Dari AWS Akun, temukan akun Manajemen.
3. Dari AWSServiceCatalogAdminFullAccess, pilih Konsol manajemen untuk masuk ke peran Konsol Manajemen AWS sebagai ini.

Untuk membersihkan Account Factory

1. Buka konsol Service Catalog di https://console.aws.amazon.com/servicecatalog/.
2. Dari menu navigasi kiri, pilih daftar Portofolio.
3. Dalam tabel Portofolio Lokal, cari portofolio bernama AWS Control Tower Account Factory Portfolio.
4. Pilih nama portofolio itu untuk membuka halaman detailnya.
5. Perluas bagian Constraints pada halaman, dan pilih tombol radio untuk kendala dengan nama produk Control Tower AWS Account Factory.
6. Pilih HAPUS BATASAN.

7. Di kotak dialog yang terbuka, tinjau informasi untuk memastikannya akurat, lalu pilih LANJUTKAN.
8. Dari bagian Produk halaman, pilih tombol radio untuk produk bernama AWS Control Tower Account Factory.
9. Pilih HAPUS PRODUK.
10. Di kotak dialog yang terbuka, tinjau informasi untuk memastikannya akurat, lalu pilih LANJUTKAN.
11. Perluas bagian Pengguna, Grup, dan Peran halaman, dan pilih kotak centang untuk semua catatan dalam tabel ini.
12. Pilih HAPUS PENGGUNA, GRUP ATAU PERAN.
13. Di kotak dialog yang terbuka, tinjau informasi untuk memastikannya akurat, lalu pilih LANJUTKAN.
14. Dari menu navigasi kiri, pilih daftar Portofolio.
15. Dalam tabel Portofolio Lokal, cari portofolio bernama AWS Control Tower Account Factory Portfolio.
16. Pilih tombol radio untuk portofolio itu, lalu pilih HAPUS PORTOFOLIO.
17. Di kotak dialog yang terbuka, tinjau informasi untuk memastikannya akurat, lalu pilih LANJUTKAN.
18. Dari menu navigasi kiri, pilih Daftar produk.
19. Pada halaman produk Admin, cari produk bernama AWS Control Tower Account Factory.
20. Pilih produk untuk membuka halaman detail produk Admin.
21. Dari Tindakan, pilih Hapus produk.
22. Di kotak dialog yang terbuka, tinjau informasi untuk memastikannya akurat, lalu pilih LANJUTKAN.

Hapus Peran dan Kebijakan AWS Control Tower

Prosedur ini memandu Anda melalui cara membersihkan peran dan kebijakan yang dibuat AWS Control Tower saat landing zone Anda disiapkan, atau yang lebih baru.

Untuk menghapus peran Pusat AWSService CatalogEndUserAccess Identitas IAM

1. Buka AWS IAM Identity Center konsol di https://console.aws.amazon.com/singlesignon/.

2. Ubah AWS Wilayah Anda ke Wilayah asal Anda, yang merupakan Wilayah tempat Anda pertama kali menyiapkan AWS Control Tower.
3. Dari menu navigasi kiri, pilih AWS akun.
4. Pilih tautan akun manajemen Anda.
5. Pilih dropdown untuk set Izin, pilih AWSServiceCatalogEndUserAccess, lalu pilih Hapus.
6. Pilih AWS akun dari panel kiri.
7. Buka tab Set izin.
8. Pilih AWSServiceCatalogEndUserAccessdan hapus.

Untuk menghapus peran IAM

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Dari menu navigasi kiri, pilih Peran.
3. Dari tabel, cari peran dengan nama AWSControlTower.
4. Untuk setiap peran dalam tabel, lakukan hal berikut:
    a. Pilih kotak centang untuk peran tersebut.
    b. Pilih Hapus peran.
    c. Di kotak dialog yang terbuka, tinjau informasi untuk memastikannya akurat, lalu pilih Ya, hapus.

Untuk menghapus kebijakan IAM

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Dari menu navigasi kiri, pilih Kebijakan.
3. Dari tabel, cari kebijakan dengan nama AWSControlTower.
4. Untuk setiap kebijakan dalam tabel, lakukan hal berikut:
    a. Pilih kotak centang untuk kebijakan.
    b. Pilih Tindakan kebijakan, dan Hapus dari menu tarik-turun.
    c. Di kotak dialog yang terbuka, tinjau informasi untuk memastikannya akurat, lalu pilih Hapus.

Bantuan sumber daya AWS Control Tower

Jika Anda mengalami masalah apa pun yang tidak dapat diselesaikan saat menghapus sumber daya AWS Control Tower, hubungi AWS Support.

Pengaturan setelah menonaktifkan landing zone

Setelah Anda menonaktifkan landing zone Anda, Anda tidak dapat berhasil mengeksekusi setup lagi sampai pembersihan manual selesai. Selain itu, tanpa pembersihan manual dari sumber daya yang tersisa ini, Anda mungkin dikenakan biaya penagihan yang tidak terduga. Anda harus memperhatikan masalah ini:

- Akun manajemen AWS Control Tower adalah bagian dari AWS Control Tower Root OU. Pastikan bahwa peran IAM dan kebijakan IAM ini dihapus dari akun manajemen:
  - Peran:
    - `AWSControlTowerAdmin`
    - `AWSControlTowerCloudTrailRole`
    - `AWSControlTowerStackSetRole`
  - Kebijakan:
    - `AWSControlTowerAdminPolicy`
    - `AWSControlTowerCloudTrailRolePolicy`
    - `AWSControlTowerStackSetRolePolicy`
- Anda mungkin ingin menghapus atau memperbarui konfigurasi IAM Identity Center yang ada untuk AWS Control Tower sebelum menyiapkan landing zone lagi, tetapi Anda tidak perlu menghapusnya.
- Anda mungkin ingin menghapus VPC yang dibuat oleh AWS Control Tower.
- Penyiapan gagal jika alamat email yang ditentukan untuk akun pencatatan atau audit dikaitkan dengan AWS akun yang ada. Anda dapat menutup AWS akun, atau menggunakan alamat email yang berbeda untuk mengatur landing zone lagi. Atau, Anda dapat menggunakan kembali akun bersama yang ada ini, dengan fitur yang memungkinkan Anda untuk membawa akun pencatatan dan audit Anda sendiri. Untuk informasi selengkapnya, lihat Pertimbangan untuk membawa akun keamanan atau pencatatan yang ada.

- Penyiapan gagal jika bucket Amazon S3 dengan nama cadangan berikut sudah ada di akun logging:
  - `aws-controltower-logs-{accountId}-{region}`(digunakan untuk ember logging).
  - `aws-controltower-s3-access-logs-{accountId}-{region}`(digunakan untuk bucket akses logging).

  Anda harus mengganti nama atau menghapus bucket ini, atau menggunakan akun lain untuk akun logging.
- Pengaturan gagal jika akun manajemen memiliki grup log yang ada,`aws-controltower/CloudTrailLogs`, di CloudWatch Log. Anda harus mengganti nama atau menghapus grup log.

Sebelum Anda mengatur di yang baru Wilayah AWS

Jika Anda berniat untuk membuat landing zone baru di AWS Wilayah baru, ikuti langkah-langkah tambahan ini.

- Masukkan perintah berikut melalui CLI:

```
aws organizations disable-aws-service-access --service-principal
 controltower.amazonaws.com
```

- Hapus EventBridge aturan Amazon yang tersisa, yang dipanggil`AWSControlTowerManagedRule`, dari akun bersama dan anggota untuk semua Wilayah yang diatur.

Panduan

Bab ini berisi prosedur panduan yang dapat membantu Anda dalam penggunaan AWS Control Tower.

Topik

- Panduan: Pindah dari ALZ ke AWS Control Tower
- Panduan: Konfigurasikan Menara Kontrol AWS Tanpa VPC
- Hapus sumber daya AWS Control Tower
- Panduan: Mengatur Grup Keamanan di AWS Control Tower Dengan AWS Firewall Manager
- Menonaktifkan landing zone AWS Control Tower

Panduan: Pindah dari ALZ ke AWS Control Tower

Banyak AWS pelanggan telah mengadopsi solusi AWS Landing Zone (ALZ) untuk menyiapkan lingkungan multi-akun yang aman, sesuai dengan standar AWS . Untuk mengurangi beban pengelolaan zona pendaratan, AWS buat layanan terkelola yang disebut AWS Control Tower.

Tidak ada fitur tambahan yang dijadwalkan untuk ALZ; itu hanya dalam dukungan jangka panjang. Oleh karena itu, kami menyarankan Anda pindah ke layanan AWS Control Tower dari ALZ. Blog yang ditautkan dalam babak ini memandu Anda melalui berbagai pertimbangan untuk langkah itu, dan menjelaskan bagaimana Anda dapat merencanakan migrasi yang sukses dari ALZ ke AWS Control Tower.

Blog: Migr AWS asikan solusi Zona Pendaratan ke AWS Control Tower

AWS Panduan Prescriptive menawarkan dokumentasi yang lebih luas, termasuk langkah-langkah untuk transisi dari ALZ ke AWS Control Tower. Pada dasarnya, Anda akan mengaktifkan tata kelola AWS Control Tower di organisasi Anda yang menjalankan ALZ, berdasarkan sejumlah prasyarat. Untuk informasi, lihat Trans isi dari Zona Pen AWS daratan ke Menara Kontrol AWS.

Panduan: Konfigurasikan Menara Kontrol AWS Tanpa VPC

Topik ini membahas cara mengonfigurasi akun AWS Control Tower Anda tanpa VPC.

Jika beban kerja Anda tidak memerlukan VPC, Anda dapat melakukan hal berikut:

- Anda dapat menghapus cloud pribadi virtual AWS Control Tower (VPC). VPC ini dibuat saat Anda mengatur zona pendaratan Anda.
- Anda dapat mengubah setelan Account Factory agar akun AWS Control Tower baru dibuat tanpa VPC terkait.

> **Important**
>
> Jika Anda menyediakan akun Account Factory dengan pengaturan akses internet VPC diaktifkan, setelan Account Factory tersebut akan menggantikan kontrol Larang akses internet untuk instans Amazon VPC yang dikelola oleh pelanggan. Untuk menghindari mengaktifkan akses internet untuk akun yang baru disediakan, Anda harus mengubah pengaturan di Account Factory.

Menghapus VPC Menara Kontrol AWS

Di luar AWS Control Tower, setiap AWS pelanggan memiliki VPC default, yang dapat Anda lihat di konsol Amazon Virtual Private Cloud (Amazon VPC) di. https://console.aws.amazon.com/vpc/ Anda akan mengenali VPC default, karena namanya selalu menyertakan kata (default) di akhir nama.

Saat Anda menyiapkan zona pendaratan AWS Control Tower, AWS Control Tower menghapus VPC AWS default Anda dan membuat VPC default AWS Control Tower baru. VPC baru dikaitkan dengan akun manajemen AWS Control Tower Anda. Topik ini mengacu pada VPC baru itu sebagai VPC Menara Kontrol.

Saat Anda melihat AWS Control Tower VPC di konsol Amazon VPC, Anda tidak akan melihat kata (default) di akhir nama. Jika Anda memiliki lebih dari satu VPC, Anda harus menggunakan rentang CIDR yang ditetapkan untuk mengidentifikasi AWS Control Tower VPC yang benar.

Anda dapat menghapus AWS Control Tower VPC, tetapi jika nantinya memerlukan VPC di AWS Control Tower, Anda harus membuatnya sendiri.

Untuk menghapus AWS Control Tower VPC

1. Buka konsol Amazon VPC di https://console.aws.amazon.com/vpc/.
2. Cari **VPC** atau pilih VPC dari opsi Katalog Layanan. Anda kemudian melihat Dashboard VPC.
3. Dari menu di sebelah kiri, pilih VPC Anda. Anda kemudian melihat daftar semua VPC Anda.

4. Identifikasi AWS Control Tower VPC berdasarkan jangkauan CIDR-nya.
5. Untuk menghapus VPC, pilih Tindakan lalu pilih H apus V PC.

VPC AWS (default) sudah ada di setiap Wilayah untuk akun manajemen AWS Control Tower. Untuk mengikuti praktik terbaik keamanan, jika Anda memilih untuk menghapus AWS Control Tower VPC, sebaiknya juga menghapus VPC AWS default yang terkait dengan akun manajemen dari semua AWS Wilayah. Oleh karena itu, untuk mengamankan akun manajemen, hapus VPC default dari setiap Wilayah, serta hapus VPC yang dibuat oleh Control Tower di wilayah asal AWS Control Tower Anda.

Secara opsional membersihkan sumber daya VPC di akun

Secara opsional, untuk membersihkan sumber daya AWS Control Tower VPC,`aws-controltower-VPC`, dari akun yang ada, Anda dapat menghapus instans tumpukan dari AWS CloudFormation StackSet`AWSControlTowerBP-VPC-ACCOUNT-FACTORY-V1`, setelah Anda memastikan bahwa tidak ada sumber daya atau dependensi sumber daya yang ada di VPC.

Buat Akun di AWS Control Tower Tanpa VPC

Jika beban kerja pengguna akhir Anda tidak memerlukan VPC, Anda dapat menggunakan metode ini untuk mengatur akun pengguna akhir yang tidak memiliki VPC yang dibuat untuk mereka secara otomatis.

Dari dasbor AWS Control Tower, Anda dapat melihat dan mengedit setelan konfigurasi jaringan Anda. Setelah Anda mengubah pengaturan sehingga akun AWS Control Tower dibuat tanpa VPC terkait, semua akun baru dibuat tanpa VPC sampai Anda mengubah pengaturan lagi.

Untuk mengkonfigurasi Account Factory untuk membuat akun tanpa VPC

1. Buka browser web, dan navigasikan ke konsol AWS Control Tower di https://console.aws.amazon.com/controltower.
2. Pilih Account Factory dari menu di sebelah kiri.
3. Anda kemudian melihat halaman Pabrik Akun dengan bagian Konfigurasi Jaringan.
4. Perhatikan pengaturan saat ini jika Anda ingin mengembalikannya nanti.
5. Pilih tombol Edit di bagian Konfigurasi Jaringan.
6. Di halaman Edit akun konfigurasi jaringan pabrik, buka opsi Konfigur asi VPC untuk akun baru.

Anda dapat mengikuti Opsi 1 atau Opsi 2, atau keduanya, untuk memastikan bahwa AWS Control Tower tidak membuat VPC saat menyediakan akun.

a. Opsi 1 - Menghapus subnet

   - Matikan sakelar sak Internet-accessible elar sub net.
   - Setel jumlah maksimum nilai subnet pribadi ke 0.

b. Opsi 2 - Menghapus AWS Wilayah

   - Kosongkan setiap kotak centang di kolom Regions untuk pembuatan VPC.

7. Pilih Simpan.

Kemungkinan Kesalahan

Ketahuilah kemungkinan kesalahan ini yang dapat terjadi saat Anda menghapus AWS Control Tower VPC atau mengonfigurasi ulang Account Factory untuk membuat akun tanpa VPC.

- Akun manajemen Anda yang ada mungkin memiliki dependensi atau sumber daya di AWS Control Tower VPC, yang dapat menyebabkan kesalahan kegagalan penghapusan.
- Jika Anda membiarkan CIDR default pada tempatnya saat menyiapkan untuk meluncurkan akun baru tanpa VPC, permintaan Anda gagal dengan kesalahan bahwa CIDR tidak valid.

Panduan: Mengatur Grup Keamanan di AWS Control Tower Dengan AWS Firewall Manager

Video ini menunjukkan cara menggunakan layanan AWS Firewall Manager untuk memberikan peningkatan keamanan jaringan untuk AWS Control Tower. Anda dapat menetapkan akun administrator keamanan yang diaktifkan untuk mengatur grup keamanan. Anda akan melihat bagaimana Anda dapat mengonfigurasi kebijakan keamanan dan menegakkan aturan keamanan untuk organisasi AWS Control Tower Anda, dan bagaimana Anda dapat memperbaiki sumber daya yang tidak sesuai dengan menerapkan kebijakan secara otomatis. Anda dapat melihat grup keamanan yang berlaku untuk setiap akun dan sumber daya (seperti instans Amazon EC2) di organisasi Anda.

Anda dapat membuat kebijakan firewall sendiri, atau Anda dapat berlangganan aturan dari vendor tepercaya.

Mengatur Grup Keamanan Dengan AWS Firewall Manager

Video ini (8:02) menjelaskan cara menyiapkan keamanan infrastruktur jaringan yang lebih baik untuk sumber daya dan beban kerja Anda di AWS Control Tower. Untuk tampilan yang lebih baik, pilih ikon di sudut kanan bawah video untuk memperbesarnya ke layar penuh. Keterangan tersedia.

Panduan Video Pengaturan Firewall di Menara Kontrol AWS.

Untuk informasi selengkapnya, lihat dokumentasi tentang cara mengatur AWS WAF.

Pemecahan Masalah

Jika Anda mengalami masalah saat menggunakan AWS Control Tower, Anda dapat menggunakan informasi berikut untuk menyelesaikannya sesuai dengan praktik terbaik kami. Jika masalah yang Anda temui berada di luar cakupan informasi berikut, atau jika masih ada setelah Anda mencoba menyelesaikannya, hubungi AWS Support.

Topik

- Peluncuran Zona Pendaratan Gagal
- Pembaruan Zona Pendaratan Gagal dengan Kesalahan KMS
- Tidak Dapat Memperbarui Zona Pendaratan
- Kesalahan zona pendaratan tidak mutakhir
- Penyediaan Akun Baru Gagal
- Gagal Mendaftarkan Akun yang Ada
- Tidak Dapat Memperbarui Akun Akun Factory
- Kesalahan Kegagalan yang Menyebutkan AWS Config
- Kesalahan portofolio AWS Control Tower Account Factory
- Menerima Kesalahan Izin Tidak Cukup
- Kontrol Detektif tidak berlaku pada akun
- Nilai melebihi kesalahan yang dikembalikan oleh AWS Organizations API
- Gagal memindahkan akun Account Factory langsung dari satu landing zone AWS Control Tower ke landing zone AWS Control Tower lainnya
- AWS Support

Peluncuran Zona Pendaratan Gagal

Penyebab umum kegagalan peluncuran landing zone:

- Kurangnya respons terhadap pesan email konfirmasi.
- CloudFormation StackSet Kegagalan.

Pesan email konfirmasi: Jika akun manajemen Anda berusia kurang dari satu jam, Anda mungkin mengalami masalah saat akun tambahan dibuat.

Tindakan yang harus diambil

Jika Anda mengalami masalah ini, periksa email Anda. Anda mungkin telah dikirimi email konfirmasi yang sedang menunggu tanggapan. Atau, kami sarankan Anda menunggu satu jam, dan kemudian coba lagi. Jika masalah berlanjut, hubungi AWS Support.

Gagal StackSets: Kemungkinan penyebab lain kegagalan peluncuran landing zone adalah CloudFormation StackSet kegagalan. AWS Wilayah Security Token Service (STS) harus diaktifkan di akun manajemen untuk semua AWS Wilayah yang diatur AWS Control Tower, sehingga penyediaan dapat berhasil; jika tidak, kumpulan tumpukan akan gagal diluncurkan.

Tindakan yang harus diambil

Pastikan untuk mengaktifkan semua wilayah titik akhir AWS Security Token Service (STS) yang diperlukan sebelum meluncurkan AWS Control Tower.

Untuk memulihkan set tumpukan yang gagal dan coba lagi pengaturan

1. Arahkan ke CloudFormation konsol yang sesuai Wilayah AWS.
2. Bersihkan tumpukan yang gagal dengan nama AWSControlTowerBP-BASELINE-CLOUDTRAIL-MASTER.
3. Tunggu penghapusan tumpukan selesai.
4. Kembali ke halaman AWS Control Tower.
5. Pilih Atur landing zone lagi.

Untuk melihat daftar AWS Control Tower Wilayah AWS yang didukung, lihatBagaimana AWS Wilayah Bekerja Dengan AWS Control Tower.

Pembaruan Zona Pendaratan Gagal dengan Kesalahan KMS

Penyebab paling umum kegagalan pembaruan landing zone adalah kebijakan AWS KMS utama yang tidak valid.

Alasan umum untuk kebijakan kunci KMS yang tidak valid:

- Salah ketik dalam kebijakan.
- Lupa menambahkan pernyataan kebijakan yang diperlukan.

- AWS Partisi salah.
- Nomor akun salah dalam polis.
- Lupa menghapus placeholder dalam kebijakan contoh.

Tindakan yang harus diambil

Tinjau kebijakan Anda untuk memeriksa kesalahan ini.

Untuk informasi selengkapnya tentang kebijakan AWS KMS utama, lihat Mengonfigurasi kunci KMS dan Prasyarat Cadangan.

Tidak Dapat Memperbarui Zona Pendaratan

AWS Control Tower tidak memutar kembali ke versi landing zone sebelumnya jika pembaruan gagal. Anda mungkin menemukan landing zone Anda dalam keadaan tak tentu. Jika demikian, hubungi AWS dukungan.

Pembaruan zona pendaratan mungkin gagal karena beberapa alasan.

- Prasyarat tidak terpenuhi
- AWS Config sumber daya ada di akun tertentu
- Akun tertutup ada

Prasyarat tidak terpenuhi

Pembaruan landing zone harus memenuhi prasyarat yang sama dengan pengaturan landing zone. Sebelum Anda memperbarui, tinjau cek pra-peluncuran.

AWS Config sumber daya ada di akun Security OU

Jangan menambahkan AWS Config sumber daya di akun Audit dan Arsip Log Anda. Proses pembaruan landing zone tidak dapat diselesaikan dengan sumber daya yang ada. Pembatasan ini mirip dengan yang berlaku untuk mendaftarkan akun atau menyiapkan landing zone untuk pertama kalinya. Untuk informasi selengkapnya, lihat Mendaftarkan akun yang memiliki AWS Config sumber daya yang ada.

Akun tertutup ada

Saat akun dalam status Tertutup atau Ditangguhkan, Anda mungkin mengalami masalah saat mencoba memperbarui landing zone. Anda harus menghapus produk yang disediakan di setiap akun yang ditutup sebelum melakukan pembaruan ke landing zone.

Pada halaman produk AWS Service Catalog yang disediakan, Anda mungkin melihat pesan kesalahan yang mirip dengan yang ini:

```
AWSControlTowerExecution role can't be assumed on the account.
```

Penyebab umum: Anda telah menangguhkan akun tanpa menghapus produk yang disediakan.

Tindakan yang harus diambil: Jika Anda melihat kesalahan ini, Anda memiliki dua opsi:

1. Hubungi AWS Support dan buka kembali akun, hapus produk yang disediakan, lalu tutup akun lagi.
2. Hapus sumber daya dari StackSets yang telah menjadi yatim piatu karena penutupan akun. (Opsi ini hanya tersedia jika StackSets memiliki instance dalam keadaan Saat ini yang tidak Anda hapus.)

Untuk menghapus sumber daya dari StackSets, lakukan ini untuk setiap akun yang ditutup:

- Masuk ke masing-masing AWS Control Tower StackSets dan hapus StackInstances dari setiap wilayah, untuk akun yang telah ditutup.
- PENTING: Pilih opsi Retain Stack sehingga hanya StackSet menghapus instance tumpukan. StackSet tidak dapat mengambil peran dari akun yang ditutup, sehingga akan gagal jika mencoba mengambil `AWSControlTowerExecution` peran, yang mengarah ke pesan kesalahan yang Anda terima.

Kesalahan zona pendaratan tidak mutakhir

Jika Anda belum memperbarui landing zone baru-baru ini, Anda mungkin menerima kesalahan saat mencoba mendapatkan kembali akses ke AWS Control Tower. Anda mungkin melihat pesan kesalahan yang mirip dengan yang ini:

```
Unable to access Control Tower
```

Akun Anda sudah tidak aktif terlalu lama. Karena tidak aktif, Anda harus memperbarui landing zone untuk akses ke AWS Control Tower.

Namun, pembaruan landing zone Anda mungkin gagal.

Langkah-langkah yang harus diambil

Masuk ke akun manajemen organisasi Anda, dan masuk sebagai pengguna root. Pengguna IAM atau pengguna Anda di IAM Identity Center harus memiliki izin administrator AWS Control Tower dan menjadi bagian dari grup. AWSControlTowerAdmins Kemudian coba pembaruan lagi.

Penyediaan Akun Baru Gagal

Jika Anda mengalami masalah ini, periksa penyebab umum ini.

Saat Anda mengisi formulir penyediaan akun, Anda mungkin memiliki:

- TagOptions yang ditentukan,
- mengaktifkan notifikasi SNS,
- mengaktifkan pemberitahuan produk yang disediakan.

Coba lagi untuk menyediakan akun Anda, tanpa menentukan salah satu opsi tersebut. Untuk informasi selengkapnya, lihat Menyediakan akun di konsol Service Catalog, dengan Account Factory.

Penyebab umum lainnya untuk kegagalan:

- Jika Anda membuat paket produk yang disediakan (untuk melihat perubahan sumber daya), penyediaan akun Anda mungkin tetap dalam status Sedang berlangsung tanpa batas waktu.
- Pembuatan akun baru di Account Factory akan gagal sementara perubahan konfigurasi AWS Control Tower lainnya sedang berlangsung. Misalnya, saat proses sedang berjalan untuk menambahkan kontrol ke OU, Account Factory akan menampilkan pesan kesalahan jika Anda mencoba menyediakan akun.

Untuk memeriksa status tindakan sebelumnya di AWS Control Tower

- Arahkan AWS CloudFormation ke> StackSets
- Periksa setiap set tumpukan yang terkait dengan AWS Control Tower (awalan: "AWSControlTower“)
- Cari CloudFormation StackSets operasi yang masih berjalan.

Jika penyediaan akun Anda memakan waktu lebih dari satu jam, sebaiknya hentikan proses penyediaan dan coba lagi.

Gagal Mendaftarkan Akun yang Ada

Jika Anda mencoba sekali untuk mendaftarkan AWS akun yang ada dan pendaftaran itu gagal, saat Anda mencoba untuk kedua kalinya, pesan kesalahan mungkin memberi tahu Anda bahwa kumpulan tumpukan ada. Untuk melanjutkan, Anda harus menghapus produk yang disediakan di Account Factory.

Jika alasan kegagalan pendaftaran pertama adalah karena Anda lupa membuat `AWSControlTowerExecution` peran di akun sebelumnya, pesan kesalahan yang akan Anda terima dengan benar memberi tahu Anda untuk membuat peran. Namun, ketika Anda mencoba membuat peran, Anda kemungkinan akan menerima pesan kesalahan lain yang menyatakan bahwa AWS Control Tower tidak dapat membuat peran tersebut. Kesalahan ini terjadi karena prosesnya telah selesai sebagian.

Dalam hal ini, Anda harus mengambil dua langkah pemulihan sebelum Anda dapat melanjutkan dengan mendaftarkan akun Anda yang ada. Pertama, Anda harus menghentikan produk yang disediakan Account Factory melalui konsol. AWS Service Catalog Selanjutnya, Anda harus menggunakan AWS Organizations konsol untuk memindahkan akun secara manual dari OU dan kembali ke root. Setelah itu selesai, buat `AWSControlTowerExecution` peran di akun, lalu isi kembali formulir akun Daftarkan.

Kemungkinan penyebab kegagalan pendaftaran lainnya adalah akun tersebut memiliki sumber daya Config AWS yang ada. Dalam hal ini, lihat Mendaftarkan akun yang memiliki AWS Config sumber daya yang ada untuk petunjuk tentang cara mengubah sumber daya yang ada.

Tidak Dapat Memperbarui Akun Akun Factory

Ketika akun berada dalam keadaan tidak konsisten, akun tidak dapat diperbarui dengan sukses dari Account Factory atau AWS Service Catalog.

Kasus 1: Anda mungkin menemukan pesan kesalahan yang mirip dengan yang ini:

```
AWS Control Tower could not baseline VPC in the managed account because of
existing resource dependencies.
```

Penyebab umum: AWS Control Tower selalu menghapus VPC AWS default selama penyediaan awal. Untuk memiliki VPC AWS default di akun, Anda harus menambahkannya setelah pembuatan akun. AWS Control Tower memiliki VPC defaultnya sendiri yang menggantikan AWS VPC default, kecuali jika Anda menyiapkan Account Factory seperti yang ditunjukkan oleh penelusuran —-sehingga AWS Control Tower tidak menyediakan VPC sama sekali. Maka akun tersebut tidak memiliki VPC. Anda harus menambahkan kembali VPC AWS default jika Anda ingin menggunakannya.

Namun, AWS Control Tower tidak mendukung AWS VPC default. Menyebarkan satu menyebabkan akun memasuki `Tainted` status. Ketika dalam keadaan itu, Anda tidak dapat memperbarui akun melalui AWS Service Catalog.

Tindakan yang harus diambil: Anda harus menghapus VPC default yang Anda tambahkan, dan kemudian Anda akan dapat memperbarui akun.

> **Note**
>
> `Tainted`Status menyebabkan masalah tindak lanjut: Akun yang tidak diperbarui dapat mencegah pengaktifan kontrol pada OU yang menjadi bagiannya.

Kasus 2: Anda mungkin melihat pesan kesalahan yang mirip dengan yang ini:

```
AWS Control Tower detects that your enrolled account has been moved to a new organizational unit.
```

Penyebab umum: Anda mencoba memindahkan akun dari satu OU terdaftar ke yang lain, tetapi aturan AWS Config lama tetap ada. Akun dalam keadaan tidak konsisten.

Tindakan yang harus diambil:

Jika pemindahan akun dimaksudkan:

- Mengakhiri akun di Service Catalog.
- Daftarkan lagi.
- Context/impact: Aturan AWS Config yang diterapkan tidak cocok dengan konfigurasi yang ditentukan oleh OU tujuan.
- AWS Aturan Config mungkin tetap dari OU sebelumnya, menyebabkan pengeluaran yang tidak diinginkan.

- Upaya untuk mendaftarkan ulang atau memperbarui akun akan gagal karena konflik penamaan sumber daya.

Jika pemindahan akun tidak disengaja:

- Kembalikan akun ke OU aslinya.
- Perbarui akun dari Service Catalog.
- Dalam parameter peluncuran, masukkan OU tempat akun awalnya berada.
- Context/impact: Jika akun tidak dikembalikan ke OU aslinya, statusnya akan tidak konsisten dengan kontrol yang ditentukan oleh OU baru yang ada di dalamnya.
- Memperbarui akun bukanlah perbaikan yang valid, karena tidak menghapus AWS Config aturan yang terkait dengan OU sebelumnya.

Kesalahan Kegagalan yang Menyebutkan AWS Config

Jika AWS Config diaktifkan di AWS Wilayah mana pun yang didukung oleh AWS Control Tower, Anda mungkin menerima pesan kesalahan karena pra-pemeriksaan gagal. Pesan tersebut mungkin tampaknya tidak menjelaskan masalah secara memadai, karena beberapa perilaku yang mendasarinya. AWS Config

Anda mungkin menerima pesan kesalahan, mirip dengan salah satu dari ini:

- `AWS Control Tower cannot create an AWS Config delivery channel because one already exists. To continue, delete the existing delivery channel and try again .`
- `AWS Control Tower cannot create an AWS Config configuration recorder because one already exists. To continue, delete the existing delivery channel and try again .`

Penyebab umum: Ketika AWS Config layanan diaktifkan pada AWS akun, itu membuat perekam konfigurasi dan saluran pengiriman dengan penamaan default. Jika Anda menonaktifkan AWS Config layanan melalui konsol, itu tidak menghapus perekam konfigurasi atau saluran pengiriman. Anda harus menghapusnya melalui CLI, atau memodifikasinya untuk penggunaan AWS Control Tower.

Jika AWS Config layanan diaktifkan di salah satu Wilayah yang didukung oleh AWS Control Tower, hal ini dapat mengakibatkan kegagalan ini.

Jika akun memiliki sumber daya AWS Config yang ada, lihat Mendaftarkan akun yang memiliki AWS Config sumber daya yang ada untuk petunjuk tentang cara mengubah sumber daya yang ada.

Tindakan yang harus diambil: Hapus perekam konfigurasi dan saluran pengiriman di semua wilayah yang didukung. Menonaktifkan AWS Config tidak cukup, perekam konfigurasi dan saluran pengiriman harus dihapus melalui CLI. Setelah menghapus perekam konfigurasi dan saluran pengiriman dari CLI, Anda dapat mencoba lagi untuk meluncurkan AWS Control Tower dan mendaftarkan akun.

Jika Anda sedang dalam proses menerapkan produk yang disediakan, Anda harus menghapus produk yang disediakan sebelum Anda mencoba lagi. Jika tidak, Anda mungkin melihat pesan kesalahan yang mirip dengan yang ini:

- `An error occurred (InvalidParametersException) when calling the ProvisionProduct operation: A stack named Stackname already exists.`

Dalam pesan, *Stackname* menentukan nama tumpukan.

Berikut adalah beberapa contoh perintah AWS Config CLI yang dapat Anda gunakan untuk menentukan status perekam konfigurasi dan saluran pengiriman Anda.

Lihat perintah:

- `aws configservice describe-delivery-channels`
- `aws configservice describe-delivery-channel-status`
- `aws configservice describe-configuration-recorders`
- `The normal response is something like "name": "default"`

Hapus perintah:

- `aws configservice stop-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-delivery-channel --delivery-channel-name NAME-FROM-DESCRIBE-OUTPUT`
- `aws configservice delete-configuration-recorder --configuration-recorder-name NAME-FROM-DESCRIBE-OUTPUT`

Untuk informasi lebih lanjut, lihat AWS Config dokumentasi

- Mengelola Perekam Konfigurasi (AWS CLI)
- Mengelola Saluran Pengiriman

Kesalahan portofolio AWS Control Tower Account Factory

Saat mencoba membuat, mendaftarkan, atau memperbarui akun, Anda mungkin melihat salah satu pesan galat berikut:

```
Your AWS IAM identity does not have access to the AWS Control Tower Account Factory portfolio in AWS Service Catalog. To resolve this, an administrator must associate your AWS IAM identity with the portfolio.
```

atau

```
No launch paths found for resource: prod-xxxx
```

Penyebab Umum:

- Anda mungkin masuk sebagai root. AWS Control Tower tidak mendukung pembuatan akun saat Anda masuk sebagai pengguna root.
- Pengguna Pusat Identitas IAM Anda belum ditambahkan ke grup izin yang sesuai. Anda mungkin perlu menambahkan pengguna IAM Identity Center Anda ke salah satu grup izin ini: AWSAccountFactory(untuk akses pengguna akhir) atau AWSServiceCatalogAdmins(untuk akses admin).
- Jika Anda diautentikasi sebagai pengguna IAM, Anda harus menambahkannya ke AWS Service Catalog portofolio sehingga memiliki izin yang benar.
- Masalah ini juga terjadi jika Anda memiliki izin yang benar, tetapi AWS Control Tower drift terdeteksi, dan perbaikan drift diperlukan. Untuk memperbaiki sebagian besar jenis drift, pilih Reset pada halaman pengaturan zona pendaratan.

Menerima Kesalahan Izin Tidak Cukup

Ada kemungkinan bahwa akun Anda mungkin tidak memiliki izin yang diperlukan untuk melakukan pekerjaan tertentu secara tertentu AWS Organizations. Jika Anda menemukan jenis kesalahan

berikut, periksa semua area izin, seperti izin IAM atau IAM Identity Center, untuk memastikan izin Anda tidak ditolak dari tempat-tempat tersebut:

```
You have insufficient permissions to perform AWS Organizations API actions.
```

Jika Anda yakin pekerjaan Anda memerlukan tindakan yang Anda coba, dan Anda tidak dapat menemukan batasan yang relevan, hubungi administrator sistem atau Support AWS Anda.

