Panduan Pengguna

AWS Organizations

AWS Organizations: Panduan Pengguna

Table of Contents

Apa itu AWS Organizations?

AWS Organizations adalah sebuah layanan pengelolaan akun yang memungkinkan Anda untuk mengkonsolidasikan beberapa Akun AWS menjadi Organisasi yang Anda buat dan kelola secara terpusat. AWS Organizations mencakup pengelolaan akun dan kemampuan tagihan terkonsolidasi yang memungkinkan Anda untuk memenuhi kebutuhan anggaran, keamanan, dan kepatuhan bisnis Anda dengan lebih baik. Sebagai administrator organisasi, Anda dapat membuat akun di organisasi Anda dan mengundang akun yang ada untuk bergabung dengan organisasi.

Panduan pengguna ini mendefinisikan konsep kunci untuk AWS Organizations, memberikan tutorial, dan menjelaskan cara membuat dan mengelola organisasi.

Topik

Fitur AWS Organizations

AWS Organizations menawarkan fitur-fitur berikut:

Pengelolaan terpusat dari semuaAkun AWS

> Anda dapat menggabungkan akun yang ada ke dalam organisasi yang memungkinkan Anda mengelola akun secara terpusat. Anda dapat membuat akun yang secara otomatis menjadi bagian dari organisasi Anda, dan Anda dapat mengundang akun lain untuk bergabung dengan organisasi Anda. Anda juga dapat melampirkan kebijakan yang memengaruhi sebagian atau semua akun Anda.

Tagihan terkonsolidasi untuk semua akun anggota

> Tagihan terkonsolidasi adalah fitur dari AWS Organizations. Anda dapat menggunakan akun pengelolaan organisasi Anda untuk mengkonsolidasikan dan membayar semua akun anggota. Dalam tagihan terkonsolidasi, akun pengelolaan juga dapat mengakses informasi penagihan, informasi akun, dan aktivitas akun anggota di organisasi mereka. Informasi ini dapat digunakan untuk layanan seperti Cost Explorer, yang dapat membantu akun pengelolaan meningkatkan performa biaya organisasi mereka.

Melakukan pengelompokan secara hierarkis atas akun Anda untuk memenuhi kebutuhan anggaran, keamanan, atau kepatuhan

Anda dapat mengelompokkan akun Anda ke unit organisasi (OU) dan melampirkan kebijakan akses yang berbeda untuk setiap OU. Misalnya, jika Anda memiliki akun yang harus mengakses layanan AWS yang memenuhi persyaratan peraturan tertentu, maka Anda dapat memasukkan akun tersebut ke dalam satu OU. Anda kemudian dapat melampirkan kebijakan untuk OU yang memblokir akses ke layanan yang tidak memenuhi persyaratan peraturan tersebut. Anda dapat membuat nest OU Anda di OU lain hingga kedalaman lima tingkat, memberikan fleksibilitas dalam cara Anda menyusun grup akun Anda.

Kebijakan untuk memusatkan kontrol atasAWS layanan dan tindakan API yang dapat diakses oleh setiap akun

Sebagai administrator akun pengelolaan organisasi, Anda dapat menggunakan kebijakan kontrol layanan (SCP) untuk menentukan izin maksimum untuk akun anggota yang ada dalam organisasi. Di SCP, Anda dapat membatasi layanan AWS mana, sumber daya, dan tindakan API individu mana yang dapat diakses pengguna dan peran dalam setiap akun anggota. Anda juga dapat menentukan syarat kapan harus membatasi akses ke layanan AWS, sumber daya, dan tindakan API. Pembatasan ini bahkan akan menimpa administrator akun anggota dalam organisasi. Saat AWS Organizations memblokir akses ke sebuah layanan, sumber daya, atau tindakan API untuk akun anggota, pengguna, atau peran dalam akun tersebut tidak dapat mengaksesnya. Blok ini tetap berlaku bahkan jika administrator akun anggota secara eksplisit memberikan izin tersebut sebuah dalam kebijakan IAM.

Untuk informasi lebih lanjut, lihat Kebijakan Pengendalian Layanan (SCPs).

Kebijakan untuk menstandarisasi tag di seluruh sumber daya di akun organisasi Anda

Anda dapat menggunakan kebijakan tag untuk mempertahankan tag yang konsisten, termasuk penanganan kasus pilihan atas kunci tag dan nilai tag.

Untuk informasi lebih lanjut, lihat Kebijakan tag

Kebijakan untuk mengontrol cara kecerdasanAWS buatan (AI) dan machine learning dapat mengumpulkan dan menyimpan data.

Anda dapat menggunakan kebijakan opt-out layanan AI untuk menolak pengumpulan dan penyimpanan data untuk salah satu layanan AI AWS yang tidak ingin Anda gunakan.

Untuk informasi lebih lanjut, lihat Kebijakan berhenti berlangganan layanan AI

Kebijakan yang mengonfigurasi backup otomatis untuk sumber daya di akun organisasi

Anda dapat menggunakan kebijakan backup untuk mengkonfigurasi dan menerapkan secara otomatis paket AWS Backup ke sumber daya di semua akun organisasi Anda.

Untuk informasi lebih lanjut, lihat Kebijakan Backup

Integrasi dan support untukAWS Identity and Access Management (IAM)

IAM menyediakan kontrol terperinci atas pengguna dan peran dalam akun individual. AWS Organizations memperluas kontrol tersebut ke tingkat akun dengan memberi Anda kontrol atas apa yang dapat dilakukan pengguna dan peran dalam akun atau grup akun. Izin yang dihasilkan adalah persimpangan logis dari apa yang diizinkan oleh AWS Organizations pada tingkat akun dan izin yang secara eksplisit diberikan oleh IAM pada tingkat pengguna atau peran dalam akun tersebut. Dengan kata lain, pengguna hanya dapat mengakses apa yang diizinkan oleh keduanya, yaitu kebijakan AWS Organizations dan kebijakan IAM. Jika salah satunya melakukan blok atas operasi, maka pengguna tidak dapat mengakses operasi tersebut.

Integrasi denganAWS layanan lain

Anda dapat memanfaatkan layanan pengelolaan multi-akun yang tersedia di AWS Organizations dengan pilihan layanan AWS untuk melakukan tugas pada semua akun yang merupakan anggota organisasi. Untuk daftar layanan dan manfaat menggunakan setiap layanan di tingkat organisasi, lihat AWS Layanan yang dapat Anda gunakan dengan AWS Organizations.

Ketika Anda mengaktifkan AWS untuk melakukan tugas atas nama Anda di akun anggota organisasi Anda, AWS Organizations menciptakan Peran yang terhubung dengan layanan IAM untuk layanan tersebut di setiap akun anggota. Peran yang terhubung dengan layanan memiliki izin IAM yang telah ditetapkan sebelumnya yang mengizinkan AWS untuk melakukan tugas tertentu di organisasi Anda dan akunnya. Agar dapat bekerja, semua akun dalam organisasi secara otomatis memiliki Peran tertaut layanan. Peran ini memungkinkan AWS Organizations untuk membuat peran tertaut layanan yang dibutuhkan oleh layanan AWS yang Anda aktifkan akses tepercaya-nya. Peran tertaut layanan tambahan ini dilampirkan ke kebijakan izin IAM yang memungkinkan layanan tertentu untuk melakukan hanya tugas-tugas yang diperlukan oleh pilihan konfigurasi Anda. Untuk informasi lebih lanjut, lihat Menggunakan AWS Organizations dengan layanan AWS lainnya.

