Panduan Pengguna

AWS Control Tower

AWS Control Tower: Panduan Pengguna

Table of Contents

Apa itu AWS Control Tower?

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 landing zone dalam waktu kurang dari satu jam. Sumber daya diatur dan dikelola atas nama Anda.

Orkestrasi AWS Control Tower memperluas kemampuan. AWS OrganizationsUntuk membantu menjaga organisasi dan akun Anda dari penyimpangan, yang merupakan perbedaan dari praktik terbaik, AWS Control Tower menerapkan kontrol (terkadang 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 Anda 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, sesuai, berdasarkan praktik terbaik yang dibuat dengan bekerja sama dengan ribuan perusahaan. Untuk informasi selengkapnya tentang bekerja dengan AWS Control Tower dan praktik terbaik yang diuraikan dalam strategi AWS multi-akun, lihat. AWS strategi multi-akun: Panduan praktik terbaik

Fitur

AWS Control Tower memiliki beberapa fitur berikut:

- Landing zone — Landing zone 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

lainnya yang Anda inginkan untuk tunduk pada peraturan kepatuhan. Sebuah landing zone dapat disesuaikan 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 Hal ini diungkapkan dalam bahasa yang sederhana. Ada tiga jenis kontrol: preventif, detektif, dan proaktif. Tiga kategori panduan berlaku untuk kontrol: wajib, sangat direkomendasikan, atau elektif. Untuk informasi selengkapnya tentang kontrol, lihatBagaimana kontrol bekerja.
- Account Factory - Account Factory adalah template akun yang dapat dikonfigurasi yang membantu membakukan 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 dari landing zone Anda ke tim administrator cloud pusat Anda. Gunakan dasbor untuk melihat akun yang disediakan di seluruh perusahaan Anda, kontrol diaktifkan untuk penegakan kebijakan, kontrol yang diaktifkan untuk deteksi berkelanjutan atas ketidaksesuaian kebijakan, dan sumber daya yang tidak sesuai yang diatur oleh akun dan OU.

Bagaimana AWS Control Tower berinteraksi dengan layanan lain AWS

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. AWSUntuk informasi selengkapnya, lihat Cara memanfaatkan AWS Control Tower dan memigrasikan beban kerja CloudEndure ke. AWS

Konfigurasi, Tata Kelola, dan Ekstensibilitas

- Konfigurasi akun otomatis: AWS Control Tower mengotomatiskan penerapan dan pendaftaran akun melalui Account Factory (atau “mesin penjual otomatis”), yang dibangun sebagai abstraksi di atas produk yang disediakan di. AWS Service CatalogAccount Factory dapat membuat dan mendaftarkan AWS akun, dan mengotomatiskan proses penerapan kontrol dan kebijakan ke akun tersebut.

- Tata kelola terpusat: Dengan menggunakan kapabilitas 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 pengelolaan akun, pembuatan akun dari AWS Organizations API, dan kebijakan kontrol layanan (SCP).

- 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 landing zone AWS Control Tower untuk mencerminkan perubahan Anda. Jika beban kerja Anda memerlukan kemampuan lanjutan lebih lanjut, Anda dapat memanfaatkan solusi AWS mitra lainnya bersama AWS Control Tower.

Apakah Anda Pengguna Pertama Kali AWS Control Tower?

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

1. Jika Anda memerlukan informasi lebih lanjut tentang cara merencanakan dan mengatur landing zone Anda, lihat Rencanakan landing zone AWS Control Tower danAWS strategi multi-akun untuk landing zone AWS Control Tower.
2. Jika Anda siap untuk membuat landing zone pertama Anda, lihatMemulai AWS Control Tower.
3. Untuk informasi tentang deteksi dan pencegahan drift, lihatMendeteksi dan mengatasi penyimpangan di AWS Control Tower.
4. Untuk detail keamanan, lihatKeamanan di AWS Control Tower.
5. Untuk informasi tentang memperbarui landing zone 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 - OU ini berisi Arsip Log dan akun Audit. Akun-akun ini sering disebut sebagai akun bersama. Saat meluncurkan landing zone, Anda dapat memilih nama yang disesuaikan untuk akun bersama ini, dan Anda memiliki opsi untuk membawa AWS akun yang ada ke AWS Control Tower untuk keamanan dan pencatatan log. Namun, ini tidak dapat diganti namanya nanti, dan akun yang ada tidak dapat ditambahkan untuk keamanan dan pencatatan setelah peluncuran awal.
- 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 kerja AWS mereka.
- Direktori IAM Identity Center — Direktori ini menampung pengguna IAM Identity Center Anda. Ini mendefinisikan ruang lingkup izin untuk setiap pengguna IAM Identity Center.
- 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:

- Menciptakan dua unit AWS Organizations organisasi (OU): Keamanan, dan Sandbox (opsional), yang terkandung dalam struktur akar organisasi.
- Membuat atau menambahkan dua akun bersama di OU Keamanan: akun Arsip Log dan akun Audit.
- 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 Akun arsip log.

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 audit.

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. AWS CloudFormation

Bagi mereka yang akrab dengan AWS: Di AWS Control Tower, kontrol preventif diimplementasikan dengan Service Control Policies (SCP). Kontrol detektif diimplementasikan dengan AWS Config aturan. Kontrol proaktif diimplementasikan dengan AWS CloudFormation kait.

Topik-Topik Terkait

- Mendeteksi dan mengatasi penyimpangan di AWS Control Tower

Cara AWS Control Tower bekerja dengan StackSets

AWS Control Tower digunakan AWS CloudFormation StackSets untuk menyiapkan sumber daya di akun Anda. 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 AWS 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 AWS 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, AWS 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, AWS 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 AWS CloudFormation Pengguna.

Terminologi

Berikut ulasan singkat dari 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 tumbuh dan meningkatkan beban kerja Anda. AWS AWS Control Tower mengandalkan AWS Organizations untuk membuat akun, 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 AWS Control Tower Anda adalah AWS Wilayah tempat landing zone AWS Control Tower Anda digunakan. Anda dapat melihat Wilayah asal Anda di pengaturan landing zone Anda.
- AWS Service Catalogmemungkinkan Anda untuk 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 templat. CloudFormation
- Instans tumpukan adalah referensi ke tumpukan di akun target dalam Wilayah.
- Tumpukan adalah kumpulan sumber AWS 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 digunakan 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 detail lebih lanjut, lihat Informasi terkait.

- 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, baseline yang dipanggil `AWSControlTowerBaseline` tersedia untuk membantu mendaftarkan OU Anda dengan AWS Control Tower. Selama pengaturan dan pembaruan landing zone, target dasar dapat berupa akun bersama, atau pengaturan khusus untuk landing zone secara keseluruhan.
- Blueprint adalah artefak yang merangkum beberapa metadata, yang menggambarkan komponen infrastruktur yang digunakan dalam akun. Misalnya, AWS CloudFormation template dapat berfungsi sebagai cetak biru untuk akun AWS Control Tower.
- Drift: Perubahan sumber daya yang diinstal dan dikonfigurasi oleh AWS Control Tower. Sumber daya tanpa drift memungkinkan AWS Control Tower berfungsi dengan baik.
- Sumber daya yang tidak sesuai: 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 menyiapkan landing zone: 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 terdaftar atau tidak terdaftar di AWS Control Tower. Ketika OU terdaftar berisi campuran akun terdaftar dan tidak terdaftar:
  - Kontrol preventif yang diaktifkan pada OU berlaku untuk semua akun di dalamnya, termasuk yang tidak terdaftar. Ini benar karena kontrol preventif ditegakkan dengan SCP di tingkat OU, bukan tingkat akun. Untuk informasi selengkapnya, lihat Warisan untuk kebijakan kontrol layanan dalam AWS Organizations dokumentasi.
  - Kontrol Detektif yang diaktifkan pada OU tidak berlaku untuk akun yang tidak terdaftar.

  Akun dapat menjadi anggota hanya satu organisasi pada satu waktu, dan biayanya ditagih ke akun manajemen untuk organisasi itu. 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 keseluruhan lingkungan AWS Control Tower Anda. Setiap kontrol memberlakukan satu aturan. Kontrol preventif diimplementasikan dengan SCP. Kontrol detektif diimplementasikan dengan AWS Config aturan. Kontrol proaktif diimplementasikan dengan AWS CloudFormation kait. Untuk informasi selengkapnya, lihat Bagaimana kontrol bekerja.
- 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.
- Nested OU: 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. Saat 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 orangtua.
- Anak OU: Setiap OU di bawah OU saat ini dalam hierarki. OU dapat memiliki banyak anak OU.
- Hirarki OU: Di AWS Control Tower, hierarki OU bersarang dapat memiliki hingga lima level. Urutan bersarang disebut sebagai Level. Bagian atas hierarki ditetapkan sebagai Level 1.
- OU tingkat atas: OU tingkat atas adalah OU apa pun yang langsung berada di bawah Root, bukan Root itu sendiri. Root tidak dianggap sebagai OU.

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 landing zone Anda. Misalnya, Anda membayar Service Catalog untuk menyediakan akun dengan Account Factory, dan AWS CloudTrail untuk acara yang dilacak di landing zone 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 dengannya. AWS ConfigUntuk detailnya, lihat AWS Config harga. Hubungi perwakilan AWS akun Anda untuk informasi lebih spesifik tentang mengelola biaya ini. Untuk mempelajari lebih lanjut tentang cara AWS Config bekerja 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 dapat dikenakan biaya duplikat, jika Anda juga ikut serta dalam jalur yang dikelola oleh AWS Control Tower. Kami tidak menyarankan menyiapkan jalur eksternal, kecuali Anda memiliki persyaratan khusus. Jika Anda memilih untuk ikut serta selama penyiapan atau pembaruan landing zone, AWS Control Tower menyiapkan dan mengaktifkan CloudTrail jejak tingkat organisasi untuk Anda di akun manajemen. Untuk informasi tentang mengelola CloudTrail biaya, lihat Mengelola CloudTrail biaya.

Mengatur

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 AWS Control Tower.

Mendaftar untuk AWS

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.

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/signup.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan mengunjungi https://aws.amazon.com/ dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

   Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.
2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .
2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

  Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuknya, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.
2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

> **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 selanjutnya

Memulai AWS Control Tower

Memulai AWS Control Tower

Prosedur memulai ini ditujukan untuk administrator AWS Control Tower. Ikuti prosedur ini saat Anda siap menyiapkan landing zone menggunakan konsol AWS Control Tower atau API.

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

Topik

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, lihat Langkah 2. Konfigurasikan dan luncurkan landing zone Anda .

> **Note**
>
> AWS Control Tower menyiapkan layanan berbayar, seperti AWS CloudTrail, Amazon AWS ConfigCloudWatch, 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, lihat Kiat 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 disebut Harapan untuk konfigurasi landing zone .

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 Siapkan landing zone.
5. Ikuti instruksi di konsol, menerima semua nilai default. Anda harus mengetikkan alamat email untuk akun Anda, akun arsip log, dan akun audit.
6. Konfirmasikan pilihan Anda dan pilih Siapkan landing zone.
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 landing zone, AWS Control Tower secara otomatis menjalankan serangkaian pemeriksaan pra-peluncuran di akun Anda. Tidak ada tindakan yang diperlukan di pihak Anda untuk pemeriksaan ini, yang memastikan bahwa akun manajemen Anda siap untuk perubahan yang membentuk landing zone Anda. Berikut adalah pemeriksaan yang dijalankan AWS Control Tower sebelum menyiapkan landing zone:

- Batas layanan yang ada Akun AWS harus cukup untuk AWS Control Tower 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 pelanggan AWS IAM Identity Center (IAM Identity Center)

- Jika AWS IAM Identity Center (Pusat Identitas IAM) sudah disiapkan, Wilayah rumah AWS Control Tower harus sama dengan Wilayah Pusat Identitas IAM.
- Pusat Identitas IAM hanya dapat diinstal di akun manajemen suatu 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 disiapkan dengan IAM Identity Center, AWS Control Tower membuat grup di direktori IAM Identity Center dan menyediakan akses ke grup ini, untuk pengguna yang Anda pilih, untuk akun anggota.
  - Active Directory: Jika IAM Identity Center untuk AWS Control Tower disiapkan dengan Active Directory, AWS Control Tower tidak mengelola direktori IAM Identity Center. Itu tidak menetapkan pengguna atau grup ke AWS akun baru.
  - Penyedia Identitas Eksternal: Jika Pusat Identitas IAM untuk AWS Control Tower disiapkan dengan penyedia identitas eksternal (iDP), AWS Control Tower membuat grup di direktori IAM Identity Center 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 IAM Identity Center 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 dan pelanggan AWS CloudTrail

- Akses tepercaya Akun AWS tidak dapat diaktifkan di akun manajemen organisasi untuk AWS Config atau CloudTrail. Untuk informasi tentang cara menonaktifkan akses tepercaya, lihat AWS Organizations dokumentasi tentang cara mengaktifkan atau menonaktifkan akses tepercaya.
- Jika Anda memiliki penyiapan AWS Config perekam, saluran pengiriman, atau agregasi yang ada di akun apa pun yang Anda rencanakan untuk didaftarkan di AWS Control Tower, Anda harus mengubah atau menghapus konfigurasi ini sebelum mulai mendaftarkan akun, setelah

landing zone disiapkan. Pemeriksaan awal ini tidak berlaku untuk akun manajemen AWS Control Tower selama peluncuran landing zone. Untuk informasi selengkapnya, lihat Daftarkan akun yang memiliki sumber daya yang ada AWS Config.

- 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 mengelola biaya ini.
- 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, Anda mungkin melihat biaya duplikat kecuali Anda menghapus jejak yang ada untuk akun tersebut sebelum Anda mendaftarkannya di AWS Control Tower. Untuk informasi tentang jalur tingkat organisasi dan AWS Control Tower, lihat. Harga

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

Memulai AWS Control Tower dari konsol

Prosedur memulai ini ditujukan untuk administrator AWS Control Tower. Ikuti prosedur ini saat Anda siap menyiapkan landing zone menggunakan konsol AWS Control Tower. Dari awal hingga akhir, dibutuhkan sekitar setengah jam. Prosedur ini membutuhkan beberapa prasyarat dan tiga langkah utama.

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

Topik

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

Langkah 1: Buat alamat email akun bersama Anda

Jika Anda menyiapkan landing zone Anda di tempat baru Akun AWS, lihatMengatur.

- Untuk mengatur landing zone Anda dengan akun bersama baru, AWS Control Tower memerlukan dua alamat email unik yang belum dikaitkan dengan akun 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 spesifik terkait AWS Control Tower.
- Jika Anda menyiapkan AWS Control Tower untuk pertama kalinya, dan jika Anda membawa akun keamanan dan arsip 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 diperuntukkan bagi 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 memerlukan akses ke semua informasi pencatatan untuk semua akun terdaftar Anda dalam OU terdaftar di landing zone Anda.

Akun-akun ini diatur di Security OU saat Anda membuat landing zone. Sebagai praktik terbaik, kami menyarankan bahwa ketika Anda melakukan tindakan di akun ini, Anda harus menggunakan pengguna Pusat Identitas IAM dengan izin cakupan yang tepat.

> **Note**
>
> Jika Anda menetapkan AWS akun yang ada sebagai akun audit dan arsip 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 landing zone 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 default mereka: arsip log dan audit. Saat Anda membaca dokumen ini, ingatlah untuk mengganti nama khusus yang Anda berikan ke akun ini pada awalnya, jika Anda memilih untuk menyesuaikannya. Anda dapat melihat akun Anda dengan nama yang disesuaikan 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 ketidakkonsistenan saat kami melakukan transisi untuk meningkatkan kejelasan nama-nama ini. Security OU sebelumnya disebut Core OU. Sandbox OU sebelumnya disebut Custom OU.

Harapan untuk konfigurasi 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. Pilihan lain tidak dapat diubah setelah pengaturan.

Item kunci untuk dikonfigurasi selama penyiapan

- Anda dapat memilih nama OU tingkat atas selama pengaturan, dan Anda juga dapat mengubah nama OU setelah Anda mengatur landing zone Anda. Secara default, OU tingkat atas 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, Anda dapat secara opsional menentukan AWS akun yang ada untuk AWS Control Tower untuk digunakan sebagai akun audit dan arsip 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 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 setiap kali Anda memperbarui landing zone Anda.

- Anda dapat secara opsional menetapkan kebijakan retensi yang disesuaikan untuk bucket log Amazon S3 dan bucket akses log, saat menyiapkan atau memperbarui landing zone.
- Anda dapat secara opsional menentukan cetak biru yang 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 Kustomisasi akun dengan Kustomisasi Account Factory (AFC).

Pilihan konfigurasi yang tidak dapat dibatalkan

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

Langkah 2. Konfigurasikan dan luncurkan landing zone Anda

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

> **Important**
>
> Mengubah Wilayah asal Anda setelah menerapkan landing zone AWS Control Tower memerlukan penonaktifan serta bantuan Support. AWS Praktek ini tidak dianjurkan.

Pelajari cara mengonfigurasi dan meluncurkan landing zone Anda menggunakan AWS CLI inMemulai AWS Control Tower menggunakan API.

Untuk mengonfigurasi dan meluncurkan landing zone Anda di konsol, lakukan serangkaian langkah berikut.

Siapkan: 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 Anda inginkan untuk AWS Control Tower. Kemudian pilih Siapkan landing zone Anda.

Langkah 2a. Tinjau dan pilih AWS Wilayah Anda

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

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

Untuk memilih AWS Wilayah tambahan untuk diatur

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 dibawa ke tata kelola oleh AWS Control Tower. Rumah Anda Pilihan wilayah tidak dapat diedit.

Untuk menolak akses ke Wilayah tertentu

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

Langkah 2b. Konfigurasikan unit organisasi (OU) Anda

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

- Foundational OU — AWS Control Tower mengandalkan Foundational OU yang awalnya bernama Security OU. Anda dapat mengubah nama OU ini selama pengaturan awal dan sesudahnya, dari halaman detail OU. OU Keamanan ini berisi dua akun bersama Anda, yang secara default disebut akun arsip log dan akun audit.
- OU Tambahan — AWS Control Tower dapat menyiapkan satu atau lebih OU Tambahan untuk Anda. Kami menyarankan Anda menyediakan setidaknya satu OU Tambahan di landing zone Anda, selain Security OU. 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 di 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 akun AWS Control Tower bersama Anda. Akun ini adalah bagian penting dari landing zone Anda. Jangan memindahkan atau menghapus akun bersama ini. Anda dapat memilih nama yang disesuaikan untuk akun audit dan arsip 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 Anda, 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 ini juga memiliki izin administrator untuk landing zone 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 pengaturan 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 maupun yang sudah ada. Jika Anda memilih AWS Control Tower membuat akun bersama baru untuk Anda, alamat email tersebut harus belum memiliki AWS akun terkait.

Untuk mengonfigurasi akun bersama, isi informasi yang diminta.

1. Di konsol, masukkan nama untuk akun yang awalnya disebut akun arsip log. Banyak pelanggan memutuskan untuk menyimpan 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 penyimpanan log untuk bucket Amazon S3 yang menyimpan AWS CloudTrail log Anda di AWS Control Tower, dalam beberapa hari atau tahun, hingga maksimal 15 tahun. Jika Anda memilih untuk tidak menyesuaikan retensi log Anda, pengaturan default adalah satu tahun untuk pencatatan akun standar dan 10 tahun untuk pencatatan akses. Fitur ini juga tersedia saat Anda memperbarui atau mengatur ulang landing zone Anda.

Akses kelola sendiri Akun AWS secara opsional

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

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

Untuk informasi selengkapnya, lihat Panduan Pusat Identitas IAM.

Konfigurasikan AWS CloudTrail jalur secara opsional

Sebagai praktik terbaik, kami menyarankan Anda mengatur pencatatan. 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 landing zone Anda.

Anda dapat mengatur dan mengelola CloudTrail jalur Anda sendiri kapan saja, termasuk jalur tingkat organisasi dan tingkat akun. Jika Anda menyiapkan CloudTrail jejak 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 pengidentifikasi yang ditampilkan di menu tarik-turun. Anda dapat menghasilkan kunci baru dengan memilih Buat kunci. Anda dapat menambahkan atau mengubah kunci KMS setiap kali Anda memperbarui landing zone Anda.

Saat Anda memilih Siapkan landing zone, AWS Control Tower melakukan pra-pemeriksaan untuk memvalidasi kunci KMS Anda. Kuncinya harus memenuhi persyaratan ini:

- Diaktifkan
- Simetris
- Bukan kunci Multi-wilayah
- Memiliki izin yang benar ditambahkan ke kebijakan
- Kunci 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.

Perbarui 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 dan. AWS Config AWS CloudTrail Sebagai praktik terbaik, kami menyarankan 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.

Untuk memperbarui kebijakan kunci KMS

1. Buka AWS KMS konsol di https://console.aws.amazon.com/kms
2. Dari panel navigasi, pilih Kunci terkelola pelanggan.
3. Dalam tabel, pilih tombol yang ingin Anda edit.
4. Di tab Kebijakan kunci, pastikan Anda dapat melihat kebijakan kunci. Jika Anda tidak dapat melihat kebijakan utama, pilih Beralih 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:aws: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:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:key/YOUR-KMS-KEY-ID",
    "Condition": {
        "StringEquals": {
            "aws:SourceArn": "arn:aws:cloudtrail:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-ID:trail/aws-controltower-BaselineCloudTrail"
        },
        "StringLike": {
            "kms:EncryptionContext:aws:cloudtrail:arn": "arn:aws: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 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:aws: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:aws:kms:YOUR-HOME-REGION:YOUR-MANAGEMENT-ACCOUNT-
ID:key/YOUR-KMS-KEY-ID",
            "Condition": {
                "StringEquals": {
                    "aws:SourceArn": "arn:aws:cloudtrail:YOUR-HOME-REGION:YOUR-
MANAGEMENT-ACCOUNT-ID:trail/aws-controltower-BaselineCloudTrail"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:cloudtrail:arn":
 "arn:aws:cloudtrail:*:YOUR-MANAGEMENT-ACCOUNT-ID:trail/*"
                }
            }
        }
    ]
}
```

Untuk melihat contoh kebijakan lainnya, lihat halaman berikut:

- Memberikan izin enkripsi di Panduan Pengguna.AWS CloudTrail
- Izin yang Diperlukan untuk Kunci KMS Saat Menggunakan Pengiriman Bucket Roless3 Tertaut Layanan) di Panduan Pengembang.AWS Config

Melindungi dari penyerang

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

The AWS Key Management Service (AWS KMS) memungkinkan Anda membuat kunci KMS Multi-region dan kunci 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 informasi selengkapnya AWS KMS, lihat Panduan AWS KMS Pengembang.

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

Konfigurasikan dan buat akun anggota yang disesuaikan secara opsional

Saat Anda mengikuti alur kerja Buat akun untuk menambahkan akun anggota, Anda dapat secara opsional menentukan cetak biru yang telah ditentukan sebelumnya yang akan 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 Kustomisasi akun dengan Kustomisasi Account Factory (AFC).

Langkah 3. Tinjau dan atur landing zone

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

Untuk menyelesaikan

1. Di konsol, tinjau izin Layanan, dan saat Anda siap, pilih Saya memahami 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 Siapkan landing zone.

Rangkaian langkah ini memulai proses pengaturan landing zone 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. AWS Sumber daya lain dibuat, dimodifikasi, atau dihapus.

⚠ Konfirmasikan langganan SNS

Alamat email yang Anda berikan untuk akun audit akan menerima AWS Pemberitahuan — Email Konfirmasi Langganan dari setiap AWS Wilayah yang didukung oleh AWS Control Tower. Untuk menerima email kepatuhan di akun audit Anda, Anda harus memilih tautan Konfirmasi langganan dalam setiap email dari setiap AWS Wilayah 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 AWS 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
- Identifikasi landing zone
- Perbarui landing zone
- Setel ulang landing zone untuk mengatasi drift
- Nonaktifkan landing zone Anda
- Contoh: Siapkan landing zone AWS Control Tower hanya dengan API
- Meluncurkan landing zone menggunakan AWS 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: Siapkan landing zone 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 Harapan 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:

- menciptakan AWS Organizations organisasi baru,
- menyiapkan alamat email akun bersama Anda,
- 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:

1. Panggil AWS Organizations `CreateOrganization` API dan aktifkan semua fitur untuk membuat Foundational OU. AWS Control Tower awalnya menamai ini Security OU. OU Keamanan ini berisi dua akun bersama Anda, yang secara default disebut akun arsip log dan akun audit.

```
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, kami sarankan Anda menamainya Sandbox OU, seperti yang diberikan dalamAWS strategi multi-akun untuk landing zone AWS Control Tower.

Langkah 2. Menyediakan akun bersama jika diperlukan:

Untuk mengatur landing zone Anda, AWS Control Tower memerlukan dua alamat email. Jika Anda menggunakan landing zone API untuk menyiapkan AWS Control Tower untuk pertama kalinya, Anda harus menggunakan AWS akun keamanan dan arsip log yang ada. Anda dapat menggunakan alamat email saat ini dari yang ada 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 spesifik terkait AWS Control Tower.

Untuk mulai menyiapkan landing zone baru, jika Anda tidak memiliki AWS akun yang ada, Anda dapat menyediakan keamanan dan mencatat AWS akun arsip menggunakan AWS Organizations API.

1. Panggil 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"
```

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

Langkah 3. Buat peran layanan yang diperlukan

Buat peran layanan IAM berikut yang memungkinkan AWS Control Tower menjalankan panggilan API yang diperlukan untuk menyiapkan landing zone Anda:

- `AWSControlTowerAdmin`
- `AWSControlTowerCloudTrailRole`

- AWSControlTowerStackSetRole
- AWSControlTowerConfigAggregatorRoleForOrganizations

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

Untuk membuat peran IAM:

1. 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": [
                "controltower:CreateLandingZone",
                "controltower:UpdateLandingZone",
                "controltower:ResetLandingZone",
                "controltower:DeleteLandingZone",
                "controltower:GetLandingZoneOperation",
                "controltower:GetLandingZone",
                "controltower:ListLandingZones",
                "controltower:ListTagsForResource",
                "controltower:TagResource",
                "controltower:UntagResource",
                "servicecatalog:*",
                "organizations:*",
                "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": "*"
        }
    ]
}
```

Langkah 2: Luncurkan landing zone

AWS Control Tower `CreateLandingZone` API memerlukan versi landing zone dan file manifes sebagai parameter input. Anda dapat menggunakan file manifes untuk mengonfigurasi fitur berikut:

- Konfigurasikan retensi log secara opsional
- Akses kelola sendiri Akun AWS secara opsional
- Konfigurasikan AWS CloudTrail jalur secara opsional
- Konfigurasikan secara opsional AWS KMS keys

Setelah mengkompilasi file manifes Anda, Anda siap untuk membuat landing zone baru.

> **Note**
>
> AWS Control Tower tidak mendukung kontrol penolakan Wilayah saat menggunakan API untuk mengonfigurasi dan meluncurkan landing zone. Setelah berhasil meluncurkan landing zone menggunakan API, Anda dapat menggunakan konsol AWS Control Tower untuk Mengonfigurasi kontrol penolakan Wilayah.

1. Hubungi AWS Control Tower `CreateLandingZone` API. API ini memerlukan versi landing zone dan file manifes sebagai input.

   ```
   aws controltower create-landing-zone --landing-zone-version 3.3 --manifest "file://
   LandingZoneManifest.json"
   ```

   Contoh LandingZoneManifestmanifes .json:

```
{
   "governedRegions": ["us-west-2","us-west-1"],
   "organizationStructure": {
       "security": {
           "name": "CORE"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   },
   "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
   },
   "securityRoles": {
        "accountId": "333333333333"
   },
   "accessManagement": {
        "enabled": true
   }
}
```

> **Note**
>
> Seperti yang ditunjukkan pada contoh, AccountIduntuk CentralizedLogging dan SecurityRoles akun harus berbeda.

Output:

```
{
```

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

2. Panggil `GetLandingZoneOperation` API untuk memeriksa status `CreateLandingZone` operasi. `GetLandingZoneOperation`API mengembalikan status`SUCCEEDED`,`FAILED`, or`IN_PROGRESS`.

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

Output:

```
{
    "operationDetails": {
        "operationType": "CREATE",
        "startTime": "Thu Nov 09 20:39:19 UTC 2023",
        "endTime": "Thu Nov 09 21:02:01 UTC 2023",
        "status": "SUCCEEDED"
    }
}
```

3. Ketika status kembali sebagai`SUCCEEDED`, Anda dapat memanggil `GetLandingZone` API untuk meninjau konfigurasi landing zone.

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

Output:

```
{
    "landingZone": {
        "arn": "arn:aws:controltower:us-
west-2:123456789012:landingzone/1A2B3C4D5E6F7G8H",
        "driftStatus": {
            "status": "IN_SYNC"
        },
        "latestAvailableVersion": "3.3",
        "manifest": {
            "accessManagement": {
                "enabled": true
```

```
            },
            "securityRoles": {
                "accountId": "333333333333"
            },
            "governedRegions": [
                "us-west-1",
                "eu-west-3",
                "us-west-2"
            ],
            "organizationStructure": {
                "sandbox": {
                    "name": "Sandbox"
                },
                "security": {
                    "name": "CORE"
                }
            },
            "centralizedLogging": {
                "accountId": "222222222222",
                "configurations": {
                    "loggingBucket": {
                        "retentionDays": 60
                    },
                    "kmsKeyArn": "arn:aws:kms:us-west-1:123456789123:key/
e84XXXXX-6bXX-49XX-9eXX-ecfXXXXXXXXX",
                    "accessLoggingBucket": {
                        "retentionDays": 60
                    }
                },
                "enabled": true
            }
        },
        "status": "PROCESSING",
        "version": "3.3"
    }
}
```

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

Saat versi landing zone baru tersedia, atau untuk membuat pembaruan lain pada konfigurasi landing zone, Anda dapat memanggil `UpdateLandingZone` API dan mereferensikan file manifes 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 manifes 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
   ```

LandingZoneManifest.json:

```
{
   "governedRegions": ["us-west-2","us-west-1"],
   "organizationStructure": {
       "security": {
           "name": "CORE"
       },
       "sandbox": {
           "name": "Sandbox"
       }
   },
   "centralizedLogging": {
        "accountId": "222222222222",
        "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": "333333333333"
   },
   "accessManagement": {
        "enabled": true
   }
}
```

Output:

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

> **Secara opsional Registrasi ulang OU untuk memperbarui akun**
>
> Untuk AWS Control Tower OU terdaftar dengan kurang dari 300 akun, Anda dapat menggunakan konsol AWS Control Tower mengakses halaman OU di dasbor dan memilih Register ulang OU 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 hanya dapat menggunakan `ResetLandingZone` API jika Anda menggunakan versi landing zone terbaru yang tersedia. Anda dapat memanggil `GetLandingZone` API dan membandingkan versi landing zone Anda dengan versi terbaru yang tersedia. Jika perlu, Anda dapat Perbarui landing zone membuat landing zone Anda menggunakan versi terbaru yang tersedia. Dalam contoh ini, kami menggunakan versi 3.3 sebagai versi terbaru.

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.

Nonaktifkan landing zone Anda

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. Panduan: Menonaktifkan Zona Pendaratan 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"
}
```

Contoh: Siapkan landing zone AWS Control Tower hanya dengan API

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

Prasyarat

Sebelum membuat landing zone 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 >controltower_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 landing zone.

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 landing zone.

```
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 landing zone dengan versi terbaru.

Anda harus mengatur landing zone 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 landing zone Anda.

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

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

Keluaran 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-ulang, 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 rinci tentang landing zone Anda

Langkah 1. Temukan ARN dari landing zone

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

Output akan mencakup identifier dari landing zone, 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"
    }
}
```

Meluncurkan landing zone menggunakan AWS CloudFormation

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

Topik

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

Prasyarat untuk meluncurkan landing zone menggunakan AWS CloudFormation

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

   Untuk instruksi yang lebih rinci, tinjau Langkah 1: Konfigurasikan landing zone .
2. Dari AWS CloudFormation konsol atau menggunakan AWS CLI, gunakan AWS 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 AWS CloudFormation

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

```
Parameters:
  Version:
    Type: String
    Description: The version number of Landing Zone
  GovernedRegions:
    Type: List
    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 AWS CloudFormation

Anda dapat menggunakan AWS CloudFormation untuk mengelola landing zone yang telah diluncurkan dengan mengimpor landing zone di AWS 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 setelah landing zone Anda sudah 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, lihat Rekomendasi untuk menyiapkan grup, peran, dan kebijakan .
- Untuk mulai mendaftarkan organisasi dan akun dari AWS Organizations penerapan Anda, lihat Mengatur organisasi dan akun yang ada.
- Pengguna akhir Anda dapat menyediakan AWS akun mereka sendiri di landing zone Anda 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 lebih lanjut tentang kemampuan AWS Control Tower, lihat Informasi terkait.
- Coba kunjungi daftar YouTube video yang dikuratori yang menjelaskan lebih lanjut tentang cara menggunakan fungsionalitas AWS Control Tower.
- Dari waktu ke waktu, Anda mungkin perlu memperbarui landing zone Anda untuk mendapatkan pembaruan backend terbaru, kontrol terbaru, dan untuk menjaga landing zone Anda. up-to-date Untuk informasi selengkapnya, lihat Manajemen pembaruan konfigurasi di AWS Control Tower.
- Jika Anda mengalami masalah saat menggunakan AWS Control Tower, lihatMemecahkan masalah.

Important

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

Batasan dan kuota di AWS Control Tower

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

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

> **Panduan Referensi Kontrol baru**
>
> Informasi tentang kontrol AWS Control Tower telah dipindahkan ke Panduan Referensi AWS Control Tower Controls.

Batasan 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 konkurensi 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. Dari 100 operasi ini, hingga 20 sekaligus dapat menjadi operasi kontrol proaktif.
  - 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.
- Alamat email akun bersama di Security OU dapat diubah, tetapi Anda harus memperbarui landing zone untuk melihat perubahan ini di konsol AWS Control Tower.
- Batas lima (5) SCP per OU berlaku untuk OU di landing zone 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 300 akun bersarang langsung tidak dapat didaftarkan atau didaftarkan ulang di AWS Control Tower. Untuk informasi lebih lanjut tentang batasan dengan mendaftarkan OU, lihatBatasan wilayah dan tumpukan.

- Kustomisasi untuk AWS Control Tower (CFCT) tidak tersedia dalam hal ini Wilayah AWS, karena beberapa dependensi tidak tersedia:
  - Asia Pasifik (Jakarta dan Osaka)
  - Israel (Tel Aviv)
  - Timur Tengah (UEA)
  - Eropa (Spanyol)
  - Asia Pasifik (Hyderabad)
  - Eropa (Zürich)
  - Kanada Barat (Calgary)

  Anda dapat menerapkan dan mengelola sumber daya di Wilayah ini dengan CFCT, jika Anda menerapkan CFCT ke Wilayah asal AWS Control Tower, tetapi Anda tidak dapat membuat CFCT di Wilayah ini.
- AWS Control Tower Account Factory for Terraform (AFT) tidak tersedia di bawah ini Wilayah AWS, karena beberapa dependensi tidak tersedia:
  - Israel (Tel Aviv)
  - Timur Tengah (UEA)
  - Eropa (Spanyol)
  - Asia Pasifik (Hyderabad)
  - Eropa (Zürich)
  - Kanada Barat (Calgary)
- Wilayah berikut tidak mendukung Pusat Identitas IAM.
  - Wilayah Timur Tengah (UEA), me-central-1
  - Wilayah Asia Pasifik (Hyderabad), ap-south-2
  - Kanada Barat (Calgary), ca-west-1

  Untuk informasi selengkapnya tentang Wilayah AWS dan dukungan untuk IAM Identity Center, lihat Wilayah dan titik akhir di Panduan Pengguna AWS Identity and Access Management.
- Wilayah berikut tidak mendukung AWS Service Catalog.
  - Kanada Barat (Calgary), ca-west-1

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 sisa operasi antri. Anda mungkin perlu menyesuaikan kode Anda untuk menunggu penyelesaian.
- Dalam batas keseluruhan 100 operasi kontrol, hingga 20 operasi sekaligus dapat menjadi operasi kontrol proaktif.
- Saat Anda menyediakan akun melalui Penyesuaian Account Factory (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 Service Quotas 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.

Kuota berikut dapat dilihat melalui konsol Service Quotas

- Kuota operasi akun bersamaan: Jumlah maksimum operasi akun bersamaan yang dapat dilakukan pada saat yang 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 Batasan wilayah dan tumpukan di dokumentasi AWS Control Tower. Default: 300, tidak dapat disesuaikan.
- Operasi bersamaan untuk unit organisasi (OU): Jumlah maksimum operasi terkait OU 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 kuota meningkat. 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 dibandingkan dengan tiga SCP.

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

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

Video: Mengotomatiskan permintaan untuk peningkatan 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. Captioning tersedia.

Panduan Video Peningkatan Kuota di AWS Control Tower.

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 tentang AWS kuota tersedia di Referensi AWS Umum.

Keterbatasan kontrol

> **Panduan Referensi Kontrol baru**
>
> Informasi tentang kontrol AWS Control Tower telah dipindahkan ke Panduan Referensi AWS Control Tower Controls.

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 dapat dikompromikan. 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 kontrol ke konfigurasi standarnya saat Anda memperbarui landing zone. Perubahan yang mungkin telah Anda buat pada SCP digantikan oleh versi standar kontrol, dengan desain.

Beberapa kontrol di AWS Control Tower tidak beroperasi di Wilayah AWS tempat AWS Control Tower tertentu tersedia, karena Wilayah tersebut tidak mendukung fungsionalitas dasar yang diperlukan. Batasan ini memengaruhi kontrol detektif tertentu, kontrol proaktif tertentu, dan kontrol tertentu dalam Standar yang dikelola Layanan Security Hub: AWS Control Tower. Untuk informasi selengkapnya tentang ketersediaan Regional, lihat dokumentasi daftar layanan Regional dan dokumentasi referensi kontrol Security Hub.

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 keikutsertaan.

Anda dapat melihat Wilayah untuk setiap kontrol di konsol AWS Control Tower.

AWS Wilayah berikut tidak mendukung kontrol yang merupakan bagian dari Standar yang dikelola Layanan Security Hub: AWS Control Tower.

- Wilayah Asia Pasifik (Hong Kong), ap-east-1
- Wilayah Asia Pasifik (Jakarta), ap-southeast-3
- Wilayah Asia Pasifik (Osaka), ap-northeast-3
- Wilayah Eropa (Milan), eu-south-1
- Wilayah Afrika (Cape Town), af-south-1
- Wilayah Timur Tengah (Bahrain), me-south-1
- Israel (Tel Aviv), il-central-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 Barat (Calgary), ca-west-1

Berikut ini Wilayah AWS tidak mendukung kontrol proaktif.

- Kanada Barat (Calgary)

Tabel berikut menunjukkan kontrol proaktif yang tidak didukung secara tertentu Wilayah AWS.

Pengidentifikasi kontrol	Wilayah yang tidak didukung
`CT.REDSHIFT.PR.5`	ap-southeast-4, ap-south-2, ap-south-2, ap-southeast-3, eu-central-2, eu-south-2, il-central-1, me-central-1
`CT.DAX.PR.2`	us-west-1
`CT.GLUE.PR.2`	Tidak didukung

Tabel berikut menunjukkan kontrol detektif AWS Control Tower yang tidak didukung secara tertentu Wilayah AWS.

Pengidentifikasi kontrol	Wilayah yang tidak didukung
`AWS-GR_AUTOSCALING_LAUNCH_CONFIG_PUBLIC_IP_DISABLED`	ap-northeast-3, ap-southeast-3, il-central-1, ap-southeast-4, ca-west-1
`AWS-GR_LAMBDA_FUNCTION_PUBLIC_ACCESS_PROHIBITED`	eu-south-2
`AWS-GR_EMR_MASTER_NO_PUBLIC_IP`	ap-northeast-3, ap-southeast-3, af-southeast-3, af-south-1, eu-south-1, il-central-1, me-central-1, eu-central-1, eu-south-2, ap-south-2, eu-

Pengidentifikasi kontrol	Wilayah yang tidak didukung
	south-2, eu-south-2, eu-central-2 u-central-2, ap-southeast-4, ca-west-1
AWS-GR_EBS_SNAPSHOT_PUBLIC_ RESTORABLE_CHECK	eu-south-2
AWS-GR_NO_UNRESTRICTED_ROUT E_TO_IGW	ap-northeast-3, ap-southeast-3, ap-southe ast-3, ap-south-2, eu-south-2, ca-west-1
AWS-GR_SAGEMAKER_NOTEBOOK_N O_DIRECT_INTERNET_ACCESS	ap-northeast-3, ap-southeast-3, af-southeast-3, af-south-1, eu-south-1, il-central-1, me-centra l-1, eu-central-1, eu-south-2, ap-south-2, eu-south-2, eu-south-2, eu-central-2 u-central-2, ap-southeast-4, ca-west-1
AWS-GR_EC2_INSTANCE_NO_PUBLIC_IP	ap-northeast-3
AWS-GR_EKS_ENDPOINT_NO_PUBL IC_ACCESS	ap-northeast-3, ap-southeast-3, af-southeast-3, af-south-1, eu-south-1, us-west-1, il-centra l-1, me-central-1, me-central-1, me-central-1, eu-south-2, ap-south-2 th-2, eu-central-2, ap-southeast-4, ca-west-1
AWS-GR_ELASTICSEARCH_IN_VPC_ONLY	ap-southeast-3, il-central-1, eu-selatan-2, ap-south-2, ap-south-2, eu-central-2, ap-southe ast-4, ca-west-1
AWS-GR_RESTRICTED_SSH	af-south-1, ap-northeast-3, ap-south-2, ap-south-2, ap-southeast-3, ap-southeast-3, ap-southeast-4, eu-central-2, eu-south-1, eu-south-1, eu-south-2, eu-south-2, il-central-il-central-1, me-central-1
AWS-GR_DMS_REPLICATION_NOT_ PUBLIC	af-south-1, ap-south-2, ap-south-2, ap-southe ast-3, ap-southeast-4, eu-central-2, eu-south-1, eu-south-1, eu-south-2, eu-south-2, il-central-1, me-central-1 -central-1, ca-west-1

Pengidentifikasi kontrol	Wilayah yang tidak didukung
AWS-GR_RDS_SNAPSHOTS_PUBLIC_PROHIBITED	af-south-1, ap-southeast-4, eu-central-2, eu-central-2, eu-south-1, eu-south-1, eu-south-2, il-central-1
AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED	ap-northeast-3
AWS-GR_ENCRYPTED_VOLUMES	af-south-1, ap-northeast-3, eu-south-1, il-central-1
AWS-GR_RESTRICTED_COMMON_PORTS	af-south-1, ap-northeast-3, eu-central-2, eu-central-2, eu-south-1, eu-south-1, eu-south-2, il-central-1, me-central-1
AWS-GR_IAM_USER_MFA_ENABLED	il-central-1, me-central-1, eu-selatan-2, ap-selatan-2, ap-south-2, eu-central-2, ap-southeast-4, ca-west-1
AWS-GR_MFA_ENABLED_FOR_IAM_CONSOLE_ACCESS	il-central-1, me-central-1, eu-selatan-2, ap-selatan-2, ap-south-2, eu-central-2, ap-southeast-4, ca-west-1
AWS-GR_SSM_DOCUMENT_NOT_PUBLIC	il-central-1, ca-west-1
AWS-GR_ROOT_ACCOUNT_MFA_ENABLED	il-central-1, me-central-1, ca-west-1
AWS-GR_S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS_PERIODIC	il-central-1, eu-south-2, eu-central-2
AWS-GR_RDS_STORAGE_ENCRYPTED	eu-central-2, eu-south-2
AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK	ap-south-2, eu-south-2
AWS-GR_REDSHIFT_CLUSTER_PUBLIC_ACCESS_CHECK	ap-south-2, ap-southeast-3, eu-south-2, ca-west-1
AWS-GR_EC2_VOLUME_INUSE_CHECK	ca-west-1

Pengidentifikasi kontrol	Wilayah yang tidak didukung
AWS-GR_EBS_OPTIMIZED_INSTANCE	ca-west-1

Batasan wilayah dan tumpukan

Jika Anda berencana untuk memperluas tata kelola ke OU dengan sejumlah besar akun di sejumlah besar akun Wilayah AWS, Anda mungkin menemukan batasan yang dibuat oleh kumpulan AWS CloudFormation tumpukan pada ukuran keseluruhan organisasi. Anda dapat memperkirakan batasan dengan rumus ini:

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

Sebagai aturan umum, kami berharap bahwa jumlah akun yang didukung saat memperluas tata kelola ke OU berkurang dengan jumlah Wilayah yang diatur.

Batasan ini menjadi jelas jika lebih dari 15 Wilayah di mana AWS Control Tower tersedia diaktifkan saat Anda memperluas tata kelola ke OU. Batas atas jumlah akun per unit organisasi (OU) berkurang.

Misalnya, jika 22 Wilayah diaktifkan, batasnya adalah 220 akun per OU, bukan 300. Jika Anda perlu memperluas tata kelola ke OU dengan lebih dari 220 akun, Anda harus mengurangi jumlah Wilayah yang diaktifkan. Pengurangan ini disebabkan oleh keterbatasan stack set.

Pedoman:

- Dengan 15 Wilayah yang diaktifkan, OU hingga 300 akun didukung
- Dengan 22 Wilayah yang diaktifkan, OU hingga 220 akun didukung
- Dengan 16 hingga 21 Wilayah yang diaktifkan, ukuran OU maksimum yang didukung berada di kisaran 220-300 akun
- Dengan 23+ Wilayah yang diaktifkan, ukuran OU maksimum yang didukung kurang dari 220 akun

Perbedaan regional untuk fungsionalitas AWS Control Tower

Perbedaan tertentu ada dalam perilaku AWS Control Tower Wilayah AWS, karena AWS Control Tower mengatur perilaku layanan lain. AWS Sebagai 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, Penyesuaian Account Factory (AFC) tidak tersedia karena Service Catalog tidak tersedia untuk mendukung fungsionalitas dasar cetak biru.
- Kontrol tertentu tidak tersedia di semua Wilayah AWS karena kurangnya fungsionalitas yang mendasarinya.
- AFT dan CFCT tidak tersedia secara keseluruhan Wilayah AWS karena kurangnya fungsionalitas yang mendasarinya.

Untuk menentukan perilaku terbaik untuk lingkungan AWS Control Tower 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?

Baru: Panduan Referensi Kontrol AWS Control Tower

Informasi tentang kontrol di AWS Control Tower telah dipindahkan ke panduan baru, Panduan Referensi Kontrol AWS Control Tower Control.

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 kebijakan berbasis IAM dan 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). 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.

Untuk menunjukkan kontrol preventif bagi pengguna dengan kebutuhan untuk mengetahui

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 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 solusiAWS 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 Bagaimana 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 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 Mengatur 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 OrganizationsSetelah 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 Organisasi pemula produksi dengan AWS Control Tower.

Contoh AWS Control Tower dengan struktur OU multi-akun yang lengkap

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.

Anda juga dapat membangun struktur OU yang lebih sederhana dan datar yang berkinerja baik dan selaras dengan panduan AWS multi-akun. Hanya karena Anda dapat membangun struktur OU hierarkis, itu tidak berarti Anda harus melakukannya.

- Untuk melihat diagram yang menunjukkan contoh kumpulan OU di lingkungan AWS Control Tower datar yang diperluas dengan panduan AWS multi-akun, lihat Contoh: Beban Kerja dalam Struktur OU Datar.
- Untuk informasi selengkapnya tentang cara kerja AWS Control Tower dengan struktur OU bersarang, lihatOU bersarang di AWS Control Tower.

- Untuk informasi selengkapnya tentang cara AWS Control Tower selaras dengan AWS panduan, lihat AWS white paper, Mengatur AWS Lingkungan Anda Menggunakan Beberapa Akun.

Diagram pada halaman tertaut menunjukkan bahwa lebih banyak OU Dasar dan lebih banyak OU Tambahan telah dibuat. OU ini melayani kebutuhan tambahan dari penyebaran yang lebih besar.

Di kolom Foundational OU, dua OU telah ditambahkan ke struktur dasar:

- Security_Prod OU - Menyediakan area read-only untuk kebijakan keamanan, serta area audit keamanan break-glass.
- Infrastruktur OU - Anda mungkin ingin memisahkan Infrastruktur OU, yang direkomendasikan sebelumnya, menjadi dua OU, Infrastructure_Test (untuk infrastruktur pra-produksi) dan Infrastructure_Prod (untuk infrastruktur produksi).

Di area OU Tambahan, beberapa OU lagi telah ditambahkan ke struktur dasar. Berikut ini adalah OU yang direkomendasikan berikutnya untuk dibuat saat lingkungan Anda tumbuh:

- Beban Kerja OU - Beban Kerja OU, direkomendasikan sebelumnya tetapi opsional, telah dipisahkan menjadi dua OU, Workloads_Test (untuk beban kerja pra-produksi) dan Workloads_Prod (untuk beban kerja produksi).
- PolicyStaging OU — Memungkinkan administrator sistem untuk menguji perubahan mereka pada kontrol dan kebijakan sebelum menerapkannya sepenuhnya.
- Suspended OU - Menawarkan lokasi untuk akun yang mungkin telah dinonaktifkan sementara.

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

- 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 AWS Control Tower mendukung penandaan untuk kontrol yang diaktifkan.
- Sebaiknya aktifkan otentikasi multi-faktor (MFA) untuk setiap akun yang dikelola AWS Control Tower.

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 .

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 cakupan 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. Sumber daya yang tidak sesuai 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 300 akun, sehingga Anda dapat memperbarui akun tersebut dengan kemampuan Register Ulang 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 150, meskipun batasnya adalah 300 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 150 akun membutuhkan sekitar 2 jam untuk mendaftar dan mengaktifkan kontrol, dan sekitar 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 Perbarui dan pindahkan akun pabrik akun dengan AWS Control Tower atau dengan AWS Service Catalog.
- 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 reset Anda.

AWS Organizations bimbingan

- 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 gunakan AWS Organizations untuk memperbarui kebijakan kontrol layanan (SCP) yang dilampirkan ke OU yang terdaftar di AWS Control Tower. Melakukannya dapat mengakibatkan kontrol memasuki status yang tidak diketahui, yang akan mengharuskan Anda untuk mengatur ulang landing zone atau mendaftarkan ulang OU Anda di AWS Control Tower. Sebagai gantinya, Anda dapat membuat SCP baru dan melampirkannya ke OU daripada mengedit SCP yang telah dibuat AWS Control Tower.
- Memindahkan akun individu, yang sudah terdaftar, ke AWS Control Tower, dari luar OU terdaftar, menyebabkan penyimpangan yang harus diselesaikan. Lihat Jenis Drift 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

> **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.

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.

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 IAM Identity Center di AWS Control Tower, atau untuk mulai menggunakan AWS IAM Identity Center

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 kerja AWS Control Tower dengan IAM Identity Center berdasarkan sumber identitas Anda, lihat Pertimbangan untuk AWS IAM Identity Center pelanggan di bagian Pemeriksaan pra-peluncuran 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 IAM Identity Center dan AWS Control Tower untuk informasi selengkapnya tentang bekerja dengan AWS Control Tower dan IAM Identity Center.

Panduan Account Factory

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 Tidak Ada Jalur Peluncuran Ditemukan Kesalahan di bagian Pemecahan Masalah pada Panduan Pengguna AWS Control Tower.

> **Note**
>
> Hingga lima akun dapat disediakan sekaligus.

Panduan untuk berlangganan Topik SNS

- 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. Sebagai 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 disebutPerbarui kebijakan kunci KMS.

Layanan berbasis AI dan AWS Control Tower

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

Kebijakan SCP opt-out AI ini dapat berlaku untuk seluruh organisasi Anda, ke OU, atau ke akun tertentu. Kebijakan-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 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
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
2.4	Tidak ada	Tidak ada

Versi	Tanggal rilis	Deskripsi
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 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 telah mengaktifkan fitur Requester Pays secara subesquently yang harus mematikannya. Untuk informasi selengkapnya, lihat kebijakan bucket Amazon S3 untuk CloudTrail dan Menggunakan bucket Requester Pays.

Tentang Pembaruan

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 Daftar ulang 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 2.9, 3.0, dan seterusnya.

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

Perbarui Zona Pendaratan 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 berikut.

Pembaruan manual

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

Untuk memperbarui landing zone Anda secara manual, 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 300 akun).
4. Dari panel navigasi kiri, pilih Organisasi.
5. Untuk memperbarui setiap akun, ikuti langkah-langkah yang diberikanPerbarui akun di konsol.

Secara opsional Registrasi ulang OU untuk memperbarui akun

Untuk AWS Control Tower OU terdaftar dengan kurang dari 300 akun, Anda dapat membuka halaman OU di dasbor dan memilih Daftar ulang OU untuk memperbarui akun di OU tersebut.

Selesaikan drift dengan Reset dan Register Ulang

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 sebagian besar jenis drift, pilih Reset pada halaman pengaturan zona pendaratan. Selain itu, Anda dapat menyelesaikan beberapa jenis drift dengan memilih untuk mendaftarkan ulang OU. Untuk informasi selengkapnya tentang jenis drift dan cara mengatasinya, lihat Jenis Drift 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 menampilkan halaman peringatan dan beberapa petunjuk tentang cara memulihkan 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 mengatasi drift pada versi landing zone, dua perilaku dimungkinkan.

- Jika Anda menggunakan versi landing zone terbaru, ketika Anda memilih Reset dan kemudian memilih Konfirmasi, sumber daya zona pendaratan drifted Anda diatur ulang ke konfigurasi AWS Control Tower yang disimpan. Versi landing zone tetap sama.
- Jika Anda tidak menggunakan versi terbaru, Anda harus memilih Perbarui. Landing zone ditingkatkan ke versi landing zone terbaru. Drift diselesaikan sebagai bagian dari proses ini.

Menyediakan dan memperbarui akun menggunakan otomatisasi

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 AWS Control Tower Account Factory 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, lihatPanduan: Mengotomatiskan Penyediaan Akun di AWS Control Tower oleh 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:

- Menggunakan AWS CloudShell untuk bekerja dengan AWS Control Tower.
- Mengotomatiskan tugas di AWS Control Tower .

Mengotomatiskan tugas di AWS Control Tower

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

- AWS Service Catalog API
- AWS Organizations API
- API AWS Control Tower
- AWS CLI

Informasi terkaitHalaman ini berisi tautan ke banyak posting blog teknis luar biasa yang dapat membantu Anda mengotomatiskan tugas di AWS Control Tower. Bagian berikut menyediakan tautan ke area dalam Panduan Pengguna AWS Control Tower 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 pembatas) melalui AWS Control Tower API. Untuk detailnya, lihat Referensi AWS Control Tower API.

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 landing zone

API landing zone AWS Control Tower membantu Anda mengotomatiskan tugas tertentu yang terkait dengan landing zone Anda. Untuk detailnya, lihat Referensi AWS Control Tower API.

Mengotomatiskan pendaftaran OU

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

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 pemutakhiran akun otomatis

Kustomisasi Pabrik Akun AWS Control Tower (AFC) membantu Anda membuat akun dari konsol AWS Control Tower, dengan AWS 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 mempertahankan 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 landing zone AWS Control Tower dan tetap selaras dengan praktik terbaik. AWS Kustomisasi diimplementasikan dengan AWS CloudFormation template dan kebijakan kontrol layanan (SCP). 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 AWS Control Tower dan Penyediaan otomatis dengan peran IAM.

Lihat juga Perbarui akun berdasarkan skrip.

Audit akun 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: Mengotomatiskan Peningkatan Batas Layanan.

Untuk blog teknis yang mencakup kasus penggunaan otomatisasi dan integrasi, lihat Otomasi 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 mengotomatisasi pengaturan akun Audit sebagai administrator yang didelegasikan untuk layanan terkait keamanan.
- Contoh yang disebut aws-control-tower-account- setup-using-step-functions menunjukkan cara mengotomatiskan praktik terbaik keamanan menggunakan Step Functions, saat menyediakan dan mengonfigurasi akun baru. Contoh ini termasuk menambahkan prinsipal ke AWS Service Catalog portofolio yang dibagikan secara organisasi dan mengaitkan grup Pusat Identitas IAM di seluruh organisasi ke akun baru secara otomatis. AWS Ini juga menggambarkan cara menghapus VPC default di setiap Wilayah.

Arsitektur Referensi AWS Keamanan mencakup contoh kode untuk mengotomatisasi tugas yang terkait dengan AWS Control Tower. Untuk informasi selengkapnya, lihat halaman Panduan AWS Preskriptif dan repositori terkait GitHub .

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

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

Menggunakan AWS CloudShell untuk bekerja dengan AWS Control Tower

AWS CloudShell adalah AWS layanan yang memfasilitasi bekerja di AWS CLI — ini adalah shell berbasis browser dan pra-otentikasi yang dapat Anda luncurkan langsung dari. AWS Management ConsoleTidak 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 AWS Management Console, AWS kredensil yang Anda gunakan untuk masuk ke konsol tersedia di sesi shell baru. Anda dapat melewatkan memasukkan kredensi konfigurasi 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 sudah diautentikasi sebelumnya. AWS CloudShell

Memperoleh 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 diakses. AWS CloudShell

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

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

Jika Anda ingin membatasi cakupan tindakan yang dapat dilakukan oleh pengguna IAM atau IAM Identity Center AWS CloudShell, Anda dapat membuat kebijakan kustom yang menggunakan kebijakan `AWSCloudShellFullAccess` terkelola sebagai templat. Untuk informasi selengkapnya tentang membatasi tindakan yang tersedia bagi pengguna CloudShell, lihat Mengelola AWS CloudShell akses dan penggunaan dengan kebijakan IAM di PanduanAWS CloudShell Pengguna.

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

Berinteraksi dengan menggunakan AWS Control TowerAWS CloudShell

Setelah Anda meluncurkan AWS CloudShell dari AWS Management Console, 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 kredensi sebelum melakukan panggilan.

Peluncuran AWS CloudShell

- Dari AWS Management Console, Anda dapat meluncurkan CloudShell dengan memilih opsi berikut yang tersedia di bilah navigasi:
  - Pilih CloudShell ikon.
  - Mulai mengetik “cloudshell” di kotak Pencarian dan kemudian pilih opsi. CloudShell

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

Menggunakan AWS CloudShell untuk membantu mengatur AWS Control Tower

Sebelum melakukan prosedur ini, kecuali dinyatakan lain, Anda harus masuk ke Wilayah asal untuk landing zone Anda, dan Anda harus masuk sebagai pengguna IAM Identity Center atau pengguna IAM dengan izin administratif untuk akun manajemen yang berisi landing zone Anda. AWS Management Console

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

   Periksa AWS Config status 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"`
2. Jika Anda memiliki AWS Config perekam atau saluran pengiriman yang perlu Anda hapus sebelum mengatur AWS Control Tower landing zone, berikut adalah beberapa perintah yang dapat Anda masukkan:

   Kelola sumber daya Anda 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 selengkapnya, lihat dokumentasi AWS Config

- 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 tepercaya. AWS OrganizationsUntuk 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 mengotomatisasi atau menyesuaikan tindakan. AWS Control Tower

   Mengaktifkan atau menonaktifkan akses layanan tepercaya

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

Buat bucket Amazon S3 dengan AWS CloudShell

Dalam contoh berikut, Anda dapat menggunakan AWS CloudShell untuk membuat bucket Amazon S3 dan kemudian menggunakan PutObjectmetode untuk menambahkan file kode sebagai objek di bucket tersebut.

1. Untuk membuat bucket di AWS Region tertentu, masukkan perintah berikut di baris CloudShell 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 penamaan ember (hanya menggunakan huruf kecil, misalnya), kesalahan berikut akan 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\""}
```

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

Menciptakan 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. AWS CloudFormation menyediakan dan mengonfigurasi sumber daya tersebut untuk Anda.