Kontrol Detektif tidak berlaku pada akun

Jika Anda baru saja memperluas penerapan AWS Control Tower ke AWS Wilayah baru, kontrol detektif yang baru diterapkan tidak berlaku pada akun baru yang Anda buat di Wilayah mana pun hingga akun individual dalam OU yang diatur oleh AWS Control Tower diperbarui. Kontrol detektif yang ada pada akun yang ada masih berlaku.

Jika Anda mencoba mengaktifkan kontrol detektif sebelum memperbarui akun Anda, Anda mungkin melihat pesan kesalahan yang mirip dengan yang ini:

```
AWS Control Tower can't enable the selected control on this OU. AWS Control Tower cannot apply the control on the OU ou-xxx-xxxxxxxx, because child accounts have dependencies that are missing. Update all child accounts under the OU, then try again.
```

Tindakan yang harus diambil: Perbarui akun.

Untuk memperbarui akun Anda dari konsol AWS Control Tower, lihatKapan harus memperbarui AWS Control Tower OU dan akun.

Untuk memperbarui beberapa akun individual secara terprogram, Anda dapat menggunakan API dari AWS Service Catalog dan AWS CLI untuk mengotomatiskan pembaruan. Untuk informasi selengkapnya tentang cara mendekati proses pembaruan, lihat iniPanduan Video. Anda dapat mengganti UpdateProvisionedProductAPI untuk ProvisionProductAPI yang ditampilkan dalam video.

Jika Anda memiliki kesulitan lebih lanjut dengan mengaktifkan kontrol detektif di akun Anda, hubungi Support AWS .

Nilai melebihi kesalahan yang dikembalikan oleh AWS Organizations API

Kemungkinan penyebab

Beban kerja Anda berjalan saat AWS Control Tower menjalankan pemindaian harian untuk memeriksa apakah SCP Anda telah hanyut.

Langkah-langkah untuk diikuti

Jika Anda mengalami pelambatan atau `rate exceeded` kesalahan API, coba langkah-langkah berikut:

- Jalankan beban kerja Anda pada waktu yang berbeda. (Lihat jadwal pemindaian invarian AWS Control Tower SCP menurut Wilayah untuk mengetahui kapan AWS Control Tower menjalankan pemindaian auditnya.)
- Jika Anda memanggil API secara langsung melalui HTTP: Gunakan AWS SDK, yang secara otomatis mencoba ulang tindakan yang gagal
- Meminta peningkatan batas melalui Service Quotas dan Support AWS

Contoh instruksi pemecahan masalah untuk pelambatan API di Elastic Beanstalk dapat ditemukan di sini: `https://aws.amazon.com/premiumsupport/knowledge-center/elastic-beanstalk-api-throttling-errors/`

Gagal memindahkan akun Account Factory langsung dari satu landing zone AWS Control Tower ke landing zone AWS Control Tower lainnya

> **Warning**
>
> Praktik ini tidak memenuhi prasyarat untuk pendaftaran akun yang memenuhi syarat, karena akun yang memenuhi syarat harus menjadi bagian dari Organisasi AWS keseluruhan yang sama, dan setiap organisasi mungkin hanya memiliki satu landing zone. Jika Anda telah mencoba melakukan tindakan ini dan Anda menemukan diri Anda menerima beberapa pesan kesalahan, berikut adalah beberapa informasi yang mungkin membantu.

Untuk memindahkan akun yang telah Anda sediakan melalui Account Factory ke landing zone lain yang dikelola oleh AWS Control Tower, di bawah akun manajemen lain, Anda harus menghapus semua peran IAM dan tumpukan yang terkait dengan akun tersebut dari OU asli. Hapus sumber daya ini dari setiap Wilayah tempat akun digunakan.

> **Note**
>
> Cara terbaik untuk menghapus sumber daya adalah dengan membatalkan penyediaan akun di OU aslinya sebelum Anda mencoba memindahkannya.

Jika Anda tidak menghapus sumber daya, pendaftaran ke OU baru akan gagal, agak spektakuler. Anda mungkin menemukan satu atau beberapa pesan kesalahan, dan Anda akan terus menerima pesan kesalahan serupa hingga peran dan tumpukan yang tersisa dihapus dari setiap Wilayah tempat akun digunakan.

Setiap kali Anda menerima pesan kesalahan, Anda harus menghapus akun dari OU baru, menghapus sumber daya lama yang merupakan subjek pesan kesalahan, dan kemudian mencoba untuk memindahkan akun kembali ke OU baru. Proses penghapusan dan penghapusan ini harus diulang untuk setiap sumber daya yang tersisa, untuk setiap Wilayah di mana akun tersebut digunakan, mungkin 10 atau 20 kali. Kesalahan berulang ini terjadi karena akun disediakan ke dalam OU dengan SCP yang mencegah penghapusan peran IAM. Anda dapat memperpendek proses pemulihan dengan menghapus semua sumber daya akun sebelum Anda mencoba lagi.

Contoh di bawah ini menunjukkan jenis pesan kegagalan yang mungkin Anda terima jika peran dan tumpukan yang tidak dihapus tetap ada. Anda kemungkinan besar akan melihat salah satu pesan ini pada satu waktu, untuk setiap kali Anda mencoba mendaftarkan akun, selama sumber daya lama tetap ada.

Nilai string ID sumber daya telah dimodifikasi untuk contoh. Nilainya tidak akan sama dalam pesan kesalahan yang mungkin Anda terima. Anda mungkin melihat pesan yang mirip dengan contoh berikut:

- `AWS Control Tower cannot create the IAM role aws-controltower-AdministratorExecutionRole because the role already exists. To continue, delete the existing IAM role and try again.`
- `AWS Control Tower cannot create the IAM role aws-controltower-ConfigRecorderRole because the role already exists. To continue, delete the existing IAM role and try again.`
- `AWS Control Tower cannot create the IAM role aws-controltower-ForwardSnsNotificationRole because the role already exists. To continue, delete the existing IAM role and try again.`

Atau Anda mungkin melihat pesan kesalahan tentang kegagalan set tumpukan, mirip dengan yang ini:

```
"Error\":\"StackSetFailState\",
\"Cause\":\"StackSetOperation on AWSControlTowerBP-BASELINE-CLOUDWATCH
with id 8aXXXXf5-e0XX-4XXa-bc4XX-dXXXXXee31
has reached SUCCEEDED state but has 1 NON-CURRENT stack instances;
here is the summary :{ StackSet Id:
AWSControlTowerBP-BASELINE-CLOUDWATCH:40XXXbf2-Xead-46a1-XXXa-eXXXXecb2ee2,
Stack instance Id:
arn:aws:cloudformation:eu-west-1:1X23456789XX:
            stack/StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-4feXXXXXX-ecXX-XXc6-
bXXX-4ae678/4feXXXXXX-ecX-4ae123458,
Status: OUTDATED,
Status Reason: ResourceLogicalId:ForwardSnsNotification,
ResourceType:AWS::Lambda::Function,
ResourceStatusReason:aws-controltower-NotificationForwarder already exists in stack
arn:aws:cloudformation:eu-west-1:1X23456789XX:
            stack/StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-4feXXXXXX-ecXX-XXc6-
bXXX-4ae678/4feXXXXXX-ecX-4ae123458.
```

Setelah semua sumber daya yang tersisa dihapus dari OU pertama, Anda akan dapat mengundang, menyediakan, atau mendaftarkan akun ke OU baru dengan sukses.

AWS Support

Jika Anda ingin memindahkan akun anggota yang ada ke paket dukungan yang berbeda, Anda dapat masuk ke setiap akun dengan kredensi akun root, membandingkan paket, dan mengatur tingkat dukungan yang Anda inginkan.

Kami menyarankan Anda memperbarui MFA dan kontak keamanan akun saat Anda membuat perubahan pada paket dukungan Anda.

Jenis baseline

Garis dasar di AWS Control Tower adalah sekelompok sumber daya dan konfigurasi spesifik yang dapat Anda terapkan ke target. Target dasar yang paling umum mungkin adalah unit organisasi (OU). Misalnya, Anda dapat mengaktifkan baseline dengan OU yang dipilih sebagai target, untuk mendaftarkan OU tersebut ke AWS Control Tower.

Selama pengaturan landing zone, AWS Control Tower secara otomatis mengaktifkan baseline tertentu pada akun integrasi layanan. Ini memungkinkan dan memperbarui baseline ini berdasarkan pengaturan dan konfigurasi landing zone Anda. AWS Control Tower membuat dan menyebarkan sumber daya ke target dengan cara yang ditentukan baseline.

Saat Anda mengaktifkan baseline pada target, baseline direpresentasikan sebagai sumber daya AWS, yang disebut sumber daya. `EnabledBaseline`

AWS Control Tower mencakup dua jenis baseline umum:

- Baseline yang dapat diaktifkan pada OU.
- Garis dasar yang dapat diaktifkan pada akun integrasi layanan, selama pengaturan landing zone.

Jenis dasar yang berlaku di tingkat OU

> **Note**
>
> Hanya Baseline yang berlaku pada level OU yang dapat langsung diaktifkan dengan API. `EnableBaseline`

- Nama: `AWSControlTowerBaseline`

  Deskripsi: Garis dasar ini mengatur sumber daya dan kontrol untuk akun anggota dalam target OU, yang diperlukan untuk pemantauan kepatuhan, audit, pemantauan keamanan, dan, secara opsional, manajemen akses. Garis dasar ini diaktifkan saat Anda mendaftarkan OU di AWS Control Tower.

  Prasyarat: Integrasi AWS Config harus diaktifkan di landing zone AWS Control Tower.

Pertimbangan: Garis dasar ini mempertahankan pengaturan zona pendaratan Wilayah menolak kontrol. Dengan kata lain, jika Region tidak diizinkan di tingkat landing zone, Region tersebut tidak diperbolehkan untuk OU tersebut ketika Anda memanggil `EnableBaseline` API untuk mendaftarkan OU.

> **Note**
>
> OU-level Wilayah menolak kontrol tidak memiliki cara untuk mengizinkan Wilayah yang zona pendaratan yang ditolak oleh Wilayah tidak mengizinkan kontrol.

Untuk informasi selengkapnya, lihat Cara SCP bekerja dengan penolakan dalam AWS Organizations dokumentasi.

Rekomendasi: Kami menyarankan Anda mengonfirmasi Wilayah di mana target OU Anda mungkin menjalankan beban kerja, dan memeriksa hasilnya terhadap landing zone Region deny control, sebelum Anda memanggil `EnableBaseline` API untuk OU, atau Anda bisa kehilangan akses ke sumber daya di Wilayah tertentu.

- Nama: `ConfigBaseline`

  Deskripsi: Garis dasar ini menyiapkan sumber daya terkait AWS Config untuk akun anggota dalam target OU yang diperlukan untuk mengaktifkan Kontrol Detektif. Sumber daya yang disiapkan adalah bagian dari sumber daya dari. AWSControlTowerBaseline

  Prasyarat: Integrasi AWS Config harus diaktifkan di landing zone AWS Control Tower.

  Pertimbangan: Garis dasar ini tidak mempertahankan pengaturan zona pendaratan Wilayah menolak kontrol. Kontrol penolakan wilayah tidak akan diaktifkan sebagai bagian dari pengaktifan ConfigBaseline.

  Batasan: AWSControlTowerBaseline dan ConfigBaseline tidak dapat diaktifkan pada OU yang sama. Hanya satu dari mereka yang diizinkan pada OU.

  > **ConfigBaseline status “Tidak diaktifkan”**
  >
  > Jika OU Anda telah `AWSControlTowerBaseline` diaktifkan, `ConfigBaseline` status ditampilkan sebagai “Tidak diaktifkan.” Ini adalah perilaku yang diharapkan. `AWSControlTowerBaseline`termasuk AWS Config fungsionalitas. Anda tidak

perlu mengaktifkan secara terpisah `ConfigBaseline` pada OU yang sudah ada`AWSControlTowerBaseline`.

- Nama: `BackupBaseline`

  Deskripsi: Garis dasar ini mengatur sumber daya dan kontrol untuk akun anggota dalam OU target. Ini diperlukan agar integrasi dengan AWS Backup dapat mengotomatiskan pencadangan data Anda di seluruh Layanan AWS, dan memusatkan manajemen kebijakan cadangan Anda.

  Prasyarat:

  - Integrasi AWS Backup harus diaktifkan di landing zone AWS Control Tower.
  - Integrasi AWS Config harus diaktifkan di landing zone AWS Control Tower.
  - `AWSControlTowerBaseline`harus diaktifkan pada target OU.

  Pertimbangan: Sebelum Anda mengaktifkan OU target, pastikan bahwa `AWSControlTowerBaseline` diaktifkan pada target OU. `BackupBaseline` Artinya, target OU harus terdaftar di AWS Control Tower.

  - Anda dapat memilih untuk mengaktifkan AWS Backup selama proses pembuatan landing zone AWS Control Tower, atau selama proses pembaruan landing zone.
  - `BackupBaseline`Ini kompatibel dengan landing zone versi 3.1 dan yang lebih baru.
  - `BackupBaseline`Ini tidak diterapkan ke akun manajemen.

Jenis dasar yang berlaku untuk akun integrasi layanan selama penyiapan landing zone

AWS Control Tower memungkinkan baseline tertentu pada akun integrasi layanan, sebagai bagian dari proses penyiapan dan pembaruan landing zone. Garis dasar untuk landing zone Anda dapat berubah saat Anda mengubah pengaturan landing zone. Misalnya, jika Anda memilih IAM Identity Center, AWS Control Tower dapat mengaktifkan versi terbaru dari `IdentityCenterBaseline` baseline di landing zone Anda.

Anda dapat melihat baseline yang diaktifkan untuk landing zone Anda dengan panggilan `ListEnabledBaselines` API.

> **Note**
>
> Dimulai dengan Landing Zone versi 4.0, digantikan oleh dua garis dasar yang berbeda: `CentralSecurityRolesBaseline` dan. AuditBaseline `CentralConfigBaseline`

- Nama: `CentralConfigBaseline`

  Deskripsi: Menyiapkan sumber daya pusat untuk pemantauan dan audit kepatuhan dalam organisasi Anda menggunakan AWS Config.
- Nama: `CentralSecurityRolesBaseline`

  Deskripsi: Menyiapkan sumber daya pusat untuk pemantauan keamanan dalam organisasi Anda.
- Nama: `AuditBaseline`

  Deskripsi: Mengatur sumber daya untuk memantau keamanan dan kepatuhan akun di organisasi Anda.
- Nama: `LogArchiveBaseline`

  Deskripsi: Menyiapkan repositori pusat untuk log aktivitas API dan konfigurasi sumber daya dari akun di organisasi Anda.
- Nama: `IdentityCenterBaseline`

  Deskripsi: Menyiapkan sumber daya bersama untuk IAM Identity Center, yang mempersiapkan `AWSControlTowerBaseline` untuk mengatur akses Pusat Identitas untuk akun.

  Pertimbangan: Garis dasar ini hanya berfungsi ketika Anda telah memilih IAM Identity Center sebagai penyedia identitas Anda pada saat Anda mengatur landing zone Anda pada awalnya, atau jika Anda kemudian mengubah pengaturan landing zone Anda untuk mengaktifkan IAM Identity Center untuk landing zone Anda. Jika Anda menggunakan penyedia identitas yang berbeda, Anda tidak akan memiliki akses untuk mengaktifkan baseline ini.
- Nama: `BackupCentralVaultBaseline`

  Deskripsi: Mengatur lemari AWS Backup besi pusat di organisasi Anda.
- Nama: `BackupAdminBaseline`

  Deskripsi: Menyiapkan admin yang didelegasikan dan AWS Backup Audit Manager.

Pendaftaran sebagian akun

Saat Anda bekerja dengan garis dasar, akun dapat ditempatkan ke status yang disebut Terdaftar sebagian.

Status ini dapat terjadi jika Anda mendaftarkan ulang OU dengan memanggil `ResetEnabledBaseline` API, karena AWS Control Tower hanya menerapkan sumber daya wajib ke akun di OU target. Akun yang kehilangan sumber daya opsional (kontrol) untuk OU induknya ditandai sebagai Terdaftar sebagian.

Jika Anda memindahkan akun yang tidak terdaftar ke OU terdaftar dan kemudian memanggil `ResetEnabledBaseline` API di OU untuk mendaftarkan akun tersebut, AWS Control Tower menerapkan sumber daya yang terkait dengan akun yang `AWSControlTowerBaseline` baru terdaftar. Namun, kontrol opsional yang diaktifkan untuk OU ini tidak diterapkan ke akun. Akun tetap dalam keadaan terdaftar sebagian.

Untuk mendaftarkan akun sepenuhnya, pilih Re-registeratau Perbarui akun di konsol. Saat Anda memilih operasi ini dari konsol, AWS Control Tower menerapkan semua sumber daya OU tersebut ke akun yang baru terdaftar, termasuk kontrol opsional yang diaktifkan untuk OU tersebut.

Variasi dalam operasi antara konsol AWS Control Tower dan API untuk baseline

Saat Anda mengubah status tata kelola OU, konsol AWS Control Tower melakukan lebih banyak operasi untuk Anda secara otomatis, dibandingkan dengan mengubah tata kelola melalui API untuk baseline.

Perbedaan

- Mendaftarkan dan menyediakan produk

  Saat Anda mendaftarkan OU melalui konsol, AWS Control Tower membuat produk Service Catalog untuk akun anggota OU, sebagai bagian dari pendaftaran setiap akun. Saat Anda mendaftarkan OU melalui `EnableBaseline` API dan AWS Control Tower tidak membuat produk yang disediakan untuk akun anggota di OU. `AWSControlTowerBaseline`
- Deregister ke OU

Setiap kali Anda membatalkan pendaftaran OU, Anda harus terlebih dahulu menghapus semua akun anggota dan OU bersarang. Kemudian, AWS Control Tower menghapus semua kontrol yang diterapkan ke OU.

- Jika Anda memilih Hapus OU OU dari konsol, AWS Control Tower melanjutkan ke deregister dan kemudian menghapus OU dari organisasi Anda.
- Namun, jika Anda membatalkan pendaftaran OU dengan memanggil `DisableBaseline` API untuk menghapus `AWSControlTowerBaseline` dari OU, AWS Control Tower tidak menghapus OU dari organisasi Anda, OU masih ada di organisasi, tidak terdaftar.

Diaktifkan baseline dan akun anggota

Saat Anda mengaktifkan baseline pada OU, konfigurasi tersebut diwarisi oleh akun anggota OU. Karena fakta warisan, kami menyebutnya baseline yang diaktifkan anak ketika kami merujuk ke akun. Garis dasar yang diterapkan ke OU disebut baseline yang diaktifkan induk. Garis dasar yang diaktifkan induk mengontrol konfigurasi baseline yang diaktifkan turunannya. Ini mirip dengan bagaimana kontrol, ketika diaktifkan pada OU, berlaku untuk setiap akun dalam OU.

Melihat status dasar akun

AWS Control Tower tidak memungkinkan Anda untuk menargetkan akun secara langsung dengan baseline. Namun, Anda dapat melacak status pemberdayaan dan penyimpangan dari setiap akun anggota melalui baseline yang diaktifkan anak warisan mereka. Untuk melihat status akun Anda, Anda dapat memanggil `ListEnabledBaselines`API dengan tanda `includeChildren` fitur.

Nonaktifkan baseline akun

AWS Control Tower tidak mengizinkan Anda menonaktifkan baseline berkemampuan anak yang ditautkan ke baseline yang diaktifkan induk. Garis dasar yang diaktifkan anak dapat dinonaktifkan jika pewarisannya melayang dan tidak lagi ditautkan ke baseline yang diaktifkan orang tua.

Garis dasar dan default versi

Jika zona landing zone AWS Control Tower Anda sudah disiapkan, dan kemudian Anda memilih untuk mengaktifkan baseline landing zone, AWS Control Tower mengaktifkan versi terbaru dari baseline yang kompatibel dengan versi landing zone Anda. Jika Anda memilih untuk mengaktifkan baseline untuk OU yang belum terdaftar di AWS Control Tower, AWS Control Tower menyediakan versi terbaru yang kompatibel dari baseline untuk OU tersebut, secara otomatis.

Kompatibilitas baseline OU dan versi landing zone

Garis dasar AWS Control Tower memungkinkan Anda menetapkan standar tata kelola di tingkat OU, bukan di tingkat landing zone, jika bisnis Anda memerlukannya. Garis dasar yang disebut `AWSControlTowerBaseline` tersedia untuk membantu mendaftarkan OU Anda dengan AWS Control Tower.

> **Note**
>
> Baseline adalah sekelompok kontrol dan sumber daya yang bekerja sama untuk membangun lingkungan tata kelola yang stabil di dalam landing zone Anda.

Saat Anda mengaktifkan baseline pada OU, dengan memanggil `EnableBaseline` API di AWS Control Tower, Anda harus menentukan versi dasar yang kompatibel dengan versi landing zone AWS Control Tower AWS Control Tower saat ini. Setelah Anda menentukan garis dasar, semua akun anggota dalam OU mengikuti garis dasar yang diberikan untuk OU. Dengan kata lain, akun baru disediakan dengan baseline yang diperbarui, dan akun anggota yang ada diatur sesuai dengan baseline baru.

Jika Anda tidak memilih baseline untuk OU dan akun yang ada, versi landing zone menentukan keseluruhan postur tata kelola, secara default. Namun, setiap OU terdaftar di landing zone Anda diberi versi dasar, yang merupakan baseline terbaru yang kompatibel dengan versi landing zone Anda saat ini. Oleh karena itu, setiap akun anggota OU dan terdaftar memiliki baseline terkait, bahkan jika Anda tidak pernah menetapkan baseline secara khusus.

Untuk OU-level baseline`AWSControlTowerBaseline`, tabel berikut menunjukkan kompatibilitas baseline dengan versi landing zone AWS Control Tower.

Versi dasar	Versi zona pendaratan	Cetak biru yang disertakan	Ubah dari baseline sebelumnya		
1.0	2.0 hingga 2.7	BP_BASELINE_CLOUDTRAIL, BP_BASELINE_CLOUDW	Tidak ada		

Versi dasar	Versi zona pendaratan	Cetak biru yang disertakan	Ubah dari baseline sebelumnya		
		ATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_ROLES, Sumber Daya IAM			
2.0	2,8 hingga 2,9	BP_BASELINE_CLOUDTRAIL, BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_ROLES, Config SLR, sumber daya IAM	Menambahkan peran AWS Config terkait layanan (SLR) dan cetak biru Config baru untuk menggunakan SLR		

Versi dasar	Versi zona pendaratan	Cetak biru yang disertakan	Ubah dari baseline sebelumnya		
3.0	3.0 hingga 3.1	BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_ROLES, Config SLR, sumber daya IAM	AWS Config Cetak biru baru. Ubah untuk merekam sumber daya global hanya di wilayah asal. CloudTrail Cetak biru dihapus		
4.0	3,2 hingga 3,3	BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_LINKED_ROLE, BP_BASELINE_SERVICE_ROLES, Config SLR, sumber daya IAM	Cetak biru SLR baru		

Versi dasar	Versi zona pendaratan	Cetak biru yang disertakan	Ubah dari baseline sebelumnya		
5.0	4.0	BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_LINKED_ROLE, BP_BASELINE_SERVICE_ROLES, Config SLR, sumber daya IAM	Menghapus Otorisasi Agregasi AWS Config. Otorisasi Agregasi AWS Config dari setiap akun anggota tidak diperlukan karena LandingZone versi 4.0 mengadopsi AWS Organizations Config Aggregator yang memiliki akses ke semua akun anggota dalam Organisasi.		

Untuk informasi selengkapnya tentang sumber daya tertentu yang dibuat di akun saat menyiapkan landing zone, lihat Sumber daya yang dibuat di akun bersama.

Jika Anda memperbarui landing zone ke versi yang mendukung versi **`AWSControlTowerBaseline`** baseline yang lebih baru, dan versi landing zone baru kompatibel dengan versi baseline yang ada, status OU Anda berubah menjadi Pembaruan yang tersedia.

- Anda dapat terus menggunakan Account Factory dan fitur lainnya tanpa segera memperbarui baseline unit organisasi (OU).
- Akun baru yang terdaftar di OU ini menerima sumber daya berdasarkan versi baseline yang ada hingga versi dasar diperbarui (dengan fitur Perluas tata kelola di konsol, atau melalui API). `UpdateEnabledBaseline`
- Setelah Anda memperbarui versi dasar, semua akun dalam OU tersebut menerima sumber daya berdasarkan versi dasar yang baru.

> **Note**
>
> Setelah memperbarui versi landing zone AWS Control Tower, jika OU menunjukkan status Pembaruan yang diperlukan di konsol, Anda harus memperbarui versi dasar pada OU tersebut.

Pertimbangan untuk baseline

- Jika OU Anda memerlukan pembaruan dasar, Anda tidak dapat menyediakan akun baru atau mendaftarkan akun yang ada ke OU tersebut.
- Setelah pembaruan landing zone, jika Anda juga berencana untuk memperbarui baseline OU, Anda harus mendaftarkan ulang OU atau memperbarui versi dasar OU Anda secara terprogram.
- Kami menyarankan Anda memperbarui ke baseline tertinggi yang kompatibel untuk versi landing zone yang Anda gunakan, sehingga Anda mendapatkan semua manfaat dari landing zone dan baseline gabungan. Misalnya, jika Anda memperbarui ke landing zone versi 3.3, Anda dapat tetap menggunakan baseline 3.0, tetapi Anda tidak mendapatkan setiap manfaat dari landing zone versi 3.3 kecuali Anda juga memperbarui ke baseline 4.0.
- Pembaruan dasar tidak dapat diputar kembali.
- Pemberdayaan dasar menargetkan satu OU pada satu waktu. Oleh karena itu, OU bersarang tidak diperbarui secara otomatis saat OU induk diperbarui. Kami menyarankan Anda memperbarui OU induk sebelum memperbarui OU bersarang.
- Saat Anda memanggil `UpdateEnabledBaseline` API atau mendaftarkan ulang OU dari konsol, OU mempertahankan semua kontrol yang diaktifkan sebelum pembaruan dasar.
- Bila beberapa versi baseline kompatibel dengan versi landing zone Anda, Anda harus menggunakan versi baseline terbaru jika Anda mengaktifkan baseline pada OU yang tidak dikelola.

Contoh: Mendaftarkan OU AWS Control Tower dengan API saja

Panduan contoh ini adalah dokumen pendamping. Untuk penjelasan, peringatan, dan informasi lebih lanjut, lihatJenis baseline.

Prasyarat

Anda harus memiliki OU yang sudah ada yang tidak terdaftar di AWS Control Tower, dan yang ingin Anda daftarkan. Atau, Anda harus memiliki OU terdaftar yang ingin Anda daftarkan ulang untuk tujuan pembaruan.

Daftarkan OU

1. Periksa apakah `IdentityCenterBaseline` diaktifkan untuk zona pendaratan. Jika demikian, dapatkan Identity Center Enabled Baseline Identity Center.

```
aws controltower list-baselines --query 'baselines[?name==`IdentityCenterBaseline`].
[arn]'
```

```
aws controltower list-enabled-baselines --query 'enabledBaselines[?
baselineIdentifier==`<Identity Center Baseline Arn>`].[arn]'
```

2. Dapatkan ARN dari OU target.

```
aws organizations describe-organizational-unit --organizational-unit-id
 <Organizational Unit ID> --query 'OrganizationalUnit.[Arn]'
```

3. Dapatkan ARN dari `AWSControlTowerBaseline` baseline.

```
aws controltower list-baselines --query 'baselines[?name==`AWSControlTowerBaseline`].
[arn]'
```

4. Buat garis `AWSControlTowerBaseline` dasar pada OU target.

   Jika Identity Center Baseline diaktifkan:

```
aws controltower enable-baseline --baseline-identifier <AWSControlTowerBaseline ARN>
 --baseline-version <BASELINE VERSION> --target-identifier <OU ARN> --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"<Identity Center Enabled
 Baseline ARN>"}]'
```

Jika Identity Center Baseline tidak diaktifkan, hilangkan *`parameters`* bendera, sebagai berikut:

```
aws controltower enable-baseline --baseline-identifier <AWSControlTowerBaseline ARN>
 --baseline-version <BASELINE VERSION> --target-identifier <OU ARN>
```

Re-register un OU

Setelah melakukan pembaruan pada pengaturan zona pendaratan, atau memperbarui versi zona pendaratan Anda, Anda harus Re-register melakukan OU untuk memberikan perubahan terbaru kepada mereka. Ikuti langkah-langkah ini untuk mendaftarkan ulang OU secara terprogram, dengan mengatur ulang sumber daya terkait dan `EnabledBaseline` sumber daya terkait. `EnabledControl`

> **Important**
>
> Jika OU memiliki kontrol opsional yang diaktifkan, Anda juga harus memanggil `ResetEnabledControl` API untuk setiap kontrol opsional yang diaktifkan setelah mengatur ulang baseline. Langkah ini memastikan bahwa kontrol opsional tetap konsisten dengan konfigurasi zona pendaratan terbaru. Jika Anda melewati langkah ini, kontrol opsional pada OU mungkin tidak mencerminkan perubahan zona pendaratan terbaru. Jika Anda tidak mengaktifkan kontrol opsional, langkah ini tidak diperlukan.

1. Dapatkan ARN dari OU target untuk mendaftar ulang.

```
aws organizations describe-organizational-unit --organizational-unit-id <OU ID> --
query 'OrganizationalUnit.[Arn]'
```

2. Dapatkan ARN sumber `EnabledBaseline` daya untuk OU target.

```
aws controltower list-enabled-baselines --query 'enabledBaselines[?
targetIdentifier==`<OUARN>`].[arn]'
```

3. Setel ulang Baseline yang Diaktifkan.

```
aws controltower reset-enabled-baseline --enabled-baseline-
identifier <EnabledBaselineArn>
```

4. Jika OU memiliki kontrol opsional yang diaktifkan, daftarkan kontrol yang diaktifkan untuk OU dan atur ulang masing-masing kontrol sehingga tetap konsisten dengan konfigurasi zona pendaratan terbaru.

   Daftar kontrol yang diaktifkan pada OU target:

   ```
   aws controltower list-enabled-controls --target-identifier <OU ARN>
   ```

   Untuk setiap kontrol opsional yang diaktifkan dikembalikan, atur ulang dengan memanggil:

   ```
   aws controltower reset-enabled-control --enabled-control-
   identifier <EnabledControlArn>
   ```

   Untuk informasi selengkapnya, lihat ResetEnabledControl Referensi API AWS Control Tower.

Contoh untuk penggunaan API baseline

Bagian ini berisi contoh parameter input dan output untuk API dasar AWS Control Tower.

`DisableBaseline`

Untuk informasi selengkapnya tentang operasi API ini, lihat DisableBaseline.

`DisableBaseline`masukan:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789"
}
```

`DisableBaseline`keluaran:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
}
```

`DisableBaseline`Contoh CLI:

```
aws controltower disable-baseline \
```

```
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/AB12CD34EF56GH789 \
    --region us-west-2
```

EnableBaseline

Untuk informasi selengkapnya tentang operasi API ini, lihat EnableBaseline.

`EnableBaseline`masukan:

```
{
    "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline:17BSJV3IGJ2QSGA2",
    "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/ou-
r9mj-4j3mzjql",
    "baselineVersion": "3.0",
    "parameters": [
        {
            "key": "IdentityCenterEnabledBaselineArn",
            "value": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
        }
    ]
}
```

`EnableBaseline`output, mengembalikan sumber daya baru:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f",
    "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAGF7TNOHRD7ES5VV"
}
```

`EnableBaseline`Contoh CLI:

Contoh ini menunjukkan mengaktifkan baseline untuk AWS Organizations organisasi yang memiliki landing zone yang ikut serta ke akses AWS IAM Identity Center, yang dikelola oleh AWS Control Tower. Untuk mengambil `EnabledBaseline` identifier Pusat Identitas Anda, Anda dapat memanggil `ListEnabledBaselines` API, memfilter pada garis dasar Pusat Identitas: `(arn:aws:controltower:`*`Region`*`::baseline/LN25R72TTG6IGPTQ)`

```
aws controltower list-enabled-baselines \
```

```
    --filter baselineIdentifiers=arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ \
    --region us-west-2
```

Respons akan menunjukkan `EnabledBaseline` detail, yang menunjukkan pengenalnya.

```
{
    "enabledBaselines": [
        {
            "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHXS7P6C4I453EZC",
            "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ",
            "targetIdentifier": "arn:aws:organizations::123456789012:account/o-
aq21sw43de5/123456789012",
            "statusSummary": {
                "status": "SUCCEEDED"
            }
        }
    ]
}
```

> **Note**
>
> Catat nilai ARN dari respons, dan berikan nilai ini sebagai parameter untuk mengaktifkan baseline default.

```
aws controltower enable-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --baseline-version 3.0 \
    --target-identifier arn:aws:organizations::123456789012:ou/o-aq21sw43de5/ou-po90-
lk87jh65 \
    --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC"}]' \
    --region us-west-2
```

Untuk organisasi dengan landing zone opted-out dari manajemen AWS Control Tower IAM Identity Center, aktifkan baseline tanpa parameter.

```
aws controltower enable-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --baseline-version 3.0 \
    --target-identifier arn:aws:organizations::123456789012:ou/o-aq21sw43de5/ou-po90-
lk87jh65 \
    --region us-west-2
```

GetBaseline

Untuk informasi selengkapnya tentang operasi API ini, lihat GetBaseline.

`GetBaseline`masukan:

```
{
    "baselineIdentifier": "arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2"
}
```

`GetBaseline`keluaran:

```
{
    "arn": "arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2",
    "name": "AWSControlTowerBaseline",
    "description": "Sets up resources and mandatory controls for member accounts within
 the target OU, required for AWS Control Tower governance.",
}
```

`GetBaseline`Contoh CLI:

```
aws controltower get-baseline \
    --baseline-identifier arn:aws:controltower:us-west-2::baseline/17BSJV3IGJ2QSGA2 \
    --region us-west-2
```

GetBaselineOperation

Untuk informasi selengkapnya tentang operasi API ini, lihat GetBaselineOperation.

`GetBaselineOperation`masukan:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
```

```
}
```

`GetBaselineOperation`keluaran:

```
{
    "baselineOperation": {
        "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f",
        "operationType": "DISABLE_BASELINE",
        "status": "FAILED",
        "startTime": "2023-01-12T19:05:00Z",
        "endTime": "2023-01-12T19:45:00Z",
        "statusMessage": "Can't perform DisableBaseline on a parent target with
 governed child OUs"
    }
}
```

`GetBaselineOperation`Contoh CLI:

```
aws controltower get-baseline-operation \
    --operation-identifier 58f12232-26be-4735-a3e9-dd30d90f021f \
    --region us-west-2
```

`GetEnabledBaseline`

Untuk informasi selengkapnya tentang operasi API ini, lihat GetEnabledBaseline.