Akses global

AWS Organizations adalah layanan global dengan titik akhir tunggal yang bekerja dari setiap dan semua Wilayah AWS. Anda tidak perlu memilih wilayah di mana akan beroperasi.

Replikasi data yang akhirnya konsisten

AWS Organizations, seperti banyak layanan AWS lainnya, akhirnya konsisten. AWS Organizations mencapai ketersediaan tinggi dengan mereplikasi data di beberapa server di pusat data AWS dalam Wilayah-nya. Jika permintaan untuk mengubah beberapa data berhasil, perubahan tersebut akan dilakukan dan disimpan dengan aman. Namun, perubahan kemudian harus direplikasi di beberapa server. Untuk informasi lebih lanjut, lihat Perubahan yang saya buat tidak selalu langsung bisa terlihat.

Gratis untuk digunakan

AWS Organizations adalah fitur dari Akun AWS yang ditawarkan tanpa biaya tambahan. Anda dikenakan biaya hanya ketika Anda mengakses layanan AWS dari akun di organisasi Anda. Untuk informasi tentang harga produk AWS lainnya, lihat Halaman harga Amazon Web Services.

Harga AWS Organizations

AWS Organizations ditawarkan tanpa biaya tambahan. Anda hanya dikenai biaya untuk sumber daya AWS yang digunakan pengguna dan peran dalam akun anggota Anda. Misalnya, Anda dikenakan biaya standar untuk instans Amazon EC2 yang digunakan oleh pengguna atau peran dalam akun anggota Anda. Untuk informasi tentang harga produk AWS lainnya, lihat Harga AWS.

Mengakses AWS Organizations

Anda dapat bekerja dengan AWS Organizations dengan salah satu cara berikut:

AWS Management Console

Konsol AWS Organizations adalah antarmuka berbasis peramban yang dapat Anda gunakan untuk mengelola organisasi dan sumber daya AWS. Anda dapat melakukan tugas apa pun di organisasi Anda dengan menggunakan konsol tersebut.

AWSAlat Baris Perintah

Anda dapat menggunakan alat baris perintah AWS untuk mengeluarkan perintah pada baris perintah sistem Anda untuk melakukan tugas AWS Organizations dan AWS. Dengan menggunakan baris perintah dapat lebih cepat dan lebih nyaman dibandingkan menggunakan konsol tersebut. Alat baris perintah juga berguna jika Anda ingin membangun skrip yang melakukan tugas AWS.

AWS menyediakan dua set alat baris perintah:

- AWS Command Line Interface (AWS CLI). Untuk informasi tentang menginstal dan menggunakan AWS CLI, lihat Panduan Pengguna AWS Command Line Interface.
- AWS Tools for Windows PowerShell. Untuk informasi tentang menginstal dan menggunakan Tools for Windows PowerShell, lihat PanduanAWS Tools for Windows PowerShell Pengguna.

AWSSDK

SDK AWS terdiri atas perpustakaan dan kode sampel untuk berbagai bahasa dan platform pemrograman (misalnya, Java, Python, Ruby, .NET, iOS, dan Android). SDK menangani tugas seperti menandatangani permintaan secara kriptografis, mengelola kesalahan, dan mencoba kembali permintaan secara otomatis. Untuk informasi selengkapnya tentang AWS SDK, termasuk cara mengunduh dan menginstalnya, lihat Alat untuk Amazon Web Services.

AWS OrganizationsAPI Kueri HTTPS

API Kueri HTTPS AWS Organizations memberikan akses program ke AWS Organizations dan AWS. API Kueri HTTPS memungkinkan Anda menerbitkan permintaan HTTPS secara langsung ke layanan. Saat Anda menggunakan HTTPS API, Anda harus menyertakan kode untuk menandatangani permintaan secara digital menggunakan kredensial Anda. Untuk informasi selengkapnya, lihat Memanggil API dengan Membuat Permintaan Kueri HTTP dan Referensi API AWS Organizations.

Support dan umpan balik untuk AWS Organizations

Kami menyambut umpan balik Anda. Anda dapat mengirim komentar ke feedback-awsorganizations@amazon.com. Anda juga dapat mengirimkan masukan dan pertanyaan Anda di forum support AWS Organizations. Untuk informasi selengkapnya tentang Forum Support AWS, lihat Forum Bantuan.

Sumber daya AWS lainnya

- Pelatihan & Kursus AWS – Tautan ke kursus specialty dan berbasis peran serta lab mandiri untuk membantu mempertajam keterampilan AWS Anda dan mendapatkan pengalaman praktis.
- Alat Developer AWS – Tautan ke alat developer dan sumber daya yang menyediakan dokumentasi, sampel kode, catatan rilis, dan informasi lainnya untuk membantu Anda membangun aplikasi inovatif dengan AWS.

- AWS Support Center – Hub untuk membuat dan mengelola kasus AWS Support Anda. Juga mencakup tautan ke sumber daya yang bermanfaat lainnya, seperti forum, Pertanyaan Umum teknis, status kesehatan layanan, dan AWS Trusted Advisor.
- AWSSupport — Halaman web utama untuk informasi tentangAWS Support one-on-one, saluran dukungan jawaban cepat, satu untuk membantu Anda membuat dan menjalankan aplikasi di cloud.
- Kontak Kami – Titik kontak pusat untuk pertanyaan tentang tagihan AWS, akun, peristiwa, penyalahgunaan, dan masalah lainnya.
- Persyaratan Situs AWS – Informasi detail tentang hak cipta dan merek dagang kami; akun, lisensi, dan akses situs Anda; serta topik lainnya.

Memulai dengan AWS Organizations

Topik berikut memberikan informasi untuk membantu Anda mulai belajar dan menggunakan AWS Organizations.

Pelajari tentang ...

[Terminologi dan konsep AWS Organizations]

Pelajari terminologi dan konsep inti yang diperlukan untuk memahami AWS Organizations. Bagian ini menjelaskan masing-masing komponen organisasi dan dasar-dasar bagaimana mereka bekerja sama untuk memberikan tingkat kendali baru atas apa yang bisa dilakukan pengguna di akun tersebut.