Ketika Anda menggunakan AWS 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 dan AWS CloudFormation template

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

AWS Control Tower mendukung pembuatan `AWS::ControlTower::EnabledControl` (sumber daya kontrol), `AWS::ControlTower::LandingZone` (zona pendaratan), dan `AWS::ControlTower::EnabledBaseline` (garis dasar) di. AWS CloudFormation Untuk informasi selengkapnya, termasuk contoh template JSON dan YAMAL untuk jenis sumber daya ini, lihat AWS Control Towerdi AWS CloudFormation Panduan Pengguna.

> **Note**
>
> Batas `EnableControl` dan `DisableControl` pembaruan AWS Control Tower adalah 100 operasi bersamaan dengan hingga 20 operasi yang berkaitan dengan kontrol Proaktif.

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

Pelajari lebih lanjut tentang AWS CloudFormation

Untuk mempelajari selengkapnya AWS CloudFormation, lihat sumber daya berikut:

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

Sesuaikan landing zone AWS Control Tower

Aspek tertentu dari zona landing zone 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 yang lebih luas dari landing zone Anda dengan kemampuan Kustomisasi untuk AWS Control Tower, kerangka kerja kustomisasi GitOps bergaya yang berfungsi dengan template dan peristiwa siklus hidup AWS AWS CloudFormation Control Tower.

Kustomisasi dari konsol AWS Control Tower

Untuk membuat penyesuaian ini ke landing zone 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 pengaturan. 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 di 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 landing zone dengan memilih AWS Wilayah tertentu untuk tata kelola. Ikuti langkah-langkah di konsol AWS Control Tower.

- Anda dapat memilih dan membatalkan pilihan AWS Wilayah untuk tata kelola saat memperbarui landing zone.
- Anda dapat mengatur kontrol Tolak Wilayah ke Diaktifkan 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, lihat. Keterbatasan kontrol

Sesuaikan dengan menambahkan kontrol opsional

- Sangat direkomendasikan dan kontrol elektif bersifat opsional, yang berarti Anda dapat menyesuaikan tingkat penegakan untuk landing zone 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 Security Hub terintegrasi memungkinkan Anda memindai lingkungan AWS Control Tower untuk memeriksa risiko keamanan.
- Kontrol proaktif opsional memungkinkan Anda untuk memeriksa AWS CloudFormation sumber daya Anda sebelum disediakan, untuk memastikan sumber daya baru akan sesuai dengan tujuan kontrol lingkungan Anda.

Sesuaikan AWS CloudTrail jalur Anda

- Saat memperbarui landing zone 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 Anda memperbarui landing zone 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 Kustomisasi akun dengan Kustomisasi Account Factory (AFC).

Mengotomatiskan penyesuaian di luar konsol AWS Control Tower

Beberapa penyesuaian tidak tersedia melalui konsol AWS Control Tower, tetapi dapat diterapkan dengan cara lain. Sebagai contoh:

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

  AFT digunakan dengan modul Terraform, tersedia di repositori AFT.
- Anda dapat menyesuaikan landing zone AWS Control Tower dengan Kustomisasi untuk AWS Control Tower (CFCT), paket fungsionalitas yang dibangun berdasarkan AWS CloudFormation templat dan kebijakan kontrol layanan (SCP). Anda dapat menerapkan templat dan kebijakan khusus ke akun individual dan unit organisasi (OU) dalam organisasi Anda.

  Kode sumber untuk CFCT tersedia di GitHub repositori.

Manfaat Kustomisasi untuk AWS Control Tower (CFCT)

Paket fungsionalitas yang kami sebut sebagai Kustomisasi untuk AWS Control Tower (CFCT) membantu Anda membuat penyesuaian yang lebih luas untuk landing zone Anda daripada yang dapat Anda buat di konsol AWS Control Tower. Ini menawarkan GitOps -style, proses otomatis. Anda dapat membentuk kembali landing zone Anda untuk memenuhi kebutuhan bisnis Anda.

Proses infrastructure-as-codepenyesuaian ini mengintegrasikan AWS CloudFormation template dengan kebijakan kontrol AWS layanan (SCP) dan peristiwa siklus hidup AWS Control Tower, sehingga penerapan sumber daya Anda tetap disinkronkan dengan landing zone 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 landing zone Anda dengan menerapkan sumber daya yang Anda tentukan.

Manfaat

- Memperluas lingkungan yang disesuaikan dan aman — Anda dapat memperluas AWS lingkungan AWS Control Tower multi-akun dengan lebih cepat, dan menggabungkan praktik AWS terbaik ke dalam alur kerja penyesuaian yang dapat diulang.
- Buat instantiasi persyaratan Anda — Anda dapat menyesuaikan landing zone AWS Control Tower untuk kebutuhan bisnis Anda, dengan AWS CloudFormation templat dan kebijakan kontrol layanan yang menyatakan maksud kebijakan Anda.
- Otomatiskan lebih lanjut dengan peristiwa siklus hidup AWS Control Tower — Peristiwa Siklus Hidup memungkinkan Anda menerapkan sumber daya berdasarkan penyelesaian rangkaian peristiwa sebelumnya. Anda dapat mengandalkan peristiwa siklus hidup untuk membantu Anda menyebarkan sumber daya ke akun dan OU, secara otomatis.
- Memperluas 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 Customizations for AWS Control Tower (CFCT) diberikan dalam posting blog AWS Architecture, Menyebarkan DNS konsisten dengan Service Catalog dan AWS Control Tower kustomisasi.
- 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 Arsitektur Referensi AWS 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 dan kebijakan kontrol layanan (SCP).

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 akan digunakan secara otomatis. Anda dapat menerapkan templat dan kebijakan khusus ke akun individual dan unit organisasi (OU) dalam organisasi Anda.

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

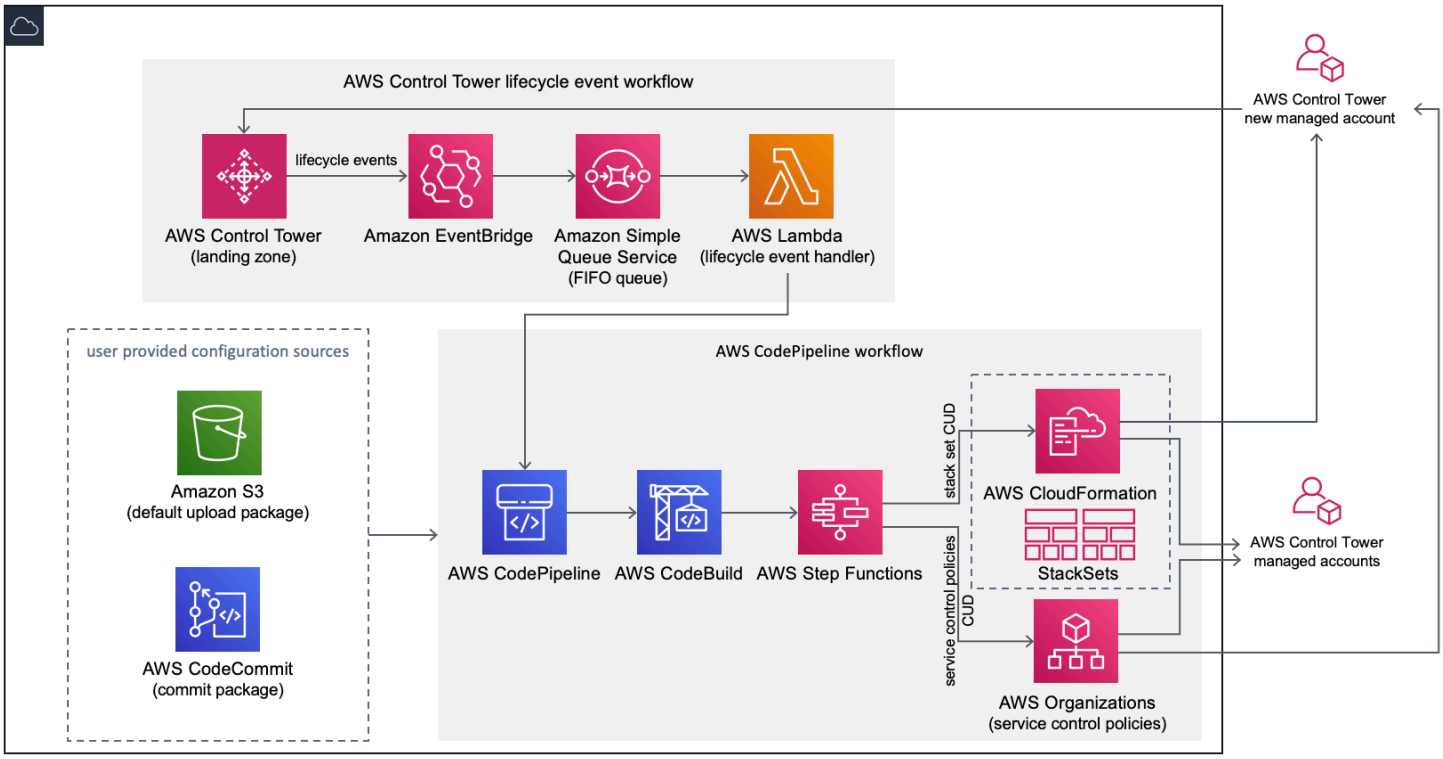
Bagian berikut memberikan pertimbangan arsitektur dan langkah-langkah konfigurasi untuk menerapkan Kustomisasi untuk AWS Control Tower (CFCT). Ini mencakup tautan ke AWS CloudFormationtemplate yang meluncurkan, mengonfigurasi, dan menjalankan AWS layanan yang diperlukan, selaras dengan praktik AWS terbaik 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 dan perubahan terbaru pada Kustomisasi untuk AWS Control Tower (CFCT), lihat file ChangeLog.md di repositori. GitHub

Gambaran umum arsitektur

Menerapkan CFCT membangun lingkungan berikut di Cloud. AWS



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 pengunggahan secara otomatis memanggil mesin status kebijakan kontrol layanan (SCP) dan mesin AWS CloudFormation StackSetsstatus untuk menerapkan SCP di tingkat OU, atau untuk menerapkan instance tumpukan di tingkat OU atau akun.

> **Catatan**
>
> Secara default, CFCT membuat bucket Amazon S3 untuk menyimpan sumber pipeline, tetapi Anda dapat mengubah lokasi ke AWS CodeCommitrepositori. 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 mengkonfigurasi AWS CodePipeline, AWS CodeBuildmemproyeksikan, dan AWS Step Functionsyang mengatur pengelolaan AWS CloudFormation StackSets dan SCP di organisasi Anda.

Saat Anda mengunggah paket konfigurasi, CFCT memanggil pipeline kode untuk menjalankan tiga 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.
- AWS CloudFormation Stage — memanggil mesin status set stack untuk menerapkan 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 dan SCP step, yang menyebarkan set tumpukan kustom dan SCP 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 dan SCP.

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 Amazon Simple Storage Service (Amazon S3) dan sumber daya repositori berbasis CodeCommit AWS Git dipertahankan 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 harga Amazon S3 dan CodeCommitAWS untuk detailnya.

Layanan komponen

AWS Layanan berikut adalah komponen Kustomisasi untuk AWS Control Tower (CFCT).

AWS CodeCommit

Berdasarkan masukan Anda ke AWS CloudFormation template, CFCT dapat membuat AWS CodeCommitrepositori dengan konfigurasi sampel yang sama yang dijelaskan di bagian Amazon Simple Storage Service.

Untuk mengkloning AWS CodeCommit repositori CFCT ke komputer lokal Anda, Anda harus membuat kredensi yang memberi Anda akses sementara ke repositori, seperti yang dijelaskan dalam Panduan Pengguna.AWS CodeCommit Untuk informasi tentang kompatibilitas versi, lihat Menyiapkan untuk AWS CodeCommit.

AWS CodePipeline

AWS CodePipeline memvalidasi, menguji, dan mengimplementasikan perubahan berdasarkan pembaruan pada paket konfigurasi, yang akan Anda buat di bucket Amazon S3 default atau repositori. AWS CodeCommit Untuk informasi selengkapnya tentang mengubah kontrol sumber konfigurasi AWS CodeCommit, lihat Menggunakan Amazon S3 sebagai Sumber Konfigurasi. Pipeline mencakup tahapan untuk memvalidasi dan mengelola file dan templat konfigurasi, 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 Systems AWS Manager Parameter Store. 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 kebijakan. `CustomControlTowerKMSKey` Rotasi tombol otomatis diaktifkan secara default.

AWS Lambda

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

Amazon Simple Notification Service

CFCT dapat mempublikasikan notifikasi, 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 saluran pipa.

Amazon Simple Storage Service

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

Contoh: Nama ember Amazon S3

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

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

Perhatikan garis bawah utama dalam nama file.

File zip ini menyediakan contoh manifes dan contoh template terkait yang menjelaskan struktur folder yang diperlukan. Contoh-contoh ini membantu Anda mengembangkan paket konfigurasi untuk menyesuaikan landing zone 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 antrean 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 selengkapnya tentang SCP, lihat AWS Organizations.

AWS Step Functions

CFCT membuat Step Functions untuk mengatur penerapan kustomisasi. Step Functions ini menerjemahkan file konfigurasi untuk menyebarkan kustomisasi sesuai kebutuhan di seluruh lingkungan.

AWS Systems Manager Parameter Store

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, Systems 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 AWS 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.

> **Catatan**
>
> 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

Anda dapat mengubah lokasi penyimpanan paket konfigurasi dari bucket S3 ke repositori AWS CodeCommit Git dengan memilih `AWS CodeCommit` opsi dalam parameter. AWS CloudFormation Opsi ini memungkinkan Anda untuk mengelola kontrol versi dengan mudah.

> **Catatan**
>
> Saat Anda menggunakan bucket S3 default, pastikan paket konfigurasi tersedia sebagai `.zip` file. Saat Anda menggunakan AWS CodeCommit repositori, pastikan bahwa paket konfigurasi ditempatkan 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.

> **Catatan**
>
> Saat Anda menggunakan AWS CodeCommit untuk menyimpan paket konfigurasi, paket tidak perlu zip. Untuk informasi tentang membuat dan menyimpan paket konfigurasi AWS CodeCommit, lihatPanduan kustomisasi CFCT.

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 AWS 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 GitHub repositori 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 AWS CloudFormation template ke akun manajemen Anda.
- Tinjau parameter template, dan sesuaikan jika perlu.

Langkah 2. Buat paket khusus

- 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

AWS 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 template dari GitHub dan kemudian luncurkan dari. 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 persetuju an manual. Untuk informasi selengkapnya, lihat the

Konfigurasi Pipa		
Parameter	Default	Deskripsi
		section called “Panduan kustomisasi CFCT”.
Alamat Email Persetujuan Pipa	<Optional Input>	Alamat email untuk pemberitahuan persetujuan. Untuk menggunakan parameter ini, Anda harus mengatur parameter Pipeline Approval Stage keYes.
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 memilihYes, Anda harus mengatur parameter CodePipeline Sumber keAWS CodeCommit .

CodeCommit Pengaturan AWS		
Parameter	Default	Deskripsi
CodeCommit Nama Repositori	`custom-control-tower-configuration`	Nama repositori Git. Untuk menggunakan parameter ini, Anda harus menyetel parameter AWS CodePipeline Source ke`AWS CodeCommit` . Nama ini digunakan untuk membuat repositori Git baru, dan harus unik. Jika Anda memberikan nama repositori Git yang ada, Anda harus mengatur Repositori yang Ada? CodeCommit parameter ke Ya dan masukkan nama yang tepat dari repositori itu.
CodeCommit Nama Cabang	`main`	Cabang Git tempat paket kustomisasi disimpan. Repositori Git dapat memiliki banyak cabang. Ini adalah nama default yang diberikan ke cabang di repositori Git. Untuk menggunakan parameter ini, Anda harus mengatur parameter CodePipeline Sumber ke`AWS CodeCommit` .

CloudFormation StackSets Konfigurasi AWS		
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.
Persentase Toleransi Kegagalan	`10`	Persentase akun, per Wilayah, yang operasi tumpukan ini dapat gagal sebelum AWS CloudForm ation menghentikan operasi di Wilayah tersebut. Nilai minimum yang diizinkan adalah 0 dan nilai maksimum yang diizinkan adalah 100. Untuk informasi selengkap nya, 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 AWS CloudFormation konsol di kolom Status. Anda akan melihat status CREATE_COMPLETE dalam waktu sekitar 15 menit.

Langkah 2. Buat paket khusus

Dengan tumpukan yang diluncurkan, Anda dapat menambahkan penyesuaian ke zona landing zone AWS Control Tower dan kebijakan kontrol layanan (SCP) AWS Control Tower 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 konsolAWS 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 GitGub 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 seperlunya. 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 bawaan, 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 akan 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 terkaitCustomControlTower-, dan yang tidak dideklarasikan dalam file manifesKey: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 konsolAWS 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`

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 KebijakanAWS 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 AWS Control Tower (CFCT) adalah untuk administrator, DevOps profesional, vendor perangkat lunak independen, arsitek infrastruktur TI, dan integrator sistem yang ingin menyesuaikan dan memperluas lingkungan AWS Control Tower mereka untuk perusahaan dan pelanggan mereka. Ini memberikan informasi tentang menyesuaikan dan memperluas lingkungan AWS Control Tower dengan paket kustomisasi CFCT.

> **Note**
>
> Untuk menyebarkan 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-item ini:

- File manifes
- Satu set template yang menyertainya
- File JSON lainnya untuk mendeskripsikan 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, tetapi Anda dapat mengubah lokasi sumber ke AWS CodeCommit repositori. Untuk informasi selengkapnya, lihat Mengedit pipeline CodePipeline di Panduan AWS CodePipeline Pengguna.

File manifes adalah file teks yang menjelaskan AWS sumber daya yang dapat Anda gunakan untuk menyesuaikan landing zone Anda. CodePipeline melakukan tugas-tugas ini:

- mengekstrak file manifes, kumpulan templat yang menyertainya, dan file JSON lainnya
- melakukan validasi manifes dan template
- memanggil bagian dalam file manifes 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

> **Note**
>
> Nama file paket konfigurasi sampel dimulai dengan garis bawah (_) sehingga tidak dipicu secara AWS CodePipeline otomatis. Ketika Anda telah menyelesaikan kustomisasi 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 tahapan 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 di-host.

2. Membangun panggung

Tahap build membutuhkan AWS CodeBuild untuk memvalidasi konten paket konfigurasi. Pemeriksaan ini termasuk menguji sintaks dan skema `manifest.yaml` file, bersama dengan semua AWS CloudFormation templat yang disertakan dalam paket atau dihosting dari jarak jauh, menggunakan dan. AWS CloudFormation `validate-template` `cfn_nag` Jika file manifes dan AWS CloudFormation template 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 pipa konfigurasi. Ini menghentikan sementara pipa selama penyebaran, 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 untuk memanggil AWS Organizations API yang membuat kebijakan kontrol layanan (SCP).

5. Tahap CloudFormation sumber daya AWS

   Tahap AWS CloudFormation 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 AWS CloudFormation sumber daya dalam urutan yang ditentukan dalam file manifes, kecuali ketergantungan sumber daya ditentukan.

Tentukan konfigurasi kustom

Anda akan menentukan konfigurasi AWS Control Tower kustom Anda dengan file manifes, 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 pada 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 ke bucket Amazon S3 yang ditentukan.

> **Note**
>
> Jika Anda menggunakan AWS CodeCommit, letakkan file di repositori tanpa zip file.

File manifes

`manifest.yaml`File ini adalah file teks yang menjelaskan AWS sumber daya Anda. Contoh berikut menunjukkan struktur file manifes.

```
---
region: String
version: 2021-03-15

resources:
  #set of CloudFormation resources or SCP 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 AWS Control Tower. Nilai ini harus berupa nama AWS Wilayah yang valid (sepertius`-east-1`,`eu-west-1`, atau`ap-southeast-1`). Wilayah beranda AWS Control Tower adalah default saat Anda membuat sumber daya AWS Control Tower khusus (seperti AWS CloudFormation StackSets), kecuali Wilayah yang lebih spesifik sumber daya ditentukan.

```
region:your-home-region
```

versi - 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 manifes.

Kata kunci berikutnya yang ditunjukkan pada contoh sebelumnya adalah kata kunci sumber daya. Bagian sumber daya dari file manifes sangat terstruktur. Ini berisi daftar rinci sumber AWS daya, yang akan digunakan secara otomatis oleh pipa CFCT. Deskripsi sumber daya dan parameter yang tersedia diberikan di bagian selanjutnya.

Bagian sumber daya dari file manifes

Topik ini menjelaskan bagian sumber daya dari file manifes, tempat Anda akan menentukan sumber daya yang diperlukan untuk penyesuaian Anda. Bagian file manifes ini dimulai pada sumber kata kunci dan berlanjut ke akhir file.

Bagian sumber daya dari file manifes menentukan AWS CloudFormation StackSets atau AWS Organizations SCP, yang diterapkan CFCT secara otomatis melalui pipeline kode. Anda dapat mencantumkan OU, akun, dan Wilayah untuk menerapkan instance tumpukan.

Instans tumpukan digunakan di tingkat akun, bukan level OU. SCP dikerahkan di tingkat OU. Untuk informasi selengkapnya, lihat Membangun kustomisasi Anda sendiri.

Contoh template 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
    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 rinci untuk kata kunci yang ditunjukkan pada contoh kode sebelumnya.

Nama — Nama yang dikaitkan dengan AWS 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 garis bawah (_). Karakter lain secara otomatis diganti dengan garis bawah (_).

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 AWS CloudFormation templat atau kebijakan kontrol AWS Organizations layanan di JSON untuk membuat sumber daya atau SCP. AWS CloudFormation

- 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://bucket-name/[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 menggunakan CFCT. Untuk contoh lainnya, lihat contoh kebijakan Bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

parameter - Menentukan nama dan nilai untuk AWS CloudFormation parameter.

- Jenis: MapList
- Wajib: Tidak

Bagian parameter berisi pasangan parameter kunci/nilai. 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 parameter properti)
  - Nilai yang Valid: a-z, A-Z, dan 0-9
- parameter_value — Nilai masukan yang terkait dengan parameter.
  - Tipe: String
  - Diperlukan: Ya (di bawah parameter properti)

deploy_method — Metode penyebaran untuk menyebarkan sumber daya ke akun. Saat ini, deploy_method mendukung penerapan sumber daya menggunakan `stack_set` opsi untuk penyebaran sumber daya melalui AWS CloudFormation StackSets, atau `scp` opsi jika Anda menerapkan SCP.

- Tipe: String
- Nilai yang Valid: `stack_set` | `scp`
- Wajib: Ya

deployment_targets — Daftar akun atau Unit Organisasi (OU), di mana CFCT akan menyebarkan AWS CloudFormation sumber daya, ditentukan sebagai akun atau organisasi_unit.

> **Note**
>
> Jika Anda ingin menerapkan SCP, targetnya harus OU, bukan akun.

- Jenis: Daftar string `account name` atau `account number` untuk menunjukkan bahwa sumber daya ini akan digunakan ke dalam daftar akun yang diberikan, atau `OU names` untuk menunjukkan bahwa sumber daya ini akan digunakan ke dalam daftar OU yang diberikan.
- Wajib: Setidaknya satu akun atau organizational_units
  - akun:

    Jenis: Daftar string `account name` atau `account number` untuk menunjukkan bahwa sumber daya ini akan digunakan ke dalam daftar akun yang diberikan.
  - organisasi_unit:

    Jenis: Daftar string `OU names` untuk menunjukkan bahwa sumber daya ini akan digunakan ke dalam daftar OU yang diberikan. Jika Anda memberikan OU yang tidak berisi akun dan properti akun tidak ditambahkan, CFCT hanya membuat kumpulan tumpukan.

    > **Note**
    >
    > ID akun manajemen organisasi bukanlah nilai yang diizinkan. CFCT tidak mendukung penerapan instance tumpukan ke dalam akun manajemen organisasi.

export_outputs - Daftar pasangan nama/nilai 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 di mana *`CfnOutput-logical-ID`* sesuai dengan variabel output template. Untuk informasi selengkapnya tentang bagian Output dalam AWS CloudFormation templat, lihat Output di AWS CloudFormation Panduan 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_outputs mungkin berisi nilai selain. `output` Misalnya, jika namanya/`org/environment-name`, nilainya mungkin`production`.

wilayah — Daftar Wilayah di mana CFCT akan menyebarkan instance AWS CloudFormation tumpukan.

- Jenis: Setiap daftar nama Wilayah AWS komersial, untuk menunjukkan bahwa sumber daya ini akan disebarkan ke dalam daftar Wilayah yang diberikan. Jika kata kunci ini tidak ada dalam file manifes, sumber daya akan digunakan di Wilayah beranda saja.
- Wajib: Tidak

Akar OU

CFCT mendukung Root sebagai nilai untuk unit organisasil (OU) `organizational_units` di bawah versi manifes V2 (2021-03-15).

- Jika Anda memilih metode penerapan`scp`, saat Anda menambahkan Root di bawah`organizational_units`, AWS Control Tower menerapkan kebijakan ke semua OU di bawah Root. Jika Anda memilih metode penerapan`stack_set`, saat Anda menambahkan Root di bawah`organizational_units`, CFCT menerapkan kumpulan tumpukan di semua akun di bawah Root yang terdaftar di AWS Control Tower, kecuali untuk akun manajemen.
- Sesuai dengan 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, penerapan AWS Control Tower menempatkan akun manajemen di bawah Root OU, sehingga memiliki akses penuh dan tidak menjalankan sumber

daya tambahan. Untuk alasan ini, AWSControlTowerExecutionperan tersebut tidak dikerahkan ke akun manajemen.

- Kami menyarankan Anda mengikuti praktik terbaik ini untuk akun manajemen. Jika Anda memiliki kasus penggunaan khusus yang mengharuskan Anda menerapkan stackset di akun manajemen, sertakan akun sebagai target penerapan dan tentukan akun pengelolaannya. Jika tidak, jangan sertakan akun sebagai target penyebaran. Anda harus membuat sumber daya yang hilang, termasuk peran IAM yang diperlukan, di akun manajemen.

Untuk menyebarkan stackset di akun manajemen, sertakan `accounts` sebagai target penyebaran dan tentukan akun manajemen. Jika tidak, jangan sertakan akun sebagai target penyebaran.

```
---
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).

Jalur lengkap (tidak termasuk Root) untuk OU bersarang diperlukan, menggunakan titik dua sebagai pemisah antara OU. Untuk metode penerapan`scp`, AWS Control Tower menerapkan SCP ke OU terakhir di jalur OU bersarang. Untuk metode penerapan`stack_set`, AWS Control Tower menerapkan set tumpukan ke semua akun di bawah OU terakhir di jalur OU bersarang.

Misalnya, perhatikan jalannya`OUName1:OUName2:OUName3`. OU terakhir di jalan adalah`OUName3`. CFCT menyebarkan SCP ke `OUName3` dan menumpuk set ke semua akun langsung di bawah`OUName3`, hanya.

```
---
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).

Bangun kustomisasi Anda sendiri

Untuk membuat kustomisasi Anda sendiri, Anda dapat memodifikasi `manifest.yaml` file dengan menambahkan atau memperbarui kebijakan kontrol layanan (SCP) dan sumber daya. AWS CloudFormation Untuk sumber daya yang harus digunakan, Anda dapat menambah atau menghapus akun dan OU. Anda dapat menambahkan atau memodifikasi templat di folder paket, membuat folder Anda sendiri, dan mereferensikan templat 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

Mengatur paket konfigurasi untuk kebijakan kontrol layanan

Bagian ini menjelaskan cara membuat paket konfigurasi untuk kebijakan kontrol layanan (SCP). Dua bagian utama dari proses ini adalah (1) siapkan file manifes, dan (2) siapkan 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 `region` ditambahkan secara otomatis selama penerapan. Itu harus cocok dengan Wilayah tempat Anda menggunakan CFCT. Wilayah ini harus sama dengan wilayah AWS Control Tower.

Untuk menambahkan SCP khusus di `example-configuration` folder dalam paket zip yang disimpan di bucket Amazon S3, buka file dan `example-manifest.yaml` mulai 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
    #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
    #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 pasangan kunci/nilai.

Anda harus menyertakan kebijakan SCP dalam format JSON untuk mendukung manifes, karena file manifes mereferensikan file JSON. Pastikan bahwa jalur file cocok dengan informasi jalur yang disediakan dalam file manifes.

- File JSON kebijakan berisi SCP 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.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"GuardPutAccountPublicAccessBlock",
         "Effect":"Deny",
         "Action":"s3:PutAccountPublicAccessBlock",
         "Resource":"arn:aws:s3:::*"
```

```
      }
   ]
}
```

Siapkan paket konfigurasi untuk AWS CloudFormation StackSets

Bagian ini menjelaskan cara menyiapkan paket konfigurasi untuk AWS CloudFormation StackSets. Dua bagian utama dari proses ini adalah: (1) siapkan file manifes, dan (2) perbarui struktur folder.

Langkah 1: Edit file manifes yang ada

Tambahkan AWS 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. 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
    #Apply to the following OU(s)
    deployment_targets:
    organizational_units: #array of strings
    - OUName1
    - OUName2
```

Cuplikan berikut menunjukkan contoh file manifes yang diedit yang berisi rincian. `resources` 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 AWS 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
    #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 AWS CloudFormation template pendukung dan file kebijakan SCP yang ada di 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 di Langkah 1.

```
- manifest.yaml
```

```
- policies/
   - block-s3-public.json
- templates/
   - transit-gateway.template
```

Pembantu 'alfred' dan file parameter AWS CloudFormation

CFCT memberi Anda mekanisme yang dikenal sebagai alfred helper untuk mendapatkan nilai kunci Penyimpanan Parameter SSM yang ditentukan dalam template. AWS CloudFormation Menggunakan alfred helper, Anda dapat menggunakan nilai yang disimpan di SSM Parameter Store dan tanpa memperbarui template. AWS CloudFormation Untuk informasi selengkapnya, lihat Apa itu AWS CloudFormation template? dalam AWS CloudFormation User Guide.

> **Important**
>
> Pembantu 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 helper 'alfred' memulihkan parameter, ia memilih instance tumpukan acak dari kumpulan tumpukan yang mengekspor variabel.

Contoh

Misalkan Anda memiliki dua set AWS CloudFormation tumpukan. Stack set 1 memiliki satu instance tumpukan dan menyebarkan ke satu akun dalam satu Wilayah. Ini menciptakan VPC Amazon 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 stack set 2, `VPC ID` dan `subnet ID` harus disimpan dalam stack set 1 menggunakan`AWS:::SSM::Parameter`. Untuk informasi selengkapnya, lihat `AWS:::SSM::Parameter` di AWS CloudFormation Panduan Pengguna.

AWS CloudFormation tumpukan set 1:

Dalam cuplikan berikut, alfred helper bisa mendapatkan nilai untuk `VPC ID` dan `subnet ID` dari penyimpanan parameter dan meneruskannya sebagai input ke mesin status. StackSet

```
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
```

AWS CloudFormation tumpukan set 2:

Cuplikan menunjukkan parameter yang ditentukan dalam file AWS CloudFormation stack 2`manifest.yaml`.

```
parameters:
      - parameter_key: VpcId
        parameter_value: $[alfred_ssm_/stack_1/vpc/id]
      - parameter_key: SubnetId
        parameter_value: $[alfred_ssm_/stack_1/subnet/id]
```

AWS CloudFormation tumpukan set 2.1:

Cuplikan menunjukkan bahwa Anda dapat mencantumkan `alfred_ssm` properti untuk mendukung parameter tipe. CommaDelimitedList Untuk informasi selengkapnya, lihat `Parameters` di AWS 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 terbantu untuk mengurangi kesalahan ketika Anda membuat `manifest.yaml` file Anda sendiri.

Peningkatan versi manifes

Untuk informasi tentang versi terbaru Kustomisasi untuk AWS Control Tower (CFCT), lihat file ChangeLog.md di repositori. GitHub

Warning

Versi 2.2.0 Kustomisasi untuk AWS Control Tower (CFCT) memperkenalkan skema manifes (versi 2021-03-15) agar selaras dengan API layanan terkait. AWS Skema manifes memungkinkan satu file manifest.yaml untuk mengelola sumber daya yang didukung (AWS CloudFormation template dan SCP) melalui alur kerja terpisah. DevOps
Kami sangat menyarankan Anda memperbarui skema manifes 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 file. `manifest.yaml` Tidak diperlukan perubahan pada konfigurasi Anda yang ada. Namun, versi 2020-01-01 ada di End of Support. Kami tidak lagi menyediakan pembaruan atau menambahkan penyempurnaan ke versi 2020-01-01. Fitur Root OU dan OU bersarang tidak didukung dalam versi 2020-01-01.

Properti usang dalam versi manifes 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 pemutakhiran wajib

Saat Anda memutakhirkan ke versi skema manifes 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 Organizations

1. Pindahkan SCP 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 baru deployment_targets. Daftar OU harus didefinisikan di bawah sub-properti organizational_units. Sub-properti akun tidak didukung untuk kebijakan organisasi.
4. Tambahkan properti baru deploy_method dengan nilai scp.

AWS 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_targets. Daftar OU harus didefinisikan di bawah sub-properti organizational_units.
4. Ubah deploy_to_accounts ke deployment_targets properti baru. Daftar akun harus didefinisikan di bawah akun sub-properti.
5. Ubah properti ssm_parameters ke properti baru export_outputs.

Langkah-langkah peningkatan yang sangat disarankan

AWS CloudFormation parameter

1. Ubah properti parameter_file ke parameter properti baru.
2. Hapus path file dalam nilai properti parameter_file.
3. Salin kunci parameter dan nilai parameter dari file JSON parameter yang ada ke dalam format baru untuk properti parameter. Ini akan membantu Anda mengelolanya dalam file manifes.

> **Note**
>
> Properti parameter_file didukung dalam manifes versi 2021-03-15.

Jaringan di AWS Control Tower

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 Membangun Infrastruktur Jaringan AWS Multi-VPC yang Dapat Diskalakan dan Aman.

Topik terkait

- Untuk informasi tentang cara kerja AWS Control Tower saat Anda mendaftarkan akun yang memiliki VPC yang sudah ada, lihat. Mendaftarkan 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 AWS Control Tower Tanpa VPC
- Untuk informasi tentang cara mengubah setelan akun untuk VPC, lihat dokumentasi Account Factory 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 AWS VPC 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.

Region deny control memblokir panggilan API ke sebagian besar layanan yang tidak diatur Wilayah AWS. Untuk informasi selengkapnya, lihat Tolak akses AWS 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.
- Saat AWS Control Tower menyiapkan akun baru di AWS Wilayah yang didukung, AWS Control Tower secara otomatis menghapus AWS VPC default, dan menyiapkan VPC baru yang dikonfigurasi oleh AWS 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 AS Barat (California Utara) 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 secara 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 pengintipan VPC-ke-VPC 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.

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 di 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-AWSControlTowerExecutionRole untuk membuat peran di semua akun di OU tersebut.

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, lihatTambahkan peran IAM yang diperlukan secara manual ke yang sudah ada Akun AWS dan daftarkan.

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

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 membantu mencegah penyerang 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, kami sangat menyarankan untuk 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.

```
{
  "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.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "012345678901"
        },
        "StringLike": {
          "aws:SourceArn": "arn:aws:controltower:us-west-2:012345678901:*"
        }
```

```
      }
    }
  ]
}
```

Contoh ini menggambarkan pernyataan `aws:SourceArn` kondisi, dengan pernyataan `aws:SourceAccount` kondisi tambahan. Untuk informasi selengkapnya, lihat Mencegah peniruan identitas 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 menggabungkan AWS Config aturan dalam 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`.

Berikut adalah kebijakan IAM (artefak JSON) yang melekat pada peran:

```
{
    "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

```
{
  "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "config:PutConfigurationAggregator",
          "config:DeleteConfigurationAggregator",
          "iam:PassRole"
          ],
        "Resource": [
          "arn:aws:iam:::role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations",
          "arn:aws:config:::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.

Kumpulan tumpukan AWS Control Tower `StackSet-AWSControlTowerBP-BASELINE-ROLES` membuat peran lintas akun khusus program ini di akun audit:

- aws-menara pengendali- AdministratorExecutionRole
- aws-menara pengendali- AuditAdministratorRole
- aws-menara pengendali- ReadOnlyExecutionRole
- 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 sebaris — Dibuat oleh AWS Control Tower, artefak mengikuti.

```
{
  "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 sebaris — Dibuat oleh AWS Control Tower, artefak mengikuti.

```
{
  "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-AuditAdministratorRole`:

```
{
  "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:GetPeregrineStatus",
                "sso:GetApplicationInstance",
                "sso:ListDirectoryAssociations",
                "sso:ListPermissionSets",
                "sso:GetPermissionSet",
                "sso:ProvisionApplicationInstanceForAWSAccount",
                "sso:ProvisionApplicationProfileForAWSAccountInstance",
                "sso:ProvisionSAMLProvider",
                "sso:ListProfileAssociations",
                "sso-directory:ListMembersInGroup",
                "sso-directory:AddMemberToGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchGroupsWithGroupName",
                "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": "*"
        }
    ]
}
```

Izinsso:GetPeregrineStatus,, sso:ProvisionApplicationInstanceForAWSAccountsso:ProvisionApplicationProfileForA dan sso:ProvisionSAMLProvide diwajibkan oleh AWS Control Tower Account Factory untuk berinteraksi dengan AWS IAM Identity Center.

Sumber daya di AWS Control Tower

- Untuk informasi umum tentang kepemilikan sumber daya di AWS Control Tower, lihatGambaran umum tentang mengelola izin akses ke sumber daya AWS Control Tower Anda.
- Untuk informasi tentang sumber daya yang dibuat AWS Control Tower di akun bersama, lihatTentang akun bersama.
- Untuk informasi tentang sumber daya yang dibuat AWS Control Tower saat menyediakan akun melalui Account Factory, lihatPertimbangan Sumber Daya untuk Account Factory.
- 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

Saat ini, AWS Control Tower didukung di AWS Wilayah berikut:

- AS Timur (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)
- Eropa (Milan)
- Afrika (Cape Town)
- Timur Tengah (Bahrain)
- Israel (Tel Aviv)
- Timur Tengah (UEA)
- Eropa (Spanyol)

- Asia Pasifik (Hyderabad)
- Eropa (Zürich)
- Asia Pasifik (Melbourne)
- Kanada Barat (Calgary)

Tentang Wilayah asal Anda

Saat Anda membuat landing zone, Wilayah yang Anda gunakan untuk akses ke konsol AWS Manajemen menjadi AWS Wilayah asal Anda untuk AWS Control Tower. Selama proses pembuatan, beberapa sumber daya disediakan di Wilayah asal. Sumber daya lain, seperti OU dan AWS akun, bersifat global.

Setelah Anda memilih Wilayah rumah, Anda tidak dapat mengubahnya.

Kontrol dan Wilayah

Saat ini, semua kontrol pencegahan bekerja secara global. Kontrol detektif dan proaktif, bagaimanapun, hanya berfungsi di Wilayah yang didukung AWS Control Tower. Untuk informasi selengkapnya tentang perilaku kontrol saat Anda mengaktifkan AWS Control Tower di Wilayah baru, lihatKonfigurasikan Wilayah AWS Control Tower Anda.

Konfigurasikan Wilayah AWS Control Tower Anda

Bagian ini menjelaskan perilaku yang dapat Anda harapkan saat memperluas landing zone AWS Control Tower Anda ke AWS Wilayah baru, atau menghapus Wilayah dari konfigurasi landing zone Anda. Umumnya, tindakan ini dilakukan melalui fungsi Update konsol AWS Control Tower.

> **Note**
>
> Kami menyarankan agar Anda menghindari perluasan landing zone AWS Control Tower ke AWS Wilayah 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 landing zone, yang berarti bahwa itu menjadi dasar landing zone Anda —

- untuk beroperasi secara aktif di semua Wilayah yang baru dipilih, dan
- untuk menghentikan sumber daya yang mengatur di Wilayah yang tidak dipilih.

Akun individual dalam unit organisasi (OU) Anda yang dikelola oleh AWS Control Tower tidak diperbarui sebagai bagian dari proses pembaruan landing zone ini. Oleh karena itu, Anda harus memperbarui akun Anda dengan mendaftarkan ulang OU Anda.

Saat mengonfigurasi Wilayah AWS Control Tower 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 Anda mengonfigurasi landing zone untuk Wilayah baru, kontrol detektif AWS Control Tower mematuhi aturan berikut:

- Apa yang ada tetap sama. Perilaku pagar pembatas, detektif maupun pencegahan, 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. Saat mengonfigurasi landing zone AWS Control Tower menjadi Wilayah baru (dengan memperbarui landing zone), Anda harus memperbarui akun yang ada di OU yang ada sebelum 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 landing zone AWS Control Tower untuk mengonfigurasi Wilayah baru dan kemudian memperbarui akun, kontrol detektif yang sudah diaktifkan di OU akan mulai bekerja pada akun tersebut di Wilayah yang baru dikonfigurasi.

Konfigurasikan Wilayah AWS Control Tower

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 landing zone pembaruan, karena mengatur Wilayah baru, atau menghapus Wilayah dari tata kelola, mengharuskan Anda memperbarui ke versi landing zone terbaru.

4. Di bawah AWS Wilayah Tambahan untuk tata kelola, cari Wilayah yang ingin Anda atur (atau hentikan pemerintahan). Kolom Negara menunjukkan Wilayah mana yang saat ini Anda atur, dan mana yang tidak.
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 Perbarui landing zone.
7. Ketika pengaturan landing zone selesai, Daftarkan ulang OU untuk memperbarui akun di Wilayah baru Anda. Untuk informasi selengkapnya, lihat Kapan harus memperbarui AWS Control Tower OU dan akun.

Metode alternatif untuk menyediakan atau memperbarui akun individual setelah mengonfigurasi Wilayah baru adalah dengan menggunakan kerangka API Service Catalog dan memperbarui akun dalam proses batch. AWS CLI 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 yang 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 jika 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) dengan landing zone. Namun, akun yang ada yang belum diperbarui tidak menerima postur tata kelola Wilayah yang diperbarui.

Secara umum, tata kelola campuran dapat membuat indikator status yang kontradiktif atau tidak akurat di konsol AWS Control Tower. Misalnya, selama tata kelola campuran, Wilayah keikutsertaan ditampilkan dengan status Tidak diatur, di OU terdaftar, untuk akun yang belum diperbarui.

> **Note**
>
> AWS Control Tower tidak mengizinkan kontrol diaktifkan selama status tata kelola campuran.

Perilaku kontrol selama pemerintahan 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 sudah ditampilkan oleh OU sebagai Governed, 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 keikutsertaan sementara akun apa pun di OU belum diperbarui, operasi `EnableControl` API di 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 Standar yang dikelola Layanan Security Hub: AWS Control Tower tidak dapat melaporkan kepatuhan secara akurat di Wilayah di mana terdapat ketidakcocokan antara konfigurasi landing zone dan akun yang tidak diperbarui.
- Tata kelola campuran tidak mengubah perilaku kontrol berbasis SCP (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

- Pilih Perbarui akun untuk setiap akun di OU yang menampilkan Perbarui status yang tersedia di halaman Organizations di konsol.
- Pilih Daftar Ulang OU di halaman Organizations, yang secara otomatis memperbarui semua akun di OU, untuk OU dengan kurang dari 300 akun.

Pertimbangan untuk mengaktifkan AWS Wilayah keikutsertaan

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 keikutsertaan. Sebaliknya, Wilayah yang aktif secara default, segera setelah Anda Akun AWS dibuat, disebut sebagai Wilayah komersial, atau hanya, Wilayah.

Istilah opt-in memiliki dasar historis. Setiap yang Wilayah AWS diperkenalkan setelah 20 Maret 2019 dianggap sebagai Wilayah keikutsertaan. Wilayah Keikutsertaan memiliki persyaratan keamanan yang lebih tinggi daripada Wilayah komersial, mengenai pembagian data IAM melalui akun yang aktif di Wilayah keikutsertaan. Semua data yang dikelola melalui layanan IAM dianggap sebagai data identitas, termasuk pengguna, grup, peran, kebijakan, penyedia identitas, data terkait mereka (misalnya, sertifikat penandatanganan X.509 atau kredensi khusus konteks), dan pengaturan tingkat akun lainnya, seperti kebijakan kata sandi dan alias akun.

Anda dapat mengaktifkan opt-in Regions secara otomatis selama pengaturan landing zone, dengan memilihnya. Landing zone Anda menjadi aktif di semua Wilayah yang dipilih.

Jika Anda memilih untuk memilih Wilayah keikutsertaan sebagai Wilayah beranda AWS Control Tower, aktifkan terlebih dahulu dengan mengikuti langkah-langkah di Mengaktifkan Wilayah, saat masuk ke Konsol AWS Manajemen. Untuk membawa akun Arsip Log dan Audit Anda sendiri dari Region opt-in, aktifkan Region tersebut secara manual terlebih dahulu.

Wilayah AWS keikutsertaan 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-south-1
- Wilayah Afrika (Cape Town), af-south-1
- Wilayah Timur Tengah (Bahrain), me-south-1

- Israel (Tel Aviv), il-central-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
- Wilayah Kanada Barat (Calgary), ca-west-1

AWS Control Tower memiliki beberapa kontrol yang bekerja secara berbeda di Wilayah keikutsertaan dibandingkan di Wilayah komersial. Untuk informasi selengkapnya, lihat Keterbatasan kontrol. Berikut adalah beberapa pertimbangan yang perlu diingat saat Anda menerapkan beban kerja ke Wilayah keikutsertaan.

> **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 keikutsertaan adalah tindakan berbeda yang dapat Anda pilih di AWS konsol, yang membuka Wilayah ke akun Anda, sehingga Anda dapat menerapkan sumber daya dan beban kerja di Wilayah.

Pertimbangan perilaku

- Jika Anda memilih untuk mengatur Wilayah keikutsertaan, kami menyarankan agar Anda tidak menonaktifkan (memilih keluar dari) Wilayah keikutsertaan yang diatur, 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 AWS Penagihan atau SDK. AWS
- Ketika AWS Control Tower memperluas tata kelola ke Wilayah keikutsertaan, 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 pembatalan pemilihan Wilayah, AWS Control Tower melewatkan penghapusan sumber daya dari Wilayah keikutsertaan jika Wilayah tersebut dinonaktifkan secara manual untuk akun

dari sumber di luar AWS Control Tower, seperti konsol AWS Penagihan atau SDK. AWS Kami menyarankan Anda menghapus sumber daya dari Wilayah yang telah dinonaktifkan, atau Anda mungkin menerima biaya penagihan tak terduga untuk sumber daya tersebut.

- Jika landing zone Anda dinonaktifkan, AWS Control Tower membersihkan sumber daya di semua Wilayah yang diatur, termasuk Wilayah keikutsertaan. Namun, AWS Control Tower tidak menonaktifkan Wilayah keikutsertaan. Anda dapat menonaktifkan Wilayah keikutsertaan sebagai langkah tambahan setelah dinonaktifkan.
- Jika Wilayah asal Anda adalah Region keikutsertaan, dan jika Anda ingin mendaftarkan akun yang ada sebagai akun Arsip Log dan Audit, Anda harus mengaktifkan Region opt-in secara manual sebelum dapat memilihnya sebagai Wilayah asal untuk landing zone Anda. Lihat Mengaktifkan Wilayah.
- Jika AWS Control Tower disiapkan dengan Wilayah keikutsertaan sebagai Wilayah asal Anda, dan jika Anda mengunjungi layanan AWS Control Tower dari AWS konsol di Wilayah lain mana pun, 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, keikutsertaan hanya untuk orang-orang di Wilayah AWS mana Anda akan menjalankan beban kerja, dan ikut serta dalam satu Wilayah pada satu waktu.

Batasan penting untuk tata kelola dan kontrol

- Jika saat ini Anda telah mengaktifkan kontrol AWS Control Tower yang tidak didukung di Wilayah keikutsertaan, Anda tidak akan dapat memperluas tata kelola AWS Control Tower ke Wilayah keikutsertaan tersebut hingga kontrol didukung di Wilayah tersebut. Untuk mengetahui informasi selengkapnya, lihat Keterbatasan kontrol.
- Jika Anda memperluas tata kelola AWS Control Tower ke Wilayah keikutsertaan di mana kontrol tertentu tidak didukung, Anda tidak akan dapat mengaktifkan kontrol tersebut di Wilayah mana pun hingga kontrol didukung di semua Wilayah yang Anda atur dengan AWS Control Tower Untuk informasi selengkapnya, lihat Keterbatasan kontrol
- Jika semua 22 Wilayah komersial di mana AWS Control Tower tersedia diaktifkan, termasuk Wilayah keikutsertaan, batas atas jumlah akun per unit organisasi (OU), saat memperluas tata kelola ke OU, akan dikurangi. Batasnya adalah 220, bukan 300 akun. Pengurangan ini disebabkan oleh StackSet keterbatasan. Jika Anda perlu memperluas tata kelola ke OU dengan lebih dari 220 akun, kurangi jumlah Wilayah yang diaktifkan.

Konfigurasikan wilayah tolak kontrol

AWS Control Tower menawarkan dua kontrol penolakan Wilayah. Satu kontrol,`GRREGIONDENY`, ketika diaktifkan, berlaku untuk seluruh landing zone. Kontrol lain,`CTMULTISERVICEPV1`, ketika diaktifkan, dapat diterapkan ke OU tertentu yang Anda tentukan. Untuk informasi selengkapnya, lihat Tolak akses AWS berdasarkan kontrol penolakan yang diminta Wilayah AWS dan Wilayah yang diterapkan pada OU.

Wilayah menolak kontrol, `GRREGIONDENY` unik, karena berlaku untuk landing zone 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 yang terdaftar.
- Kontrol ini tidak dapat dikonfigurasi untuk masing-masing OU.

> **Note**
>
> Sebelum Anda mengaktifkan Wilayah tolak kontrol, pastikan bahwa Anda tidak memiliki sumber daya yang ada di Wilayah ini, karena Anda tidak akan memiliki akses ke sumber daya Anda setelah Anda menerapkan kontrol. Saat kontrol diaktifkan, Anda tidak akan dapat menyebarkan sumber daya di Wilayah yang ditolak.

Kontrol penolakan Wilayah melarang akses ke AWS layanan, berdasarkan konfigurasi Wilayah AWS Control Tower Anda. Ini menolak akses ke AWS Wilayah dengan status Tidak Diatur. Wilayah menolak kontrol juga menolak akses ke Wilayah di mana AWS Control Tower tidak tersedia. Anda tidak dapat menolak akses ke Wilayah asal Anda. AWS Layanan global tertentu, seperti IAM dan AWS Organizations, dibebaskan dari Wilayah menolak kontrol. Untuk mempelajari lebih lanjut, lihat Menolak akses AWS berdasarkan permintaan Wilayah AWS.

Saat Anda mengaktifkan kontrol, itu berlaku untuk semua OU tingkat atas yang terdaftar dalam hierarki Anda, dan itu diwarisi oleh OU yang lebih rendah dalam rantai. Saat Anda menghapus kontrol, kontrol akan dihapus pada semua OU terdaftar, 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.

- Nama kontrol penuh: Tolak akses AWS berdasarkan AWS Wilayah yang diminta
- Deskripsi pagar pembatas: Melarang akses ke operasi yang tidak terdaftar di layanan global dan regional di luar Wilayah yang ditentukan.
- Ini adalah kontrol elektif dengan panduan pencegahan.

Untuk melihat template SCP kontrol penolakan Wilayah, lihat Tolak akses AWS berdasarkan permintaan Wilayah AWS dalam referensi AWS Control Tower Control. AWS Control Tower SCP mirip dengan SCP untuk AWS Organizations, tetapi tidak identik.

Anda dapat menentukan titik akhir layanan Regional pada halaman Layanan Regional.

Pertimbangan untuk Wilayah Tingkat OU menolak kontrol

Pertimbangan utama tentang kontrol penolakan Wilayah OU-level adalah untuk menentukan bagaimana ia akan berinteraksi dengan landing zone Region deny control, jika keduanya diaktifkan. Untuk informasi selengkapnya, lihat Kontrol penolakan wilayah yang diterapkan pada OU.

Menyediakan dan mengelola akun di AWS Control Tower

Bab ini mencakup ikhtisar dan prosedur untuk menyediakan dan mengelola akun anggota di zona landing zone AWS Control Tower Anda.

Ini juga mencakup ikhtisar dan prosedur untuk mendaftarkan AWS akun yang ada ke AWS Control Tower.

Untuk informasi selengkapnya tentang akun di AWS Control Tower, lihatTentang Akun AWS di AWS Control Tower. Untuk informasi tentang mendaftarkan beberapa akun ke AWS Control Tower, lihat. Daftarkan unit organisasi yang ada dengan AWS Control Tower

> **Note**
>
> Anda dapat melakukan hingga lima (5) operasi terkait akun secara bersamaan, termasuk penyediaan, pembaruan, dan pendaftaran.

Metode penyediaan

AWS Control Tower menyediakan beberapa metode untuk membuat dan memperbarui akun anggota. Beberapa metode terutama berbasis konsol, dan beberapa metode terutama otomatis.

Ikhtisar

Cara standar untuk membuat akun anggota adalah melalui Account Factory, produk berbasis konsol yang merupakan bagian dari Service Catalog. Jika landing zone Anda tidak dalam keadaan drift, Anda dapat menggunakan Create account sebagai metode untuk menambahkan akun baru dari konsol, serta Mendaftarkan akun untuk mendaftarkan akun yang ada ke AWS Control AWS Tower.

Dengan Account Factory, Anda dapat menyediakan akun dasar, dengan mengandalkan pengaturan default AWS Control Tower. Anda juga dapat menyediakan akun khusus yang memenuhi persyaratan untuk kasus penggunaan khusus.

Kustomisasi Account Factory (AFC) adalah cara menyediakan akun yang disesuaikan dari konsol AWS Control Tower, dan mengotomatiskan penyesuaian dan penerapan akun Anda. Ini memungkinkan penyediaan otomatis berbasis konsol, setelah beberapa langkah pengaturan satu kali, yang menghilangkan kebutuhan untuk menulis skrip atau mengatur saluran pipa. Untuk informasi selengkapnya, lihat Kustomisasi akun dengan Kustomisasi Account Factory (AFC).

Metode berbasis konsol:

- 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 fitur akun Daftarkan dalam AWS Control Tower, jika landing zone Anda tidak dalam keadaan drift. Lihat Daftarkan akun yang ada.
- 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 Penyediaan Akun Otomatis dengan Peran IAM.
- Terraform: Dari AWS Control Tower Account Factory for Terraform (AFT), yang mengandalkan Account Factory dan GitOps model untuk memungkinkan otomatisasi penyediaan dan pembaruan akun. Lihat Menyediakan akun dengan AWS Control Tower Account Factory untuk Terraform (AFT) .
- Kustomisasi Account Factory di konsol AWS Control Tower: Setelah 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 AWS CloudFormation templat, atau templat Terraform.

> **Note**
>
> AWS 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 asal.

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 Untuk langkah-langkah untuk mendaftarkan yang sudah ada Akun AWS menggunakan konsol AWS Control Tower, lihatDaftarkan akun yang ada.

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.

Izin yang diperlukan untuk akun

Izin yang diperlukan untuk setiap metode penyediaan dan pembaruan akun dibahas di setiap bagian, masing-masing. Dengan izin grup pengguna yang sesuai, penyedia dapat menentukan garis dasar standar dan konfigurasi jaringan untuk akun apa pun di organisasi mereka.

> **Note**
>
> Saat menyediakan akun, pemohon akun selalu harus memiliki `CreateAccount` dan izin. `DescribeCreateAccountStatus` Set izin ini adalah bagian dari peran Admin, dan diberikan secara otomatis ketika pemohon mengasumsikan peran Admin. Jika Anda mendelegasikan izin ke akun penyediaan, Anda mungkin perlu menambahkan izin ini secara langsung untuk pemohon akun.

Saat membuat akun dari konsol AWS Control Tower dengan Account Factory, Anda harus masuk ke akun dengan pengguna IAM yang `AWSServiceCatalogEndUserFullAccess` kebijakan diaktifkan, bersama dengan izin untuk menggunakan konsol AWS Control Tower, dan Anda tidak dapat masuk sebagai pengguna Root.

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 Peran dan akun.

> 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

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, termasuk sumber daya dalam bentuk templat Account Factory dan sumber daya lainnya di landing zone Anda. Sumber daya ini dapat mencakup peran IAM, AWS CloudTrail jejak, 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.

Pertimbangan untuk membawa akun keamanan atau pencatatan yang ada

Sebelum menerima akun Akun AWS keamanan atau logging, 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 mengaktifkan kemampuan penolakan, kontrol penolakan Wilayah mencegah akses ke sumber daya di Wilayah yang ditolak. Wilayah AWS

Lihat akun Anda

Halaman Organisasi mencantumkan semua OU dan akun di organisasi Anda, terlepas dari status OU atau pendaftaran di AWS Control Tower. Anda dapat melihat dan mendaftarkan akun anggota ke AWS Control Tower—secara individu atau grup OU—jika setiap akun memenuhi prasyarat untuk pendaftaran.

Untuk melihat akun tertentu di halaman Organisasi, Anda dapat memilih Akun hanya dari menu tarik-turun di kanan atas, lalu pilih nama akun Anda dari tabel. Atau, Anda dapat memilih nama OU induk dari tabel, dan Anda dapat 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 satunya:

- Tidak terdaftar — Akun ini adalah anggota OU induk, tetapi tidak sepenuhnya dikelola oleh AWS Control Tower. Jika OU induk terdaftar, akun diatur oleh kontrol pencegahan yang dikonfigurasi untuk OU induk terdaftarnya, tetapi kontrol detektif OU tidak berlaku untuk akun ini. Jika OU induk tidak terdaftar, tidak ada kontrol yang berlaku untuk akun ini.
- Mendaftar — 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.
- Terdaftar - 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 di negara bagian ini masih Terdaftar, tetapi akun harus diperbarui untuk mencerminkan perubahan terbaru yang dibuat pada lingkungan Anda. Untuk memperbarui satu akun, navigasikan ke halaman detail akun dan pilih Perbarui akun.

  Jika Anda memiliki beberapa akun dengan status ini di bawah satu OU, Anda dapat memilih untuk mendaftarkan ulang OU dan memperbarui akun tersebut bersama-sama.

Sumber daya yang dibuat di akun bersama

Bagian ini menunjukkan sumber daya yang dibuat AWS Control Tower di akun bersama, saat Anda menyiapkan landing zone.

Untuk informasi tentang sumber daya akun anggota, lihatPertimbangan Sumber Daya untuk Account Factory.

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	audit log archive
AWS Organizations	OU	Security Sandbox
AWS Organizations	Kebijakan Kontrol Layanan	aws-guardrails-*
AWS CloudFormation	Tumpukan	AWSControlTowerBP-BASELINE-CLOUDTRAIL-MASTER

AWS service	Tipe sumber daya	Nama sumber daya
		AWSControlTowerBP-BASELINE-CONFIG-MASTER(dalam versi 2.6 dan yang lebih baru)

AWS service	Tipe sumber daya	Nama sumber daya
AWS CloudFormation	StackSets	AWSControlTowerBP-BASELINE-CLOUDTRAIL(Tidak diterapkan di 3.0 dan yang lebih baru) AWSControlTowerBP_BASELINE_SERVICE_LINKED_ROLE (Deployed in 3.2 and later) AWSControlTowerBP-BASELINE-CLOUDWATCH AWSControlTowerBP-BASELINE-CONFIG AWSControlTowerBP-BASELINE-ROLES AWSControlTowerBP-BASELINE-SERVICE-ROLES AWSControlTowerBP-SECURITY-TOPICS AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED AWSControlTowerLoggingResources

AWS service	Tipe sumber daya	Nama sumber daya
		AWSControlTowerSecurityResources AWSControlTowerExecutionRole
AWS Service Catalog	Produk	AWS Control Tower Account Factory
AWS Config	Agregator	aws-controltower-ConfigAggregatorForOrganizations
AWS CloudTrail	Trail	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch Log	aws-controltower/CloudTrailLogs
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

AWS 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.

Sumber daya akun arsip log

Saat Anda mengatur landing zone, AWS sumber daya berikut akan dibuat dalam akun arsip log Anda.

AWS service	Tipe sumber daya	Nama Sumber Daya
AWS CloudFormation	Tumpukan	StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED- StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH- StackSet-AWSControlTowerBP-BASELINE-CONFIG- StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL- StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES- StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In 3.2 and later)

AWS service	Tipe sumber daya	Nama Sumber Daya
		StackSet-AWSControlTowerBP-BASELINE-ROLES- StackSet-AWSControlTowerLoggingResources-
AWS Config	Aturan AWS Config	AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIBIT
AWS CloudTrail	Jalan setapak	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 AWSControlTowerExecution
AWS Identity and Access Management	Kebijakan	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	Topik	aws-controltower-SecurityNotifications
AWS Lambda	Aplikasi	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*
AWS Lambda	Fungsi	aws-controltower-NotificationForwarder
Amazon Simple Storage Service	Bucket	aws-controltower-logs-* aws-controltower-s3-access-logs-*

Sumber daya akun audit

Saat menyiapkan landing zone, AWS sumber daya berikut akan dibuat dalam akun audit Anda.

AWS service	Tipe sumber daya	Nama sumber daya
AWS CloudFormation	Tumpukan	StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-READ-PROHIBITED- StackSet-AWSControlTowerGuardrailAWS-GR-AUDIT-BUCKET-PUBLIC-WRITE-PROHIBITED- StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH- StackSet-AWSControlTowerBP-BASELINE-CONFIG- StackSet-AWSControlTowerBP-BASELINE-CLOUDTRAIL- StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES- StackSet-AWSControlTowerBP-BASELINE-SERVICE-LINKED-ROLE-(In 3.2 and later) StackSet-AWSControlTowerBP-SECURITY-TOPICS- StackSet-AWSControlTowerBP-BASELINE-ROLES-

AWS service	Tipe sumber daya	Nama sumber daya
		StackSet-AWSControlTowerSecurityResources-*
AWS Config	Agregator	aws-controltower-GuardrailsComplianceAggregator
AWS Config	Aturan AWS Config	AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_READ_PROHIBITED AWSControlTower_AWS-GR_AUDIT_BUCKET_PUBLIC_WRITE_PROHIBITED
AWS CloudTrail	Trail	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
AWS Identity and Access Management	Kebijakan	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	Topik	aws-controltower-AggregateSecurityNotifications aws-controltower-AllConfigNotifications aws-controltower-SecurityNotifications
AWS Lambda	Fungsi	aws-controltower-NotificationForwarder

Tentang akun bersama

Tiga khusus Akun AWS dikaitkan dengan AWS Control Tower; akun manajemen, akun audit, dan akun arsip log. Akun-akun ini biasanya disebut sebagai akun bersama, atau terkadang sebagai akun inti.

- Anda dapat memilih nama yang disesuaikan untuk akun audit dan arsip log saat menyiapkan landing zone. Untuk informasi tentang mengubah nama akun, lihat Mengubah nama sumber daya AWS Control Tower secara eksternal.
- Anda juga dapat menentukan yang sudah ada Akun AWS sebagai akun keamanan atau logging AWS Control Tower, selama proses penyiapan landing zone awal. Opsi ini menghilangkan kebutuhan AWS Control Tower untuk membuat akun baru yang dibagikan. (Ini adalah pilihan satu kali.)

Untuk informasi selengkapnya tentang akun bersama dan sumber daya terkait, lihatSumber daya yang dibuat di akun bersama.

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 bersama.

Akun arsip log

Akun bersama arsip log diatur secara otomatis saat Anda membuat landing zone.

Akun ini berisi bucket Amazon S3 pusat untuk menyimpan salinan semua AWS CloudTrail dan AWS Config log file untuk semua akun lain di landing zone Anda. Sebagai praktik terbaik, kami

merekomendasikan untuk membatasi akses akun arsip log ke tim yang bertanggung jawab atas kepatuhan dan investigasi, serta alat keamanan atau audit terkait mereka. Akun ini dapat digunakan untuk audit keamanan otomatis, atau untuk 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 AWS Control Tower landing zone versi 3.3.

Untuk informasi selengkapnya tentang peran dan sumber daya yang tersedia di akun arsip log, lihat Sumber daya akun arsip log

> **Note**
>
> Log ini tidak dapat diubah. Semua log disimpan untuk tujuan audit dan investigasi kepatuhan yang terkait dengan aktivitas akun.

Akun audit

Akun bersama ini diatur secara otomatis saat Anda membuat landing zone.

Akun audit harus dibatasi untuk tim keamanan dan kepatuhan dengan peran lintas akun auditor (read-only) dan administrator (akses penuh) untuk 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 audit juga menerima pemberitahuan melalui layanan Amazon Simple Notification Service (Amazon SNS). Tiga kategori pemberitahuan dapat diterima:

- 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 pemberitahuan akun ke akun audit 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 audit, lihatSumber daya akun audit.

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 audit menerima email AWS Pemberitahuan - Konfirmasi Langganan dari setiap email yang Wilayah AWS didukung oleh AWS Control Tower. Untuk menerima email kepatuhan di akun audit Anda, Anda harus memilih tautan Konfirmasi langganan dalam setiap email dari masing-masing yang Wilayah AWS didukung oleh AWS Control Tower.

Tentang akun anggota

Akun anggota adalah akun tempat pengguna Anda melakukan AWS beban kerja mereka. Akun anggota ini dapat dibuat di Account Factory, oleh pengguna IAM Identity Center dengan hak istimewa Admin di konsol Service Catalog, atau dengan metode otomatis. Saat dibuat, akun anggota ini ada di

OU yang dibuat di konsol AWS Control Tower, atau terdaftar di AWS Control Tower. Untuk informasi lebih lanjut, lihat topik terkait ini:

- Menyediakan dan mengelola akun dengan Account Factory
- Mengotomatiskan tugas di AWS Control Tower
- AWS Organizations Terminology and Concepts dalam AWS Organizations User Guide

Lihat juga Menyediakan akun dengan AWS Control Tower Account Factory untuk Terraform (AFT) .

> **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 Account Factory

Daftarkan yang sudah ada Akun AWS

Anda dapat memperluas tata kelola AWS Control Tower ke individu, yang ada Akun AWS saat Anda mendaftarkannya 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 AWS Control Tower OU.

> **Note**
>
> Anda tidak dapat mendaftarkan akun yang ada untuk dijadikan akun audit atau arsip log Anda kecuali selama penyiapan landing zone awal.

Siapkan akses tepercaya terlebih dahulu

Sebelum Anda dapat mendaftarkan 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 AWS CloudFormation dapat

menerapkan tumpukan 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, AWS CloudFormation dapat membuat, memperbarui, atau menghapus tumpukan di beberapa akun dan Wilayah AWS dengan satu operasi. AWS Control Tower mengandalkan kemampuan kepercayaan ini sehingga dapat menerapkan peran dan izin ke akun yang ada sebelum memindahkannya ke unit organisasi terdaftar, dan dengan demikian membawa mereka di bawah tata kelola.

Untuk mempelajari lebih lanjut tentang akses tepercaya dan AWS CloudFormation StackSets, lihat AWS CloudFormationStackSetsdan AWS Organizations.

Apa yang terjadi selama pendaftaran akun

Selama proses pendaftaran, AWS Control Tower melakukan tindakan berikut:

- Memberi dasar 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 templat kumpulan tumpukan ini dan pastikan templat tersebut tidak bertentangan dengan kebijakan Anda yang ada.
- Mengidentifikasi akun melalui AWS IAM Identity Center atau AWS Organizations.
- Menempatkan akun ke dalam 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.
- Mengaktifkan AWS Config 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

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 Anda mendaftarkannya di AWS Control Tower.
- Jika Anda memindahkan akun ke OU terdaftar—misalnya melalui AWS Organizations konsol—dan Anda tidak melanjutkan untuk mendaftarkan akun ke AWS Control Tower, Anda mungkin ingin menghapus jejak tingkat akun yang tersisa untuk akun tersebut. Jika Anda memiliki penyebaran CloudTrail jejak yang ada, Anda akan dikenakan biaya duplikat CloudTrail .

Jika Anda memperbarui landing zone dan memilih untuk keluar dari jalur tingkat organisasi, atau jika landing zone Anda lebih tua dari versi 3.0, CloudTrail jejak tingkat organisasi tidak berlaku untuk akun Anda.

Mendaftarkan 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 yang ada atau VPC AWS default 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 Membuat Akun di AWS Control Tower Tanpa VPC.

Prasyarat untuk pendaftaran

Prasyarat ini diperlukan sebelum Anda dapat mendaftarkan yang sudah ada di AWS Control Akun AWS Tower:

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 Kepercayaan Peran:

   ```
   {
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Principal": {
           "AWS": "arn:aws:iam::Management Account ID: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, tinjau Daftarkan 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 AWS Control Tower.

> **Note**
>
> 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 sudah ada, Anda mungkin melihat biaya duplikat kecuali Anda menghapus jejak yang ada untuk akun tersebut sebelum Anda mendaftarkannya di AWS Control Tower.

Daftarkan akun yang ada

Fitur akun Daftar tersedia di konsol AWS Control Tower, untuk mendaftar yang sudah ada Akun AWS sehingga diatur oleh AWS Control Tower. Untuk informasi selengkapnya, lihat Mendaftarkan yang sudah ada Akun AWS.

Kemampuan akun Pendaftaran tersedia saat landing zone Anda tidak dalam keadaan drift. Untuk melihat kemampuan ini di konsol:

- Arahkan ke halaman Organisasi di AWS Control Tower.
- 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.
- Ikuti langkah-langkah untuk mendaftarkan akun individual, seperti yang ditunjukkan di Langkah-langkah untuk mendaftarkan akun bagian.

> **Note**
>
> Saat Anda mendaftarkan yang sudah ada Akun AWS, pastikan untuk memverifikasi alamat email yang ada. Jika tidak, akun baru dapat dibuat.

Kesalahan tertentu mungkin mengharuskan Anda me-refresh halaman dan mencoba lagi. Jika landing zone Anda dalam keadaan drift, Anda mungkin tidak dapat menggunakan kemampuan akun Daftar dengan sukses. Anda harus menyediakan akun baru melalui Account Factory hingga drift landing zone Anda teratasi.

Saat mendaftarkan akun dari konsol AWS Control Tower, Anda harus masuk ke akun dengan pengguna yang `AWSServiceCatalogEndUserFullAccess` kebijakan tersebut diaktifkan, 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 AWS Service Catalog dan pabrik akun AWS Control Tower, karena Anda akan memperbarui akun lainnya. Prosedur pembaruan diberikan di bagian yang disebut[Perbarui dan pindahkan akun pabrik akun dengan AWS Control Tower atau dengan AWS Service Catalog](#).

Langkah-langkah untuk mendaftarkan akun

Setelah AdministratorAccessizin (kebijakan) diberlakukan di akun Anda yang ada, ikuti langkah-langkah berikut untuk mendaftarkan akun:

Untuk mendaftarkan akun individual di AWS Control Tower

- Arahkan ke halaman AWS Control Tower Organization.
- Pada halaman Organisasi, akun yang memenuhi syarat untuk didaftarkan memungkinkan Anda memilih Mendaftar dari menu tarik-turun Tindakan di bagian atas bagian. Akun-akun ini juga menampilkan tombol Daftarkan akun saat Anda melihatnya di halaman Detail akun.
- Ketika Anda memilih Daftarkan akun, Anda akan melihat halaman Daftar akun, di mana Anda diminta untuk menambahkan `AWSControlTowerExecution` peran ke akun. Untuk beberapa instruksi, lihat[Tambahkan peran IAM yang diperlukan secara manual ke yang sudah ada Akun AWS dan daftarkan](#).
- Selanjutnya, pilih OU terdaftar dari daftar drop-down. Jika akun sudah dalam OU terdaftar, daftar ini akan menampilkan OU.
- Pilih Daftarkan akun.
- Anda akan melihat pengingat modal untuk menambahkan `AWSControlTowerExecution` peran dan mengonfirmasi tindakan.
- Pilih Mendaftar.
- AWS Control Tower memulai proses pendaftaran, dan Anda diarahkan kembali ke halaman detail Akun.

Penyebab umum kegagalan pendaftaran

- Untuk mendaftarkan akun yang 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 Wilayah asal Anda, atau di Wilayah mana pun yang didukung oleh AWS Control Tower. Akun AWS
- Anda dapat masuk ke akun yang perlu ditambahkan ke Portofolio Account Factory di AWS Service Catalog. Akun 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 Account Factory, Anda akan menerima kesalahan saat mencoba menambahkan akun. Untuk petunjuk tentang cara memberikan akses ke AWS Service Catalog portofolio, lihat Memberikan akses kepada pengguna.
- Anda dapat 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 melalui AWS CLI sebelum Anda dapat mendaftarkan akun. Lihat informasi yang lebih lengkap di Daftarkan akun yang memiliki sumber daya yang ada AWS Config dan Berinteraksi dengan menggunakan AWS Control TowerAWS CloudShell.
- Jika akun tersebut milik OU lain dengan akun manajemen, termasuk AWS Control Tower OU 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 atau pendaftaran akun gagal, karena AWS Control Tower tidak mendukung penandaan sumber daya. Untuk bantuan, hubungi perwakilan akun Anda, atau AWS Support.

Untuk informasi selengkapnya tentang cara AWS Control Tower bekerja dengan peran saat Anda membuat akun baru atau mendaftarkan akun yang ada, lihat Peran dan akun.

> **Tip**
>
> Jika Anda tidak dapat mengonfirmasi bahwa yang sudah ada Akun AWS 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 direkomendasikan di bagian berikut.

Direkomendasikan: Anda dapat mengatur pendekatan dua langkah untuk pendaftaran akun

- Pertama, gunakan paket AWS Config kesesuaian untuk mengevaluasi bagaimana akun Anda mungkin terpengaruh oleh beberapa kontrol AWS Control Tower. Untuk menentukan bagaimana pendaftaran ke AWS Control Tower dapat memengaruhi akun Anda, lihat Memperluas tata kelola AWS Control Tower menggunakan AWS Config paket 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 melakukan evaluasi, jika memutuskan untuk menyiapkan landing zone 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 dalam AWS Wilayah yang tidak memiliki dukungan AWS Control Tower. Anda dapat menggunakan paket kesesuaian untuk mengelola sumber daya di akun yang ada di Wilayah di mana AWS Control Tower tidak digunakan.

Bagaimana jika akun tidak memenuhi prasyarat?

Ingatlah bahwa, sebagai prasyarat, akun yang memenuhi syarat untuk terdaftar dalam 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 ini untuk memindahkan akun ke organisasi yang sama dengan AWS Control Tower.

Langkah-langkah persiapan untuk membawa akun ke organisasi yang sama dengan AWS Control Tower

1. Jatuhkan 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 Mengundang AWS akun untuk bergabung dengan organisasi Anda di Panduan AWS Organizations Pengguna.
3. Terima undangannya. Akun muncul di akar 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 yang ada.)
3. Menghapus atau memodifikasi perekam AWS Config konfigurasi atau saluran pengiriman yang ada melalui AWS CLI atau AWS CloudShell. Untuk informasi selengkapnya, lihat Contoh perintah AWS Config CLI untuk status sumber daya dan Daftarkan akun yang memiliki sumber daya yang ada AWS Config

Setelah Anda menyelesaikan langkah-langkah persiapan ini, Anda dapat mendaftarkan akun ke AWS Control Tower. Untuk informasi selengkapnya, lihat Langkah-langkah untuk mendaftarkan akun. 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 menjaga AWS CloudFormation tumpukan yang diterapkan, hapus instance tumpukan dari kumpulan tumpukan, dan pilih Pertahankan tumpukan untuk instance.
2. Mengakhiri produk yang disediakan akun di Account Factory AWS Service Catalog . (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 AWS Organizations kuota Anda.)
4. Bersihkan akun jika sumber daya tetap ada, lalu tutup, mengikuti langkah-langkah penutupan akunBatalkan kelola akun.
5. Jika Anda memiliki OU yang Ditangguhkan dengan kontrol yang ditentukan, Anda dapat memindahkan akun ke sana alih-alih melakukan Langkah 1.

Contoh perintah AWS Config CLI untuk status sumber daya

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`

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`*

Tambahkan peran IAM yang diperlukan secara manual ke yang sudah ada Akun AWS dan daftarkan

Jika Anda telah menyiapkan zona landing zone AWS Control Tower, Anda dapat mulai mendaftarkan akun organisasi Anda ke OU yang terdaftar di AWS Control Tower. Jika Anda belum menyiapkan landing zone, ikuti langkah-langkah seperti yang dijelaskan dalam Panduan Pengguna AWS Control Tower di Memulai, Langkah 2. Setelah landing zone 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 pasal 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 Anda 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 Beralih Peran.
5. Pada formulir Switch role, isi kolom 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 didefinisikan 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 AWS Management Console sebagai anak.

8. Setelah selesai, tetaplah di akun anak untuk bagian selanjutnya dari prosedur.
9. Catat ID akun manajemen, karena Anda harus memasukkannya pada 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 mana 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 menempelkan:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
      "Effect":"Allow",
      "Principal":{
         "AWS": "arn:aws:iam::Management Account ID:root"
         },
         "Action": "sts:AssumeRole",
         "Condition": {}
      }
   ]
  }
```

6. Ketika diminta untuk melampirkan kebijakan, pilih AdministratorAccess.
7. Pilih Selanjutnya: Tanda.
8. Anda mungkin melihat layar opsional berjudul Tambahkan tag. Lewati layar ini untuk saat ini dengan memilih Berikutnya:Ulasan
9. Pada layar Tinjauan, di bidang Nama peran, masukkan`AWSControlTowerExecution`.
10. Masukkan deskripsi singkat di kotak Deskripsi, seperti Memungkinkan 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 individual, seperti yang ditunjukkan pada Langkah-langkah untuk mendaftarkan akun halaman.
3. Verifikasi pendaftaran.
   - Dari AWS Control Tower, pilih Organisasi di navigasi kiri.
   - Cari akun yang baru saja Anda daftarkan. Keadaan awalnya akan menunjukkan status Mendaftar.
   - Ketika negara berubah menjadi Terdaftar, langkah itu berhasil.

Untuk melanjutkan proses ini, masuk ke setiap akun di organisasi yang ingin Anda daftarkan di AWS Control Tower. Ulangi langkah-langkah prasyarat dan langkah-langkah pendaftaran untuk setiap akun.

Pendaftaran akun otomatis AWS Organizations

Anda dapat menggunakan metode pendaftaran yang dijelaskan dalam posting blog yang disebut Daftarkan akun yang ada ke AWS Control Tower untuk mendaftarkan AWSAWS Organizations akun Anda ke AWS Control Tower dengan proses terprogram.

Template YAMM 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 memiliki sumber daya yang ada AWS Config

Topik ini memberikan step-by-step pendekatan untuk cara mendaftarkan akun yang memiliki AWS Config sumber daya yang ada. Untuk contoh cara memeriksa sumber daya yang ada, lihatContoh perintah AWS Config CLI untuk status sumber daya.

> **Note**
>
> 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 sepenuhnya, sebelum Anda dapat mendaftarkan akun ini ke AWS Control Tower untuk tujuan ini. Untuk akun yang tidak dimaksudkan untuk menjadi akun Audit dan Arsip Log, Anda dapat mengubah sumber daya Config yang ada.

Contoh sumber AWS Config 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

Asumsi

- Anda telah menerapkan 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 AWS Control Tower yang diatur oleh akun manajemen.
- Akun Anda bukan akun manajemen AWS Control Tower.
- Akun Anda tidak dalam penyimpangan tata kelola.

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. Anda akan dapat mengirimkan tiket dukungan tunggal untuk semua akun yang ingin Anda daftarkan, seperti yang dijelaskan dalamLangkah 1: Hubungi dukungan pelanggan dengan tiket, untuk menambahkan akun ke daftar izin AWS Control Tower, yang berikut.

Batasan

- Akun hanya dapat didaftarkan dengan menggunakan alur kerja AWS Control Tower untuk memperluas tata kelola.
- 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.

> **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.

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 pelanggan dengan tiket, untuk menambahkan akun ke daftar izin AWS Control Tower

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
- Wilayah beranda 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 AWS 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 apa pun

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 setiap AWS Wilayah

Untuk langkah ini, informasi berikut diperlukan tentang penyiapan AWS Control Tower Anda.

- `LOGGING_ACCOUNT`- ID akun Logging
- `AUDIT_ACCOUNT`- ID akun Audit
- `IAM_ROLE_ARN`- peran IAM ARN dibuat pada Langkah 1
- `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 sumber daya saluran AWS Config 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: Nama bucket logging dari akun logging AWS Control Tower

  `aws-controltower-logs-LOGGING_ACCOUNT-HOME_REGION`
- ***S3KeyPrefix: ORGANISASI_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=aws-controltower-
logs-LOGGING_ACCOUNT_ID-
HOME_REGION,s3KeyPrefix="ORGANIZATION_ID",configSnapshotDeliveryProperties={deliveryFrequency=T
controltower-AllConfigNotifications --region CURRENT_REGION
```

Langkah 5c. Memodifikasi AWS Config sumber daya otorisasi agregasi

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 AWS 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 ada.

1. Arahkan ke AWS CloudFormation konsol akun manajemen.
2. Buat yang baru StackSet dengan nama CustomerCreatedConfigResourcesForControlTower.
3. Salin dan perbarui template berikut:

```
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::${AWS::AccountId}:role/aws-controltower-
ConfigRecorderRole-customer-created
      RecordingGroup:
        AllSupported: true
        IncludeGlobalResourceTypes: GLOBAL_RESOURCE_RECORDING
        ResourceTypes: []
  CustomerCreatedConfigDeliveryChannel:
    Type: AWS::Config::DeliveryChannel
    Properties:
      Name: aws-controltower-BaselineConfigDeliveryChannel-customer-created
      ConfigSnapshotDeliveryProperties:
        DeliveryFrequency: TwentyFour_Hours
      S3BucketName: aws-controltower-logs-LOGGING_ACCOUNT-HOME_REGION
      S3KeyPrefix: ORGANIZATION_ID
      SnsTopicARN: !Sub arn:aws:sns:${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 BucketName bidang **S3**, ganti LOGGING_ACCOUNT_ID dan HOME_REGION*

b. *Di KeyPrefix bidang **S3**, ganti ORGANIZATION_ID*

c. *Di bidang **SnsTopicARN**, ganti AUDIT_ACCOUNT*

d. Di AuthorizedAccountIdbidang, ganti *AUDIT_ACCOUNT*

e. Di AuthorizedAwsRegionbidang, ganti *HOME_REGION*

4. Selama penyebaran di AWS 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-register OU.

Menyediakan dan mengelola akun dengan Account Factory

Bab ini mencakup ikhtisar dan prosedur untuk menyediakan akun anggota baru di landing zone 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 landing zone Anda. Secara default, pengguna IAM Identity Center yang menyediakan akun harus berada dalam `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 yang sudah ada Akun AWS ke AWS Control Tower, akun tersebut harus mengaktifkan `AWSControlTowerExecution` peran tersebut. Untuk informasi selengkapnya tentang cara mendaftarkan akun yang ada, lihatDaftarkan yang sudah ada Akun AWS.

Untuk informasi selengkapnya tentang izin, lihat Izin yang diperlukan untuk akun.

Menyediakan akun dengan AWS Service Catalog 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 secara terprogram, dengan AWS CLI 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 penyesuaian, lihatKustomisasi akun dengan Kustomisasi Account Factory (AFC).

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 AWS Management Console 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:

    - SSO UserEmail dapat berupa alamat email baru, atau alamat email yang terkait dengan pengguna IAM Identity Center 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 di SSO UserEmail, 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 menyegarkan halaman untuk memperbarui informasi status yang ditampilkan.

> **Note**
>
> Hingga lima akun dapat disediakan sekaligus.

Pertimbangan untuk mengelola akun di Account Factory

Anda dapat memperbarui, membatalkan kelola, 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 akun (OU).

> **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 IAM Identity Center. Akun yang dibuat sebelumnya tidak dihapus. Untuk informasi tentang menghapus alamat email pengguna IAM Identity Center sebelumnya dari Pusat Identitas IAM, lihat Menonaktifkan Pengguna.

Perbarui dan pindahkan akun pabrik akun dengan AWS Control Tower atau dengan AWS Service Catalog

Cara termudah untuk memperbarui akun terdaftar adalah melalui konsol AWS Control Tower. Pembaruan akun individual berguna untuk menyelesaikan penyimpangan, seperti. Akun Anggota yang Dipindahkan Pembaruan akun juga diperlukan sebagai bagian dari pembaruan landing zone penuh.

Jika Anda memindahkan akun dari satu unit organisasi (OU) ke yang lain, ingatlah bahwa kontrol yang diterapkan oleh OU baru mungkin berbeda dari kontrol di OU sebelumnya. Pastikan bahwa kontrol di OU baru memenuhi persyaratan kebijakan Anda untuk akun tersebut.

Kontrol perilaku saat akun dipindahkan antara OU

Saat Anda memindahkan akun di antara OU, kontrol untuk OU tujuan diterapkan ke akun. Namun, kontrol yang diterapkan ke akun dari OU sebelumnya tidak dihapus. Perilaku yang tepat dari kontrol khusus untuk implementasi kontrol yang aktif pada OU sebelumnya dan OU tujuan.

- Untuk kontrol yang diterapkan dengan AWS Config aturan: Kontrol dari OU sebelumnya tidak dihapus. Kontrol ini harus dihapus secara manual.
- Untuk kontrol yang diterapkan dengan SCP: Kontrol berbasis SCP dari OU sebelumnya adalah dihapus. Kontrol berbasis SCP untuk tujuan OU mulai berlaku pada akun ini.
- Untuk kontrol yang diimplementasikan dengan AWS CloudFormation kait: Perilaku ini tergantung pada status kontrol di OU baru.
  - Jika tujuan OU tidak memiliki kontrol berbasis kait aktif: Yang lama kontrol tetap aktif untuk akun yang dipindahkan, kecuali Anda menghapusnya secara manual.
  - Jika tujuan OU memiliki kontrol kait aktif: Kontrol lama adalah dihapus dan kontrol di OU tujuan diterapkan ke akun.

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 menunjukkan status Pembaruan yang tersedia.
3. Selanjutnya Anda akan melihat halaman Detail akun untuk akun yang Anda pilih.
4. Di kanan atas, pilih Perbarui akun.

Perbarui produk yang disediakan

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.

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:

      - SSO UserEmail (Tersedia dalam detail produk yang disediakan)
      - AccountEmail(Tersedia dalam detail produk yang disediakan)
      - SSO UserFirstName (Tersedia di Pusat Identitas IAM)
      - SSOU SerLastName (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 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.

Mengubah alamat email dari akun terdaftar

Untuk mengubah alamat email akun anggota terdaftar di AWS Control Tower, ikuti prosedur di bagian ini.

> **Note**
>
> Prosedur berikut tidak memungkinkan Anda mengubah alamat email akun manajemen, akun arsip log, atau akun audit. Untuk informasi selengkapnya tentang itu, lihat Bagaimana cara mengubah alamat email yang terkait dengan AWS akun saya? atau hubungi AWS Support.

Untuk mengubah alamat email akun yang dibuat AWS Control Tower

1. Pulihkan kata sandi pengguna root untuk akun tersebut. Anda dapat mengikuti langkah-langkah dalam artikel Bagaimana cara memulihkan AWS kata 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 tercermin AWS Organizations. Anda mungkin mengalami penundaan saat perubahan alamat email selesai diperbarui.
4. Perbarui produk yang disediakan di Service Catalog menggunakan alamat email yang sebelumnya milik akun. Proses untuk memperbarui produk yang disediakan termasuk mengaitkan alamat email baru dengan produk yang disediakan. Dengan cara ini perubahan alamat email berlaku di AWS Control Tower. Gunakan alamat email baru untuk pembaruan produk yang selanjutnya disediakan.

Untuk mengubah kata sandi atau alamat email akun anggota yang Anda buat AWS Organizations, lihat Mengakses akun anggota sebagai pengguna root di Panduan AWS Organizations Pengguna.

Mengubah nama akun 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

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 pengaturan Akun, seperti yang Anda lakukan untuk yang lain Akun AWS.
5. AWS Control Tower secara otomatis memperbarui dirinya sendiri untuk mencerminkan perubahan nama. Pembaruan ini tidak akan tercermin dalam produk yang disediakan di. AWS Service Catalog

Konfigurasikan Account Factory dengan pengaturan Amazon Virtual Private Cloud

Account Factory memungkinkan Anda membuat baseline 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 izinnya. Secara default, semua OU ada di daftar izinkan, yang berarti bahwa akun dapat disediakan di bawahnya. Anda dapat menonaktifkan OU tertentu untuk penyediaan akun melalui. AWS Service Catalog

Anda dapat melihat opsi konfigurasi VPC Amazon yang tersedia untuk pengguna akhir Anda saat mereka menyediakan akun baru.

Untuk mengonfigurasi 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 Account Factory untuk menavigasi ke halaman konfigurasi jaringan Account Factory. Di sana Anda dapat melihat pengaturan jaringan default 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 Account Factory baru yang mungkin dibuat oleh pengguna akhir Anda, dan masukkan pengaturan Anda ke dalam bidang.

- Pilih dinonaktifkan atau diaktifkan untuk membuat subnet publik di Amazon VPC. Secara default, subnet yang dapat diakses internet tidak diizinkan.

> **Note**
>
> Jika Anda mengatur konfigurasi VPC pabrik akun sehingga subnet publik diaktifkan saat menyediakan akun baru, pabrik akun mengonfigurasi Amazon VPC untuk membuat NAT Gateway. 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 kisaran 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 Anda berikan bisa tumpang tindih.
- Pilih wilayah atau semua wilayah untuk membuat VPC saat akun disediakan. Secara default semua wilayah yang tersedia dipilih.
- Dari daftar, pilih jumlah Availability Zones untuk mengonfigurasi subnet di setiap VPC. Nomor default dan yang direkomendasikan adalah 3.
- Pilih Simpan.

Anda dapat mengatur opsi konfigurasi ini untuk membuat akun baru yang tidak menyertakan VPC. Lihat langkah-langkahnya.

Batalkan kelola akun

Jika Anda membuat akun di Account Factory atau mendaftarkan akun Akun AWS, dan Anda tidak lagi ingin akun tersebut dikelola oleh AWS Control Tower di landing zone, Anda dapat membatalkan kelola akun tersebut dari konsol AWS Control Tower.

Saat Anda membatalkan pengelolaan akun AWS Control Tower, semua sumber daya yang disediakan oleh AWS Control Tower akan dihapus, termasuk cetak biru apa pun. Akun dipindahkan

dari AWS Control Tower OU 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.

Membatalkan pengelolaan akun juga dapat dilakukan di konsol Service Catalog oleh pengguna IAM Identity Center di `AWSAccountFactory` grup, dengan menghentikan Provisioned Product. Untuk informasi selengkapnya tentang pengguna atau grup Pusat Identitas IAM, lihat Mengelola pengguna dan mengakses melalui AWS IAM Identity Center. Prosedur berikut menjelaskan cara membatalkan pengelolaan akun anggota di Service Catalog.

Untuk membatalkan kelola akun yang terdaftar

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 tidak dikelola, statusnya berubah menjadi Tidak Terdaftar.
7. Jika Anda tidak lagi membutuhkan akun, tutuplah. Untuk informasi selengkapnya tentang menutup AWS akun, lihat Menutup akun di Panduan AWS Billing Pengguna

Saat Anda membatalkan pengelolaan akun yang disesuaikan, AWS Control Tower menghapus sumber daya yang telah diterapkan cetak biru, serta sumber daya lain yang dibuat AWS Control Tower dalam akun tersebut. Setelah Anda membatalkan kelola akun, Anda dapat menutup akun melalui AWS Organizations.

> **Note**
>
> Akun yang tidak dikelola tidak ditutup atau dihapus. Ketika akun tidak dikelola, 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 Account Factory dan mengubah alamat email pengguna IAM Identity Center untuk akun tersebut. Untuk informasi selengkapnya, lihat Perbarui dan pindahkan akun pabrik akun dengan AWS Control Tower atau dengan AWS Service Catalog.

Panduan Video

Video ini (3:25) menjelaskan cara menghapus akun dari AWS Control Tower, mendapatkan akses root ke akun, dan akhirnya menutup akun. 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. Captioning tersedia.

Panduan Video untuk Menutup Akun di AWS Control Tower.

Anda dapat melihat daftar AWS YouTube video yang menjelaskan tugas umum di AWS Control Tower.

Menutup akun yang dibuat di Account Factory

Akun yang dibuat di Account Factory adalah Akun AWS. Untuk informasi tentang penutupan Akun AWS, lihat Menutup akun di Panduan Referensi Manajemen AWS Akun.

> **Note**
>
> Menutup akun Akun AWS tidak sama dengan membatalkan pengelolaan akun dari AWS Control Tower—ini adalah tindakan terpisah. Anda harus membatalkan kelola akun sebelum Anda 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 satu per satu dengan kredensi root. AWS Organizations Namun, Anda tidak dapat menutup akun manajemen Anda dengan cara ini.

Saat Anda memanggil AWS Organizations CloseAccountAPI, atau menutup akun di AWS Organizations konsol, akun anggota diisolasi selama 90 hari, seperti yang Akun AWS akan terjadi. Akun menunjukkan status Ditangguhkan di AWS Control Tower dan AWS Organizations. Jika Anda mencoba bekerja dengan akun selama 90 hari tersebut, AWS Control Tower memberikan pesan kesalahan.

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 kelola akun anggota sebelum Anda menutup akun itu. Jika Anda menutup akun anggota tanpa terlebih dahulu membatalkan pengelolaannya, AWS Control Tower menunjukkan status akun sebagai Ditangguhkan, tetapi juga sebagai Terdaftar. Akibatnya, jika Anda mencoba mendaftarkan ulang OU akun selama waktu 90 hari tersebut, AWS Control Tower menghasilkan pesan kesalahan. Akun yang ditangguhkan pada dasarnya memblokir tindakan pendaftaran ulang dengan kegagalan pra-pemeriksaan. Jika Anda menghapus akun dari OU, Anda dapat mendaftarkan ulang OU, tetapi AWS dapat menghasilkan kesalahan mengenai metode pembayaran yang hilang untuk akun tersebut. Untuk mengatasi kendala ini, buat OU lain, dan pindahkan akun ke OU itu sebelum Anda mencoba mendaftar ulang. Sebaiknya beri nama OU ini sebagai Suspended OU.

> **Note**
>
> Jika Anda tidak membatalkan kelola akun sebelum Anda menutupnya, Anda harus menghapus produk yang disediakan akun AWS Service Catalog setelah 90 hari tersebut selesai.

Untuk informasi selengkapnya, lihat AWS Organizations dokumentasi tentang CloseAccountAPI.

Pertimbangan Sumber Daya untuk Account Factory

Ketika 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-* StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-* StackSet-AWSControlTowerBP-BASELINE-CONFIG-* StackSet-AWSControlTowerBP-BASELINE-ROLES-* StackSet-AWSControlTowerBP-BASELINE-SERVICE-ROLES-*
AWS CloudTrail	Trail	aws-controltower-BaselineCloudTrail
Amazon CloudWatch	CloudWatch Aturan Acara	aws-controltower-ConfigComplianceChangeEventRule
Amazon CloudWatch	CloudWatch Log	aws-controltower/CloudTrail Logs /aws/lambda/aws-controltower-NotificationForwarder
AWS Identity and Access Management	Peran	aws-controltower-AdministratorExecutionRole aws-controltower-CloudWatchLogsRole

AWS layanan	Tipe sumber daya	Nama sumber daya
		aws-controltower-ConfigRecorderRole aws-controltower-ForwardSnsNotificationRole aws-controltower-ReadOnlyExecutionRole AWSControlTowerExecution
AWS Identity and Access Management	Kebijakan	AWSControlTowerServiceRolePolicy
Amazon Simple Notification Service	Topik	aws-controltower-SecurityNotifications
AWS Lambda	Aplikasi	StackSet-AWSControlTowerBP-BASELINE-CLOUDWATCH-*
AWS Lambda	Fungsi	aws-controltower-NotificationForwarder

Kustomisasi akun dengan Kustomisasi Account Factory (AFC)

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 menyiapkan kustomisasi pabrik akun, AWS Control Tower mengotomatiskan proses ini untuk penyediaan di masa mendatang, sehingga Anda tidak perlu memelihara saluran pipa apa pun. Akun yang disesuaikan tersedia untuk digunakan segera setelah sumber daya disediakan.

Akun khusus Anda disediakan di pabrik akun, melalui AWS 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 spesifik yang Anda perlukan saat akun disediakan. Cetak biru yang telah ditentukan sebelumnya, dibangun dan dikelola oleh

AWS mitra, juga tersedia. Untuk informasi selengkapnya tentang cetak biru yang dikelola mitra, lihat Pustaka Memulai.AWS Service Catalog

> **Note**
>
> AWS Control Tower berisi kontrol proaktif, yang memantau AWS CloudFormation sumber daya di AWS Control Tower. Secara opsional, Anda dapat mengaktifkan kontrol ini di landing zone Anda. Ketika 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.

Cetak biru akun Anda disimpan dalam Akun AWS, yang untuk tujuan kami disebut sebagai akun hub. Blueprints disimpan dalam bentuk produk Service Catalog. Kami menyebut produk ini cetak biru, untuk membedakannya dari produk Service Catalog lainnya. Untuk mempelajari lebih lanjut tentang cara membuat produk Service Catalog, lihat Membuat produk di Panduan AWS Service Catalog Administrator.

Terapkan cetak biru ke akun yang ada

Anda juga dapat menerapkan cetak biru yang disesuaikan ke akun yang ada, dengan mengikuti langkah-langkah Perbarui akun di konsol AWS Control Tower. Lihat perinciannya di Perbarui akun di konsol.

> **Sebelum Anda mulai**
>
> Sebelum Anda mulai membuat akun khusus dengan AWS Control Tower Account Factory, Anda harus memiliki lingkungan landing zone AWS Control Tower yang diterapkan, dan Anda harus memiliki unit organisasi (OU) yang terdaftar di AWS Control Tower, tempat akun yang baru dibuat akan ditempatkan.

Untuk informasi selengkapnya tentang bekerja dengan AFC, lihat Mengotomatiskan penyesuaian akun menggunakan Kustomisasi Account Factory di AWS Control Tower.

Persiapan untuk kustomisasi

- 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.
- Jika Anda berencana untuk mendaftar Akun AWS ke AWS Control Tower dan menyesuaikannya, Anda harus terlebih dahulu menambahkan `AWSControlTowerExecution` peran tersebut ke akun tersebut, seperti yang Anda lakukan untuk akun lain yang Anda daftarkan ke AWS Control Tower.
- Jika Anda berencana untuk menggunakan cetak biru mitra yang memiliki persyaratan berlangganan marketplace, Anda harus mengonfigurasinya dari akun manajemen AWS Control Tower sebelum menerapkan cetak biru mitra sebagai cetak biru penyesuaian pabrik akun.

Topik

Siapkan untuk kustomisasi

Bagian selanjutnya memberikan langkah-langkah untuk menyiapkan Account Factory untuk proses kustomisasi. Kami menyarankan Anda menyiapkan admin yang didelegasikan untuk akun hub, sebelum memulai langkah-langkah ini.

Ringkasan

- Langkah 1. Buat peran yang diperlukan. Buat peran IAM yang memberikan izin kepada AWS Control Tower untuk memiliki akses ke akun (hub), tempat produk Service Catalog, 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 membuat dasar 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 sesuai di Account Factory, di konsol AWS Control Tower, saat membuat akun.

Langkah 1. Buat peran yang diperlukan

Sebelum mulai menyesuaikan akun, Anda harus menyiapkan peran yang berisi hubungan kepercayaan antara AWS Control Tower dan akun hub Anda. Saat diasumsikan, peran tersebut memberikan akses AWS Control Tower untuk mengelola akun hub. Peran itu harus diberi nama AWSControlTowerBlueprintAccess.

AWS Control Tower mengasumsikan peran ini untuk membuat sumber daya Portofolio atas nama Anda AWS Service Catalog, lalu 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.

Arahkan ke konsol IAM untuk mengatur peran yang diperlukan.

Untuk mengatur peran dalam akun AWS Control Tower yang terdaftar

1. Buat federasi atau masuk sebagai prinsipal di akun manajemen AWS Control Tower.
2. Dari prinsipal federasi di akun manajemen, asumsikan atau alihkan peran ke `AWSControlTowerExecution` peran di akun AWS Control Tower terdaftar yang Anda pilih untuk dijadikan akun hub cetak biru.

3. Dari `AWSControlTowerExecution` peran di akun AWS Control Tower yang terdaftar, buat `AWSControlTowerBlueprintAccess` peran dengan izin dan hubungan kepercayaan yang tepat.

> **Note**
>
> Untuk mematuhi panduan praktik AWS terbaik, penting bagi Anda untuk segera keluar dari `AWSControlTowerExecution` peran tersebut 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 tidak perlu berasumsi sebelum melanjutkan pengaturan peran. `AWSControlTowerBlueprintAccess`

Untuk mengatur peran dalam akun anggota yang tidak terdaftar

1. Federasi atau masuk sebagai kepala sekolah di akun yang ingin Anda tetapkan sebagai akun hub, melalui metode pilihan Anda.
2. Saat masuk sebagai prinsipal di akun, buat `AWSControlTowerBlueprintAccess` peran dengan izin dan hubungan kepercayaan yang tepat.

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 dalam memberikan akses hak istimewa paling sedikit. Saat Anda membuat kebijakan sendiri, ganti istilah *`YourManagementAccountId`*dengan

ID acccount aktual akun manajemen AWS Control Tower Anda, dan ganti istilah tersebut *YourControlTowerUserRole*dengan pengenal peran IAM untuk akun manajemen Anda.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                "arn:aws:iam::YourManagementAccountId:role/service-role/
AWSControlTowerAdmin",
                "arn:aws:iam::YourManagementAccountId:role/YourControlTowerUserRole"
                ]
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Kebijakan izin yang diperlukan

AWS Control Tower mengharuskan kebijakan terkelola yang diberi nama `AWSServiceCatalogAdminFullAccess` harus dilampirkan ke `AWSControlTowerBlueprintAccess` peran. Kebijakan ini memberikan izin yang AWS Service Catalog dicari ketika AWS Control Tower mengizinkan AWS Control Tower 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 peran tersebut. `AWSControlTowerBlueprintAccess`
- 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 templat 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 templat saat membuat produk. AWS Service Catalog

> **Important**
>
> Sebagai hasil dari HashiCorp lisensi Terraform yang diperbarui, AWS Service Catalog mengubah dukungan untuk produk Terraform Open Source dan menyediakan produk ke jenis produk baru, yang disebut Eksternal. Untuk mempelajari lebih lanjut tentang bagaimana perubahan ini memengaruhi AFC, termasuk cara memperbarui cetak biru akun yang ada ke jenis produk Eksternal, tinjau Transisi ke jenis produk Eksternal.

Ringkasan langkah-langkah untuk membuat cetak biru

- Buat atau unduh AWS CloudFormation templat 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 (terkadang 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 templat dan kemudian pilih Pilih file. Pilih atau tempel templat 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 AWS CloudFormation template dari repositori arsitektur AWS Service Catalog referensi. Salah satu contoh dari repositori itu membantu menyiapkan rencana cadangan untuk sumber daya Anda.

Berikut adalah 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: nodejs16.x
      Handler: index.handler
      Timeout: 5
      Code:
        ZipFile: >
          const response = require("cfn-response");
          exports.handler = function (event, context) {
            const awsAccountId = context.invokedFunctionArn.split(":")[4]
            const connectionString= "fake connection string that's specific to account
" + awsAccountId;
            const responseData = {
              Value: connectionString,
            }
            response.send(event, context, response.SUCCESS, responseData);
            return connectionString;
          };

  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 konsol. AWS Service Catalog Untuk informasi selengkapnya, lihat Mengelola produk di Panduan Adminstrator Service Catalog.

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.

> **Note**
>
> Anda harus menyiapkan akun hub kustomisasi dan menambahkan setidaknya satu cetak biru (produk Service Catalog) 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 tersebut, pilih produk Service Catalog yang sudah ada (cetak biru yang ada).
3. Pilih versi cetak biru yang tepat (produk Service Catalog), jika Anda memiliki lebih dari satu versi.
4. (Opsional) Anda dapat menambahkan atau mengubah kebijakan penyediaan cetak biru pada saat ini dalam proses. Kebijakan penyediaan cetak biru ditulis dalam JSON dan dilampirkan ke peran IAM, sehingga dapat menyediakan sumber daya yang ditentukan dalam templat cetak biru. AWS Control Tower membuat peran ini di akun anggota sehingga Service Catalog dapat menyebarkan sumber daya menggunakan kumpulan AWS CloudFormation tumpukan. Peran ini bernama `AWSControlTower-BlueprintExecution-bp-`*`xxxx`*. `AdministratorAccess`Kebijakan ini diterapkan di sini secara default.
5. Pilih Wilayah AWS atau Wilayah tempat Anda ingin menyebarkan akun berdasarkan cetak biru ini.

6. Jika cetak biru Anda berisi parameter, Anda dapat memasukkan nilai untuk parameter ke dalam bidang tambahan dalam alur kerja AWS Control Tower. Nilai tambahan dapat mencakup: 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 kustom saat Anda membuat akun baru: AWS

1. Buka AWS Control Tower di AWS Management Console.
2. Pilih Akun pabrik 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 di mana akun Anda akan ditambahkan.
6. Perluas bagian kustomisasi pabrik Akun.
7. Masukkan ID akun hub blueprint yang berisi produk Service Catalog Anda dan pilih Validasi. Untuk informasi selengkapnya tentang akun hub cetak biru, lihat. Kustomisasi akun dengan Kustomisasi Account Factory (AFC)
8. Pilih menu tarik-turun yang berisi semua cetak biru dari Daftar Produk Service Catalog Anda (semua cetak biru kustom 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 diisi sebelumnya.
10. Terakhir, pilih di mana 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 hanya dapat diterapkan ke satu Wilayah, 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.

Daftarkan dan sesuaikan akun

Untuk mendaftarkan dan menyesuaikan akun di konsol AWS Control Tower.

1. Arahkan ke konsol AWS Control Tower dan pilih Organization dari navigasi kiri.
2. Anda akan melihat daftar akun Anda yang tersedia. Identifikasi akun yang ingin Anda daftarkan dengan cetak biru khusus. Kolom Status 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 di mana akun Anda akan menjadi anggota.
6. Selesaikan bagian kustomisasi pabrik Akun menggunakan langkah yang sama seperti 7-12 dari prosedur Buat akun. Untuk informasi selengkapnya, lihat Akun Penyediaan Account Factory dengan AWS Service Catalog.

Anda dapat melihat status progres 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 akun Perbarui di konsol AWS Control Tower, dan pilih cetak biru baru untuk ditambahkan ke akun. Untuk informasi selengkapnya, lihat Memperbarui 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 ditimpa.

> **Note**
>
> Satu cetak biru dapat diterapkan per akun AWS Control Tower.

Perbarui cetak biru

Prosedur berikut menjelaskan cara memperbarui cetak biru khusus dan cara menerapkannya.

Untuk memperbarui cetak biru kustom Anda

1. Perbarui AWS CloudFormation template Anda atau file tar.gz Terraform (cetak biru) dengan konfigurasi baru Anda.
2. Simpan cetak biru yang diperbarui sebagai versi baru di. AWS Service Catalog

Untuk menerapkan cetak biru Anda yang diperbarui

1. Arahkan ke halaman Organisasi di konsol AWS Control Tower.
2. Filter halaman Organisasi berdasarkan nama dan versi cetak biru.
3. Ikuti proses Perbarui akun, dan terapkan versi cetak biru terbaru di akun Anda.

Jika pembaruan cetak biru tidak berhasil

AWS Control Tower memungkinkan pembaruan cetak biru saat produk yang disediakan dalam status. `AVAILABLE` Jika produk yang Anda sediakan dalam `TAINTED` keadaan, 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 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 Perbarui akun untuk menghapus cetak biru dan mengembalikan akun ke konfigurasi default AWS Control Tower.

Saat Anda memasuki alur kerja akun Perbarui 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 Perbarui 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 masing-masing mitra membantu Anda membuat akun yang disesuaikan, yang telah dikonfigurasi sebelumnya untuk bekerja dengan penawaran produk dari mitra tertentu.

Untuk melihat daftar lengkap cetak biru mitra AWS Control Tower, navigasikan ke Service Catalog Getting Started Library di konsol Anda. Cari jenis sumber AWS Control Tower Blueprints.

Pertimbangan untuk Kustomisasi Account Factory (AFC)

- AFC mendukung kustomisasi menggunakan produk AWS Service Catalog cetak biru tunggal saja.
- Produk AWS Service Catalog cetak biru harus dibuat di akun hub, dan di Wilayah yang sama dengan Wilayah home AWS Control Tower landing zone.

- Peran `AWSControlTowerBlueprintAccess` 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 menerapkan 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 cetak biru tidak dapat diubah. AWS Service Catalog
- AWS Control Tower tidak mendukung penghapusan cetak biru yang ada dan menambahkan cetak biru baru dalam satu operasi pembaruan cetak biru. 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 yang disesuaikan, atau akun yang tidak disesuaikan. Jika Anda tidak membuat atau mendaftarkan akun yang disesuaikan dengan cetak biru, AWS Control Tower membuat produk yang disediakan Account Factory (melalui Service Catalog) 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 solusi

Saat membuat `AWSControlTowerBlueprintAccess` peran dari akun AWS Control Tower, Anda harus masuk sebagai prinsipal menggunakan `AWSControlTowerExecution` peran tersebut. Jika Anda masuk seperti yang lain, `CreateRole` operasi dicegah oleh SCP, seperti yang ditunjukkan dalam 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 sesudahnya, 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 akun tersebut 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 AWS CloudFormation untuk membuat atas nama Anda. StackSet AWS CloudFormation memerlukan akses ke akun terkelola Anda untuk membuat AWS CloudFormation tumpukan di. StackSet Meskipun AWS CloudFormation sudah memiliki hak administrator di akun yang dikelola melalui `AWSControlTowerExecution` peran, peran ini tidak dapat diasumsikan oleh. AWS CloudFormation

Sebagai bagian dari mengaktifkan cetak biru, AWS Control Tower menciptakan peran dalam akun anggota, yang AWS CloudFormation dapat diasumsikan untuk menyelesaikan tugas manajemen. StackSet Cara termudah untuk mengaktifkan cetak biru khusus Anda melalui pabrik akun adalah dengan menggunakan kebijakan izinkan semua, karena kebijakan tersebut kompatibel dengan templat cetak biru apa pun.

Namun, praktik terbaik menyarankan bahwa Anda harus membatasi izin untuk AWS CloudFormation di akun target. Anda dapat memberikan kebijakan yang disesuaikan, yang diterapkan AWS Control Tower pada peran yang dibuatnya AWS CloudFormation untuk digunakan. Misalnya, jika cetak biru Anda membuat Parameter SSM yang disebut sesuatu yang penting, Anda dapat memberikan kebijakan berikut:

```
{
    "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"
        }
    ]
}
```

`AllowCloudFormationActionsOnStacks`Pernyataan ini diperlukan untuk semua kebijakan kustom AFC; AWS CloudFormation menggunakan peran ini untuk membuat instance tumpukan, oleh karena itu memerlukan izin untuk melakukan AWS CloudFormation tindakan pada tumpukan. `AllowSsmParameterActions`Bagian ini khusus untuk template yang diaktifkan.

Selesaikan masalah izin

Ketika 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 memastikan bahwa kebijakan tersebut cukup untuk mengaktifkan cetak biru, pastikan AWS CloudFormation izin diberikan, dan Anda dapat membuat tumpukan secara langsung menggunakan peran tersebut.

Izin tambahan diperlukan untuk membuat produk Service Catalog berbasis Terraform

Saat Anda membuat produk AWS Service Catalog Eksternal dengan file konfigurasi Terraform untuk AFC, AWS Service Catalog izin tertentu harus ditambahkan ke kebijakan IAM kustom AFC Anda, selain izin yang diperlukan untuk membuat sumber daya yang ditentukan dalam templat Anda. Jika Anda memilih kebijakan Admin lengkap default, Anda tidak perlu menambahkan izin tambahan ini.

```
{
    "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 AWS Service Catalog, lihat Langkah 5: Membuat peran peluncuran di Panduan Administrator Service Catalog.

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.

> **Note**
>
> 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.

Dengan AFT, Anda membuat file Terraform permintaan akun, yang berisi input yang memanggil alur kerja AFT. Setelah penyediaan dan pembaruan akun selesai, alur kerja AFT berlanjut dengan menjalankan kerangka kerja penyediaan akun AFT dan langkah-langkah penyesuaian akun.

Prasyarat

Sebelum memulai dengan AFT, Anda harus membuat yang berikut:

- Lingkungan AFT yang sepenuhnya digunakan. Untuk informasi selengkapnya, lihat Ikhtisar AWS Control Tower Account Factory untuk Terraform (AFT) dan Menerapkan AWS Control Tower Account Factory untuk Terraform (AFT)
- Satu atau lebih `git` repositori AFT di lingkungan AFT Anda yang sepenuhnya digunakan. Untuk informasi selengkapnya, lihat Langkah pasca-penerapan untuk AFT.

> **Tip**
>
> Secara opsional, Anda dapat membuat folder template akun di aft-account-customizationsrepositori.

Untuk informasi tentang Wilayah AWS di mana AFT memiliki batasan penerapan, lihat Batasan dan kuota di AWS Control Tower danKeterbatasan kontrol.

Menyediakan akun baru dengan AFT

Untuk menyediakan akun baru dengan AFT, buat file Terraform permintaan akun. File ini berisi input untuk parameter dalam aft-account-requestrepositori. Setelah membuat file Terraform permintaan akun, 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 pipeline penyediaan akun AFT.

Permintaan akun Parameter file Terraform

Anda harus menyertakan parameter berikut dalam file Terraform permintaan akun Anda. Anda dapat melihat contoh permintaan akun Terraform file di. GitHub

- Nilai `module name` harus unik sesuai Akun AWS permintaan.

- Nilai `module source` adalah jalur ke modul Terraform permintaan akun yang disediakan AFT.
- Nilai `control_tower_parameters` menangkap input yang diperlukan untuk membuat akun AWS Control Tower. Nilai termasuk bidang masukan berikut:
  - `AccountEmail`
  - `AccountName`
  - `ManagedOrganizationalUnit`
  - `SSOUserEmail`
  - `SSOUserFirstName`
  - `SSOUserLastName`

> **Note**
>
> Masukan yang Anda berikan tidak `control_tower_parameters` dapat diubah selama penyediaan akun.
> Format yang didukung untuk menentukan `ManagedOrganizationalUnit` dalam aft-account-requestrepositori termasuk dan. `OUName` `OUName (OU-ID)`

- `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 termasuk bidang masukan berikut:
  - `change_reason`
  - `change_requested_by`
- `custom_fields`menangkap metadata tambahan dengan kunci dan nilai yang diterapkan sebagai parameter SSM di akun penjual 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 peraturan dapat menggunakan tambahan Aturan AWS Config. Metadata yang Anda kumpulkan `custom_fields` dapat meminta pemrosesan tambahan selama penyediaan dan pembaruan akun. Jika bidang kustom dihapus dari permintaan akun, bidang kustom akan dihapus dari Penyimpanan Parameter SSM untuk akun vended.

- (Opsional) `account_customizations_name` menangkap folder template akun di aft-account-customizationsrepositori. Untuk informasi selengkapnya, lihat Penyesuaian 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 inginkan agar AFT sediakan atau kaskade beberapa permintaan akun dalam satu file Terraform permintaan akun.

Perbarui akun yang ada

Anda dapat memperbarui akun yang disediakan AFT dengan mengedit permintaan akun yang dikirimkan sebelumnya dan menjalankan`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`, dan parameter lain dalam file Terraform permintaan akun. Untuk informasi selengkapnya, lihat Menyediakan akun baru dengan AFT.

> **Note**
>
> Masukan yang Anda berikan tidak `control_tower_parameters` dapat diubah selama penyediaan akun.
> Format yang didukung untuk menentukan `ManagedOrganizationalUnit` dalam aft-account-requestrepositori termasuk dan. `OUName` `OUName (OU-ID)`

Perbarui akun yang tidak disediakan AFT

Anda dapat memperbarui akun AWS Control Tower yang dibuat di luar AFT dengan menentukan akun di aft-account-requestrepositori.

> **Note**
>
> Pastikan semua detail akun sudah benar dan konsisten dengan organisasi AWS Control Tower dan masing-masing produk AWS Service Catalog yang disediakan.

Prasyarat untuk memperbarui yang sudah ada dengan AFT Akun AWS

- Akun AWS Harus terdaftar di AWS Control Tower.
- Akun AWS Harus menjadi bagian dari organisasi AWS Control Tower.

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 yang berikut:

- Sebuah landing zone AWS Control Tower. Untuk informasi selengkapnya, lihat Merencanakan landing zone AWS Control Tower Anda.
- Wilayah rumah untuk zona landing zone AWS Control Tower Anda. Untuk informasi selengkapnya, lihat Cara Wilayah AWS bekerja dengan 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 ingin memilih penyedia VCS yang berbeda, 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 Anda

Selesaikan langkah-langkah dalam 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 AdministratorAccesskredensi. 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 (disarankan)

Kami menyarankan Anda membuat OU terpisah di AWS organisasi Anda. Di sinilah Anda menyebarkan akun manajemen AFT. Buat OU baru dengan 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. Akun manajemen AWS Control Tower, yang terkait dengan landing zone AWS Control Tower

Anda, menjual akun manajemen AFT. 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 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 `1.2.0` atau yang lebih baru.

Langkah 5: 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 AdministratorAccesskredensi. 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.

Modul AFT menyertakan `aft_enable_vpc` parameter yang menentukan apakah AWS Control Tower menyediakan sumber daya akun dalam virtual private cloud (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.

> **Note**
>
> Mengaktifkan kembali `aft_enable_vpc` parameter (mengalihkan nilai dari `false` ke`true`) mungkin mengharuskan Anda menjalankan `terraform apply` perintah dua kali berturut-turut.

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 6: 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.

Langkah-langkah pasca-penerapan

Setelah penyebaran infrastruktur AFT selesai, ikuti langkah-langkah tambahan ini untuk menyelesaikan proses penyiapan dan bersiap-siap untuk menyediakan akun.

Langkah 1: (Opsional) Lengkap CodeConnections dengan penyedia VCS yang Anda inginkan

Jika Anda memilih penyedia VCS pihak ketiga, AFT menetapkan 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: (Wajib) Isi setiap repositori

AFT mengharuskan Anda mengelola empat repositori:

1. Permintaan akun — Repositori ini menangani penempatan atau pembaruan permintaan akun. Contoh 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 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 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 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.

Ikhtisar AWS Control Tower Account Factory 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 dari penyediaan akun berbasis Terraform sambil memungkinkan Anda untuk mengatur akun Anda dengan AWS Control Tower.

Dengan AFT Anda membuat file Terraform permintaan akun 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 pipeline penyediaan akun AFT.

AFT mendukung Terraform Cloud, 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 penelusuran permintaan kustomisasi akun. Setiap kali Anda mengirimkan permintaan kustomisasi akun, AFT menghasilkan token penelusuran unik yang melewati mesin AWS Step Functions status penyesuaian AFT, yang mencatat token sebagai bagian dari pelaksanaannya. Anda kemudian dapat menggunakan kueri wawasan Amazon CloudWatch Logs untuk mencari rentang stempel waktu dan mengambil token permintaan. Akibatnya, Anda dapat melihat muatan yang menyertai token, sehingga Anda dapat melacak permintaan penyesuaian akun Anda di seluruh alur kerja AFT. Untuk informasi tentang CloudWatch Log dan Step Functions, lihat berikut ini:

- Apa itu Amazon CloudWatch Logs? di Panduan Pengguna CloudWatch Log Amazon
- Apa itu AWS Step Functions? di Panduan AWS Step Functions Pengembang

AFT menggabungkan kemampuan AWS layanan lain sebagaiLayanan komponen, untuk membangun kerangka kerja, dengan saluran pipa yang menyebarkan Terraform Infrastructure as Code (IAc). AFT memungkinkan Anda untuk:

- Kirim permintaan penyediaan akun dan perbarui dalam model GitOps
- Metadata akun toko dan riwayat audit
- Terapkan tag tingkat akun
- Tambahkan penyesuaian ke semua akun, ke satu set akun, atau ke akun individual

- Aktifkan opsi fitur

AFT membuat akun terpisah, yang disebut akun manajemen AFT, untuk menyebarkan kemampuan AFT. Sebelum Anda dapat mengatur AFT, Anda harus memiliki landing zone AWS Control Tower yang sudah 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: AFT secara native bergantung AWS CodeCommit, tetapi mendukung sumber alternatif untuk. 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 Enterprise Support AWS

> **Note**
>
> Pipeline AFT tidak dimaksudkan untuk digunakan dalam menyebarkan sumber daya, seperti instans Amazon EC2, yang diperlukan akun Anda untuk menjalankan aplikasi Anda. Ini ditujukan 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. Captioning tersedia.

Panduan Video Penyediaan Akun Otomatis di AWS Control Tower.

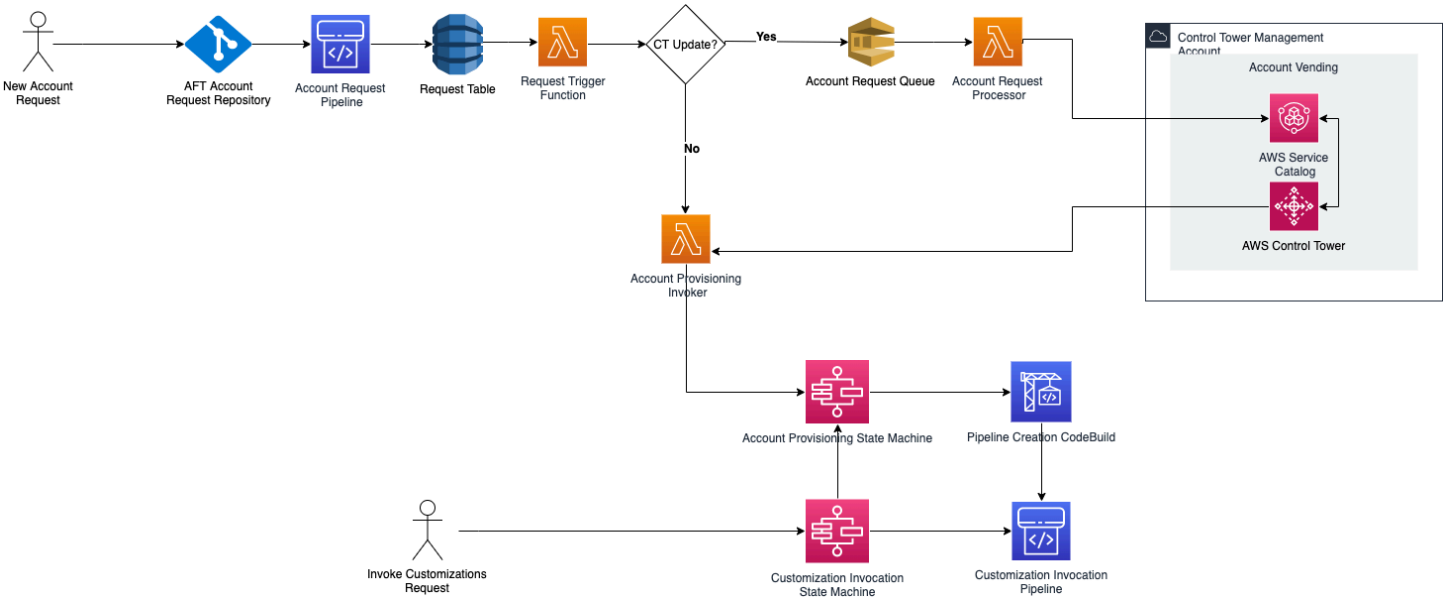
Arsitektur AFT

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 first-in-first-out urutan. 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 vended.
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



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 terapkan di lingkungan AFT Anda.

Konfigurasi AFT default mencakup alokasi AWS PrivateLink 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 VPC Amazon untuk NAT Gateway. Hubungi perwakilan AWS akun Anda untuk informasi lebih spesifik tentang mengelola biaya ini. Anda dapat mengubah pengaturan default ini untuk AFT.

Versi Terraform dan AFT

Account Factory for Terraform (AFT) mendukung versi Terraform atau yang lebih baru. `1.2.0` Anda harus memberikan versi Terraform sebagai parameter input untuk proses penerapan AFT, seperti yang ditunjukkan pada contoh berikut.

```
terraform_version = "1.2.0"
```

Distribusi terraform

AFT mendukung tiga distribusi Terraform:

- Edisi Komunitas Terraform
- Awan 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 Terraform Cloud 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 Terraform Cloud:
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"
```

Awan Terraform

Saat Anda memilih Terraform Cloud sebagai distribusi Anda, AFT membuat ruang kerja untuk komponen berikut di organisasi Terraform Cloud Anda, yang memulai alur kerja berbasis API.

- Permintaan akun
- Kustomisasi AFT untuk akun yang disediakan AFT
- Kustomisasi akun untuk akun yang disediakan AFT
- Kustomisasi global untuk akun yang disediakan AFT

Terraform Cloud mengelola konfigurasi status Terraform yang dihasilkan.

Saat Anda memilih Terraform Cloud sebagai distribusi Anda, berikan parameter input berikut:

- `terraform_distribution = "tfc"`

- `terraform_token`— Parameter ini berisi nilai token Terraform Cloud. 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 Terraform Cloud Anda.

> **Note**
>
> Beberapa penerapan AFT dalam satu organisasi Terraform Cloud tidak didukung.

Untuk informasi tentang cara menyiapkan Terraform Cloud, 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 alur kerja berbasis API 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

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 default

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 lebih lanjut 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 default

Saat Anda mengaktifkan opsi ini, AFT menghapus semua VPC AWS default di akun manajemen 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
```

Lihat VPC default dan subnet default untuk mempelajari lebih lanjut tentang VPC default.

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.

Tabel sumber daya yang awalnya dibuat, berdasarkan akun

AWS Control Tower Account Factory untuk akun manajemen Terraform

AWS layanan	Jenis sumber daya	Nama sumber daya
AWS Identity and Access Management	Peran	AWSAFTAdministrator AWSAFTExecution AWSAFTService aws-ct-aft-*
AWS Identity and Access Management	Kebijakan	aws-ct-aft-*
CodeCommit	Repositori	aws-ct-aft-*
CodeBuild	Membangun Proyek	aws-ct-aft-*
Kode Pipa	Alur	*-baseline-*
Amazon S3	Bucket	*-aws-ct-aft-* aws-ct-aft-*
Lambda	Fungsi	aws-ct-aft-*
Lambda	Lapisan	aws-ct-aft-common-layer
DynamoDB	Tabel	aws-ct-aft-request aws-ct-aft-request-audit aws-ct-aft-request-metadata aws-ct-aft-controltower-events
Step Functions	Mesin Negara	aws-ct-aft-prebaseline aws-ct-aft-prebaseline-customizations aws-ct-aft-trigger-baseline

AWS layanan	Jenis sumber daya	Nama sumber daya
		aws-ct-aft-features
VPC	VPC	aws-ct-aft-vpc
Amazon SNS	Topik	aws-ct-aft-notifications aws-ct-aft-failure-notifications
Amazon EventBridge	Bus peristiwa	aws-ct-aft-events-from-ct-management
Amazon EventBridge	Aturan acara	aws-ct-aft-capture-ct-events aws-ct-aft-lambda-account-request-processor
Layanan Manajemen Kunci (KMS)	Kunci yang Dikelola Pelanggan	*-aws-ct-aft-* aws-ct-aft-*
AWS Systems Manager	Menyimpan parameter	/aws-ct-aft/account/* /aws/ct-aft/config/*
Amazon SQS	Antrean	aws-ct-aft-account-request.fifo aws-ct-aft-account-request-dlg.fifo
CloudWatch	Grup log	/aws/*/aws-ct-aft-* aws-ct-aft-*
AWS Support Center (Opsional)	Paket Support	Enterprise

AWS akun yang disediakan melalui AWS Control Tower Account Factory untuk Terraform

AWS layanan	Jenis 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	Jenis sumber daya	Nama sumber daya
AWS Identity and Access Management	Peran	AWSAFTExecutionRole AWSAFTExecution aws-ct-aft-controltower-events-rule
AWS Systems Manager	Menyimpan parameter	/aws-ct-aft/account/aws-ct-aft-management/account-id
AWS Organizations (Opsional)	Kebijakan Kontrol Layanan	aws-ct-aft-protect-resources
CloudTrail (Opsional)	Jejak	aws-ct-aft-BaselineCloudTrail
Pusat Dukungan AWS (Opsional)	Paket Support	Enterprise

Akun arsip log AWS Control Tower

AWS layanan	Jenis sumber daya	Nama sumber daya
AWS Identity and Access Management	Peran	AWSAFTExecutionRole AWSAFTExecution

AWS layanan	Jenis sumber daya	Nama sumber daya
		aws-ct-aft-cloudtrail-data-events-role
Layanan Manajemen Kunci (KMS)	Kunci yang Dikelola Pelanggan	*-aws-ct-aft-kms-gd-findings
Amazon S3	Bucket	*-aws-ct-aft-logs* aws-ct-aft-s3-access-logs*
AWS Support Center (Opsional)	Paket Support	Enterprise

Akun audit AWS Control Tower

AWS layanan	Jenis sumber daya	Nama sumber daya
AWS Identity and Access Management	Peran	AWSAFTExecutionRole AWSAFTExecution
AWS Support Center (Opsional)	Paket Support	Enterprise

Peran yang dibutuhkan

Secara umum, peran dan kebijakan merupakan bagian dari manajemen identitas dan akses (IAM) di AWS. Lihat Panduan PenggunaAWS IAM untuk informasi lebih lanjut.

AFT membuat beberapa peran dan kebijakan IAM dalam manajemen AFT dan akun manajemen AWS Control Tower untuk mendukung pengoperasian pipeline AFT. Peran ini dibuat berdasarkan model akses hak istimewa terkecil, yang membatasi izin untuk kumpulan tindakan dan sumber daya minimal yang diperlukan untuk setiap peran dan kebijakan. Peran dan kebijakan ini diberikan `key:value` pasangan AWS tag, seperti `managed_by:AFT` untuk identifikasi.

Selain peran IAM ini, AFT menciptakan tiga peran penting:

- `AWSAFTAdmin`peran
- `AWSAFTExecution`peran
- `AWSAFTService`peran

Peran ini dijelaskan di bagian berikut.

AWSAFTAdmin Peran tersebut, 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 dapat melakukan tindakan yang terkait dengan penyediaan dan penyesuaian akun.

Berikut adalah kebijakan inline (artefak JSON) yang dilampirkan pada peran: `AWSAFTAdmin`

```
{
    "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 peran tersebut. `AWSAFTAdmin` Nomor placeholder diganti dengan nomor `012345678901` ID akun manajemen AFT.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:root"
      },
```

```
      "Action": "sts:AssumeRole"
    }
  ]
}
```

AWSAFTExecution Peran tersebut, dijelaskan

Saat Anda menerapkan AFT, `AWSAFTExecution` peran tersebut dibuat di manajemen AFT dan akun manajemen AWS Control Tower. Kemudian, pipeline AFT menciptakan `AWSAFTExecution` peran di setiap akun yang disediakan AFT selama tahap penyediaan akun AFT.

AFT menggunakan `AWSControlTowerExecution` peran awalnya, untuk membuat `AWSAFTExecution` peran dalam akun tertentu. `AWSAFTExecution`Peran ini memungkinkan pipeline AFT untuk menjalankan langkah-langkah yang dilakukan selama tahap 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 awal sumber daya Anda. Ingatlah bahwa `AWSAFTService` peran tersebut dimaksudkan untuk penyediaan akun, dan `AWSAFTExecution` peran tersebut ditujukan 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 yang dikelola AWS

Artefak JSON berikut menunjukkan kebijakan IAM (hubungan kepercayaan) yang melekat pada peran tersebut. `AWSAFTExecution` Nomor placeholder diganti dengan nomor `012345678901` ID akun manajemen AFT.

Kebijakan kepercayaan untuk `AWSAFTExecution`

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

```
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::012345678901:role/AWSAFTAdmin"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

AWSAFTService Peran tersebut, dijelaskan

`AWSAFTService`Peran ini menyebarkan sumber daya AFT di semua akun yang terdaftar dan dikelola, termasuk akun bersama dan akun manajemen. Sumber daya sebelumnya hanya digunakan oleh peran tersebut. `AWSAFTExecution`

`AWSAFTService`Peran ini dimaksudkan untuk digunakan oleh infrastruktur layanan untuk menyebarkan sumber daya selama tahap penyediaan, dan `AWSAFTExecution` peran tersebut 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 yang dikelola AWS

Artefak JSON berikut menunjukkan kebijakan IAM (hubungan kepercayaan) yang melekat pada peran tersebut. `AWSAFTService` Nomor placeholder diganti dengan nomor `012345678901` ID akun manajemen AFT.

Kebijakan kepercayaan untuk `AWSAFTService`

```
{
  "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 layanan AWS yang diperlukan oleh pipeline AFT. AFT juga membuat bucket S3 backend Terraform, di Wilayah AWS primer dan sekunder, untuk menyimpan status Terraform yang dihasilkan selama alur kerja pipeline AFT.
- Amazon Simple Notification Service — AFT membuat topik Amazon Simple Notification Service (SNS) di akun manajemen AFT, yang menyimpan notifikasi 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 untuk 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 paket Terraform untuk kode sumber AFT dalam berbagai tahap pembuatan.
- AWS CodePipeline — AFT membuat CodePipeline pipeline AWS di akun manajemen AFT untuk diintegrasikan dengan penyedia CodeStar koneksi AWS yang Anda pilih 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.

- AWS Systems Manager Parameter Store — AFT menyiapkan AWS Systems Manager Parameter Store 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 pipeline 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 di akun manajemen AFT ke dalam lingkungan jaringan terpisah, untuk meningkatkan keamanan.
- AWS KMS — AFT menggunakan AWS Key Management Service (KMS) AWS 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 memiliki rotasi tahunan yang diaktifkan secara default.
- AWS Identity and Access Management (IAM) — AFT mengikuti model Least Privilege yang direkomendasikan. Ini menciptakan peran dan kebijakan AWS Identity and Access Management (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 pipeline AFT.
- AWS Step Functions — AFT membuat mesin status AWS Step Functions di akun manajemen AFT. Mesin status ini mengatur dan mengotomatiskan proses dan langkah-langkah untuk kerangka kerja dan penyesuaian penyediaan akun AFT.
- 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 AWS di manajemen AFT dan akun manajemen AWS Control Tower, yang memicu beberapa langkah yang diperlukan selama menjalankan alur kerja pipeline AFT
- AWS CloudTrail (Opsional) — Saat fitur ini diaktifkan, AFT membuat jejak CloudTrail organisasi AWS 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 Support (Opsional) — Saat fitur ini diaktifkan, AFT mengaktifkan paket AWS Enterprise Support untuk akun yang disediakan oleh AFT. Secara default, akun AWS dibuat dengan paket AWS Basic Support diaktifkan.

Pipa penyediaan akun AFT

Setelah tahap penyediaan akun pipa selesai, kerangka kerja AFT berlanjut. Ini 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 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 AWSAFTExecutionIAM di akun yang baru disediakan. AFT mengasumsikan 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 penerapan AFT.
7. Menerapkan kustomisasi penyediaan akun AFT yang Anda berikan. Bagian selanjutnya menceritakan lebih lanjut tentang cara mengatur penyesuaian ini dengan mesin status AWS Step Functions, di repositori. `git` Tahap ini kadang-kadang disebut sebagai tahap kerangka 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 berjalan untuk melakukan tahap (berikutnya, global)Kustomisasi akun.
9. Memanggil pipeline penyesuaian akun untuk setiap akun yang disediakan (dan ditargetkan).
10. Mengirim pemberitahuan keberhasilan atau kegagalan ke topik SNS, dari mana Anda dapat mengambil pesan.

Siapkan kustomisasi 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. Kustomisasi kerangka kerja

penyediaan akun ini diterapkan pada setiap akun yang disediakan, sebelum tahap kustomisasi 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 kerja penyediaan akun AFT memanggil mesin status AWS Step Functions, yang Anda tentukan, untuk mengimplementasikan penyesuaian Anda. Lihat dokumentasi AWS Step Functions untuk mempelajari lebih lanjut tentang kemungkinan integrasi mesin status.

Berikut adalah beberapa integrasi umum.

- AWS Lambda berfungsi dalam bahasa pilihan Anda
- Tugas AWS ECS atau AWS Fargate, menggunakan kontainer Docker
- Aktivitas AWS Step Functions menggunakan pekerja khusus, yang dihosting baik di AWS maupun di tempat
- Integrasi Amazon SNS atau SQS

Jika tidak ada mesin status AWS Step Functions yang ditentukan, tahap akan berlalu dengan no-op. Untuk membuat mesin status penyesuaian penyediaan akun AFT, ikuti petunjuk di. Buat mesin status penyesuaian penyediaan akun AFT Anda Sebelum Anda menambahkan kustomisasi, pastikan Anda memiliki prasyarat di tempat.

Jenis integrasi ini bukan bagian dari AWS Control Tower, dan tidak dapat ditambahkan selama tahap pra-API global penyesuaian 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 sepenuhnya dikerahkan. 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 Langkah-langkah pasca-penerapan.

Buat mesin status penyesuaian penyediaan akun AFT Anda

Langkah 1: Ubah definisi mesin negara

Ubah contoh definisi mesin `customizations.asl.json` negara. Contoh ini tersedia di `git` repositori yang Anda siapkan untuk menyimpan kustomisasi penyediaan akun AFT, dalam langkah pasca-penerapan Anda. Lihat Panduan Pengembang AWS Step Functions untuk mempelajari lebih lanjut 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 khusus Anda. Misalnya, jika Anda memilih untuk memanggil fungsi Lambda dalam definisi tugas mesin status 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 dan penyesuaian penyediaan akun AFT

AFT menjalankan kerangka kerja penyediaan akun dan langkah-langkah penyesuaian untuk setiap akun yang dijual melalui pipeline 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.

Ikhtisar

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, lihatMemanggil kembali 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.
- `git`Repositori terisi sebelumnya untuk penyesuaian global dan penyesuaian akun di lingkungan Anda. Lihat Langkah 3: Isi setiap repositori Langkah-langkah pasca-penerapan untuk informasi lebih lanjut.

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 di bawah folder api_helpers/python 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 penyesuaian 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 folder ***[account_customizations_name] /api_helpers/python*** yang ada 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.

Memanggil kembali 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. event-source-based Pemanggilan ulang memungkinkan Anda untuk 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 mengaktifkan kembali penyesuaian untuk akun yang disediakan AFT.

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 akun yang disediakan AFT.

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 akun yang disediakan AFT akan dipanggil kembali.

> **Note**
>
> Jika versi AWS Control Tower 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.

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 *“ID AKUN-AKUN ANDA” 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.

Alternatif untuk kontrol versi kode sumber di AFT

AFT secara native menggunakan AWS CodeCommit sistem kontrol versi kode sumber (VCS), tetapi memungkinkan CodeConnectionsyang lain yang memenuhi persyaratan bisnis Anda atau arsitektur yang ada. Anda dapat menentukan VCS pihak ketiga sebagai bagian dari prasyarat penerapan AFT.

AFT mendukung alternatif kontrol kode sumber berikut:

- GitHub
- GitHub Server Perusahaan
- BitBucket

Jika Anda memilih AWS CodeCommit sebagai VCS Anda, tidak ada langkah tambahan yang diperlukan. Secara default, 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 yang didukung AFT 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 penyesuaian 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"`,, atau `"github""githubenterprise"`, berdasarkan kasus penggunaan Anda.
- github_enterprise_url: Hanya untuk pelanggan GitHub Enterprise, tentukan URL-nya. GitHub
- account_request_repo_name: Secara default, nilai ini diatur untuk pengguna. `aft-account-request` AWS CodeCommit Jika Anda membuat repositori dengan nama baru di CodeCommit atau di lingkungan penyedia VCS pihak ketiga yang didukung AFT, perbarui nilai input ini dengan nama repositori Anda yang sebenarnya. Untuk BitBucket, Github, dan GitHub Enterprise, nama repositori harus memiliki format. `[Org]/[Repo]`
- account_customizations_repo_name: Secara default, nilai ini diatur untuk pengguna. `aft-account-customizations` AWS CodeCommit Jika Anda membuat repositori dengan nama baru di CodeCommit atau di lingkungan penyedia VCS pihak ketiga yang didukung AFT, perbarui nilai input ini dengan nama repositori Anda. Untuk BitBucket, Github, dan GitHub Enterprise, nama repositori harus memiliki format. `[Org]/[Repo]`
- account_provisioning_customizations_repo_name: Secara default, nilai ini diatur untuk pengguna. `aft-account-provisioning-customizations` AWS CodeCommit Jika Anda membuat repositori dengan nama baru di AWS CodeCommit atau di lingkungan penyedia VCS pihak ketiga yang didukung AFT, perbarui nilai input ini dengan nama repositori Anda. Untuk BitBucket, Github, dan GitHub Enterprise, nama repositori harus memiliki format. `[Org]/[Repo]`
- global_customizations_repo_name: Secara default, nilai ini diatur untuk pengguna. `aft-global-customizations` AWS CodeCommit Jika Anda membuat repositori dengan nama baru di CodeCommit atau di lingkungan penyedia VCS pihak ketiga yang didukung AFT, perbarui nilai input ini dengan nama repositori Anda. Untuk BitBucket, Github, dan GitHub Enterprise, 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.

Langkah 3: Selesaikan AWS CodeStar koneksi untuk penyedia VCS pihak ketiga

Saat penerapan Anda berjalan, AFT membuat AWS CodeCommit repositori yang diperlukan, atau membuat AWS CodeStar 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 AWS CodeStar koneksi yang tertunda. Lihat AWS CodeStar dokumentasi untuk instruksi lebih lanjut tentang menyelesaikan AWS CodeStar koneksi.

Perlindungan data

Model tanggung jawabAWS bersama berlaku untuk perlindungan data di AFT. Untuk tujuan perlindungan data, kami merekomendasikan praktik terbaik berikut untuk keamanan.

- Ikuti pedoman Perlindungan Data yang disediakan oleh AWS Control Tower. Untuk detailnya, lihat Perlindungan Data di AWS Control Tower.
- Pertahankan konfigurasi status Terraform yang dihasilkan pada saat penerapan AFT. Untuk detailnya, lihat Terapkan AWS Control Tower Account Factory untuk Terraform (AFT).
- Putar kredenal sensitif secara berkala seperti yang diarahkan oleh kebijakan keamanan organisasi Anda. Contoh rahasia adalah token Terraform, `git` token, dan sebagainya.

Enkripsi saat istirahat

AFT membuat bucket Amazon S3, topik Amazon SNS, antrian Amazon SQS, dan database Amazon DynamoDB yang dienkripsi saat istirahat dengan kunci Layanan Manajemen Kunci. AWS Kunci KMS yang dibuat oleh AFT memiliki rotasi tahunan yang diaktifkan secara default. Jika Anda memilih distribusi Terraform Cloud atau Terraform Enterprise dari Terraform, AFT menyertakan SecureString parameter AWS Systems Manager untuk menyimpan nilai token Terraform yang sensitif.

AFT menggunakan AWS layanan yang dijelaskan dalam Layanan komponen yang, secara default, dienkripsi saat istirahat. Untuk detailnya, lihat AWS dokumentasi untuk setiap AWS layanan komponen AFT, dan pelajari tentang praktik perlindungan data yang diikuti oleh setiap layanan.

Enkripsi dalam perjalanan

AFT bergantung pada AWS layanan yang dijelaskan dalam Layanan komponen yang menggunakan enkripsi dalam perjalanan, 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 Terraform Cloud 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 akan 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 PanduanAWS Billing Pengguna.

Untuk menghapus akun dari saluran 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 Terraform Cloud 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 kustomisasi, dan status penyesuaian global

   Contoh: Terraform Cloud atau Terraform Enterprise

   Saat Anda memilih Terraform Cloud atau Terraform Enterprise, Anda menemukan folder untuk setiap akun di bucket Amazon `aft-backend-`*`012345678901`*`-primary-region` `aft-backend-`*`012345678901`*`-secondary-region` S3 dan Amazon. Folder ini terkait dengan status pipeline kustomisasi.

Metrik operasional

Secara default, Account Factory for Terraform (AFT) mengirimkan metrik operasional anonim ke. AWSKami 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 KebijakanAWS 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
    }
```

Account Factory untuk panduan pemecahan masalah Terraform (AFT)

Bagian ini dapat membantu Anda memecahkan masalah umum yang mungkin Anda temui saat menggunakan Account Factory for Terraform (AFT).

Topik

Masalah umum

- Melebihi AWS kuota sumber daya

  Jika grup log Anda menunjukkan bahwa Anda melebihi kuota AWS sumber daya, hubungi Support AWS . Account Factory menggunakan Layanan AWS kuota sumber daya yang mencakup AWS CodeBuild, AWS Organizations, dan AWS Systems Manager. Untuk informasi selengkapnya, lihat berikut ini:

  - Apa itu AWS CodeBuild? dalam CodeBuild User Guide.
  - Apa itu AWS Organizations? dalam Panduan Pengguna Organizations.
  - Apa itu AWS Systems Manager? dalam Panduan Pengguna Systems Manager.
- 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 dengan upaya terbaik.

- Izin peran Account Factory tidak mencukupi

  Account Factory membuat peran dan kebijakan IAM untuk mengelola penyebaran dan penyesuaian akun vended. Jika Anda mengubah peran atau kebijakan ini, saluran Account Factory mungkin tidak dapat melakukan tindakan tertentu. Untuk informasi selengkapnya, lihat Peran 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 drift secara otomatis. Untuk informasi tentang menyelesaikan drift, lihat Mendeteksi dan menyelesaikan drift di AWS Control Tower.

  Drift tidak terdeteksi ketika unit organisasi (OU) diubah secara manual. Hal ini disebabkan 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 Service Catalog (layanan yang mengelola detail akun). Jika Anda mengubah OU secara manual, drift tidak terdeteksi karena permintaan akun tidak berubah.

Masalah yang terkait dengan penyediaan/pendaftaran akun

- Permintaan akun (alamat email/nama) sudah ada

  Masalah ini biasanya mengakibatkan kegagalan produk Service Catalog 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 Log Anda.
  - Tinjau kegagalan yang dipancarkan ke topik Amazon SNS. `aft-failure-notifications`
- Permintaan akun yang salah

  Pastikan permintaan akun Anda mengikuti skema yang diharapkan. Sebagai contoh, lihat terraform-aws-control_tower_account_factory di. GitHub
- Kuota sumber daya Exceeded AWS Organizations

  Pastikan permintaan akun Anda tidak melebihi kuota AWS Organizations sumber daya. Untuk informasi selengkapnya, lihat Quotas for AWS Organizations.

Masalah yang terkait dengan pemanggilan kustomisasi

- Akun target tidak dionboard ke Account Factory

  Pastikan semua akun yang disertakan dalam permintaan kustomisasi telah di-onboard ke Account Factory. Untuk informasi selengkapnya, lihat Memperbarui akun yang sudah ada.
- Akun yang menargetkan permintaan kustomisasi ada di **`aft-request-metadata`** tabel DynamoDB, tetapi tidak di repositori permintaan akun

  Format permintaan permintaan kustomisasi Anda untuk mengecualikan akun yang melanggar dengan melakukan salah satu hal berikut:
  - Di `aft-request-metadata` tabel DynamoDB, hapus entri yang mereferensikan akun yang tidak lagi ada di repositori permintaan akun Anda.
  - Tidak menggunakan “semua” sebagai target.
  - Tidak menargetkan OU yang menjadi milik akun tersebut.
  - Tidak menargetkan akun secara langsung.
- Menggunakan token yang salah untuk Terraform Cloud

  Pastikan Anda mengatur token yang benar. Terraform Cloud 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 kustomisasi akun

Jika Anda mengalami masalah terkait alur kerja penyesuaian akun, pastikan versi AFT Anda 1.8.0 atau lebih tinggi, dan Anda menghapus semua instance metadata terkait akun dari tabel permintaan DynamoDB Anda.

Untuk informasi tentang AFT versi 1.8.0, lihat Rilis 1.8.0 di. 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 penyesuaian. Untuk informasi selengkapnya, lihat Pemecahan masalah dengan penelusuran 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 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.

Untuk kontrol yang merupakan bagian dari Standar AWS Security Hub yang Dikelola Layanan: 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: Penyimpangan akun dan drift SCP 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.
- Jika akun dipindahkan antara sumber dan tujuan yang sama OU beberapa kali, tanpa memperbaiki drift terlebih dahulu, satu notifikasi dikirim, meskipun akun tersebut berpindah di antara OU tersebut lebih dari satu kali.

Jenis penyimpangan akun

- Akun dipindahkan antara OU
- 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.

Jenis penyimpangan kebijakan

- SCP diperbarui
- SCP melekat pada OU
- SCP terlepas dari OU
- SCP dilampirkan ke akun

Untuk informasi selengkapnya, lihat Tipe of Governance Drift.

Menyelesaikan drift

Meskipun deteksi otomatis, langkah-langkah untuk menyelesaikan penyimpangan harus dilakukan melalui konsol.

- 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 300 akun, Anda dapat menyelesaikan penyimpangan di akun yang disediakan Account Factory, atau drift SCP, dengan memilih Registrasi ulang OU 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.

⚠ Saat Anda mengambil tindakan untuk mengatasi drift pada versi landing zone, dua perilaku dimungkinkan.

- Jika Anda menggunakan versi landing zone terbaru, ketika Anda memilih Reset dan kemudian memilih Konfirmasi, sumber daya zona pendaratan drifted Anda diatur ulang ke konfigurasi AWS Control Tower yang disimpan. Versi landing zone tetap sama.
- Jika Anda tidak menggunakan versi terbaru, Anda harus memilih Perbarui. Landing zone ditingkatkan ke versi landing zone terbaru. Drift diselesaikan sebagai bagian dari proses ini.

Pertimbangan tentang pemindaian drift dan SCP

AWS Control Tower memindai SCP terkelola Anda setiap hari untuk memverifikasi bahwa kontrol yang sesuai diterapkan dengan benar dan tidak hanyut. Untuk mengambil SCP dan menjalankan pemeriksaan, 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 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 sepertiRate 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 yang Diperlukan untuk Menggunakan AWS Control Tower Console.
- Jangan hapus semua OU Tambahan: Jika Anda menghapus unit organisasi yang awalnya bernama Sandbox selama penyiapan landing zone oleh AWS Control Tower, landing zone Anda akan berada dalam keadaan drift, tetapi Anda masih dapat menggunakan AWS Control Tower. 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, seperti menghapus akun logging dari Security OU, landing zone Anda akan berada dalam keadaan drift. Landing zone harus disetel ulang sebelum Anda dapat melanjutkan menggunakan konsol AWS Control Tower.

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 yang Diizinkan di Luar AWS Control Tower Console

- Ubah nama OU terdaftar.
- Ubah nama Security OU.
- Ubah nama akun anggota di OU non-dasar.

- Ubah nama akun bersama AWS Control Tower di OU Keamanan.
- 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 dengan AWS Service Catalog 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 Drift 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:

- Akun Anggota yang Dipindahkan
- Akun Anggota yang Dihapus
- Pembaruan Tidak Direncanakan ke SCP Terkelola
- SCP Terlampir pada Akun Anggota
- SCP Terlampir ke OU Terkelola
- SCP Terpisah dari OU Terkelola
- Dihapus Foundational OU
- Drift kontrol Security Hub

- Akses tepercaya dinonaktifkan

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.

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 drift, lihat Jangan menghapus peran yang diperlukan di bagian yang dipanggilJenis drift untuk segera diselesaikan.

AWS Control Tower tidak mencari penyimpangan terkait layanan lain yang bekerja dengan akun manajemen, termasuk CloudTrail CloudWatch, Pusat Identitas IAM,, AWS CloudFormation AWS Config, dan sebagainya. Tidak ada deteksi drift yang tersedia di akun anak, karena akun ini dilindungi oleh kontrol wajib preventif.

Namun, ia melaporkan penyimpangan terkait kontrol yang merupakan bagian dari Standar yang AWS Security Hub dikelola Layanan: AWS Control Tower.

Akun Anggota yang Dipindahkan

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. Berikut ini adalah contoh notifikasi Amazon SNS 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 300 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 300 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 Daftar ulang untuk OU yang berisi akun (opsi tercepat untuk beberapa akun). Untuk informasi selengkapnya, lihat Daftarkan unit organisasi yang ada dengan AWS Control Tower.
- Memperbarui produk yang disediakan di Account Factory. Untuk informasi selengkapnya, lihat Perbarui dan pindahkan akun pabrik akun dengan AWS Control Tower atau dengan AWS Service Catalog.

  > **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 300 akun, resolusi drift mungkin tergantung pada jenis akun mana yang telah dipindahkan, seperti yang dijelaskan dalam paragraf berikutnya. Untuk informasi selengkapnya, lihat Perbarui Zona Pendaratan Anda.
  - Jika akun yang disediakan Account Factory dipindahkan - Di OU dengan kurang dari 300 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 300 akun, Anda harus menyelesaikan penyimpangan dengan membuat pembaruan ke setiap akun yang dipindahkan, baik melalui konsol AWS Control Tower atau produk yang disediakan karena registrasi ulang OU tidak akan melakukan pembaruan. Untuk informasi selengkapnya, lihat Perbarui dan pindahkan akun pabrik akun dengan AWS Control Tower atau dengan AWS Service Catalog.

- 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 Zona Pendaratan Anda.

> ⚠ Nama bidang yang tidak digunakan lagi
>
> Nama bidang `MasterAccountID` telah diubah `ManagementAccountID` untuk mematuhi AWS pedoman. Nama lama sudah usang. Mulai tahun 2022, skrip yang berisi nama bidang yang tidak digunakan lagi tidak akan berfungsi lagi.

Akun Anggota yang Dihapus

Jenis penyimpangan ini dapat terjadi ketika akun anggota dihapus dari unit organisasi AWS Control Tower terdaftar. Contoh berikut menunjukkan notifikasi Amazon SNS saat jenis drift ini 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 Perbarui dan pindahkan akun pabrik akun dengan AWS Control Tower atau dengan AWS Service Catalog.

- 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 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 Amazon SNS 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 300 akun, Anda dapat menyelesaikannya dengan:

- Menavigasi ke halaman Organisasi di konsol AWS Control Tower untuk mendaftarkan ulang OU (opsi tercepat). Untuk informasi selengkapnya, lihat Daftarkan unit organisasi yang ada dengan AWS Control Tower.
- Memperbarui landing zone Anda (opsi lebih lambat). Untuk informasi selengkapnya, lihat Perbarui Zona Pendaratan Anda.

Ketika jenis drift ini terjadi di OU dengan lebih dari 300 akun, selesaikan dengan memperbarui landing zone Anda. Untuk informasi selengkapnya, lihat Perbarui Zona Pendaratan Anda.

SCP Terlampir ke OU Terkelola

Jenis drift ini dapat terjadi ketika SCP untuk kontrol terpasang ke OU lainnya. Kejadian ini sangat umum terjadi saat Anda mengerjakan OU Anda dari luar konsol AWS Control Tower. Berikut ini adalah contoh notifikasi Amazon SNS saat jenis drift ini terdeteksi.

```
{
  "Message" : "AWS Control Tower has detected that the managed service control
 policy 'aws-guardrails-012345 (p-tEXAMPLE)' has been attached to 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-ou'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_ATTACHED_TO_OU",
  "RemediationStep" : "Update Control Tower Setup",
  "OrganizationalUnitId" : "ou-0123-1EXAMPLE",
  "PolicyId" : "p-tEXAMPLE"
}
```

Resolusi

Ketika jenis penyimpangan ini terjadi di OU dengan hingga 300 akun, Anda dapat menyelesaikannya dengan:

- Menavigasi ke halaman Organisasi di konsol AWS Control Tower untuk mendaftarkan ulang OU (opsi tercepat). Untuk informasi selengkapnya, lihat Daftarkan unit organisasi yang ada dengan AWS Control Tower.

- Memperbarui landing zone Anda (opsi lebih lambat). Untuk informasi selengkapnya, lihat Perbarui Zona Pendaratan Anda.

Ketika jenis drift ini terjadi di OU dengan lebih dari 300 akun, selesaikan dengan memperbarui landing zone Anda. Untuk informasi selengkapnya, lihat Perbarui Zona Pendaratan Anda.

SCP Terpisah 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 Amazon SNS 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 300 akun, Anda dapat menyelesaikannya dengan:

- Menavigasi ke OU di konsol AWS Control Tower untuk mendaftarkan ulang OU (opsi tercepat). Untuk informasi selengkapnya, lihat Daftarkan 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 Zona Pendaratan Anda.

Ketika jenis drift ini terjadi di OU dengan lebih dari 300 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 Zona Pendaratan Anda.

SCP Terlampir pada Akun Anggota

Jenis drift ini dapat terjadi ketika SCP untuk kontrol dilampirkan ke akun di konsol Organizations. Guardrail dan SCP mereka dapat diaktifkan di OU (dan dengan demikian diterapkan ke semua akun terdaftar OU) melalui konsol AWS Control Tower. Berikut ini adalah contoh notifikasi Amazon SNS saat jenis drift ini terdeteksi.