`GetEnabledBaseline`masukan:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHCR4CJTSI4W07MZ"
}
```

`GetEnabledBaseline`keluaran:

```
{
    "enabledBaselineDetails": {
        "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ",
        "baselineIdentifier": "arn:aws:controltower:us-
west-2::baseline:17BSJV3IGJ2QSGA2",
```

```
        "baselineVersion": "3.0",
        "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/ou-
r9mj-4j3mzjql",
        "statusSummary": {
            "status": "SUCCEEDED",
            "lastOperationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
        },
        "parameters": [
            {
                "key": "IdentityCenterEnabledBaselineArn",
                "value": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
            }
        ]
    }
}
```

`GetEnabledBaseline`Contoh CLI:

```
aws controltower get-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
    --region us-west-2
```

`ListBaselines`

Untuk informasi selengkapnya tentang operasi API ini, lihat ListBaselines.

`ListBaselines`input (menggunakan input opsional):

```
{
    "nextToken": "AbCd1234",
    "maxResults": "4"
}
```

`ListBaselines`keluaran:

```
{
    "baselines": [
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/4T4HA1KMO10S6311",
            "name": "AuditBaseline",
```

```
            "description": "Sets up resources to monitor security and compliance of
 accounts in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/J8HX46AHS5MIKQPD",
            "name": "LogArchiveBaseline",
            "description": "Sets up a central repository for logs of API activities and
 resource configurations from accounts in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/LN25R72TTG6IGPTQ",
            "name": "IdentityCenterBaseline",
            "description": "Sets up shared resources for AWS Identity Center, which
 prepares the AWSControlTowerBaseline to set up Identity Center access for accounts."
        },
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/17BSJV3IGJ2QSGA2",
            "name": "AWSControlTowerBaseline",
            "description": "Sets up resources and mandatory controls for member
 accounts within the target OU, required for AWS Control Tower governance."
        },
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/3WPD0NA6TJ9AOMU2",
            "name": "BackupCentralVaultBaseline",
            "description": "Sets up central AWS Backup vault in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/H6C5JFCJJ3CPU3J5",
            "name": "BackupAdminBaseline",
            "description": "Sets up delegated admin and AWS Backup Audit Manager."
        },
        {
            "arn": "arn:aws:controltower:us-east-1::baseline/APO9ATVPBKFRRGLK",
            "name": "BackupBaseline",
            "description": "Sets up local Backup vault and attach Backup policy."
        }
    ]
}
```

`ListBaselines`Contoh CLI:

```
aws controltower list-baselines \
    --region us-west-2
```

ListEnabledBaselines

`ListEnabledBaselines`API memiliki parameter opsional yang memungkinkan Anda untuk melihat garis dasar yang berlaku untuk akun yang merupakan anggota OU. Contoh berikut menunjukkan beberapa perintah CLI yang dapat Anda gunakan untuk melihat garis dasar untuk akun. AWS Control Tower mengacu pada baseline ini, yang diaktifkan pada OU, tetapi berlaku untuk setiap akun dalam OU, sebagai baseline yang diaktifkan anak, karena mereka memperoleh konfigurasi tata kelola mereka dari baseline yang diterapkan pada OU.

Untuk informasi selengkapnya tentang operasi API ini, lihat ListEnabledBaselines.

`ListEnabledBaselines`masukan untuk menampilkan baseline yang diaktifkan anak:

```
aws controltower list-enabled-baselines --include-children
```

`ListEnabledBaselines`output untuk melihat garis dasar yang diaktifkan anak:

```
{
    "enabledBaselines": [
        {
            "arn": "arn:aws:controltower:us-east-1:666355521292:enabledbaseline/
XO2UQ1PC6BB5085S5",
            "baselineIdentifier": "arn:aws:controltower:us-east-1::baseline/
APO9ATVPBKFRRGLK",
            "baselineVersion": "1.0",
            "statusSummary": {
                "lastOperationIdentifier": "07d6d2b8-e357-4f96-ba00-98ea88143445",
                "status": "SUCCEEDED"
            },
            "targetIdentifier": "arn:aws:organizations::666355521292:ou/o-vaex10vaey/
ou-k86y-ld9k8vpu"
        },
        {
            "arn": "arn:aws:controltower:us-east-1:666355521292:enabledbaseline/
XAFPKQQXOJB50ZWQH",
            "baselineIdentifier": "arn:aws:controltower:us-east-1::baseline/
APO9ATVPBKFRRGLK",
            "baselineVersion": "1.0",
            "parentIdentifier": "arn:aws:controltower:us-
east-1:666355521292:enabledbaseline/XOIZ4G08CWB50ZWON",
            "statusSummary": {
                "lastOperationIdentifier": "3508793e-48c8-4895-965b-3dc6abd52b6b",
```

```
                "status": "SUCCEEDED"
            },
            "targetIdentifier": "arn:aws:organizations::666355521292:account/o-
vaex10vaey/183295447314"
        }
]
```

> **Note**
>
> Pada contoh sebelumnya, `parentIdentifier` bidang menunjukkan baseline yang diaktifkan dari OU induk untuk baseline yang diaktifkan anak ini.

Lihat semua baseline yang diterapkan pada target tertentu (OU atau akun):

```
aws controltower list-enabled-baselines \
    --filter '{
        "targetIdentifiers": ["TARGET_ARN"]
    }
```

Lihat semua OU yang memiliki garis dasar tertentu:

```
aws controltower list-enabled-baselines \
    --filter '{
        "baselineIdentifiers": ["BASELINE_ARN"]
    }'
```

Lihat semua OU dan akun yang memiliki baseline tertentu:

```
aws controltower list-enabled-baselines \
    --filter '{
        "baselineIdentifiers": ["BASELINE_ARN"]
    }'  \
    --include-children
```

Lihat semua akun di OU yang mengaktifkan Baseline B:

```
### First fetch the enabled baseline record for Baseline B on the OU
 aws controltower list-enabled-baselines \
    --filter '{
```

```
        "targetIdentifiers": ["OU_TARGET_ARN"],
        "baselineIdentifiers": ["BASELINE_ARN_FOR_BASELINE_B"]
    }'

### Call ListEnabled baseline to fetch all accounts that have their parent as the
 enabled baseline record on the OU
aws controltower list-enabled-baselines \
    --filter '{
        "parentIdentifiers": ["ENABLED_BASELINE_ARN_FOR_OU"]
    }' \
    --include-children
```

Lebih lanjut tentang baseline yang diaktifkan anak

- Anda dapat menggunakan `GetEnabledBaseline` API untuk melihat informasi mendetail tentang baseline yang diaktifkan anak tertentu
- Anda dapat menggunakan `GetBaselineOperation` API untuk melihat operasi yang dilakukan pada baseline yang diaktifkan anak
- Anda tidak dapat memanggil API tulis apa pun, seperti`EnableBaseline`,, `ResetEnabledBaseline` atau `UpdateEnabledBaselineDisableBaseline`, pada baseline yang diaktifkan anak secara langsung.
- Sumber daya dasar yang diaktifkan anak dapat dimodifikasi hanya dengan menggunakan layanan AWS Control Tower, melalui operasi yang dilakukan pada OU induk, atau melalui Account Factory.

Contoh untuk menggunakan filter:

`ListEnabledBaselines`masukan (tidak ada filter):

```
{
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

`ListEnabledBaselines`input (hanya `baselineIdentifiers` filter):

```
{
    "filter": {
```

```
        "baselineIdentifiers": ['arn:aws:controltower:us-
east-1::baseline/17BSJV3IGJ2QSGA2', 'arn:aws:controltower:us-
east-1::baseline/12GZU8CKZKVMS2AW']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

`ListEnabledBaselines`input (hanya `targetIdentifiers` filter):

```
{
    "filter": {
        "targetIdentifiers": ['arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-
xqj7-fex1u317', 'arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-xqj7-11q6n2cf']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 2
}
```

`ListEnabledBaselines`masukan (`baselineIdentifiers`dan `targetIdentifiers` filter):

```
{
    "filter": {
        "baselineIdentifiers": ['arn:aws:controltower:us-
east-1::baseline/17BSJV3IGJ2QSGA2']
        "targetIdentifiers": ['arn:aws:organizations::123456789012:ou/o-s9511vn103/ou-
xqj7-fex1u317']
    },
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
}
```

`ListEnabledBaselines`keluaran:

```
{
    "enabledBaselines": [
        {
            "arn": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ",
            "baselineIdentifier": "arn:aws:controltower:us-
east-1::baseline:17BSJV3IGJ2QSGA2",
            "baselineVersion": "3.0",
```

```
            "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-kgj0txdhpa/
ou-r9mj-4j3mzjql",
            "statusSummary": {
                "status": "SUCCEEDED",
                "lastOperationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f"
            }
        },
        {
            "arn": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAJ9NKW88AA4W9CLL",
            "baselineIdentifier": "arn:aws:controltower:us-
east-1::baseline:17BSJV3IGJ2QSGA2",
            "baselineVersion": "4.0",
            "targetIdentifier": "arn:aws:organizations::123456789012:ou/o-s9511vn103/
ou-xqj7-fex1u317",
            "statusSummary": {
            "status": "FAILED",
                "lastOperationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
            }
        }
    ],
    "nextToken": "e2bXXXXX6cab"
}
```

Contoh CLI dengan satu jenis filter (`baselineIdentifiers`filter):

```
aws controltower list-enabled-baselines \
    --filter baselineIdentifiers=arn:aws:controltower:us-
west-2::baseline/17BSJV3IGJ2QSGA2,arn:aws:controltower:us-west-2::baseline/
LN25R72TTG6IGPTQ \
    --region us-west-2
```

Contoh CLI menggunakan beberapa filter (`baselineIdentifiers`dan `targetIdentifiers` filter):

```
aws controltower list-enabled-baselines \
    --filter targetIdentifiers=arn:aws:organizations::123456789012:ou/o-
aq21sw43de5/ou-po90-lk87jh65,baselineIdentifiers=arn:aws:controltower:us-
west-2::baseline/17BSJV3IGJ2QSGA2 \
    --region us-west-2
```

ResetEnabledBaseline

Untuk informasi selengkapnya tentang operasi API ini, lihat ResetEnabledBaseline.

`ResetEnabledbaseline`masukan:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAJ9NKW88AA4W9CLL"
}
```

`ResetEnabledBaseline`keluaran:

```
{
    "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

`ResetEnabledBaseline`Contoh CLI:

```
aws controltower reset-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
    --region us-west-2
```

UpdateEnabledBaseline

Untuk informasi selengkapnya tentang operasi API ini, lihat UpdateEnabledBaseline.

`UpdateEnabledBaseline`masukan:

```
{
    "enabledBaselineIdentifier": "arn:aws:controltower:us-
east-1:123456789012:enabledbaseline/XAJ9NKW88AA4W9CLL",
    "baselineVersion": "4.0",
    "parameters": [
        {
            "key": "IdentityCenterEnabledBaselineArn",
            "value": "arn:aws:controltower:us-east-1:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
        }
    ]
```

```
}
```

`UpdateEnabledBaseline`keluaran:

```
{
    "operationIdentifier": "81e02df1-2b4d-48f0-838f-3833b93dcdc0"
}
```

`UpdateEnabledBaseline`Contoh CLI:

```
aws controltower update-enabled-baseline \
    --enabled-baseline-identifier arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC \
    --baseline-version 4.0
    --parameters
 '[{"key":"IdentityCenterEnabledBaselineArn","value":"arn:aws:controltower:us-
west-2:123456789012:enabledbaseline/XAHXS7P6C4I453EZC"}]' \
    --region us-west-2
```

Informasi dan tautan tambahan

Topik ini mencakup tautan ke posting blog yang relevan, dokumentasi teknis, dan informasi terkait yang dapat membantu Anda saat Anda bekerja dengan AWS Control Tower. Sumber mencakup beberapa kasus penggunaan umum dan praktik terbaik untuk kemampuan AWS Control Tower, dan beberapa peningkatan tambahan.

Tutorial dan lab

- Lab Menara Kontrol AWS — Laboratorium ini memberikan gambaran tingkat tinggi tentang tugas-tugas umum yang terkait dengan AWS Control Tower.
- Pada dasbor AWS Control Tower, pilih Dapatkan panduan yang dipersonalisasi jika Anda memiliki kasus penggunaan dalam pikiran tetapi Anda tidak yakin harus mulai dari mana.
- Coba kunjungi YouTube daftar putar AWS Cloud Operations ini dan cari AWS Control Tower untuk menemukan video yang menjelaskan lebih lanjut tentang cara menggunakan fungsionalitas AWS Control Tower.

Jaringan

Siapkan pola yang dapat diulang dan dikelola untuk jaringan di AWS. Pelajari lebih lanjut tentang desain, otomatisasi, dan peralatan yang biasa digunakan oleh pelanggan.

- AWS Mulai Cepat Arsitektur VPC — Panduan Memulai Cepat ini menyediakan landasan jaringan berdasarkan praktik AWS terbaik untuk infrastruktur AWS Cloud Anda. Ini membangun AWS Virtual Private Network lingkungan dengan subnet publik dan pribadi di mana Anda dapat meluncurkan AWS layanan dan sumber daya lainnya.
- Self-service VPC di AWS Control Tower menggunakan Katalog Layanan AWS — Posting blog ini menjelaskan cara mengatur Account Factory sehingga Anda dapat menyediakan akun dengan VPC khusus.
- Menerapkan Serverless Transit Network Orchestrator (STNO) di AWS Control Tower — Posting blog ini menunjukkan cara mengotomatiskan akses konektivitas jaringan di seluruh akun. Blog ini ditujukan untuk administrator AWS Control Tower, atau mereka yang bertanggung jawab untuk mengelola jaringan di AWS lingkungan mereka.

Keamanan, identitas, dan pencatatan

Perluas postur keamanan Anda, integrasikan dengan penyedia identitas eksternal atau yang sudah ada, dan pusatkan sistem pencatatan.

Keamanan

- Mengotomatiskan Per AWS Security Hub CSPM ingatan dengan peristiwa siklus hidup AWS Control Tower — Posting blog ini menjelaskan cara mengotomatiskan pengaktifan dan konfigurasi Security Hub CSPM di lingkungan multi-akun AWS Control Tower pada akun yang ada dan yang baru.
- Mengaktifkan AWS Identity and Access Management — Posting blog ini menjelaskan cara meningkatkan visibilitas keamanan organisasi Anda dengan mengaktifkan dan memusatkan temuan Penganalisis Akses IAM.
- AWS Systems Manager Parameter Store menyediakan penyimpanan hierarkis yang aman untuk manajemen data konfigurasi dan manajemen rahasia. Anda dapat menggunakannya untuk berbagi informasi konfigurasi di lokasi yang aman, untuk digunakan oleh AWS Systems Manager dan oleh AWS CloudFormation. Misalnya, Anda dapat menyimpan daftar Wilayah tempat Anda ingin menerapkan paket kesesuaian.

Identitas

- Tautkan identitas pengguna Azure AD ke AWS akun dan aplikasi untuk masuk tunggal — Posting blog ini menjelaskan cara menggunakan Azure AD dengan IAM Identity Center dan AWS Control Tower.
- Kelola akses ke AWS secara terpusat untuk pengguna Okta dengan AWS IAM Identity Center — Posting blog ini menjelaskan cara menggunakan Okta dengan IAM Identity Center dan AWS Control Tower.

Pencatatan log

- AWS Solusi Pencatatan Terpusat — Posting solusi ini menjelaskan solusi Pencatatan Terpusat yang memungkinkan organisasi mengumpulkan, menganalisis, dan menampilkan log AWS di beberapa akun dan Wil AWS ayah.
- Untuk informasi tentang melihat AWS Config sumber daya Anda, lihat Dasbor Kepatuhan Sumber Daya Konfigurasi.

Menyebarkan sumber daya dan mengelola beban kerja

Menyebarkan dan mengelola sumber daya dan beban kerja.

- Memulai Integrasi Perpustakaan - Posting blog ini menjelaskan portofolio Memulai yang dapat Anda gunakan.
- Penyebaran Cloud Custodian secara berkelanjutan ke AWS Control Tower

Bekerja dengan organisasi dan akun yang ada

Bekerja dengan AWS organisasi dan akun yang ada.

- Mendaftar kan akun — Topik panduan pengguna ini menjelaskan cara mendaftarkan AWS akun yang ada di AWS Control Tower.
- Bawa akun di bawah AWS Control Tower — Posting blog ini menjelaskan cara menerapkan AWS Control Tower ke AWS organisasi Anda yang sudah ada.
- Perluas tata kelola AWS Control Tower menggunakan paket kesesuaian AWS Config — Posting blog ini menjelaskan cara menerapkan paket AWS Config kesesuaian untuk membantu membawa akun dan organisasi yang ada ke dalam tata kelola oleh AWS Control Tower.
- Cara Mendeteksi dan Mengurangi Pelanggaran Guardrail dengan AWS Control Tower — Posting blog ini menjelaskan cara menambahkan kontrol dan cara berlangganan notifikasi SNS sehingga Anda dapat diberitahu melalui email tentang pelanggaran kepatuhan kontrol.

Otomatisasi dan integrasi

Otomatiskan pembuatan akun dan integrasikan peristiwa siklus hidup dengan AWS Control Tower.

- Peristiwa siklus hidup — Posting blog ini menjelaskan cara menggunakan peristiwa siklus hidup dengan AWS Control Tower.
- Otomatisasi pembuatan akun — Posting blog ini menjelaskan cara mengatur pembuatan akun otomatis di AWS Control Tower.
- Otomatisasi log aliran Amazon VPC — Posting blog ini menjelaskan cara mengotomatiskan dan memusatkan Log Aliran Amazon VPC di lingkungan multi-akun.

- Otomatiskan penandaan VPC dengan peristiwa siklus hidup AWS Control Tower — Posting blog ini menjelaskan cara mengotomatiskan penandaan sumber daya untuk VPC, melalui peristiwa siklus hidup di AWS Control Tower.
- Manajemen akun otomatis — Posting blog ini menjelaskan cara mengotomatiskan tugas manajemen akun setelah lingkungan Menara Kontrol AWS Anda diatur.

Migrasi beban kerja

Gunakan AWS layanan lain dengan AWS Control Tower untuk membantu migrasi beban kerja.

- CloudEndure migrasi — Posting blog ini menjelaskan cara menggabungkan CloudEndure dan AWS layanan lainnya dengan AWS Control Tower untuk membantu migrasi beban kerja.

Layanan AWS terkait

AWS Control Tower bertindak sebagai lapisan orkestrasi untuk AWS Organizations. Oleh karena itu, melalui konsol AWS Organizations dan API, Anda memiliki akses ke lebih dari 20 layanan AWS lain yang bekerja dengan AWS Control Tower. Layanan tambahan ini tidak dapat diakses secara langsung melalui konsol AWS Control Tower.

- Untuk daftar lengkap layanan yang tersedia untuk AWS Control Tower melalui AWS Organizations, lihat Layanan AWS yang dapat Anda gunakan dengan AWS Organizations.
- Untuk mengaktifkan kemampuan multi-akun untuk layanan AWS terkait ini, Anda harus mengaktifkan akses tepercaya. Untuk informasi selengkapnya, lihat Menggunakan Organisasi AWS dengan layanan AWS lainnya.

  > **Note**
  >
  > Ingatlah bahwa Pusat Identitas AWS IAM AWS Config,, dan AWS CloudTrail disiapkan untuk Anda di AWS Control Tower dan terintegrasi sepenuhnya. Anda tidak perlu mengubah akses tepercaya atau pengaturan administrasi yang didelegasikan untuk layanan ini.

- Beberapa AWS layanan yang tersedia AWS Organizations dapat menggunakan administrasi yang didelegasikan, termasuk AWS Systems Manager dan AWS Firewall Manager. Untuk informasi selengkapnya, lihat Meng konfigurasi Administrator yang Delegasi, dan Mengaktifkan akun

administrator yang didelegasikan untuk Firewall Manager. Lihat juga video ini, Mengatur grup keamanan dengan AWS Firewall Manager.

AWS Marketplace jawaban

Temukan solusi dari AWS Marketplace.

- AWS Control Tower Marketplace — AWS Marketplace menawarkan berbagai solusi untuk AWS Control Tower untuk membantu Anda mengintegrasikan perangkat lunak pihak ketiga. Solusi ini membantu memecahkan infrastruktur utama dan kasus penggunaan operasional termasuk manajemen identitas, keamanan untuk lingkungan multi-akun, jaringan terpusat, intelijen operasional, dan informasi keamanan dan manajemen acara (SIEM).

Catatan rilis AWS Control Tower

Bagian berikut menunjukkan detail tentang rilis AWS Control Tower, sejak dimulainya layanan. Beberapa rilis memerlukan pembaruan untuk landing zone AWS Control Tower, dan rilis lainnya dimasukkan ke dalam layanan secara otomatis.

Fitur dan rilis terdaftar dalam urutan kronologis terbalik (terbaru pertama) berdasarkan tanggal di mana mereka secara resmi diumumkan kepada publik.

Topik

- Januari 2026 - Sekarang
- Januari 2025 - Desember 2025
- Januari - Desember 2024
- Januari - Desember 2023
- Januari - Desember 2022
- Januari - Desember 2021
- Januari - Desember 2020
- Juni - Desember 2019

Januari 2026 - Sekarang

Sejak Januari 2026, AWS Control Tower telah merilis pembaruan berikut:

- Account Factory for Terraform (AFT) mendukung proses penyesuaian khusus paket
- AWS Control Tower tersedia di European Sovereign Cloud

Account Factory for Terraform (AFT) mendukung proses penyesuaian khusus paket

September 16, 2026

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

Kerangka kerja kustomisasi akun AWS Control Tower, Account Factory for Terraform (AFT), kini mendukung proses penyesuaian khusus paket (hanya-baca). Anda dapat meneruskan

`plan_only` input ke mesin `aft-invoke-customizations` status untuk melihat pratinjau perubahan Terraform yang akan diterima akun. Ini memungkinkan Anda meninjau perubahan tanpa menerapkannya. AFT berjalan `terraform plan` alih-alih `terraform apply` di semua distribusi Terraform yang didukung. AFT dapat mengekspor output paket JSON ke bucket Amazon S3 terenkripsi di akun manajemen AFT. Pada distribusi Community Edition (open source), AFT mengekspor output secara default. Di Terraform Cloud dan Terraform Enterprise, ekspor ikut serta`aft_plan_output_export_enabled`, dan Anda juga dapat melihat hasil di UI run HCP Terraform.

Untuk informasi selengkapnya, lihat Penyesuaian akun.

AWS Control Tower tersedia di European Sovereign Cloud

Januari 13, 2026

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

AWS Control Tower sekarang tersedia di European Sovereign Cloud. Untuk informasi selengkapnya tentang AWS Control Tower di European Sovereign Cloud, lihat Panduan Pengguna AWS Control Tower untuk European Sovereign Cloud.

Januari 2025 - Desember 2025

Sejak Januari 2025, AWS Control Tower telah merilis pembaruan berikut:

- Zona pendaratan Menara Kontrol AWS versi 4.0
- AWS Control Tower menambahkan 279 tambahan AWS Config kontrol ke Katalog Kontrol
- AWS Control Tower tersedia di Wilayah Asia Pasifik (Selandia Baru)
- AWS Control Tower mendukung pendaftaran akun otomatis
- AWS Control Tower memperbarui versi Python
- AWS Control Tower mendukung alamat IPv6
- AWS Control Tower mengurangi penyimpangan

  Account Factory untuk Terraform versi 1.15.0 tersedia
- Kontrol yang diperbarui dengan jenis instance Nitro
- AWS Control Tower tersedia di Wilayah Asia Pasifik (Taipei)
- Mendukung Menara Kontrol AWS PrivateLink

- Dukungan untuk kerangka kerja industri tambahan, metadata yang diperbarui
- Service-linked AWS Config mengendalikan
- Tampilan konsol kontrol yang diaktifkan memberikan visibilitas terpusat
- the section called “Account Factory for Terraform (AFT) mendukung konfigurasi baru saat penerapan”
- AWS Control Tower memperkenalkan pelaporan tingkat akun untuk API dasar
- the section called “AWS Control Tower tersedia di AWS Wilayah Asia Pasifik (Thailand) dan Meksiko (Tengah)”
- Tambahan AWS Config kontrol tersedia
- Menghapus pendaftaran dan menghapus tindakan untuk OU
- the section called “Katalog Kontrol mendukung alamat IPv6”

Zona pendaratan Menara Kontrol AWS versi 4.0

November 17, 2025

(Diperlukan pembaruan untuk zona pendaratan AWS Control Tower ke versi 4.0. Untuk informasi, lihatPerbarui landing zone Anda).

Zona pendaratan AWS Control Tower 4.0 adalah pembaruan besar yang memperkenalkan Controls-Only pengalaman fleksibel, memungkinkan pelanggan menyesuaikan cara mereka menerapkan dan mengelola lingkungan multi-akun AWS mereka. Rilis ini secara signifikan mengubah cara AWS Control Tower terintegrasi dengan layanan AWS dan mengelola sumber daya organisasi. Untuk informasi tentang perubahan utama, lihatPanduan migrasi Landing Zone v4.0.

Perubahan dan Fitur Utama

- Integrasi Layanan Opsional - zona pendaratan 4.0 memungkinkan Anda memilih integrasi layanan mana yang akan diaktifkan di lingkungan Anda. Menonaktifkan integrasi akan membersihkan sumber daya AWS Control Tower yang digunakan khusus untuk integrasi tersebut di akun terkelola dan akun pusat integrasi layanan. Anda sekarang dapat secara selektif mengaktifkan atau menonaktifkan integrasi layanan:
  - AWS Config
  - AWS CloudTrail
  - Peran Keamanan

- AWS Backup

Penting: Jika Anda ingin menonaktifkan integrasi AWS Config, Anda juga harus menonaktifkan Peran Keamanan, Pusat Identitas IAM, dan integrasi AWS Backup.

- Sumber Daya Khusus alih-alih menggunakan sumber daya bersama - zona pendaratan 4.0 sekarang menciptakan sumber daya khusus untuk layanan utama. Pemisahan ini memberikan isolasi sumber daya yang lebih baik dan kontrol yang lebih terperinci atas sumber daya khusus layanan:
  - Pisahkan bucket S3 untuk AWS Config
  - Pisahkan bucket S3 untuk AWS CloudTrail
  - Topik SNS individu untuk setiap layanan

- Struktur Organisasi Fleksibel - zona pendaratan 4.0 menghilangkan persyaratan struktur organisasi sebelumnya:
  - Anda tidak lagi diharuskan menggunakan OU Keamanan
  - Anda dapat menentukan struktur organisasi Anda sendiri
  - Satu-satunya persyaratan adalah bahwa semua akun hub harus berada di OU yang sama
- Pengalaman kontrol khusus - Anda sekarang dapat membuat pengaturan zona pendaratan minimal yang mencakup:
  - Integrasi Dasar AWS Organisations
  - Kemampuan untuk mengaktifkan kontrol tanpa mengaktifkan `AWSControlTowerBaseline` baseline
  - Konfigurasi tata kelola khusus berdasarkan kebutuhan Anda
- Perubahan Konfigurasi AWS - Zona Pendaratan 4.0 memperkenalkan beberapa peningkatan pada implementasi integrasi AWS Config:
  - Config baru berbicara baseline khusus untuk kontrol detektif
  - Service-linked Agregator konfigurasi (SLCA) di akun hub Config
  - Penggantian organisasi tradisional dan agregator akun
- Manifest Opsional:
  - Bidang manifes sekarang opsional, memungkinkan Anda:
    - Buat zona pendaratan tanpa integrasi layanan apa pun

- Lebih banyak fleksibilitas dalam pengaturan awal
- Opsi penerapan yang disesuaikan

AWS Control Tower menambahkan 279 tambahan AWS Config kontrol ke Katalog Kontrol

14 November 2025

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower sekarang menyertakan 279 AWS Config kontrol tambahan sebagai bagian dari Katalog Kontrol. Anda dapat melihat kontrol di konsol AWS Control Tower, dan melalui API.

Kontrol tertentu memiliki hubungan dengan kontrol lain. Hubungan ini juga diekspresikan dalam konsol AWS Control Tower dan di API. Jenis hubungan termasuk Komplementer, Saling eksklusif, dan Alternatif.

AWS Control Tower tersedia di Wilayah Asia Pasifik (Selandia Baru)

Oktober 28, 2025

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower sekarang tersedia di Wilayah Asia Pasifik (Selandia Baru).

Untuk daftar lengkap Wilayah tempat AWS Control Tower tersedia, lihat Tabel AWS Wilayah.

AWS Control Tower mendukung pendaftaran akun otomatis

Oktober 15, 2025

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

Untuk pelanggan yang mengoperasikan zona pendaratan AWS Control Tower versi 3.1 atau lebih tinggi, AWS Control Tower sekarang memungkinkan pendaftaran akun secara otomatis ke OU. Jika Anda memilih pendaftaran akun secara otomatis, AWS Control Tower menerapkan sumber daya dasar dan kontrol OU yang diaktifkan ke akun, saat Anda memindahkannya ke OU baru. Kontrol dan garis dasar dari OU sebelumnya dihapus. Dalam kebanyakan kasus, tidak ada penyimpangan yang dibuat oleh tindakan ini.

Untuk mengaktifkan pendaftaran otomatis: Anda dapat memilih pendaftaran otomatis akun di halaman Peng aturan zona landas di konsol AWS Control Tower, atau dengan memanggil Menara Kontrol AWS `CreateLandingZone` atau `UpdateLandingZone` API, dengan nilai `RemediationType` parameter disetel ke Inheritance Drift.

Untuk menerapkan pendaftaran otomatis: Setelah memilih opsi ini di halaman Pengaturan, Anda dapat memindahkan akun melalui AWS Organizations konsol, AWS Organizations **`MoveAccount`** API, atau konsol AWS Control Tower.

Untuk membatalkan pendaftaran akun dengan pendaftaran otomatis: Jika Anda memindahkan akun di luar OU yang terdaftar, AWS Control Tower akan menghapus semua sumber daya dasar dan kontrol yang digunakan secara otomatis.

Untuk informasi selengkapnya tentang pendaftaran otomatis, lihatSecara opsional mengkonfigurasi pendaftaran otomatis untuk akun.

Rilis ini juga mencakup pembaruan untuk kebijakan terkelola dan kebijakan terkelola baru. Kami memperbarui AWS ControlTowerServiceRolePolicy dan menambahkan yang baru AWS ControlTowerIdentityCenterManagementPolicy.

Kami memperbarui Menara Kontrol AWS `CreateLandingZone` dan `UpdateLandingZone` API untuk menambahkan yang baru`RemediationType`, yang disebut`Inheritance Drift`.

AWS Control Tower memperbarui versi Python

3 September 2025

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

Python versi 3.9 sedang tidak digunakan lagi. AWS Control Tower telah memperbarui versi Python di lingkungan AWS Control Tower Anda. Tidak ada tindakan yang diperlukan, dan pembaruan ini tidak memengaruhi beban kerja Anda yang ada.

AWS Control Tower mengurangi penyimpangan

Agustus 20, 2025

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower telah memperbarui fungsionalitas penyimpangan kebijakan kontrol layanan (SCP). Dengan rilis ini, dua jenis penyimpangan tata kelola ditangani langsung oleh AWS Control Tower dan tidak lagi menyebabkan penyimpangan di lingkungan Anda.

Dua jenis penyimpangan tata kelola dihapus

- SCP dilampirkan ke OU terkelola - Jenis penyimpangan ini terjadi ketika SCP untuk kontrol dilampirkan ke OU lain. Kejadian ini sangat umum terjadi ketika Anda memperbarui OU dari luar konsol AWS Control Tower.
- SCP yang dilampirkan ke akun anggota — Jenis penyimpangan ini biasanya terjadi ketika SCP untuk kontrol dilampirkan ke akun dari luar konsol AWS Control Tower.

Untuk informasi selengkapnya tentang drift, lihat Men deteksi dan menyelesaikan penyimpangan di AWS Control Tower.

AWS Control Tower mendukung alamat IPv6

Agustus 18, 2025

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower API sekarang mendukung alamat Internet Protocol versi 6 (IPv6) melalui titik akhir dual-stack baru kami. Titik akhir yang ada yang mendukung IPv4 tetap tersedia untuk kompatibilitas mundur. Domain dual-stack baru tersedia baik dari internet atau dari dalam Amazon Virtual Private Cloud (VPC) menggunakan. AWS PrivateLink

Account Factory untuk Terraform versi 1.15.0 tersedia

Juli 28, 2025

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

Versi 1.15.0 Pabrik Akun Menara Kontrol AWS untuk Terraform (AFT) tersedia. Untuk informasi selengkapnya, lihat GitHub repositori AFT.

Kontrol yang diperbarui dengan jenis instance Nitro

Juli 24, 2025

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower telah memperbarui delapan kontrol proaktif di Katalog Kontrol (sebelumnya disebut Control Library) yang menerapkan tipe intance Amazon EC2. Pembaruan ini memungkinkan Anda untuk membuat instance beberapa jenis instance Nitro baru, dan menghapus beberapa jenis instance u-series yang tidak digunakan lagi.

Kontrol yang diperbarui

- CT.AUTOSCALING.PR.10
- CT.AUTOSCALING.PR.11
- CT.EC2.PR.15
- CT.EC2.PR.16
- CT.EC2.PR.17
- CT.EC2.PR.18
- CT.EC2.PR.19
- CT.EC2.PR.20

Jenis instans baru tersedia

- c8gd
- c8gn
- i7i
- m8gd
- p6-b200
- r8gd

Jenis instans dihapus

- u-12tb1
- u-18tb1
- u-24tb1
- u-9tb1

Kontrol yang diperbarui tersedia di semua Wilayah AWS tempat AWS Control Tower tersedia. Untuk daftar Wilayah di mana AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

AWS Control Tower tersedia di Wilayah Asia Pasifik (Taipei)

Juli 23, 2025

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower sekarang tersedia di Wilayah Asia Pasifik (Taipei):

Untuk daftar lengkap Wilayah tempat AWS Control Tower tersedia, lihat Tabel AWS Wilayah.

Mendukung Menara Kontrol AWS PrivateLink

Juni 30, 2025

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower sekarang mendukung AWS PrivateLink. Anda dapat memanggil AWS Control Tower dan Control Catalog API dari dalam Amazon Virtual Private Cloud (VPC) tanpa melintasi internet publik. AWS PrivateLink menyediakan konektivitas pribadi antara cloud pribadi virtual (VPC), layanan dan sumber daya yang didukung, dan jaringan lokal Anda. AWS PrivateLink dukungan untuk AWS Control Tower tersedia di semua Wilayah AWS tempat AWS Control Tower tersedia.

Dukungan untuk kerangka kerja industri tambahan, metadata yang diperbarui

Juni 12, 2025

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

Dengan rilis ini, AWS Control Tower diperluas untuk menyertakan dukungan untuk 10 kerangka kerja industri. Untuk daftar kerangka kerja, lihat Kerangka kerja yang didukung.

Misalnya, Anda dapat memulai dengan menavigasi ke halaman Katalog Kontrol di konsol AWS Control Tower dan mencari kerangka kerja, seperti PCI-DSS-v4.0, untuk melihat semua kontrol yang terkait dengan kerangka kerja tersebut. Atau Anda dapat memeriksa kontrol dan kerangka kerja secara terprogram, dengan memanggil API baru `ListControlMappings`.

Definisi metadata yang terkait dengan kontrol berubah, untuk lebih mendukung framewok industri tambahan ini. Perubahan metadata dapat memengaruhi cara Anda mengevaluasi kontrol untuk pengaktifan. Misalnya, nilai untuk NIST, PCI, dan metadata CIS mungkin telah berubah. Kami menyarankan Anda melihat pemetaan untuk kontrol yang diaktifkan, di halaman detail kontrol di konsol.

Di konsol dan API, kami memperkenalkan 3 bidang metadata baru. Secara kolektif, bidang ini menggambarkan hierarki yang membantu Anda memahami cara mengkategorikan dan

mengaktifkan kontrol. Bidang tersebut adalah: Domain, Objective, dan Common control. Kami telah mendefinisikan ulang tujuan kontrol kami untuk menyelaraskan lebih baik dengan cakupan kerangka kerja industri yang lebih luas yang tersedia. Untuk informasi selengkapnya tentang hierarki ini, lihat ikhtis ar Ontologi.

- Perubahan metadata ini tercermin dalam konsol AWS Control Tower, dan pengalaman konsol konsisten di seluruh AWS Control Tower dan AWS Config konsol.
- Untuk melihat informasi kontrol di konsol AWS Control Tower, Anda harus menambahkan `controlcatalog` izin tambahan ke kebijakan IAM Anda. Untuk informasi selengkapnya, lihat Izin yang diperlukan untuk menggunakan konsol AWS Control Tower.
- Setiap kontrol sekarang memiliki bidang baru yang disebut`GovernedResources`, yang menunjukkan jenis sumber daya yang diatur kontrol. Dalam beberapa kasus, bidang ini menunjukkan awalan layanan untuk sumber daya, dan dalam kasus lain, itu bisa kosong. Untuk informasi selengkapnya, lihat `GetControl` dan `ListControls`.

Dengan rilis ini, kami telah mengganti nama P ustaka Kontrol menjadi Katalog Kontrol, untuk konsistensi dengan terminologi lainnya.

Service-linked AWS Config mengendalikan

Juni 12, 2025

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower mengumumkan dukungan untuk kontrol detektif AWS Control Tower yang akan digunakan sebagai aturan terkait layanan AWS Config .

Dengan rilis ini, AWS Control Tower sekarang menerapkan aturan Konfigurasi terkait layanan langsung di akun terdaftar Anda, menggantikan metode penerapan sebelumnya dengan AWS CloudFormation kumpulan tumpukan. Perubahan ini secara signifikan meningkatkan kecepatan penerapan. Selain itu, aturan Konfigurasi terkait layanan ini membantu memastikan tata kelola sumber daya Anda yang konsisten, karena aturan tersebut mencegah penyimpangan konfigurasi yang tidak disengaja yang dapat disebabkan oleh perubahan manual pada kumpulan CloudFormation tumpukan atau aturan Konfigurasi.

Ke depan, semua kontrol AWS Control Tower yang diterapkan oleh AWS Config aturan akan digunakan dengan mekanisme ini, yang secara langsung memanggil AWS Config API.

> **Important**
>
> Sebelum Anda mengadopsi aturan Konfigurasi terkait layanan, tinjau penyesuaian yang ada, seperti remediasi, yang telah Anda buat untuk aturan Konfigurasi di luar AWS Control Tower, karena penyesuaian ini akan dihapus selama transisi. AWS Config API tidak mendukung penambahan konfigurasi remediasi untuk aturan terkait layanan. AWS Config Lihat `PutRemediationConfigurations`.

Detail dan tindakan yang diperlukan

- Saat Anda Memperbarui atau Meng atur ulang zona pendaratan, AWS Control Tower memperbarui kontrol Wajib yang mengatur OU Keamanan. Untuk menyelesaikan upgrade, Anda juga harus Reset setiap kontrol detektif yang diimplementasikan dengan AWS Config aturan, atau Re-register OU.
- Cakupan penuh dari peningkatan ini berlaku untuk Anda jika versi zona pendaratan AWS Control Tower Anda adalah 3.2 atau lebih tinggi. Saat Anda menerapkan pembaruan ini, AWS Config aturan yang ada diubah menjadi aturan Konfigurasi yang dikelola layanan, bersama dengan metode penerapan baru.
- Jika zona pendaratan Anda adalah versi 3.1 atau lebih rendah, aturan Config baru apa pun akan diterapkan dengan metode baru, bukan lagi dengan Stack Sets. Aturan Konfigurasi Anda yang ada TIDAK diperbarui menjadi aturan Konfigurasi yang dikelola layanan. Mereka akan tetap dari tipe standar.
- Anda dapat mengidentifikasi aturan konfigurasi terkait layanan dengan ARN sumber dayanya, yang memiliki bentuk:

```
arn:aws:config:*:*:config-rule/aws-service-rule/controltower.*/*
```

Fungsionalitas kontrol yang dimaksudkan, ketika diimplementasikan oleh AWS Config aturan terkait layanan, tidak berubah. Aturan konfigurasi detektif yang terkait dengan layanan di AWS Control Tower dapat mengidentifikasi sumber daya yang tidak sesuai dalam akun Anda, seperti pelanggaran kebijakan, dan memberikan peringatan melalui dasbor. Untuk menjaga konsistensi, mencegah penyimpangan konfigurasi, dan menyederhanakan pengalaman pengguna Anda secara keseluruhan, aturan ini sekarang hanya dapat dimodifikasi melalui AWS Control Tower.

Sebagai bagian dari rilis ini, kami menambahkan empat izin baru ke kebijakan untuk peran terkait layanan (SLR) `AWSServiceRoleForAWSControlTower`, sehingga Anda dapat mengaktifkan dan menonaktifkan AWS Config aturan terkait layanan untuk akun terdaftar Anda.