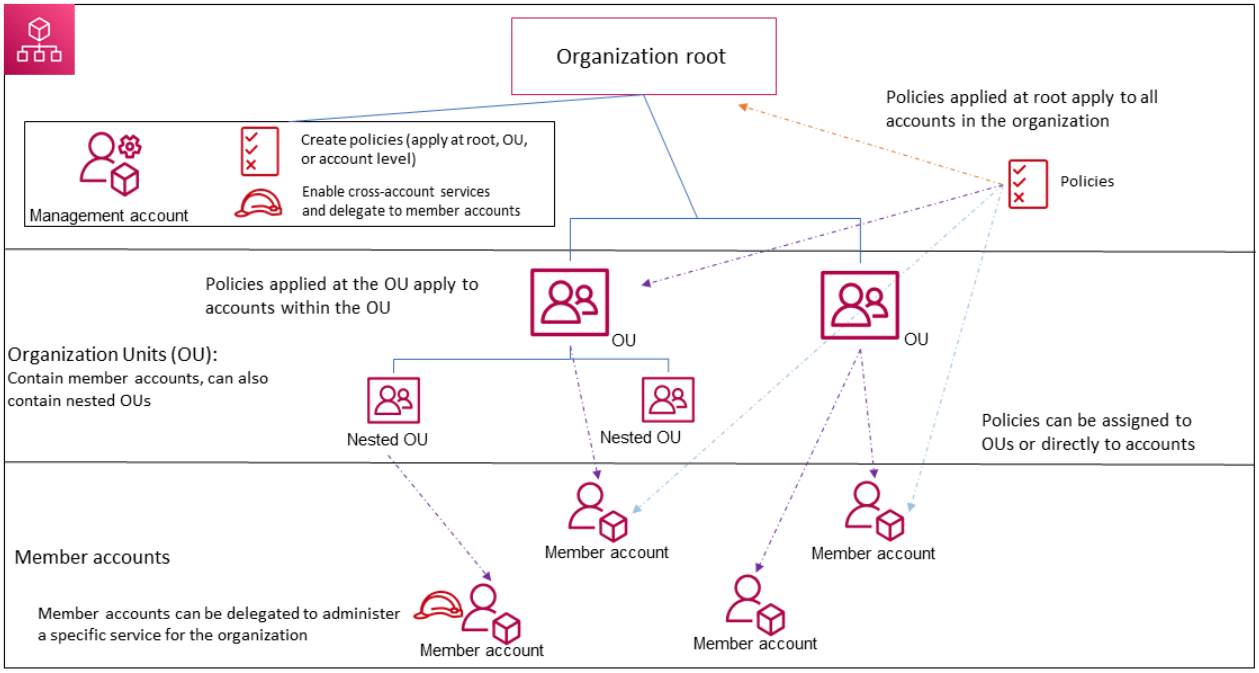
[Tagihan Terkonsolidasi untuk Organizations]

Salah satu fitur utama tentang AWS Organizations adalah konsolidasi penagihan semua akun di organisasi Anda. Pelajari selengkapnya tentang bagaimana penagihan ditangani dalam suatu organisasi dan bagaimana berbagai diskon bekerja ketika dibagi di beberapa akun. Konten ini ada di Panduan Pengguna AWS Billing.

Terminologi dan konsep AWS Organizations

Untuk membantu Anda memulai AWS Organizations, topik ini menjelaskan beberapa konsep utama.

Diagram berikut menunjukkan organisasi dasar yang terdiri dari lima akun yang disusun menjadi empat unit organisasi (oU) di bawah root. Organisasi juga memiliki beberapa kebijakan yang melekat pada beberapa OU atau secara langsung ke akun. Untuk deskripsi masing-masing item ini, lihat definisi dalam topik ini.



Organisasi

Entitas yang Anda buat untuk mengkonsolidasikan AWS akun sehingga Anda dapat mengelola mereka sebagai satu unit. Anda dapat menggunakan konsol AWS Organizations untuk secara terpusat melihat dan mengelola semua akun dalam organisasi Anda. Sebuah organisasi memiliki satu akun manajemen bersama dengan nol atau lebih akun anggota. Anda dapat mengorganisasi akun dalam struktur hierarkis seperti pohon dengan root di bagian atas dan unit-unit organisasi bersarang di bawah root. Setiap akun dapat secara langsung berada di dalam root, atau ditempatkan di salah satu OU dalam hirarki. Sebuah organisasi memiliki fungsi yang ditentukan oleh perangkat fitur yang Anda aktifkan.

root

Kontainer induk untuk semua akun untuk organisasi Anda. Jika Anda menerapkan kebijakan ke root, itu berlaku untuk semua unit organisasi (OU) dan akun di dalam organisasi tersebut.

> **Note**
>
> Saat ini, Anda hanya dapat memiliki satu root. AWS Organizations secara otomatis membuatnya untuk Anda saat membuat sebuah organisasi.

Unit organisasi (OU)

Sebuah kontainer untuk akun di dalam root. OU juga dapat berisi OU lainnya, yang memungkinkan Anda untuk membuat hirarki yang menyerupai pohon terbalik, dengan akar di bagian atas dan cabang OU yang mencapai ke bawah, yang berakhir di akun yang membentuk daun-daun pohon. Ketika Anda menerapkan kebijakan untuk salah satu simpul dalam hirarki, kebijakan itu mengalir ke bawah dan mempengaruhi semua cabang (OU) dan daun (akun) di bawahnya. OU dapat memiliki tepat satu induk, dan saat ini setiap akun dapat menjadi anggota dari satu OU.

Akun

Akun di Organizations adalah Akun AWS standar yang berisi sumber daya AWS dan identitas yang dapat mengakses sumber daya tersebut.

> **Tip**
>
> AWSAkun tidak sama dengan akun pengguna. pengguna AWS adalah identitas yang Anda buat menggunakan AWS Identity and Access Management (IAM) dan mengambil bentuk Pengguna IAM dengan kredensial jangka panjang, atau IAM role dengan kredensial jangka pendek. Akun AWS tunggal dapat, dan biasanya berisi banyak pengguna dan peran.

Ada dua jenis akun dalam suatu organisasi: satu akun yang ditetapkan sebagai akun manajemen, dan satu atau lebih akun anggota.

- akun manajemen adalah akun yang Anda gunakan untuk membuat organisasi. Dari akun manajemen organisasi, Anda dapat melakukan hal-hal sebagai berikut:
  - Buat akun di organisasi
  - Undang akun lain yang ada ke organisasi
  - Hapus akun dari organisasi
  - Tentukan akun administrator yang didelegasikan
  - Kelola undangan
  - Terapkan kebijakan untuk entitas (root, OU, atau akun) dalam organisasi
  - Aktifkan integrasi dengan layanan yang didukung AWS untuk menyediakan fungsionalitas layanan di semua akun di organisasi.

Akun manajemen memiliki tanggung jawab Akun Pembayar dan bertanggung jawab untuk membayar semua biaya yang diperoleh oleh akun anggota. Anda tidak dapat mengubah akun manajemen organisasi.

- Akun anggota merupakan semua akun lainnya dalam sebuah organisasi. Akun dapat menjadi anggota dari hanya satu organisasi pada suatu waktu. Anda dapat melampirkan kebijakan ke akun untuk menerapkan kendali hanya untuk satu akun tersebut.

> **Note**
>
> Anda dapat menunjuk beberapa akun anggota untuk menjadi akun administrator yang didelegasikan. Lihat Administrator yang didelegasikan, di bawah ini.

Administrator yang didelegasikan

Kami menyarankan Anda menggunakan akun manajemen Organisasi dan pengguna serta perannya hanya untuk tugas yang harus dilakukan oleh akun tersebut. Kami menyarankan Anda menyimpan AWS sumber daya Anda di akun anggota lain di organisasi dan menjauhkannya dari akun manajemen. Ini karena fitur keamanan seperti Kebijakan kontrol layanan Organisasi (SCP) tidak membatasi pengguna atau peran apa pun dalam akun manajemen. Memisahkan sumber daya Anda dari akun manajemen Anda juga dapat membantu Anda memahami biaya pada faktur Anda. Dari akun manajemen organisasi, Anda dapat menunjuk satu atau beberapa akun anggota sebagai akun administrator yang didelegasikan untuk membantu Anda menerapkan rekomendasi ini. Ada dua jenis administrator yang didelegasikan:

- Administrator yang didelegasikan untuk Organisasi: Dari akun ini, Anda dapat mengelola kebijakan organisasi dan melampirkan kebijakan ke entitas (root, OU, atau akun) dalam organisasi. Akun manajemen dapat mengontrol izin delegasi pada tingkat granular. Lihat Administrator yang didelegasikan untuk AWS Organizations untuk informasi selengkapnya.
- Administrator yang didelegasikan untuk suatu AWS layanan: Dari akun ini, Anda dapat mengelola AWS layanan yang terintegrasi dengan Organisasi. Akun manajemen dapat mendaftarkan akun anggota yang berbeda sebagai administrator yang didelegasikan untuk layanan yang berbeda sesuai kebutuhan. Akun ini memiliki izin administratif untuk layanan tertentu, serta izin untuk tindakan hanya-baca Organisasi. Lihat Administrator yang didelegasikan untuk AWS layanan yang bekerja dengan Organisasi untuk informasi selengkapnya.