```
{
  "Message" : "AWS Control Tower has detected that the managed service control policy
 'aws-guardrails-012345 (p-tEXAMPLE)' has been attached to the member account 'account-
email@amazon.com (012345678909)'. For more information, including steps to resolve this
 issue, see 'https://docs.aws.amazon.com/console/controltower/scp-detached-account'",
  "ManagementAccountId" : "012345678912",
  "OrganizationId" : "o-123EXAMPLE",
  "DriftType" : "SCP_ATTACHED_TO_ACCOUNT",
  "RemediationStep" : "Re-register this organizational unit (OU)",
  "AccountId" : "012345678909",
  "PolicyId" : "p-tEXAMPLE"
}
```

Resolusi

Jenis penyimpangan ini terjadi pada akun daripada OU.

Ketika jenis drift ini terjadi untuk akun di Foundational OU, seperti Security OU, resolusinya adalah memperbarui landing zone Anda. Untuk informasi selengkapnya, lihat Perbarui Zona Pendaratan Anda.

Ketika jenis penyimpangan ini terjadi di OU non-dasar dengan hingga 300 akun, Anda dapat menyelesaikannya dengan:

- Melepaskan AWS Control Tower SCP dari akun pabrik akun.

- Menavigasi ke OU di konsol AWS Control Tower untuk mendaftarkan ulang OU (opsi tercepat). Untuk informasi selengkapnya, lihat Daftarkan unit organisasi yang ada dengan AWS Control Tower.

Ketika jenis penyimpangan ini terjadi di OU dengan lebih dari 300 akun, Anda dapat mencoba menyelesaikannya dengan memperbarui konfigurasi pabrik akun untuk akun tersebut. Mungkin tidak mungkin untuk menyelesaikannya dengan sukses. Untuk informasi selengkapnya, lihat Perbarui Zona Pendaratan 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 notifikasi Amazon SNS 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

Drift kontrol Security Hub

Jenis drift ini terjadi ketika kontrol yang merupakan bagian dari AWS Security Hub Service-Managed Standard: AWS Control Tower melaporkan keadaan drift. AWS Security Hub Layanan itu sendiri tidak melaporkan keadaan drift untuk kontrol ini. Sebagai gantinya, layanan mengirimkan temuannya ke AWS Control Tower.

Drift kontrol Security Hub juga dapat dideteksi jika AWS Control Tower belum menerima pembaruan status dari Security Hub lebih dari 24 jam. Jika temuan tersebut tidak diterima seperti yang diharapkan, AWS Control Tower memverifikasi bahwa kontrol dalam drift. Contoh berikut menunjukkan notifikasi Amazon SNS 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" : "PYBETSAGNUZB",
"ControlName" : "EBS snapshots should not be publicly restorable",
"ApiControlIdentifier" : "arn:aws:controltower:us-east-1::control/PYBETSAGNUZB",
"Region" : "us-east-1"
}
```

Resolusi

Untuk OU dengan kurang dari 300 akun, resolusinya adalah mendaftarkan ulang OU, yang mengatur ulang kontrol ke keadaan semula. Untuk OU apa pun, 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 Amazon SNS

Berikut ini adalah contoh notifikasi Amazon SNS 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.

Jika Anda mengelola sumber daya di luar AWS Control Tower

AWS Control Tower menyiapkan akun, unit organisasi, dan sumber daya lainnya atas nama Anda, tetapi Anda adalah pemilik sumber daya ini. Anda dapat mengubah sumber daya ini di 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 mendamaikan 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 landing zone Anda, untuk memperbarui informasi yang ditampilkan di konsol AWS Control Tower.

Secara umum, perubahan yang Anda lakukan di luar konsol AWS Control Tower ke sumber daya AWS Control Tower menciptakan status drift yang dapat diselesaikan di landing zone Anda. Untuk informasi lebih lanjut tentang perubahan ini, lihatPerubahan sumber daya yang dapat diperbaiki.

Tugas yang membutuhkan reset landing zone

- Menghapus Keamanan OU (Kasus khusus, tidak boleh dilakukan dengan ringan.)
- Menghapus akun bersama dari Security OU (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 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 membuat perubahan dalam postur tata kelola ketika merekonsiliasi perubahan Anda. Untuk informasi selengkapnya tentang memperbarui produk yang disediakan, lihat Memperbarui 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 mungkin ditampilkan.

Membuat OU

Unit Organisasi (OU) yang dibuat di luar AWS Control Tower disebut sebagai Tidak Terdaftar. Mereka ditampilkan di halaman Organisasi, tetapi tidak diatur oleh kontrol AWS Control Tower.

Membuat akun

Akun yang dibuat di luar AWS Control Tower disebut Unenrolled. 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 mendaftarkan akun, buka halaman Organisasi atau halaman detail Akun di AWS Control Tower dan pilih Daftar 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 Anda menggunakan AWS Service Catalog, Anda juga harus mengatur ulang landing zone Anda untuk memastikan bahwa AWS Control Tower tetap konsisten 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” di. Mendeteksi dan mengatasi penyimpangan di AWS Control Tower

AWS Control Tower menampilkan nama OU pada halaman Organisasi di dasbor AWS Control Tower. Anda dapat melihat kapan operasi reset landing zone Anda telah berhasil.

Mengganti nama akun terdaftar

Setiap AWS akun memiliki nama tampilan yang dapat diubah oleh pengguna root akun di AWS Billing and Cost Management 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 Mengelola AWS akun di Panduan Pengguna AWS Penagihan.

Menghapus Keamanan OU

Jenis drift ini adalah kasus khusus. Jika Anda menghapus Security OU, Anda akan melihat halaman pesan kesalahan, meminta Anda untuk mengatur ulang landing zone Anda. Anda harus mengatur ulang landing zone sebelum dapat melakukan 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 landing zone menciptakan OU Keamanan baru dan memindahkan dua akun bersama ke OU Keamanan baru. AWS Control Tower menandai akun Log Archive dan Audit sebagai drifted. Proses yang sama menyelesaikan penyimpangan di akun ini.

Jika Anda menentukan bahwa Anda harus menghapus OU Keamanan, inilah yang perlu Anda ketahui:

Sebelum Anda dapat menghapus Security OU, Anda harus memastikan tidak mengandung akun. Secara khusus, Anda harus menghapus akun Arsip Log dan Audit dari OU. Kami menyarankan Anda memindahkan akun ini ke OU lain.

> **Note**
>
> Tindakan menghapus OU Keamanan Anda tidak boleh dilakukan tanpa pertimbangan. Tindakan tersebut dapat menimbulkan kekhawatiran kepatuhan jika pencatatan ditangguhkan sementara, dan karena beberapa kontrol mungkin tidak ditegakkan.

Untuk informasi umum tentang drift, lihat “Menyelesaikan Drift” di. Mendeteksi dan mengatasi penyimpangan di AWS Control Tower

Menghapus akun dari Security OU

Kami tidak menyarankan Anda menghapus salah satu akun bersama dari organisasi Anda atau memindahkannya dari Security OU. 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 dijalankan`organizations:InviteAccountToOrganization`. Jika Anda tidak memiliki izin tersebut, ikuti langkah-langkah perbaikan manual, yang menggunakan konsol AWS Control Tower dan konsol. AWS Organizations
- Mulai dari AWS Organizations konsol: Proses remediasi ini adalah prosedur manual yang sedikit lebih lama dan sepenuhnya. Saat mengikuti langkah-langkah perbaikan manual, Anda akan beralih antara AWS Organizations konsol dan konsol AWS Control Tower. Saat bekerja di AWS Organizations, Anda memerlukan pengguna atau peran dengan kebijakan `AWSOrganizationsFullAccess` terkelola atau yang setara. Saat bekerja di konsol AWS Control Tower, Anda memerlukan pengguna atau peran dengan kebijakan `AWSControlTowerServiceRolePolicy` terkelola atau yang setara, dan izin untuk menjalankan semua tindakan AWS Control Tower (controltower: *).
- Jika langkah-langkah remediasi tidak memulihkan akun, hubungi AWS Support.

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 diubah atau dihapus.
- Akun 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 untuk 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 reset 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 dijalankan. `organizations:InviteAccountToOrganization` Jika Anda tidak memiliki izin tersebut, gunakan prosedur remediasi manual yang dijelaskan nanti dalam topik ini.
2. Pada halaman terdeteksi drift zona pendaratan, pilih Undangan Ulang untuk memulihkan penghapusan akun bersama dengan mengundang kembali akun bersama ke dalam organisasi. Email yang dibuat secara otomatis dikirim ke alamat email untuk akun tersebut.
3. Terima undangan untuk membawa akun bersama kembali ke organisasi. Lakukan salah satu hal berikut:
   - Masuk ke akun bersama yang telah dihapus, lalu buka https://console.aws.amazon.com/organizations/home#/invites
   - 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 arahkan ke Undangan.
4. Masuk lagi ke akun manajemen, atau muat ulang konsol AWS Control Tower jika sudah terbuka. Anda akan melihat halaman drift zona pendaratan. Pilih Reset untuk memperbaiki landing zone.
5. Tunggu proses reset selesai.

Jika remediasi berhasil, akun bersama muncul dalam keadaan normal dan kepatuhan.

Jika langkah-langkah remediasi tidak memulihkan akun, hubungi AWS Support.

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 `AWSOrganizationsFullAccess` terkelola atau yang setara.
2. Undang akun bersama kembali ke organisasi. Untuk informasi tentang persyaratan, prasyarat, dan prosedur untuk mengundang akun AWS Organizations, lihat Mengundang akun ke organisasi Anda di AWS Panduan Pengguna.AWS Organizations

3. Masuk ke akun bersama yang telah dihapus, lalu buka https://console.aws.amazon.com/organizations/home#/invites untuk menerima undangan.
4. Masuk lagi ke akun manajemen.
5. Masuk ke konsol AWS Control Tower sebagai pengguna atau peran dengan kebijakan `AWSControlTowerServiceRolePolicy` terkelola atau yang setara, dan izin untuk menjalankan semua tindakan AWS Control Tower (controltower: *).
6. Anda akan melihat halaman drift zona pendaratan dengan opsi untuk mengatur ulang landing zone. Pilih Reset untuk memperbaiki landing zone.
7. Tunggu proses reset selesai.

Jika remediasi berhasil, akun bersama muncul dalam keadaan normal dan kepatuhan.

Jika langkah-langkah remediasi tidak memulihkan akun, hubungi AWS Support.

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 seperti yang dipersyaratkan oleh pengalaman konsol. Oleh karena itu, alamat email akun bersama dan 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 semua AWS Config aturan yang diterapkan 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 dari AWS Organizations saat OU dihapus. Ini memperbarui daftar OU di Account Factory, sehingga daftar OU terdaftar tetap konsisten.

> **Note**
>
> Di AWS Service Catalog, Account Factory diperbarui untuk menghapus OU yang dihapus dari daftar OU yang tersedia di mana Anda dapat menyediakan akun.

Menghapus akun terdaftar dari OU

Saat Anda menghapus akun yang terdaftar, AWS Control Tower menerima pemberitahuan dan membuat pembaruan, sehingga informasinya 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, pergi ke AWS Service Catalog, pilih produk yang disediakan, dan kemudian pilih Terminate.

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 ada yang dibuat di luar AWS Control Tower, Anda dapat membawanya ke tata kelola AWS Control Tower.

Untuk akun yang ada AWS Organizations dan AWS akun, sebagian besar pelanggan lebih suka mendaftarkan grup akun dengan mendaftarkan seluruh unit organisasi (OU) yang berisi akun. Anda juga dapat mendaftarkan akun satu per satu. Untuk informasi selengkapnya tentang mendaftarkan akun individual, lihatDaftarkan yang sudah ada Akun AWS.

Terminologi

- Saat Anda membawa organisasi yang ada ke AWS Control Tower, itu disebut mendaftarkan organisasi, atau memperluas tata kelola ke organisasi.
- Saat Anda membawa AWS akun ke AWS Control Tower, itu disebut mendaftarkan akun.

Lihat OU dan akun Anda

Pada halaman AWS Control Tower Organization, 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 status OU atau pendaftaran di AWS Control Tower. Cara mudah untuk melihat akun Anda di halaman Organisasi adalah dengan memilih Akun hanya dari menu tarik-turun 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 akan menampilkan akun dan OU Anda dalam hierarki. Ini adalah lokasi sentral untuk memantau dan mengambil tindakan pada semua sumber daya AWS Control Tower Anda. Untuk informasi lebih lanjut tentang halaman Organisasi, Anda dapat melihat panduan video.

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. Captioning tersedia.

Panduan Video Bekerja dengan Halaman Organisasi di AWS Control Tower.

Topik

- Daftarkan unit organisasi yang ada dengan AWS Control Tower
- Daftarkan yang sudah ada Akun AWS

Memperluas tata kelola ke organisasi yang ada

Anda dapat menambahkan tata kelola AWS Control Tower ke organisasi yang sudah ada dengan menyiapkan landing zone (LZ) sebagaimana diuraikan dalam Panduan Pengguna AWS Control Tower di Memulai, Langkah 2.

Inilah yang diharapkan saat Anda menyiapkan landing zone AWS Control Tower di organisasi yang sudah ada.

- Anda dapat memiliki satu landing zone per AWS Organizations organisasi.
- AWS Control Tower menggunakan akun manajemen dari AWS Organizations organisasi Anda yang ada sebagai akun pengelolaannya. 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 meluncurkan landing zone atau mendaftarkan OU, kontrol AWS Control Tower berlaku secara otomatis ke semua akun yang terdaftar di OU tersebut.
- Anda dapat Mendaftarkan AWS akun tambahan yang ada ke dalam 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 ada.

Untuk memeriksa prasyarat lain untuk pendaftaran dan pendaftaran, lihat Memulai AWS Control Tower.

Berikut detail selengkapnya tentang bagaimana kontrol AWS Control Tower tidak berlaku untuk OU Anda di organisasi AWS yang tidak menyiapkan zona pendaratan AWS Control Tower:

- Akun baru yang dibuat di luar AWS Control Tower Account Factory tidak terikat oleh kontrol OU yang terdaftar.
- Akun baru yang dibuat di OU yang tidak terdaftar di AWS Control Tower tidak terikat oleh kontrol, kecuali jika Anda secara khusus Mendaftarkan akun tersebut ke AWS Control Tower. Lihat Daftarkan yang sudah ada Akun AWS untuk informasi selengkapnya tentang mendaftarkan akun.
- Organisasi tambahan yang ada, akun yang ada, dan OU baru apa pun atau akun apa pun yang Anda buat di luar AWS Control Tower, tidak terikat oleh kontrol AWS Control Tower, kecuali jika Anda mendaftarkan OU secara terpisah atau mendaftarkan akun.

Untuk informasi selengkapnya tentang cara menerapkan AWS Control Tower ke OU dan akun yang ada, lihatDaftarkan unit organisasi yang ada dengan AWS Control Tower.

Untuk ikhtisar proses penyiapan zona landing zone AWS Control Tower di organisasi Anda yang ada, lihat video di bagian selanjutnya.

> **Note**
>
> Selama penyiapan, AWS Control Tower melakukan pra-pemeriksaan untuk menghindari masalah umum. Namun, jika saat ini Anda menggunakan solusi Zona AWS Pendaratan 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 landing zone Anda saat ini. Juga, lihat Bagaimana jika akun tidak memenuhi prasyarat? informasi tentang memindahkan akun dari satu landing zone ke landing zone lainnya.

Video: Aktifkan Zona Pendaratan yang ada AWS Organizations

Video ini (7:48), menjelaskan cara menyiapkan dan mengaktifkan landing zone AWS Control Tower di AWS Organizations struktur yang ada. Untuk tampilan yang lebih baik, pilih ikon di sudut kanan bawah video untuk memperbesarnya ke layar penuh. Captioning tersedia.

Aktifkan AWS Control Tower untuk organisasi yang ada

Pertimbangan untuk IAM Identity Center 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 IAM Identity Center sudah diaktifkan, dan jika Anda menggunakan IAM Identity Center Directory, AWS Control Tower menambahkan sumber daya seperti set izin, grup, dan sebagainya, dan melanjutkan seperti biasa.
- Jika direktori lain (eksternal, AD, AD Terkelola) disiapkan, AWS Control Tower tidak mengubah konfigurasi yang ada. Untuk detail selengkapnya, lihat Pertimbangan untuk pelanggan AWS IAM Identity Center (IAM Identity Center).

Akses ke AWS layanan lain

Setelah Anda membawa organisasi Anda ke dalam 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 AWS Control Tower

Bab ini mencantumkan ekspektasi 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. Fitur Register and Re-register berfungsi dengan OU bersarang, kecuali untuk perubahan perilaku 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. Captioning tersedia.

Panduan Video Mengelola OU Bersarang di AWS Control Tower.

Untuk panduan mengenai praktik terbaik untuk OU bersarang dan landing zone Anda, lihat posting blog Mengatur zona landing AWS Control Tower Anda dengan OU bersarang.

Perluas dari struktur OU datar ke struktur OU bersarang

Jika Anda membuat landing zone 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 sumber OU (datar) ke OU tujuan (bersarang). Begini caranya:
   a. Pergi ke OU dari mana Anda ingin memindahkan akun.
   b. Pilih semua akun di OU.
   c. Pilih Pindah.

   > **Note**
   >
   > Langkah ini harus dilakukan di AWS Organizations konsol di karena AWS Control Tower tidak memiliki fitur Move.

3. Buka OU bersarang di AWS Control Tower dan Daftar atau daftarkan ulang. Semua akun di OU bersarang akan didaftarkan.
   - Jika Anda membuat OU di AWS Control Tower, daftarkan ulang OU.
   - Jika Anda membuat OU di AWS Organizations, Daftarkan OU untuk pertama kalinya.
4. Setelah akun Anda dipindahkan dan didaftarkan, hapus OU tingkat atas yang kosong, baik dari AWS Organizations konsol atau dari konsol AWS Control Tower.

Pra-cek pendaftaran OU bersarang

Untuk mendukung keberhasilan pendaftaran OU bersarang Anda dan akun anggotanya, AWS Control Tower melakukan serangkaian pra-pemeriksaan. Prakecek yang sama ini dilakukan saat mendaftarkan OU tingkat atas atau OU bersarang. Untuk informasi selengkapnya, lihat Penyebab umum kegagalan saat 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 menyebarkan `AWSControlTowerExecution` peran ke akun di bawah target OU, dan ke akun di semua OU yang bersarang di bawah target OU, bahkan ketika niat Anda adalah mendaftarkan OU target saja. Peran ini memberikan setiap pengguna izin Administrator akun manajemen pada akun apa pun yang memiliki `AWSControlTowerExecution` peran tersebut. Peran tersebut 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 jika Anda mengembalikan peran tersebut ke akun. Untuk menghapus `AWSControlTowerExecution` peran dari akun, Anda harus masuk di bawah `AWSControlTowerExecution` peran, karena tidak ada prinsipal IAM lain yang diizinkan untuk menghapus peran yang dikelola oleh AWS Control Tower.

Untuk informasi tentang cara membatasi akses peran, lihat Ketentuan 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 akan memperbarui semua akun yang 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.
- Mendaftarkan kembali akun anggota terdaftar.
- Membuat login IAM Identity Center untuk akun anggota yang baru terdaftar.

- Memperbarui akun anggota terdaftar yang ada untuk mencerminkan perubahan landing zone Anda.
- Pembaruan kontrol yang dikonfigurasi untuk OU ini dan akun anggotanya.

Pertimbangan untuk pendaftaran OU bersarang

- Anda tidak dapat mendaftarkan OU di bawah inti OU (Security OU).
- 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 terdaftar pada suatu waktu (beberapa mungkin telah dihapus).
- Anda dapat mendaftarkan OU yang berada di bawah OU yang lebih tinggi yang melayang, tetapi drift tidak diperbaiki oleh tindakan itu.

Keterbatasan OU bersarang

- OU dapat bersarang maksimal 5 tingkat jauh di bawah akar.
- OU bersarang di bawah target OU harus didaftarkan atau didaftarkan ulang secara terpisah.
- Jika target OU berada di Level 2 atau di bawah dalam hierarki, yaitu, jika bukan OU tingkat atas, kontrol pencegahan yang diaktifkan pada OU yang lebih tinggi diberlakukan pada OU ini dan semua OU di bawahnya, secara otomatis.
- Kegagalan pendaftaran OU tidak menyebarkan pohon hierarki. Anda dapat melihat detail tentang status OU bersarang di halaman detail OU induk.
- Kegagalan pendaftaran 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 atas semua OU tempat kontrol diaktifkan, termasuk OU bersarang. Lihat status kepatuhan AWS Control Tower untuk OU dan akunw.
- OU ditampilkan sebagai tidak patuh hanya jika memiliki akun yang tidak patuh, terlepas dari di mana OU berada dalam hierarki OU.
- Jika OU bersarang tidak patuh, OU induknya tidak secara otomatis dianggap tidak patuh.
- Pada halaman detail OU atau detail Akun, Anda dapat melihat daftar sumber daya yang tidak sesuai yang mungkin menyebabkan OU atau akun Anda menunjukkan status yang tidak sesuai.

OU bersarang dan drift

Dalam situasi tertentu, drift dapat mencegah pendaftaran OU bersarang.

Harapan untuk OU 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 drifted 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 dalam drift, kontrol yang melindungi AWS Config sumber daya mungkin dalam drift. Dalam situasi ini, AWS Control Tower memblokir tindakan apa pun yang memerlukan pembuatan atau pembaruan AWS Config sumber daya, termasuk penerapan kontrol detektif.

OU dan kontrol bersarang

Ketika 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 pencegahan ditegakkan pada OU bersarang.
- Kontrol pencegahan wajib diberlakukan pada semua akun di bawah OU dan OU bersarangnya.

- Kontrol preventif memengaruhi semua akun dan OU yang bersarang di bawah target OU, bahkan jika akun dan OU tersebut tidak terdaftar.

Detektif dan kontrol 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 pewarisan yang diaktifkan

Anda dapat melihat kontrol yang diwariskan untuk setiap OU, di 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 secara langsung untuk OU bersarang.

Status warisan

- Status yang diwarisi menunjukkan bahwa kontrol diaktifkan oleh warisan saja, dan belum diterapkan langsung ke OU.
- Status Diaktifkan berarti kontrol diberlakukan pada OU ini, terlepas dari statusnya di OU lainnya.
- Status Gagal berarti kontrol tidak diberlakukan pada OU ini, terlepas dari statusnya di OU lainnya.

> **Note**
>
> Status yang Diwarisi menunjukkan bahwa kontrol diterapkan ke OU yang lebih tinggi di pohon, dan diberlakukan pada OU ini, tetapi tidak ditambahkan langsung ke OU ini.

Jika landing zone Anda bukan versi saat ini

Setiap baris dalam tabel kontrol Diaktifkan mewakili satu kontrol yang diaktifkan pada satu, OU individu.

OU bersarang dan akarnya

Root bukan OU, dan tidak dapat didaftarkan atau didaftarkan ulang. Anda juga tidak dapat membuat akun langsung di root. Root tidak dapat tidak patuh 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.

Daftarkan unit organisasi yang ada dengan AWS Control Tower

Cara efisien untuk membawa banyak 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 dengan landing zone AWS Control Tower Anda. Anda dapat mendaftarkan OU yang berisi hingga 300 akun. Jika OU berisi lebih dari 300 akun, Anda tidak dapat mendaftarkannya di AWS Control Tower.

Saat Anda mendaftarkan OU, akun anggotanya terdaftar ke zona landing zone AWS Control Tower. Mereka diatur oleh kontrol yang berlaku untuk OU mereka.

Note

Jika Anda belum memiliki zona landing zone AWS Control Tower, mulailah dengan menyiapkan landing zone, baik di organisasi baru yang dibuat oleh AWS Control Tower, atau di AWS Organizations organisasi yang sudah ada. Untuk detail selengkapnya tentang cara mengatur landing zone, lihatMemulai 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 tumpukan 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-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 OU Anda memiliki 5 akun secara total, dan 4 di antaranya berhasil terdaftar, tetapi satu akun gagal mendaftar selama proses Register OU. Anda dapat memilih Daftar Ulang OU untuk membawa akun ke dalam pendaftaran, setelah Anda memastikan akun memenuhi prasyarat pendaftaran.

Prasyarat pengguna IAM untuk mendaftarkan OU

Identitas AWS Identity and Access Management (IAM) Anda (pengguna atau peran) atau identitas pengguna IAM Identity Center harus disertakan pada portofolio Account Factory yang sesuai ketika Anda melakukan operasi Register OU, meskipun Anda sudah memiliki `Admin` izin. Jika tidak, pembuatan produk yang disediakan akan gagal saat pendaftaran. Kegagalan terjadi karena AWS Control Tower bergantung pada kredensi 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 Service Catalog > Account Factory > AWS Control Tower Account Factory Portfolio. Kemudian pilih tab yang disebut Grup, peran, dan pengguna untuk melihat identitas IAM atau IAM Identity Center Anda. Untuk informasi selengkapnya tentang cara memberikan akses, lihat dokumentasi untuk AWS Service Catalog.

Daftarkan OU yang ada

Di konsol AWS Control Tower, di halaman Organisasi, Anda dapat melihat semua OU dan akun organisasi Anda dalam hierarki, termasuk OU yang terdaftar di AWS Control Tower, dan akun yang tidak terdaftar.

Secara umum, OU yang tidak terdaftar dibuat di AWS Organizations, dan mereka tidak diatur oleh landing zone lainnya. Anda dapat mendaftarkan OU yang ada yang berisi hingga 300 akun. Jika OU berisi lebih dari 300 akun, Anda tidak dapat mendaftarkannya di AWS Control Tower.

Untuk mendaftarkan OU yang ada

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 Daftarkan unit organisasi dari menu tarik-turun Tindakan di kanan atas, atau sebagai alternatif, pilih nama OU sehingga Anda dapat melihat halaman detail OU untuk OU itu.
4. Pada halaman detail OU, di kanan atas Anda dapat memilih Register OU dari menu dropdown Actions.

Proses pendaftaran membutuhkan waktu minimal 10 menit untuk memperpanjang tata kelola ke OU, dan hingga 2 menit tambahan untuk setiap akun tambahan.

Hasil pendaftaran OU yang ada

Setelah Anda mendaftarkan OU yang ada, `AWSControlTowerExecution` peran tersebut memungkinkan AWS Control Tower untuk 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 pencatatan organisasi Anda, sehingga semua log untuk setiap akun dikirim ke akun logging.
- `AWSControlTowerExecution`memastikan bahwa kontrol AWS Control Tower yang Anda pilih berlaku secara otomatis ke setiap akun individual di OU Anda, serta 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 terkandung dalam kontrol AWS Control Tower. Tim keamanan dan kepatuhan Anda dapat memverifikasi bahwa semua persyaratan terpenuhi, dan 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. Selain itu, Anda mungkin telah membuat akun lain yang tidak terdaftar di OU yang tidak terdaftar tersebut. 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

Untuk membuat OU baru di AWS Control Tower

1. Arahkan ke halaman Organisasi.
2. Pilih Buat unit organisasi dari menu tarik-turun Buat sumber daya di kanan atas.
3. Tentukan nama di bidang nama OU.
4. Di dropdown 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 landing zone Anda tidak up to date, Anda akan melihat daftar datar alih-alih hierarki di menu dropdown. Bahkan jika landing zone Anda termasuk OU bersarang, Anda tidak akan melihat L5 OU di dropdown, karena Anda tidak dapat membuat OU baru di bawah L5 OU. Untuk informasi selengkapnya tentang OU bersarang di AWS Control Tower, lihatOU bersarang di AWS Control Tower.

Penyebab umum kegagalan saat pendaftaran atau pendaftaran ulang

Jika pendaftaran (atau pendaftaran ulang) OU atau akun anggotanya gagal, Anda dapat mengunduh file yang berisi laporan terperinci yang menunjukkan pra-pemeriksaan mana yang tidak lulus. 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.

Secara umum, ketika Anda mendaftar 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 kembali akun tersebut atau OU.

Kesalahan Zona Pendaratan

- Zona pendaratan belum siap

  Setel ulang landing zone Anda saat ini, atau perbarui ke versi terbaru.

Kesalahan OU

- Melebihi jumlah SCP maksimum

  Anda mungkin melebihi batas untuk kebijakan kontrol layanan (SCP) per OU, atau Anda mungkin telah mencapai kuota lain. Batas 5 SCP per OU berlaku untuk semua OU di landing zone AWS Control Tower Anda. Jika Anda memiliki lebih banyak SCP daripada kuota yang diizinkan, Anda harus menghapus atau menggabungkan SCP.

- SCP yang Bertentangan

  SCP yang ada dapat diterapkan ke OU atau akun, yang mencegah AWS Control Tower mendaftarkan akun. Periksa SCP yang diterapkan untuk kebijakan apa pun yang dapat mencegah AWS Control Tower berfungsi. Pastikan untuk memeriksa SCP yang diwarisi dari OU yang lebih tinggi dalam hierarki.
- Melebihi kuota set tumpukan

  Kuota set tumpukan mungkin telah terlampaui. Jika Anda memiliki lebih banyak instance daripada yang diizinkan oleh kuota, Anda harus menghapus beberapa instance tumpukan. Untuk informasi lebih lanjut, lihat kuota AWS CloudFormation dalam Panduan Pengguna AWS CloudFormation .
- Melebihi batas akun

  AWS Control Tower membatasi setiap OU hingga 300 akun selama pendaftaran.

Kesalahan akun

- Pra-cek 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 di semua AWS Wilayah AWS CLI di mana akun manajemen AWS Control Tower 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 (IAM Identity Center). Jika Pusat Identitas IAM sudah disiapkan, wilayah asal AWS Control Tower harus sama dengan Wilayah Pusat Identitas IAM.

- Topik SNS yang bertentangan

  Akun ini 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 Service Catalog 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. Petunjuk untuk menambahkan peran tersedia di[Tambahkan peran IAM yang diperlukan secara manual ke yang sudah ada Akun AWS dan daftarkan](#).

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 mendaftarkan ulang OU.

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 Daftar Ulang.
- Jika Anda memiliki lebih dari satu OU terdaftar di landing zone Anda, daftarkan 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 di. AWS Service CatalogLihat Perbarui akun di konsol.

Perbarui beberapa akun di OU yang sama

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. Di bawah Tindakan di kanan atas, pilih Daftar Ulang OU.

Ulangi langkah-langkah ini untuk setiap OU di organisasi AWS Control Tower Anda, jika Anda perlu memperbarui semua akun dan OU Anda.

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:

- Bidang Status menunjukkan apakah akun saat ini terdaftar dengan AWS Control Tower (Terdaftar), apakah akun belum pernah terdaftar (Tidak terdaftar), atau apakah pendaftaran gagal sebelumnya (Pendaftaran gagal).
- Saat Anda mendaftarkan ulang OU, `AWSControlTowerExecution` peran ditambahkan ke semua akun dengan status Tidak terdaftar atau Pendaftaran gagal.

- AWS Control Tower membuat login masuk tunggal (IAM Identity Center) untuk akun baru yang terdaftar.
- Akun terdaftar 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 Daftarkan yang sudah ada Akun AWS.

> **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

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 Perbarui produk yang disediakan dan Memperbarui produk di Panduan Administrator Service Catalog.

Layanan terintegrasi

AWS Control Tower adalah layanan yang dibangun di atas AWS layanan lain, untuk membantu Anda 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 Well-Architected Tool AWS . Lihat juga Panduan Lingkungan Cloud Manajemen dan Tata Kelola.

Topik

- Menyebarkan Lingkungan dengan AWS CloudFormation
- Memantau Acara dengan CloudTrail
- Memantau Sumber Daya dan Layanan dengan CloudWatch
- Mengatur Konfigurasi Sumber Daya dengan AWS Config
- Mengelola Izin untuk Entitas dengan IAM
- AWS Key Management Service
- Jalankan Fungsi Komputasi Tanpa Server dengan Lambda
- Kelola Akun Melalui AWS Organizations
- Simpan Objek dengan Amazon S3
- Pantau lingkungan Anda dengan Security Hub
- Akun penyediaan melalui AWS Service Catalog
- Lacak Peringatan Melalui Layanan Pemberitahuan Sederhana Amazon
- Membangun Aplikasi Terdistribusi dengan AWS Step Functions

Menyebarkan Lingkungan dengan AWS CloudFormation

AWS CloudFormation memungkinkan Anda untuk membuat dan menyediakan penyebaran AWS infrastruktur yang dapat diprediksi dan berulang kali. Ini membantu Anda memanfaatkan AWS produk untuk membangun aplikasi yang sangat andal, sangat terukur, dan hemat biaya di cloud tanpa khawatir membuat dan mengonfigurasi infrastruktur yang mendasarinya. AWS AWS CloudFormation memungkinkan Anda untuk menggunakan file template untuk membuat dan menghapus koleksi

sumber daya bersama-sama sebagai satu unit (tumpukan). Untuk informasi selengkapnya, lihat Panduan Pengguna AWS CloudFormation.

AWS Control Tower menggunakan AWS CloudFormation stackset untuk menerapkan kontrol pada akun. Untuk informasi selengkapnya tentang cara AWS CloudFormation dan AWS Control Tower bekerja sama, lihat Menciptakan 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 jejak Anda, dan mengontrol cara administrator mengaktifkan dan menonaktifkan CloudTrail log. 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 mengatur, 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 Pemantauan.

Mengatur Konfigurasi Sumber Daya dengan AWS Config

AWS Config memberikan tampilan rinci tentang sumber daya yang terkait dengan AWS akun Anda, termasuk bagaimana mereka dikonfigurasi, bagaimana mereka terkait satu sama lain, dan bagaimana konfigurasi dan hubungan mereka 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 memonitor dan merekam sumber daya di AWS Control Tower, dan cara tagihannya kepada Anda, lihatPantau perubahan sumber daya dengan AWS Config.

AWS Control Tower digunakan Aturan AWS Config untuk mengimplementasikan kontrol detektif. Untuk informasi selengkapnya, lihat Tentang kontrol di AWS Control Tower.

Mengelola Izin untuk Entitas dengan IAM

AWS Identity and Access Management (IAM) adalah AWS layanan untuk mengendalikan akses ke AWS layanan lain. Dengan IAM, Anda dapat mengelola pengguna, kredensi keamanan secara terpusat — seperti kunci akses, dan izin — yang menentukan AWS sumber daya yang dapat diakses oleh pengguna dan aplikasi Anda.

Saat Anda mengatur landing zone, sejumlah grup dapat dibuat secara AWS IAM Identity Center otomatis, jika Anda memilih IAM sebagai penyedia identitas Anda. Grup ini memiliki set izin yang merupakan kebijakan izin yang telah ditentukan sebelumnya dari IAM. Pengguna akhir Anda juga dapat menggunakan IAM untuk menentukan ruang lingkup izin untuk 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 IAM Identity Center 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 sebuah 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 dengan kunci AWS KMS enkripsi. Untuk selengkapnya AWS KMS, lihat Panduan Pengembang AWS KMS.

Untuk informasi tentang cara mengatur AWS KMS kunci dengan AWS Control Tower, lihat Mengkonfigurasi 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 overhead administrasi tambahan. Saat Anda mengunggah kode, 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 web atau aplikasi 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.

Kelola 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 Organizations, 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, Organizations membantu mengelola penagihan secara terpusat; mengontrol akses, kepatuhan, dan keamanan; dan berbagi sumber daya di seluruh akun anggota AWS Anda. Akun dikelompokkan ke dalam kelompok logis, yang disebut unit organisasi (OU). Untuk informasi selengkapnya tentang Organizations, lihat Panduan AWS Organizations Pengguna.

AWS Control Tower menggunakan OU berikut:

- Root — Kontainer induk untuk semua akun dan semua OU lainnya di landing zone Anda.
- Keamanan - OU ini berisi akun arsip log, akun audit, dan sumber daya yang mereka miliki.
- Sandbox - OU ini dibuat saat Anda mengatur landing zone Anda. Itu dan OU anak lainnya di landing zone 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 landing zone melalui konsol AWS Control Tower di halaman Unit Organisasi.

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 untuk itu dan akunnya. Untuk informasi tentang mendaftarkan OU, lihat Mendaftarkan 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. AWS Management Console Untuk informasi selengkapnya, lihat Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Saat menyiapkan landing zone, bucket Amazon S3 dibuat di akun arsip log untuk memuat semua log di semua akun di landing zone Anda.

Pantau lingkungan Anda dengan Security Hub

AWS Control Tower terintegrasi dengan AWS Security Hub melalui standar Security Hub yang disebut Service-Managed Standard: AWS Control Tower. Untuk informasi selengkapnya, lihat standar Security Hub.

Akun 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 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 Service Catalog.

Di AWS Control Tower, administrator cloud pusat dan pengguna akhir Anda dapat menyediakan akun khusus di landing zone Anda menggunakan AWS Service Catalog produk, yang disebut “cetak biru khusus”. Untuk informasi lebih lanjut, lihat Step2. Buat AWS Service Catalog produk.

AWS Control Tower juga dapat menggunakan Service Catalog API untuk mengotomatiskan penyediaan dan pembaruan akun lebih lanjut. Untuk detailnya, lihat Panduan AWS Service Catalog Pengembang.

Transisi ke jenis produk AWS Service Catalog Eksternal

AWS Service Catalog mengubah dukungan untuk produk Terraform Open Source dan menyediakan produk ke jenis produk baru, yang disebut Eksternal. Untuk mempelajari lebih lanjut tentang transisi ini, tinjau 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 mentransisikan akun ini ke jenis produk Eksternal, Anda perlu membuat perubahan di AWS Control Tower AWS Service Catalog dan AWS Control Tower.

Untuk transisi ke jenis produk Eksternal

1. Tingkatkan Mesin Referensi Terraform Anda yang ada AWS Service Catalog untuk menyertakan dukungan untuk jenis produk Sumber Terbuka Eksternal dan Terraform. Untuk petunjuk tentang memperbarui Mesin Referensi Terraform Anda, tinjau Repositori.AWS Service Catalog GitHub
2. Di AWS Service Catalog, duplikat semua produk Terraform Open Source yang ada (cetak biru), dengan duplikat menggunakan jenis produk Eksternal yang baru. Jangan hentikan 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, tinjau 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 Sumber Terraform diperbarui ke cetak biru Eksternal, kembali ke 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 AWS CloudFormationatau 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 lebih lanjut, tinjau Pengaturan 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 dalam 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.

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 notifikasi langsung 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 drift di dalam landing zone Anda. Untuk informasi selengkapnya, lihat Mendeteksi dan mengatasi penyimpangan di AWS Control Tower.

Kami juga menggunakan Amazon Simple Notification Service 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 tidak sesuai. AWS Config secara otomatis memelihara daftar akun di OU Anda. Anda harus berlangganan secara manual, menggunakan email atau jenis langganan apa pun yang memungkinkan SNS. Pernyataan tersebut `arn:aws:sns:`*`homeregion`*`:`*`account`*`:aws-controltower-AggregateSecurityNotifications` 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 landing zone 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 mengautentikasi bahwa Anda adalah pengguna yang disetujui. AWS Misalnya, jika Anda menggunakan konsol AWS Control Tower, Anda mengautentikasi identitas Anda dengan memberikan AWS kredensil Anda, seperti yang disediakan oleh administrator Anda.

Setelah Anda mengautentikasi identitas Anda, IAM mengontrol akses Anda AWS dengan sekumpulan izin yang ditentukan pada serangkaian operasi dan sumber daya tertentu. Jika Anda seorang administrator akun, Anda dapat menggunakan IAM untuk mengontrol akses pengguna IAM lainnya ke sumber daya yang terkait dengan akun Anda.

Topik

Autentikasi

Anda memiliki akses ke AWS salah satu jenis identitas berikut:

- AWS pengguna root akun — Ketika Anda 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, patuhi 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 kredensil pengguna IAM untuk masuk guna mengamankan AWS halaman web seperti Konsol AWS Manajemen, Forum AWS Diskusi, atau Pusat Dukungan. AWS AWS praktik terbaik merekomendasikan agar Anda membuat pengguna IAM Identity Center alih-alih pengguna IAM, karena ada lebih banyak risiko keamanan saat Anda membuat pengguna IAM yang memiliki kredensi jangka panjang.

  Jika Anda harus membuat pengguna IAM untuk tujuan tertentu, selain kredensi masuk, Anda dapat membuat kunci akses untuk setiap pengguna IAM. Anda dapat menggunakan kunci 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 mengautentikasi permintaan API masuk. Untuk informasi selengkapnya tentang mengautentikasi permintaan, lihat Proses Penandatanganan Versi Tanda Tangan 4 di Referensi AWS 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 AWS 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 layanan untuk mengambil alih. Peran layanan ini harus mencakup semua izin yang diperlukan untuk layanan untuk mengakses AWS sumber daya yang dibutuhkan. Peran layanan bervariasi dari layanan ke layanan, tetapi

banyak yang memungkinkan Anda memilih izin selama Anda memenuhi persyaratan yang didokumentasikan 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 kredensi sementara untuk aplikasi yang berjalan pada instans Amazon EC2 dan membuat permintaan CLI atau API. AWS AWS Ini lebih baik untuk 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 kredensi sementara. Untuk informasi selengkapnya, lihat Menggunakan IAM role untuk memberikan izin ke aplikasi yang berjalan di instans Amazon EC2 dalam Panduan pengguna IAM.

- Otentikasi pengguna IAM Identity Center ke portal pengguna IAM Identity Center dikendalikan oleh direktori yang telah Anda sambungkan ke IAM Identity Center. 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 AWS Identitas IAM. Untuk informasi selengkapnya, lihat Akses Masuk Tunggal di AWS IAM Identity Center Panduan Pengguna.
  - Tingkat izin apa yang telah diberikan kepada pengguna akhir di konsol Pusat Identitas AWS IAM untuk memungkinkan mereka akses yang sesuai ke akun tersebut. AWS Untuk informasi selengkapnya, lihat Set Izin di Panduan AWS IAM Identity Center Pengguna.

Kontrol akses

Untuk membuat, memperbarui, menghapus, atau mencantumkan sumber daya AWS Control Tower, atau AWS sumber daya lain di landing zone, Anda memerlukan izin untuk melakukan operasi, dan Anda memerlukan izin untuk mengakses sumber daya terkait. Selain itu, untuk melakukan operasi secara terprogram, Anda memerlukan kunci akses yang valid.

Bagian berikut menjelaskan cara mengelola izin untuk AWS Control Tower:

Topik

- Gambaran umum tentang mengelola izin akses ke sumber daya AWS Control Tower Anda
- Menggunakan kebijakan berbasis identitas (kebijakan IAM) untuk AWS Control Tower

Bekerja dengan AWS IAM Identity Center 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 provder 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 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 PanduanAWS 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. 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 menyediakan 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

Akun	Set izin	Deskripsi
		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

Akun	Set izin	Deskripsi
		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 layanan dan sumber daya di akun ini.

AWSAuditAccountAdmins

Akun	Set izin	Deskripsi
Akun audit	AWSAdministratorAccess	Pengguna memiliki akses administrator di akun ini.

Gambaran umum tentang mengelola izin akses ke sumber daya AWS Control Tower Anda

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 tentang administrator, 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 setiap pengguna dan peran memerlukan izin, 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 utamanya adalah landing zone. AWS Control Tower juga mendukung jenis sumber daya tambahan, kontrol, kadang-kadang disebut sebagai pagar pembatas. Namun, untuk AWS Control Tower, Anda dapat mengelola kontrol hanya dalam konteks landing zone yang ada. Kontrol dapat disebut sebagai subresource.

Sumber daya dan subsumber daya 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, AWS Control Tower Referensi API AWS Control Tower.

Untuk informasi selengkapnya tentang AWS CloudFormation sumber daya di AWS Control Tower, lihat Panduan AWS CloudFormation Pengguna.

Tentang kepemilikan sumber daya

AWS Akun 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 mengautentikasi permintaan pembuatan sumber daya. Contoh berikut menggambarkan cara kerjanya:

- Jika Anda menggunakan kredensi pengguna root AWS akun AWS akun Anda untuk menyiapkan landing zone, AWS akun Anda adalah pemilik sumber daya.
- Jika Anda membuat pengguna IAM di AWS akun Anda dan memberikan izin untuk menyiapkan landing zone kepada pengguna tersebut, pengguna dapat menyiapkan landing zone selama akun mereka memenuhi prasyarat. Namun, AWS akun Anda, tempat pengguna berada, memiliki sumber daya landing zone.
- Jika Anda membuat peran IAM di AWS akun dengan izin untuk menyiapkan landing zone, siapa pun yang dapat mengambil peran tersebut dapat menyiapkan landing zone. AWS Akun Anda, tempat perannya berada, memiliki sumber daya landing zone.

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)

Anda dapat melampirkan kebijakan ke identitas IAM Anda. Misalnya, Anda dapat melakukan hal berikut:

- Lampirkan kebijakan izin ke pengguna atau grup di akun Anda — Untuk memberikan izin pengguna untuk membuat sumber daya AWS Control Tower, seperti menyiapkan landing zone, 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 akun lain (AWS Akun B), atau administrator dapat membuat peran yang memberikan izin ke layanan lain. AWS

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 mengidentifikasi Akun B sebagai kepala sekolah yang dapat mengambil peran.
3. Sebagai prinsipal, administrator Akun B dapat memberikan izin kepada pengguna di Akun B untuk mengambil peran tersebut. Dengan mengasumsikan 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 lainnya, termasuk akses terprogram ke sumber daya.

Untuk memberikan akses, tambahkan izin ke pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

  Buat rangkaian izin. Ikuti petunjuk dalam Buat set izin dalam Panduan Pengguna AWS IAM Identity Center .
- Pengguna yang dikelola di IAM melalui penyedia identitas:

  Buat peran untuk federasi identitas. Ikuti petunjuk dalam Membuat peran untuk penyedia identitas pihak ketiga (federasi) di Panduan Pengguna IAM.
- Pengguna IAM:
  - Buat peran yang dapat diambil pengguna Anda. Ikuti petunjuk dalam Membuat peran untuk pengguna IAM dalam Panduan Pengguna IAM.
  - (Tidak disarankan) Pasang kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti petunjuk di 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 landing zone AWS Control Tower, Anda memerlukan pengguna atau peran dengan kebijakan AdministratorAccessterkelola. (arn:aws:iam: :aws:policy/) AdministratorAccess

Untuk membuat peran untuk Layanan AWS (konsol IAM)

1. Masuk ke AWS Management Console 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 jenis entitas Tepercaya, pilih Layanan AWS.
4. Untuk kasus Layanan atau 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 Izin, opsi bergantung pada kasus penggunaan yang Anda pilih:
   - Jika layanan menentukan izin untuk peran tersebut, Anda tidak dapat memilih kebijakan izin.
   - Pilih dari serangkaian kebijakan izin terbatas.
   - Pilih dari semua kebijakan izin.
   - Pilih kebijakan tanpa izin, buat kebijakan setelah peran dibuat, lalu lampirkan kebijakan ke peran.
7. (Opsional) Tetapkan batas izin. Ini adalah fitur lanjutan yang tersedia untuk peran layanan, tetapi bukan peran tertaut layanan.
   a. Buka bagian Setel 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 Peran, opsi bergantung pada layanan:
   - Jika layanan menentukan 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.

> **Important**
>
> Saat Anda memberi nama peran, perhatikan hal berikut:
>
> - Nama peran harus unik di dalam diri 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 tersebut 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 tersebut.
11. (Opsional) Untuk mengedit kasus penggunaan dan izin untuk peran, di 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 nilai kunci. Untuk informasi selengkapnya tentang penggunaan tanda di IAM, lihat Menandai sumber daya IAM di Panduan Pengguna IAM.
13. Tinjau peran lalu pilih Buat peran.

Cara menggunakan editor kebijakan JSON untuk membuat kebijakan

1. Masuk ke AWS Management Console 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 membuat atau mengedit kebijakan AWS Management Console, Anda dapat membuat templat kebijakan JSON atau YAMB yang dapat Anda gunakan dalam AWS CloudFormation templat.

   Untuk melakukannya, di editor Kebijakan pilih Tindakan, lalu pilih Buat CloudFormation templat. Untuk mempelajari selengkapnya AWS CloudFormation, 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 penggunaan tanda di IAM, lihat Menandai sumber daya IAM di Panduan Pengguna IAM.
11. Pilih Buat kebijakan untuk menyimpan kebijakan baru Anda.

Untuk menggunakan editor visual dalam pembuatan kebijakan

1. Masuk ke AWS Management Console 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, temukan 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 lebih banyak izin.
5. Di Tindakan yang diizinkan, pilih tindakan yang akan ditambahkan ke kebijakan. Anda bisa memilih tindakan dengan cara berikut:

   - Pilih kotak centang untuk semua tindakan.
   - Pilih Tambahkan 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 secara terpisah yang diizinkan 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 Amazon Resource Names (ARN) di Panduan Pengguna IAM. Untuk informasi tentang penggunaan ARN dalam

`Resource` elemen kebijakan, lihat elemen kebijakan IAM JSON: Sumber daya dalam Panduan Pengguna IAM.

- Pilih Apa saja di akun ini di samping sumber daya untuk memberikan izin ke sumber daya apa pun dari jenis itu.
- Pilih Semua untuk memilih semua sumber daya untuk layanan ini.

7. (Opsional) Pilih Ketentuan permintaan - 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 Otorisasi 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 Condition Key, Qualifier, dan Operator kondisi, lalu masukkan Nilai. Untuk menambahkan lebih dari satu nilai, pilih Tambah. Anda dapat mempertimbangkan nilai-nilai sebagai terhubung oleh `OR` operator logis. Setelah selesai, pilih Tambahkan kondisi.

   Untuk menambahkan lebih dari satu kondisi, pilih Tambahkan 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 dalam 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 membuat atau mengedit kebijakan AWS Management Console, Anda dapat membuat templat kebijakan JSON atau YAMB yang dapat Anda gunakan dalam AWS CloudFormation templat.

   Untuk melakukannya, di editor Kebijakan pilih Tindakan, lalu pilih Buat CloudFormation templat. Untuk mempelajari selengkapnya AWS CloudFormation, 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 dimaksud.
12. (Opsional) Tambahkan metadata ke kebijakan dengan melampirkan tanda sebagai pasangan nilai kunci. Untuk informasi selengkapnya tentang penggunaan tanda di IAM, lihat Menandai sumber daya IAM di Panduan Pengguna IAM.
13. Pilih Buat kebijakan untuk menyimpan kebijakan baru Anda.

Untuk memberikan akses terprogram

Pengguna membutuhkan akses terprogram jika mereka ingin berinteraksi dengan AWS luar. AWS Management Console Cara untuk memberikan akses terprogram tergantung pada jenis pengguna yang mengakses AWS.

Untuk memberi pengguna akses terprogram, pilih salah satu opsi berikut.

Pengguna mana yang membutuhkan akses terprogram?	Untuk	Oleh
Identitas tenaga kerja (Pengguna yang dikelola di Pusat Identitas IAM)	Gunakan kredenal sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk AWS CLI, lihat Mengkonfigurasi yang akan AWS CLI digunakan AWS IAM Identity Center dalam Panduan AWS Command Line Interface Pengguna. • Untuk AWS SDK, alat, dan AWS API, lihat autentikasi Pusat Identitas IAM di Panduan Referensi AWS SDK dan Alat.
IAM	Gunakan kredenal sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk dalam Menggunakan kredensi sementara dengan AWS sumber daya di Panduan Pengguna IAM.
IAM	(Tidak direkomendasikan) Gunakan kredenal jangka panjang untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk mengetahui AWS CLI, lihat Mengautentikasi menggunakan kredensi pengguna IAM di Panduan Pengguna.AWS Command Line Interface

Pengguna mana yang membutuhkan akses terprogram?	Untuk	Oleh
		• Untuk AWS SDK dan alat bantu, lihat Mengautentikasi menggunakan kredensil jangka panjang di Panduan Referensi AWS SDK dan Alat. • Untuk AWS API, lihat Mengelola 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 prinsipal AWS layanan lain, lihat Ketentuan 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 bingung, yang terjadi jika entitas memaksa entitas yang lebih istimewa untuk melakukan tindakan, seperti dengan peniruan identitas lintas layanan. Untuk informasi umum tentang kondisi kebijakan, lihat jugaMenentukan kondisi dalam kebijakan.

Untuk informasi selengkapnya tentang penggunaan 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.

Kebijakan berbasis sumber daya

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 landing zone melalui konsol AWS Control Tower, atau API landing zone. Untuk menyiapkan landing zone, Anda harus menjadi pengguna IAM dengan izin administratif sebagaimana didefinisikan dalam kebijakan IAM.

Elemen-elemen berikut adalah yang paling dasar yang dapat Anda identifikasi dalam suatu 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 Tindakan yang ditentukan oleh AWS Control Tower.
- Efek – Anda menentukan efek ketika pengguna meminta tindakan tertentu—baik mengizinkan maupun menolak. 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.
- Principal — Dalam kebijakan berbasis identitas (kebijakan IAM), pengguna yang melekat pada kebijakan tersebut adalah prinsipal 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 menyatakan kondisi, Anda dapat menggunakan kunci kondisi yang telah ditentukan. Tidak ada kunci kondisi khusus untuk AWS Control Tower. Namun, ada tombol kondisi AWS-wide yang dapat

Anda gunakan sesuai kebutuhan. Untuk daftar lengkap tombol AWS-wide, lihat Kunci yang Tersedia untuk Ketentuan di Panduan Pengguna IAM.

Mencegah peniruan identitas lintas layanan

Pada tahun AWS, peniruan lintas layanan dapat mengakibatkan masalah wakil yang membingungkan. Ketika satu layanan memanggil layanan lain, peniruan identitas 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 sediakan alat untuk membantu Anda melindungi data Anda, sehingga hanya layanan dengan izin yang 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 hanya ingin satu sumber daya dikaitkan dengan akses lintas layanan.
- Gunakan `aws:SourceAccount` jika Anda ingin mengizinkan sumber daya apa pun di akun itu dikaitkan dengan penggunaan lintas layanan.
- Jika `aws:SourceArn` nilainya tidak berisi ID akun, seperti ARN untuk bucket Amazon S3, Anda harus menggunakan kedua kondisi tersebut untuk membatasi izin.
- Jika Anda menggunakan kedua kondisi, dan jika `aws:SourceArn` nilainya berisi ID akun, `aws:SourceAccount` nilai dan akun dalam `aws:SourceArn` nilai harus menunjukkan ID akun yang sama saat digunakan dalam pernyataan kebijakan yang sama

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 Gambaran umum tentang mengelola izin akses ke sumber daya AWS Control Tower Anda.

Izin yang Diperlukan untuk Menggunakan AWS Control Tower Console

AWS Control Tower membuat tiga peran secara otomatis saat Anda menyiapkan landing zone. Ketiga peran tersebut diperlukan untuk memungkinkan akses konsol. AWS Control Tower membagi izin menjadi tiga peran sebagai praktik terbaik untuk membatasi akses ke serangkaian tindakan dan sumber daya minimal.

Tiga peran yang dibutuhkan

- AWS ControlTowerAdmin peran
- AWS ControlTowerStackSetRole
- AWS ControlTowerCloudTrailRole

Kami menyarankan Anda membatasi akses ke kebijakan kepercayaan peran Anda untuk peran ini. Untuk informasi selengkapnya, lihat Ketentuan opsional untuk hubungan kepercayaan peran Anda.

AWS ControlTowerAdmin peran

Peran ini memberi AWS Control Tower akses ke infrastruktur yang penting untuk mempertahankan landing zone. `AWS ControlTowerAdmin`Peran tersebut membutuhkan kebijakan terkelola terlampir dan kebijakan kepercayaan peran untuk peran IAM. Kebijakan kepercayaan peran adalah kebijakan berbasis sumber daya, yang menentukan prinsip mana yang dapat mengambil peran tersebut.