```
config:DescribeConfigRules
config:TagResource
config:PutConfigRule
config:DeleteConfigRule
```

Tampilan konsol kontrol yang diaktifkan memberikan visibilitas terpusat

Mei 21, 2025

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower menambahkan halaman baru di konsol yang menampilkan semua kontrol Anda yang diaktifkan dalam satu tampilan terpusat. Sebelumnya, kontrol hanya dapat dilihat dengan akun atau OU tempat mereka diaktifkan. Tampilan konsolidasi memudahkan Anda mengidentifikasi kesenjangan dalam tata kelola kontrol Anda, dalam skala besar.

Pada halaman Kontrol yang diaktifkan, Anda dapat memfilter kontrol menurut perilaku: Pencegahan, Detektif, atau Proaktif. Anda juga dapat memfilter sesuai dengan implementasi kontrol, seperti SCP. Untuk setiap kontrol, Anda dapat melihat berapa banyak OU yang mengaktifkan kontrol ini.

Untuk melihat halaman Kontrol yang diaktifkan, navigasikan ke bagian Kontrol di konsol AWS Control Tower.

Account Factory for Terraform (AFT) mendukung konfigurasi baru saat penerapan

Mei 13, 2025

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

Kerangka penyesuaian akun AWS Control Tower, Account Factory for Terraform (AFT), sekarang mendukung tiga konfigurasi opsional tambahan pada saat penerapan. Anda dapat menerapkan AFT ke cloud pribadi virtual khusus (VPC), menentukan nama proyek Terraform untuk penerapan AFT Anda, dan menandai sumber daya yang dibuat AFT.

Untuk informasi selengkapnya, lihat Men yebarkan AWS Control Tower Account Factory untuk Terraform (AFT).

AWS Control Tower memperkenalkan pelaporan tingkat akun untuk API dasar

12 Mei 2025

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

Anda sekarang dapat melihat status drift dan pendaftaran akun secara terprogram untuk akun yang diatur, dengan memanggil API dasar. Dengan kemampuan ini, Anda dapat mengidentifikasi kapan konfigurasi dasar akun dan OU disinkron kan, atau tidak sinkron. Untuk melihat status drift secara terprogram, Anda dapat memanggil `ListEnabledBaselines` API untuk garis dasar yang diaktifkan. Untuk melihat status akun individual secara terprogram dengan `ListEnabledBaselines` API, gunakan flag. `includeChildren` Anda dapat memfilter berdasarkan status ini, dan hanya melihat akun dan OU yang memerlukan perhatian Anda.

Men `AWS ControlTowerBaseline` yiapkan konfigurasi praktik terbaik, kontrol, dan sumber daya yang diperlukan untuk tata kelola. Saat Anda mengaktifkan baseline ini pada unit organisasi (OU), akun anggota dalam OU terdaftar ke AWS Control Tower secara otomatis. API dasar AWS Control Tower menyertakan CloudFormation dukungan, yang memungkinkan Anda membangun otomatisasi yang mengelola OU dan akun Anda dengan infrastruktur sebagai kode (IAC).

Untuk mempelajari lebih lanjut tentang API ini, tinjau Garis Dasar di Panduan Pengguna Menara Kontrol AWS. API dasar dan kemampuan pelaporan yang baru diluncurkan untuk status drift dan pendaftaran akun tersedia di semua Wilayah AWS tempat AWS Control Tower tersedia. Untuk daftar Wilayah AWS tempat AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

AWS Control Tower tersedia di AWS Wilayah Asia Pasifik (Thailand) dan Meksiko (Tengah)

9 Mei 2025

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower sekarang tersedia di Wil AWS ayah berikut:

- Asia Pasifik (Thailand)

- Meksiko (Tengah)

Untuk daftar lengkap Wilayah tempat AWS Control Tower tersedia, lihat Tabel AWS Wilayah.

Tambahan AWS Config kontrol tersedia

April 11, 2025

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower sekarang mendukung 223 AWS Config aturan terkelola tambahan untuk berbagai kasus penggunaan, seperti keamanan, biaya, daya tahan, dan operasi. Dengan peluncuran ini, Anda sekarang dapat menggunakan AWS Control Tower untuk mencari dan menemukan AWS Config aturan yang Anda perlukan untuk mengatur lingkungan multi-akun Anda; kemudian mengaktifkan dan mengelola kontrol langsung dari AWS Control Tower.

Untuk memulai dari konsol AWS Control Tower, buka Katalog Kontrol dan cari kontrol dengan filter implementasi AWS Config. Anda dapat mengaktifkan kontrol langsung dari konsol AWS Control Tower.

Untuk detail selengkapnya, lihat AWS Config Kontrol terintegrasi yang tersedia di AWS Control Tower.

Dengan peluncuran ini, kami telah memperbarui `GetControl` API `ListControls` dan untuk mendukung tiga bidang baru: CreateTime, Tingkat Ke parahan, dan Implementasi, yang dapat Anda gunakan saat mencari kontrol di Katalog Kontrol. Misalnya, Anda sekarang dapat secara terprogram menemukan AWS Config aturan tingkat keparahan tinggi yang dibuat setelah evaluasi terakhir Anda.

Anda dapat mencari AWS Config aturan baru di semua Wilayah AWS tempat AWS Control Tower tersedia. Untuk menerapkan aturan, lihat daftar yang didukung Wilayah AWS untuk aturan tersebut, untuk melihat di mana aturan tersebut dapat diaktifkan.

Menghapus pendaftaran dan menghapus tindakan untuk OU

8 April 2025

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower sekarang mendukung tindakan konsol terpisah untuk membatalkan pendaftaran OU dan menghapus OU. Anda harus membatalkan pendaftaran OU sebelum menghapusnya. Anda dapat menghapus OU dari AWS Control Tower dengan membatalkan pendaftaran.

Untuk informasi selengkapnya, lihat Menghapus OU.

Katalog Kontrol mendukung alamat IPv6

April 2, 2025

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower Control Catalog API sekarang mendukung alamat Internet Protocol versi 6 (IPv6) melalui titik akhir dual-stack baru kami. Titik akhir Katalog Kontrol yang ada yang mendukung IPv4 tetap tersedia untuk kompatibilitas mundur. Domain dual-stack baru tersedia baik dari internet atau dari dalam Amazon Virtual Private Cloud (VPC) menggunakan. AWS PrivateLink

Januari - Desember 2024

Pada tahun 2024, AWS Control Tower merilis pembaruan berikut:

- Dukungan AWS Control Tower CfCT GitHub dan RCP
- AWS Control Tower menambahkan kontrol preventif dengan kebijakan deklaratif
- AWS Control Tower menambahkan opsi paket cadangan preskriptif
- AWS Control Tower terintegrasi AWS Config mengendalikan
- AWS Control Tower meningkatkan manajemen hook dan menambahkan Regions kontrol proaktif
- AWS Control Tower meluncurkan kebijakan kontrol sumber daya terkelola
- AWS Control Tower melaporkan penyimpangan kebijakan kontrol
- `ResetEnabledControl`API baru
- Kontrol pembaruan katalog `GetControl` API
- Menara Kontrol AWS mendukung AFT GitLab
- AWS Control Tower tersedia di AWS Wilayah Asia Pasifik (Malaysia)
- AWS Control Tower mendukung hingga 1000 akun per OU
- AWS Control Tower menambahkan pilihan versi zona pendaratan

- API kontrol deskriptif tersedia, akses yang diperluas ke Wilayah dan kontrol
- AWS Control Tower mendukung AFT dan CfCT di Wilayah pilihan
- AWS Control Tower menambahkan `ListLandingZoneOperations` API
- AWS Control Tower mendukung hingga 100 operasi kontrol bersamaan
- AWS Control Tower tersedia di AWS Kanada Barat (Calgary)
- AWS Control Tower mendukung penyesuaian kuota layanan mandiri
- AWS Control Tower merilis Panduan Referensi Kontrol
- AWS Control Tower memperbarui dan mengganti nama dua kontrol proaktif
- Kontrol yang tidak digunakan lagi tidak tersedia
- AWS Control Tower mendukung penandaan `EnabledControl` sumber daya di CloudFormation
- AWS Control Tower mendukung API untuk pendaftaran OU dan konfigurasi dengan garis dasar

Dukungan AWS Control Tower CfCT GitHub dan RCP

Desember 9, 2024

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower sekarang mendukung GitHub TM ™ sebagai opsi untuk sistem kontrol versi pihak ketiga (VCS) dan sumber konfigurasi untuk Kustomisasi untuk AWS Control Tower (CFCT). Untuk informasi lebih lanjut, lihat. Siapkan GitHub sebagai sumber konfigurasi

AWS Control Tower sekarang mendukung kebijakan kontrol sumber daya (RCP) untuk Kustomisasi untuk AWS Control Tower (CFCT). Untuk informasi selengkapnya, lihat Panduan kustomisasi CfCT.

AWS Control Tower menambahkan kontrol preventif dengan kebijakan deklaratif

Desember 1, 2024

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower sekarang mendukung kontrol preventif yang diimplementasikan oleh kebijakan deklaratif dari AWS Organizations. Kebijakan deklaratif diterapkan langsung di tingkat layanan.

Pendekatan ini memastikan bahwa konfigurasi yang ditentukan diberlakukan, bahkan ketika fitur atau API baru diperkenalkan oleh layanan. Untuk informasi selengkapnya, lihat Kontrol yang diimplementasikan dengan kebijakan deklaratif.

AWS Control Tower menambahkan opsi paket cadangan preskriptif

25 November 2024

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower sekarang mendukung paket preskriptif AWS Backup yang memungkinkan Anda memasukkan alur kerja cadangan dan pemulihan data langsung ke zona pendaratan Anda. Rencana pencadangan mencakup aturan yang telah ditentukan sebelumnya, seperti hari retensi, frekuensi pencadangan, dan jendela waktu di mana pencadangan terjadi. Aturan ini menentukan cara membuat cadangan AWS sumber daya Anda di semua akun anggota yang diatur. Saat Anda menerapkan rencana cadangan ke zona pendaratan, AWS Control Tower memastikan bahwa rencana tersebut konsisten untuk semua akun anggota, dan selaras dengan rekomendasi praktik terbaik dari AWS Backup.

Untuk informasi selengkapnya, lihat AWS Backup dan AWS Control Tower.

AWS Control Tower terintegrasi AWS Config mengendalikan

November 21, 2024

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower telah mengintegrasikan AWS Config kontrol terpilih, sehingga kontrol tersebut dapat dilihat dan dikelola oleh AWS Control Tower.

Untuk informasi selengkapnya, lihat AWS Config Kontrol terintegrasi yang tersedia di AWS Control Tower

AWS Control Tower meningkatkan manajemen hook dan menambahkan Regions kontrol proaktif

20 November 2024

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

Dengan rilis ini, Anda dapat memanfaatkan kapasitas penuh CloudFormation kait, tanpa batasan oleh AWS Control Tower. Selain itu, kontrol proaktif tersedia di Wilayah Kanada Barat (Calgary) dan Wilayah Asia Pasifik (Malaysia).

Sebelumnya, semua CloudFormation kait di lingkungan Anda perlu dilindungi oleh CT.CLOUDFORMATION.PR.1 kontrol, sehingga hanya AWS Control Tower yang dapat memodifikasinya. Dengan rilis ini, Anda dapat menerapkan CloudFormation kait, dan memodifikasi kait ini, tanpa batasan yang sebelumnya diperlukan oleh layanan AWS Control Tower.

Jika saat ini Anda menerapkan kontrol proaktif, Anda dapat pindah ke fungsionalitas kait yang ditingkatkan ini. Untuk mengatur ulang semua kontrol proaktif pada OU, atur ulang kontrol proaktif tunggal yang aktif pada OU tersebut. Anda dapat melakukan reset dengan memanggil `ResetEnabledControl` API, atau dengan memperbarui kontrol dari konsol, dengan fungsi Reset. Saat Anda menyelesaikan tugas reset ini untuk kontrol proaktif apa pun, AWS Control Tower memindahkan semua kait kontrol proaktif pada OU ke kemampuan baru. Ulangi proses ini untuk setiap OU yang menerapkan kontrol proaktif.

Setelah mengatur ulang kontrol proaktif apa pun, hapus CT.CLOUDFORMATION.PR.1 kontrol pada OU Menara Kontrol AWS Anda, kecuali jika Anda mengaktifkan kontrol tersebut untuk tujuan lain. Jika Anda tidak mematikan CT.CLOUDFORMATION.PR.1 kontrol, Anda tidak akan dapat membuat dan memodifikasi CloudFormation kait Anda yang lain.

Untuk informasi selengkapnya, lihat Memperbarui kait kontrol proaktif.

AWS Control Tower meluncurkan kebijakan kontrol sumber daya terkelola

15 November 2024

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower menawarkan jenis kontrol preventif baru, yang diimplementasikan dengan kebijakan kontrol sumber daya (RCP). Kontrol ini membantu Anda membangun perimeter data di seluruh lingkungan AWS Control Tower Anda, untuk melindungi sumber daya Anda dari akses yang tidak diinginkan.

Misalnya, Anda dapat mengaktifkan RCP-based kontrol untuk Amazon S3,, AWS Security Token Service AWS Key Management Service, Amazon SQS, dan AWS Secrets Manager layanan. RCP-based Kontrol dapat memberlakukan persyaratan seperti “Memerlukan bahwa sumber daya Amazon S3 organisasi hanya dapat diakses oleh prinsipal IAM milik organisasi, atau oleh AWS layanan,” terlepas dari izin yang diberikan pada kebijakan bucket individual.

Anda dapat mengonfigurasi RCP-based kontrol baru, dan kontrol SCP-based pencegahan tertentu yang ada, untuk menentukan pengecualian AWS IAM untuk prinsipal dan sumber daya. Jika Anda tidak ingin prinsipal atau sumber daya diatur oleh kontrol, Anda dapat mengonfigurasi pengecualian.

Dengan menggabungkan kontrol preventif, proaktif, dan detektif di AWS Control Tower, Anda dapat memantau apakah AWS lingkungan multi-akun Anda aman dan dikelola sesuai dengan praktik terbaik, seperti standar Praktik AWS Terbaik Keamanan Dasar.

Kontrol RCP-based preventif baru ini tersedia di Wilayah AWS tempat AWS Control Tower tersedia. Untuk daftar lengkap Wilayah AWS tempat AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

AWS Control Tower melaporkan penyimpangan kebijakan kontrol

November 15, 2024

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower sekarang melaporkan penyimpangan kebijakan kontrol, untuk kontrol yang diimplementasikan dengan kebijakan kontrol sumber daya (RCP), dan kontrol yang merupakan bagian dari Service-managed Standar CSPM Hub Keamanan: AWS Control Tower. Jenis penyimpangan ini dapat diatasi melalui `ResetEnabledControl` API baru. Untuk informasi selengkapnya, lihat Jenis penyimpangan tata kelola.

`ResetEnabledControl`API baru

14 November 2024

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower mengumumkan API baru untuk membantu Anda mengelola penyimpangan kontrol secara terprogram. Anda dapat memperbaiki penyimpangan kontrol dan mengatur ulang kontrol ke konfigurasi yang dimaksudkan. `ResetEnabledControl`API bekerja dengan kontrol Menara Kontrol AWS opsional, termasuk kontrol yang sangat direkomendasikan dan Elective.

Pengecualian kontrol

- Kontrol yang diimplementasikan dengan kebijakan kontrol layanan (SCP) tidak dapat diatur ulang dengan API ini. Untuk informasi selengkapnya, lihat `ResetEnabledControl`.
- Kontrol wajib tidak dapat diatur ulang, karena mereka melindungi sumber daya AWS Control Tower.

- Kontrol penolakan wilayah untuk zona pendaratan harus diatur ulang melalui konsol.

Penyimpangan kontrol terjadi ketika kontrol AWS Control Tower dimodifikasi di luar AWS Control Tower, misalnya dari AWS Organizations konsol. Menyelesaikan penyimpangan membantu memastikan kepatuhan Anda terhadap persyaratan tata kelola.

Kontrol pembaruan katalog **`GetControl`** API

8 November 2024

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower sekarang mendukung `GetControl` API yang diperbarui yang mencakup dua bidang baru: `Implementation` tipe untuk semua kontrol, dan `Parameters` untuk kontrol tertentu yang dapat dikonfigurasi.

`GetControl`API adalah bagian dari `controlcatalog` namespace AWS Control Tower.

Untuk informasi selengkapnya, lihat `GetControl API` di Referensi API Katalog Kontrol.

Rilis ini mencakup perubahan terkait yang ditampilkan di konsol AWS Control Tower.

- Semua AWS Security Hub CSPM kontrol yang ada memiliki nilai `Implementation` parameternya diubah dari AWS Config aturan ke AWS Security Hub CSPM. Panel bantuan konsol yang sesuai dimodifikasi untuk mencerminkan perubahan ini.
- Semua kontrol Hook yang ada memiliki nilai `Implementation` parameternya diubah dari aturan CloudFormation penjaga ke CloudFormation kait. Panel bantuan konsol yang sesuai dimodifikasi untuk mencerminkan perubahan ini.

Menara Kontrol AWS mendukung AFT GitLab

Oktober 23, 2024

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower sekarang mendukung GitLab TM ™ dan GitLab Self-managed sebagai opsi untuk sistem kontrol versi pihak ketiga (VCS) dan sumber konfigurasi untuk Account Factory for Terraform (AFT).

AWS Control Tower tersedia di AWS Wilayah Asia Pasifik (Malaysia)

Oktober 21, 2024

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower tersedia di Wil AWS ayah Asia Pasifik (Malaysia).

Untuk daftar lengkap Wilayah tempat AWS Control Tower tersedia, lihat Tabel AWS Wilayah.

AWS Control Tower mendukung hingga 1000 akun per OU

Agustus 30, 2024

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower telah meningkatkan jumlah maksimum akun yang diizinkan per unit organisasi (OU) dari 300 menjadi 1000. Sekarang, Anda dapat mendaftarkan hingga 1000 orang Akun AWS ke dalam tata kelola AWS Control Tower sekaligus, tanpa mengubah struktur OU Anda. Proses pendaftaran OU dan pendaftaran ulang juga lebih efisien, membutuhkan waktu yang jauh lebih sedikit untuk menerapkan sumber daya dasar AWS Control Tower ke akun Anda.

Beberapa batasan akun masih berlaku karena keterbatasan jumlah set CloudFormation tumpukan yang tersedia. Secara khusus, jumlah maksimum akun yang dapat Anda daftarkan di OU mungkin berbeda, tergantung pada jumlah Wilayah yang Anda miliki di bawah pemerintahan. Untuk mempelajari selengkapnya, kunjungi Batasan berdasarkan AWS layanan yang mendasarinya di Panduan Pengguna Menara Kontrol AWS . Untuk daftar lengkap Wilayah AWS tempat AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

AWS Control Tower menambahkan pilihan versi zona pendaratan

Agustus 15, 2024

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

Jika Anda menjalankan zona pendaratan AWS Control Tower versi 3.1 ke atas, Anda dapat memperbarui atau memperbaiki zona pendaratan di tempat pada versi saat ini, atau Anda dapat meningkatkan ke versi pilihan Anda. Sebelumnya, setiap pembaruan atau perbaikan zona pendaratan memerlukan peningkatan ke versi zona pendaratan terbaru.

Dengan pemilihan versi zona pendaratan, Anda memiliki lebih banyak fleksibilitas untuk merencanakan peningkatan versi sambil mengevaluasi perubahan potensial pada lingkungan Anda.

Anda tidak perlu memilih antara memperbaiki drift agar tetap sesuai, memperbarui konfigurasi zona pendaratan Anda, atau meningkatkan ke versi zona pendaratan terbaru. Jika Anda menjalankan zona pendaratan versi 3.1 atau lebih tinggi, Anda dapat memilih untuk tetap menggunakan versi saat ini, atau meningkatkan ke versi yang lebih baru, saat memperbarui atau mengatur ulang konfigurasi zona pendaratan Anda.

API kontrol deskriptif tersedia, akses yang diperluas ke Wilayah dan kontrol

Agustus 6, 2024

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower menambahkan dua operasi API baru yang membantu Anda menemukan informasi lebih lanjut tentang kontrol yang tersedia, secara terprogram. Fungsionalitas ini memudahkan penyebaran kontrol dengan otomatisasi.

- `GetControl`API mengembalikan detail tentang kontrol yang diaktifkan, termasuk pengidentifikasi target, ringkasan informasi kontrol, daftar Wilayah target, dan status penyimpangan.
- `ListControls`API mengembalikan daftar halaman dari semua kontrol yang tersedia di pustaka kontrol AWS Control Tower.

API ini dicapai melalui namespace Katalog AWS Kontrol. Katalog AWS Kontrol adalah bagian dari AWS Control Tower, yang mencakup kontrol yang membantu Anda mengelola AWS layanan lain, bukan hanya AWS Control Tower. Katalog yang diperluas ini menggabungkan kontrol dari beberapa AWS layanan, sehingga Anda dapat melihat AWS kontrol sesuai dengan beberapa kasus penggunaan umum, seperti: keamanan, biaya, daya tahan, dan operasi. Untuk informasi selengkapnya, lihat Referensi API Katalog Kontrol.

Ketersediaan Wilayah yang Diperluas

Dimulai dengan rilis ini, Anda dapat memperluas tata kelola AWS Control Tower ke Wilayah AWS tempat beberapa kontrol yang (sudah) diaktifkan tidak tersedia. Selain itu, Anda sekarang dapat mengaktifkan kontrol tertentu di lebih banyak Wilayah, meskipun kontrol tidak didukung di semua Wilayah yang Anda atur.

Sebelumnya, AWS Control Tower mencegah Anda memperluas tata kelola ke Wilayah atau mengaktifkan kontrol, jika tidak menawarkan konsistensi di semua kontrol yang diaktifkan dan Wilayah yang diatur. Dengan rilis ini, Anda memiliki lebih banyak fleksibilitas, serta lebih banyak tanggung jawab untuk memastikan bahwa konfigurasi Anda benar untuk semua kontrol yang

diaktifkan dan semua Wilayah yang diatur. API kontrol AWS Control Tower dan API katalog kontrol dapat membantu Anda mendapatkan informasi tentang Wil AWS ayah tempat Anda dilindungi oleh kontrol yang diaktifkan, dan Wilayah tempat kontrol tambahan dapat digunakan. Informasi wilayah dan kontrol juga tersedia di konsol AWS Control Tower.

AWS Control Tower mendukung AFT dan CfCT di Wilayah pilihan

Juli 18, 2024

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

Saat ini, kerangka kustomisasi AWS Control Tower Account Factory for Terraform (AFT) dan Kustomisasi untuk AWS Control Tower (CfCT) tersedia di lima tambahan Wilayah AWS: Asia Pasifik (Hyderabad, Jakarta dan Osaka), Israel (Tel Aviv), dan Timur Tengah (UEA).

Account Factory for Terraform (AFT) menyiapkan pipeline Terraform untuk membantu Anda menyediakan dan menyesuaikan akun di AWS Control Tower. Kustomisasi untuk AWS Control Tower (cFct) membantu Anda menyesuaikan zona pendaratan AWS Control Tower dan akun dengan CloudFormation templat dan kebijakan kontrol layanan (SCP).

Untuk mempelajari selengkapnya, kunjungi halaman Pabrik Akun untuk Terraform dan Kustomisasi untuk Menara Kontrol AWS; di Panduan Pengguna Menara Kontrol AWS. Anda juga mungkin ingin meninjau catatan rilis di halaman AFT Github dan halaman CfCT Github. AFT dan CFCT didukung di semua Wil AWS ayah, dengan beberapa pengecualian. Untuk informasi lebih spesifik, lihat Batasan wilayah.

AWS Control Tower menambahkan **`ListLandingZoneOperations`** API

Juni 26, 2024

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower telah menambahkan API yang memungkinkan Anda mengambil daftar operasi yang baru-baru ini diterapkan ke zona pendaratan Anda, dan operasi yang sedang berlangsung. API dapat mengembalikan riwayat operasi zona pendaratan dan pengenalnya hingga 90 hari. Untuk contoh penggunaan, lihat Melihat status operasi zona pendaratan Anda.

Untuk informasi selengkapnya tentang `ListLandingZoneOperations` API, lihat `ListLandingZoneOperations` di Referensi API AWS Control Tower.

AWS Control Tower mendukung hingga 100 operasi kontrol bersamaan

Mei 20, 2024

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower sekarang mendukung beberapa operasi kontrol dengan konkurensi yang lebih tinggi. Anda dapat mengirimkan hingga 100 operasi kontrol Menara Kontrol AWS, di beberapa unit organisasi (OU), secara bersamaan, dari konsol atau dengan API. Hingga sepuluh (10) operasi dapat berjalan secara bersamaan, dan yang tambahan mengantri. Dengan cara ini, Anda dapat mengatur konfigurasi yang lebih standar di beberapa Akun AWS, tanpa beban operasional operasi kontrol berulang.

Untuk memantau status operasi kontrol yang sedang berlangsung dan antrian, Anda dapat menavigasi ke halaman Operasi terbaru yang baru di konsol AWS Control Tower, atau Anda dapat memanggil `ListControlOperations` API baru.

Pustaka AWS Control Tower berisi lebih dari 500 kontrol, yang memetakan berbagai tujuan kontrol, kerangka kerja, dan layanan. Untuk tujuan kontrol tertentu, seperti Enkripsi data saat diam, Anda dapat mengaktifkan beberapa kontrol dengan operasi kontrol tunggal, untuk membantu Anda mencapai tujuan. Kemampuan ini memfasilitasi pengembangan yang dipercepat, memungkinkan adopsi kontrol praktik terbaik yang lebih cepat, dan mengurangi kompleksitas operasional.

AWS Control Tower tersedia di AWS Kanada Barat (Calgary)

3 Mei 2024

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

Mulai hari ini, Anda dapat mengaktifkan AWS Control Tower di Wilayah Kanada Barat (Calgary). Jika Anda telah menggunakan AWS Control Tower dan ingin memperluas fitur tata kelola ke Wilayah ini, Anda dapat melakukannya dengan API zona pendaratan AWS Control Tower. Atau dari konsol, buka halaman Peng aturan di dasbor AWS Control Tower Anda, pilih Wilayah Anda, lalu perbarui zona pendaratan Anda.

Wilayah Kanada Barat (Calgary) tidak mendukung AWS Service Catalog. Untuk alasan ini, beberapa fungsi AWS Control Tower berbeda. Perubahan fungsi yang paling menonjol adalah Account Factory tidak tersedia. Jika Anda memilih Kanada Barat (Calgary) sebagai Wilayah asal Anda, prosedur untuk memperbarui akun, menyiapkan otomatisasi akun, dan proses lain yang melibatkan Katalog Layanan berbeda dari di Wilayah lain.

Penyediaan akun

Untuk membuat dan menyediakan akun baru di Wilayah Kanada Barat (Calgary), kami sarankan Anda membuat akun di luar AWS Control Tower, lalu mendaftarkannya ke OU terdaftar. Untuk informasi selengkapnya, lihat M endaftarkan akun yang sudah ada dan Lang kah-langkah untuk mendaftarkan akun.

API Katalog Layanan tidak tersedia di Wilayah Kanada Barat (Calgary). Contoh skrip yang ditampilkan dalam Men gotomatiskan penyediaan akun di AWS Control Tower oleh API Katalog Layanan tidak dapat diterapkan.

Kustomisasi Pabrik Akun (AFC), Pabrik Akun untuk Terraform (AFT), dan Kustomisasi untuk Menara Kontrol AWS (CfCT) tidak tersedia di Kanada Barat (Calgary), karena kurangnya dependensi mendasar lainnya untuk Menara Kontrol AWS. Jika Anda memperluas tata kelola ke Wilayah Kanada Barat (Calgary), Anda dapat terus mengelola cetak biru AFC di semua Wilayah yang didukung AWS Control Tower, selama Katalog Layanan tersedia di Wilayah asal Anda.

Kontrol

Kontrol dan kontrol proaktif untuk AWS Security Hub CSPM Service-Managed Standar: Menara Kontrol AWS tidak tersedia di Wilayah Kanada Barat (Calgary). Kontrol preventif tidak `CT.CLOUDFORMATION.PR.1` tersedia di Kanada Barat (Calgary) karena hanya diperlukan untuk mengaktifkan kontrol proaktif berbasis kait. Kontrol detektif tertentu berdasarkan tidak AWS Config tersedia. Lihat perinciannya di Batasan kontrol.

Penyedia identitas

Pusat Identitas IAM tidak tersedia di Kanada Barat (Calgary). Rekomendasi praktik terbaik adalah mengatur zona pendaratan Anda di Wilayah tempat Pusat Identitas IAM tersedia. Atau, Anda memiliki opsi untuk mengelola sendiri konfigurasi akses akun Anda jika Anda menggunakan penyedia identitas eksternal di Kanada Barat (Calgary).

Tidak tersedianya Katalog Layanan di Wilayah Kanada Barat (Calgary) tidak berpengaruh pada Wilayah lain yang didukung oleh AWS Control Tower. Perbedaan ini hanya berlaku jika Wilayah rumah Anda adalah Kanada Barat (Calgary).

Untuk daftar lengkap Wilayah tempat AWS Control Tower tersedia, lihat Tabel AWS Wilayah.

AWS Control Tower mendukung penyesuaian kuota layanan mandiri

April 25, 2024