Undangan

Proses meminta akun yang lain untuk bergabung dengan organisasi Anda. Undangan hanya dapat dikeluarkan oleh akun manajemen organisasi. Undangan diperluas hingga ID akun atau alamat email yang terkait dengan akun yang diundang. Setelah akun yang diundang menerima undangan, akun tersebut menjadi sebuah akun anggota dalam organisasi. Undangan juga dapat dikirim ke semua akun anggota saat ini ketika organisasi membutuhkan semua anggota untuk menyetujui perubahan dari hanya mendukung fitur penagihan konsolidasi menjadi mendukung semua fitur dalam organisasi. Undangan bekerja berdasarkan akun yang bertukar jabat tangan. Anda mungkin tidak melihat jabat tangan saat bekerja di konsol AWS Organizations. Tetapi jika Anda menggunakan API AWS CLI atau AWS Organizations, Anda harus bekerja langsung dengan jabat tangan.

Jabat Tangan

Sebuah proses multi-langkah pertukaran informasi antara dua pihak. Salah satu kegunaan utamanya dalam AWS Organizations adalah untuk melayani sebagai implementasi yang mendasari untuk undangan. Pesan jabat tangan dilewatkan antara dan ditanggapi oleh inisiator dan penerima jabat tangan. Pesan dilewatkan dengan cara yang membantu memastikan bahwa kedua belah pihak tahu apa status saat ini. Jabat tangan juga digunakan ketika mengubah organisasi dari yang hanya mendukung fitur penagihan konsolidasi menjadi mendukung semua fitur yang ditawarkan oleh AWS Organizations. Anda biasanya perlu berinteraksi langsung dengan jabat tangan hanya jika Anda bekerja dengan API AWS Organizations atau alat baris perintah seperti AWS CLI.

Perangkat fitur yang tersedia

- Semua fitur — Perangkat fitur default yang tersedia untuk AWS Organizations. Ini mencakup semua fungsi penagihan terkonsolidasi, serta fitur canggih yang memberi Anda kendali lebih besar atas akun di organisasi Anda. Misalnya, bila semua fitur diaktifkan, akun manajemen organisasi memiliki kendali penuh atas apa yang dapat dilakukan akun anggota. Akun manajemen dapat menerapkan SCP untuk membatasi layanan dan tindakan yang pengguna (termasuk pengguna root) dan peran dalam akun dapat mengakses. Akun manajemen juga dapat mencegah akun anggota meninggalkan organisasi. Anda juga dapat mengaktifkan integrasi dengan AWS layanan yang didukung agar layanan tersebut menyediakan fungsionalitas di semua akun di organisasi Anda.

  Anda dapat membuat organisasi dengan semua fitur yang telah diaktifkan, atau Anda dapat mengaktifkan semua fitur dalam organisasi yang awalnya hanya mendukung fitur penagihan

terkonsolidasi. Untuk mengaktifkan semua fitur, semua akun anggota diundang harus menyetujui perubahan dengan menerima undangan yang dikirim ketika akun manajemen mulai proses.

- Penagihan gabungan - Kumpulan fitur ini menyediakan fungsionalitas penagihan bersama, tetapi tidak menyertakan fitur yang lebih canggih. AWS Organizations Misalnya, Anda tidak dapat mengaktifkan AWS layanan lain untuk berintegrasi dengan organisasi agar dapat bekerja di semua akunnya, atau menggunakan kebijakan untuk membatasi apa yang dapat dilakukan pengguna dan peran di akun yang berbeda. Untuk menggunakan fitur AWS Organizations, Anda harus mengaktifkan semua fitur di organisasi Anda.

Kebijakan kontrol layanan (SCP)

Kebijakan yang menentukan layanan dan tindakan yang dapat digunakan oleh pengguna dan peran dalam akun yang SCP pengaruhi. SCP mirip dengan kebijakan izin IAM kecuali bahwa mereka tidak memberikan izin apa pun. Sebaliknya, SCP menentukan izin maksimum untuk sebuah organization, unit organisasi (OU), atau akun. Ketika Anda melampirkan SCP ke root organisasi Anda atau OU, SCP membatasi izin untuk entitas dalam akun anggota.

Izinkan daftar vs tolak daftar

Izinkan daftar dan tolak daftar adalah strategi pelengkap yang dapat Anda gunakan untuk menerapkan SCP untuk mem-filter izin yang tersedia untuk akun.

- Strategi izinkan daftar — Anda secara eksplisit menentukan akses yang diizinkan. Semua akses lainnya secara implisit diblokir. Secara default, AWS Organizations melampirkan sebuah kebijakan terkelola AWS yang disebut `FullAWSAccess` ke semua root, OU, dan akun. Hal ini membantu memastikan bahwa, ketika Anda membangun organisasi Anda, tidak ada yang diblokir sampai Anda menginginkannya diblokir. Dengan kata lain, secara default semua izin dizinkan. Saat Anda siap untuk membatasi izin, Anda mengganti kebijakan `FullAWSAccess` dengan sebuah kebijakan yang memungkinkan hanya perangkat izin yang lebih terbatas dan diinginkan. Pengguna dan peran dalam akun yang terpengaruh kemudian dapat menjalankan hanya tingkat akses tersebut, meskipun kebijakan IAM mereka mengizinkan semua tindakan. Jika Anda mengganti kebijakan default pada root, semua akun dalam organisasi dipengaruhi oleh pembatasan tersebut. Anda tidak dapat menambahkan izin kembali pada tingkat yang lebih rendah dalam hirarki karena SCP tidak pernah memberikan izin; SCP hanya menyaring izin-izin tersebut.
-

Strategi daftar tolak — Anda secara eksplisit menentukan akses yang tidak diizinkan. Semua akses lainnya diizinkan. Dalam skenario ini, semua izin diizinkan kecuali secara eksplisit diblokir. Ini adalah perilaku default AWS Organizations. Secara default, AWS Organizations melampirkan sebuah kebijakan terkelola AWS yang disebut `FullAWSAccess` ke semua root, OU, dan akun. Hal ini memungkinkan setiap akun untuk mengakses layanan atau operasi tanpa pembatasan yang diberlakukan oleh AWS Organizations. Berbeda dengan teknik izinkan daftar yang dijelaskan di atas, ketika menggunakan tolak daftar, Anda meninggalkan kebijakan `FullAWSAccess` default di tempat (yang mengizinkan "semua"). Tapi kemudian Anda melampirkan kebijakan tambahan yang secara eksplisit menolak akses ke layanan dan tindakan yang tidak diinginkan. Sama seperti dengan kebijakan izin IAM, sebuah penolakan eksplisit terhadap tindakan layanan menimpa setiap pemberian izin terhadap tindakan itu.