Berikut contoh cuplikan untuk kebijakan kepercayaan peran ini:

```
{
  "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 bernama`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 inline, misalnya:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*"
        }
    ]
}
```

2. Kebijakan terkelola yang mengikuti, yaitu`AWS ControlTowerServiceRolePolicy`.

AWS ControlTowerServiceRolePolicy

AWS ControlTowerServiceRolePolicyIni adalah kebijakan AWS terkelola yang mendefinisikan izin untuk membuat dan mengelola sumber daya AWS Control Tower, seperti AWS CloudFormation stackset dan instance tumpukan, file AWS CloudTrail log, agregator konfigurasi untuk AWS Control Tower, AWS Organizations serta akun dan unit organisasi (OU) yang diatur oleh AWS Control Tower.

Pembaruan kebijakan terkelola ini dirangkum dalam tabel,[Kebijakan terkelola untuk AWS Control Tower](#).

Untuk informasi selengkapnya, lihat AWSControlTowerServiceRolePolicydi Panduan Referensi Kebijakan Terkelola AWS.

Nama Kebijakan Terkelola: `AWS ControlTowerServiceRolePolicy`

Artefak JSON untuk `AWS ControlTowerServiceRolePolicy` adalah sebagai berikut:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:CreateStackInstances",
                "cloudformation:CreateStackSet",
                "cloudformation:DeleteStack",
                "cloudformation:DeleteStackInstances",
                "cloudformation:DeleteStackSet",
                "cloudformation:DescribeStackInstance",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackSet",
                "cloudformation:DescribeStackSetOperation",
                "cloudformation:ListStackInstances",
                "cloudformation:UpdateStack",
                "cloudformation:UpdateStackInstances",
                "cloudformation:UpdateStackSet"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:type/resource/AWS-IAM-Role"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "account:EnableRegion",
                "account:ListRegions",
                "account:GetRegionOptStatus"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "cloudformation:CreateStack",
                "cloudformation:CreateStackInstances",
                "cloudformation:CreateStackSet",
                "cloudformation:DeleteStack",
                "cloudformation:DeleteStackInstances",
                "cloudformation:DeleteStackSet",
                "cloudformation:DescribeStackInstance",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackSet",
                "cloudformation:DescribeStackSetOperation",
                "cloudformation:GetTemplate",
                "cloudformation:ListStackInstances",
                "cloudformation:UpdateStack",
                "cloudformation:UpdateStackInstances",
                "cloudformation:UpdateStackSet"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:stack/AWSControlTower*/*",
                "arn:aws:cloudformation:*:*:stack/StackSet-AWSControlTower*/*",
                "arn:aws:cloudformation:*:*:stackset/AWSControlTower*:*",
                "arn:aws:cloudformation:*:*:stackset-target/AWSControlTower*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:CreateTrail",
                "cloudtrail:DeleteTrail",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail",
                "cloudtrail:PutEventSelectors",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:PutRetentionPolicy"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:aws-controltower/CloudTrailLogs:*",
                "arn:aws:cloudtrail:*:*:trail/aws-controltower*"
            ]
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::aws-controltower*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution",
                "arn:aws:iam::*:role/AWSControlTowerBlueprintAccess"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudtrail:DescribeTrails",
                "ec2:DescribeAvailabilityZones",
                "iam:ListRoles",
                "logs:CreateLogGroup",
                "logs:DescribeLogGroups",
                "organizations:CreateAccount",
                "organizations:DescribeAccount",
                "organizations:DescribeCreateAccountStatus",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribePolicy",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy",
                "organizations:ListRoots",
                "organizations:MoveAccount",
                "servicecatalog:AssociatePrincipalWithPortfolio"
            ],
            "Resource": "*"
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetRole",
                "iam:GetUser",
                "iam:ListAttachedRolePolicies",
                "iam:GetRolePolicy"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/service-role/AWSControlTowerStackSetRole",
                "arn:aws:iam::*:role/service-role/AWSControlTowerCloudTrailRole",
                "arn:aws:iam::*:role/service-role/
AWSControlTowerConfigAggregatorRoleForOrganizations"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "config:DeleteConfigurationAggregator",
                "config:PutConfigurationAggregator",
                "config:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/aws-control-tower": "managed-by-control-tower"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
```

```
            "Condition": {
                "StringLike": {
                    "organizations:ServicePrincipal": [
                        "config.amazonaws.com",
                        "cloudtrail.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "cloudtrail.amazonaws.com"
                }
            }
        }
    ]
}
```

Kebijakan kepercayaan peran:

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "controltower.amazonaws.com"
         ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Kebijakan inline adalah`AWSControlTowerAdminPolicy`:

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

AWS ControlTowerStackSetRole

AWS CloudFormation mengasumsikan peran ini untuk menerapkan set tumpukan di akun yang dibuat oleh AWS Control Tower. Kebijakan Inline:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": [
                "arn:aws:iam::*:role/AWSControlTowerExecution"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Kebijakan kepercayaan

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudformation.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
```

```
    ]
}
```

AWS ControlTowerCloudTrailRole

AWS Control Tower memungkinkan CloudTrail sebagai praktik terbaik dan menyediakan peran ini CloudTrail. CloudTrailmengasumsikan peran ini untuk membuat dan menerbitkan CloudTrail log. Kebijakan Inline:

```
{
    "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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "cloudtrail.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWSControlTowerBlueprintAccess persyaratan peran

AWS Control Tower mengharuskan Anda untuk membuat `AWSControlTowerBlueprintAccess` peran di akun hub cetak biru yang ditentukan, dalam organisasi yang sama.

Nama peran

Nama peran harus`AWSControlTowerBlueprintAccess`.

Kebijakan kepercayaan peran

Peran harus diatur untuk mempercayai prinsip-prinsip berikut:

- Prinsipal yang menggunakan AWS Control Tower di akun manajemen.
- `AWSControlTowerAdmin`Peran dalam akun manajemen.

Contoh berikut menunjukkan kebijakan kepercayaan paling tidak memiliki hak istimewa. Saat Anda membuat kebijakan sendiri, ganti istilah *`YourManagementAccountId`*dengan ID acccount aktual akun manajemen AWS Control Tower Anda, dan ganti istilah tersebut *`YourControlTowerUserRole`*dengan pengenal peran IAM untuk akun manajemen Anda.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::YourManagementAccountId:role/service-role/
AWSControlTowerAdmin",

 "arn:aws:iam::YourManagementAccountId:role/YourControlTowerUserRole"
                ]
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

Izin peran

Anda diminta untuk melampirkan kebijakan yang dikelola AWSServiceCatalogAdminFullAccesske peran tersebut.

AWSServiceRoleForAWSControlTower

Peran ini memberi AWS Control Tower akses ke akun Arsip Log, akun Audit, dan akun anggota, untuk operasi yang penting untuk mempertahankan landing zone, seperti memberi tahu Anda tentang sumber daya yang hanyut.

`AWSServiceRoleForAWSControlTower`Peran tersebut membutuhkan kebijakan terkelola terlampir dan kebijakan kepercayaan peran untuk peran IAM.

Kebijakan terkelola untuk peran ini: `AWSControlTowerAccountServiceRolePolicy`

Kebijakan kepercayaan peran:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "controltower.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWSControlTowerAccountServiceRolePolicy

Kebijakan yang AWS dikelola ini memungkinkan AWS Control Tower memanggil AWS layanan yang menyediakan konfigurasi akun otomatis dan tata kelola terpusat atas nama Anda.

Kebijakan ini berisi izin minimum AWS Control Tower untuk menerapkan penerusan AWS Security Hub temuan untuk sumber daya yang dikelola oleh kontrol Security Hub yang merupakan bagian dari Standar yang dikelola Layanan Security Hub: AWS Control Tower, dan mencegah perubahan yang membatasi kemampuan mengelola akun pelanggan. Ini adalah bagian dari proses deteksi AWS Security Hub drift latar belakang yang tidak secara langsung diprakarsai oleh pelanggan.

Kebijakan ini memberikan izin untuk membuat EventBridge aturan Amazon, khususnya untuk kontrol Security Hub, di setiap akun anggota, dan aturan ini harus menentukan EventPattern persisnya.

Selain itu, aturan hanya dapat beroperasi berdasarkan aturan yang dikelola oleh prinsipal layanan kami.

Prinsipal layanan: `controltower.amazonaws.com`

Artefak JSON untuk `AWSControlTowerAccountServiceRolePolicy` adalah sebagai berikut:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
  //For creating the managed rule
   "Sid": "AllowPutRuleOnSpecificSourcesAndDetailTypes",
   "Effect": "Allow",
   "Action": "events:PutRule",
   "Resource": "arn:aws:events:*:*:rule/*ControlTower*",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "events:source": "aws.securityhub"
    },
    "Null": {
     "events:detail-type": "false"
    },
    "StringEquals": {
     "events:ManagedBy": "controltower.amazonaws.com",
     "events:detail-type": "Security Hub Findings - Imported"
    }
   }
  },
  // Other operations to manage the managed rule
  {
   "Sid": "AllowOtherOperationsOnRulesManagedByControlTower",
   "Effect": "Allow",
   "Action": [
    "events:DeleteRule",
    "events:EnableRule",
    "events:DisableRule",
    "events:PutTargets",
    "events:RemoveTargets"
   ],
   "Resource": "arn:aws:events:*:*:rule/*ControlTower*",
   "Condition": {
    "StringEquals": {
     "events:ManagedBy": "controltower.amazonaws.com"
```

```
    }
   }
  },
  // More managed rule permissions
  {
   "Sid": "AllowDescribeOperationsOnRulesManagedByControlTower",
   "Effect": "Allow",
   "Action": [
    "events:DescribeRule",
    "events:ListTargetsByRule"
   ],
   "Resource": "arn:aws:events:*:*:rule/*ControlTower*"
  },
  // Add permission to publish the security notifications to SNS
  {
   "Sid": "AllowControlTowerToPublishSecurityNotifications",
   "Effect": "Allow",
   "Action": "sns:publish",
   "Resource": "arn:aws:sns:*:*:aws-controltower-AggregateSecurityNotifications",
   "Condition": {
    "StringEquals": {
     "aws:PrincipalAccount": "${aws:ResourceAccount}"
    }
   }
  },
  // For drift verification
  {
   "Sid": "AllowActionsForSecurityHubIntegration",
   "Effect": "Allow",
   "Action": [
    "securityhub:DescribeStandardsControls",
    "securityhub:GetEnabledStandards"
   ],
   "Resource": "arn:aws:securityhub:*:*:hub/default"
  }
 ]
}
```

Pembaruan kebijakan terkelola ini dirangkum dalam tabel,[Kebijakan terkelola untuk AWS Control Tower](#).

Kebijakan terkelola untuk AWS Control Tower

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.

Perubahan	Deskripsi	Tanggal
AWSControlTowerAccountServiceRolePolicy—Kebijakan baru	AWS Control Tower menambahkan peran terkait layanan baru yang memungkinkan AWS Control Tower membuat dan mengelola aturan peristiwa, dan berdasarkan aturan tersebut, untuk mengelola deteksi drift untuk kontrol yang terkait dengan Security Hub. Perubahan ini diperlukan agar pelanggan dapat melihat sumber daya yang hanyut di konsol, ketika sumber daya tersebut terkait dengan kontrol Security Hub yang merupakan bagian dari Standar yang dikelola Layanan Security Hub: AWS Control Tower.	22 Mei 2023
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`	6 April 2023

Perubahan	Deskripsi	Tanggal
	API yang diterapkan oleh layanan Manajemen AWS Akun, agar keikutsertaan Wilayah AWS tersedia untuk akun pelanggan di landing zone (Akun manajemen, akun arsip log, akun Audit, akun anggota OU). Perubahan ini diperlukan agar pelanggan dapat memiliki opsi untuk memperluas tata kelola Wilayah oleh AWS Control Tower ke dalam Wilayah keikutsertaan.	

Perubahan	Deskripsi	Tanggal
AWS ControlTowerServiceRolePolicy – Pembaruan ke kebijakan yang ada	AWS Control Tower menambahkan izin baru yang memungkinkan AWS Control Tower `AWSControlTowerBlueprintAccess` berperan dalam akun blueprint (hub), yang merupakan akun khusus dalam suatu organisasi, yang berisi cetak biru yang telah ditentukan sebelumnya yang disimpan dalam satu atau beberapa Produk Service Catalog. AWS Control Tower mengambil `AWSControlTowerBlueprintAccess` peran untuk melakukan tiga tugas: membuat Portofolio Service Catalog, menambahkan cetak biru Produk 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

Perubahan	Deskripsi	Tanggal
AWS ControlTowerServiceRolePolicy – Pembaruan ke kebijakan yang ada	AWS Control Tower menambahkan izin baru yang memungkinkan pelanggan menyiapkan AWS CloudTrail jejak tingkat organisasi, mulai dari landing zone versi 3.0. CloudTrail Fitur berbasis organisasi mengharuskan pelanggan untuk 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

Perubahan	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 landing zone. Saat memperbarui kunci KMS, AWS CloudFormation perlu izin untuk memanggil API. AWS CloudTrail `PutEventSelector` Perubahan kebijakan adalah mengizinkan AWS ControlTowerAdminperan memanggil AWS CloudTrail `PutEventSelector` API.	28 Juli 2021
AWS Control Tower mulai melacak perubahan	AWS Control Tower mulai melacak perubahan untuk kebijakan yang AWS dikelola.	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 tanggung 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. Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS .

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 sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi yang lebih lengkap tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-2.

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

AWS Control Tower menggunakan bucket Amazon S3 dan database Amazon DynamoDB yang dienkripsi saat istirahat menggunakan Amazon S3-Managed Keys (SSE-S3) untuk mendukung landing zone Anda. 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 menggunakan AWS untuk membuat aplikasi yang sesuai dengan HIPAA.
- 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— 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 Diffie-Hellman (DHE) atau Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Sebagian besar sistem modern seperti Java 7 dan sistem yang lebih baru mendukung mode ini.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan prinsipal 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. Untuk informasi selengkapnya, lihat 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 lebih detail:

Topik

- Menggunakan Notifikasi AWS 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.

Jalur tingkat organisasi

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 di akun audit

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`Kondisi 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 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.

Kebijakan ini tidak memengaruhi fungsionalitas beban kerja Anda yang ada. Kebijakan 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
```

Untuk informasi selengkapnya tentang kunci kondisi ini, lihat dokumentasi IAM dan posting blog IAM berjudul "Gunakan kontrol yang dapat diskalakan untuk AWS layanan yang mengakses sumber daya Anda.”

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 CloudWatch Events memberikan aliran peristiwa sistem yang mendekati real-time yang menjelaskan perubahan AWS sumber daya. CloudWatch Peristiwa memungkinkan 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. CloudWatchKemampuan log memungkinkan Anda melakukan kueri yang lebih terperinci dan akurat daripada yang biasanya dapat Anda gunakan. CloudTrail

Untuk informasi selengkapnya, lihat Mencatat Tindakan AWS Control Tower dengan AWS CloudTrail.

Mencatat Tindakan AWS Control Tower 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 AWS Control Tower sebagai peristiwa. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail peristiwa secara berkelanjutan ke bucket Amazon S3, termasuk peristiwa untuk AWS Control Tower.

Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. 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 dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, termasuk cara mengonfigurasi dan mengaktifkannya, lihat PanduanAWS CloudTrail Pengguna.

Informasi AWS Control Tower di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuat akun. Ketika aktivitas peristiwa yang didukung terjadi di AWS Control Tower, aktivitas tersebut direkam dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di AWS akun Anda. Untuk informasi selengkapnya, lihat Melihat Acara dengan Riwayat CloudTrail Acara.

> **Note**
>
> Dalam rilis AWS Control Tower sebelum landing zone 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 peristiwa untuk AWS Control Tower, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan 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 menindaklanjuti 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 Notifikasi Amazon SNS untuk CloudTrail
- Menerima File CloudTrail Log dari Beberapa Wilayah dan Menerima File CloudTrail Log dari Beberapa Akun

AWS Control Tower mencatat tindakan berikut sebagai peristiwa dalam file CloudTrail log:

API Publik

- `DisableControl`
- `EnableControl`
- `GetControlOperation`
- `ListEnabledControls`

API lainnya

- `SetupLandingZone`
- `UpdateAccountFactoryConfig`
- `ManageOrganizationalUnit`
- `CreateManagedAccount`
- `EnableGuardrail`
- `GetLandingZoneStatus`
- `GetHomeRegion`
- `ListManagedAccounts`
- `DescribeManagedAccount`
- `DescribeAccountFactoryConfig`

- `DescribeGuardrailForTarget`
- `DescribeManagedOrganizationalUnit`
- `ListEnabledGuardrails`
- `ListGuardrailViolations`
- `ListGuardrails`
- `ListGuardrailsForTarget`
- `ListManagedAccountsForGuardrail`
- `ListManagedAccountsForParent`
- `ListManagedOrganizationalUnits`
- `ListManagedOrganizationalUnitsForGuardrail`
- `GetGuardrailComplianceStatus`
- `DescribeGuardrail`
- `ListDirectoryGroups`
- `DescribeSingleSignOn`
- `DescribeCoreService`
- `GetAvailableUpdates`

Setiap peristiwa atau entri log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut:

- Apakah permintaan itu dibuat dengan kredenal pengguna root atau AWS Identity and Access Management (IAM).
- Apakah permintaan dibuat dengan kredensial keamanan sementara untuk suatu peran atau pengguna gabungan.
- Apakah permintaan itu dibuat oleh AWS layanan lain.
- Apakah permintaan ditolak karena akses ditolak atau diproses dengan sukses.

Untuk informasi lain, lihat Elemen userIdentity CloudTrail .

Contoh: Entri File Log AWS Control Tower

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 manapun 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 arsip log.

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 semua akun yang terdaftar. Melalui saluran pengiriman ini, ia mencatat semua perubahan yang direkam oleh AWS Config di akun arsip log, di mana mereka disimpan ke folder di bucket Amazon Simple Storage Service.

Mengelola 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.

Melihat data AWS Config 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

Kueri data AWS Config perekam 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 Amazon QuickSight

Anda dapat memvisualisasikan dan meminta sumber daya yang direkam oleh AWS Config seluruh organisasi Anda. Untuk informasi selengkapnya, lihat Memvisualisasikan AWS Config data menggunakan Amazon Athena dan Amazon. QuickSight

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.

AWS Config Biaya tinggi

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 AWS Config yang 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 AWS Control Tower

Beberapa peristiwa yang dicatat oleh AWS Control Tower adalah peristiwa siklus hidup. Tujuan peristiwa siklus hidup adalah untuk menandai penyelesaian 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 unit organisasi (OU), akun, dan kontrol.

Karakteristik peristiwa siklus hidup AWS Control Tower

- Untuk setiap peristiwa siklus hidup, log peristiwa menunjukkan apakah tindakan Control Tower yang berasal berhasil diselesaikan, atau gagal.

- AWS CloudTrail secara otomatis mencatat setiap peristiwa siklus hidup sebagai acara layanan non-API AWS . Untuk informasi selengkapnya, lihat Panduan AWS CloudTrail Pengguna.
- Setiap acara siklus hidup juga dikirimkan ke layanan Amazon dan EventBridge Amazon CloudWatch Events.

Peristiwa siklus hidup di AWS Control Tower menawarkan dua manfaat utama:

- Karena peristiwa siklus hidup mendaftarkan penyelesaian tindakan AWS Control Tower, Anda dapat membuat aturan Amazon EventBridge atau aturan CloudWatch Acara Amazon 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 mengandalkan beberapa layanan untuk mengimplementasikan tindakannya. Oleh karena itu, setiap peristiwa siklus hidup direkam 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 mendasari telah berhasil diselesaikan, status peristiwa siklus hidup dicatat sebagai Berhasil.
- Jika salah satu sub-langkah yang mendasari tidak berhasil diselesaikan, status peristiwa siklus hidup dicatat sebagai Gagal.

Setiap peristiwa siklus hidup menyertakan stempel waktu yang dicatat yang menunjukkan kapan tindakan AWS Control Tower dimulai, dan stempel waktu lain yang ditampilkan saat peristiwa siklus hidup selesai, menandai keberhasilan atau kegagalan.

Melihat peristiwa siklus hidup di Control Tower

Anda dapat melihat peristiwa siklus hidup dari halaman Aktivitas di dasbor AWS Control Tower.

- Untuk menavigasi ke halaman Aktivitas, pilih Aktivitas 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 dalam 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 dari CreateManagedAccount dan UpdateManagedAccount peristiwa 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 membuat akun setelah kesalahan, atau saat 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 UpdateManagedAccountuntuk mencari peristiwa siklus hidup serta peristiwa siklus hidup. CreateManagedAccount

Nama acara siklus hidup

Setiap peristiwa siklus hidup diberi nama sedemikian rupa sehingga sesuai dengan tindakan AWS Control Tower yang berasal, yang juga direkam oleh AWS. CloudTrail Jadi, misalnya, peristiwa siklus hidup yang berasal dari peristiwa AWS Control Tower `CreateManagedAccount` CloudTrail 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 oleh “//” 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 rangkaian 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 account factory.
- `EnableGuardrail`: Log mencatat apakah AWS Control Tower berhasil menyelesaikan setiap tindakan untuk mengaktifkan kontrol pada OU yang dibuat oleh AWS Control Tower.
- `DisableGuardrail`: Log mencatat apakah AWS Control Tower berhasil menyelesaikan setiap tindakan untuk menonaktifkan kontrol pada OU yang dibuat oleh AWS Control Tower.
- `SetupLandingZone`: Log mencatat apakah AWS Control Tower berhasil menyelesaikan setiap tindakan untuk menyiapkan landing zone.
- `UpdateLandingZone`: Log mencatat apakah AWS Control Tower berhasil menyelesaikan setiap tindakan untuk memperbarui landing zone 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 tata kelola Perpanjang selesai dengan sukses.

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 account factory. Acara ini sesuai dengan peristiwa AWS Control Tower `CreateManagedAccount` CloudTrail . Log peristiwa siklus hidup mencakup `accountName` dan `accountId` dari akun yang baru dibuat, dan `organizationalUnitName` dan `organizationalUnitId` dari OU di mana akun telah 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 yang terkait dengan akun yang dibuat sebelumnya dengan menggunakan account factory. Acara ini sesuai dengan peristiwa AWS Control Tower `UpdateManagedAccount` CloudTrail. Log peristiwa siklus hidup mencakup `accountName` dan `accountId` dari akun terkait, dan `organizationalUnitName` dan `organizationalUnitId` dari OU di mana 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":"624281831893"
                    },
                "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 peristiwa AWS Control Tower `EnableGuardrail` CloudTrail . Log peristiwa siklus hidup mencakup `guardrailId` dan `guardrailBehavior` kontrol, dan `organizationalUnitName` dan `organizationalUnitId` dari 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 peristiwa AWS Control Tower `DisableGuardrail` CloudTrail . Log peristiwa siklus hidup mencakup `guardrailId` dan `guardrailBehavior` kontrol, dan `organizationalUnitName` dan `organizationalUnitId` dari 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 landing zone. Acara ini sesuai dengan peristiwa AWS Control Tower `SetupLandingZone` CloudTrail . Log peristiwa siklus hidup menyertakan`rootOrganizationalId`, yang merupakan ID organisasi yang dibuat AWS Control Tower dari akun manajemen. Entri log juga mencakup `organizationalUnitName` dan `organizationalUnitId` untuk masing-masing OU, dan `accountName` dan `accountId` untuk setiap akun, yang dibuat saat AWS Control Tower menyiapkan landing zone.

```
{
    "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 landing zone yang ada. Acara ini sesuai dengan peristiwa AWS Control Tower `UpdateLandingZone`

CloudTrail . Log peristiwa siklus hidup menyertakan`rootOrganizationalId`, yang merupakan ID organisasi (diperbarui) yang diatur oleh AWS Control Tower. Entri log juga mencakup `organizationalUnitName` dan `organizationalUnitId` untuk masing-masing OU, dan `accountName` dan `accountId` untuk setiap akun, yang dibuat sebelumnya, ketika AWS Control Tower awalnya mengatur landing zone.

```
{
    "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 peristiwa AWS Control Tower `RegisterOrganizationalUnit` CloudTrail . Log peristiwa siklus hidup mencakup `organizationalUnitName` dan `organizationalUnitId` dari OU yang dibawa AWS Control Tower di bawah tata kelolanya.

```
{
    "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 peristiwa AWS Control Tower `DeregisterOrganizationalUnit` CloudTrail . Log peristiwa siklus hidup mencakup `organizationalUnitName` dan `organizationalUnitId` OU tempat AWS Control Tower menonaktifkan fitur tata kelolanya.

```
{
    "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 deregistered an
 organizational unit, and enabled mandatory guardrails on the new 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 peristiwa AWS Control Tower `PrecheckOrganizationalUnit` CloudTrail . Log peristiwa siklus hidup berisi bidang untuk,, dan `failedPrechecks` nilai `IdName`, untuk setiap sumber daya tempat AWS Control Tower telah melakukan pemeriksaan awal selama proses pendaftaran OU.

Log peristiwa juga berisi informasi tentang akun bersarang tempat precheck dilakukan, termasuk, `accountNameaccountId`, dan `failedPrechecks` bidang.

Jika `failedPrechecks` nilainya kosong, itu berarti semua precheck untuk sumber daya itu berhasil lolos.

- Acara 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"
}
```

Menggunakan Notifikasi AWS Pengguna dengan AWS Control Tower

Anda dapat menggunakan PemberitahuanAWS 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, notifikasi AWS Chatbotobrolan, atau pemberitahuan push Aplikasi SelulerAWS 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 area bell/notifikasi di 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 notifikasi yang mungkin ingin Anda terima adalah jika terdapat temuan kritis dan tingkat keparahan yang tinggi dari Security Hub. 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"]
      }
    }
  }
}
```

Penyaringan acara

- 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 9 event names 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
        }
    }
}
```

Panduan

Bab ini berisi prosedur panduan yang dapat membantu Anda dalam penggunaan AWS Control Tower.

Topik

Panduan: Pindah dari ALZ ke AWS Control Tower

Banyak AWS pelanggan telah mengadopsi solusi AWS Landing Zone (ALZ) untuk menyiapkan lingkungan AWS multi-akun yang aman, sesuai, dan aman. Untuk mengurangi beban pengelolaan landing zone, 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 untuk pindah ke layanan AWS Control Tower dari ALZ. Blog yang ditautkan dalam chapter ini memandu Anda melalui berbagai pertimbangan untuk langkah itu, dan ini menjelaskan bagaimana Anda dapat merencanakan migrasi yang sukses dari ALZ ke AWS Control Tower.

Blog: Migrasikan solusi Zona AWS Pendaratan ke AWS Control Tower

AWS Prescriptive Guidance 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 ada yang menjalankan ALZ, berdasarkan sejumlah prasyarat. Untuk selengkapnya, lihat Transisi dari Zona AWS Pendaratan ke AWS Control Tower.

Panduan: Mengotomatiskan Penyediaan Akun di AWS Control Tower oleh 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.

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:

```
{
  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.

Panduan: Konfigurasikan AWS Control Tower 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 AWS Control Tower virtual private cloud (VPC) virtual. VPC ini dibuat saat Anda mengatur landing zone.
- Anda dapat mengubah pengaturan Account Factory sehingga 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 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.

Hapus AWS Control Tower VPC

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 landing zone 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 Control Tower VPC.

Saat Anda melihat AWS Control Tower VPC di konsol VPC Amazon, 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 VPC AWS Control Tower yang benar.

Anda dapat menghapus AWS Control Tower VPC, tetapi jika nanti Anda 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 Service Catalog. Anda kemudian melihat Dasbor VPC.

3. Dari menu di sebelah kiri, pilih VPC Anda. Anda kemudian melihat daftar semua VPC Anda.
4. Identifikasi AWS Control Tower VPC berdasarkan rentang CIDR-nya.
5. Untuk menghapus VPC, pilih Tindakan dan kemudian pilih Hapus VPC.

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 hapus AWS VPC default yang terkait dengan akun manajemen dari semua Wilayah. AWS Oleh karena itu, untuk mengamankan akun manajemen, hapus VPC default dari setiap Wilayah, serta menghapus VPC yang dibuat oleh Control Tower di wilayah asal AWS Control Tower Anda.

Membuat Akun di AWS Control Tower Tanpa VPC

Jika beban kerja pengguna akhir Anda tidak memerlukan VPC, Anda dapat menggunakan metode ini untuk menyiapkan akun pengguna akhir yang tidak memiliki VPC yang dibuat untuk mereka secara otomatis.

Dari dasbor AWS Control Tower, Anda dapat melihat dan mengedit pengaturan konfigurasi jaringan Anda. Setelah Anda mengubah pengaturan sehingga akun AWS Control Tower dibuat tanpa VPC terkait, semua akun baru dibuat tanpa VPC hingga 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 Account Factory dengan bagian Network Configuration.
4. Perhatikan pengaturan saat ini jika Anda bermaksud memulihkannya nanti.
5. Pilih tombol Edit di bagian Konfigurasi Jaringan.
6. Di halaman konfigurasi jaringan pabrik Edit akun, buka bagian opsi Konfigurasi VPC untuk akun baru.

   Anda dapat mengikuti Opsi 1 atau Opsi 2, atau keduanya, untuk memastikan AWS Control Tower tidak membuat VPC saat menyediakan akun.

   a. Opsi 1 - Menghapus subnet

      - Matikan sakelar sakelar sakelar subnet yang dapat diakses Internet.

- Atur jumlah maksimum nilai subnet pribadi ke 0.

b. Opsi 2 - Menghapus AWS Wilayah

- Hapus setiap kotak centang di kolom Regions for VPC creation.

7. Pilih Simpan.

Kemungkinan Kesalahan

Waspadai 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 di tempat saat mengatur 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 menunjukkan kepada Anda cara menggunakan layanan AWS Firewall Manager untuk memberikan peningkatan keamanan jaringan Anda untuk AWS Control Tower. Anda dapat menetapkan akun administrator keamanan yang diaktifkan untuk menyiapkan grup keamanan. Anda akan melihat bagaimana Anda dapat mengonfigurasi kebijakan keamanan dan menerapkan aturan keamanan untuk organisasi AWS Control Tower Anda, dan bagaimana Anda dapat memulihkan 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 Anda sendiri, atau Anda dapat berlangganan aturan dari vendor tepercaya.

Mengatur Grup Keamanan Dengan AWS Firewall Manager

Video ini (8:02) menjelaskan cara mengatur 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. Captioning tersedia.

Panduan Video Penyiapan Firewall di AWS Control Tower.

Untuk informasi selengkapnya, lihat dokumentasi tentang cara mengatur AWS WAF.

Panduan: Menonaktifkan Zona Pendaratan 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, AWS Control Tower melakukan tindakan berikut.

- Menonaktifkan setiap kontrol detektif diaktifkan di landing zone. AWS Control Tower menghapus AWS 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 akan melepaskan dan menghapus kebijakan sepenuhnya.
- Menghapus semua cetak biru yang digunakan sebagai. AWS 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. `OrganizationsFullAccessRole`
  - 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. `OrganizationsFullAccessRole`

- 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.

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 dua unit organisasi (OU), bernama Security dan Sandbox. 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 akun AWS dan kumpulan izin Pusat Identitas IAM tidak dihapus.
- Direktori IAM Identity Center tidak diubah.

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`

Bucket Amazon S3

Selama penyiapan, AWS Control Tower membuat bucket di akun logging untuk logging dan akses logging. Saat Anda menonaktifkan landing zone, sumber daya berikut tidak akan dihapus:

- Logging dan logging access S3 bucket di akun logging tidak dihapus.
- Isi bucket akses logging dan logging tidak dihapus.

Akun Bersama

Dua akun bersama (Audit dan Arsip Log) dibuat di OU Keamanan selama penyiapan AWS Control Tower. Saat Anda menonaktifkan landing zone Anda:

- Akun bersama 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 pabrik akun untuk membuat akun AWS 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-MANAGEMENT` Grup log ini tidak dihapus. Sebaliknya, cetak biru dihapus dan sumber daya dipertahankan.

- Grup log ini harus dihapus secara manual sebelum Anda mengatur landing zone lain.

> **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 bersama dan 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 dalam[Kelola Sumber Daya AWS Control Tower](#).

Kelola 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 Panduan: Menonaktifkan Zona Pendaratan 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. AWS Management Console

> **Warning**
>
> Ini adalah tindakan destruktif yang dapat memperkenalkan penyimpangan tata kelola ke penyiapan AWS Control Tower Anda. Mereka tidak bisa dibatalkan.

Topik

Hapus SCP

AWS Control Tower menggunakan kebijakan kontrol layanan (SCP) untuk kontrolnya. Prosedur ini membahas cara menghapus SCP yang secara khusus terkait dengan AWS Control Tower.

Untuk menghapus AWS Organizations SCP

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 AWS CloudFormation StackSets

1. Buka AWS 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 ID AWS akun 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 ID AWS akun yang Anda buat catatan di langkah 3.b, dipisahkan dengan koma. Misalnya: *123456789012*, *098765431098*, dan sebagainya.
   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 AWS CloudFormation tumpukan

1. Buka AWS CloudFormation konsol di https://console.aws.amazon.com/cloudformation.
2. Dari dasbor Stacks, cari semua tumpukan dengan awalan. AWSControlTower
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 AWS Management Console 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 TowerAWS Account Factory.
6. Pilih HAPUS KENDALA.
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 AWSServiceCatalogEndUserAccess 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 Perizinan set.
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 tersebut.
    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.

Cara menonaktifkan landing zone

Untuk menonaktifkan landing zone AWS Control Tower Anda, ikuti prosedur yang diberikan di sini.

> **Note**
>
> Kami menyarankan Anda membatalkan kelola akun Anda yang terdaftar sebelum dinonaktifkan.

1. Arahkan ke halaman Pengaturan Zona Landing di konsol AWS Control Tower.
2. Pilih Donaktifkan landing zone Anda di bagian Donaktifkan landing zone Anda.
3. 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.

4. 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.
5. 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.

6. 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
```

Tugas pembersihan manual diperlukan setelah dinonaktifkan

- 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 set CloudFormation tumpukan AWS 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.

Pengaturan setelah menonaktifkan landing zone

Setelah Anda menonaktifkan landing zone Anda, Anda tidak dapat berhasil menjalankan 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 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 Anda menaikkan 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 logging 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 aturan terkelola yang tersisa`AWSControlTowerManagedRule`, dipanggil, dari akun bersama dan anggota untuk semua Wilayah yang diatur.

> **Note**
>
> Anda tidak dapat menyiapkan landing zone baru di organisasi dengan OU tingkat atas bernama Security atau Sandbox. Anda harus mengganti nama atau menghapus OU ini untuk mengatur landing zone lagi.

Memecahkan 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.

Peluncuran Zona Pendaratan Gagal

Penyebab umum kegagalan peluncuran landing zone:

- Kurangnya respons terhadap pesan email konfirmasi.
- AWS 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 AWS 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 melihat daftar AWS Control Tower Wilayah AWS yang didukung, lihatBagaimana AWS Wilayah Bekerja Dengan AWS Control Tower.

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 dengan AWS Service Catalog 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 AWS 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.
- Konteks/dampak: Aturan AWS Config Deployed 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.
- Konteks/dampak: Jika akun tidak dikembalikan ke OU aslinya, statusnya akan tidak konsisten dengan kontrol yang ditentukan oleh OU baru di dalamnya.
- Memperbarui akun bukanlah perbaikan yang valid, karena tidak menghapus AWS Config aturan yang terkait dengan OU sebelumnya.

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 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 sudah 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

Tidak Ada Jalur Peluncuran Ditemukan Kesalahan

Saat Anda mencoba membuat akun baru, Anda mungkin melihat pesan kesalahan yang mirip dengan yang ini:

```
No launch paths found for resource: prod-dpqqfywxxxx
```

Pesan kesalahan ini dihasilkan oleh AWS Service Catalog, yang merupakan layanan terintegrasi yang membantu menyediakan akun di AWS Control Tower.

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 terlampaui kesalahan yang dikembalikan oleh API AWS Organizations

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 ini removing-and-deleting 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, target dasar dapat berupa akun bersama atau landing zone secara keseluruhan. Garis dasar tertentu dapat diaktifkan dan diperbarui 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 untuk target, baseline direpresentasikan sebagai AWS CloudFormation sumber daya, yang disebut sumber daya. `EnabledBaseline`

AWS Control Tower mencakup empat jenis dasar penting:

- Satu jenis dapat berlaku untuk OU yang terdaftar di AWS Control Tower, atau ke OU yang ingin Anda daftarkan dengan menerapkan baseline.
- Tiga tipe dasar dapat diterapkan ke landing zone atau akun bersama, selama pengaturan awal atau selama pembaruan landing zone.

Jenis dasar yang berlaku di tingkat OU, untuk mendaftar dan memperbarui OU

- Nama: `AWSControlTowerBaseline`

  Deskripsi: Menyiapkan sumber daya dan kontrol wajib untuk akun anggota dalam OU target, yang diperlukan untuk tata kelola 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**
  >
  > Wilayah tingkat OU menolak kontrol tidak memiliki cara untuk mengizinkan Wilayah yang tidak diizinkan oleh zona pendaratan yang tidak diizinkan oleh Wilayah.

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.

> **Note**
>
> Garis dasar zona pendaratan berperilaku berbeda dari garis dasar tingkat OU.

AWS Control Tower memungkinkan baseline yang berlaku di level landing zone secara otomatis, 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.

Jenis baseline yang mungkin berlaku untuk landing zone atau akun bersama

- Nama: `AuditBaseline`

  Deskripsi: Menyiapkan sumber daya untuk memantau keamanan dan kepatuhan akun di organisasi Anda. Anda tidak dapat mengubah baseline ini, ini diterapkan oleh AWS Control Tower.
- Nama: `LogArchiveBaseline`

  Deskripsi: Menyiapkan repositori pusat untuk log aktivitas API dan konfigurasi sumber daya dari akun di organisasi Anda. Anda tidak dapat mengubah baseline ini, ini diterapkan oleh AWS Control Tower.
- 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.

Pendaftaran sebagian akun

Saat Anda bekerja dengan baseline, akun dapat ditempatkan ke dalam 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 Daftar ulang atau 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.

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 baseline level OU`AWSControlTowerBaseline`, tabel berikut menunjukkan kompatibilitas baseline dengan versi landing zone AWS Control Tower.

Versi dasar	Versi zona pendaratan	Cetak biru yang disertakan	Termasuk kontrol	Ubah dari baseline sebelumnya	
1.0	2.0 hingga 2.7	BP_BASELINE_CLOUDTRAIL, BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_ROLES, Sumber Daya IAM	Semua kontrol wajib	Tidak ada	
2.0	2,8 hingga 2,9	BP_BASELINE_CLOUDT	Semua kontrol wajib	Menambahkan peran	

Versi dasar	Versi zona pendaratan	Cetak biru yang disertakan	Termasuk kontrol	Ubah dari baseline sebelumnya	
		RAIL, BP_BASELINE_CLOUDWATCH, BP_BASELINE_CONFIG, BP_BASELINE_ROLES, BP_BASELINE_SERVICE_ROLES, Config SLR, sumber daya IAM		AWS Config terkait layanan (SLR) dan cetak biru Config baru untuk menggunakan SLR	
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	Semua kontrol wajib	AWS Config Cetak biru baru. Ubah untuk merekam sumber daya global hanya di wilayah asal. CloudTrail Cetak biru yang dihapus	

Versi dasar	Versi zona pendaratan	Cetak biru yang disertakan	Termasuk kontrol	Ubah dari baseline sebelumnya	
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	Semua kontrol wajib	Cetak biru SLR baru	

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 pabrik akun dan fitur lainnya tanpa memperbarui baseline OU segera, kecuali dalam kasus pembaruan landing zone dari 2.x ke 3.x.
- 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**
>
> Jika Anda memperbarui landing zone AWS Control Tower dari versi 2.X apa pun ke versi 3.X apa pun, Anda juga harus memperbarui versi dasar pada OU Anda, karena perubahan dari jalur tingkat akun ke tingkat organisasi. AWS CloudTrail Di konsol, OU Anda akan menampilkan status Pembaruan yang diperlukan.

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 AWS Control Tower OU hanya dengan API

Panduan contoh ini adalah dokumen pendamping. Untuk penjelasan, peringatan, dan informasi lebih lanjut, lihat. Jenis 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 landing zone. Jika demikian, dapatkan Identity Center Enabled Baseline identifier.

```
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 target OU.

```
aws organizations describe-organizational-unit --organizational-unit-id
 <Organizational Unit ID> --query 'OrganizationalUnit.[Arn]'
```

3. Dapatkan ARN dari baseline. `AWSControlTowerBaseline`

```
aws controltower list-baselines --query 'baselines[?name==`AWSControlTowerBaseline`].
[arn]'
```

4. Buat `AWSControlTowerBaseline` baseline pada target OU.

   Jika Garis Dasar Pusat Identitas 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 Garis Dasar Pusat Identitas tidak diaktifkan, hilangkan *`parameters`* bendera, sebagai berikut:

```

aws controltower enable-baseline --baseline-identifier <AWSControlTowerBaseline ARN>
 --baseline-version <BASELINE VERSION> --target-identifier <OU ARN>
```

Registrasi ulang OU

Setelah Anda melakukan pembaruan pada pengaturan landing zone, atau memperbarui versi landing zone Anda, Anda harus mendaftar ulang OU untuk memberi mereka perubahan terbaru. Ikuti langkah-langkah ini untuk mendaftarkan ulang OU secara terprogram, dengan mengatur ulang sumber daya terkait. `EnabledBaseline`

1. Dapatkan ARN dari target OU untuk mendaftar ulang.

```
aws organizations describe-organizational-unit --organizational-unit-id <OU ID> --
query 'OrganizationalUnit.[Arn]'
```

2. Dapatkan ARN `EnabledBaseline` sumber daya untuk target OU.

```
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>
```

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`kekuaran:

```
{
    "operationIdentifier": "58f12232-26be-4735-a3e9-dd30d90f021f",
    "arn": "arn:aws:controltower:us-west-2:123456789012:enabledbaseline/
XAHCR4CJTSI4W07MZ"
}
```

`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-west-1::baseline/4T4HA1KMO10S6311",
            "name": "AuditBaseline",
            "description": "Sets up resources to monitor security and compliance of
 accounts in your organization."
        },
        {
            "arn": "arn:aws:controltower:us-west-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-west-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-west-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."
        }
    ]
}
```

`ListBaselines`Contoh CLI:

```
aws controltower list-baselines \
    --region us-west-2
```

`ListEnabledBaselines`

Untuk informasi selengkapnya tentang operasi API ini, lihat ListEnabledBaselines.

`ListEnabledBaselines`masukan (tidak ada filter):

```
{
    "nextToken": "bde7-XX0c6fXXXXXX",
    "maxResults": 5
```

```
}
```

`ListEnabledBaselines`sinput (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`sinput (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`sinput (`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 terkait

Topik ini mencantumkan kasus penggunaan umum dan praktik terbaik untuk kemampuan AWS Control Tower dan penyempurnaan tambahan. Topik ini juga mencakup tautan ke posting blog yang relevan, dokumentasi teknis, dan sumber daya terkait yang dapat membantu Anda saat Anda bekerja dengan AWS Control Tower.

Tutorial dan lab

- AWS Control Tower lab — Laboratorium ini memberikan gambaran umum tingkat tinggi tentang tugas-tugas umum yang terkait dengan AWS Control Tower.
- Di dasbor AWS Control Tower, pilih Dapatkan panduan yang dipersonalisasi jika Anda memiliki kasus penggunaan, tetapi Anda tidak yakin harus mulai dari mana.
- Coba kunjungi daftar YouTube video yang dikuratori 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 Arsitektur VPC Mulai Cepat — Panduan Mulai Cepat ini menyediakan fondasi 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.
- VPC swalayan di AWS Control Tower menggunakan AWS Service Catalog — Posting blog ini menjelaskan cara menyiapkan Account Factory sehingga Anda dapat menyediakan akun dengan VPC yang disesuaikan.
- 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 logging.

Keamanan

- Mengotomatiskan AWS Security Hub Peringatan dengan peristiwa siklus hidup AWS Control Tower — Posting blog ini menjelaskan cara mengotomatiskan pengaktifan dan konfigurasi Security Hub 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 IAM Access Analyzer.
- 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 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 sistem 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 AWS Wilayah.

Menyebarkan sumber daya dan mengelola beban kerja

Menyebarkan dan mengelola sumber daya dan beban kerja.

- Integrasi Perpustakaan Memulai - Posting blog ini menjelaskan portofolio Memulai yang dapat Anda gunakan.
- Penerapan Cloud Custodian secara berkelanjutan ke AWS Control Tower

Bekerja dengan organisasi dan akun yang ada

Bekerja dengan AWS organisasi dan akun yang ada.

- Mendaftarkan akun — Topik panduan pengguna ini menjelaskan cara mendaftarkan AWS akun yang ada di AWS Control Tower.
- Bawa akun di AWS Control Tower — Postingan blog ini menjelaskan cara menerapkan AWS Control Tower ke AWS organisasi Anda yang ada.
- Perluas tata kelola AWS Control Tower menggunakan paket kesesuaian AWS Config — Posting blog ini menjelaskan cara AWS Config menerapkan paket kesesuaian untuk membantu membawa akun dan organisasi yang ada ke dalam tata kelola oleh AWS Control Tower.
- Cara Mendeteksi dan Mengurangi Pelanggaran Pagar Pembatas dengan AWS Control Tower — Posting blog ini menjelaskan cara menambahkan kontrol dan cara berlangganan notifikasi SNS sehingga Anda dapat diberi tahu 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.
- Mengotomatiskan 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 VPC Amazon 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 AWS Control Tower Anda disiapkan.

Memigrasi 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 lainnya 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 AWS Organizations dengan layanan AWS lainnya.

  > **Note**
  >
  > Ingat bahwa AWS IAM Identity Center, 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 selengkapnya, lihat Mengonfigurasi Administrator Delegasi, dan Mengaktifkan akun administrator

yang didelegasikan untuk Firewall Manager. Lihat juga video ini, Siapkan grup keamanan dengan AWS Firewall Manager.

AWS Marketplace solusi

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 yang memerlukan pembaruan untuk landing zone AWS Control Tower, serta rilis yang 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. Karena mungkin ada jeda antara ketika fitur atau rilis didokumentasikan dan ketika diumumkan secara resmi, tanggal yang tercantum untuk fitur atau rilis di sini mungkin sedikit berbeda dari tanggal diRiwayat dokumen.

Fitur dirilis pada tahun 2024

Fitur dirilis pada tahun 2023

Fitur dirilis pada tahun 2022

Fitur dirilis pada tahun 2021

Fitur dirilis pada tahun 2020

Fitur dirilis pada 2019

Januari 2024 - Sekarang

Sejak Januari 2024, AWS Control Tower telah merilis pembaruan berikut:

- AWS Control Tower mendukung hingga 100 operasi kontrol bersamaan
- AWS Control Tower tersedia di AWS Kanada Barat (Calgary)
- AWS Control Tower mendukung penyesuaian kuota swalayan
- AWS Control Tower merilis Panduan Referensi Kontrol
- AWS Control Tower memperbarui dan mengganti nama dua kontrol proaktif
- Kontrol usang tidak lagi tersedia
- AWS Control Tower mendukung `EnabledControl` sumber daya penandaan di AWS CloudFormation
- AWS Control Tower mendukung API untuk pendaftaran dan konfigurasi OU dengan baseline

AWS Control Tower mendukung hingga 100 operasi kontrol bersamaan

Mei 20, 2024

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

AWS Control Tower sekarang mendukung beberapa operasi kontrol dengan konkurensi yang lebih tinggi. Anda dapat mengirimkan hingga 100 operasi kontrol AWS Control Tower, di beberapa unit organisasi (OU), secara bersamaan, dari konsol atau dengan API. Hingga sepuluh (10) operasi dapat berjalan secara bersamaan, dan yang tambahan diantrian. 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 baru di konsol AWS Control Tower, atau Anda dapat memanggil API baru `ListControlOperations`.

Pustaka AWS Control Tower berisi lebih dari 500 kontrol, yang dipetakan ke berbagai tujuan kontrol, kerangka kerja, dan layanan. Untuk tujuan kontrol tertentu, seperti Enkripsi data saat istirahat, Anda dapat mengaktifkan beberapa kontrol dengan satu operasi kontrol, 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 landing zone AWS Control Tower.)

Mulai hari ini, Anda dapat mengaktifkan AWS Control Tower di Wilayah Canada West (Calgary). Jika Anda telah menerapkan AWS Control Tower dan ingin memperluas fitur tata kelola ke Wilayah ini, Anda dapat melakukannya dengan AWS Control Tower landing zone API. Atau dari konsol, buka halaman Pengaturan di dasbor AWS Control Tower, pilih Wilayah, lalu perbarui landing zone Anda.

Wilayah Kanada Barat (Calgary) tidak mendukung. AWS Service Catalog Untuk alasan ini, beberapa fungsi AWS Control Tower berbeda. Perubahan fungsionalitas yang paling menonjol adalah Account Factory tidak tersedia. Jika Anda memilih Canada West (Calgary) sebagai Wilayah asal Anda, prosedur untuk memperbarui akun, menyiapkan otomatisasi akun, dan proses lain yang melibatkan Service Catalog berbeda dari di Wilayah lain.

Akun penyediaan

Untuk membuat dan menyediakan akun baru di Wilayah Kanada Barat (Calgary), sebaiknya Anda membuat akun di luar AWS Control Tower, lalu mendaftarkannya ke OU terdaftar. Untuk informasi selengkapnya, lihat Mendaftarkan akun yang ada dan Langkah-langkah untuk mendaftarkan akun.

Service Catalog API tidak tersedia di Wilayah Canada West (Calgary). Contoh skrip yang ditampilkan dalam penyediaan akun Automate di AWS Control Tower by Service Catalog API tidak dapat diterapkan.

Kustomisasi Account Factory (AFC), Account Factory for Terraform (AFT), dan Kustomisasi untuk AWS Control Tower (CFCT) tidak tersedia di Canada West (Calgary), karena kurangnya dependensi mendasar lainnya untuk AWS Control Tower. 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 Service Catalog tersedia di Wilayah asal Anda.

Kontrol

Kontrol dan kontrol proaktif untuk Standar yang AWS Security Hub Dikelola Layanan: AWS Control Tower tidak tersedia di Wilayah Canada West (Calgary). Kontrol pencegahan 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 Keterbatasan kontrol.

Penyedia identitas

IAM Identity Center tidak tersedia di Canada West (Calgary). Rekomendasi praktik terbaik adalah mengatur landing zone Anda di Wilayah di mana IAM Identity Center tersedia. Atau, Anda memiliki opsi untuk mengelola sendiri konfigurasi akses akun Anda jika Anda menggunakan penyedia identitas eksternal di Kanada Barat (Calgary).

Tidak tersedianya Service Catalog di Wilayah Canada West (Calgary) tidak berpengaruh pada Wilayah lain yang didukung oleh AWS Control Tower. Perbedaan ini hanya berlaku jika wilayah asal Anda adalah Kanada Barat (Calgary).

Untuk daftar lengkap Wilayah di mana AWS Control Tower tersedia, lihat Tabel AWS Wilayah.

AWS Control Tower mendukung penyesuaian kuota swalayan

April 25, 2024

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

AWS Control Tower kini mendukung penyesuaian kuota swalayan melalui konsol Service Quotas. Untuk informasi selengkapnya, lihat Meminta peningkatan kuota.

AWS Control Tower merilis Panduan Referensi Kontrol

April 21, 2024

(Tidak diperlukan pembaruan untuk landing zone 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 AWS Control Tower. Panduan Referensi Kontrol mencakup kontrol dalam format yang diperluas. Untuk informasi selengkapnya, lihat Panduan Referensi AWS Control Tower Controls.

AWS Control Tower memperbarui dan mengganti nama dua kontrol proaktif

Maret 26, 2024

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

AWS Control Tower telah mengganti nama dua kontrol proaktif agar selaras dengan pembaruan ke Amazon Service. OpenSearch

- [CT.OPENSEARCH.PR.8] Memerlukan domain Layanan Elasticsearch untuk menggunakan TLSv1.2
- [CT.OPENSEARCH.PR.16] Memerlukan domain OpenSearch Layanan Amazon untuk menggunakan TLSv1.2

Kami memperbarui nama kontrol dan artefak untuk dua kontrol ini agar selaras dengan rilis terbaru dari OpenSearch Layanan Amazon, yang sekarang mendukung Transport Layer Security (TLS) versi 1.3 di antara opsi keamanan transportasinya untuk keamanan titik akhir domain.

Untuk menambahkan dukungan untuk 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 Nonaktifkan dan Aktifkan kontrol untuk menyebarkan artefak terbaru.

Tidak ada kontrol proaktif lain yang terpengaruh oleh perubahan ini. Kami menyarankan Anda meninjau kontrol ini, untuk memastikan bahwa mereka memenuhi tujuan kontrol Anda.

Untuk pertanyaan atau masalah, hubungi AWS Support.

Kontrol usang tidak lagi tersedia

Maret 12, 2024

(Tidak diperlukan pembaruan untuk landing zone 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 **`EnabledControl`** sumber daya penandaan di AWS CloudFormation

Februari 22, 2024

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

Rilis AWS Control Tower ini memperbarui perilaku `EnabledControl` sumber daya, agar lebih selaras 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 AWS CloudFormation templat. Sebelumnya, Anda dapat menambahkan tag melalui konsol AWS Control Tower dan API saja.

AWS Control Tower `GetEnabledControlEnableControl`,, dan operasi `ListTagsforResource` API diperbarui dengan rilis ini, karena mereka bergantung pada fungsionalitas `EnabledControl` sumber daya.

Untuk informasi selengkapnya, lihat Menandai `EnabledControl` sumber daya di AWS Control Tower dan `EnabledControl`di Panduan AWS CloudFormation Pengguna.

AWS Control Tower mendukung API untuk pendaftaran dan konfigurasi OU dengan baseline

Februari 14, 2024

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

API ini mendukung pendaftaran OU terprogram dengan `EnableBaseline` panggilan tersebut. Saat Anda mengaktifkan baseline pada OU, akun anggota dalam OU didaftarkan ke dalam 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 ekstra agar kontrol opsional diaktifkan.

Garis dasar AWS Control Tower mewujudkan praktik terbaik untuk tata kelola AWS Control Tower dari akun OU dan anggota. Misalnya, ketika Anda mengaktifkan baseline pada OU, akun anggota dalam OU menerima kelompok sumber daya yang ditentukan, termasuk, Pusat Identitas IAM AWS CloudTrail AWS Config, dan peran IAM yang diperlukan AWS .