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower kini mendukung penyesuaian kuota layanan mandiri melalui konsol Kuota Layanan. Untuk informasi selengkapnya, lihat Meminta peningkatan kuota.

AWS Control Tower merilis Panduan Referensi Kontrol

April 21, 2024

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower merilis Panduan Referensi Kontrol, dokumen baru tempat Anda dapat menemukan informasi terperinci tentang kontrol yang khusus untuk lingkungan AWS Control Tower. Sebelumnya, materi ini disertakan dalam Panduan Pengguna Menara Kontrol AWS. Panduan Referensi Kontrol mencakup kontrol dalam format yang diperluas. Untuk informasi selengkapnya, lihat Panduan Referensi Kontrol Menara Kontrol AWS.

AWS Control Tower memperbarui dan mengganti nama dua kontrol proaktif

Maret 26, 2024

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower telah mengganti nama dua kontrol proaktif agar selaras dengan pembaruan Amazon OpenSearch Service.

- [CT.OPENSEARCH.PR.8] M emerlukan domain Layanan Elasticsearch untuk digunakan TLSv1.2
- [CT.OPENSEARCH.PR.16] Memerlukan domain OpenSearch Layanan Amazon untuk digunakan TLSv1.2

Kami memperbarui nama kontrol dan artefak untuk kedua kontrol ini agar selaras dengan rilis terbaru dari Amazon OpenSearch Service, yang sekarang mendukung Transport Layer Security (TLS) versi 1.3 di antara opsi keamanan transportasi untuk keamanan titik akhir domain.

Untuk menambahkan dukungan TLSv1.3 untuk kontrol ini, kami telah memperbarui artefak dan nama kontrol untuk mencerminkan maksud dari kontrol. Mereka sekarang mengevaluasi versi TLS minimum dari domain layanan. Untuk membuat pembaruan ini di lingkungan Anda, Anda harus Men on aktifkan dan Mengaktifkan kontrol untuk menerapkan artefak terbaru.

Tidak ada kontrol proaktif lain yang terpengaruh oleh perubahan ini. Kami menyarankan Anda meninjau kontrol ini, untuk memastikan bahwa kontrol tersebut memenuhi tujuan kontrol Anda.

Untuk pertanyaan atau masalah, hubungi AWS Dukungan.

Kontrol yang tidak digunakan lagi tidak tersedia

Maret 12, 2024

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower telah menghentikan beberapa kontrol. Kontrol ini tidak lagi tersedia.

- CT.ATHENA.PR.1
- CT.CODEBUILD.PR.4
- CT.AUTOSCALING.PR.3
- SH.Athena.1
- SH.Codebuild.5
- SH.AutoScaling.4
- SH.SNS.1
- SH.SNS.2

AWS Control Tower mendukung penandaan **`EnabledControl`** sumber daya di CloudFormation

Februari 22, 2024

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

Rilis AWS Control Tower ini memperbarui perilaku sumber `EnabledControl` daya, untuk menyelaraskan lebih baik dengan kontrol yang dapat dikonfigurasi, dan untuk meningkatkan kemampuan mengelola lingkungan AWS Control Tower Anda dengan otomatisasi. Dengan rilis ini, Anda dapat menambahkan tag ke `EnabledControl` sumber daya yang dapat dikonfigurasi melalui CloudFormation template. Sebelumnya, Anda hanya dapat menambahkan tag melalui konsol AWS Control Tower dan API.

Operasi AWS Control Tower `GetEnabledControl`,`EnableControl`, dan `ListTagsforResource` API diperbarui dengan rilis ini, karena bergantung pada fungsionalitas `EnabledControl` sumber daya.

Untuk informasi selengkapnya, lihat Menandai `EnabledControl` sumber daya di AWS Control Tower dan `EnabledControl` di Panduan CloudFormation Pengguna.

AWS Control Tower mendukung API untuk pendaftaran OU dan konfigurasi dengan garis dasar

Februari 14, 2024

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

API ini mendukung pendaftaran OU terprogram dengan `EnableBaseline` panggilan. Saat Anda mengaktifkan baseline pada OU, akun anggota dalam OU terdaftar ke tata kelola AWS Control Tower. Peringatan tertentu mungkin berlaku. Misalnya, pendaftaran OU melalui konsol AWS Control Tower memungkinkan kontrol opsional serta kontrol wajib. Saat memanggil API, Anda mungkin perlu menyelesaikan langkah tambahan agar kontrol opsional diaktifkan.

Dasar AWS Control Tower me wujudkan praktik terbaik untuk tata kelola AWS Control Tower dari OU dan akun anggota. Misalnya, saat Anda mengaktifkan baseline pada OU, akun anggota dalam OU menerima grup sumber daya yang ditentukan, termasuk, Pusat Identitas IAM AWS CloudTrail AWS Config, dan peran AWS IAM yang diperlukan.

Garis dasar tertentu kompatibel dengan versi zona pendaratan AWS Control Tower tertentu. AWS Control Tower dapat menerapkan baseline kompatibel terbaru ke zona pendaratan Anda, saat Anda mengubah pengaturan zona pendaratan Anda. Untuk informasi selengkapnya, lihat Kompatibilitas baseline OU dan versi landing zone.

Rilis ini mencakup empat penting Jenis baseline

- `AWSControlTowerBaseline`
- `AuditBaseline`
- `LogArchiveBaseline`
- `IdentityCenterBaseline`

Dengan API baru dan garis dasar yang ditentukan, Anda dapat mendaftarkan OU dan mengotomatiskan alur kerja penyediaan OU Anda. API juga dapat mengelola OU yang sudah berada di bawah tata kelola AWS Control Tower, sehingga Anda dapat mendaftarkan ulang OU setelah pembaruan zona pendaratan. API menyertakan dukungan untuk CloudFormation

`EnabledBaseline` sumber daya, yang memungkinkan Anda mengelola OU Anda dengan infrastruktur sebagai kode (IAC).

API Dasar

- EnableBaseline, UpdateEnabledBaseline, DisableBaseline: Ambil tindakan pada baseline untuk OU.
- GetEnabledBaseline, ListEnabledBaselines: Temukan konfigurasi untuk garis dasar yang diaktifkan.
- GetBaselineOperation: Melihat status operasi dasar tertentu.
- ResetEnabledBaseline: Memperbaiki penyimpangan sumber daya pada OU dengan baseline yang diaktifkan (termasuk OU bersarang dan penyimpangan kontrol wajib). Juga memperbaiki penyimpangan untuk kontrol penolakan Wilayah tingkat zona pendaratan
- GetBaseline, ListBaselines: Temukan konten dari garis dasar AWS Control Tower.

Untuk mempelajari lebih lanjut tentang API ini, tinj au Garis Das ar di Panduan Pengguna Menara Kontrol AWS, dan Referensi API. API baru tersedia di Wilayah AWS tempat AWS Control Tower tersedia, kecuali Wil GovCloud ayah (AS). Untuk daftar Wilayah AWS tempat AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

Januari - Desember 2023

Pada tahun 2023, AWS Control Tower merilis pembaruan berikut:

- Transisi ke baru AWS Service Catalog Jenis produk eksternal (fase 3)
- Zona pendaratan Menara Kontrol AWS versi 3.3
- Transisi ke baru AWS Service Catalog Jenis produk eksternal (fase 2)
- AWS Control Tower mengumumkan kontrol untuk membantu kedaulatan digital
- API zona pendaratan Menara Kontrol AWS
- API penandaan kontrol Menara Kontrol AWS
- AWS Control Tower tersedia di AWS Asia Pacific (Melbourne)
- Transisi ke yang baru AWS Service Catalog Jenis produk eksternal (fase 1)
- AWS Control Tower menambahkan API kontrol baru
- AWS Control Tower menambahkan kontrol baru

- AWS Control Tower mendeteksi penyimpangan akses tepercaya
- AWS Control Tower tersedia dalam empat tambahan Wilayah AWS
- AWS Control Tower tersedia di AWS Israel (Tel Aviv)
- AWS Control Tower menambahkan 28 kontrol proaktif baru
- AWS Control Tower menghentikan dua kontrol
- Zona pendaratan Menara Kontrol AWS versi 3.2
- AWS Control Tower menambahkan pemetaan Email-to-ID untuk IAM Identity Center
- AWS Control Tower menambahkan lebih banyak AWS Security Hub CSPM mengendalikan
- AWS Control Tower menerbitkan metadata untuk AWS Security Hub CSPM mengendalikan
- AWS Control Tower menambahkan Kustomisasi Pabrik Akun (AFC) untuk Terraform
- AWS Control Tower menambahkan pusat identitas IAM yang dikelola sendiri
- AWS Control Tower menambahkan catatan tata kelola campuran
- AWS Control Tower menambahkan kontrol proaktif baru
- AWS Control Tower memperbarui kontrol Amazon EC2
- AWS Control Tower tersedia dalam tujuh tambahan Wilayah AWS
- Kustomisasi Pabrik Akun AWS Control Tower (AFC) dan pelacakan permintaan secara umum tersedia
- Zona pendaratan Menara Kontrol AWS versi 3.1
- Kontrol proaktif AWS Control Tower umumnya tersedia

Transisi ke baru AWS Service Catalog Jenis produk eksternal (fase 3)

Desember 14, 2023

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower tidak lagi mendukung Terraform Open Source sebagai jenis produk (cetak biru) saat membuat produk baru. Akun AWS Untuk informasi selengkapnya dan petunjuk tentang memperbarui cetak biru akun Anda, tinjau Trans isi ke jenis produk AWS Service Catalog Eksternal.

Jika Anda tidak memperbarui cetak biru akun untuk menggunakan jenis produk Eksternal, Anda hanya dapat memperbarui atau menghentikan akun yang Anda sediakan menggunakan cetak biru Terraform Open Source.

Zona pendaratan Menara Kontrol AWS versi 3.3

Desember 14, 2023

(Diperlukan pembaruan untuk zona pendaratan AWS Control Tower ke versi 3.3. Untuk informasi, lihatPerbarui landing zone Anda).

Pembaruan kebijakan bucket S3 di akun AWS Control Tower Audit

Kami telah mengubah kebijakan bucket Audit Amazon S3 yang diterapkan AWS Control Tower di akun, sehingga suatu `aws:SourceOrgID` kondisi harus dipenuhi untuk izin penulisan apa pun. Dengan rilis ini, AWS layanan memiliki akses ke sumber daya Anda hanya jika permintaan berasal dari organisasi atau unit organisasi (OU) Anda.

Anda dapat menggunakan kunci `aws:SourceOrgID` kondisi dan menetapkan nilai ke ID organisasi Anda di elemen kondisi kebijakan bucket S3 Anda. Kondisi ini memastikan bahwa CloudTrail hanya dapat menulis log atas nama akun dalam organisasi Anda ke bucket S3 Anda; hal ini mencegah CloudTrail log di luar organisasi Anda menulis ke bucket AWS Control Tower S3 Anda.

Kami membuat perubahan ini untuk memperbaiki potensi kerentanan keamanan, tanpa mempengaruhi fungsionalitas beban kerja Anda yang ada. Untuk melihat kebijakan yang diperbarui, lihatKebijakan bucket Amazon S3 untuk pencatatan.

Untuk informasi selengkapnya tentang kunci kondisi baru, lihat dokumentasi IAM dan posting blog IAM berjudul "Gunakan kontrol yang dapat diskalakan untuk AWS layanan yang mengakses sumber daya Anda."

Pembaruan kebijakan dalam topik AWS Config SNS

Kami menambahkan kunci `aws:SourceOrgID` kondisi baru ke kebijakan untuk topik AWS Config SNS.Untuk melihat kebijakan yang diperbarui, lihat Kebijakan topik AWS Config SNS.

Pembaruan untuk zona pendaratan Kontrol Region Deny

- Dihapus`discovery-marketplace:`. Tindakan ini tercakup dalam peng `aws-marketplace:*` ecualian.
- Ditambahkan `quicksight:DescribeAccountSubscription`

CloudFormation Template yang diperbarui

Kami memperbarui CloudFormation template untuk stack bernama `BASELINE-CLOUDTRAIL-MASTER` sehingga tidak menunjukkan penyimpangan saat AWS KMS enkripsi tidak digunakan.

Transisi ke baru AWS Service Catalog Jenis produk eksternal (fase 2)

Desember 7, 2023

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

HashiCorp memperbarui lisensi Terraform mereka. Akibatnya, perubahan dukungan untuk AWS Service Catalog produk Terraform Open Source dan produk yang disediakan menjadi jenis produk baru, yang disebut Eksternal.

Untuk menghindari gangguan pada beban kerja dan AWS sumber daya yang ada di akun Anda, ikuti langkah-langkah transisi AWS Control Tower dalam Trans isi ke jenis produk AWS Service Catalog Eksternal sebelum 14 Desember 2023.

AWS Control Tower mengumumkan kontrol untuk membantu kedaulatan digital

November 27, 2023

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower mengumumkan 65 kontrol ter AWS kelola baru, untuk membantu Anda memenuhi persyaratan kedaulatan digital Anda. Dengan rilis ini, Anda dapat menemukan kontrol ini di bawah grup kedaulatan digital baru di konsol AWS Control Tower. Anda dapat menggunakan kontrol ini untuk membantu mencegah tindakan dan mendeteksi perubahan sumber daya terkait lokasi data, pembatasan akses terperinci, enkripsi, dan kemampuan ketahanan. Kontrol ini dirancang untuk membuatnya lebih mudah bagi Anda untuk memenuhi persyaratan dalam skala besar. Untuk informasi selengkapnya tentang kontrol kedaulatan digital, lihat Kontrol yang meningkatkan perlindungan kedaulatan digital.

Misalnya, Anda dapat memilih untuk mengaktifkan kontrol yang membantu menegakkan strategi enkripsi dan ketahanan Anda, seperti Memer lukan cache AWS AppSync API agar enkripsi dalam transit diaktifkan atau Memer lukan Firewall AWS Jaringan untuk digunakan di beberapa Zona Ketersediaan. Anda juga dapat menyesuaikan kontrol penolakan AWS Control Tower Region untuk menerapkan batasan regional yang paling sesuai dengan kebutuhan bisnis unik Anda.

Rilis ini menghadirkan kemampuan penolakan AWS Control Tower Region yang ditingkatkan dengan baik. Anda dapat menerapkan kontrol penolakan Wilayah baru yang diberi parameter di tingkat OU,

untuk meningkatkan perincian tata kelola, sambil mempertahankan tata kelola Wilayah tambahan di tingkat zona pendaratan. Kontrol penolakan Wilayah yang dapat disesuaikan ini membantu Anda menerapkan batasan regional yang paling sesuai dengan kebutuhan bisnis unik Anda. Untuk informasi selengkapnya tentang kontrol penolakan wilayah baru yang dapat dikonfigurasi, lihat Kontrol penolakan wilayah yang diterapkan ke OU.

Sebagai alat baru untuk peningkatan penolakan Wilayah baru, rilis ini menyertakan API baru`UpdateEnabledControl`,, yang memungkinkan Anda mengatur ulang kontrol yang diaktifkan ke pengaturan default. API ini sangat membantu dalam kasus penggunaan di mana Anda perlu menyelesaikan penyimpangan dengan cepat, atau untuk menjamin secara terprogram bahwa kontrol tidak dalam keadaan drift. Untuk informasi selengkapnya tentang API baru, lihat Referensi API AWS Control Tower

Kontrol proaktif baru

- CT.APIGATEWAY.PR.6: Memerlukan domain REST Amazon API Gateway untuk menggunakan kebijakan keamanan yang menentukan versi protokol TLS minimum TLSv1.2
- CT.APPSYNC.PR.2: Memerlukan AWS AppSync GraphQL API untuk dikonfigurasi dengan visibilitas pribadi
- CT.APPSYNC.PR.3: Memerlukan bahwa AWS AppSync GraphQL API tidak diautentikasi dengan kunci API
- CT.APPSYNC.PR.4: Memerlukan cache AWS AppSync GraphQL API agar enkripsi dalam transit diaktifkan.
- CT.APPSYNC.PR.5: Memerlukan cache AWS AppSync GraphQL API agar enkripsi saat istirahat diaktifkan.
- CT.AUTOSCALING.PR.9: Memerlukan volume Amazon EBS yang dikonfigurasi melalui konfigurasi peluncuran Amazon EC2 Auto Scaling untuk mengenkripsi data saat diam
- CT.AUTOSCALING.PR.10: Memerlukan grup Amazon EC2 Auto Scaling untuk hanya menggunakan jenis instans AWS Nitro saat mengganti template peluncuran
- CT.AUTOSCALING.PR.11: Hanya memerlukan jenis instans AWS Nitro yang mendukung enkripsi lalu lintas jaringan antar instans untuk ditambahkan ke grup Amazon EC2 Auto Scaling, saat mengganti template peluncuran
- CT.DAX.PR.3: Memerlukan cluster DynamoDB Accelerator untuk mengenkripsi data dalam transit dengan Transport Layer Security (TLS)
- CT.DMS.PR.2: Memerlukan Endpoint AWS Database Migration Service (DMS) untuk mengenkripsi koneksi untuk titik akhir sumber dan target

- CT.EC2.PR.15: Memerlukan instans Amazon EC2 untuk menggunakan jenis instans AWS Nitro saat membuat dari jenis sumber daya `AWS::EC2::LaunchTemplate`
- CT.EC2.PR.16: Memerlukan instans Amazon EC2 untuk menggunakan jenis instans AWS Nitro saat dibuat menggunakan jenis sumber daya `AWS::EC2::Instance`
- CT.EC2.PR.17: Memerlukan host khusus Amazon EC2 untuk menggunakan jenis instans AWS Nitro
- CT.EC2.PR.18: Memerlukan armada Amazon EC2 untuk mengganti hanya templat peluncuran dengan jenis instans AWS Nitro
- CT.EC2.PR.19: Memerlukan instans Amazon EC2 untuk menggunakan jenis instans nitro yang mendukung enkripsi dalam transit antar instans saat dibuat menggunakan jenis sumber daya `AWS::EC2::Instance`
- CT.EC2.PR.20: Memerlukan armada Amazon EC2 untuk mengganti hanya template peluncuran dengan jenis instans AWS Nitro yang mendukung enkripsi saat transit antar instans
- CT.ELASTICACHE.PR.8: Memerlukan grup ElastiCache replikasi Amazon versi Redis yang lebih baru agar otentikasi RBAC diaktifkan
- CT.MQ.PR.1: Memerlukan broker Amazon MQ ActiveMQ untuk menggunakan mode active/standby penerapan untuk ketersediaan tinggi
- CT.MQ.PR.2: Memerlukan broker Amazon MQ Rabbit MQ untuk menggunakan mode Multi-AZ cluster untuk ketersediaan tinggi
- CT.MSK.PR.1: Memerlukan cluster Amazon Managed Streaming untuk Apache Kafka (MSK) untuk menerapkan enkripsi dalam transit antara node broker cluster
- CT.MSK.PR.2: Memerlukan Amazon Managed Streaming untuk cluster Apache Kafka (MSK) untuk dikonfigurasi dengan dinonaktifkan PublicAccess
- CT.NETWORK-FIREWALL.PR.5: Memerlukan firewall AWS Network Firewall untuk digunakan di beberapa Zona Ketersediaan
- CT.RDS.PR.26: Memerlukan Proxy DB Amazon RDS untuk memerlukan koneksi Transport Layer Security (TLS)
- CT.RDS.PR.27: Memerlukan grup parameter cluster Amazon RDS DB untuk memerlukan koneksi Transport Layer Security (TLS) untuk jenis mesin yang didukung
- CT.RDS.PR.28: Memerlukan grup parameter Amazon RDS DB untuk memerlukan koneksi Transport Layer Security (TLS) untuk jenis mesin yang didukung
- CT.RDS.PR.29: Memerlukan cluster Amazon RDS tidak dikonfigurasi agar dapat diakses publik melalui properti 'PubliclyAccessible'

- CT.RDS.PR.30: Memerlukan instance database Amazon RDS memiliki enkripsi saat diam yang dikonfigurasi untuk menggunakan kunci KMS yang Anda tentukan untuk jenis mesin yang didukung
- CT.S3.PR.12: Memerlukan titik akses Amazon S3 untuk memiliki konfigurasi Blokir Akses Publik (BPA) dengan semua opsi disetel ke true

Kontrol preventif baru

- CT.APPSYNC.PV.1Memerlukan AWS AppSync GraphQL API dikonfigurasi dengan visibilitas pribadi
- CT.EC2.PV.1Memerlukan snapshot Amazon EBS untuk dibuat dari volume EC2 terenkripsi
- CT.EC2.PV.2Memerlukan volume Amazon EBS terlampir dikonfigurasi untuk mengenkripsi data saat diam
- CT.EC2.PV.3Memerlukan agar snapshot Amazon EBS tidak dapat dipulihkan secara publik
- CT.EC2.PV.4Memerlukan agar API langsung Amazon EBS tidak dipanggil
- CT.EC2.PV.5Melarang penggunaan impor dan ekspor VM Amazon EC2
- CT.EC2.PV.6Melarang penggunaan tindakan Amazon EC RequestSpotFleet 2 dan API yang tidak digunakan lagi RequestSpotInstances
- CT.KMS.PV.1Memer AWS KMS lukan kebijakan utama untuk memiliki pernyataan yang membatasi pembuatan AWS KMS hibah untuk AWS layanan
- CT.KMS.PV.2Memerlukan bahwa kunci AWS KMS asimetris dengan bahan kunci RSA yang digunakan untuk enkripsi tidak memiliki panjang kunci 2048 bit
- CT.KMS.PV.3Memerlukan AWS KMS kunci dikonfigurasi dengan pemeriksaan keamanan penguncian kebijakan bypass diaktifkan
- CT.KMS.PV.4Memerlukan bahwa kunci AWS KMS yang dikelola pelanggan (CMK) dikonfigurasi dengan materi kunci yang berasal dari CloudHSM AWS
- CT.KMS.PV.5Memerlukan bahwa kunci yang AWS KMS dikelola pelanggan (CMK) dikonfigurasi dengan bahan kunci yang diimpor
- CT.KMS.PV.6Memerlukan bahwa AWS KMS kunci yang dikelola pelanggan (CMK) dikonfigurasi dengan materi kunci yang berasal dari penyimpanan kunci eksternal (XKS)
- CT.LAMBDA.PV.1Memerlukan URL AWS Lambda fungsi untuk menggunakan AWS IAM-based otentikasi
- CT.LAMBDA.PV.2Memerlukan URL AWS Lambda fungsi untuk dikonfigurasi untuk akses hanya oleh prinsipal di dalam Anda Akun AWS

API zona pendaratan Menara Kontrol AWS

November 26, 2023

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower kini menawarkan API yang membantu Anda mengelola zona pendaratan secara terprogram. API ini memungkinkan Anda membuat, memperbarui, dan mengatur ulang zona pendaratan, serta mengambil informasi tentang konfigurasi dan operasi zona pendaratan Anda. Untuk informasi selengkapnya, lihat contoh API zona pendaratan.

API zona pendaratan tersedia di semua Wilayah AWS tempat AWS Control Tower tersedia, kecuali Wil GovCloud ayah (AS). Untuk daftar Wilayah AWS tempat AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

API penandaan kontrol Menara Kontrol AWS

November 10, 2023

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower kini menawarkan API yang membantu Anda menandai kontrol yang diaktifkan secara terprogram. API ini memungkinkan Anda untuk menambahkan, menghapus, dan mencantumkan tag untuk kontrol yang diaktifkan. Untuk informasi selengkapnya, lihat Menandai sumber daya AWS Control Tower.

API penandaan kontrol tersedia di semua Wilayah AWS tempat AWS Control Tower tersedia, kecuali Wilayah GovCloud (AS). Untuk daftar Wilayah AWS tempat AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

AWS Control Tower tersedia di AWS Asia Pacific (Melbourne)

3 November 2023

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower tersedia di Asia Pasifik (Melbourne). Untuk daftar lengkap Wilayah tempat AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

Transisi ke yang baru AWS Service Catalog Jenis produk eksternal (fase 1)

Oktober 31, 2023

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

HashiCorp memperbarui lisensi Terraform mereka. Akibatnya, perubahan dukungan untuk AWS Service Catalog produk Terraform Open Source dan produk yang disediakan menjadi jenis produk baru, yang disebut Eksternal.

Untuk menghindari gangguan pada beban kerja dan AWS sumber daya yang ada di akun Anda, ikuti langkah-langkah transisi AWS Control Tower dalam Trans isi ke jenis produk AWS Service Catalog Eksternal sebelum 14 Desember 2023.

AWS Control Tower menambahkan API kontrol baru

Oktober 27, 2023

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower kini menawarkan API baru`UpdateEnabledControl`, yang memungkinkan Anda memperbarui kontrol yang diaktifkan. API ini sangat membantu dalam kasus penggunaan di mana Anda perlu menyelesaikan penyimpangan dengan cepat, atau untuk menjamin secara terprogram bahwa kontrol tidak dalam keadaan drift. Untuk informasi selengkapnya tentang API baru, lihat Referensi API AWS Control Tower.

`UpdateEnabledControl`API tersedia di semua Wilayah AWS tempat AWS Control Tower tersedia, kecuali Wil GovCloud ayah (AS). Untuk daftar Wilayah AWS tempat AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

AWS Control Tower menambahkan kontrol baru

Oktober 20, 2023

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower telah menambahkan 22 kontrol baru ke perpustakaan kontrol AWS Control Tower. Kontrol ini membantu Anda menerapkan praktik terbaik untuk AWS sumber daya Anda. Untuk informasi selengkapnya tentang kontrol baru, lihat Kategori kontrol.

Kontrol baru tersedia di semua Wilayah AWS tempat AWS Control Tower tersedia. Untuk daftar Wilayah AWS tempat AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

AWS Control Tower mendeteksi penyimpangan akses tepercaya

Oktober 13, 2023

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower sekarang mendeteksi dan melaporkan penyimpangan untuk pengaturan akses tepercaya. Pengaturan akses tepercaya memungkinkan AWS Control Tower berinteraksi dengan AWS layanan lain atas nama Anda. Jika pengaturan ini diubah di luar AWS Control Tower, AWS Control Tower akan mendeteksi penyimpangan dan melaporkannya di konsol AWS Control Tower. Untuk informasi selengkapnya tentang penyimpangan akses tepercaya, lihat Jenis penyimpangan tata kelola.

Deteksi penyimpangan akses tepercaya tersedia di semua Wilayah AWS tempat AWS Control Tower tersedia. Untuk daftar Wilayah AWS tempat AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

AWS Control Tower tersedia dalam empat tambahan Wilayah AWS

September 29, 2023

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower tersedia dalam empat tambahan Wilayah AWS: Asia Pasifik (Hyderabad), Asia Pasifik (Jakarta), Eropa (Spanyol), dan Eropa (Zurich). Untuk daftar lengkap Wilayah tempat AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

AWS Control Tower tersedia di AWS Israel (Tel Aviv)

Agustus 1, 2023

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower tersedia di Israel (Tel Aviv). Untuk daftar lengkap Wilayah tempat AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

AWS Control Tower menambahkan 28 kontrol proaktif baru

Juli 27, 2023

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower telah menambahkan 28 kontrol proaktif baru ke perpustakaan kontrol AWS Control Tower. Kontrol ini membantu Anda menerapkan praktik terbaik untuk AWS sumber daya Anda. Untuk informasi selengkapnya tentang kontrol baru, lihat Kategori kontrol.

Kontrol baru tersedia di semua Wilayah AWS tempat AWS Control Tower tersedia. Untuk daftar Wilayah AWS tempat AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

AWS Control Tower menghentikan dua kontrol

Juli 27, 2023

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower telah menghentikan dua kontrol: CT.CLOUDFORMATION.PR.2 dan. CT.CLOUDFORMATION.PR.3 Kontrol ini tidak lagi tersedia di pustaka kontrol AWS Control Tower. Untuk informasi selengkapnya tentang kontrol yang tidak digunakan lagi, lihat Kategori kontrol.

Kontrol yang tidak digunakan lagi tidak tersedia di mana pun. Wilayah AWS

Zona pendaratan Menara Kontrol AWS versi 3.2

Juni 16, 2023

(Diperlukan pembaruan untuk zona pendaratan AWS Control Tower ke versi 3.2. Untuk informasi, lihatPerbarui landing zone Anda).

Zona pendaratan AWS Control Tower versi 3.2 membawa kontrol yang merupakan bagian dari AWS Security Hub CSPM Service-Managed Standar: Menara Kontrol AWS ke ketersediaan umum. Ini memperkenalkan kemampuan untuk melihat status drift kontrol yang merupakan bagian dari standar ini di konsol AWS Control Tower.

Pembaruan ini mencakup peran terkait layanan (SLR) baru, yang disebut. AWSServiceRoleForAWSControlTower Peran ini membantu Menara Kontrol AWS dengan membuat A EventBridge turan Terkelola, yang disebut AWSControlTowerManagedRule di setiap akun anggota. Aturan terkelola AWS Security Hub CSPM ini mengumpulkan peristiwa Pencarian, dari dengan AWS Control Tower dapat menentukan penyimpangan kontrol.

Aturan ini adalah aturan terkelola pertama yang dibuat oleh AWS Control Tower. Aturan tidak diterapkan oleh tumpukan; itu diterapkan langsung dari EventBridge API. Anda dapat melihat aturan di EventBridge konsol, atau melalui EventBridge API. Jika `managed-by` bidang diisi, itu akan menampilkan prinsipal layanan AWS Control Tower.

Sebelumnya, AWS Control Tower mengambil AWSControlTowerExecution peran untuk melakukan operasi di akun anggota. Peran dan aturan baru ini lebih selaras dengan prinsip praktik terbaik untuk mengizinkan hak istimewa paling sedikit saat melakukan operasi di AWS lingkungan

multi-akun. Peran baru ini menyediakan izin cakupan yang secara khusus memungkinkan: membuat aturan terkelola di akun anggota, mempertahankan aturan terkelola, menerbitkan pemberitahuan keamanan melalui SNS, dan memverifikasi drift. Untuk informasi selengkapnya, lihat AWSServiceRoleForAWSControlTower.

Pembaruan zona pendaratan 3.2 juga menyer StackSet takan sumber daya baru di akun manajemen`BP_BASELINE_SERVICE_LINKED_ROLE`, yang awalnya menerapkan peran terkait layanan.