Kebijakan penolakan layanan Kecerdasan Buatan (AI)

Jenis kebijakan yang membantu Anda menstandardisasi pengaturan penolakan untuk Layanan AI AWS di semua akun di organisasi Anda. Layanan AI AWS tertentu dapat menyimpan dan menggunakan konten pelanggan yang diproses oleh layanan tersebut untuk pengembangan dan perbaikan terus menerus dari layanan Amazon AI dan teknologi. Sebagai pelanggan AWS, Anda dapat menggunakan Kebijakan penolakan layanan AI untuk memilih agar konten Anda tidak disimpan atau digunakan untuk peningkatan layanan.

Kebijakan Backup

Jenis kebijakan yang membantu Anda melakukan standarisasi dan menerapkan strategi cadangan untuk sumber daya di semua akun di organisasi Anda. Dalam Kebijakan backup, Anda dapat mengkonfigurasi dan menyebarkan rencana cadangan untuk sumber daya Anda.

Kebijakan tag

Jenis kebijakan yang membantu Anda melakukan standardisasi tag di seluruh sumber daya di semua akun di organisasi Anda. Dalam kebijakan tag, Anda dapat menentukan aturan pemberian tag untuk sumber daya tertentu.

Tutorial AWS Organizations

Gunakan tutorial di bagian ini untuk mempelajari cara melakukan tugas menggunakan AWS Organizations.

Tutorial: Membuat dan mengonfigurasi organisasi

Bangun dan jalankan step-by-step instruksi untuk membuat organisasi Anda, mengundang akun anggota pertama Anda, membuat hierarki OU yang berisi akun Anda, dan menerapkan beberapa kebijakan kontrol layanan (SCP).

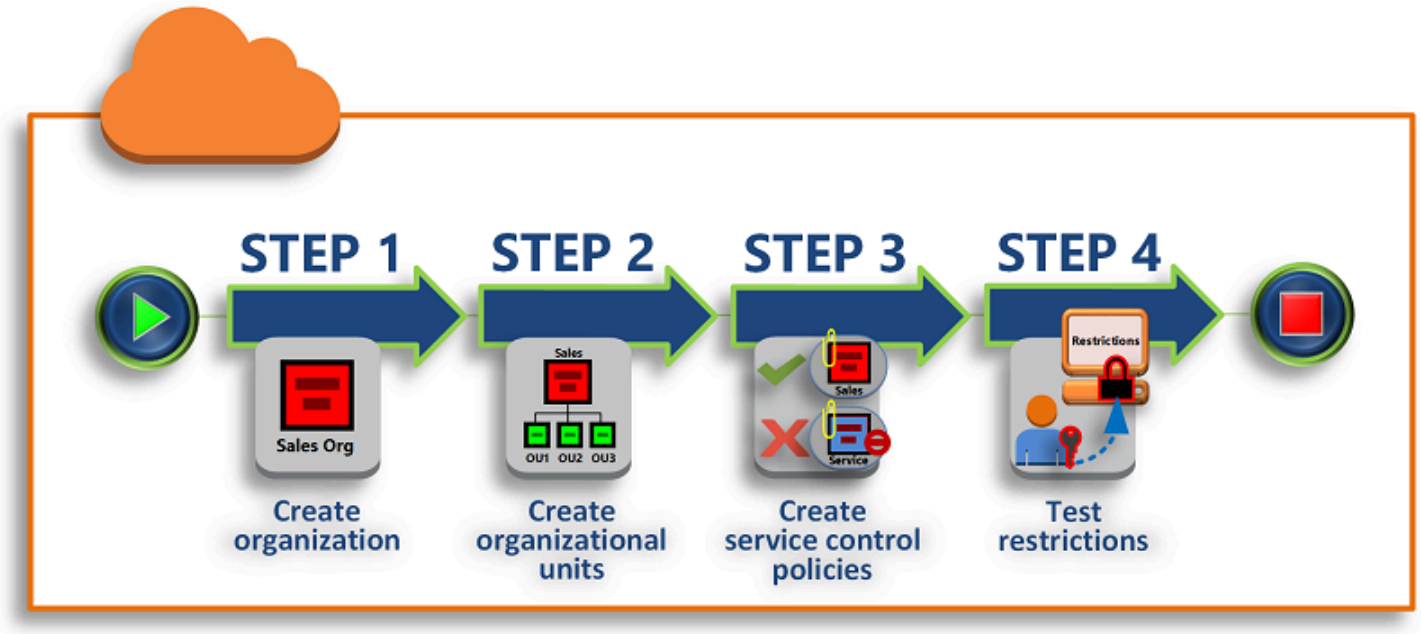
Tutorial: Pantau perubahan penting pada organisasi Anda dengan Amazon EventBridge

Pantau perubahan utama di organisasi Anda dengan mengonfigurasi Amazon EventBridge untuk memicu alarm dalam bentuk email, pesan teks SMS, atau entri log saat tindakan yang Anda tentukan terjadi di organisasi Anda. Misalnya, banyak organisasi ingin tahu kapan akun baru dibuat atau kapan akun mencoba meninggalkan organisasi.

Tutorial: Membuat dan mengonfigurasi organisasi

Dalam tutorial ini, Anda akan membuat organisasi Anda dan mengonfigurasinya dengan dua akun anggota AWS. Anda membuat salah satu akun anggota di organisasi Anda, dan Anda mengundang akun lain untuk bergabung dengan organisasi Anda. Selanjutnya, Anda menggunakan teknik daftar izinkan untuk menentukan bahwa administrator akun hanya dapat mendelegasikan layanan dan tindakan yang terdaftar secara eksplisit. Hal ini memungkinkan administrator untuk memvalidasi layanan baru yang diperkenalkan AWS sebelum mereka mengizinkan penggunaannya oleh orang lain di perusahaan Anda. Dengan cara itu, jika AWS memperkenalkan layanan baru, ia tetap dilarang sampai administrator menambahkan layanan tersebut ke daftar diizinkan dalam kebijakan yang sesuai. Tutorial ini juga menunjukkan cara menggunakan daftar penolakan untuk memastikan bahwa tidak ada pengguna di akun anggota yang dapat mengubah konfigurasi untuk log audit yang AWS CloudTrail dibuat.

Ilustrasi berikut menunjukkan langkah-langkah utama dari tutorial tersebut.



Langkah 1: Buat organisasi Anda

Pada langkah ini, Anda akan membuat organisasi dengan Akun AWS Anda sebagai akun pengelolaan. Anda juga mengundang satu Akun AWS untuk bergabung dengan organisasi Anda, dan Anda membuat akun kedua sebagai akun anggota.

Langkah 2: Buat unit organisasi

Selanjutnya, Anda membuat dua unit organisasi (OU) di organisasi baru Anda dan menempatkan akun anggota di OU tersebut.

Langkah 3: Buat kebijakan kontrol layanan

Anda dapat menerapkan pembatasan pada tindakan apa saja yang dapat didelegasikan kepada pengguna dan peran dalam akun anggota dengan menggunakan kebijakan kontrol layanan (SCP). Pada langkah ini, Anda membuat dua SCP dan melampirkannya ke OU yang ada di organisasi Anda.

Langkah 4: Menguji kebijakan organisasi Anda

Anda dapat masuk sebagai pengguna dari masing-masing akun pengujian dan melihat efek yang diberikan SCP pada akun tersebut.