Garis dasar tertentu kompatibel dengan versi landing zone AWS Control Tower tertentu. AWS Control Tower dapat menerapkan baseline terbaru yang kompatibel ke landing zone Anda, saat Anda mengubah pengaturan landing zone. Untuk informasi selengkapnya, lihat Kompatibilitas baseline OU dan versi landing zone.

Rilis ini mencakup empat hal 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 landing zone. API menyertakan dukungan untuk AWS CloudFormation

`EnabledBaseline` sumber daya, yang memungkinkan Anda mengelola OU Anda dengan infrastruktur sebagai kode (IAc).

API dasar

- EnableBaseline, UpdateEnabledBaseline, DisableBaseline: Ambil tindakan pada garis dasar untuk OU.
- GetEnabledBaseline, ListEnabledBaselines: Temukan konfigurasi untuk garis dasar yang diaktifkan.
- GetBaselineOperation: Lihat status operasi dasar tertentu.
- ResetEnabledBaseline: Perbaiki penyimpangan sumber daya pada OU dengan baseline yang diaktifkan (termasuk OU bersarang dan penyimpangan kontrol wajib). Juga memulihkan penyimpangan untuk landing-zone-level Wilayah yang menolak kontrol
- GetBaseline, ListBaselines: Temukan konten baseline AWS Control Tower.

Untuk mempelajari lebih lanjut tentang API ini, tinjau Baseline di Panduan Pengguna AWS Control Tower, dan Referensi API. API baru tersedia di Wilayah AWS tempat AWS Control Tower tersedia, kecuali Wilayah GovCloud (AS). Untuk daftar Wilayah AWS tempat AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

Januari 2023 - Sekarang

Sejak Januari 2023, AWS Control Tower telah merilis pembaruan berikut:

- Transisi ke jenis produk AWS Service Catalog Eksternal baru (fase 3)
- AWS Control Tower landing zone versi 3.3
- Transisi ke jenis produk AWS Service Catalog Eksternal baru (fase 2)
- AWS Control Tower mengumumkan kontrol untuk membantu kedaulatan digital
- AWS Control Tower mendukung API landing zone
- AWS Control Tower mendukung penandaan untuk kontrol yang diaktifkan
- AWS Control Tower tersedia di Wilayah Asia Pasifik (Melbourne)
- Transisi ke jenis produk AWS Service Catalog Eksternal baru (fase 1)
- API kontrol baru tersedia
- AWS Control Tower menambahkan kontrol tambahan
- Jenis drift baru dilaporkan: akses tepercaya dinonaktifkan

- Empat tambahan Wilayah AWS
- AWS Control Tower tersedia di Wilayah Tel Aviv
- AWS Control Tower meluncurkan 28 kontrol proaktif baru
- AWS Control Tower menghentikan dua kontrol
- AWS Control Tower landing zone versi 3.2
- AWS Control Tower menangani akun berdasarkan ID
- Kontrol detektif Security Hub tambahan tersedia di pustaka kontrol AWS Control Tower
- AWS Control Tower menerbitkan tabel metadata kontrol
- Dukungan Terraform untuk Kustomisasi Account Factory
- AWS Manajemen mandiri IAM Identity Center tersedia untuk landing zone
- AWS Control Tower menangani tata kelola campuran untuk OU
- Tersedia kontrol proaktif tambahan
- Kontrol proaktif Amazon EC2 yang diperbarui
- Tujuh tambahan Wilayah AWS tersedia
- Account Factory untuk penelusuran permintaan kustomisasi akun Terraform (AFT)
- AWS Control Tower landing zone versi 3.1
- Kontrol proaktif umumnya tersedia

Transisi ke jenis produk AWS Service Catalog Eksternal baru (fase 3)

Desember 14, 2023

(Tidak diperlukan pembaruan untuk landing zone 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 Transisi 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 Sumber Terraform Open Source.

AWS Control Tower landing zone versi 3.3

Desember 14, 2023

(Pembaruan diperlukan untuk landing zone AWS Control Tower ke versi 3.3. Untuk informasi, lihatPerbarui Zona Pendaratan Anda).

Pembaruan kebijakan bucket S3 di akun AWS Control Tower Audit

Kami telah memodifikasi kebijakan bucket Audit Amazon S3 yang diterapkan AWS Control Tower di akun, sehingga `aws:SourceOrgID` kondisi harus dipenuhi untuk izin menulis 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 menyetel nilainya ke ID organisasi 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; ini mencegah CloudTrail log di luar organisasi Anda menulis ke bucket AWS Control Tower S3 Anda.

Kami membuat perubahan ini untuk memulihkan potensi kerentanan keamanan, tanpa memengaruhi fungsionalitas beban kerja Anda yang ada. Untuk melihat kebijakan yang diperbarui, lihatKebijakan bucket Amazon S3 di akun audit.

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 SNS. AWS Config

Pembaruan untuk kontrol wilayah Deny landing zone

- Dihapus`discovery-marketplace:`. Tindakan ini dicakup oleh `aws-marketplace:*` pengecualian.
- Ditambahkan `quicksight:DescribeAccountSubscription`

AWS CloudFormation Template diperbarui

Kami memperbarui AWS CloudFormation template untuk tumpukan bernama `BASELINE-CLOUDTRAIL-MASTER` sehingga tidak menunjukkan penyimpangan ketika AWS KMS enkripsi tidak digunakan.

Transisi ke jenis produk AWS Service Catalog Eksternal baru (fase 2)

Desember 7, 2023

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

HashiCorp memperbarui lisensi Terraform mereka. Akibatnya, AWS Service Catalog mengubah dukungan untuk produk Terraform Open Source dan menyediakan produk ke jenis produk baru, yang disebut Eksternal.

Untuk menghindari gangguan pada beban kerja dan AWS sumber daya yang ada di akun Anda, ikuti langkah transisi AWS Control Tower dalam Transisi ke jenis produk AWS Service Catalog Eksternal paling lambat 14 Desember 2023.

AWS Control Tower mengumumkan kontrol untuk membantu kedaulatan digital

November 27, 2023

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

AWS Control Tower mengumumkan 65 kontrol AWS terkelola 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 residensi data, pembatasan akses terperinci, enkripsi, dan kemampuan ketahanan. Kontrol ini dirancang untuk memudahkan Anda menangani persyaratan dalam skala besar. Untuk informasi lebih lanjut 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 Memerlukan cache AWS AppSync API agar enkripsi saat transit diaktifkan atau Memerlukan Firewall AWS Jaringan untuk diterapkan di beberapa Availability Zone. Anda juga dapat menyesuaikan kontrol penolakan Wilayah AWS Control Tower untuk menerapkan batasan regional yang paling sesuai dengan kebutuhan bisnis unik Anda.

Rilis ini menghadirkan kemampuan penolakan Wilayah AWS Control Tower AWS yang disempurnakan dengan baik. Anda dapat menerapkan kontrol penolakan Wilayah berparameter baru di tingkat OU, untuk meningkatkan perincian tata kelola, sambil mempertahankan tata kelola Wilayah

tambahan di tingkat landing zone. 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 drift dengan cepat, atau untuk menjamin secara terprogram bahwa kontrol tidak dalam keadaan drift. Untuk informasi selengkapnya tentang API baru, lihat AWS Control Tower API Referensi

Kontrol proaktif baru

- CT.APIGATEWAY.PR.6: Memerlukan domain Amazon API Gateway REST 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: Mengharuskan AWS AppSync GraphQL API tidak diautentikasi dengan kunci API
- CT.APPSYNC.PR.4: Memerlukan cache AWS AppSync GraphQL API agar enkripsi saat 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 Auto Scaling Amazon EC2 untuk mengenkripsi data saat istirahat
- CT.AUTOSCALING.PR.10: Memerlukan grup Auto Scaling Amazon EC2 untuk AWS hanya menggunakan jenis instans 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 Auto Scaling Amazon EC2, saat mengganti template peluncuran
- CT.DAX.PR.3: Memerlukan klaster DynamoDB Accelerator untuk mengenkripsi data dalam perjalanan 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 tipe 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 template peluncuran tersebut dengan AWS tipe instans Nitro
- CT.EC2.PR.19: Memerlukan instans Amazon EC2 untuk menggunakan jenis instans nitro yang mendukung enkripsi dalam perjalanan antar instance saat dibuat menggunakan tipe sumber daya `AWS::EC2::Instance`
- CT.EC2.PR.20: Memerlukan armada Amazon EC2 untuk mengganti hanya template peluncuran tersebut dengan tipe instans AWS Nitro yang mendukung enkripsi saat transit antar instans
- CT.ELASTICACHE.PR.8: Memerlukan grup ElastiCache replikasi Amazon dari versi Redis yang lebih baru agar otentikasi RBAC diaktifkan
- CT.MQ.PR.1: Memerlukan broker Amazon MQ ActiveMQ untuk menggunakan mode penerapan aktif/siaga untuk ketersediaan tinggi
- CT.MQ.PR.2: Memerlukan broker MQ Amazon MQ Rabbit untuk menggunakan mode cluster multi-AZ untuk ketersediaan tinggi
- CT.MSK.PR.1: Memerlukan klaster Amazon Managed Streaming for Apache Kafka (MSK) untuk menerapkan enkripsi saat transit antar node broker cluster
- CT.MSK.PR.2: Memerlukan cluster Amazon Managed Streaming for Apache Kafka (MSK) untuk dikonfigurasi dengan dinonaktifkan PublicAccess
- CT.NETWORK-FIREWALL.PR.5: Memerlukan firewall AWS Network Firewall untuk digunakan di beberapa Availability Zone
- CT.RDS.PR.26: Memerlukan Proxy Amazon RDS DB untuk meminta koneksi Transport Layer Security (TLS)
- CT.RDS.PR.27: Memerlukan grup parameter cluster Amazon RDS DB untuk meminta koneksi Transport Layer Security (TLS) untuk tipe engine yang didukung
- CT.RDS.PR.28: Memerlukan grup parameter Amazon RDS DB untuk meminta koneksi Transport Layer Security (TLS) untuk jenis engine yang didukung
- CT.RDS.PR.29: Memerlukan klaster Amazon RDS yang tidak dikonfigurasi agar dapat diakses publik melalui properti '' PubliclyAccessible

- CT.RDS.PR.30: Mengharuskan instans database Amazon RDS memiliki enkripsi saat istirahat yang dikonfigurasi untuk menggunakan kunci KMS yang Anda tentukan untuk jenis engine yang didukung
- CT.S3.PR.12: Memerlukan jalur akses Amazon S3 untuk memiliki konfigurasi Block Public Access (BPA) dengan semua opsi disetel ke true

Kontrol preventif baru

- CT.APPSYNC.PV.1Mengharuskan AWS AppSync GraphQL API dikonfigurasi dengan visibilitas pribadi
- CT.EC2.PV.1Memerlukan snapshot Amazon EBS dibuat dari volume EC2 terenkripsi
- CT.EC2.PV.2Mengharuskan volume Amazon EBS terlampir dikonfigurasi untuk mengenkripsi data saat istirahat
- CT.EC2.PV.3Mengharuskan snapshot Amazon EBS tidak dapat dipulihkan secara publik
- CT.EC2.PV.4Mengharuskan API langsung Amazon EBS tidak dipanggil
- CT.EC2.PV.5Larang penggunaan impor dan ekspor Amazon EC2 VM
- CT.EC2.PV.6Larang penggunaan tindakan Amazon EC2 dan API yang tidak digunakan lagi RequestSpotFleet RequestSpotInstances
- CT.KMS.PV.1Memerlukan kebijakan AWS KMS kunci untuk memiliki pernyataan yang membatasi pembuatan AWS KMS hibah untuk layanan AWS
- CT.KMS.PV.2Mengharuskan kunci AWS KMS asimetris dengan bahan kunci RSA yang digunakan untuk enkripsi tidak memiliki panjang kunci 2048 bit
- CT.KMS.PV.3Mengharuskan AWS KMS kunci dikonfigurasi dengan pemeriksaan keamanan penguncian kebijakan bypass diaktifkan
- CT.KMS.PV.4Mengharuskan kunci yang AWS KMS dikelola pelanggan (CMK) dikonfigurasi dengan materi utama yang berasal dari CloudHSM AWS
- CT.KMS.PV.5Mengharuskan kunci yang AWS KMS dikelola pelanggan (CMK) dikonfigurasi dengan materi kunci yang diimpor
- CT.KMS.PV.6Mengharuskan kunci yang AWS KMS dikelola pelanggan (CMK) dikonfigurasi dengan materi kunci yang berasal dari penyimpanan kunci eksternal (XKS)
- CT.LAMBDA.PV.1Memerlukan URL AWS Lambda fungsi untuk menggunakan otentikasi AWS berbasis IAM

- CT.LAMBDA.PV.2Memerlukan URL AWS Lambda fungsi untuk dikonfigurasi untuk akses hanya oleh prinsipal di dalam Akun AWS
- CT.MULTISERVICE.PV.1: Tolak akses berdasarkan permintaan untuk unit organisasi AWS Wilayah AWS

Kontrol detecive baru yang meningkatkan postur tata kelola kedaulatan digital Anda adalah bagian dari AWS Control Tower Standar yang Dikelola Layanan. AWS Security Hub

Kontrol detektif baru

- SH.ACM.2: Sertifikat RSA yang dikelola oleh ACM harus menggunakan panjang kunci minimal 2.048 bit
- SH.AppSync.5: AWS AppSync GraphQL API tidak boleh diautentikasi dengan kunci API
- SH.CloudTrail.6: Pastikan bucket S3 yang digunakan untuk menyimpan CloudTrail log tidak dapat diakses publik:
- SH.DMS.9: Titik akhir DMS harus menggunakan SSL
- SH.DocumentDB.3: Cuplikan cluster manual Amazon DocumentDB tidak boleh bersifat publik
- SH.DynamoDB.3: Cluster DynamoDB Accelerator (DAX) harus dienkripsi saat istirahat
- SH.EC2.23: EC2 Transit Gateways seharusnya tidak secara otomatis menerima permintaan lampiran VPC
- SH.EKS.1: Titik akhir klaster EKS tidak boleh diakses publik
- SH.ElastiCache.3: grup ElastiCache replikasi harus mengaktifkan failover otomatis
- SH.ElastiCache.4: grup ElastiCache replikasi seharusnya diaktifkan encryption-at-rest
- SH.ElastiCache.5: grup ElastiCache replikasi seharusnya diaktifkan encryption-in-transit
- SH.ElastiCache.6: grup ElastiCache replikasi versi Redis sebelumnya harus mengaktifkan Redis AUTH
- SH.EventBridge.3: bus acara EventBridge khusus harus memiliki kebijakan berbasis sumber daya terlampir
- SH.KMS.4: rotasi AWS KMS kunci harus diaktifkan
- SH.Lambda.3: Fungsi Lambda harus dalam VPC
- SH.MQ.5: Pialang ActiveMQ harus menggunakan mode penerapan aktif/siaga
- SH.MQ.6: Broker RabbitMQ harus menggunakan mode penerapan cluster

- SH.MSK.1: Cluster MSK harus dienkripsi dalam perjalanan di antara node broker
- SH.RDS.12: Autentikasi IAM harus dikonfigurasi untuk cluster RDS
- SH.RDS.15: Cluster RDS DB harus dikonfigurasi untuk beberapa Availability Zone
- SH.S3.17: Ember S3 harus dienkripsi saat istirahat dengan kunci AWS KMS

Untuk informasi selengkapnya tentang kontrol yang ditambahkan ke AWS Control Tower Standar yang AWS Security Hub Dikelola Layanan, lihat Kontrol yang berlaku untuk Standar yang Dikelola Layanan: AWS Control Tower dalam dokumentasi. AWS Security Hub

Untuk daftar yang tidak mendukung kontrol tertentu Wilayah AWS yang merupakan bagian dari AWS Control Tower Standar AWS Security Hub yang Dikelola Layanan, lihat Wilayah Tidak Didukung.

Kontrol baru yang dapat dikonfigurasi untuk penolakan Wilayah di tingkat OU

CT.MULTISERVICE.PV.1: Kontrol ini menerima parameter untuk menentukan Wilayah yang dikecualikan, prinsip IAM, dan Tindakan yang diizinkan, pada tingkat OU, bukan untuk seluruh zona landing AWS Control Tower. Ini adalah kontrol preventif, yang diterapkan oleh Kebijakan Kontrol Layanan (SCP).

Untuk informasi selengkapnya, lihat Kontrol penolakan wilayah yang diterapkan pada OU.

`UpdateEnabledControl`API

Rilis AWS Control Tower ini menambahkan dukungan API berikut untuk kontrol:

- `EnableControl`API yang diperbarui dapat mengonfigurasi kontrol yang dapat dikonfigurasi.
- `GetEnabledControl`API yang diperbarui menunjukkan parameter yang dikonfigurasi pada kontrol yang diaktifkan.
- `UpdateEnabledControl`API baru dapat mengubah parameter pada kontrol yang diaktifkan.

Untuk informasi selengkapnya, lihat Referensi API AWS Control Tower.

AWS Control Tower mendukung API landing zone

November 26, 2023

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

AWS Control Tower sekarang mendukung konfigurasi landing zone dan peluncuran menggunakan API. Anda dapat membuat, memperbarui, mendapatkan, membuat daftar, mengatur ulang, dan menghapus zona pendaratan menggunakan API.

API berikut memungkinkan Anda untuk mengatur dan mengelola landing zone Anda secara terprogram menggunakan AWS CloudFormation atau. AWS CLI

AWS Control Tower mendukung API berikut untuk zona pendaratan:

- `CreateLandingZone`—Panggilan API ini membuat landing zone menggunakan versi landing zone dan file manifes.
- `GetLandingZoneOperation`—Panggilan API ini mengembalikan status operasi landing zone tertentu.
- `GetLandingZone`—Panggilan API ini menampilkan detail tentang landing zone yang ditentukan, termasuk versi, file manifes, dan status.
- `UpdateLandingZone`—Panggilan API ini memperbarui versi landing zone atau file manifes.
- `ListLandingZone`—Panggilan API ini mengembalikan satu pengenal landing zone (ARN) untuk pengaturan landing zone di akun manajemen.
- `ResetLandingZone`—Panggilan API ini me-reset landing zone ke parameter yang ditentukan pada pembaruan terbaru, yang dapat memperbaiki drift. Jika landing zone belum diperbarui, panggilan ini mengatur ulang landing zone ke parameter yang ditentukan saat pembuatan.
- `DeleteLandingZone`—Panggilan API ini menonaktifkan landing zone.

Untuk memulai dengan landing zone API, lihatMemulai AWS Control Tower menggunakan API.

AWS Control Tower mendukung penandaan untuk kontrol yang diaktifkan

November 10, 2023

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

AWS Control Tower sekarang mendukung penandaan sumber daya untuk kontrol yang diaktifkan, dari konsol AWS Control Tower atau melalui API. Anda dapat menambahkan, menghapus, atau mencantumkan tag untuk kontrol yang diaktifkan.

Dengan merilis API berikut, Anda dapat mengonfigurasi tag untuk kontrol yang Anda aktifkan di AWS Control Tower. Tag membantu Anda mengelola, mengidentifikasi, mengatur, mencari, dan memfilter

sumber daya. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya.

AWS Control Tower mendukung API berikut untuk penandaan kontrol:

- `TagResource`—Panggilan API ini menambahkan tag ke kontrol yang diaktifkan di AWS Control Tower.
- `UntagResource`—Panggilan API ini menghapus tag dari kontrol yang diaktifkan di AWS Control Tower.
- `ListTagsForResource`—Panggilan API ini mengembalikan tag untuk kontrol yang diaktifkan di AWS Control Tower.

API kontrol AWS Control Tower tersedia di Wilayah AWS tempat AWS Control Tower tersedia. Untuk daftar lengkap tentang Wilayah AWS AWS Control Tower yang tersedia, lihat Tabel AWS Wilayah. Untuk daftar lengkap AWS Control Tower API, lihat Referensi API.

AWS Control Tower tersedia di Wilayah Asia Pasifik (Melbourne)

November 3, 2023

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

AWS Control Tower tersedia di Wilayah Asia Pasifik (Melbourne).

Jika Anda sudah menggunakan AWS Control Tower dan ingin memperluas fitur tata kelola ke Wilayah ini di akun Anda, buka halaman Pengaturan di dasbor AWS Control Tower, pilih Wilayah, lalu perbarui landing zone Anda. Setelah pembaruan landing zone, Anda harus memperbarui semua akun yang diatur oleh AWS Control Tower, untuk membawa akun dan OU Anda di bawah tata kelola di Wilayah baru. Untuk informasi selengkapnya, lihat Tentang Pembaruan.

Untuk daftar lengkap Wilayah di mana AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

Transisi ke jenis produk AWS Service Catalog Eksternal baru (fase 1)

Oktober 31, 2023

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

HashiCorp memperbarui lisensi Terraform mereka. Akibatnya, dukungan yang AWS Service Catalog diperbarui untuk produk Terraform Open Source dan menyediakan produk ke jenis produk baru, yang disebut Eksternal.

AWS Control Tower tidak mendukung penyesuaian Account Factory yang bergantung pada jenis produk AWS Service Catalog Eksternal. Untuk menghindari gangguan pada beban kerja dan AWS sumber daya yang ada di akun Anda, ikuti langkah transisi AWS Control Tower dalam urutan yang disarankan ini, sebelum 14 Desember 2023:

1. Tingkatkan Mesin Referensi Terraform Anda yang ada AWS Service Catalog untuk menyertakan dukungan untuk jenis produk Sumber Terbuka Eksternal dan Terraform. Untuk petunjuk tentang memperbarui Mesin Referensi Terraform Anda, tinjau Repositori.AWS Service Catalog GitHub
2. Buka AWS Service Catalog dan duplikat cetak biru Terraform Open Source yang ada untuk menggunakan jenis produk Eksternal yang baru. Jangan hentikan cetak biru Terraform Open Source yang ada.
3. Lanjutkan menggunakan cetak biru Terraform Open Source yang ada untuk membuat atau memperbarui akun di AWS Control Tower.

API kontrol baru tersedia

Oktober 14, 2023

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

AWS Control Tower kini mendukung API tambahan yang dapat Anda gunakan untuk menerapkan dan mengelola kontrol AWS Control Tower, sesuai skala besar. Untuk informasi selengkapnya tentang API kontrol AWS Control Tower, lihat Referensi API.

AWS Control Tower menambahkan API kontrol baru.

- `GetEnabledControl`—Panggilan API memberikan detail tentang kontrol yang diaktifkan.

Kami juga memperbarui API ini:

`ListEnabledControls`—Panggilan API ini mencantumkan kontrol yang diaktifkan oleh AWS Control Tower pada unit organisasi yang ditentukan dan akun yang dikandungnya. Sekarang mengembalikan informasi tambahan dalam suatu `EnabledControlSummary` objek.

Dengan API ini, Anda dapat melakukan beberapa operasi umum secara terprogram. Sebagai contoh:

- Dapatkan daftar semua kontrol yang telah Anda aktifkan dari pustaka kontrol AWS Control Tower.
- Untuk kontrol apa pun yang diaktifkan, Anda bisa mendapatkan informasi tentang Wilayah di mana kontrol didukung, pengenal kontrol (ARN), status drift kontrol, dan ringkasan status kontrol.

API kontrol AWS Control Tower tersedia di Wilayah AWS tempat AWS Control Tower tersedia. Untuk daftar lengkap tentang Wilayah AWS AWS Control Tower yang tersedia, lihat Tabel AWS Wilayah. Untuk daftar lengkap AWS Control Tower API, lihat Referensi API.

AWS Control Tower menambahkan kontrol tambahan

Oktober 5, 2023

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

AWS Control Tower mengumumkan kontrol proaktif dan detektif baru.

Kontrol proaktif di AWS Control Tower diimplementasikan melalui AWS CloudFormation Hooks, yang mengidentifikasi dan memblokir sumber daya yang tidak sesuai sebelum menyediakannya. AWS CloudFormation Kontrol proaktif melengkapi kemampuan kontrol preventif dan detektif yang ada di AWS Control Tower.

Kontrol proaktif baru

- [CT.ATHENA.PR.1] Memerlukan workgroup Amazon Athena untuk mengenkripsi hasil kueri Athena saat istirahat
- [CT.ATHENA.PR.2] Memerlukan workgroup Amazon Athena untuk mengenkripsi hasil kueri Athena saat istirahat dengan kunci (KMS) AWS Key Management Service
- [CT.CLOUDTRAIL.PR.4] Memerlukan penyimpanan data acara AWS CloudTrail Lake untuk mengaktifkan enkripsi saat istirahat dengan AWS KMS kunci
- [CT.DAX.PR.2] Memerlukan klaster Amazon DAX untuk menyebarkan node ke setidaknya tiga Availability Zone
- [CT.EC2.PR.14] Memerlukan volume Amazon EBS yang dikonfigurasi melalui template peluncuran Amazon EC2 untuk mengenkripsi data saat istirahat
- [CT.EKS.PR.2] Memerlukan klaster Amazon EKS untuk dikonfigurasi dengan enkripsi rahasia menggunakan AWS kunci Layanan Manajemen Kunci (KMS)
- [CT.ELASTICLOADBALANCING.PR.14] Memerlukan Network Load Balancer agar penyeimbangan beban lintas zona diaktifkan
- [CT.ELASTICLOADBALANCING.PR.15] Mengharuskan grup target Elastic Load Balancing v2 tidak secara eksplisit menonaktifkan penyeimbangan beban lintas zona
- [CT.EMR.PR.1] Mengharuskan konfigurasi keamanan Amazon EMR (EMR) dikonfigurasi untuk mengenkripsi data saat istirahat di Amazon S3

- [CT.EMR.PR.2] Mengharuskan konfigurasi keamanan Amazon EMR (EMR) dikonfigurasi untuk mengenkripsi data saat istirahat di Amazon S3 dengan kunci AWS KMS
- [CT.EMR.PR.3] Mengharuskan konfigurasi keamanan Amazon EMR (EMR) dikonfigurasi dengan enkripsi disk lokal volume EBS menggunakan kunci AWS KMS
- [CT.EMR.PR.4] Mengharuskan konfigurasi keamanan Amazon EMR (EMR) dikonfigurasi untuk mengenkripsi data dalam perjalanan
- [CT.GLUE.PR.1] Memerlukan pekerjaan AWS Glue untuk memiliki konfigurasi keamanan terkait
- [CT.GLUE.PR.2] Memerlukan konfigurasi keamanan AWS Glue untuk mengenkripsi data di target AWS Amazon S3 menggunakan kunci KMS
- [CT.KMS.PR.2] Mengharuskan kunci AWS KMS asimetris dengan bahan kunci RSA yang digunakan untuk enkripsi memiliki panjang kunci lebih besar dari 2048 bit
- [CT.KMS.PR.3] Memerlukan kebijakan AWS KMS kunci untuk memiliki pernyataan yang membatasi pembuatan AWS KMS hibah untuk layanan AWS
- [CT.LAMBDA.PR.4] Memerlukan izin AWS Lambda lapisan untuk memberikan akses ke AWS organisasi atau AWS akun tertentu
- [CT.LAMBDA.PR.5] Memerlukan URL AWS Lambda fungsi untuk menggunakan otentikasi AWS berbasis IAM
- [CT.LAMBDA.PR.6] Memerlukan kebijakan CORS URL AWS Lambda fungsi untuk membatasi akses ke asal tertentu
- [CT.NEPTUNE.PR.4] Memerlukan cluster DB Amazon Neptunus untuk mengaktifkan ekspor log CloudWatch Amazon untuk log audit
- [CT.NEPTUNE.PR.5] Memerlukan cluster DB Amazon Neptunus untuk mengatur periode retensi cadangan lebih besar dari atau sama dengan tujuh hari
- [CT.REDSHIFT.PR.9] Mengharuskan grup parameter cluster Amazon Redshift dikonfigurasi untuk menggunakan Secure Sockets Layer (SSL) untuk enkripsi data dalam perjalanan

Kontrol proaktif baru ini tersedia dalam komersial di Wilayah AWS mana AWS Control Tower tersedia. Untuk detail selengkapnya tentang kontrol ini, lihat Kontrol proaktif. Untuk detail selengkapnya tentang tempat kontrol tersedia, lihat Batasan kontrol.

Kontrol detektif baru

Kontrol baru ditambahkan ke Standar yang Dikelola Layanan Security Hub: AWS Control Tower. Kontrol ini membantu Anda meningkatkan postur tata kelola Anda. Mereka bertindak sebagai bagian

dari Security Hub Service-Managed Standard: AWS Control Tower, setelah Anda mengaktifkannya di OU tertentu.

- [SH.Athena.1] Kelompok kerja Athena harus dienkripsi saat istirahat
- [SH.Neptune.1] Cluster DB Neptunus harus dienkripsi saat istirahat
- [SH.Neptune.2] Cluster DB Neptunus harus menerbitkan log audit ke Log CloudWatch
- [SH.Neptune.3] Snapshot cluster DB Neptunus seharusnya tidak bersifat publik
- [SH.Neptune.4] Cluster DB Neptunus harus mengaktifkan perlindungan penghapusan
- [SH.Neptune.5] Cluster DB Neptunus harus mengaktifkan cadangan otomatis
- [SH.Neptune.6] Snapshot cluster DB Neptunus harus dienkripsi saat istirahat
- [SH.Neptune.7] Cluster DB Neptunus harus mengaktifkan otentikasi basis data IAM
- [SH.Neptune.8] Cluster DB Neptunus harus dikonfigurasi untuk menyalin tag ke snapshot
- [SH.RDS.27] Cluster RDS DB harus dienkripsi saat istirahat

Kontrol AWS Security Hub detektif baru tersedia di sebagian besar Wilayah AWS tempat AWS Control Tower tersedia. Untuk detail selengkapnya tentang kontrol ini, lihat Kontrol yang berlaku untuk Service-Managed Standard: AWS Control Tower. Untuk detail selengkapnya tentang di mana kontrol tersedia, lihatKeterbatasan kontrol.

Jenis drift baru dilaporkan: akses tepercaya dinonaktifkan

September 21, 2023

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

Setelah menyiapkan zona landing zone AWS Control Tower, Anda dapat menonaktifkan akses tepercaya ke AWS Control Tower AWS Organizations. Namun, hal itu menyebabkan penyimpangan.

Dengan tipe drift yang dinonaktifkan akses tepercaya, AWS Control Tower memberi tahu Anda kapan jenis drift ini terjadi, sehingga Anda dapat memperbaiki zona landing zone AWS Control Tower. Untuk informasi selengkapnya, lihat Jenis penyimpangan tata kelola.

Empat tambahan Wilayah AWS

September 13, 2023

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

AWS Control Tower sekarang tersedia di Asia Pasifik (Hyderabad), Eropa (Spanyol dan Zurich), dan Timur Tengah (UEA).

Jika Anda sudah menggunakan AWS Control Tower dan ingin memperluas fitur tata kelola ke Wilayah ini di akun Anda, buka halaman Pengaturan di dasbor AWS Control Tower, pilih Wilayah, lalu perbarui landing zone Anda. Setelah pembaruan landing zone, Anda harus memperbarui semua akun yang diatur oleh AWS Control Tower, untuk membawa akun dan OU Anda di bawah tata kelola di Wilayah baru. Untuk informasi selengkapnya, lihat Tentang Pembaruan.

Untuk daftar lengkap Wilayah di mana AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

AWS Control Tower tersedia di Wilayah Tel Aviv

Agustus 28, 2023

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

AWS Control Tower mengumumkan ketersediaan di Wilayah Israel (Tel Aviv).

Jika Anda sudah menggunakan AWS Control Tower dan ingin memperluas fitur tata kelola ke Wilayah ini di akun Anda, buka halaman Pengaturan di dasbor AWS Control Tower, pilih Wilayah, lalu perbarui landing zone Anda. Setelah pembaruan landing zone, Anda harus memperbarui semua akun yang diatur oleh AWS Control Tower, untuk membawa akun dan OU Anda di bawah tata kelola di Wilayah baru. Untuk informasi selengkapnya, lihat Tentang Pembaruan.

Untuk daftar lengkap Wilayah di mana AWS Control Tower tersedia, lihat Wilayah AWS Tabel.

AWS Control Tower meluncurkan 28 kontrol proaktif baru

Juli 24, 2023

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

AWS Control Tower menambahkan 28 kontrol proaktif baru, untuk membantu Anda mengelola AWS lingkungan.

Kontrol proaktif meningkatkan kemampuan tata kelola AWS Control Tower di seluruh AWS lingkungan multi-akun Anda, dengan memblokir sumber daya yang tidak sesuai sebelum disediakan. Kontrol ini membantu mengelola AWS layanan seperti Amazon CloudWatch, Amazon Neptunus, Amazon, dan ElastiCache AWS Step Functions Amazon DocumentDB. Kontrol baru membantu Anda memenuhi tujuan kontrol seperti membuat pencatatan dan pemantauan, mengenkripsi data saat istirahat, atau meningkatkan ketahanan.

Berikut adalah daftar lengkap kontrol baru:

- [CT.APPSYNC.PR.1] Memerlukan GraphQL API agar logging diaktifkan AWS AppSync
- [CT.CLOUDWATCH.PR.1] Memerlukan alarm CloudWatch Amazon agar tindakan dikonfigurasi untuk status alarm
- [CT.CLOUDWATCH.PR.2] Memerlukan grup log CloudWatch Amazon untuk dipertahankan setidaknya selama satu tahun
- [CT.CLOUDWATCH.PR.3] Memerlukan grup log CloudWatch Amazon untuk dienkripsi saat istirahat dengan kunci KMS AWS
- [CT.CLOUDWATCH.PR.4] Memerlukan tindakan alarm Amazon untuk diaktifkan CloudWatch
- [CT.DOCUMENTDB.PR.1] Memerlukan cluster Amazon DocumentDB untuk dienkripsi saat istirahat
- [CT.DOCUMENTDB.PR.2] Memerlukan cluster Amazon DocumentDB agar pencadangan otomatis diaktifkan
- [CT.DYNAMODB.PR.2] Memerlukan tabel Amazon DynamoDB untuk dienkripsi saat istirahat menggunakan kunci AWS KMS
- [CT.EC2.PR.13] Memerlukan instans Amazon EC2 agar pemantauan terperinci diaktifkan
- [CT.EKS.PR.1] Memerlukan klaster Amazon EKS untuk dikonfigurasi dengan akses publik yang dinonaktifkan ke titik akhir server API Kubernetes cluster
- [CT.ELASTICACHE.PR.1] Memerlukan Amazon untuk cluster Redis agar cadangan otomatis diaktifkan ElastiCache
- [CT.ELASTICACHE.PR.2] Memerlukan ElastiCache Amazon untuk cluster Redis agar upgrade versi minor otomatis diaktifkan
- [CT.ELASTICACHE.PR.3] Memerlukan ElastiCache Amazon untuk grup replikasi Redis agar failover otomatis diaktifkan
- [CT.ELASTICACHE.PR.4] Memerlukan grup replikasi Amazon ElastiCache agar enkripsi diaktifkan saat istirahat
- [CT.ELASTICACHE.PR.5] Memerlukan ElastiCache Amazon untuk grup replikasi Redis agar enkripsi saat transit diaktifkan
- [CT.ELASTICACHE.PR.6] Memerlukan cluster cache Amazon ElastiCache untuk menggunakan grup subnet khusus
- [CT.ELASTICACHE.PR.7] Memerlukan grup replikasi ElastiCache Amazon dari versi Redis sebelumnya untuk memiliki otentikasi Redis AUTH

- [CT.ELASTICBEANSTALK.PR.3] Memerlukan lingkungan Elastic Beanstalk untuk memiliki konfigurasi logging AWS
- [CT.LAMBDA.PR.3] Memerlukan AWS Lambda fungsi untuk berada di Amazon Virtual Private Cloud (VPC) yang dikelola pelanggan
- [CT.NEPTUNE.PR.1] Memerlukan cluster DB Amazon Neptunus untuk memiliki otentikasi basis data (IAM) AWS Identity and Access Management
- [CT.NEPTUNE.PR.2] Memerlukan cluster DB Amazon Neptunus agar perlindungan penghapusan diaktifkan
- [CT.NEPTUNE.PR.3] Memerlukan cluster DB Amazon Neptunus agar enkripsi penyimpanan diaktifkan
- [CT.REDSHIFT.PR.8] Memerlukan cluster Amazon Redshift untuk dienkripsi
- [CT.S3.PR.9] Mengharuskan bucket Amazon S3 mengaktifkan Kunci Objek S3
- [CT.S3.PR.10] Memerlukan bucket Amazon S3 agar enkripsi sisi server dikonfigurasi menggunakan kunci AWS KMS
- [CT.S3.PR.11] Memerlukan bucket Amazon S3 agar versi diaktifkan
- [CT.STEPFUNCTIONS.PR.1] Memerlukan mesin status agar logging diaktifkan AWS Step Functions
- [CT.STEPFUNCTIONS.PR.2] Memerlukan mesin status agar penelusuran diaktifkan AWS Step Functions AWS X-Ray

Kontrol proaktif di AWS Control Tower diimplementasikan melalui AWS CloudFormation Hooks, yang mengidentifikasi dan memblokir sumber daya yang tidak sesuai sebelum menyediakannya. AWS CloudFormation Kontrol proaktif melengkapi kemampuan kontrol preventif dan detektif yang ada di AWS Control Tower.

Kontrol proaktif baru ini tersedia di semua Wilayah AWS tempat AWS Control Tower tersedia. Untuk detail selengkapnya tentang kontrol ini, lihat Kontrol proaktif.

AWS Control Tower menghentikan dua kontrol

Juli 18, 2023

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

AWS Control Tower melakukan tinjauan rutin terhadap kontrol keamanannya untuk memastikan bahwa kontrol tersebut mutakhir dan masih dianggap sebagai praktik terbaik. Dua kontrol berikut

telah usang, efektif 18 Juli 2023, dan mereka akan dihapus dari pustaka kontrol, efektif 18 Agustus 2023. Anda tidak dapat lagi mengaktifkan kontrol ini pada unit organisasi mana pun. Anda dapat memilih untuk menonaktifkan kontrol ini sebelum tanggal penghapusan.

- [SH.S3.4] Bucket S3 harus mengaktifkan enkripsi sisi server
- [CT.S3.PR.7] Memerlukan bucket Amazon S3 agar enkripsi sisi server dikonfigurasi

Alasan penghentian

Mulai Januari 2023, Amazon S3 mengonfigurasi enkripsi default pada semua bucket tidak terenkripsi baru dan yang sudah ada untuk menerapkan enkripsi sisi server dengan kunci terkelola S3 (SSE-S3) sebagai tingkat dasar enkripsi untuk objek baru yang diunggah ke bucket ini. Tidak ada perubahan yang dilakukan pada konfigurasi enkripsi default untuk bucket yang sudah ada yang sudah memiliki enkripsi SSE-S3 atau sisi server dengan AWS kunci Key Management Service (AWS KMS) (SSE-KMS) yang dikonfigurasi.

AWS Control Tower landing zone versi 3.2

Juni 16, 2023

(Pembaruan diperlukan untuk landing zone AWS Control Tower ke versi 3.2. Untuk informasi, lihatPerbarui Zona Pendaratan Anda).

AWS Control Tower landing zone versi 3.2 menghadirkan kontrol yang merupakan bagian dari Standar yang AWS Security Hub Dikelola Layanan: AWS Control Tower 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 AWS Control Tower dengan membuat Aturan EventBridge Terkelola, yang disebut AWSControlTowerManagedRuledi setiap akun anggota. Aturan terkelola ini mengumpulkan peristiwa AWS Security Hub Finding, dari AWS Control Tower dapat menentukan penyimpangan kontrol.

Aturan ini adalah aturan terkelola pertama yang dibuat oleh AWS Control Tower. Aturan ini tidak digunakan oleh tumpukan; itu diterapkan langsung dari API. EventBridge Anda dapat melihat aturan di EventBridge konsol, atau melalui EventBridge API. Jika `managed-by` bidang diisi, itu akan menampilkan prinsip layanan AWS Control Tower.

Sebelumnya, AWS Control Tower AWSControlTowerExecutionberperan untuk melakukan operasi di akun anggota. Peran dan aturan baru ini lebih selaras dengan prinsip praktik terbaik yang memungkinkan hak istimewa paling sedikit saat melakukan operasi di lingkungan AWS multi-akun. Peran baru ini memberikan izin cakupan ke bawah yang secara khusus memungkinkan: membuat aturan terkelola di akun anggota, mempertahankan aturan terkelola, menerbitkan pemberitahuan keamanan melalui SNS, dan memverifikasi penyimpangan. Untuk informasi selengkapnya, lihat AWSServiceRoleForAWSControlTower.

Pembaruan landing zone 3.2 juga menyertakan StackSet sumber daya baru di akun manajemen`BP_BASELINE_SERVICE_LINKED_ROLE`, yang awalnya menyebarkan peran terkait layanan.

Saat melaporkan drift kontrol Security Hub (di landing zone 3.2 dan versi lebih baru), AWS Control Tower menerima pembaruan status harian dari Security Hub. Meskipun kontrol aktif di setiap Wilayah yang diatur, AWS Control Tower mengirimkan peristiwa AWS Security Hub Finding ke Wilayah home AWS Control Tower saja. Untuk informasi selengkapnya, lihat Security Hub mengontrol pelaporan drift.

Perbarui ke kontrol Tolak Wilayah

Versi landing zone ini juga menyertakan pembaruan ke kontrol Region Deny.

Layanan global dan API ditambahkan

- AWS Billing and Cost Management (`billing:*`)
- AWS CloudTrail (`cloudtrail:LookupEvents`) untuk memungkinkan visibilitas peristiwa global di akun anggota.
- AWS Penagihan Konsolidasi () `consolidatedbilling:*`
- AWS Manajemen Console Mobile Application (`consoleapp:*`)
- AWS Tingkat Gratis (`freetier:*`)
- AWS Invoicing (`invoicing:*`)
- AWS IQ () `iq:*`
- AWS Pemberitahuan Pengguna (`notifications:*`)
- AWS Kontak Pemberitahuan Pengguna (`notifications-contacts:*`)
- Amazon Payments (`payments:*`)
- AWS Pengaturan Pajak (`tax:*`)

Layanan global dan API dihapus

- Dihapus `s3:GetAccountPublic` karena ini bukan tindakan yang valid.
- Dihapus `s3:PutAccountPublic` karena ini bukan tindakan yang valid.

AWS Control Tower menangani akun berdasarkan ID

Juni 14, 2023

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

AWS Control Tower kini membuat dan mengelola akun yang Anda buat di AWS Account Factory dengan melacak ID akun, bukan alamat email akun.

Saat menyediakan akun, pemohon akun selalu harus memiliki `CreateAccount` dan izin. `DescribeCreateAccountStatus` Set izin ini adalah bagian dari peran Admin, dan diberikan secara otomatis ketika pemohon mengasumsikan peran Admin. Jika Anda mendelegasikan izin ke akun penyediaan, Anda mungkin perlu menambahkan izin ini secara langsung untuk pemohon akun.

Kontrol detektif Security Hub tambahan tersedia di pustaka kontrol AWS Control Tower

Juni 12, 2023

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

AWS Control Tower telah menambahkan sepuluh kontrol AWS Security Hub detektif baru ke perpustakaan kontrol AWS Control Tower. Kontrol baru ini menargetkan layanan seperti API Gateway AWS CodeBuild, Amazon Elastic Compute Cloud (EC2), Amazon Elastic Load Balancer, Amazon Redshift, Amazon, dan. SageMaker AWS WAF Kontrol baru ini membantu Anda meningkatkan postur tata kelola dengan memenuhi tujuan kontrol, seperti Menetapkan pencatatan dan pemantauan, Batasi akses jaringan, dan Enkripsi data saat istirahat.

Kontrol ini bertindak sebagai bagian dari Standar yang Dikelola Layanan Security Hub: AWS Control Tower, setelah Anda mengaktifkannya di OU tertentu.

- [SH.Account.1] Informasi kontak keamanan harus disediakan untuk Akun AWS
- [Sh.apigateway.8] Rute API Gateway harus menentukan jenis otorisasi
- [Sh.apigateway.9] Pencatatan akses harus dikonfigurasi untuk Tahapan API Gateway V2

- [SH. CodeBuild.3] CodeBuild Log S3 harus dienkripsi
- [SH.EC2.25] Template peluncuran EC2 tidak boleh menetapkan IP publik ke antarmuka jaringan
- [SH.ELB.1] Application Load Balancer harus dikonfigurasi untuk mengalihkan semua permintaan HTTP ke HTTPS
- [Sh.Redshift.10] Cluster Redshift harus dienkripsi saat istirahat
- [SH. SageMaker.2] instance SageMaker notebook harus diluncurkan dalam VPC khusus
- [SH. SageMaker.3] Pengguna seharusnya tidak memiliki akses root ke instance SageMaker notebook
- [SH.WAF.10] ACL web WAFV2 harus memiliki setidaknya satu aturan atau kelompok aturan

Kontrol AWS Security Hub detektif baru tersedia di semua Wilayah AWS tempat AWS Control Tower tersedia. Untuk detail selengkapnya tentang kontrol ini, lihat Kontrol yang berlaku untuk Service-Managed Standard: AWS Control Tower.

AWS Control Tower menerbitkan tabel metadata kontrol

Juni 7, 2023

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

AWS Control Tower sekarang menyediakan tabel lengkap metadata kontrol sebagai bagian dari dokumentasi yang diterbitkan. Saat bekerja dengan API kontrol, Anda dapat mencari ControliDentifier API masing-masing kontrol, yang merupakan ARN unik yang terkait dengan masing-masing. Wilayah AWS Tabel mencakup kerangka kerja dan tujuan kontrol yang dicakup oleh setiap kontrol. Sebelumnya, informasi ini hanya tersedia di konsol.

Tabel juga menyertakan metadata untuk kontrol Security Hub yang merupakan bagian dari AWS Security Hub Service-Managed Standard:AWS Control Tower. Untuk detail selengkapnya, lihat Tabel metadata kontrol.

Untuk daftar singkat pengidentifikasi kontrol, dan beberapa contoh penggunaan, lihat Pengidentifikasi sumber daya untuk API dan kontrol.

Dukungan Terraform untuk Kustomisasi Account Factory

Juni 6, 2023

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

AWS Control Tower menawarkan dukungan wilayah tunggal untuk Terraform melalui Kustomisasi Account Factory (AFC). Dimulai dengan rilis ini, Anda dapat menggunakan AWS Control Tower dan Service Catalog bersama-sama, untuk menentukan cetak biru akun AFC, di open source Terraform. Anda dapat menyesuaikan yang baru dan yang sudah ada Akun AWS, sebelum Anda menyediakan sumber daya di AWS Control Tower. Secara default, fitur ini memungkinkan Anda untuk menerapkan dan memperbarui akun, dengan Terraform, di Wilayah home AWS Control Tower Anda.

Cetak biru akun menjelaskan sumber daya dan konfigurasi spesifik yang diperlukan saat disediakan. Akun AWS Anda dapat menggunakan cetak biru sebagai templat untuk membuat beberapa Akun AWS dalam skala besar.

Untuk memulai, gunakan Mesin Referensi Terraform aktif. GitHub Mesin Referensi mengonfigurasi kode dan infrastruktur yang diperlukan agar mesin open source Terraform dapat bekerja dengan Service Catalog. Proses penyiapan satu kali ini membutuhkan waktu beberapa menit. Setelah itu, Anda dapat menentukan persyaratan akun khusus Anda di Terraform, lalu menerapkan akun Anda dengan alur kerja pabrik akun AWS Control Tower yang terdefinisi dengan baik. Pelanggan yang lebih suka bekerja dengan Terraform dapat menggunakan kustomisasi akun AWS Control Tower dalam skala besar dengan AFC, dan mendapatkan akses langsung ke setiap akun setelah disediakan.

Untuk mempelajari cara membuat kustomisasi ini, lihat Membuat Produk dan Memulai Terraform open source di dokumentasi Service Catalog. Fitur ini tersedia di semua Wilayah AWS tempat AWS Control Tower tersedia.

AWS Manajemen mandiri IAM Identity Center tersedia untuk landing zone

Juni 6, 2023

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

AWS Control Tower kini mendukung pilihan penyedia identitas opsional untuk landing zone AWS Control Tower, yang dapat Anda konfigurasikan selama penyiapan atau pembaruan. Secara default, landing zone dipilih untuk menggunakan AWS IAM Identity Center, selaras dengan panduan praktik terbaik yang ditentukan dalam Mengatur Lingkungan Anda Menggunakan Beberapa Akun. AWS Anda sekarang memiliki tiga alternatif:

- Anda dapat menerima default dan mengizinkan AWS Control Tower menyiapkan dan mengelola Pusat Identitas AWS IAM untuk Anda.
- Anda dapat memilih untuk mengelola sendiri Pusat AWS Identitas IAM, untuk mencerminkan kebutuhan bisnis spesifik Anda.

- Anda dapat secara opsional membawa dan mengelola sendiri penyedia identitas pihak ketiga, dengan menghubungkannya melalui IAM Identity Center, jika diperlukan. Anda harus menggunakan opsionalitas penyedia identitas jika lingkungan peraturan Anda mengharuskan Anda untuk menggunakan penyedia tertentu, atau jika Anda beroperasi di Wilayah AWS tempat Pusat Identitas AWS IAM tidak tersedia.

Untuk informasi selengkapnya, lihat Panduan Pusat Identitas IAM.

Pemilihan penyedia identitas di tingkat akun tidak didukung. Fitur ini hanya berlaku untuk landing zone secara keseluruhan. Opsionalitas penyedia identitas AWS Control Tower tersedia di semua Wilayah AWS tempat AWS Control Tower tersedia.

AWS Control Tower menangani tata kelola campuran untuk OU

Juni 1, 2023

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

Dengan rilis ini, AWS Control Tower mencegah kontrol diterapkan ke unit organisasi (OU), jika OU tersebut dalam keadaan tata kelola campuran. Tata kelola campuran terjadi di OU jika akun tidak diperbarui setelah AWS Control Tower memperluas tata kelola ke yang baru Wilayah AWS, atau menghapus tata kelola. Rilis ini membantu Anda menjaga akun anggota OU tersebut dalam kepatuhan yang seragam. Untuk informasi selengkapnya, lihat Hindari tata kelola campuran saat mengonfigurasi Wilayah.

Tersedia kontrol proaktif tambahan

19 Mei 2023

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

AWS Control Tower menambahkan 28 kontrol proaktif baru untuk membantu Anda mengatur lingkungan multi-akun dan memenuhi tujuan kontrol tertentu, seperti enkripsi data saat istirahat, atau membatasi akses jaringan. Kontrol proaktif diimplementasikan dengan AWS CloudFormation kait yang memeriksa sumber daya Anda sebelum disediakan. Kontrol baru dapat membantu mengatur AWS layanan seperti Amazon OpenSearch Service, Amazon EC2 Auto Scaling, Amazon, Amazon SageMaker API Gateway, dan Amazon Relational Database Service (RDS).

Kontrol proaktif didukung di semua iklan di Wilayah AWS mana AWS Control Tower tersedia.

OpenSearch Layanan Amazon

- [CT.OPENSEARCH.PR.1] Memerlukan domain Elasticsearch untuk mengenkripsi data saat istirahat
- [CT.OPENSEARCH.PR.2] Memerlukan domain Elasticsearch untuk dibuat di VPC Amazon yang ditentukan pengguna
- [CT.OPENSEARCH.PR.3] Memerlukan domain Elasticsearch untuk mengenkripsi data yang dikirim antar node
- [CT.OPENSEARCH.PR.4] Memerlukan domain Elasticsearch untuk mengirim log kesalahan ke Amazon Logs CloudWatch
- [CT.OPENSEARCH.PR.5] Memerlukan domain Elasticsearch untuk mengirim log audit ke Amazon Logs CloudWatch
- [CT.OPENSEARCH.PR.6] Memerlukan domain Elasticsearch untuk memiliki kesadaran zona dan setidaknya tiga node data
- [CT.OPENSEARCH.PR.7] Memerlukan domain Elasticsearch untuk memiliki setidaknya tiga node master khusus
- [CT.OPENSEARCH.PR.8] Memerlukan domain Layanan Elasticsearch untuk menggunakan TLSv1.2
- [CT.OPENSEARCH.PR.9] Memerlukan domain Layanan Amazon OpenSearch untuk mengenkripsi data saat istirahat
- [CT.OPENSEARCH.PR.10] Memerlukan domain Layanan Amazon untuk dibuat di OpenSearch VPC Amazon yang ditentukan pengguna
- [CT.OPENSEARCH.PR.11] Memerlukan domain Layanan OpenSearch Amazon untuk mengenkripsi data yang dikirim antar node
- [CT.OPENSEARCH.PR.12] Memerlukan domain Layanan Amazon untuk mengirim log kesalahan ke OpenSearch Amazon Logs CloudWatch
- [CT.OPENSEARCH.PR.13] Memerlukan domain Layanan Amazon untuk mengirim log audit ke OpenSearch Amazon Logs CloudWatch
- [CT.OPENSEARCH.PR.14] Memerlukan domain Layanan OpenSearch Amazon untuk memiliki kesadaran zona dan setidaknya tiga node data
- [CT.OPENSEARCH.PR.15] Memerlukan domain Layanan Amazon OpenSearch untuk menggunakan kontrol akses berbutir halus
- [CT.OPENSEARCH.PR.16] Memerlukan domain Layanan Amazon untuk menggunakan TLSv1.2 OpenSearch

Amazon EC2 Auto Scaling

- [CT.AUTOSCALING.PR.1] Memerlukan grup Auto Scaling Amazon EC2 untuk memiliki beberapa Availability Zone
- [CT.AUTOSCALING.PR.2] Memerlukan konfigurasi peluncuran grup Auto Scaling Amazon EC2 untuk mengonfigurasi instans Amazon EC2 untuk IMDSv2
- [CT.AUTOSCALING.PR.3] Memerlukan konfigurasi peluncuran Auto Scaling Amazon EC2 untuk memiliki batas respons metadata single-hop
- [CT.AUTOSCALING.PR.4] Memerlukan grup Auto Scaling Amazon EC2 yang terkait dengan Amazon Elastic Load Balancing (ELB) agar pemeriksaan kesehatan ELB diaktifkan
- [CT.AUTOSCALING.PR.5] Mengharuskan konfigurasi peluncuran grup Auto Scaling Amazon EC2 tidak memiliki instans Amazon EC2 dengan alamat IP publik
- [CT.AUTOSCALING.PR.6] Memerlukan grup Auto Scaling Amazon EC2 untuk menggunakan beberapa jenis instans
- [CT.AUTOSCALING.PR.8] Memerlukan grup Auto Scaling Amazon EC2 agar templat peluncuran EC2 dikonfigurasi

Amazon SageMaker

- [CT.SAGEMAKER.PR.1] Memerlukan instance notebook Amazon untuk mencegah akses internet langsung SageMaker
- [CT.SAGEMAKER.PR.2] Memerlukan instance notebook Amazon untuk digunakan dalam SageMaker VPC Amazon khusus
- [CT.SAGEMAKER.PR.3] Memerlukan instance notebook Amazon agar akses root tidak diizinkan SageMaker

Amazon API Gateway

- [CT.APIGATEWAY.PR.5] Memerlukan Amazon API Gateway V2 Websocket dan rute HTTP untuk menentukan jenis otorisasi

Amazon Relational Database Service (RDS)

- [CT.RDS.PR.25] Memerlukan kluster basis data Amazon RDS agar logging dikonfigurasi

Untuk informasi selengkapnya, lihat Kontrol proaktif.