Saat melaporkan penyimpangan kontrol CSPM Security Hub (di zona pendaratan 3.2 dan yang lebih baru), AWS Control Tower menerima pembaruan status harian dari Security Hub CSPM. Meskipun kontrol aktif di setiap Wilayah yang diatur, AWS Control Tower mengirimkan peristiwa Fin AWS Security Hub CSPM ding hanya ke Wilayah beranda Menara Kontrol AWS. Untuk informasi selengkapnya, lihat Pelaporan penyimpangan kontrol Hub Keamanan.

Perbarui ke kontrol Region Deny

Versi zona pendaratan ini juga menyertakan pembaruan untuk kontrol Region Deny.

Layanan global dan API ditambahkan

- AWS Manajemen Penagihan dan Biaya (`billing:*`)
- AWS CloudTrail (`cloudtrail:LookupEvents`) untuk memungkinkan visibilitas peristiwa global di akun anggota.
- AWS Penagihan Konsolidasi (`consolidatedbilling:*`)
- AWS Aplikasi Seluler Konsol Manajemen (`consoleapp:*`)
- AWS Tingkat Gratis (`freetier:*`)
- AWS Invoicing (`invoicing:*`)
- AWS IQ (`iq:*`)
- AWS Pemberitahuan Pengguna (`notifications:*`)
- AWS Kontak Pemberitahuan Pengguna (`notifications-contacts:*`)
- Pembayaran Amazon (`payments:*`)
- AWS Pengaturan Pajak (`tax:*`)

Layanan global dan API dihapus

- D `s3:GetAccountPublic` ihapus karena ini bukan tindakan yang valid.

- D `s3:PutAccountPublic` ihapus karena ini bukan tindakan yang valid.

AWS Control Tower menambahkan pemetaan Email-to-ID untuk IAM Identity Center

Juli 13, 2023

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower kini mendukung pemetaan Email-to-ID untuk IAM Identity Center. Fitur ini memungkinkan Anda memetakan alamat email ke ID pengguna Pusat Identitas IAM, yang memudahkan pengelolaan akses pengguna ke lingkungan AWS Control Tower Anda. Untuk informasi selengkapnya tentang pemetaan Email-to-ID, lihat Integrasi dengan Pusat Identitas IAM.

Email-to-ID pemetaan tersedia di semua Wilayah AWS tempat AWS Control Tower tersedia. Untuk daftar Wilayah AWS tempat AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

AWS Control Tower menambahkan lebih banyak AWS Security Hub CSPM mengendalikan

Juni 29, 2023

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower telah menambahkan lebih banyak AWS Security Hub CSPM kontrol ke perpustakaan kontrol AWS Control Tower. Kontrol ini membantu Anda menerapkan praktik terbaik untuk AWS sumber daya Anda. Untuk informasi selengkapnya tentang kontrol baru, lihat Kategori kontrol.

Kontrol baru tersedia di semua Wilayah AWS tempat AWS Control Tower tersedia. Untuk daftar Wilayah AWS tempat AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

AWS Control Tower menerbitkan metadata untuk AWS Security Hub CSPM mengendalikan

Juni 22, 2023

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower sekarang menerbitkan metadata untuk AWS Security Hub CSPM kontrol. Metadata ini mencakup informasi tentang kontrol, seperti ID kontrol, judul kontrol, dan deskripsi kontrol. Untuk informasi selengkapnya tentang metadata, lihat Metadata kontrol.

Metadata kontrol tersedia di semua Wilayah AWS tempat AWS Control Tower tersedia. Untuk daftar Wilayah AWS tempat AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

AWS Control Tower menambahkan Kustomisasi Pabrik Akun (AFC) untuk Terraform

Juni 15, 2023

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower sekarang mendukung Kustomisasi Pabrik Akun (AFC) untuk Terraform. Fitur ini memungkinkan Anda menggunakan Terraform untuk menyesuaikan akun AWS Control Tower Anda. Untuk informasi selengkapnya tentang AFC untuk Terraform, lihat Kustomisasi Pabrik Akun untuk Terraform.

AFC untuk Terraform tersedia di semua Wilayah AWS tempat AWS Control Tower tersedia. Untuk daftar Wilayah AWS tempat AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

AWS Control Tower menambahkan pusat identitas IAM yang dikelola sendiri

Juni 8, 2023

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower sekarang mendukung pusat identitas IAM yang dikelola sendiri. Fitur ini memungkinkan Anda menggunakan penyedia identitas Anda sendiri dengan AWS Control Tower. Untuk informasi selengkapnya tentang pusat identitas IAM yang dikelola sendiri, lihat Pusat identitas IAM.

Self-managed Pusat identitas IAM tersedia di semua Wilayah AWS tempat AWS Control Tower tersedia. Untuk daftar Wilayah AWS tempat AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

AWS Control Tower menambahkan catatan tata kelola campuran

Juni 1, 2023

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower sekarang menyertakan catatan tentang tata kelola campuran. Catatan ini menjelaskan cara AWS Control Tower bekerja dengan AWS layanan lain untuk menyediakan tata kelola bagi AWS sumber daya Anda. Untuk informasi selengkapnya tentang tata kelola campuran, lihat T ata kelola campuran.

Catatan tata kelola campuran tersedia di semua Wilayah AWS tempat AWS Control Tower tersedia. Untuk daftar Wilayah AWS tempat AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

AWS Control Tower menambahkan kontrol proaktif baru

Mei 25, 2023

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower telah menambahkan kontrol proaktif baru ke perpustakaan kontrol AWS Control Tower. Kontrol ini membantu Anda menerapkan praktik terbaik untuk AWS sumber daya Anda. Untuk informasi selengkapnya tentang kontrol baru, lihat Kategori kontrol.

Kontrol baru tersedia di semua Wilayah AWS tempat AWS Control Tower tersedia. Untuk daftar Wilayah AWS tempat AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

AWS Control Tower memperbarui kontrol Amazon EC2

Mei 18, 2023

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower telah memperbarui kontrol Amazon EC2 di pustaka kontrol Menara Kontrol AWS. Pembaruan ini meningkatkan keamanan dan keandalan lingkungan AWS Control Tower Anda. Untuk informasi selengkapnya tentang kontrol yang diperbarui, lihat Kategori kontrol.

Kontrol yang diperbarui tersedia di semua Wilayah AWS tempat AWS Control Tower tersedia. Untuk daftar Wilayah AWS tempat AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

AWS Control Tower tersedia dalam tujuh tambahan Wilayah AWS

Mei 11, 2023

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower tersedia di tujuh tambahan Wilayah AWS: Asia Pasifik (Osaka), Kanada (Tengah), Eropa (Milan), Eropa (Stockholm), Timur Tengah (Bahrain), Timur Tengah (UEA), dan Amerika Selatan (São Paulo). Untuk daftar lengkap Wilayah di mana AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

Kustomisasi Pabrik Akun AWS Control Tower (AFC) dan pelacakan permintaan secara umum tersedia

April 27, 2023

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

Kustomisasi Pabrik Akun AWS Control Tower (AFC) dan pelacakan permintaan sekarang tersedia secara umum. AFC memungkinkan Anda menyesuaikan akun AWS Control Tower Anda, dan pelacakan permintaan memungkinkan Anda melacak status permintaan AWS Control Tower Anda. Untuk informasi selengkapnya tentang AFC dan pelacakan permintaan, lihat Kustomisasi Pabrik Akun dan Pelacakan Permintaan.

AFC dan pelacakan permintaan tersedia di semua Wilayah AWS tempat AWS Control Tower tersedia. Untuk daftar Wilayah AWS tempat AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

Zona pendaratan Menara Kontrol AWS versi 3.1

9 Februari 2023

(Diperlukan pembaruan untuk zona pendaratan AWS Control Tower ke versi 3.1. Untuk informasi, lihatPerbarui landing zone Anda)

Zona pendaratan AWS Control Tower versi 3.1 mencakup pembaruan berikut:

- Dengan rilis ini, AWS Control Tower menonaktifkan pencatatan akses yang tidak perlu untuk bucket logging akses Anda, yaitu bucket Amazon S3 tempat log akses disimpan di akun Log Archive, sambil terus mengaktifkan logging akses server untuk bucket S3. Rilis ini juga mencakup pembaruan pada kontrol Region Deny yang memungkinkan tindakan tambahan untuk layanan global, seperti R Dukungan encana dan AWS Artifact.
- Penonaktifan logging akses server untuk bucket logging akses AWS Control Tower menyebabkan Security Hub CSPM membuat temuan untuk bucket logging akses akun Log Archive, karena AWS Security Hub CSPM aturan, [S3.9] logging akses server bucket S3 harus diaktifkan. Sejalan dengan Security Hub CSPM, kami sarankan Anda menekan temuan khusus ini, seperti yang

dinyatakan dalam deskripsi CSPM Security Hub dari aturan ini. Untuk informasi tambahan, lihat informasi tentang temuan yang ditekan.

- Logging akses untuk bucket logging (reguler) di akun Log Archive tidak berubah di versi 3.1. Sejalan dengan praktik terbaik, peristiwa akses untuk bucket tersebut dicatat sebagai entri log di bucket logging akses. Untuk informasi selengkapnya tentang pencatatan akses, lihat Pencatatan permintaan menggunakan pencatatan akses server di dokumentasi Amazon S3.
- Kami membuat pembaruan kontrol Region Deny. Pembaruan ini memungkinkan tindakan oleh lebih banyak layanan global. Untuk detail SCP ini, lihat Men olak akses AWS berdasarkan permintaan Wilayah AWS dan Kontrol yang meningkatkan perlindungan residensi data.

  Layanan global ditambahkan:

  - AWS Account Management (`account:*`)
  - AWS Aktifkan (`activate:*`)
  - AWS Artifact (`artifact:*`)
  - AWS Billing Conductor (`billingconductor:*`)
  - AWS Compute Optimizer (`compute-optimizer:*`)
  - AWS Data Pipeline (`datapipeline:GetAccountLimits`)
  - AWS Device Farm(`devicefarm:*`)
  - AWS Marketplace (`discovery-marketplace:*`)
  - Amazon ECR (`ecr-public:*`)
  - AWS License Manager (`license-manager:ListReceivedLicenses`)
  - AWS Layar cahaya () `lightsail:Get*`
  - Penjelajah Sumber Daya AWS (`resource-explorer-2:*`)
  - Amazon S3 (`s3:CreateMultiRegionAccessPoint`,`s3:GetBucketPolicyStatus`,`s3:PutMultiRegionAcc`
  - AWS Rencana Tabungan (`savingsplans:*`)
  - Pusat Identitas IAM () `sso:*`
  - AWS Support App (`supportapp:*`)
  - Dukungan Rencana (`supportplans:*`)
  - AWS Keberlanjutan (`sustainability:*`)
  - AWS Resource Groups Tagging API (`tag:GetResources`)

- AWS Marketplace Wawasan Vendor (`vendor-insights:ListEntitledSecurityProfiles`)

Kontrol proaktif AWS Control Tower umumnya tersedia

April 13, 2023

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

Kontrol proaktif AWS Control Tower sekarang tersedia secara umum. Kontrol proaktif membantu Anda menerapkan praktik terbaik untuk AWS sumber daya Anda. Untuk informasi selengkapnya tentang kontrol proaktif, lihat Kontrol proaktif.

Kontrol proaktif tersedia di semua Wilayah AWS tempat AWS Control Tower tersedia. Untuk daftar Wilayah AWS tempat AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

Januari - Desember 2022

Pada tahun 2022, AWS Control Tower merilis pembaruan berikut:

- Operasi akun bersamaan
- Kustomisasi Pabrik Akun (AFC)
- Kontrol komprehensif membantu AWS penyediaan dan manajemen sumber daya
- Status kepatuhan dapat dilihat untuk semua AWS Config aturan
- API untuk kontrol dan baru CloudFormation sumber daya
- CfCT mendukung penghapusan set tumpukan
- Retensi log yang disesuaikan
- Perbaikan penyimpangan peran tersedia
- Zona pendaratan Menara Kontrol AWS versi 3.0
- Halaman Organisasi menggabungkan tampilan OU dan akun
- Pembuatan dan pendaftaran akun yang disederhanakan
- AFT mendukung kustomisasi otomatis untuk akun AWS Control Tower bersama
- Operasi bersamaan untuk semua kontrol opsional
- Akun keamanan dan logging yang ada
- Zona pendaratan Menara Kontrol AWS versi 2.9

- Zona pendaratan Menara Kontrol AWS versi 2.8

Operasi akun bersamaan

Desember 16, 2022

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower sekarang mendukung tindakan bersamaan di pabrik akun. Anda dapat membuat, memperbarui, atau mendaftarkan hingga lima (5) akun sekaligus. Kirim hingga lima tindakan berturut-turut dan lihat status penyelesaian setiap permintaan, sementara akun Anda selesai dibangun di latar belakang. Misalnya, Anda tidak lagi harus menunggu setiap proses selesai sebelum memperbarui akun lain, atau sebelum Anda mendaftarkan ulang seluruh unit organisasi (OU).

Kustomisasi Pabrik Akun (AFC)

November 28, 2022

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

Kustomisasi pabrik akun memungkinkan Anda menyesuaikan akun baru dan akun yang sudah ada dari dalam konsol AWS Control Tower. Kemampuan penyesuaian baru ini memberi Anda fleksibilitas untuk menentukan cetak biru akun, yang merupakan CloudFormation templat yang terdapat dalam produk Katalog Layanan khusus. Cetak biru menyediakan sumber daya dan konfigurasi yang sepenuhnya disesuaikan. Anda juga dapat memilih menggunakan cetak biru yang telah ditentukan sebelumnya, dibuat dan dikelola oleh AWS mitra, yang membantu Anda menyesuaikan akun untuk kasus penggunaan tertentu.

Sebelumnya, pabrik akun AWS Control Tower tidak mendukung penyesuaian akun di konsol. Dengan pembaruan pabrik akun ini, Anda dapat menentukan persyaratan akun sebelumnya dan menerapkannya sebagai bagian dari alur kerja yang terdefinisi dengan baik. Anda dapat menerapkan cetak biru untuk membuat akun baru, mendaftarkan AWS akun lain ke AWS Control Tower, dan memperbarui akun AWS Control Tower yang ada.

Saat Anda menyediakan, mendaftarkan, atau memperbarui akun di pabrik akun, Anda akan memilih cetak biru untuk diterapkan. Sumber daya yang ditentukan dalam cetak biru disediakan di akun Anda. Ketika akun Anda selesai dibangun, semua konfigurasi khusus tersedia untuk digunakan segera.

Untuk memulai penyesuaian akun, Anda dapat menentukan sumber daya untuk kasus penggunaan yang dimaksudkan dalam produk Katalog Layanan. Anda juga dapat memilih solusi yang dikelola

mitra dari Perpustakaan Mem AWS ulai. Untuk informasi selengkapnya, lihat Sesuaikan akun dengan Kustomisasi Pabrik Akun (AFC).

Kontrol komprehensif membantu AWS penyediaan dan manajemen sumber daya

November 28, 2022

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower sekarang mendukung manajemen kontrol yang komprehensif, termasuk kontrol proaktif opsional baru, yang diimplementasikan melalui CloudFormation kait. Kontrol ini disebut sebagai proaktif karena mereka memeriksa sumber daya Anda — sebelum sumber daya digunakan — untuk menentukan apakah sumber daya baru akan mematuhi kontrol yang diaktifkan di lingkungan Anda.

Lebih dari 130 kontrol proaktif baru membantu Anda memenuhi tujuan kebijakan spesifik untuk lingkungan Menara Kontrol AWS Anda; dengan memenuhi persyaratan kerangka kerja kepatuhan standar industri; dan dengan mengatur interaksi AWS Control Tower di lebih dari dua puluh AWS layanan lainnya.

Pustaka kontrol Menara Kontrol AWS mengklasifikasikan kontrol ini menurut AWS layanan dan sumber daya terkait. Untuk detail selengkapnya, lihat Kontrol proaktif.

Dengan rilis ini, AWS Control Tower juga terintegrasi dengan AWS Security Hub CSPM, melalui Security Hub CSPM Service-Managed Standard baru: AWS Control Tower, yang mendukung standar F AWS oundational Security Best Practices (FSBP). Anda dapat melihat lebih dari 160 kontrol CSPM Security Hub bersama kontrol AWS Control Tower di konsol, dan Anda dapat memperoleh skor keamanan CSPM Security Hub untuk lingkungan AWS Control Tower Anda. Untuk informasi selengkapnya, lihat Kontrol Hub Keamanan.

Status kepatuhan dapat dilihat untuk semua AWS Config aturan

November 18, 2022

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower sekarang menampilkan status kepatuhan dari semua AWS Config aturan yang digunakan ke unit organisasi yang terdaftar di AWS Control Tower. Anda dapat melihat status kepatuhan semua AWS Config aturan yang memengaruhi akun Anda di AWS Control Tower,

terdaftar atau tidak terdaftar, tanpa menavigasi di luar konsol AWS Control Tower. Pelanggan dapat memilih untuk mengatur aturan konfigurasi, yang disebut kontrol detektif, di AWS Control Tower, atau mengaturnya secara langsung melalui AWS Config layanan. Aturan yang diterapkan oleh AWS Config ditampilkan, bersama dengan aturan yang diterapkan oleh AWS Control Tower.

Sebelumnya, AWS Config aturan yang diterapkan melalui AWS Config layanan tidak terlihat di konsol AWS Control Tower. Pelanggan harus menavigasi ke AWS Config layanan untuk mengidentifikasi AWS Config aturan yang tidak sesuai. Sekarang Anda dapat mengidentifikasi AWS Config aturan yang tidak sesuai dalam konsol AWS Control Tower. Untuk melihat status kepatuhan dari semua aturan Konfigurasi Anda, buka halaman detail akun di konsol AWS Control Tower. Anda akan melihat daftar yang menunjukkan status kepatuhan kontrol yang dikelola oleh AWS Control Tower dan aturan Config yang digunakan di luar AWS Control Tower.

API untuk kontrol dan baru CloudFormation sumber daya

September 1, 2022

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower sekarang mendukung pengelolaan kontrol terprogram, juga dikenal sebagai pag ar pembatas, melalui serangkaian panggilan API. Sumber CloudFormation daya baru mendukung fungsionalitas API untuk kontrol. Untuk lebih jelasnya, lihat Otomatisasi tugas di AWS Control Tower danBuat AWS Control Tower sumber daya dengan AWS CloudFormation.

API ini memungkinkan Anda untuk mengaktifkan, menonaktifkan, dan melihat status aplikasi kontrol di pustaka AWS Control Tower. API menyertakan dukungan untuk CloudFormation, sehingga Anda dapat mengelola AWS sumber daya sebagai infrastructure-as-code (IaC). AWS Control Tower menyediakan kontrol preventif dan detektif opsional yang mengekspresikan niat kebijakan Anda mengenai seluruh unit organisasi (OU), dan setiap AWS akun dalam OU. Aturan ini tetap berlaku saat Anda membuat akun baru atau membuat perubahan pada akun yang ada.

API termasuk dalam rilis ini

- EnableControl— Panggilan API ini mengaktifkan kontrol. Ini memulai operasi asinkron yang menciptakan AWS sumber daya pada unit organisasi tertentu dan akun yang dikandungnya.
- DisableControl— Panggilan API ini mematikan kontrol. Ini memulai operasi asinkron yang menghapus AWS sumber daya pada unit organisasi tertentu dan akun yang dikandungnya.
- GetControlOperation— Mengembalikan status tertentu EnableControl atau DisableControl operasi.

- ListEnabledControls— Mencantumkan kontrol yang diaktifkan oleh AWS Control Tower pada unit organisasi yang ditentukan dan akun yang dikandungnya.

Untuk melihat daftar nama kontrol untuk kontrol opsional, lihat Pen gidentifikasi sumber daya untuk API dan kontrol, di Panduan Pengguna AWS Control Tower.

CfCT mendukung penghapusan set tumpukan

Agustus 26, 2022

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

Kustomisasi untuk AWS Control Tower (CfCT) sekarang mendukung penghapusan kumpulan tumpukan, dengan menetapkan parameter dalam file. `manifest.yaml` Untuk informasi selengkapnya, lihat Hapus set tumpukan.

> **Important**
>
> Ketika Anda awalnya menetapkan nilai `enable_stack_set_deletion` ke`true`, saat berikutnya Anda memanggil cfCt, SEMUA sumber daya yang dimulai dengan awalan`CustomControlTower-`, yang memiliki tag kunci terkait`Key:AWS_Solutions, Value: CustomControlTowerStackSet`, dan yang tidak dideklarasikan dalam file manifes, dipentaskan untuk dihapus.

Retensi log yang disesuaikan

Agustus 15, 2022

(Diperlukan pembaruan untuk zona pendaratan AWS Control Tower. Untuk informasi, lihatPerbarui landing zone Anda)

AWS Control Tower kini menyediakan kemampuan untuk menyesuaikan kebijakan retensi untuk bucket Amazon S3 yang menyimpan CloudTrail log AWS Control Tower Anda. Anda dapat menyesuaikan kebijakan penyimpanan log Amazon S3 Anda, dengan penambahan hari atau tahun, hingga maksimal 15 tahun.

Jika Anda memilih untuk tidak menyesuaikan retensi log, pengaturan default adalah 1 tahun untuk pencatatan akun standar, dan 10 tahun untuk log akses.

Fitur ini tersedia untuk pelanggan lama melalui AWS Control Tower saat Anda memperbarui atau memperbaiki zona pendaratan, dan untuk pelanggan baru melalui penyiapan AWS Control Tower

Perbaikan penyimpangan peran tersedia

Agustus 11, 2022

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower sekarang mendukung perbaikan untuk pergeseran peran. Anda dapat memulihkan peran yang diperlukan tanpa perbaikan penuh zona pendaratan Anda. Jika jenis perbaikan drift ini diperlukan, halaman kesalahan konsol menyediakan langkah-langkah untuk memulihkan peran, sehingga zona pendaratan Anda sekali lagi tersedia.

Zona pendaratan Menara Kontrol AWS versi 3.0

Juli 29, 2022

(Diperlukan pembaruan untuk zona pendaratan AWS Control Tower ke versi 3.0. Untuk informasi, lihatPerbarui landing zone Anda)

Zona pendaratan AWS Control Tower versi 3.0 mencakup pembaruan berikut:

- Pilihan untuk memilih AWS CloudTrail jalur tingkat organisasi, atau memilih keluar dari CloudTrail jalur yang dikelola oleh AWS Control Tower.
- Dua kontrol detektif baru untuk menentukan AWS CloudTrail apakah aktivitas log di akun Anda.
- Opsi untuk mengumpulkan AWS Config informasi tentang sumber daya global di Wilayah rumah Anda saja.
- Pembaruan untuk kontrol penolakan Wilayah.
- Pembaruan untuk kebijakan terkelola, AWSControlTowerServiceRolePolicy.
- Kami tidak lagi membuat peran IAM `aws-controltower-CloudWatchLogsRole` dan grup CloudWatch log `aws-controltower/CloudTrailLogs` di setiap akun terdaftar. Sebelumnya, kami membuat ini di setiap akun untuk jejak akunnya. Dengan jejak organisasi, kami hanya membuat satu di akun manajemen.

Bagian berikut memberikan rincian lebih lanjut tentang setiap kemampuan baru.

Organization-level CloudTrail jejak di Menara Kontrol AWS

Dengan zona pendaratan versi 3.0, AWS Control Tower sekarang mendukung jalur tingkat organisasi AWS CloudTrail .

Saat memperbarui zona pendaratan AWS Control Tower ke versi 3.0, Anda memiliki opsi untuk memilih AWS CloudTrail jalur tingkat organisasi sebagai preferensi pencatatan Anda, atau memilih keluar dari CloudTrail jalur yang dikelola oleh AWS Control Tower. Saat Anda memperbarui ke versi 3.0, AWS Control Tower menghapus jejak tingkat akun yang ada untuk akun terdaftar setelah masa tunggu 24 jam. AWS Control Tower tidak menghapus jejak tingkat akun untuk akun yang tidak terdaftar. Dalam kasus yang tidak mungkin terjadi bahwa pembaruan zona pendaratan Anda tidak berhasil, tetapi kegagalan terjadi setelah AWS Control Tower telah membuat jejak tingkat organisasi, Anda mungkin dikenakan biaya duplikat untuk jalur tingkat organisasi dan tingkat akun, hingga operasi pembaruan Anda berhasil diselesaikan.

Melanjutkan dari zona pendaratan 3.0, AWS Control Tower tidak lagi mendukung jalur tingkat akun yang AWS dikelola. Sebagai gantinya, AWS Control Tower membuat jejak tingkat organisasi, yang aktif atau tidak aktif, sesuai dengan pilihan Anda.

> **Note**
>
> Setelah memperbarui ke versi 3.0 atau yang lebih baru, Anda tidak memiliki opsi untuk melanjutkan dengan CloudTrail jejak tingkat akun yang dikelola oleh AWS Control Tower.

Tidak ada data logging yang hilang dari log akun agregat Anda, karena log tetap berada di bucket Amazon S3 yang ada tempat penyimpanan data tersebut. Hanya jejak yang dihapus, bukan log yang ada. Jika Anda memilih opsi untuk menambahkan jejak tingkat organisasi, AWS Control Tower membuka jalur baru ke folder baru dalam bucket Amazon S3 Anda dan terus mengirimkan informasi logging ke lokasi tersebut. Jika Anda memilih untuk memilih keluar dari jalur yang dikelola oleh AWS Control Tower, log Anda yang ada tetap berada di bucket, tidak berubah.

Konvensi penamaan jalur untuk penyimpanan log

- Log jejak akun disimpan dengan jalur formulir ini: `/org id/AWSLogs/…`
- Log jejak organisasi disimpan dengan jalur formulir ini: `/org id/AWSLogs/org id/…`

Jalur yang dibuat AWS Control Tower untuk jalur tingkat organisasi Anda berbeda dari CloudTrail jalur default untuk jejak tingkat organisasi yang dibuat secara manual, yang akan memiliki bentuk berikut:

- `/AWSLogs/org id/…`

Untuk informasi selengkapnya tentang penamaan CloudTrail jalur, lihat Menemukan file CloudTrail log Anda.

> **Tip**
>
> Jika Anda berencana untuk membuat dan mengelola jalur tingkat akun Anda sendiri, kami sarankan Anda membuat jalur baru sebelum menyelesaikan pembaruan ke zona pendaratan AWS Control Tower versi 3.0, untuk memulai pencatatan segera.

Kapan saja, Anda dapat memilih untuk membuat CloudTrail jalur tingkat akun atau tingkat organisasi baru dan mengelolanya sendiri. Opsi untuk memilih CloudTrail jalur tingkat organisasi yang dikelola oleh AWS Control Tower tersedia selama pembaruan zona pendaratan ke versi 3.0 atau yang lebih baru. Anda dapat memilih dan memilih keluar dari jalur tingkat organisasi, setiap kali Anda memperbarui zona pendaratan Anda.

Jika log Anda dikelola oleh layanan pihak ketiga, pastikan untuk memberikan nama jalur baru ke layanan Anda.

> **Note**
>
> Untuk zona pendaratan di versi 3.0 atau yang lebih baru, AWS CloudTrail jalur tingkat akun tidak didukung oleh AWS Control Tower. Anda dapat membuat dan memelihara jejak tingkat akun Anda sendiri kapan saja, atau Anda dapat memilih jalur tingkat organisasi yang dikelola oleh AWS Control Tower.

Cat AWS Config at sumber daya di Wilayah asal saja

Di zona pendaratan versi 3.0, AWS Control Tower telah memperbarui konfigurasi dasar AWS Config sehingga hanya mencatat sumber daya global di Wilayah asal. Setelah Anda memperbarui ke versi 3.0, perekaman sumber daya untuk sumber daya global hanya diaktifkan di Wilayah rumah Anda.

Konfigurasi ini dianggap sebagai praktik terbaik. Ini direkomendasikan oleh AWS Security Hub CSPM dan AWS Config, dan menciptakan penghematan biaya dengan mengurangi jumlah item konfigurasi yang dibuat ketika sumber daya global dibuat, dimodifikasi, atau dihapus. Sebelumnya, setiap kali

sumber daya global dibuat, diperbarui, atau dihapus, baik oleh pelanggan atau oleh AWS layanan, item konfigurasi dibuat untuk setiap item di setiap Wilayah yang diatur.

Dua kontrol detektif baru untuk AWS CloudTrail logging

Sebagai bagian dari perubahan AWS CloudTrail jalur tingkat organisasi, AWS Control Tower memperkenalkan dua kontrol detektif baru yang memeriksa apakah CloudTrail diaktifkan. Kontrol pertama memiliki panduan wajib, dan diaktifkan pada OU Keamanan selama pengaturan atau pembaruan zona pendaratan 3.0 dan yang lebih baru. Kontrol kedua memiliki panduan yang sangat direkomendasikan, dan secara opsional diterapkan ke OU apa pun selain OU Keamanan, yang sudah memiliki perlindungan kontrol wajib yang diberlakukan.

Kontrol wajib: Mendeteksi apakah akun bersama di bawah unit organisasi Keamanan memiliki AWS CloudTrail atau CloudTrail Lake diaktifkan

Kontrol yang sangat disarankan: Mendeteksi apakah akun telah AWS CloudTrail atau CloudTrail Lake diaktifkan

Untuk informasi selengkapnya tentang kontrol baru, lihat pustaka kontrol Menara Kontrol AWS.

Pembaruan untuk kontrol penolakan Wilayah

Kami memperbarui NotAction daftar di kontrol penolakan Wilayah untuk menyertakan tindakan oleh beberapa layanan tambahan, tercantum di bawah ini:

```
        "chatbot:*",
        "s3:GetAccountPublic",
        "s3:DeleteMultiRegionAccessPoint",
        "s3:DescribeMultiRegionAccessPointOperation",
        "s3:GetMultiRegionAccessPoint",
        "s3:GetMultiRegionAccessPointPolicy",
        "s3:GetMultiRegionAccessPointPolicyStatus",
        "s3:ListMultiRegionAccessPoints",
        "s3:GetStorageLensConfiguration",
        "s3:GetStorageLensDashboard",
        "s3:ListStorageLensConfigurations"
        "s3:GetAccountPublicAccessBlock",
        "s3:PutAccountPublic",
        "s3:PutAccountPublicAccessBlock",
```

Panduan Video

Video ini (3:07) menjelaskan cara memperbarui zona pendaratan AWS Control Tower yang ada ke versi 3. Untuk tampilan yang lebih baik, pilih ikon di sudut kanan bawah video untuk memperbesarnya ke layar penuh. Keterangan tersedia.

Panduan Video Pembaruan Zona Pendaratan Menara Kontrol AWS yang Ada ke Zona Pendaratan 3.

Halaman Organisasi menggabungkan tampilan OU dan akun

Juli 18, 2022

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower)

Halaman Organisasi baru di AWS Control Tower menampilkan tampilan hierarkis (pohon) dari semua unit organisasi (OU) dan akun. Ini menggabungkan informasi dari OU dan halaman Akun, yang ada sebelumnya.

Pada halaman baru, Anda dapat melihat hubungan antara OU induk dan OU dan akun bersarang mereka, Anda dapat mengambil tindakan pada pengelompokan sumber daya. Anda dapat mengonfigurasi tampilan halaman. Misalnya, Anda dapat memperluas atau menciutkan tampilan hierarkis, memfilter tampilan untuk melihat akun atau OU saja, memilih untuk hanya melihat akun terdaftar dan OU terdaftar, atau Anda dapat melihat grup sumber daya terkait. Lebih mudah untuk memastikan bahwa seluruh organisasi Anda diperbarui dengan benar.

Pembuatan dan pendaftaran akun yang disederhanakan

Juni 30, 2022

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower kini menyediakan alur kerja yang disederhanakan untuk membuat dan mendaftarkan akun. Anda dapat membuat akun baru atau mendaftarkan akun yang sudah ada dalam satu alur kerja, tanpa menavigasi ke konsol Katalog Layanan. Untuk informasi selengkapnya, lihat Mendaftarkan akun yang sudah ada dari konsol AWS Control Tower.

AFT mendukung kustomisasi otomatis untuk akun AWS Control Tower bersama

Mei 27, 2022

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower)

Account Factory for Terraform (AFT) sekarang dapat secara terprogram menyesuaikan dan memperbarui akun Anda yang dikelola oleh AWS Control Tower, termasuk akun manajemen, akun audit, dan akun arsip log, bersama dengan akun terdaftar Anda. Anda dapat memusatkan kustomisasi akun dan manajemen pembaruan, sambil melindungi keamanan konfigurasi akun Anda, karena Anda mencakup peran yang melakukan pekerjaan.

Peran AWSAFTexecution yang ada sekarang menerapkan penyesuaian di semua akun. Anda dapat mengatur izin IAM dengan batasan yang membatasi akses peran AWSaftExecution sesuai dengan persyaratan bisnis dan keamanan Anda. Anda juga dapat secara terprogram mendelegasikan izin penyesuaian yang disetujui dalam peran itu, untuk pengguna tepercaya. Sebagai praktik terbaik, kami sarankan Anda membatasi izin pada izin yang diperlukan untuk menerapkan penyesuaian yang diperlukan.

AFT sekarang membuat peran AWSAFTService baru untuk menerapkan sumber daya AFT di semua akun terkelola, termasuk akun bersama dan akun manajemen. Sumber daya sebelumnya dikerahkan oleh peran AWSaftExecution.

Akun bersama dan manajemen AWS Control Tower tidak disediakan melalui pabrik akun, sehingga mereka tidak memiliki produk yang disediakan terkait. AWS Service Catalog Oleh karena itu, Anda tidak dapat memperbarui akun bersama dan manajemen di Katalog Layanan.

Operasi bersamaan untuk semua kontrol opsional

Mei 18, 2022

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower)

AWS Control Tower sekarang mendukung operasi bersamaan untuk kontrol preventif, serta untuk kontrol detektif.

Dengan fitur baru ini, kontrol opsional apa pun sekarang dapat diterapkan atau dihapus secara bersamaan, sehingga meningkatkan kemudahan penggunaan dan kinerja untuk semua kontrol opsional. Anda dapat mengaktifkan beberapa kontrol opsional tanpa menunggu operasi kontrol individual selesai. Satu-satunya waktu terbatas adalah ketika AWS Control Tower sedang dalam proses penyiapan zona pendaratan, atau saat memperluas tata kelola ke organisasi baru.

Fungsionalitas yang didukung untuk kontrol preventif:

- Terapkan dan hapus kontrol pencegahan yang berbeda pada OU yang sama.

- Terapkan dan hapus kontrol pencegahan yang berbeda pada OU yang berbeda, secara bersamaan.
- Terapkan dan hapus kontrol pencegahan yang sama pada beberapa OU, secara bersamaan.
- Anda dapat menerapkan dan menghapus kontrol pencegahan dan detektif, secara bersamaan.

Anda dapat mengalami peningkatan konkurensi kontrol ini di semua versi AWS Control Tower yang dirilis.

Saat Anda menerapkan kontrol preventif ke OU bersarang, kontrol preventif memengaruhi semua akun dan OU yang bersarang di bawah OU target, bahkan jika akun dan OU tersebut tidak terdaftar di AWS Control Tower. Kontrol preventif diimplementasikan menggunakan Kebijakan Kontrol Layanan (SCP), yang merupakan bagian dari AWS Organizations. Kontrol detektif diimplementasikan menggunakan AWS Config aturan. Guardrails tetap berlaku saat Anda membuat akun baru atau membuat perubahan pada akun yang sudah ada, dan AWS Control Tower menyediakan laporan ringkasan tentang bagaimana setiap akun sesuai dengan kebijakan yang Anda aktifkan. Untuk daftar lengkap kontrol yang tersedia, lihat pust aka kontrol Menara Kontrol AWS.

Akun keamanan dan logging yang ada

Mei 16, 2022

(Tersedia selama pengaturan awal.)

AWS Control Tower sekarang menyediakan opsi bagi Anda untuk menentukan akun yang ada sebagai AWS akun keamanan atau logging AWS Control Tower, selama proses penyiapan zona pendaratan awal. Opsi ini menghilangkan kebutuhan AWS Control Tower untuk membuat akun baru bersama. Akun keamanan, yang disebut akun Audit secara default, adalah akun terbatas yang memberi tim keamanan dan kepatuhan akses ke semua akun di zona pendaratan Anda. Akun logging, yang disebut akun Log Archive secara default, berfungsi sebagai repositori. Ini menyimpan log aktivitas API dan konfigurasi sumber daya dari semua akun di zona pendaratan Anda.

Dengan menghadirkan akun keamanan dan logging yang ada, lebih mudah untuk memperluas tata kelola AWS Control Tower ke organisasi Anda yang sudah ada, atau pindah ke AWS Control Tower dari zona pendaratan alternatif. Opsi bagi Anda untuk menggunakan akun yang ada ditampilkan selama pengaturan zona pendaratan awal. Ini termasuk pemeriksaan selama proses penyiapan, yang memastikan penerapan berhasil. AWS Control Tower menerapkan peran dan kontrol yang diperlukan pada akun Anda yang ada. Itu tidak menghapus atau menggabungkan sumber daya atau data yang ada di akun ini.

Batasan: Jika Anda berencana untuk membawa AWS akun yang ada ke AWS Control Tower sebagai akun audit dan arsip log, dan jika akun tersebut memiliki AWS Config sumber daya yang ada, Anda harus menghapus AWS Config sumber daya yang ada sebelum Anda dapat mendaftarkan akun ke AWS Control Tower.

Zona pendaratan Menara Kontrol AWS versi 2.9

April 22, 2022

(Diperlukan pembaruan untuk zona pendaratan AWS Control Tower ke versi 2.9. Untuk informasi, lihatPerbarui landing zone Anda)

Zona pendaratan AWS Control Tower versi 2.9 memperbarui penerus notifikasi Lambda untuk menggunakan runtime Python versi 3.9. Pembaruan ini membahas penghentian Python versi 3.6, yang direncanakan untuk Juli 2022. Untuk informasi terbaru, lihat halaman penghentian Python.

Zona pendaratan Menara Kontrol AWS versi 2.8

Februari 10, 2022

(Diperlukan pembaruan untuk zona pendaratan AWS Control Tower ke versi 2.8. Untuk informasi, lihatPerbarui landing zone Anda)

Zona pendaratan AWS Control Tower versi 2.8 menambahkan fungsionalitas yang selaras dengan pembaruan terbaru untuk Praktik AWS Terbaik Keamanan Dasar.

Dalam rilis ini:

- Logging akses dikonfigurasi untuk bucket log akses di akun Arsip Log, untuk melacak akses ke bucket log akses S3 yang ada.
- Dukungan untuk kebijakan siklus hidup ditambahkan. Log akses untuk bucket log akses S3 yang ada disetel ke waktu retensi default 10 tahun.
- Selain itu, rilis ini memperbarui AWS Control Tower untuk menggunakan AWS Service Linked Role (SLR) yang disediakan oleh AWS Config, di semua akun terkelola (tidak termasuk akun manajemen), sehingga Anda dapat mengatur dan mengelola aturan Konfigurasi agar sesuai dengan praktik AWS Config terbaik. Pelanggan yang tidak melakukan upgrade akan terus menggunakan peran mereka yang ada.
- Rilis ini merampingkan proses konfigurasi AWS Control Tower KMS untuk mengenkripsi AWS Config data, dan meningkatkan pesan status terkait di. CloudTrail

- Rilis ini mencakup pembaruan ke kontrol penolakan Wilayah, untuk memungkinkan `route53-application-recovery` fitur tersebut masuk`us-west-2`.
- Pembaruan: Pada 15 Februari 2022, kami menghapus antrian huruf mati untuk fungsi AWS Lambda.

Rincian tambahan:

- Jika Anda menonaktifkan zona pendaratan, AWS Control Tower tidak menghapus peran terkait AWS Config layanan.
- Jika Anda menonaktifkan akun Account Factory, AWS Control Tower tidak menghapus peran terkait AWS Config layanan.

Untuk memperbarui zona pendaratan Anda ke 2.8, navigasikan ke halaman pengaturan zona pendaratan, pilih versi 2.8, lalu pilih Per barui. Setelah memperbarui zona pendaratan, Anda harus memperbarui semua akun yang diatur oleh AWS Control Tower, seperti yang diberikan dalamManajemen pembaruan konfigurasi di AWS Control Tower.

Januari - Desember 2021

Pada tahun 2021, AWS Control Tower merilis pembaruan berikut:

- Kemampuan wilayah menolak
- Fitur residensi data
- AWS Control Tower memperkenalkan penyediaan dan kustomisasi akun Terraform
- Acara siklus hidup baru tersedia
- AWS Control Tower mengaktifkan OU bersarang
- Konkurensi kontrol detektif
- Dua Wilayah baru tersedia
- Pemutusan wilayah
- AWS Control Tower bekerja dengan AWS Sistem Manajemen Kunci
- Kontrol berganti nama, fungsionalitas tidak berubah
- AWS Control Tower memindai SCP setiap hari untuk memeriksa penyimpangan
- Nama yang disesuaikan untuk OU dan akun

- Zona pendaratan Menara Kontrol AWS versi 2.7
- Tiga baru AWS Wilayah yang tersedia
- Hanya mengatur Wilayah yang dipilih
- AWS Control Tower kini memperluas tata kelola ke OU yang ada di AWS organisasi
- AWS Control Tower menyediakan pembaruan akun massal

Kemampuan wilayah menolak

November 30, 2021

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower.)

AWS Control Tower kini menyediakan kemampuan Region delete, yang membantu Anda membatasi akses ke AWS layanan dan operasi untuk akun terdaftar di lingkungan AWS Control Tower Anda. Fitur Penolakan Wilayah melengkapi fitur pemilihan Wilayah dan Penghapusan Pilihan Wilayah yang ada di Menara Kontrol AWS. Bersama-sama, fitur-fitur ini membantu Anda mengatasi masalah kepatuhan dan peraturan, sambil menyeimbangkan biaya yang terkait dengan ekspansi ke Wilayah tambahan.

Misalnya, AWS pelanggan di Jerman dapat menolak akses ke AWS layanan di Wilayah di luar Wilayah Frankfurt. Anda dapat memilih Wilayah terbatas selama proses pengaturan Menara Kontrol AWS, atau di halaman pengaturan zona pendaratan. Fitur Penolakan Wilayah tersedia saat Anda memperbarui versi zona pendaratan AWS Control Tower Anda. AWS Layanan tertentu dikecualikan dari kemampuan penolakan wilayah. Untuk mempelajari selengkapnya, lihat Meng onfigurasi kontrol penolakan wilayah.

Fitur residensi data

November 30, 2021

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower)

AWS Control Tower sekarang menawarkan kontrol yang dibuat khusus untuk membantu memastikan bahwa setiap data pelanggan yang Anda unggah ke AWS layanan hanya terletak di Wil AWS ayah yang Anda tentukan. Anda dapat memilih Wil AWS ayah atau Wilayah tempat data pelanggan Anda disimpan dan diproses. Untuk daftar lengkap Wil AWS ayah tempat AWS Control Tower tersedia, lihat Tabel AWS Wilayah.

Untuk kontrol terperinci, Anda dapat menerapkan kontrol tambahan, seperti Mel arang koneksi Amazon Virtual Private Network (VPN), atau Melarang akses internet untuk instans Amazon VPC. Anda dapat melihat status kepatuhan kontrol di konsol AWS Control Tower. Untuk daftar lengkap kontrol yang tersedia, lihat pust aka kontrol Menara Kontrol AWS.

AWS Control Tower memperkenalkan penyediaan dan kustomisasi akun Terraform

November 29, 2021

(Pembaruan opsional untuk zona pendaratan AWS Control Tower)

Anda sekarang dapat menggunakan Terraform untuk menyediakan dan memperbarui akun khusus melalui AWS Control Tower, dengan AWS Control Tower Account Factory for Terraform (AFT).

AFT menyediakan infrastruktur Terraform tunggal sebagai pipeline kode (IAc), yang menyediakan akun yang dikelola oleh AWS Control Tower. Penyesuaian selama penyediaan membantu memenuhi kebijakan bisnis dan keamanan Anda, sebelum Anda memberikan akun kepada pengguna akhir.

Pipeline pembuatan akun otomatis AFT memantau hingga penyediaan akun selesai, dan kemudian berlanjut, memicu modul Terraform tambahan yang meningkatkan akun dengan penyesuaian yang diperlukan. Sebagai bagian tambahan dari proses penyesuaian, Anda dapat mengonfigurasi pipeline untuk menginstal modul Terraform kustom Anda sendiri, dan Anda dapat memilih untuk menambahkan salah satu Opsi Fitur AFT, yang disediakan oleh AWS untuk penyesuaian umum.

Mulailah dengan AWS Control Tower Account Factory untuk Terraform dengan mengikuti langkah-langkah yang disediakan dalam Panduan Pengguna AWS Control Tower,Terapkan AWS Control Tower Account Factory untuk Terraform (AFT), dan dengan mengunduh AFT untuk instans Terraform Anda. AFT mendukung distribusi Terraform Cloud, Terraform Enterprise, dan Terraform Open Source.

Acara siklus hidup baru tersedia

November 18, 2021

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower)

Per `PrecheckOrganizationalUnit` istiwa mencatat apakah ada sumber daya yang memblokir tugas Per panjang tata kelola agar tidak berhasil, termasuk sumber daya di OU bersarang. Untuk informasi selengkapnya, lihat `PrecheckOrganizationalUnit`.

AWS Control Tower mengaktifkan OU bersarang

November 16, 2021

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower)

AWS Control Tower kini memungkinkan Anda untuk menyertakan OU bersarang sebagai bagian dari zona pendaratan Anda.

AWS Control Tower menyediakan dukungan untuk unit organisasi bersarang (OU), memungkinkan Anda mengatur akun ke dalam beberapa tingkat hierarki, dan untuk menerapkan kontrol preventif secara hierarkis. Anda dapat mendaftarkan OU yang berisi OU bersarang, membuat dan mendaftarkan OU di bawah OU induk, dan mengaktifkan kontrol pada OU terdaftar apa pun, terlepas dari kedalamannya. Untuk mendukung fungsi ini, konsol menunjukkan jumlah akun yang diatur dan OU.

Dengan OU bersarang, Anda dapat menyelaraskan OU Menara Kontrol AWS Anda dengan strategi AWS multi-akun, dan Anda dapat mengurangi waktu yang diperlukan untuk mengaktifkan kontrol pada beberapa OU, dengan menerapkan kontrol di tingkat OU induk.

Pertimbangan utama

1. Anda dapat mendaftarkan OU multi-level yang ada dengan AWS Control Tower satu OU pada satu waktu, dimulai dengan OU tingkat atas dan kemudian melanjutkan ke bawah pohon. Untuk informasi selengkapnya, lihat Perluas dari struktur OU datar ke struktur OU bersarang.
2. Akun langsung di bawah OU terdaftar terdaftar terdaftar secara otomatis. Akun yang lebih jauh di bawah pohon dapat didaftarkan dengan mendaftarkan OU induk langsungnya.
3. Kontrol preventif (SCP) diwarisi ke bawah hierarki secara otomatis; SCP yang diterapkan ke induk diwarisi oleh semua OU bersarang.
4. Kontrol detektif (aturan AWS konfigurasi) TIDAK diwariskan secara otomatis.
5. Kepatuhan terhadap kontrol detektif dilaporkan oleh masing-masing OU.
6. Penyimpangan SCP pada OU mempengaruhi semua akun dan OU di bawahnya.
7. Anda tidak dapat membuat OU bersarang baru di bawah OU Keamanan (OU inti).

Konkurensi kontrol detektif

5 November 2021

(Pembaruan opsional untuk zona pendaratan AWS Control Tower)

Kontrol detektif AWS Control Tower sekarang mendukung operasi bersamaan untuk kontrol detektif, meningkatkan kemudahan penggunaan dan kinerja. Anda dapat mengaktifkan beberapa kontrol detektif tanpa menunggu operasi kontrol individu selesai.

Fungsi yang didukung:

- Aktifkan kontrol detektif yang berbeda pada OU yang sama (misalnya, Men deteksi Apakah MFA untuk Pengguna Root Diaktifkan dan Men deteksi Apakah Akses Tulis Publik ke Bucket Amazon S3 Diizinkan).
- Aktifkan kontrol detektif yang berbeda pada OU yang berbeda, secara bersamaan.
- Pesan kesalahan pagar pembatas telah ditingkatkan untuk memberikan panduan tambahan untuk operasi konkurensi kontrol yang didukung.

Tidak didukung dalam rilis ini:

- Mengaktifkan kontrol detektif yang sama pada beberapa OU secara bersamaan tidak didukung.
- Kon kurensi kontrol preventif tidak didukung.

Anda dapat mengalami peningkatan konkurensi kontrol detektif di semua versi AWS Control Tower. Disarankan agar pelanggan yang saat ini tidak menggunakan versi 2.7 melakukan pembaruan zona pendaratan untuk memanfaatkan fitur lain, seperti pemilihan Wilayah dan penghapusan pemilihan, yang tersedia di versi terbaru.

Dua Wilayah baru tersedia

Juli 29, 2021

(Diperlukan pembaruan untuk zona pendaratan AWS Control Tower)

AWS Control Tower sekarang tersedia di dua Wil AWS ayah tambahan: Amerika Selatan (Sao Paulo), dan Eropa (Paris). Pembaruan ini memperluas ketersediaan AWS Control Tower ke 15 Wil AWS ayah.

Jika Anda baru mengenal AWS Control Tower, Anda dapat langsung meluncurkannya di salah satu Wilayah yang didukung. Selama peluncuran, Anda dapat memilih Wilayah di mana Anda ingin AWS Control Tower membangun dan mengatur lingkungan multi-akun Anda.

Jika Anda sudah memiliki lingkungan AWS Control Tower dan ingin memperluas atau menghapus fitur tata kelola AWS Control Tower di satu atau beberapa Wilayah yang didukung, buka halaman Pengaturan Zona Pen daratan di dasbor Menara Kontrol AWS Anda, lalu pilih Wilayah. Setelah memperbarui zona pendaratan, Anda harus memperbarui semua akun yang diatur oleh AWS Control Tower.

Pemutusan wilayah

Juli 29, 2021

(Pembaruan opsional untuk zona pendaratan AWS Control Tower)

Penghentian pemilihan Wilayah Menara Kontrol AWS meningkatkan kemampuan Anda untuk mengelola jejak geografis sumber daya AWS Control Tower Anda. Anda dapat membatalkan pilihan Wilayah yang tidak lagi ingin Anda atur oleh Menara Kontrol AWS. Fitur ini memberi Anda kemampuan untuk mengatasi masalah kepatuhan dan peraturan sambil menyeimbangkan biaya yang terkait dengan perluasan ke Wilayah tambahan.

Pembatalan wilayah tersedia saat Anda memperbarui versi zona pendaratan AWS Control Tower.

Saat Anda menggunakan Account Factory untuk membuat akun baru atau mendaftarkan akun anggota yang sudah ada sebelumnya, atau ketika Anda memilih Per panjang Tata Kelola untuk mendaftarkan akun di unit organisasi yang sudah ada sebelumnya, AWS Control Tower menerapkan kemampuan tata kelolainya—yang mencakup pencatatan, pemantauan, dan kontrol terpusat— di Wilayah pilihan Anda di akun. Memilih untuk membatalkan pilihan Wilayah dan menghapus tata kelola AWS Control Tower dari Wilayah tersebut akan menghapus fungsionalitas tata kelola tersebut, tetapi tidak menghambat kemampuan pengguna Anda untuk menyebarkan AWS sumber daya atau beban kerja ke Wilayah tersebut.

AWS Control Tower bekerja dengan AWS Sistem Manajemen Kunci

Juli 28, 2021

(Pembaruan opsional untuk zona pendaratan AWS Control Tower)

AWS Control Tower memberi Anda opsi untuk menggunakan AWS kunci Key Management Service (AWS KMS). Kunci disediakan dan dikelola oleh Anda, untuk mengamankan layanan yang digunakan AWS Control Tower, termasuk AWS CloudTrail, AWS Config, dan data Amazon S3 terkait. AWS Enkripsi KMS adalah tingkat enkripsi yang ditingkatkan di atas SSE-S3 enkripsi yang digunakan AWS Control Tower secara default.

Integrasi dukungan AWS KMS ke AWS Control Tower selaras dengan Praktik AWS Terbaik Keamanan Dasar, yang merekomendasikan lapisan keamanan tambahan untuk file log sensitif Anda. Anda harus menggunakan AWS KMS—managed keys (SSE-KMS) untuk enkripsi saat diam. AWS Dukungan enkripsi KMS tersedia saat Anda menyiapkan zona pendaratan baru atau saat memperbarui zona pendaratan AWS Control Tower yang ada.

Untuk mengkonfigurasi fungsi ini, Anda dapat memilih Konfigurasi Kunci KMS selama pengaturan zona pendaratan awal Anda. Anda dapat memilih kunci KMS yang ada, atau Anda dapat memilih tombol yang mengarahkan Anda ke konsol AWS KMS untuk membuat yang baru. Anda juga memiliki fleksibilitas untuk mengubah dari enkripsi default ke SSE-KMS, atau ke SSE-KMS kunci yang berbeda.

Untuk zona pendaratan AWS Control Tower yang ada, Anda dapat melakukan pembaruan untuk mulai menggunakan kunci AWS KMS.

Kontrol berganti nama, fungsionalitas tidak berubah

Juli 26, 2021

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower)

AWS Control Tower sedang merevisi nama dan deskripsi kontrol tertentu untuk mencerminkan niat kebijakan kontrol dengan lebih baik. Nama dan deskripsi yang direvisi membantu Anda memahami secara lebih intuitif cara kontrol mewujudkan kebijakan akun Anda. Misalnya, kami mengubah sebagian nama kontrol detektif dari “Disallow” menjadi “Detect” karena kontrol detektif itu sendiri tidak menghentikan tindakan tertentu, itu hanya mendeteksi pelanggaran kebijakan dan memberikan peringatan melalui dasbor.

Fungsi kontrol, panduan, dan implementasi tetap tidak berubah. Hanya nama kontrol dan deskripsi yang telah direvisi.

AWS Control Tower memindai SCP setiap hari untuk memeriksa penyimpangan

Mei 11, 2021

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower)

AWS Control Tower sekarang melakukan pemindaian otomatis harian terhadap SCP terkelola Anda untuk memverifikasi bahwa kontrol yang sesuai diterapkan dengan benar dan bahwa kontrol tersebut

belum hanyut. Jika pemindaian menemukan penyimpangan, Anda akan menerima pemberitahuan. AWS Control Tower hanya mengirimkan satu notifikasi per masalah drift, jadi jika zona pendaratan Anda sudah dalam keadaan drift, Anda tidak akan menerima pemberitahuan tambahan kecuali item drift baru ditemukan.

Nama yang disesuaikan untuk OU dan akun

April 16, 2021

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower)

AWS Control Tower sekarang memungkinkan Anda menyesuaikan penamaan zona pendaratan Anda. Anda dapat mempertahankan nama yang direkomendasikan AWS Control Tower untuk unit organisasi (OU) dan akun inti, atau Anda dapat mengubah nama-nama ini selama proses pengaturan zona pendaratan awal.

Nama default yang disediakan AWS Control Tower untuk OU dan akun inti cocok dengan panduan praktik terbaik AWS multi-akun. Namun, jika perusahaan Anda memiliki kebijakan penamaan tertentu, atau jika Anda sudah memiliki OU atau akun yang ada dengan nama yang direkomendasikan yang sama, OU baru dan fungsi penamaan akun memberi Anda fleksibilitas untuk mengatasi kendala tersebut.

Secara terpisah dari perubahan alur kerja selama penyiapan, OU yang sebelumnya dikenal sebagai Core OU sekarang disebut OU Keamanan, dan OU sebelumnya dikenal sebagai OU Kustom sekarang disebut Sandbox OU. Kami membuat perubahan ini untuk meningkatkan keselarasan kami dengan panduan praktik AWS terbaik secara keseluruhan untuk penamaan.

Pelanggan baru akan melihat nama-nama OU baru ini. Pelanggan yang ada akan terus melihat nama asli OU ini. Anda mungkin mengalami beberapa inkonsistensi dalam penamaan OU saat kami memperbarui dokumentasi kami ke nama-nama baru.

Untuk memulai menggunakan AWS Control Tower dari AWS Management Console, buka konsol AWS Control Tower, dan pilih Si apkan zona pendaratan di kanan atas. Untuk informasi tambahan, Anda dapat membaca tentang merencanakan zona pendaratan AWS Control Tower Anda.

Zona pendaratan Menara Kontrol AWS versi 2.7

April 8, 2021

(Diperlukan pembaruan untuk zona pendaratan AWS Control Tower ke versi 2.7. Untuk informasi, lihatPerbarui landing zone Anda)

Dengan AWS Control Tower versi 2.7, AWS Control Tower memperkenalkan empat kontrol Arsip Log preventif wajib baru yang menerapkan kebijakan hanya pada sumber daya AWS Control Tower. Kami telah menyesuaikan panduan pada empat kontrol Arsip Log yang ada dari wajib ke elektif, karena mereka menetapkan kebijakan untuk sumber daya di luar AWS Control Tower. Perubahan dan perluasan kontrol ini memberikan kemampuan untuk memisahkan tata kelola Log Archive untuk sumber daya dalam AWS Control Tower dari tata kelola sumber daya di luar AWS Control Tower.

Empat kontrol yang diubah dapat digunakan bersama dengan kontrol wajib baru untuk menyediakan tata kelola ke kumpulan Arsip AWS Log yang lebih luas. Lingkungan AWS Control Tower yang ada akan mengaktifkan keempat kontrol yang diubah ini secara otomatis, untuk konsistensi lingkungan; namun, kontrol elektif ini sekarang dapat dinonaktifkan. Lingkungan AWS Control Tower yang baru harus mengaktifkan semua kontrol elektif. Lingkungan yang ada harus menonaktifkan kontrol yang sebelumnya wajib sebelum menambahkan enkripsi ke bucket Amazon S3 yang tidak digunakan oleh AWS Control Tower.

Kontrol wajib baru:

- Larang Perubahan Konfigurasi Enkripsi untuk Bucket S3 yang Dibuat AWS Control Tower di Arsip Log
- Larang Perubahan Konfigurasi Logging untuk Bucket S3 yang Dibuat AWS Control Tower di Arsip Log
- Larang Perubahan Kebijakan Bucket untuk AWS Control Tower Buat Bucket S3 di Arsip Log
- Larang Perubahan Konfigurasi Siklus Hidup untuk Bucket S3 yang Dibuat AWS Control Tower di Arsip Log

Pedoman diubah dari Wajib menjadi Pilihan:

- Larang Perubahan Konfigurasi Enkripsi untuk semua Bucket Amazon S3 [Sebelumnya: Aktifkan Enkripsi saat Istirahat untuk Arsip Log]
- Larang Perubahan Konfigurasi Logging untuk semua Bucket Amazon S3 [Sebelumnya: Aktifkan Akses Logging untuk Arsip Log]
- Larang Perubahan Kebijakan Bucket untuk semua Bucket Amazon S3 [Sebelumnya: Larang Perubahan Kebijakan pada Arsip Log]
- Melarang Perubahan Konfigurasi Siklus Hidup untuk semua Bucket Amazon S3 [Sebelumnya: Tetapkan Kebijakan Retensi untuk Arsip Log]

AWS Control Tower versi 2.7 menyertakan perubahan pada cetak biru zona pendaratan AWS Control Tower yang dapat menyebabkan ketidakcocokan dengan versi sebelumnya setelah Anda memutakhirkan ke 2.7.

- Secara khusus, AWS Control Tower versi 2.7 diaktifkan `BlockPublicAccess` secara otomatis pada bucket S3 yang digunakan oleh AWS Control Tower. Anda dapat menonaktifkan default ini jika beban kerja Anda memerlukan akses di seluruh akun. Untuk informasi selengkapnya tentang apa yang terjadi dengan `BlockPublicaccess` diaktifkan, lihat Mem blokir akses publik ke penyimpanan Amazon S3 Anda.
- AWS Control Tower versi 2.7 menyertakan persyaratan untuk HTTPS. Semua permintaan yang dikirim ke bucket S3 yang digunakan oleh AWS Control Tower harus menggunakan lapisan soket aman (SSL). Hanya permintaan HTTPS yang diizinkan untuk dilewati. Jika Anda menggunakan HTTP (tanpa SSL) sebagai titik akhir untuk mengirim permintaan, perubahan ini memberi Anda kesalahan akses ditolak, yang berpotensi merusak alur kerja Anda. Perubahan ini tidak dapat dikembalikan setelah pembaruan 2.7 ke zona pendaratan Anda.

  Kami menyarankan Anda mengubah permintaan Anda untuk menggunakan TLS alih-alih HTTP.

Tiga baru AWS Wilayah yang tersedia

April 8, 2021

(Diperlukan pembaruan untuk zona pendaratan AWS Control Tower)

AWS Control Tower tersedia di tiga Wil AWS ayah tambahan: Wilayah Asia Pasifik (Tokyo), Wilayah Asia Pasifik (Seoul), dan Wilayah Asia Pasifik (Mumbai). Diperlukan pembaruan zona pendaratan ke versi 2.7 untuk memperluas tata kelola ke Wilayah ini.

Zona pendaratan Anda tidak diperluas secara otomatis ke Wilayah ini ketika Anda melakukan pembaruan ke versi 2.7, Anda harus melihat dan memilihnya di tabel Wilayah untuk dimasukkan.

Hanya mengatur Wilayah yang dipilih

Februari 19, 2021

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower)

Pemilihan Wilayah Menara Kontrol AWS memberikan kemampuan yang lebih baik untuk mengelola jejak geografis sumber daya AWS Control Tower Anda. Untuk memperluas jumlah Wilayah tempat

Anda meng-host AWS sumber daya atau beban kerja — untuk kepatuhan, peraturan, biaya, atau alasan lainnya — Anda sekarang dapat memilih Wilayah tambahan yang akan diatur.

Pilihan wilayah tersedia saat Anda menyiapkan zona pendaratan baru atau memperbarui versi zona pendaratan AWS Control Tower Anda. Saat Anda menggunakan Account Factory untuk membuat akun baru atau mendaftarkan akun anggota yang sudah ada sebelumnya, atau saat Anda menggunakan Ex tend Governance untuk mendaftarkan akun di unit organisasi yang sudah ada sebelumnya, AWS Control Tower menerapkan kemampuan tata kelola pencatatan, pemantauan, dan kontrol terpusat di Wilayah pilihan Anda di akun. Untuk informasi selengkapnya tentang memilih Wilayah, lihatKonfigurasikan Wilayah Menara Kontrol AWS Anda.

AWS Control Tower kini memperluas tata kelola ke OU yang ada di AWS organisasi

Januari 28, 2021

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower)

Perluas tata kelola ke unit organisasi (OU) yang ada (yang tidak ada di AWS Control Tower) dari dalam konsol AWS Control Tower. Dengan fitur ini, Anda dapat membawa OU tingkat atas dan akun yang disertakan di bawah tata kelola AWS Control Tower. Untuk informasi tentang memperluas tata kelola ke seluruh OU, lihatMendaftarkan unit organisasi yang ada dengan AWS Control Tower.

Saat Anda mendaftarkan OU, AWS Control Tower melakukan serangkaian pemeriksaan untuk memastikan keberhasilan perpanjangan tata kelola dan pendaftaran akun dalam OU. Untuk informasi selengkapnya tentang masalah umum yang terkait dengan pendaftaran awal OU, lihatPenyebab umum kegagalan selama pendaftaran atau pendaftaran ulang.

Anda juga dapat mengunjungi halaman web produk AWS Control Tower atau mengunjungi YouTube untuk menonton video ini tentang memulai dengan AWS Control Tower untuk AWS Organizations.

AWS Control Tower menyediakan pembaruan akun massal

Januari 28, 2021

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower)

Dengan fitur pembaruan massal, Anda sekarang dapat memperbarui semua akun di unit AWS Organizations organisasi terdaftar (OU) yang berisi hingga 300 akun, dengan satu klik, dari dasbor

AWS Control Tower. Ini sangat berguna jika Anda memperbarui zona pendaratan AWS Control Tower dan juga harus memperbarui akun terdaftar Anda untuk menyelaraskannya dengan versi zona pendaratan saat ini.

Fitur ini juga membantu Anda memperbarui akun saat memperbarui zona pendaratan AWS Control Tower untuk memperluas ke wilayah baru, atau ketika Anda ingin mendaftarkan ulang OU untuk memastikan bahwa semua akun di OU tersebut memiliki kontrol terbaru yang diterapkan. Pembaruan akun massal menghilangkan kebutuhan untuk memperbarui satu akun pada satu waktu atau menggunakan skrip eksternal untuk melakukan pembaruan pada beberapa akun.

Untuk informasi tentang memperbarui zona pendaratan, lihatPerbarui landing zone Anda.

Untuk informasi tentang mendaftarkan atau mendaftarkan ulang OU, lihatMendaftarkan unit organisasi yang ada dengan AWS Control Tower.

Januari - Desember 2020

Pada tahun 2020, AWS Control Tower merilis pembaruan berikut:

- Konsol AWS Control Tower sekarang terhubung ke eksternal AWS Aturan Config
- AWS Control Tower sekarang tersedia di Wilayah tambahan
- Pembaruan pagar pembatas
- Konsol AWS Control Tower menunjukkan detail lebih lanjut tentang OU dan akun
- Gunakan AWS Control Tower untuk menyiapkan multi-akun baru AWS lingkungan di AWS Organizations
- Kustomisasi untuk solusi AWS Control Tower
- Ketersediaan umum AWS Control Tower versi 2.3
- Single-step penyediaan akun di AWS Control Tower
- Alat penonaktifan Menara Kontrol AWS
- Pemberitahuan peristiwa siklus hidup AWS Control Tower

Konsol AWS Control Tower sekarang terhubung ke eksternal AWS Aturan Config

Desember 29, 2020

(Diperlukan pembaruan untuk zona pendaratan AWS Control Tower ke versi 2.6. Untuk informasi, lihatPerbarui landing zone Anda)

AWS Control Tower sekarang menyertakan agregator tingkat organisasi, yang membantu mendeteksi aturan konfigurasi eksternal AWS . Ini memberi Anda visibilitas di konsol AWS Control Tower untuk melihat keberadaan aturan AWS Konfigurasi yang dibuat secara eksternal selain aturan Konfigur AWS asi yang dibuat oleh AWS Control Tower. Agregator memungkinkan AWS Control Tower mendeteksi aturan eksternal dan menyediakan tautan ke konsol AWS Config tanpa memerlukan AWS Control Tower untuk mendapatkan akses ke akun yang tidak dikelola.

Dengan fitur ini, Anda sekarang memiliki tampilan konsolidasi kontrol detektif yang diterapkan ke akun Anda sehingga Anda dapat melacak kepatuhan dan menentukan apakah Anda memerlukan kontrol tambahan untuk akun Anda. Untuk selengkapnya, lihat Bagaimana AWS Control Tower menggabungkan AWS Config aturan di OU dan akun yang tidak dikelola.

AWS Control Tower sekarang tersedia di Wilayah tambahan

November 18, 2020

(Diperlukan pembaruan untuk zona pendaratan AWS Control Tower ke versi 2.5. Untuk informasi, lihatPerbarui landing zone Anda)

AWS Control Tower sekarang tersedia di 5 Wil AWS ayah tambahan:

- Wilayah Asia Pasifik (Singapura)
- Wilayah Eropa (Frankfurt)
- Wilayah Eropa (London)
- Wilayah Eropa (Stockholm)
- Wilayah Kanada (Pusat)

Penambahan 5 Wil AWS ayah ini adalah satu-satunya perubahan yang diperkenalkan untuk versi 2.5 dari AWS Control Tower.

AWS Control Tower juga tersedia di Wilayah AS Timur (Virginia Utara), Wilayah AS Timur (Ohio), Wilayah AS Barat (Oregon), Wilayah Eropa (Irlandia), dan Wilayah Asia Pasifik (Sydney). Dengan peluncuran ini AWS Control Tower sekarang tersedia di 10 Wil AWS ayah.

Pembaruan zona pendaratan ini mencakup semua Wilayah yang terdaftar dan tidak dapat dibatalkan. Setelah memperbarui zona pendaratan Anda ke versi 2.5, Anda harus memperbarui semua akun

terdaftar secara manual agar AWS Control Tower diatur di 10 Wil AWS ayah yang didukung. Untuk informasi, lihat Konfigurasikan Wilayah Menara Kontrol AWS Anda.

Pembaruan pagar pembatas

8 Oktober 2020

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower)

Versi yang diperbarui telah dirilis untuk kontrol wajib`AWS-GR_IAM_ROLE_CHANGE_PROHIBITED`.

Perubahan pada kontrol ini diperlukan karena akun yang terdaftar secara otomatis ke AWS Control Tower harus mengaktifkan `AWSControlTowerExecution` peran tersebut. Versi kontrol sebelumnya mencegah peran ini dibuat.

Untuk informasi selengkapnya, lihat Melarang Perubahan Peran AWS IAM yang Disetel oleh AWS Control Tower dan CloudFormation di Panduan Referensi Kontrol Menara Kontrol AWS.

Konsol AWS Control Tower menunjukkan detail lebih lanjut tentang OU dan akun

Juli 22, 2020

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower)

Anda dapat melihat organisasi dan akun yang tidak terdaftar di AWS Control Tower, bersama organisasi dan akun yang terdaftar.

Di dalam konsol AWS Control Tower, Anda dapat melihat detail lebih lanjut tentang AWS akun dan unit organisasi (OU) Anda. Halaman Akun sekarang mencantumkan semua akun di organisasi Anda, terlepas dari OU atau status pendaftaran di AWS Control Tower. Anda sekarang dapat mencari, mengurutkan, dan memfilter di semua tabel.

Gunakan AWS Control Tower untuk menyiapkan multi-akun baru AWS lingkungan di AWS Organizations

April 22, 2020

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower)

AWS Organizations pelanggan sekarang dapat menggunakan AWS Control Tower untuk mengelola unit organisasi (OU) dan akun yang baru dibuat dengan memanfaatkan kemampuan baru ini:

- Pel AWS Organizations anggan yang sudah ada sekarang dapat mengatur zona pendaratan baru untuk unit organisasi baru (OU) di akun manajemen mereka yang ada. Anda dapat membuat OU baru di AWS Control Tower dan membuat akun baru di OU tersebut dengan tata kelola AWS Control Tower.
- AWS Organizations pelanggan dapat mendaftarkan akun yang ada menggunakan proses pendaftaran akun atau melalui skrip.

AWS Control Tower menyediakan layanan orkestrasi yang menggunakan AWS layanan lain. Ini dirancang untuk organisasi dengan banyak akun dan tim yang mencari cara termudah untuk mengatur AWS lingkungan multi-akun baru atau yang sudah ada dan mengatur dalam skala besar. Dengan organisasi yang diatur oleh AWS Control Tower, administrator cloud tahu bahwa akun dalam organisasi sesuai dengan kebijakan yang ditetapkan. Pembangun mendapat manfaat karena mereka dapat menyediakan AWS akun baru dengan cepat, tanpa kekhawatiran yang tidak semestinya tentang kepatuhan.