Tak satu pun dari langkah-langkah yang ada dalam tutorial ini menimbulkan biaya ke tagihan AWS Anda. AWS Organizations adalah layanan gratis.

Prasyarat

Tutorial ini mengasumsikan bahwa Anda memiliki akses ke kedua Akun AWS yang ada (Anda membuat akun yang ketiga sebagai bagian dari tutorial ini) dan bahwa Anda dapat masuk ke masing-masing akun sebagai administrator.

Tutorial ini mengacu pada akun sebagai berikut:

- `111111111111` — Akun yang Anda gunakan untuk membuat organisasi. Akun ini menjadi akun pengelolaan. Pemilik akun ini memiliki alamat email `OrgAccount111@example.com`.
- `222222222222` — Akun yang Anda undang untuk bergabung dengan organisasi sebagai akun anggota. Pemilik akun ini memiliki alamat email `member222@example.com`.
- `333333333333` — Akun yang Anda buat sebagai anggota organisasi. Pemilik akun ini memiliki alamat email `member333@example.com`.

Ganti nilai di atas dengan nilai-nilai yang terkait dengan akun pengujian Anda. Kami merekomendasikan agar Anda tidak menggunakan akun produksi untuk tutorial ini.

Langkah 1: Buat organisasi Anda

Pada langkah ini, Anda masuk ke akun 111111111111 sebagai administrator, membuat organisasi dengan akun tersebut sebagai akun pengelolaan, dan mengundang akun yang ada, 222222222222, untuk bergabung sebagai akun anggota.

AWS Management Console

1. Masuk ke AWS sebagai administrator dari akun 111111111111 dan buka konsol AWS Organizations.
2. Pada halaman pengenalan, pilih Membuat organisasi.
3. Di kotak dialog konfirmasi, pilih Membuat organisasi.

> **Note**
>
> Secara default, organisasi dibuat dengan semua fitur diaktifkan. Anda juga dapat membuat organisasi dengan hanya Fitur tagihan terkonsolidasi yang diaktifkan.

AWS membuat organisasi dan menunjukkan halaman Akun AWS kepada Anda. Jika Anda berada di halaman yang berbeda, pilih Akun AWS di panel navigasi yang ada di sebelah kiri.

Jika akun yang Anda gunakan tidak pernah memverifikasi alamat emailnya dengan AWS, maka sebuah email verifikasi akan secara otomatis dikirim ke alamat yang terkait dengan akun pengelolaan Anda. Mungkin ada waktu tunda sebelum Anda menerima email verifikasi.

4. Verifikasi alamat email Anda dalam waktu 24 jam. Untuk informasi lebih lanjut, lihat Verifikasi alamat email.

Sekarang Anda memiliki organisasi dengan akun Anda sebagai satu-satunya anggota. Ini adalah akun pengelolaan organisasi.

Undang akun yang ada untuk bergabung dengan organisasi Anda

Setelah Anda memiliki organisasi, Anda dapat mulai mengisinya dengan akun. Pada langkah-langkah di bagian ini, Anda mengundang akun yang ada untuk bergabung sebagai anggota organisasi Anda.

AWS Management Console

Untuk mengundang akun yang sudah ada untuk bergabung

1. Arahkan ke halaman Akun AWS, dan pilih Tambahkan Akun AWS.
2. Pada Tambahkan Akun AWS halaman, pilih Undang yang sudah ada Akun AWS.
3. Di dalam kotak Alamat email atau ID akun dari Akun AWS untuk mengundang, masukkan alamat email pemilik akun yang ingin Anda undang, mirip dengan berikut ini: **`member222@example.com`**. Atau, jika Anda tahu Nomor ID dari Akun AWS tersebut, maka Anda dapat memasukkannya sebagai gantinya.
4. Ketik teks yang Anda inginkan ke dalam kotak Pesan yang akan disertakan dalam pesan email undangan. Teks ini disertakan dalam email yang dikirim ke pemilik akun.
5. Pilih Kirim undangan. AWS Organizations akan mengirimkan undangan ke pemilik akun.

> **Important**
>
> Perluas pesan kesalahan jika ditunjukkan. Jika kesalahan menunjukkan bahwa Anda melebihi batas akun untuk organisasi atau bahwa Anda tidak dapat menambahkan akun karena organisasi Anda masih melakukan inisialisasi, tunggu hingga satu jam

setelah Anda membuat organisasi dan coba lagi. Jika kesalahan tetap ada, kontak AWS Support.

6. Untuk tujuan tutorial ini, Anda sekarang harus menerima undangan Anda sendiri. Lakukan salah satu langkah berikut untuk membuka halaman Undangan di konsol:

   - Buka email yang dikirim oleh AWS dari akun manajemen dan pilih tautan untuk menerima undangan. Saat diminta untuk masuk, lakukan sebagai administrator di akun anggota yang diundang.
   - Buka konsol AWS Organizations dan arahkan ke halaman Undangan.

7. Pada halaman Akun AWS, pilih Terima lalu pilih Konfirmasi.

   > **Tip**
   >
   > Tanda terima undangan dapat ditunda dan Anda mungkin harus menunggu sebelum dapat menerima undangan.

8. Keluar dari akun anggota Anda dan masuk lagi sebagai administrator di akun pengelolaan Anda.

Buat sebuah akun anggota

Di langkah-langkah yang pada bagian ini, Anda akan membuat sebuah Akun AWS yang secara otomatis menjadi anggota organisasi. Kami menyebut akun ini di tutorial sebagai 333333333333.

AWS Management Console

Untuk membuat akun anggota

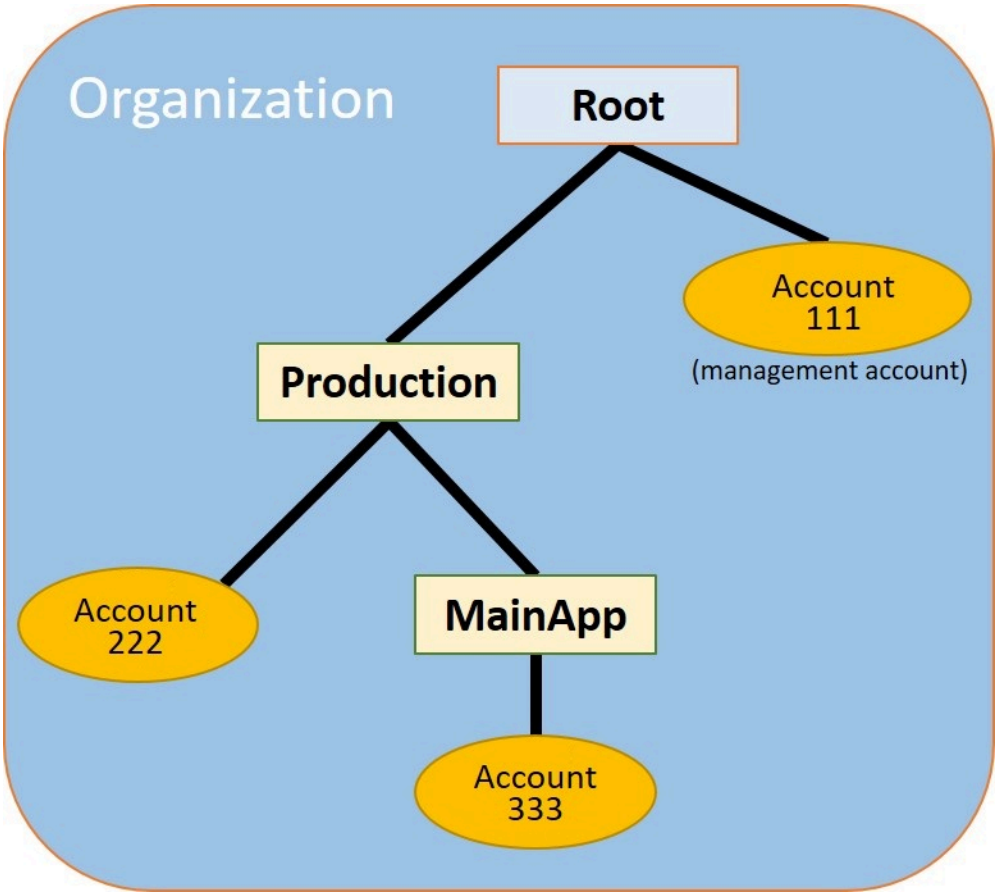
1. Pada konsol AWS Organizations, pada halaman Akun AWS, pilih Tambahkan Akun AWS.
2. Pada halaman Tambahkan Akun AWS, pilih Buat Akun AWS.
3. Untuk nama Akun AWS, masukkan nama untuk akun, seperti **`MainApp Account`**.
4. Untuk Alamat email pengguna root akun, masukkan alamat email individu yang menerima komunikasi atas nama akun. Nilai ini harus unik secara global. Tidak ada dua akun yang dapat memiliki alamat email yang sama. Misalnya, Anda dapat menggunakan sesuatu seperti **`mainapp@example.com`**.