Kontrol proaktif Amazon EC2 yang diperbarui

2 Mei 2023

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

AWS Control Tower telah memperbarui dua kontrol proaktif: CT.EC2.PR.3 danCT.EC2.PR.4.

Untuk CT.EC2.PR.3 kontrol yang diperbarui, AWS CloudFormation penerapan apa pun yang mereferensikan daftar awalan untuk sumber daya grup keamanan diblokir dari penerapan, kecuali untuk port 80 atau 443.

Untuk CT.EC2.PR.4 kontrol yang diperbarui, AWS CloudFormation penyebaran apa pun yang mereferensikan daftar awalan untuk sumber daya grup keamanan diblokir jika port 3389, 20, 23, 110, 143, 3306, 8080, 1433, 9200, 9300, 25, 445, 135, 135, 21, 1434, 4333, 5432, 5500, 5500, 5601, 22, 3000, 5000, 8088, 8888.

Tujuh tambahan Wilayah AWS tersedia

April 19, 2023

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

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). Wilayah tambahan untuk AWS Control Tower ini, yang disebut Wilayah keikutsertaan, tidak aktif secara default, kecuali Wilayah AS Barat (California Utara), yang aktif secara default.

Beberapa kontrol di AWS Control Tower tidak beroperasi di beberapa tambahan ini Wilayah AWS jika AWS Control Tower tersedia, karena Wilayah tersebut tidak mendukung fungsionalitas dasar yang diperlukan. Lihat perinciannya di Keterbatasan kontrol.

Di antara wilayah-wilayah baru ini, CFCT tidak tersedia di Asia Pasifik (Jakarta dan Osaka). Ketersediaan di tempat lain Wilayah AWS tidak berubah.

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

Titik akhir VPCe yang diperlukan oleh AFT tidak tersedia di Wilayah Timur Tengah (Bahrain). Pelanggan yang menerapkan AFT di Wilayah ini diharuskan untuk menerapkan dengan parameter. `aft_vpc_endpoints=false` Untuk informasi selengkapnya, lihat parameter dalam file README.

AWS Control Tower VPC memiliki dua Availability Zone di Wilayah AS Barat (California N.)`us-west-1`, karena keterbatasan di Amazon EC2. Di AS Barat (California Utara), enam subnet dibagi menjadi dua Availability Zone. Untuk informasi selengkapnya, lihat Ikhtisar AWS Control Tower dan VPC.

AWS Control Tower menambahkan izin baru `AWSControlTowerServiceRolePolicy` yang memungkinkan AWS Control Tower melakukan panggilan ke`EnableRegion`,`ListRegions`, dan `GetRegionOptStatus` API yang diterapkan oleh layanan Manajemen AWS Akun, agar tambahan ini Wilayah AWS tersedia untuk akun bersama Anda di landing zone (Akun manajemen, akun arsip Log, akun Audit), dan akun anggota OU Anda. Untuk informasi selengkapnya, lihat Kebijakan terkelola untuk AWS Control Tower.

Account Factory untuk penelusuran permintaan kustomisasi akun Terraform (AFT)

Februari 16, 2023

AFT mendukung penelusuran permintaan kustomisasi akun. Setiap kali Anda mengirimkan permintaan kustomisasi akun, AFT menghasilkan token penelusuran unik yang melewati mesin AWS Step Functions status kustomisasi AFT, yang mencatat token sebagai bagian dari pelaksanaannya. Anda dapat menggunakan kueri wawasan Amazon CloudWatch Logs untuk mencari rentang stempel waktu dan mengambil token permintaan. Akibatnya, Anda dapat melihat muatan yang menyertai token, sehingga Anda dapat melacak permintaan penyesuaian akun Anda di seluruh alur kerja AFT. Untuk informasi selengkapnya tentang AFT, lihat Ikhtisar AWS Control Tower Account Factory untuk Terraform. Untuk informasi tentang CloudWatch Log dan Step Functions, lihat berikut ini:

- Apa itu Amazon CloudWatch Logs? di Panduan Pengguna CloudWatch Log Amazon
- Apa itu AWS Step Functions? di Panduan AWS Step Functions Pengembang

AWS Control Tower landing zone versi 3.1

9 Februari 2023

(Pembaruan diperlukan untuk landing zone AWS Control Tower ke versi 3.1. Untuk informasi, lihatPerbarui Zona Pendaratan Anda)

AWS Control Tower landing zone versi 3.1 mencakup pembaruan berikut:

- Dengan rilis ini, AWS Control Tower menonaktifkan pencatatan akses yang tidak perlu untuk bucket logging akses Anda, yang merupakan bucket Amazon S3 tempat log akses disimpan di akun Arsip Log, sambil terus mengaktifkan pencatatan akses server untuk bucket S3. Rilis ini juga mencakup pembaruan pada kontrol Region Deny yang memungkinkan tindakan tambahan untuk layanan global, seperti AWS Support Paket dan AWS Artifact.
- Penonaktifan pencatatan akses server untuk bucket logging akses AWS Control Tower menyebabkan Security Hub membuat temuan untuk bucket logging akses akun Arsip Log, karena AWS Security Hub aturan, pencatatan akses server bucket [S3.9] S3 harus diaktifkan. Sejalan dengan Security Hub, sebaiknya Anda menekan temuan khusus ini, seperti yang dinyatakan dalam deskripsi Security Hub dari aturan ini. Untuk informasi tambahan, lihat informasi tentang temuan yang ditekan.
- Pencatatan akses untuk bucket logging (reguler) di akun Arsip Log tidak berubah di versi 3.1. Sejalan dengan praktik terbaik, peristiwa akses untuk bucket tersebut direkam sebagai entri log di bucket logging akses. Untuk informasi selengkapnya tentang pencatatan akses, lihat Permintaan logging 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 Tolak akses AWS berdasarkan permintaan Wilayah AWS dan Kontrol yang meningkatkan perlindungan residensi data.

  Layanan global menambahkan:

  - 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 Lightsail () `lightsail:Get*`
- Penjelajah Sumber Daya AWS (`resource-explorer-2:*`)
- Amazon S3 (`s3:CreateMultiRegionAccessPoint`,,`s3:GetBucketPolicyStatus`) `s3:PutMultiRegionAccessPointPolicy`
- AWS Savings Plans (`savingsplans:*`)
- Pusat Identitas IAM () `sso:*`
- AWS Support App (`supportapp:*`)
- AWS Support Rencana (`supportplans:*`)
- AWS Keberlanjutan () `sustainability:*`
- AWS Resource Groups Tagging API (`tag:GetResources`)
- AWS Marketplace Wawasan Vendor () `vendor-insights:ListEntitledSecurityProfiles`

Kontrol proaktif umumnya tersedia

Januari 24, 2023

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

Kontrol proaktif opsional, yang sebelumnya diumumkan dalam status pratinjau, sekarang tersedia secara umum. Kontrol ini disebut sebagai proaktif karena mereka memeriksa sumber daya Anda — sebelum sumber daya digunakan — untuk menentukan apakah sumber daya baru mematuhi kontrol yang diaktifkan di lingkungan Anda. Untuk informasi selengkapnya, lihat Kontrol komprehensif membantu dalam penyediaan dan manajemen AWS sumber daya.

Januari - Desember 2022

Pada tahun 2022, AWS Control Tower merilis pembaruan berikut:

- Operasi akun bersamaan
- Kustomisasi Account Factory (AFC)
- Kontrol komprehensif membantu dalam penyediaan dan manajemen AWS sumber daya
- Status kepatuhan dapat dilihat untuk semua AWS Config aturan
- API untuk kontrol dan sumber AWS CloudFormation daya baru

- CFCT mendukung penghapusan set tumpukan
- Retensi log yang disesuaikan
- Perbaikan drift peran tersedia
- AWS Control Tower landing zone versi 3.0
- Halaman Organisasi menggabungkan tampilan OU dan akun
- Mendaftar dan memperbarui akun anggota individu yang lebih mudah
- AFT mendukung kustomisasi otomatis untuk akun AWS Control Tower bersama
- Operasi bersamaan untuk semua kontrol opsional
- Akun keamanan dan pencatatan yang ada
- AWS Control Tower landing zone versi 2.9
- AWS Control Tower landing zone versi 2.8

Operasi akun bersamaan

Desember 16, 2022

(Tidak diperlukan pembaruan untuk landing zone 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 Account Factory (AFC)

November 28, 2022

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

Kustomisasi pabrik akun memungkinkan Anda menyesuaikan akun baru dan yang sudah ada dari dalam konsol AWS Control Tower. Kemampuan kustomisasi baru ini memberi Anda fleksibilitas untuk menentukan cetak biru akun, yang merupakan AWS CloudFormation templat yang terdapat dalam produk Service Catalog 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 akun lain ke AWS Control Tower, dan memperbarui AWS akun AWS Control Tower yang ada.

Saat Anda menyediakan, mendaftarkan, atau memperbarui akun di pabrik akun, Anda akan memilih cetak biru yang akan diterapkan. Sumber daya yang ditentukan dalam cetak biru disediakan di akun Anda. Ketika akun Anda telah selesai dibangun, semua konfigurasi kustom tersedia untuk digunakan segera.

Untuk memulai dengan menyesuaikan akun, Anda dapat menentukan sumber daya untuk kasus penggunaan yang dimaksudkan dalam produk Service Catalog. Anda juga dapat memilih solusi yang dikelola mitra dari Pustaka AWS Memulai. Untuk informasi selengkapnya, lihat Kustomisasi akun dengan Kustomisasi Account Factory (AFC).

Kontrol komprehensif membantu dalam penyediaan dan manajemen AWS sumber daya

November 28, 2022

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

AWS Control Tower sekarang mendukung manajemen kontrol yang komprehensif, termasuk kontrol proaktif opsional baru, yang diimplementasikan melalui AWS 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 AWS Control Tower Anda; dengan memenuhi persyaratan kerangka kerja kepatuhan standar industri; dan dengan mengatur interaksi AWS Control Tower di lebih dari dua puluh layanan lainnya. AWS

Pustaka kontrol AWS Control Tower 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, melalui Security Hub Service-Managed Standard yang baru: AWS Control Tower, yang mendukung standar AWS Foundational Security Best Practices (FSBP). Anda dapat melihat lebih dari 160 kontrol Security Hub bersama kontrol AWS Control Tower di konsol, dan Anda dapat memperoleh skor keamanan Security Hub untuk lingkungan AWS Control Tower Anda. Untuk informasi selengkapnya, lihat Kontrol Security Hub.

Status kepatuhan dapat dilihat untuk semua AWS Config aturan

November 18, 2022

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

AWS Control Tower sekarang menampilkan status kepatuhan semua AWS Config aturan yang diterapkan 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 Config, yang disebut kontrol detektif, di AWS Control Tower, atau mengaturnya secara langsung melalui layanan. AWS Config 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 aturan yang tidak sesuai. AWS Config Sekarang Anda dapat mengidentifikasi AWS Config aturan yang tidak sesuai dalam konsol AWS Control Tower. Untuk melihat status kepatuhan semua aturan Config 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 diterapkan di luar AWS Control Tower.

API untuk kontrol dan sumber AWS CloudFormation daya baru

September 1, 2022

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

AWS Control Tower sekarang mendukung manajemen kontrol terprogram, juga dikenal sebagai pagar pembatas, melalui serangkaian panggilan API. AWS CloudFormation Sumber daya baru mendukung fungsionalitas API untuk kontrol. Untuk lebih jelasnya, lihat Mengotomatiskan tugas di AWS Control Tower dan Menciptakan AWS Control Tower sumber daya dengan AWS CloudFormation.

API ini memungkinkan Anda mengaktifkan, menonaktifkan, dan melihat status aplikasi kontrol di pustaka AWS Control Tower. API menyertakan dukungan untuk AWS CloudFormation, sehingga Anda dapat mengelola AWS sumber daya sebagai infrastructure-as-code (IAc). AWS Control Tower menyediakan kontrol preventif dan detektif opsional yang menyatakan maksud 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 yang disertakan dalam rilis ini

- EnableControl— Panggilan API ini mengaktifkan kontrol. Ini memulai operasi asinkron yang menciptakan AWS sumber daya pada unit organisasi yang ditentukan 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 EnableControlatau DisableControloperasi.
- ListEnabledControls— Daftar 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 Pengidentifikasi sumber daya untuk API dan kontrol, di Panduan Pengguna AWS Control Tower.

CFCT mendukung penghapusan set tumpukan

Agustus 26, 2022

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

Kustomisasi untuk AWS Control Tower (CFCT) sekarang mendukung penghapusan set tumpukan, dengan menetapkan parameter dalam file. `manifest.yaml` Untuk informasi selengkapnya, lihat Hapus set tumpukan.

> **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.

Retensi log yang disesuaikan

Agustus 15, 2022

(Pembaruan diperlukan untuk landing zone AWS Control Tower. Untuk informasi, lihatPerbarui Zona Pendaratan Anda)

AWS Control Tower kini menyediakan kemampuan untuk menyesuaikan kebijakan retensi untuk bucket Amazon S3 yang menyimpan log AWS Control Tower Anda. CloudTrail Anda dapat menyesuaikan kebijakan penyimpanan log Amazon S3 Anda, dalam beberapa hari atau tahun, hingga maksimal 15 tahun.

Jika Anda memilih untuk tidak menyesuaikan penyimpanan log Anda, pengaturan default adalah 1 tahun untuk pencatatan akun standar, dan 10 tahun untuk pencatatan akses.

Fitur ini tersedia untuk pelanggan lama melalui AWS Control Tower saat Anda memperbarui atau memperbaiki landing zone, dan untuk pelanggan baru melalui proses penyiapan AWS Control Tower.

Perbaikan drift peran tersedia

Agustus 11, 2022

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

AWS Control Tower sekarang mendukung perbaikan untuk drift peran. Anda dapat mengembalikan peran yang diperlukan tanpa perbaikan penuh dari landing zone Anda. Jika jenis perbaikan drift ini diperlukan, halaman kesalahan konsol menyediakan langkah-langkah untuk memulihkan peran, sehingga landing zone Anda sekali lagi tersedia.

AWS Control Tower landing zone versi 3.0

Juli 29, 2022

(Pembaruan diperlukan untuk landing zone AWS Control Tower ke versi 3.0. Untuk informasi, lihatPerbarui Zona Pendaratan Anda)

AWS Control Tower landing zone versi 3.0 mencakup pembaruan berikut:

- Opsi untuk memilih jalur tingkat organisasi, atau memilih keluar dari AWS CloudTrail 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 asal Anda saja.
- Pembaruan ke Wilayah menolak kontrol.
- Pembaruan untuk kebijakan terkelola, AWSControlTowerServiceRolePolicy.
- Kami tidak lagi membuat peran IAM `aws-controltower-CloudWatchLogsRole` dan grup CloudWatch log `aws-controltower/CloudTrailLogs` di setiap akun yang 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.

CloudTrail Jalur tingkat organisasi di AWS Control Tower

Dengan landing zone versi 3.0, AWS Control Tower kini mendukung jalur tingkat organisasi AWS CloudTrail .

Saat memperbarui landing zone AWS Control Tower ke versi 3.0, Anda memiliki opsi untuk memilih AWS CloudTrail jalur tingkat organisasi sebagai preferensi logging 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. Jika pembaruan landing zone 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.

Ke depan dari landing zone 3.0, AWS Control Tower tidak lagi mendukung jalur tingkat akun yang mengelola. AWS 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 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 di mana mereka disimpan. 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 pencatatan ke lokasi tersebut. Jika Anda memilih untuk memilih keluar dari jalur yang dikelola oleh AWS Control Tower, log yang ada tetap ada 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 CloudTrail Anda berbeda dari 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 jejak tingkat akun Anda sendiri, kami sarankan Anda membuat jejak baru sebelum menyelesaikan pembaruan ke AWS Control Tower landing zone versi 3.0, untuk segera memulai pencatatan.

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 landing zone ke versi 3.0 atau yang lebih baru. Anda dapat memilih dan memilih keluar dari jalur tingkat organisasi, setiap kali Anda memperbarui landing zone 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.

Rekam AWS Config sumber daya di wilayah asal saja

Di landing zone versi 3.0, AWS Control Tower telah memperbarui konfigurasi baseline 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 asal Anda.

Konfigurasi ini dianggap sebagai praktik terbaik. Hal ini direkomendasikan oleh AWS Security Hub 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 logging AWS CloudTrail

Sebagai bagian dari perubahan AWS CloudTrail jalur tingkat organisasi, AWS Control Tower memperkenalkan dua kontrol detektif baru yang memeriksa apakah diaktifkan. CloudTrail Kontrol pertama memiliki panduan Wajib, dan diaktifkan pada OU Keamanan selama pengaturan atau pembaruan landing zone 3.0 dan yang lebih baru. Kontrol kedua memiliki Panduan yang sangat direkomendasikan, dan secara opsional diterapkan ke OU selain OU Keamanan, yang sudah memiliki perlindungan kontrol wajib diberlakukan.

Kontrol wajib: Mendeteksi apakah akun bersama di bawah unit organisasi Keamanan telah AWS CloudTrail atau CloudTrail Lake diaktifkan

Kontrol yang sangat disarankan: Deteksi apakah akun telah AWS CloudTrail atau CloudTrail Lake diaktifkan

Untuk informasi selengkapnya tentang kontrol baru, lihat pustaka kontrol AWS Control Tower.

Pembaruan untuk Wilayah menolak kontrol

Kami memperbarui NotActiondaftar di Wilayah menolak kontrol untuk menyertakan tindakan oleh beberapa layanan tambahan, yang 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 landing zone 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. Captioning tersedia.

Panduan Video untuk Memperbarui Zona Pendaratan AWS Control Tower yang Ada ke Zona Pendaratan 3.

Halaman Organisasi menggabungkan tampilan OU dan akun

Juli 18, 2022

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower)

Halaman Organisasi baru di AWS Control Tower menampilkan tampilan hierarkis semua unit organisasi (OU) dan akun. Ini menggabungkan informasi dari halaman OU dan Akun, yang ada sebelumnya.

Di 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 mengkonfigurasi 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.

Mendaftar dan memperbarui akun anggota individu yang lebih mudah

Mei 31, 2022

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower)

AWS Control Tower sekarang memberi Anda kemampuan yang lebih baik untuk memperbarui dan mendaftarkan akun anggota satu per satu. Setiap akun menunjukkan kapan tersedia untuk pembaruan, sehingga Anda dapat lebih mudah memastikan bahwa akun anggota Anda menyertakan konfigurasi terbaru. Anda dapat memperbarui landing zone Anda, memulihkan penyimpangan akun, atau mendaftarkan akun ke OU terdaftar, dalam beberapa langkah efisien.

Saat Anda memperbarui akun, Anda tidak perlu menyertakan seluruh unit organisasi (OU) akun di setiap tindakan pembaruan. Akibatnya, waktu yang diperlukan untuk memperbarui akun individu sangat berkurang.

Anda dapat mendaftarkan akun ke AWS Control Tower OU dengan bantuan lebih lanjut dari konsol AWS Control Tower. Akun yang sudah ada yang Anda daftarkan di AWS Control Tower harus tetap memenuhi prasyarat akun, dan Anda harus menambahkan peran tersebut. `AWSControlTowerExecution` Kemudian, Anda dapat memilih OU terdaftar dan mendaftarkan akun ke dalamnya dengan memilih tombol Daftar.

Kami telah memisahkan fungsionalitas akun Daftarkan dari alur kerja Buat akun di pabrik akun, untuk membuat lebih banyak perbedaan antara proses serupa ini, dan membantu menghindari kesalahan penyiapan saat Anda memasukkan informasi akun.

AFT mendukung kustomisasi otomatis untuk akun AWS Control Tower bersama

Mei 27, 2022

(Tidak diperlukan pembaruan untuk landing zone 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 penyesuaian akun dan memperbarui manajemen, sekaligus melindungi keamanan konfigurasi akun Anda, karena Anda mencakup peran yang melakukan pekerjaan.

AWSAFTExecutionPeran yang ada sekarang menyebarkan penyesuaian di semua akun. Anda dapat mengatur izin IAM dengan batasan yang membatasi akses AWSAFTExecutionperan sesuai dengan persyaratan bisnis dan keamanan Anda. Anda juga dapat secara terprogram mendelegasikan izin penyesuaian yang disetujui dalam peran tersebut, untuk pengguna tepercaya. Sebagai praktik

terbaik, kami menyarankan Anda membatasi izin untuk izin yang diperlukan untuk menerapkan penyesuaian yang diperlukan.

AFT sekarang membuat AWSAFTServiceperan baru untuk menyebarkan sumber daya AFT di semua akun terkelola, termasuk akun bersama dan akun manajemen. Sumber daya sebelumnya dikerahkan oleh peran tersebut. AWSAFTExecution

Akun bersama dan manajemen AWS Control Tower tidak disediakan melalui pabrik akun, sehingga akun tersebut tidak memiliki produk yang disediakan sesuai. AWS Service Catalog Oleh karena itu, Anda tidak dapat memperbarui akun bersama dan manajemen di Service Catalog.

Operasi bersamaan untuk semua kontrol opsional

Mei 18, 2022

(Tidak diperlukan pembaruan untuk landing zone 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 individu selesai. Satu-satunya waktu terbatas adalah ketika AWS Control Tower sedang dalam proses penyiapan landing zone, atau saat memperluas tata kelola ke organisasi baru.

Fungsionalitas yang didukung untuk kontrol pencegahan:

- 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 target OU, meskipun 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 Anda yang sudah ada, dan AWS Control Tower memberikan laporan ringkasan tentang bagaimana setiap akun sesuai dengan kebijakan Anda yang diaktifkan. Untuk daftar lengkap kontrol yang tersedia, lihat pustaka kontrol AWS Control Tower.

Akun keamanan dan pencatatan yang ada

Mei 16, 2022

(Tersedia selama pengaturan awal.)

AWS Control Tower sekarang menyediakan opsi bagi Anda untuk menentukan AWS akun yang ada sebagai akun keamanan atau logging AWS Control Tower, selama proses penyiapan landing zone awal. Opsi ini menghilangkan kebutuhan AWS Control Tower untuk membuat akun baru yang dibagikan. Akun keamanan, yang disebut akun Audit secara default, adalah akun terbatas yang memberi tim keamanan dan kepatuhan Anda akses ke semua akun di landing zone 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 landing zone Anda.

Dengan menghadirkan akun keamanan dan pencatatan yang ada, akan lebih mudah untuk memperluas tata kelola AWS Control Tower ke organisasi Anda yang ada, atau pindah ke AWS Control Tower dari landing zone alternatif. Opsi bagi Anda untuk menggunakan akun yang ada ditampilkan selama pengaturan landing zone awal. Ini termasuk pemeriksaan selama proses penyiapan, yang memastikan penerapan berhasil. AWS Control Tower mengimplementasikan 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 dapat mendaftarkan akun ke AWS Control Tower.

AWS Control Tower landing zone versi 2.9

April 22, 2022

(Pembaruan diperlukan untuk landing zone AWS Control Tower ke versi 2.9. Untuk informasi, lihatPerbarui Zona Pendaratan Anda)

AWS Control Tower landing zone versi 2.9 memperbarui notifikasi forwarder 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.

AWS Control Tower landing zone versi 2.8

Februari 10, 2022

(Pembaruan diperlukan untuk landing zone AWS Control Tower ke versi 2.8. Untuk informasi, lihatPerbarui Zona Pendaratan Anda)

AWS Control Tower landing zone versi 2.8 menambahkan fungsionalitas yang selaras dengan pembaruan terbaru pada Praktik Terbaik Keamanan AWS Dasar.

Dalam rilis ini:

- Pencatatan akses dikonfigurasi untuk bucket log akses di akun Arsip Log, untuk melacak akses ke bucket log akses S3 yang ada.
- Support 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 Peran Tertaut AWS Layanan (SLR) yang disediakan oleh AWS Config, di semua akun terkelola (tidak termasuk akun manajemen), sehingga Anda dapat mengatur dan mengelola aturan Konfigurasi agar AWS Config sesuai dengan praktik 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 pengiriman pesan status terkait. CloudTrail
- Rilis ini mencakup pembaruan ke kontrol penolakan Wilayah, untuk memungkinkan `route53-application-recovery` fitur masuk`us-west-2`.
- Pembaruan: Pada 15 Februari 2022, kami menghapus antrian surat mati untuk fungsi AWS Lambda.

Detail tambahan:

- Jika Anda menonaktifkan landing zone, AWS Control Tower tidak menghapus peran AWS Config terkait layanan.
- Jika Anda membatalkan penyediaan akun Account Factory, AWS Control Tower tidak menghapus peran AWS Config terkait layanan.

Untuk memperbarui landing zone Anda ke 2.8, navigasikan ke halaman pengaturan zona pendaratan, pilih versi 2.8, lalu pilih Perbarui. Setelah memperbarui landing zone, Anda harus memperbarui semua akun yang diatur oleh AWS Control Tower, seperti yang diberikan. Manajemen pembaruan konfigurasi di AWS Control Tower

Januari - Desember 2021

Pada tahun 2021, AWS Control Tower merilis pembaruan berikut:

- Wilayah menolak kemampuan
- Fitur residensi data
- AWS Control Tower memperkenalkan penyediaan dan penyesuaian akun Terraform
- Acara siklus hidup baru tersedia
- AWS Control Tower memungkinkan OU bersarang
- Konkurensi kontrol detektif
- Dua Wilayah baru tersedia
- Pencabutan wilayah
- AWS Control Tower bekerja dengan Sistem Manajemen AWS Utama
- Kontrol berganti nama, fungsionalitas tidak berubah
- AWS Control Tower memindai SCP setiap hari untuk memeriksa drift
- Nama yang disesuaikan untuk OU dan akun
- AWS Control Tower landing zone versi 2.7
- Tiga AWS Wilayah baru tersedia
- Mengatur Wilayah yang dipilih saja
- AWS Control Tower sekarang memperluas tata kelola ke OU yang ada di organisasi Anda AWS
- AWS Control Tower menyediakan pembaruan akun massal

Wilayah menolak kemampuan

November 30, 2021

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower.)

AWS Control Tower sekarang menyediakan kemampuan penolakan Wilayah, 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 pembatalan pilihan Wilayah yang ada di AWS Control Tower. Bersama-sama, fitur-fitur ini membantu Anda mengatasi masalah kepatuhan dan peraturan, sambil menyeimbangkan biaya yang terkait dengan perluasan 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 penyiapan AWS Control Tower, atau di halaman pengaturan zona pendaratan. Fitur penolakan Wilayah tersedia saat Anda memperbarui versi landing zone AWS Control Tower. AWS Layanan tertentu dikecualikan dari kemampuan penolakan Wilayah. Untuk mempelajari lebih lanjut, lihat Mengonfigurasi kontrol penolakan Wilayah.

Fitur residensi data

November 30, 2021

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower)

AWS Control Tower kini menawarkan kontrol yang dibuat khusus untuk membantu memastikan bahwa data pelanggan yang Anda unggah ke AWS layanan hanya terletak di AWS Wilayah yang Anda tentukan. Anda dapat memilih AWS Wilayah atau Wilayah tempat data pelanggan Anda disimpan dan diproses. Untuk daftar lengkap AWS Wilayah di mana AWS Control Tower tersedia, lihat Tabel AWS Wilayah.

Untuk kontrol granular, Anda dapat menerapkan kontrol tambahan, seperti Larang koneksi Amazon Virtual Private Network (VPN), atau Larang akses internet untuk instans VPC Amazon. Anda dapat melihat status kepatuhan kontrol di konsol AWS Control Tower. Untuk daftar lengkap kontrol yang tersedia, lihat pustaka kontrol AWS Control Tower.

AWS Control Tower memperkenalkan penyediaan dan penyesuaian akun Terraform

November 29, 2021

(Pembaruan opsional untuk zona landing zone AWS Control Tower)

Anda sekarang dapat menggunakan Terraform untuk menyediakan dan memperbarui akun yang disesuaikan 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.

Pipa 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 for 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 landing zone AWS Control Tower)

`PrecheckOrganizationalUnit`Peristiwa mencatat apakah sumber daya apa pun memblokir tugas Perluas tata kelola agar tidak berhasil, termasuk sumber daya di OU bersarang. Untuk informasi selengkapnya, lihat `PrecheckOrganizationalUnit`.

AWS Control Tower memungkinkan OU bersarang

November 16, 2021

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower)

AWS Control Tower sekarang memungkinkan Anda untuk menyertakan OU bersarang sebagai bagian dari landing zone Anda.

AWS Control Tower menyediakan dukungan untuk unit organisasi bersarang (OU), memungkinkan Anda mengatur akun ke dalam beberapa tingkat hierarki, dan untuk menegakkan kontrol preventif secara hierarki. 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 AWS Control Tower OU 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 sekaligus, 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 secara otomatis. Akun lebih jauh ke bawah pohon dapat didaftarkan dengan mendaftarkan OU induk langsung mereka.
3. Kontrol preventif (SCP) diwariskan ke bawah hierarki secara otomatis; SCP yang diterapkan ke induk diwarisi oleh semua OU bersarang.
4. Kontrol Detektif (aturan AWS Config) TIDAK diwarisi secara otomatis.
5. Kepatuhan terhadap kontrol detektif dilaporkan oleh masing-masing OU.
6. Penyimpangan SCP pada OU memengaruhi semua akun dan OU di bawahnya.
7. Anda tidak dapat membuat OU bersarang baru di bawah Security OU (Core OU).

Konkurensi kontrol detektif

November 5, 2021

(Pembaruan opsional untuk zona landing zone 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.

Fungsionalitas yang didukung:

- Aktifkan kontrol detektif yang berbeda pada OU yang sama (misalnya, Deteksi Apakah MFA untuk Pengguna Root Diaktifkan dan 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 diperbaiki 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.
- Konkurensi 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 landing zone untuk memanfaatkan fitur lain, seperti pemilihan Wilayah dan pembatalan pilihan, yang tersedia dalam versi terbaru.

Dua Wilayah baru tersedia

Juli 29, 2021

(Pembaruan diperlukan untuk zona landing zone AWS Control Tower)

AWS Control Tower sekarang tersedia di dua AWS Wilayah tambahan: Amerika Selatan (Sao Paulo), dan Eropa (Paris). Pembaruan ini memperluas ketersediaan AWS Control Tower ke 15 AWS Wilayah.

Jika Anda baru mengenal AWS Control Tower, Anda dapat langsung meluncurkannya di salah satu Wilayah yang didukung. Selama peluncuran, Anda dapat memilih Wilayah yang Anda inginkan AWS Control Tower untuk 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 Landing di dasbor AWS Control Tower, lalu pilih Wilayah. Setelah memperbarui landing zone, Anda harus memperbarui semua akun yang diatur oleh AWS Control Tower.

Pencabutan wilayah

Juli 29, 2021

(Pembaruan opsional untuk zona landing zone AWS Control Tower)

Pembatalan pemilihan Wilayah AWS Control Tower meningkatkan kemampuan Anda untuk mengelola jejak geografis sumber daya AWS Control Tower Anda. Anda dapat membatalkan pilihan Wilayah yang tidak ingin lagi diatur oleh AWS Control Tower. Fitur ini memberi Anda kemampuan

untuk mengatasi masalah kepatuhan dan peraturan sambil menyeimbangkan biaya yang terkait dengan perluasan ke Wilayah tambahan.

Pembatalan pilihan wilayah tersedia saat Anda memperbarui versi landing zone AWS Control Tower.

Saat Anda menggunakan Account Factory untuk membuat akun baru atau mendaftarkan akun anggota yang sudah ada sebelumnya, atau saat Anda memilih Perluas Tata Kelola untuk mendaftarkan akun di unit organisasi yang sudah ada sebelumnya, AWS Control Tower menerapkan kemampuan tata kelolanya — 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 menerapkan AWS sumber daya atau beban kerja ke Wilayah tersebut.

AWS Control Tower bekerja dengan Sistem Manajemen AWS Utama

Juli 28, 2021

(Pembaruan opsional untuk zona landing zone 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 diterapkan AWS Control Tower, termasuk AWS CloudTrail AWS Config, dan data Amazon S3 terkait. AWS Enkripsi KMS adalah tingkat enkripsi yang ditingkatkan melalui enkripsi SSE-S3 yang digunakan AWS Control Tower secara default.

Integrasi dukungan AWS KMS ke AWS Control Tower sejalan dengan Praktik Terbaik Keamanan AWS Dasar, yang merekomendasikan lapisan keamanan tambahan untuk file log sensitif Anda. Anda harus menggunakan kunci yang AWS dikelola KMS (SSE-KMS) untuk enkripsi saat istirahat. AWS Dukungan enkripsi KMS tersedia saat Anda menyiapkan landing zone baru atau saat Anda memperbarui zona landing zone AWS Control Tower yang ada.

Untuk mengonfigurasi fungsi ini, Anda dapat memilih Konfigurasi Kunci KMS selama pengaturan landing zone 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 kunci SSE-KMS yang berbeda.

Untuk landing zone 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 landing zone AWS Control Tower)

AWS Control Tower merevisi nama dan deskripsi kontrol tertentu untuk mencerminkan maksud kebijakan kontrol dengan lebih baik. Nama dan deskripsi yang direvisi membantu Anda memahami secara lebih intuitif cara-cara kontrol mewujudkan kebijakan akun Anda. Misalnya, kami mengubah sebagian nama kontrol detektif dari “Larang” menjadi “Deteksi” karena kontrol detektif itu sendiri tidak menghentikan tindakan tertentu, hanya mendeteksi pelanggaran kebijakan dan memberikan peringatan melalui dasbor.

Fungsionalitas kontrol, panduan, dan implementasi tetap tidak berubah. Hanya nama dan deskripsi kontrol yang telah direvisi.

AWS Control Tower memindai SCP setiap hari untuk memeriksa drift

Mei 11, 2021

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower)

AWS Control Tower sekarang melakukan pemindaian otomatis harian SCP terkelola Anda untuk memverifikasi bahwa kontrol yang sesuai diterapkan dengan benar dan belum hanyut. Jika pemindaian menemukan penyimpangan, 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 pemberitahuan tambahan kecuali item drift baru ditemukan.

Nama yang disesuaikan untuk OU dan akun

April 16, 2021

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower)

AWS Control Tower sekarang memungkinkan Anda untuk menyesuaikan penamaan landing zone Anda. Anda dapat menyimpan nama yang direkomendasikan AWS Control Tower untuk unit organisasi (OU) dan akun inti, atau Anda dapat memodifikasi nama-nama ini selama proses penyiapan landing zone awal.

Nama default yang disediakan AWS Control Tower untuk akun OU dan 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 sudah ada dengan nama yang direkomendasikan yang sama, fungsi OU dan penamaan akun yang baru memberi Anda fleksibilitas untuk mengatasi kendala tersebut.

Terpisah dari perubahan alur kerja selama pengaturan, OU sebelumnya dikenal sebagai Core OU sekarang disebut Security OU, dan OU sebelumnya dikenal sebagai Custom OU 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 sudah ada akan terus melihat nama asli OU ini. Anda mungkin mengalami beberapa ketidakkonsistenan dalam penamaan OU saat kami memperbarui dokumentasi kami ke nama baru.

Untuk memulai AWS Control Tower dari AWS Management Console, buka konsol AWS Control Tower, dan pilih Siapkan landing zone di kanan atas. Untuk informasi tambahan, Anda dapat membaca tentang perencanaan landing zone AWS Control Tower Anda.

AWS Control Tower landing zone versi 2.7

April 8, 2021

(Pembaruan diperlukan untuk landing zone AWS Control Tower ke versi 2.7. Untuk informasi, lihatPerbarui Zona Pendaratan Anda)

Dengan AWS Control Tower versi 2.7, AWS Control Tower memperkenalkan empat kontrol Log Archive pencegahan wajib baru yang menerapkan kebijakan hanya pada sumber daya AWS Control Tower. Kami telah menyesuaikan panduan tentang empat kontrol Arsip Log yang ada dari wajib ke elektif, karena mereka menetapkan kebijakan untuk sumber daya di luar AWS Control Tower. Perubahan dan ekspansi kontrol ini memberikan kemampuan untuk memisahkan tata kelola Arsip Log untuk sumber daya dalam AWS Control Tower dari tata kelola sumber daya di luar AWS Control Tower.

Keempat kontrol yang diubah dapat digunakan bersama dengan kontrol wajib baru untuk menyediakan tata kelola ke set Arsip Log yang lebih luas. AWS Lingkungan AWS Control Tower yang ada akan membuat keempat kontrol yang diubah ini diaktifkan 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 AWS Control Tower Membuat Bucket S3 di Arsip Log
- Larang Perubahan Konfigurasi Logging untuk AWS Control Tower Membuat Bucket S3 di Arsip Log
- Larang Perubahan Kebijakan Bucket untuk AWS Control Tower Membuat Bucket S3 di Arsip Log
- Larang Perubahan pada Konfigurasi Siklus Hidup untuk AWS Control Tower Membuat Bucket S3 di Arsip Log

Panduan berubah dari Wajib menjadi Pilihan:

- Larang Perubahan Konfigurasi Enkripsi untuk semua Bucket Amazon S3 [Sebelumnya: Aktifkan Enkripsi saat Istirahat untuk Arsip Log]
- Larang Perubahan pada Konfigurasi Logging untuk semua Bucket Amazon S3 [Sebelumnya: Aktifkan Pencatatan Akses untuk Arsip Log]
- Larang Perubahan Kebijakan Bucket untuk semua Bucket Amazon S3 [Sebelumnya: Larang Perubahan Kebijakan pada Arsip Log]
- Larang 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 landing zone AWS Control Tower yang dapat menyebabkan ketidakcocokan dengan versi sebelumnya setelah Anda meningkatkan ke 2.7.

- Secara khusus, AWS Control Tower versi 2.7 memungkinkan `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 Memblokir 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 secure socket layer (SSL). Hanya permintaan HTTPS yang diizinkan untuk lulus. 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 landing zone Anda.

Kami menyarankan Anda mengubah permintaan Anda untuk menggunakan TLS alih-alih HTTP.

Tiga AWS Wilayah baru tersedia

April 8, 2021

(Pembaruan diperlukan untuk zona landing zone AWS Control Tower)

AWS Control Tower tersedia di tiga AWS Wilayah tambahan: Wilayah Asia Pasifik (Tokyo), Wilayah Asia Pasifik (Seoul), dan Wilayah Asia Pasifik (Mumbai). Pembaruan landing zone ke versi 2.7 diperlukan untuk memperluas tata kelola ke Wilayah ini.

Landing zone 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.

Mengatur Wilayah yang dipilih saja

Februari 19, 2021

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower)

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.

Pemilihan wilayah tersedia saat Anda menyiapkan landing zone baru atau memperbarui versi landing zone AWS Control Tower. Saat Anda menggunakan Account Factory untuk membuat akun baru atau mendaftarkan akun anggota yang sudah ada sebelumnya, atau saat Anda menggunakan Perluas Tata Kelola untuk mendaftarkan akun di unit organisasi yang sudah ada sebelumnya, AWS Control Tower menerapkan kemampuan tata kelola untuk pencatatan, pemantauan, dan kontrol terpusat di Wilayah pilihan Anda di akun. Untuk informasi selengkapnya tentang memilih Wilayah, lihat[Konfigurasikan Wilayah AWS Control Tower Anda](#).

AWS Control Tower sekarang memperluas tata kelola ke OU yang ada di organisasi Anda AWS

Januari 28, 2021

(Tidak diperlukan pembaruan untuk landing zone 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, lihat. Daftarkan unit organisasi yang ada dengan AWS Control Tower

Saat Anda mendaftarkan OU, AWS Control Tower melakukan serangkaian pemeriksaan untuk memastikan perpanjangan tata kelola dan pendaftaran akun yang berhasil dalam OU. Untuk informasi lebih lanjut tentang masalah umum yang terkait dengan pendaftaran awal OU, lihatPenyebab umum kegagalan saat pendaftaran atau pendaftaran ulang.

Anda juga dapat mengunjungi halaman web produk AWS Control Tower atau mengunjungi YouTube untuk menonton video tentang memulai AWS Control Tower ini. AWS Organizations

AWS Control Tower menyediakan pembaruan akun massal

Januari 28, 2021

(Tidak diperlukan pembaruan untuk landing zone 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 landing zone AWS Control Tower dan juga harus memperbarui akun terdaftar Anda untuk menyelaraskannya dengan versi landing zone saat ini.

Fitur ini juga membantu Anda memperbarui akun saat memperbarui zona landing AWS Control Tower untuk memperluas ke wilayah baru, atau saat 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 landing zone, lihatPerbarui Zona Pendaratan Anda.

Untuk informasi tentang mendaftar atau mendaftarkan ulang OU, lihatDaftarkan 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 aturan AWS Config eksternal
- AWS Control Tower sekarang tersedia di Wilayah tambahan
- Pembaruan pagar pembatas
- Konsol AWS Control Tower menampilkan detail lebih lanjut tentang OU dan akun
- Gunakan AWS Control Tower untuk menyiapkan AWS lingkungan multi-akun baru di AWS Organizations
- Kustomisasi untuk solusi AWS Control Tower
- Ketersediaan umum AWS Control Tower versi 2.3
- Penyediaan akun satu langkah di AWS Control Tower
- Alat penonaktifan AWS Control Tower
- Pemberitahuan acara siklus hidup AWS Control Tower

Konsol AWS Control Tower sekarang terhubung ke aturan AWS Config eksternal

Desember 29, 2020

(Pembaruan diperlukan untuk landing zone AWS Control Tower ke versi 2.6. Untuk informasi, lihatPerbarui Zona Pendaratan Anda)

AWS Control Tower sekarang menyertakan agregator tingkat organisasi, yang membantu mendeteksi aturan Config eksternal. AWS Ini memberi Anda visibilitas di konsol AWS Control Tower untuk melihat keberadaan aturan Config yang dibuat secara eksternal selain aturan AWS Config yang dibuat AWS oleh AWS Control Tower. Agregator memungkinkan AWS Control Tower mendeteksi aturan eksternal dan menyediakan tautan ke konsol AWS Config tanpa perlu 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 Cara 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

(Pembaruan diperlukan untuk landing zone AWS Control Tower ke versi 2.5. Untuk informasi, lihatPerbarui Zona Pendaratan Anda)

AWS Control Tower sekarang tersedia di 5 AWS Wilayah tambahan:

- Wilayah Asia Pasifik (Singapura)
- Wilayah Eropa (Frankfurt)
- Wilayah Eropa (London)
- Wilayah Eropa (Stockholm)
- Wilayah Kanada (Pusat)

Penambahan 5 AWS Wilayah ini adalah satu-satunya perubahan yang diperkenalkan untuk AWS Control Tower versi 2.5.

AWS Control Tower juga tersedia di Wilayah AS Timur (Virginia N.), 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 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 . Untuk informasi, lihat Konfigurasikan Wilayah AWS Control Tower Anda.

Pembaruan pagar pembatas

Oktober 8, 2020

(Tidak diperlukan pembaruan untuk landing zone 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 pada Peran AWS IAM yang Diatur oleh AWS Control Tower dan AWS CloudFormation di Panduan Referensi AWS Control Tower Control Tower.

Konsol AWS Control Tower menampilkan detail lebih lanjut tentang OU dan akun

Juli 22, 2020

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower)

Anda dapat melihat organisasi dan akun Anda yang tidak terdaftar di AWS Control Tower, bersama organisasi dan akun yang terdaftar.

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.

Gunakan AWS Control Tower untuk menyiapkan AWS lingkungan multi-akun baru di AWS Organizations

April 22, 2020

(Tidak diperlukan pembaruan untuk landing zone 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:

- AWS Organizations Pelanggan yang sudah ada sekarang dapat menyiapkan landing zone 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 scripting.

AWS Control Tower menyediakan layanan orkestrasi yang menggunakan layanan lain. AWS 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 di 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 pengaturan landing zone, lihatRencanakan landing zone AWS Control Tower. Anda juga dapat mengunjungi halaman web produk AWS Control Tower atau mengunjungi YouTube untuk menonton video tentang memulai AWS Control Tower ini. AWS Organizations

Selain perubahan ini, kemampuan penyediaan akun Cepat di AWS Control Tower diubah namanya menjadi akun Enroll. Sekarang memungkinkan pendaftaran akun yang ada serta pembuatan AWS akun baru. Untuk informasi selengkapnya, lihat Daftarkan akun yang ada.

Kustomisasi untuk solusi AWS Control Tower

Maret 17, 2020

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower)

AWS Control Tower sekarang menyertakan implementasi referensi baru yang memudahkan Anda menerapkan templat dan kebijakan khusus ke landing zone AWS Control Tower Anda.

Dengan penyesuaian AWS Control Tower, Anda dapat menggunakan AWS CloudFormation templat untuk menerapkan sumber daya baru ke akun yang ada dan baru dalam organisasi Anda. Anda juga dapat menerapkan kebijakan kontrol layanan kustom (SCP) ke akun tersebut selain SCP yang sudah disediakan oleh AWS Control Tower. Kustomisasi untuk pipeline AWS Control Tower terintegrasi dengan peristiwa siklus hidup AWS Control Tower dan notifikasi (Peristiwa Siklus Hidup di AWS Control Tower) untuk memastikan bahwa penerapan sumber daya tetap sinkron dengan landing zone Anda.

Dokumentasi penerapan untuk arsitektur solusi AWS Control Tower ini tersedia melalui halaman web AWS Solusi.

Ketersediaan umum AWS Control Tower versi 2.3

Maret 5, 2020

(Pembaruan diperlukan untuk landing zone AWS Control Tower. Untuk informasi, lihatPerbarui Zona Pendaratan Anda.)

AWS Control Tower sekarang tersedia di Wilayah Asia Pasifik (Sydney), selain AWS Wilayah AS Timur (Ohio), AS Timur (Virginia N.), 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 Pengaturan di dasbor AWS Control Tower Anda. Dari sana, perbarui landing zone Anda ke rilis terbaru. Kemudian, perbarui akun Anda satu per satu.

> **Note**
>
> Memperbarui landing zone Anda tidak secara otomatis memperbarui akun Anda. Jika Anda memiliki lebih dari beberapa akun, pembaruan yang diperlukan dapat memakan waktu. Oleh karena itu, kami menyarankan agar Anda menghindari perluasan landing zone AWS Control Tower Anda ke Wilayah di mana Anda tidak memerlukan beban kerja Anda untuk dijalankan.

Untuk informasi tentang perilaku kontrol detektif yang diharapkan sebagai hasil penerapan ke Wilayah baru, lihat Mengonfigurasi Wilayah AWS Control Tower Anda.

Penyediaan akun satu langkah di AWS Control Tower

Maret 2, 2020

(Tidak diperlukan pembaruan untuk landing zone 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 Account Factory di konsol AWS Control Tower, lalu pilih Penyediaan akun Cepat. AWS Control Tower menetapkan alamat email yang sama ke akun yang disediakan dan pengguna masuk tunggal (IAM Identity Center) yang dibuat untuk akun tersebut. Jika Anda mengharuskan kedua alamat email ini berbeda, Anda harus menyediakan akun Anda melalui Service Catalog.

Perbarui akun yang Anda buat melalui penyediaan akun cepat dengan menggunakan Service Catalog dan pabrik akun AWS Control Tower, sama seperti pembaruan ke akun lainnya.

> **Note**
>
> Pada April 2020, kemampuan penyediaan akun Cepat diubah namanya menjadi akun Daftarkan. 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 Daftarkan akun yang ada.

Alat penonaktifan AWS Control Tower

Februari 28, 2020

(Tidak diperlukan pembaruan untuk landing zone 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 menggunakan AWS Control Tower untuk perusahaan Anda, atau jika Anda memerlukan pemindahan besar-besaran sumber daya organisasi Anda, Anda mungkin ingin membersihkan sumber daya yang dibuat saat pertama kali menyiapkan landing zone Anda.

Untuk menonaktifkan landing zone Anda dengan menggunakan proses yang sebagian besar otomatis, hubungi AWS Support untuk mendapatkan bantuan dengan langkah-langkah tambahan yang diperlukan. Untuk informasi lebih lanjut tentang penonaktifan, lihat. Panduan: Menonaktifkan Zona Pendaratan AWS Control Tower

Pemberitahuan acara siklus hidup AWS Control Tower

Januari 22, 2020

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower)

AWS Control Tower mengumumkan ketersediaan notifikasi peristiwa siklus hidup. Peristiwa 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 peristiwa.

AWS Control Tower mencatat peristiwa siklus hidup setelah menyelesaikan tindakan berikut yang dapat dilakukan menggunakan layanan: membuat atau memperbarui landing zone; 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 lingkungan multi-akun AWS praktik terbaik. Diperlukan waktu beberapa menit untuk menyelesaikan aksi 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.

Januari - Desember 2019

Mulai 1 Januari 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

(Pembaruan diperlukan untuk landing zone AWS Control Tower. Untuk informasi, lihatPerbarui Zona Pendaratan Anda.)

AWS Control Tower versi 2.2 menyediakan tiga kontrol preventif baru yang mencegah penyimpangan di akun:

- Larang Perubahan pada Grup CloudWatch Log Amazon Logs yang disiapkan oleh AWS Control Tower
- Larang Penghapusan Otorisasi AWS Config Agregasi yang Dibuat oleh AWS Control Tower
- Larang Penghapusan Arsip Log

Kontrol adalah aturan tingkat tinggi yang menyediakan tata kelola berkelanjutan untuk lingkungan Anda secara keseluruhan AWS . Saat Anda membuat landing zone AWS Control Tower, 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 (disengaja atau disengaja) dalam status kepatuhan ini dapat terjadi. Deteksi drift membantu Anda mengidentifikasi sumber daya yang memerlukan perubahan atau pembaruan konfigurasi untuk menyelesaikan penyimpangan. Untuk informasi selengkapnya, lihat Mendeteksi dan mengatasi penyimpangan di AWS Control Tower.

Kontrol elektif baru di AWS Control Tower

September 05, 2019

(Tidak diperlukan pembaruan untuk landing zone AWS Control Tower)

AWS Control Tower sekarang mencakup empat kontrol elektif baru berikut:

- Larang Hapus Tindakan di Bucket Amazon S3 Tanpa MFA
- Larang Perubahan Konfigurasi Replikasi untuk Bucket Amazon S3
- Larang Tindakan sebagai Pengguna Root
- Larang Pembuatan Kunci Akses untuk Pengguna Root

Kontrol adalah aturan tingkat tinggi yang menyediakan tata kelola berkelanjutan untuk lingkungan Anda secara keseluruhan AWS . Guardrails 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 landing zone AWS Control Tower)

AWS Control Tower sekarang mencakup delapan kontrol detektif baru berikut:

- Deteksi Apakah Pembuatan Versi untuk Bucket Amazon S3 Diaktifkan
- Mendeteksi Apakah MFA Diaktifkan untuk Pengguna IAM Konsol AWS
- Mendeteksi Apakah MFA Diaktifkan untuk Pengguna IAM
- Mendeteksi Apakah Optimasi Amazon EBS Diaktifkan untuk Instans Amazon EC2

- Mendeteksi Apakah Volume Amazon EBS Terlampir ke Instans Amazon EC2
- Mendeteksi Apakah Akses Publik ke Instans Basis Data Amazon RDS Diaktifkan
- Deteksi Apakah Akses Publik ke Snapshot Basis Data Amazon RDS Diaktifkan
- Mendeteksi Apakah Enkripsi Penyimpanan Diaktifkan untuk Instans Basis Data Amazon RDS

Kontrol adalah aturan tingkat tinggi yang menyediakan tata kelola berkelanjutan untuk lingkungan Anda secara keseluruhan AWS . 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 landing zone 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 landing zone baru dan saat Anda menyediakan akun anak baru.

Ketersediaan umum AWS Control Tower versi 2.1

Juni 24, 2019

(Pembaruan diperlukan untuk landing zone AWS Control Tower. Untuk selengkapnya, lihat Memperbarui 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 mengatur AWS lingkungan multi-akun baru mereka dan mengatur dalam skala besar. Dengan AWS Control Tower, Anda dapat membantu memastikan bahwa akun di organisasi Anda sesuai dengan kebijakan yang ditetapkan. Pengguna akhir di tim terdistribusi dapat menyediakan AWS akun baru dengan cepat.

Dengan AWS Control Tower, Anda dapat menyiapkan landing zone yang menggunakan praktik terbaik seperti mengonfigurasi struktur multi-akun menggunakan AWS Organizations, mengelola

identitas pengguna, dan akses gabungan, mengaktifkan penyediaan akun melalui Service Catalog AWS IAM Identity Center, dan membuat arsip log terpusat menggunakan dan. AWS CloudTrail AWS Config

Untuk tata kelola yang sedang berlangsung, Anda dapat mengaktifkan kontrol pra-konfigurasi, yang merupakan aturan yang jelas untuk keamanan, operasi, dan kepatuhan. Guardrails membantu mencegah penyebaran sumber daya yang tidak sesuai dengan kebijakan dan terus memantau sumber daya yang diterapkan 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 diaktifkan untuk menyiapkan landing zone dan menerapkan kontrol yang dipilih.

Riwayat dokumen

- Pembaruan dokumentasi terbaru: 20 Mei 2024

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
AWS Control Tower mendukung hingga 100 operasi kontrol bersamaan	Peningkatan kuota operasi kontrol bersamaan menjadi 100.	20 Mei 2024
AWS Control Tower tersedia di AWS Wilayah Calgary West (Kanada)	AWS Control Tower tersedia di Wilayah Canada West (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 AWS CloudFormation	AWS Control Tower mendukung penambahan tag ke `EnabledControl` sumber daya, melalui AWS 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 Security Hub tambahan tersedia	AWS Control Tower menambahkan sepuluh kontrol baru ke pustaka kontrol, untuk Standar yang Dikelola Layanan 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	Dukungan wilayah tunggal 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 selengkapnya, 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 AWS 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, AWS CloudFormation sumber daya	AWS Control Tower sekarang mendukung aktivasi dan penonaktifan kontrol melalui serangkaian panggilan API, dan AWS 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 sekarang 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 pencegahan 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.