Untuk informasi tentang menyiapkan zona pendaratan, lihatRencanakan landing zone AWS Control Tower. Anda juga dapat mengunjungi halaman web produk AWS Control Tower atau mengunjungi YouTube untuk menonton video ini tentang memulai dengan AWS Control Tower untuk AWS Organizations.

Selain perubahan ini, kemampuan penyedi aan akun Cepat di AWS Control Tower diganti namanya menjadi Enroll account. Sekarang memungkinkan pendaftaran AWS akun yang ada serta pembuatan akun baru. Untuk informasi selengkapnya, lihat Mendaftarkan akun yang sudah ada dari konsol AWS Control Tower.

Kustomisasi untuk solusi AWS Control Tower

Maret 17, 2020

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower)

AWS Control Tower kini menyertakan implementasi referensi baru yang memudahkan Anda menerapkan templat dan kebijakan khusus ke zona pendaratan AWS Control Tower Anda.

Dengan penyesuaian untuk AWS Control Tower, Anda dapat menggunakan CloudFormation templat untuk menyebarkan sumber daya baru ke akun yang ada dan akun baru dalam organisasi Anda. Anda juga dapat menerapkan kebijakan kontrol layanan khusus (SCP) ke akun tersebut selain SCP yang sudah disediakan oleh AWS Control Tower. Kustomisasi untuk pipeline AWS Control Tower

terintegrasi dengan peristiwa dan pemberitahuan siklus hidup AWS Control Tower (Peristiwa Siklus Hidup di Menara Kontrol AWS) untuk memastikan penerapan sumber daya tetap sinkron dengan zona pendaratan Anda.

Dokumentasi penerapan untuk arsitektur solusi AWS Control Tower ini tersedia melalui halaman web AWS Solusi.

Ketersediaan umum AWS Control Tower versi 2.3

5 Maret 2020

(Diperlukan pembaruan untuk zona pendaratan AWS Control Tower. Untuk informasi, lihatPerbarui landing zone Anda.)

AWS Control Tower sekarang tersedia di Wilayah Asia Pasifik (Sydney), selain Wil AWS ayah AS Timur (Ohio), AS Timur (Virginia Utara), AS Barat (Oregon), dan Eropa (Irlandia). Penambahan Wilayah Asia Pasifik (Sydney) adalah satu-satunya perubahan yang diperkenalkan untuk AWS Control Tower versi 2.3.

Jika Anda belum pernah menggunakan AWS Control Tower sebelumnya, Anda dapat meluncurkannya hari ini di salah satu Wilayah yang didukung. Jika Anda sudah menggunakan AWS Control Tower dan ingin memperluas fitur tata kelola ke Wilayah Asia Pasifik (Sydney) di akun Anda, buka halaman Peng aturan di dasbor AWS Control Tower Anda. Dari sana, perbarui zona pendaratan Anda ke rilis terbaru. Kemudian, perbarui akun Anda secara individual.

> **Note**
>
> Memperbarui zona pendaratan Anda tidak memperbarui akun Anda secara otomatis. Jika Anda memiliki lebih dari beberapa akun, pembaruan yang diperlukan dapat memakan waktu. Untuk alasan itu, kami menyarankan Anda menghindari memperluas zona pendaratan AWS Control Tower ke Wilayah di mana Anda tidak memerlukan beban kerja untuk dijalankan.

Untuk informasi tentang perilaku kontrol detektif yang diharapkan sebagai akibat dari penerapan ke Wilayah baru, lihat Meng onfigurasi Wilayah Menara Kontrol AWS Anda.

Single-step penyediaan akun di AWS Control Tower

Maret 2, 2020

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower)

AWS Control Tower sekarang mendukung penyediaan akun satu langkah melalui konsol AWS Control Tower. Fitur ini memungkinkan Anda untuk menyediakan akun baru dari dalam konsol AWS Control Tower.

Untuk menggunakan formulir yang disederhanakan, navigasikan ke Ac count Factory di konsol AWS Control Tower, lalu pilih Penyedi aan akun Cepat. AWS Control Tower menetapkan alamat email yang sama ke akun yang disediakan dan pengguna single sign-on (IAM Identity Center) yang dibuat untuk akun tersebut. Jika Anda memerlukan dua alamat email ini berbeda, Anda harus menyediakan akun Anda melalui Katalog Layanan.

Perbarui akun yang Anda buat melalui penyediaan akun cepat dengan menggunakan Katalog Layanan dan pabrik akun AWS Control Tower, seperti pembaruan ke akun lainnya.

> **Note**
>
> Pada bulan April 2020, kemampuan penye diaan akun Cepat berganti nama menjadi Akun Daftar. Pada Juni 2022, kemampuan untuk membuat dan memperbarui akun di konsol AWS Control Tower dipisahkan dari kemampuan untuk mendaftarkan AWS akun. Untuk informasi selengkapnya, lihat Mendaftarkan akun yang sudah ada dari konsol AWS Control Tower.

Alat penonaktifan Menara Kontrol AWS

Februari 28, 2020

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower)

AWS Control Tower sekarang mendukung alat penonaktifan otomatis untuk membantu Anda membersihkan sumber daya yang dialokasikan oleh AWS Control Tower. Jika Anda tidak lagi berniat untuk menggunakan AWS Control Tower untuk perusahaan Anda, atau jika Anda memerlukan penempatan ulang besar-besaran sumber daya organisasi Anda, Anda mungkin ingin membersihkan sumber daya yang dibuat saat Anda menyiapkan zona pendaratan.

Untuk menonaktifkan zona pendaratan Anda dengan menggunakan proses yang sebagian besar otomatis, hubungi AWS Dukungan untuk mendapatkan bantuan dengan langkah-langkah tambahan yang diperlukan. Untuk informasi lebih lanjut tentang penonaktifan, lihat. Menonaktifkan landing zone AWS Control Tower

Pemberitahuan peristiwa siklus hidup AWS Control Tower

Januari 22, 2020

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower)

AWS Control Tower mengumumkan ketersediaan pemberitahuan peristiwa siklus hidup. Per istiwa siklus hidup menandai penyelesaian tindakan AWS Control Tower yang dapat mengubah status sumber daya seperti unit organisasi (OU), akun, dan kontrol yang dibuat dan dikelola oleh AWS Control Tower. Peristiwa siklus hidup direkam sebagai AWS CloudTrail peristiwa dan dikirimkan ke Amazon EventBridge sebagai acara.

AWS Control Tower mencatat peristiwa siklus hidup pada penyelesaian tindakan berikut yang dapat dilakukan menggunakan layanan: membuat atau memperbarui zona pendaratan; membuat atau menghapus OU; mengaktifkan atau menonaktifkan kontrol pada OU; dan menggunakan pabrik akun untuk membuat akun baru atau memindahkan akun ke OU lain.

AWS Control Tower menggunakan beberapa AWS layanan untuk membangun dan mengatur AWS lingkungan multi-akun praktik terbaik. Diperlukan waktu beberapa menit untuk menyelesaikan tindakan AWS Control Tower. Anda dapat melacak peristiwa siklus hidup di CloudTrail log untuk memverifikasi apakah tindakan AWS Control Tower yang berasal berhasil diselesaikan. Anda dapat membuat EventBridge aturan untuk memberi tahu Anda saat CloudTrail merekam peristiwa siklus hidup atau untuk secara otomatis memicu langkah berikutnya dalam alur kerja otomatisasi Anda.

Juni - Desember 2019

Dari 24 Juni hingga 31 Desember 2019, AWS Control Tower merilis pembaruan berikut:

- Ketersediaan umum AWS Control Tower versi 2.2
- Kontrol elektif baru di AWS Control Tower
- Kontrol detektif baru di AWS Control Tower
- AWS Control Tower menerima alamat email untuk akun bersama dengan domain berbeda dari akun manajemen
- Ketersediaan umum AWS Control Tower versi 2.1

Ketersediaan umum AWS Control Tower versi 2.2

November 13, 2019

(Diperlukan pembaruan untuk zona pendaratan AWS Control Tower. Untuk informasi, lihatPerbarui landing zone Anda.)

AWS Control Tower versi 2.2 menyediakan tiga kontrol pencegahan baru yang mencegah penyimpangan dalam akun:

- Melarang Perubahan pada Grup CloudWatch Log Amazon yang disiapkan oleh AWS Control Tower
- Melarang Penghapusan Otorisasi AWS Config Agregasi yang Dibuat oleh AWS Control Tower
- Melarang Penghapusan Arsip Log

Kontrol adalah aturan tingkat tinggi yang menyediakan tata kelola berkelanjutan untuk AWS lingkungan Anda secara keseluruhan. Saat Anda membuat zona pendaratan AWS Control Tower, zona pendaratan dan semua unit organisasi (OU), akun, dan sumber daya sesuai dengan aturan tata kelola yang diberlakukan oleh kontrol pilihan Anda. Saat Anda dan anggota organisasi Anda menggunakan zona pendaratan, perubahan (tidak disengaja atau disengaja) dalam status kepatuhan ini dapat terjadi. Deteksi drift membantu Anda mengidentifikasi sumber daya yang memerlukan perubahan atau pembaruan konfigurasi untuk mengatasi penyimpangan. Untuk informasi selengkapnya, lihat Mendeteksi dan mengatasi penyimpangan di AWS Control Tower.

Kontrol elektif baru di AWS Control Tower

05 September 2019

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower)

AWS Control Tower sekarang menyertakan empat kontrol elektif baru berikut:

- Larang Tindakan Hapus di Bucket Amazon S3 Tanpa MFA
- Melarang Perubahan Konfigurasi Replikasi untuk Bucket Amazon S3
- Melarang Tindakan sebagai Pengguna Root
- Larang Pembuatan Kunci Akses untuk Pengguna Root

Kontrol adalah aturan tingkat tinggi yang menyediakan tata kelola berkelanjutan untuk AWS lingkungan Anda secara keseluruhan. Pagar pembatas memungkinkan Anda untuk mengekspresikan niat kebijakan Anda. Untuk informasi selengkapnya, lihat Tentang kontrol di AWS Control Tower.

Kontrol detektif baru di AWS Control Tower

Agustus 25, 2019

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower)

AWS Control Tower sekarang mencakup delapan kontrol detektif baru berikut:

- Mendeteksi apakah Pembuatan Versi untuk Bucket Amazon S3 Diaktifkan
- Mendeteksi apakah MFA diaktifkan untuk Pengguna IAM dari Konsol AWS
- Mendeteksi apakah MFA diaktifkan untuk Pengguna IAM
- Mendeteksi apakah Amazon EBS Optimization diaktifkan untuk Instans Amazon EC2
- Mendeteksi apakah Volume Amazon EBS Terlampir ke Instans Amazon EC2
- Mendeteksi apakah Akses Publik ke Instans Database Amazon RDS Diaktifkan
- Mendeteksi apakah Akses Publik ke Snapshot Database Amazon RDS Diaktifkan
- Mendeteksi apakah Enkripsi Penyimpanan Diaktifkan untuk Instans Database Amazon RDS

Kontrol adalah aturan tingkat tinggi yang menyediakan tata kelola berkelanjutan untuk AWS lingkungan Anda secara keseluruhan. Kontrol detektif mendeteksi ketidakpatuhan sumber daya dalam akun Anda, seperti pelanggaran kebijakan, dan memberikan peringatan melalui dasbor. Untuk informasi selengkapnya, lihat Tentang kontrol di AWS Control Tower.

AWS Control Tower menerima alamat email untuk akun bersama dengan domain berbeda dari akun manajemen

Agustus 01, 2019

(Tidak diperlukan pembaruan untuk zona pendaratan AWS Control Tower)

Di AWS Control Tower, Anda sekarang dapat mengirimkan alamat email untuk akun bersama (arsip log dan anggota audit) dan akun anak (dijual menggunakan pabrik akun) yang domainnya berbeda dari alamat email akun manajemen. Fitur ini hanya tersedia saat Anda membuat zona pendaratan baru dan saat Anda menyediakan akun anak baru.

Ketersediaan umum AWS Control Tower versi 2.1

24 Juni 2019

(Diperlukan pembaruan untuk zona pendaratan AWS Control Tower. Untuk informasi, lihat Memper barui Zona Pendaratan Anda.)

AWS Control Tower sekarang tersedia secara umum dan didukung untuk penggunaan produksi. AWS Control Tower ditujukan untuk organisasi dengan banyak akun dan tim yang mencari cara termudah untuk menyiapkan AWS lingkungan multi-akun baru mereka dan mengatur dalam skala besar. Dengan AWS Control Tower, Anda dapat membantu memastikan bahwa akun di organisasi Anda mematuhi kebijakan yang ditetapkan. Pengguna akhir di tim terdistribusi dapat menyediakan AWS akun baru dengan cepat.

Menggunakan AWS Control Tower, Anda dapat mengatur zona pendaratan yang menggunakan praktik terbaik seperti mengonfigurasi struktur multi-akun menggunakan AWS Organizations, mengelola identitas pengguna dan akses federasi dengan AWS IAM Identity Center, mengaktifkan penyediaan akun melalui Katalog Layanan, dan membuat arsip log terpusat menggunakan dan. AWS CloudTrail AWS Config

Untuk tata kelola berkelanjutan, Anda dapat mengaktifkan kontrol pra-konfigurasi, yang merupakan aturan yang jelas untuk keamanan, operasi, dan kepatuhan. Pagar pembatas membantu mencegah penyebaran sumber daya yang tidak sesuai dengan kebijakan dan terus memantau sumber daya yang digunakan untuk ketidaksesuaian. Dasbor AWS Control Tower menyediakan visibilitas terpusat ke AWS lingkungan termasuk akun yang disediakan, kontrol diaktifkan, dan status kepatuhan akun.

Anda dapat mengatur lingkungan multi-akun baru dengan satu klik di konsol AWS Control Tower. Tidak ada biaya tambahan atau komitmen di muka untuk menggunakan AWS Control Tower. Anda hanya membayar untuk AWS layanan yang Anda aktifkan untuk mengatur zona pendaratan dan menerapkan kontrol yang dipilih.

Riwayat dokumen

- Pembaruan dokumentasi terbaru: 30 Desember 2025

Tabel berikut menjelaskan perubahan penting pada Panduan Pengguna AWS Control Tower. Untuk notifikasi tentang pembaruan dokumentasi, Anda dapat berlangganan ke umpan RSS.

Perubahan	Deskripsi	Tanggal
Account Factory for Terraform (AFT) mendukung proses kustomisasi khusus paket	AFT sekarang mendukung kustomisasi plan-only (read-only) yang berjalan melalui `plan_only` input ke mesin status. `aft-invoke-customizations` AFT mengekspor output paket ke bucket Amazon S3 terenkripsi secara default pada distribusi Edisi Komunitas (sumber terbuka). Ekspor ikut serta di Terraform Cloud dan Terraform Enterprise.	September 16, 2026
Memperbarui ke kebijakan terkelola	Diperbarui AWS ControlTowerServiceRolePolicy.	19 Mei 2026
Memperbarui ke kebijakan terkelola	Diperbarui AWS ControlTowerAccountServiceRolePolicy.	19 Mei 2026
Memperbarui ke kebijakan terkelola	Diperbarui AWS ControlTowerAccountServiceRolePolicy.	Desember 30, 2025
AWS Control Tower landing zone versi 4.0 dengan lingkungan kontrol khusus	AWS Control Tower landing zone versi 4.0 sekarang tersedia dengan integrasi layanan opsional dan lingkungan kontrol khusus.	November 17, 2025

AWS Control Tower mencakup 279 AWS Config kontrol tambahan	Katalog Kontrol yang Diperbarui untuk menyertakan 279 AWS Config kontrol tambahan.	November 14, 2025
Memperbarui ke kebijakan terkelola	Diperbarui AWS ControlTowerAccountServiceRolePolicy.	November 10, 2025
Kebijakan terkelola yang diperbarui	Diperbarui AWS ControlTowerServiceRolePolicyuntuk mendukung AWS CloudTrail integrasi opsional Landing Zone 4.0. Pola sumber daya Amazon CloudWatch Logs berubah dari `aws-controltower/CloudTrailLogs*:*` menjadi `aws-controltower/CloudTrailLogs:*` memungkinkan pengelolaan grup log dengan sufiks unik. Pembaruan yang kompatibel ke belakang ini memungkinkan pelanggan untuk mengaktifkan dan menonaktifkan AWS CloudTrail integrasi beberapa kali, dengan grup log dibuat ulang dengan sufiks unik setiap kali untuk menghindari konflik penamaan.	November 5, 2025

Kebijakan terkelola baru	Menambahkan dokumentasi untuk kebijakan AWSControlTowerCloudTrailRolePolicyterkelola. Kebijakan terkelola ini menggantikan kebijakan inline yang sebelumnya digunakan oleh AWS ControlTowerCloudTrailRole, memungkinkan AWS untuk memperbarui kebijakan tanpa campur tangan pelanggan.	November 5, 2025
AWS Control Tower tersedia di Wilayah Asia Pasifik (Selandia Baru)	AWS Control Tower tersedia di Wilayah Auckland, Selandia Baru.	Oktober 28, 2025
AWS Control Tower mendukung pendaftaran akun otomatis	Pendaftaran akun otomatis dan perpindahan antar OU.	Oktober 15, 2025
Pembaruan ke kebijakan terkelola, kebijakan terkelola baru	Diperbarui AWS ControlTowerServiceRolePolicydan ditambahkan baru AWS ControlTowerIdentityCenterManagementPolicy.	Oktober 14, 2025
AWS Control Tower memperbarui versi Python	Versi Python yang diperbarui di lingkungan AWS Control Tower	September 3, 2025
AWS Control Tower mendukung IPv6	AWS Control Tower menambahkan dukungan untuk titik akhir IPv6.	Agustus 18, 2025
Account Factory untuk Terraform versi 1.15.0	AFT versi 1.15.0 tersedia.	Juli 28, 2025

Kontrol yang diperbarui dengan tipe instans Nitro	Memperbarui delapan kontrol proaktif untuk menambahkan jenis instance baru.	Juli 24, 2025
AWS Control Tower tersedia di Asia Pasifik (Taipei)	AWS Control Tower menambahkan dukungan untuk Asia Pasifik (Taipei).	Juli 23, 2025
AWS Control Tower mendukung AWS PrivateLink	AWS Control Tower menambahkan dukungan untuk AWS PrivateLink.	Juni 30, 2025
Service-linked AWS Config kontrol	AWS Control Tower menerapkan kontrol terkait layanan AWS Config .	Juni 12, 2025
Metadata yang ditingkatkan. kontrol tambahan, kerangka kerja baru	AWS Control Tower memperkenalkan kontrol terintegrasi tambahan dari AWS Config, dengan metadata yang disempurnakan untuk semua kontrol di Katalog Kontrol, dan dukungan untuk lebih banyak kerangka kerja industri.	Juni 12, 2025
Tampilan kontrol yang diaktifkan	AWS Control Tower memperkenalkan tampilan konsol komprehensif dari kontrol yang diaktifkan.	21 Mei 2025
AFT mendukung konfigurasi baru	AWS Control Tower AFT mendukung tiga konfigura si opsional tambahan saat penerapan.	13 Mei 2025

Garis dasar yang ditingkatkan	AWS Control Tower sekarang melaporkan penyimpangan dasar.	12 Mei 2025
AWS Control Tower tersedia di Wilayah AWS Asia Pasifik (Thailand) dan Meksiko (Tengah)	Wilayah berikut tersedia: Asia Pasifik (Thailand) dan Meksiko (Tengah).	9 Mei 2025
AWS Control Tower menambahkan 233 AWS Config kontrol	Menambahkan kontrol Config baru, tabel metadata yang dirubah, tabel Region, halaman pengenal Global.	April 11, 2025
AWS Control Tower memperbarui peran terkait layanan	Pembaruan ke`AWSControlTowerAccountServiceRolePolicy` .	Desember 10, 2024
AWS Control Tower CfCT mendukung GitHub	Opsi baru untuk sumber konfigurasi pihak ketiga.	Desember 9, 2024
Kontrol preventif AWS Control Tower dengan kebijakan deklaratif	Jenis kebijakan baru menerapkan jenis kontrol preventif baru.	Desember 1, 2024
AWS Control Tower terintegrasi dengan Backup AWS	Anda dapat menyiapkan paket untuk mencadangkan sumber daya AWS Control Tower Anda.	November 25, 2024
AWS Control Tower mengintegrasikan AWS Config kontrol	AWS Control Tower mengintegrasikan AWS Config kontrol yang dipilih.	November 21, 2024
AWS Control Tower meningkatkan manajemen hook	AWS Control Tower sekarang mengelola kait untuk kontrol proaktif.	November 20, 2024

Drift kebijakan pengendalian dilaporkan	AWS Control Tower melaporkan jenis drift baru.	November 15, 2024
AWS Control Tower meluncurkan kebijakan kontrol sumber daya terkelola	Jenis kontrol pencegahan baru, diimplementasikan dengan RCP.	November 15, 2024
AWS Control Tower menambahkan ResetEnabledControl API	API baru untuk mengelola drift kontrol.	November 14, 2024
`GetControl` API yang Diperbarui	Dua bidang kontrol baru untuk`GetControl` .	November 8, 2024
AWS Control Tower AFT mendukung Gitlab	Opsi baru untuk sumber konfigurasi pihak ketiga.	Oktober 23, 2024
AWS Control Tower tersedia di Wilayah AWS Asia Pasifik (Malaysia)	Wilayah baru tersedia, Malaysia (Kuala Lumpur).	Oktober 21, 2024
AWS Control Tower mendukung hingga 1000 akun per OU	Peningkatan batas akun per OU.	Agustus 30, 2024
AWS Control Tower menambahkan pemilihan versi landing zone	Perbarui atau perbaiki landing zone Anda tanpa pindah ke versi terbaru, jika Anda menjalankan 3.1 atau yang lebih baru.	Agustus 15, 2024
GetControl dan operasi ListControls API tersedia	Dua operasi Katalog Kontrol baru membantu Anda menemukan informasi selengkapnya tentang kontrol.	Agustus 6, 2024
AWS Control Tower mendukung AFT dan CFCT di Wilayah keikutsertaan	AFT dan CFCT tersedia dalam tambahan Wilayah AWS.	Juli 18, 2024

AWS Control Tower menambahkan `ListLandingZoneOperations` API	API baru yang memungkinkan Anda mengambil operasi terbaru untuk landing zone Anda.	Juni 26, 2024
AWS Control Tower mendukung hingga 100 operasi kontrol bersamaan	Peningkatan kuota operasi kontrol bersamaan menjadi 100.	Mei 20, 2024
AWS Control Tower tersedia di AWS Wilayah Calgary West (Kanada)	AWS Control Tower tersedia di Wilayah Kanada Barat (Calgary).	3 Mei 2024
AWS Control Tower mendukung penyesuaian kuota swalayan	AWS Control Tower terintegrasi dengan AWS Service Quotas di konsol.	April 25, 2024
Dokumentasi yang dipindahkan untuk kontrol ke panduan baru	AWS Control Tower menerbitkan Panduan Referensi Kontrol.	April 21, 2024
Menandai `EnabledControl` sumber daya di CloudFormation	AWS Control Tower mendukung penambahan tag ke `EnabledControl` sumber daya, melalui CloudFormation templat.	Februari 22, 2024
API dasar tersedia	AWS Control Tower merilis API baru untuk mendaftarkan OU secara terprogram.	Februari 14, 2024
AWS Control Tower landing zone versi 3.3	AWS Control Tower landing zone versi 3.3 tersedia.	14 Desember 2023
AWS Control Tower mengumumkan kontrol untuk membantu kedaulatan digital	AWS Control Tower merilis sekelompok kontrol untuk membantu pelanggan dengan persyaratan kedaulatan digital.	27 November 2023

AWS Control Tower mendukung API landing zone	AWS Control Tower mendukung konfigurasi dan peluncuran zona pendaratan menggunakan API baru.	26 November 2023
AWS Control Tower mendukung kontrol yang diaktifkan penandaan	AWS Control Tower mendukung penandaan kontrol yang diaktifkan, di konsol dan dengan API baru.	10 November 2023
AWS Control Tower tersedia di Asia Pasifik (Melbourne) Wilayah AWS	Tersedia di Wilayah Asia Pasifik (Melbourne).	3 November 2023
API kontrol baru tersedia	AWS Control Tower merilis API kontrol baru.	Oktober 14, 2023
AWS Control Tower meluncurkan kontrol baru	AWS Control Tower merilis kontrol proaktif dan detektif baru.	5 Oktober 2023
AWS Control Tower melaporkan penyimpangan dari menonaktifkan akses tepercaya	AWS Control Tower memberi tahu pelanggan saat drift terjadi, jika pelanggan mematikan akses tepercaya ke AWS Control Tower di. AWS Organizations	21 September 2023
AWS Control Tower tersedia dalam empat tambahan Wilayah AWS	Tersedia di Asia Pasifik (Hyderabad), Eropa (Spanyol dan Zurich), dan Timur Tengah (UEA).	13 September 2023
AWS Control Tower tersedia di Wilayah Tel Aviv	AWS Control Tower tersedia di Wilayah Tel Aviv, il-central-1.	28 Agustus 2023
AWS Control Tower meluncurkan 28 kontrol proaktif baru	AWS Control Tower merilis 28 kontrol proaktif baru.	Juli 24, 2023

AWS Control Tower menghentikan 2 kontrol	AWS Control Tower akan menghapus dua kontrol dari pustaka kontrol, efektif 18 Agustus 2023.	Juli 18, 2023
AWS Control Tower landing zone 3.2 tersedia	AWS Control Tower landing zone versi 3.2 tersedia.	Juni 16, 2023
AWS Control Tower menangani akun berdasarkan ID	AWS Control Tower melacak ID AWS akun, bukan alamat email akun.	Juni 14, 2023
Kontrol detektif CSPM Security Hub tambahan tersedia	AWS Control Tower menambahkan sepuluh kontrol baru ke pustaka kontrol, untuk Service-Managed Standar CSPM Security Hub: AWS Control Tower.	12 Juni 2023
AWS Control Tower menerbitkan tabel metadata kontrol	AWS Control Tower sekarang menyediakan tabel metadata kontrol sebagai bagian dari dokumentasi yang diterbitkan.	Juni 7, 2023
Dukungan Terraform untuk Kustomisasi Account Factory	Single-region dukungan untuk cetak biru sumber terbuka Terraform di AFC.	6 Juni 2023
AWS Manajemen mandiri IAM tersedia untuk landing zone	AWS Control Tower kini mendukung pelanggan dalam memilih penyedia identitas mereka untuk landing zone.	6 Juni 2023

Peran baru ditambahkan	AWS Control Tower menambahkan peran terkait layanan baru AWSServiceRoleForAWSControlTower, dan kebijakan terkait,. AWSControlTowerAccountServiceRolePolicy	1 Juni 2023
Pembaruan tata kelola campuran	Pembaruan untuk memberi tahu pelanggan tentang tata kelola campuran.	1 Juni 2023
Tersedia kontrol proaktif tambahan	Kontrol proaktif baru membantu Anda dalam mengatur lingkungan multi-akun Anda dan memenuhi tujuan kontrol tertentu.	19 Mei 2023
Tujuh Wilayah tambahan tersedia	AWS Control Tower sekarang tersedia dalam tujuh tambahan Wilayah AWS: California Utara (San Francisco), Asia Pasifik (Hong Kong, Jakarta, dan Osaka), Eropa (Milan), Timur Tengah (Bahrain), dan Afrika (Cape Town).	19 April 2023
Ubah ke kebijakan terkelola	Kami mengubah AWSControlTowerServiceRolePolicysehingga AWS Control Tower dapat memanggil`EnableRegion` ,`ListRegions` , `GetRegionOptStatus` API yang diimplementasikan oleh layanan Manajemen AWS Akun.	6 April 2023

Penelusuran permintaan kustomisasi akun umumnya tersedia	AWS Control Tower sekarang mendukung kemampuan untuk melacak permintaan penyesuaian akun menggunakan alur kerja Account Factory for Terraform (AFT).	16 Februari 2023
Pembaruan praktik terbaik IAM	Panduan yang diperbarui untuk menyelaraskan dengan rekomendasi praktik terbaik IAM. Untuk informasi lebih lanjut, lihat Praktik terbaik keamanan di IAM.	15 Februari 2023
AWS Control Tower landing zone 3.1 tersedia	AWS Control Tower landing zone 3.1 tersedia.	9 Februari 2023
Kontrol proaktif umumnya tersedia	Kontrol proaktif diluncurkan dari status pratinjau hingga ketersediaan umum.	Januari 24, 2023
Operasi akun bersamaan	AWS Control Tower sekarang mendukung hingga lima (5) tindakan bersamaan di pabrik akun. Anda dapat membuat, memperbarui, atau mendaftarkan hingga lima akun sekaligus.	16 Desember 2022
Kontrol proaktif membantu dalam penyediaan sumber daya	AWS Control Tower sekarang mendukung kontrol proaktif, diimplementasikan melalui CloudFormation kait.	28 November 2022

Kustomisasi akun pabrik tersedia	AWS Control Tower sekarang mendukung penyediaan akun dengan templat akun yang dapat disesuaikan, yang disebut cetak biru, langsung dari konsol AWS Control Tower.	28 November 2022
Status kepatuhan dapat dilihat untuk semua AWS Config aturan	AWS Control Tower sekarang menampilkan status kepatuhan semua AWS Config aturan yang diterapkan ke unit organisasi yang terdaftar di AWS Control Tower.	18 November 2022
Ubah ke kebijakan terkelola	Kami mengubah AWSControlTowerServiceRolePolicysehingga AWS Control Tower dapat mengambil `AWSControlTowerBlueprintAccess` peran, yang diperlukan untuk penyesuaian Account Factory.	28 Oktober 2022
API untuk kontrol, CloudFormation sumber daya	AWS Control Tower sekarang mendukung aktivasi dan penonaktifan kontrol melalui serangkaian panggilan API, dan CloudFormation sumber daya baru.	September 1, 2022
CfCT mendukung penghapusan set tumpukan	CFCT mendukung penghapusan kumpulan tumpukan, dengan menetapkan parameter dalam file manifes.	26 Agustus 2022

Retensi log yang disesuaikan	Anda dapat menyesuaikan kebijakan penyimpanan untuk bucket Amazon S3 yang menyimpan CloudTrail log AWS Control Tower Anda, dalam beberapa hari atau tahun, hingga maksimal 15 tahun.	Agustus 15, 2022
Perbaikan drift peran tersedia	AWS Control Tower mendukung perbaikan untuk drift peran, tanpa perbaikan penuh dari landing zone.	Agustus 11, 2022
Versi 3.0 tersedia	AWS Control Tower landing zone versi 3.0 berubah dari jalur berbasis akun menjadi AWS CloudTrail jalur berbasis organisasi, dan memperbar ui kebijakan terkelola untuk mengaktifkan jejak tingkat organisasi. Ini memungkin kan Anda untuk mengumpul kan AWS Config informasi di Wilayah asal Anda saja. Versi 3.0 juga mencakup pembaruan ke wilayah penolakan kontrol, dan dua kontrol detektif baru.	Juli 29, 2022
Halaman Organisasi menggabungkan tampilan OU dan akun	Halaman Organisasi baru di AWS Control Tower menampilkan tampilan hierarkis semua unit Organisasi (OU) dan akun.	18 Juli 2022

Ubah ke kebijakan terkelola	Kami mengubah AWSControlTowerServiceRolePolicysehingga pelanggan dapat memiliki AWS CloudTrail jalur tingkat organisasi ke log agregat. AWS CloudTrail	Juni 20, 2022
Mendaftar dan memperbarui akun anggota yang lebih mudah	AWS Control Tower sekarang memberi Anda kemampuan untuk mendaftarkan dan memperbarui akun anggota secara individual, dari dalam landing zone Anda. Setiap akun menunjukkan kapan tersedia untuk pembaruan . Kami memisahkan tombol Daftarkan akun dari alur kerja Buat akun di Account Factory.	31 Mei 2022
AFT mendukung kustomisasi untuk akun bersama	AWS Control Tower Account Factory untuk Terraform sekarang mendukung penyesuaian untuk akun manajemen AWS Control Tower, arsip log, dan akun audit.	Mei 27, 2022
Operasi bersamaan untuk semua kontrol opsional	AWS Control Tower sekarang memungkinkan Anda untuk menerapkan dan menghapus pagar pencegahan opsional secara bersamaan, serta kontrol detektif.	Mei 18, 2022

Akun keamanan dan pencatatan yang ada	AWS Control Tower sekarang mendukung kemampuan untuk menghadirkan akun keamanan dan logging yang ada, daripada membuat akun baru selama pengaturan landing zone.	Mei 16, 2022
Versi 2.9 tersedia	AWS Control Tower landing zone versi 2.9 memperbarui notifikasi forwarder Lambda untuk menggunakan runtime Python versi 3.9.	22 April 2022
Dukungan yang diperbarui untuk praktik AWS terbaik, versi 2.8 tersedia	AWS Control Tower landing zone versi 2.8 memberikan dukungan tambahan untuk memastikan beban kerja dan AWS akun Anda selaras dengan AWS praktik terbaik.	Februari 10, 2022
Wilayah menolak kontrol	AWS Control Tower sekarang menyertakan kontrol yang membantu Anda membatasi akses ke AWS Wilayah, untuk mengatasi masalah kepatuhan dan peraturan.	30 November 2021
Kontrol residensi data	AWS Control Tower kini mendukung kontrol yang membantu Anda mengelola residensi data dengan kontrol granular.	30 November 2021

Pabrik Akun AWS Control Tower untuk Terraform	AWS Control Tower sekarang mendukung Terraform untuk penyediaan dan pembaruan akun otomatis.	29 November 2021
Acara siklus hidup baru tersedia	`PrecheckOrganizationalUnit` Peristiwa mencatat apakah sumber daya apa pun memblokir tugas Perluas tata kelola agar tidak berhasil, termasuk sumber daya di OU bersarang.	18 November 2021
OU bersarang tersedia	AWS Control Tower sekarang memungkinkan landing zone Anda berisi struktur OU bersarang.	November 16, 2021
Konkurensi kontrol detektif	Kontrol detektif AWS Control Tower sekarang mendukung mengaktifkan dan menonaktifkan operasi secara bersamaan.	November 5, 2021
Dua wilayah baru tersedia	AWS Control Tower sekarang tersedia di dua AWS Wilayah baru, Wilayah Eropa (Paris) dan Wilayah Amerika Selatan (São Paulo).	29 Juli 2021
Pembatalan seleksi wilayah	Anda dapat membatalkan pilihan AWS Wilayah yang tidak lagi ingin Anda atur melalui AWS Control Tower.	29 Juli 2021

Kunci KMS tersedia	Anda dapat secara opsional membuat atau memilih kunci KMS yang Anda kelola, untuk mengenkripsi data dan sumber daya Anda.	28 Juli 2021
Ubah ke kebijakan terkelola	Kami mengubah AWSControlTowerServiceRolePolicysehingga pelanggan dapat menggunakan kunci enkripsi KMS mereka sendiri untuk AWS CloudTrail log.	28 Juli 2021
Nama kontrol berubah, fungsionalitas tidak berubah	Nama dan deskripsi kontrol tertentu diperbarui untuk lebih mencerminkan niat kebijakan kontrol, tanpa perubahan fungsionalitas.	26 Juli 2021
Pemindaian otomatis SCP terkelola	AWS Control Tower melakukan pemindaian otomatis harian SCP terkelola untuk memeriksa penyimpangan.	11 Mei 2021
Nama yang disesuaikan untuk OU dan akun	AWS Control Tower memungkinkan Anda memberikan nama yang disesuaikan selama proses penyiapan landing zone, untuk OU dan akun penting, tanpa membuat drift.	16 April 2021

Menonaktifkan landing zone adalah layanan mandiri	AWS Control Tower sekarang memungkinkan Anda untuk menonaktifkan landing zone tanpa menghubungi AWS Support. Penonaktifan adalah proses semi-otomatis yang tidak dapat dibatalkan. Ini tidak sama dengan menghapus semua sumber daya AWS Control Tower secara manual.	9 April 2021
Tiga Wilayah tambahan	AWS Control Tower kini tersedia di tiga AWS Wilayah tambahan: Wilayah Asia Pasifik (Tokyo), Wilayah Asia Pasifik (Seoul), dan Wilayah Asia Pasifik (Mumbai).	8 April 2021
Kontrol Log Archive baru, landing zone versi 2.7 tersedia	Empat kontrol Arsip Log baru menyediakan tata kelola Arsip Log atas sumber daya AWS Control Tower, terpisah dari tata kelola sumber daya di luar AWS Control Tower. Panduan tentang empat kontrol yang ada telah berubah dari wajib menjadi pilihan. Versi 2.7 dari AWS Control Tower landing zone menyertakan persyaratan untuk HTTPS, yang tidak dapat dibatalkan setelah Anda memperbarui.	8 April 2021

Pemilihan wilayah	Pemilihan Wilayah AWS Control Tower memberikan kemampuan yang lebih baik untuk mengelola jejak geografis sumber daya AWS Control Tower Anda. Untuk memperluas jumlah Wilayah tempat Anda menampung AWS sumber daya atau beban kerja — untuk kepatuhan, peraturan, biaya, atau alasan lainnya — Anda sekarang dapat memilih Wilayah tambahan yang akan diatur.	19 Februari 2021
Daftarkan OU dan atur semua akunnya dengan AWS Control Tower sekaligus	AWS Control Tower menambahkan kemampuan untuk mendaftarkan OU, yang merupakan cara untuk membawa beberapa akun ke dalam tata kelola pada saat yang bersamaan.	28 Januari 2021

Beberapa pembaruan akun di OU terdaftar	Anda sekarang dapat memperbarui semua akun di unit AWS Organizations organisasi terdaftar (OU) yang berisi hingga 300 akun, dengan satu klik, dari dasbor AWS Control Tower. Fitur pembaruan beberapa akun, juga disebut sebagai pembaruan massal, menghilangkan kebutuhan untuk memperbarui satu akun pada satu waktu, atau menggunakan skrip eksternal untuk melakukan pembaruan pada beberapa akun secara bersamaan.	28 Januari 2021
Peran baru untuk menggabungkan OU dan akun yang tidak dikelola	Peran baru membantu dalam mendeteksi AWS Config aturan eksternal, sehingga AWS Control Tower tidak perlu mendapatkan akses ke akun yang tidak dikelola.	29 Desember 2020

AWS Control Tower tersedia di lebih banyak AWS Wilayah.	AWS Control Tower sekarang tersedia untuk digunakan di Wilayah Asia Pasifik (Singapura), Wilayah Eropa (Frankfurt), Wilayah Eropa (London), Wilayah Eropa (Stockholm), dan Wilayah Kanada (Tengah). Dengan peluncuran ini AWS Control Tower sekarang tersedia di 10 AWS Wilayah. Pembaruan landing zone ini mencakup semua Wilayah yang terdaftar, dan tidak dapat dibatalkan. Setelah memperbarui landing zone ke versi 2.5, Anda harus memperbarui secara manual semua akun AWS Control Tower yang terdaftar untuk mengatur di 10 Wilayah yang didukung AWS .	18 November 2020
Kontrol pembaruan	Versi yang diperbarui telah dirilis untuk kontrol wajib`AWS-GR_IAM_ROLE_CHANGE_PROHIBITED` . Kontrol yang diperbarui memungkinkan pendaftaran akun otomatis yang lebih mudah.	8 Oktober 2020

Halaman informasi terkait sekarang tersedia untuk AWS Control Tower	Halaman informasi terkait memudahkan Anda menemukan tugas umum yang mungkin bermanfaat setelah menyiapkan landing zone AWS Control Tower Anda.	18 September 2020
Konsol AWS Control Tower menampilkan detail lebih lanjut tentang OU dan akun.	Dalam konsol AWS Control Tower, Anda dapat melihat detail lebih lanjut tentang AWS akun dan unit organisasi (OU) Anda. Halaman 'Akun' sekarang mencantumkan semua akun di organisasi Anda, terlepas dari status OU atau pendaftaran di AWS Control Tower. Anda sekarang dapat mencari, mengurutkan, dan memfilter di semua tabel.	22 Juli 2020
AWS Control Tower memungkinkan organisasi yang ada untuk menyiapkan landing zone	Anda sekarang dapat meluncurkan landing zone untuk AWS Control Tower di organisasi yang ada, untuk membawa organisasi ke dalam tata kelola. Kemampuan penyediaan akun Cepat di AWS Control Tower diubah namanya menjadi akun Enroll dan sekarang memungkinkan pendaftaran akun yang ada serta pembuatan AWS akun baru.	16 April 2020

AWS Control Tower sekarang tersedia di Asia Pasifik	AWS Control Tower sekarang tersedia untuk digunakan di AWS Wilayah Asia Pasifik (Sydney). Rilis ini memerlukan pembaruan manual untuk akun vended, pembaruan hanya jika Anda berencana untuk menjalankan beban kerja di Asia Pasifik (Sydney).	3 Maret 2020
Menonaktifkan zona landing zone AWS Control Tower dimungkinkan	AWS Support dapat membantu Anda menonaktifkan landing zone secara permanen melalui proses yang sebagian besar otomatis yang menjaga organisasi Anda, meskipun beberapa pembersihan manual diperlukan.	27 Februari 2020
Penyediaan akun cepat tersedia di AWS Control Tower	Penyediaan akun cepat memudahkan peluncuran akun anggota baru saat landing zone Anda diperbarui, dengan fitur akun Daftarkan.	20 Februari 2020
Peristiwa siklus hidup dilacak di AWS Control Tower	Peristiwa siklus hidup memberikan detail tambahan untuk peristiwa AWS Control Tower tertentu, untuk mempermudah otomatisasi alur kerja.	12 Desember 2019
Halaman Pengaturan dan Aktivitas tersedia untuk AWS Control Tower	Halaman Pengaturan dan Aktivitas memudahkan untuk memperbarui landing zone Anda dan melihat peristiwa yang dicatat.	November 30, 2019

Kontrol preventif tambahan tersedia untuk AWS Control Tower	Kontrol preventif di AWS Control Tower menjaga organisasi dan sumber daya Anda selaras dengan lingkungan Anda.	6 September 2019
Kontrol detektif tambahan tersedia untuk AWS Control Tower	Kontrol Detektif di AWS Control Tower memberikan informasi tentang status organisasi dan sumber daya Anda.	27 Agustus 2019
AWS Control Tower sekarang tersedia secara umum	AWS Control Tower adalah layanan yang menawarkan cara termudah untuk mengatur dan mengatur AWS lingkungan multi-akun Anda dalam skala besar.	24 Juni 2019

AWS Glosarium

Untuk AWS terminologi terbaru, lihat AWS glosarium di Referensi.Glosarium AWS

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.