5. Untuk Nama IAM role, Anda dapat membiarkan ini kosong untuk secara otomatis menggunakan nama peran default `OrganizationAccountAccessRole`, atau Anda dapat memberikan nama Anda sendiri. Peran ini memungkinkan Anda mengakses akun anggota baru saat masuk sebagai pengguna IAM di akun pengelolaan. Untuk tutorial ini, biarkan kosong untuk menginstruksikan AWS Organizations membuat peran dengan nama default.
6. Pilih Buat Akun AWS. Anda mungkin perlu menunggu sebentar dan menyegarkan halaman untuk melihat akun baru muncul di halaman Akun AWS.

> **Important**
>
> Jika Anda mengalami kesalahan yang menunjukkan bahwa Anda melampaui batas akun untuk organisasi atau tidak dapat menambahkan akun karena organisasi Anda masih menginisialisasi, tunggu hingga satu jam setelah Anda membuat organisasi dan coba lagi. Jika kesalahan tetap ada, kontak AWS Support.

Langkah 2: Buat unit organisasi

Pada langkah-langkah di bagian ini, Anda akan membuat unit organisasi (OU) dan menempatkan akun anggota Anda di dalamnya. Setelah selesai, hirarki Anda akan terlihat seperti ilustrasi berikut. Akun pengelolaan tetap ada di root. Satu akun anggota dipindahkan ke OU Produksi, dan akun anggota lainnya dipindahkan ke MainApp OU, yang merupakan anak dari Produksi.



AWS Management Console

Untuk membuat dan mengisi OU

> **Note**
>
> Pada langkah-langkah berikut, Anda berinteraksi dengan objek yang dapat Anda pilih pada nama dari objek itu sendiri, atau tombol radio yang ada di sebelah objek.
>
> - Jika Anda memilih nama objek, maka Anda membuka halaman baru yang menampilkan detail objek.
> - Jika Anda memilih tombol radio di sebelah objek, Anda sedang mengidentifikasi objek yang akan ditindaklanjuti oleh tindakan lain, seperti memilih opsi menu.
>
> Langkah-langkah berikutnya, karena Anda memilih tombol radio, maka Anda kemudian dapat bertindak pada objek yang terkait dengan memilih pada menu.

1. Pada konsol AWS Organizations navigasikan ke halaman Akun AWS.
2. Pilih kotak centang
   
   yang ada di sebelah kontainer Root.
3. Pada tab Anak-anak, pilih Tindakan, dan kemudian di bawah Unit organisasi, Pilih Buat baru.
4. Pada halaman Buat unit organisasi di Root, untuk Nama unit organisasi, masukkan **`Production`** lalu pilih Buat unit organisasi.
5. Pilih kotak centang
   
   yang ada di sebelah OU Produksi.
6. Pilih Tindakan, dan kemudian di bawah Unit organisasi, pilih Buat baru.
7. Pada halaman Buat unit organisasi dalam Produksi, untuk nama OU kedua, masukkan **`MainApp`** lalu pilih Buat unit organisasi.

   Sekarang Anda dapat memindahkan akun anggota Anda ke OU ini.
8. Kembali ke halaman Akun AWS, dan kemudian perluas pohon di bawah OU Produksi Anda dengan memilih segitiga
   
   yang ada di sebelahnya. Ini menampilkan MainAppOU sebagai anak Produksi.
9. Di samping 33333333333333, pilih kotak centang
   
   (bukan namanya), pilih Tindakan, dan kemudian di bawah, pilih Pindahkan. Akun AWS
10. Pada halaman Pindah Akun AWS '333333333333', pilih segitiga di sebelah Produksi untuk memperluasnya. Di samping MainApp, pilih tombol radio
    
    (bukan namanya), lalu pilih Pindahkan Akun AWS.
11. Di samping 22222222222222, pilih kotak centang
    
    (bukan namanya), pilih Tindakan, dan kemudian di bawah, pilih Pindahkan. Akun AWS
12. Pada halaman Pindah Akun AWS '222222222222', di sebelah Produksi, pilih tombol radio (bukan namanya), lalu pilih Pindahkan. Akun AWS

Langkah 3: Buat kebijakan kontrol layanan

Pada langkah-langkah di bagian ini, Anda akan membuat tiga kebijakan kontrol layanan (SCP) dan melampirkannya ke root dan ke OU untuk membatasi apa yang dapat dilakukan pengguna di akun organisasi. SCP pertama mencegah siapa pun di salah satu akun anggota dari membuat atau memodifikasi log AWS CloudTrail yang Anda konfigurasi. Akun manajemen tidak terpengaruh oleh SCP apa pun, jadi setelah Anda menerapkan CloudTrail SCP, Anda harus membuat log apa pun dari akun manajemen.

Mengaktifkan jenis kebijakan kontrol layanan untuk organisasi

Sebelum Anda dapat melampirkan kebijakan jenis apa pun ke root atau OU apa pun dalam root, Anda harus mengaktifkan jenis kebijakan untuk organisasi. Jenis kebijakan tidak diaktifkan secara default. Langkah-langkah di bagian ini menunjukkan cara mengaktifkan jenis kebijakan kontrol layanan (SCP) untuk organisasi Anda.

AWS Management Console

Untuk mengaktifkan SCP untuk organisasi Anda

1. Arahkan ke halaman Kebijakan, lalu pilih Kebijakan kontrol layanan.
2. Pada halaman Kebijakan kontrol layanan, pilih Mengaktifkan kebijakan kontrol layanan.

   Banner hijau akan muncul untuk memberi tahu Anda bahwa kini Anda dapat membuat SCP di organisasi Anda.

Buat SCP Anda

Sekarang kebijakan kontrol layanan sudah diaktifkan di organisasi Anda, Anda dapat membuat tiga kebijakan yang Anda butuhkan untuk tutorial ini.

AWS Management Console

Untuk membuat SCP pertama yang memblokir tindakan CloudTrail konfigurasi

1. Arahkan ke halaman Kebijakan, lalu pilih Kebijakan kontrol layanan.
2. Pada halaman Kebijakan kontrol layanan, pilih Buat kebijakan.
3. Untuk Nama kebijakan, masukkan **`Block CloudTrail Configuration Actions`**.

4. Di bagian Kebijakan, dalam daftar layanan di sebelah kanan, pilih CloudTrail untuk layanan. Kemudian pilih tindakan berikut: AddTags, CreateTrail, DeleteTrail, RemoveTags, StartLogging, StopLogging, dan UpdateTrail.
5. Masih di panel kanan, pilih Tambahkan sumber daya dan tentukan CloudTraildan Semua Sumber Daya. Kemudian pilih Tambah sumber daya.

   Pernyataan kebijakan di sebelah kiri harus terlihat mirip dengan yang berikut ini.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1234567890123",
            "Effect": "Deny",
            "Action": [
                "cloudtrail:AddTags",
                "cloudtrail:CreateTrail",
                "cloudtrail:DeleteTrail",
                "cloudtrail:RemoveTags",
                "cloudtrail:StartLogging",
                "cloudtrail:StopLogging",
                "cloudtrail:UpdateTrail"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

6. Pilih Buat kebijakan.

Kebijakan kedua mendefinisikan daftar diizinkan dari semua layanan dan tindakan yang Anda ingin aktifkan untuk pengguna dan peran dalam OU Produksi. Setelah selesai, pengguna yang ada di OU Produksi dapat mengakses layanan dan tindakan yang tercantum saja.

AWS Management Console

Untuk membuat kebijakan kedua yang memungkinkan layanan yang disetujui untuk OU Produksi

1. Dari halaman Kebijakan kontrol layanan, pilih Buat kebijakan.

2. Untuk Nama kebijakan, masukkan **`Allow List for All Approved Services`**.
3. Posisikan kursor Anda pada panel sebelah kanan bagian Kebijakan dan tempelkan dalam kebijakan seperti berikut ini.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt1111111111111",
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "elasticloadbalancing:*",
                "codecommit:*",
                "cloudtrail:*",
                "codedeploy:*"
              ],
            "Resource": [ "*" ]
        }
    ]
}
```

4. Pilih Buat kebijakan.

Kebijakan akhir memberikan daftar penolakan layanan yang diblokir dari penggunaan di MainApp OU. Untuk tutorial ini, Anda memblokir akses ke Amazon DynamoDB di akun apa pun yang ada di OU. MainApp

AWS Management Console

Untuk membuat kebijakan ketiga yang menolak akses ke layanan yang tidak dapat digunakan di OU MainApp

1. Dari halaman Kebijakan kontrol layanan, pilih Buat kebijakan.
2. Untuk Nama kebijakan, masukkan **`Deny List for MainApp Prohibited Services`**.
3. Di bagian Kebijakan yang ada di sebelah kiri, pilih Amazon DynamoDB untuk layanan. Untuk tindakan, pilih Semua tindakan.
4. Masih di panel sebelah kiri, pilih Tambah sumber daya dan tentukan DynamoDB dan Semua sumber daya. Kemudian pilih Tambah sumber daya.

Pernyataan kebijakan yang ada di sebelah kanan melakukan pembaruan sehingga terlihat mirip dengan berikut ini.

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

5. Pilih Buat kebijakan untuk menyimpan SCP.

Tempel SCP untuk OU Anda

Sekarang karena SCP sudah ada dan diaktifkan untuk root Anda, maka Anda dapat melampirkannya ke root dan OU.

AWS Management Console

Untuk melampirkan kebijakan ke root dan OU

1. Arahkan ke halaman Akun AWS.
2. Pada halaman Akun AWS, pilih Root (namanya, bukan tombol radio) untuk menavigasi ke halaman detailnya.
3. Pada halaman detail Root, pilih tab Kebijakan, dan kemudian di bawah Kebijakan Kontrol Layanan, pilih Lampirkan.
4. Pada halaman Melampirkan kebijakan kontrol layanan, pilih tombol radio yang ada di samping SCP bernama `Block CloudTrail Configuration Actions`, lalu pilih Lampirkan. Dalam tutorial ini, Anda melampirkannya ke root sehingga memengaruhi semua akun anggota untuk mencegah siapa pun mengubah cara Anda mengonfigurasi CloudTrail.

   Halaman detail Root, tab Kebijakan sekarang menunjukkan bahwa dua SCP dilampirkan ke root: yang baru saja Anda lampirkan dan SCP `FullAWSAccess` default.

5. Navigasikan kembali ke Akun AWS, dan pilih OU Produksi (namanya, bukan tombol radio) untuk menavigasi ke halaman detailnya.
6. Pada halaman detail OU Produksi, pilih tab Kebijakan.
7. Di bawah Kebijakan Kontrol Layanan, pilih Lampirkan.
8. Pada halaman Melampirkan kebijakan kontrol layanan, pilih tombol radio yang ada di samping `Allow List for All Approved Services`, lalu pilih Lampirkan. Hal ini memungkinkan pengguna atau peran yang ada dalam akun anggota di OU Produksi untuk mengakses layanan yang disetujui.
9. Pilih tab Kebijakan lagi untuk melihat apakah dua SCP terlampir pada OU: satu yang Anda baru saja lampirkan dan SCP `FullAWSAccess` default. Namun, karena SCP `FullAWSAccess` juga sebuah daftar diizinkan yang memungkinkan semua layanan dan tindakan, maka Anda sekarang harus melepaskan SCP ini untuk memastikan bahwa hanya layanan yang disetujui yang diperbolehkan.
10. Untuk menghapus kebijakan default dari OU Produksi, pilih tombol radio untuk Penuh AWSAccess, pilih Lepaskan, lalu pada kotak dialog konfirmasi, pilih Lepaskan kebijakan.

    Setelah Anda menghapus kebijakan default ini, semua akun anggota di bawah OU Produksi akan segera kehilangan akses ke semua tindakan dan layanan yang tidak ada pada daftar diizinkan SCP yang Anda lampirkan di langkah-langkah sebelumnya. Setiap permintaan untuk menggunakan tindakan yang tidak disertakan dalam Daftar Diizinkan untuk Semua Layanan Disetujui SCP akan ditolak. Hal ini berlaku bahkan jika administrator di akun memberikan akses ke layanan lain dengan melampirkan kebijakan izin IAM untuk pengguna di salah satu akun anggota.
11. Sekarang Anda dapat melampirkan SCP bernama `Deny List for MainApp Prohibited services` untuk mencegah siapa pun di akun di MainApp OU menggunakan salah satu layanan terbatas.

    Untuk melakukan ini, navigasikan ke Akun AWShalaman, pilih ikon segitiga untuk memperluas cabang Produksi OU, dan kemudian pilih MainAppOU (namanya, bukan tombol radio) untuk menavigasi ke isinya.
12. Pada halaman MainAppdetail, pilih tab Kebijakan.
13. Di bawah Kebijakan Kontrol Layanan, pilih Lampirkan, lalu dalam daftar kebijakan yang tersedia, pilih tombol radio di samping Tolak Daftar untuk Layanan MainApp Terlarang, lalu pilih Lampirkan kebijakan.

Langkah 4: Menguji kebijakan organisasi Anda

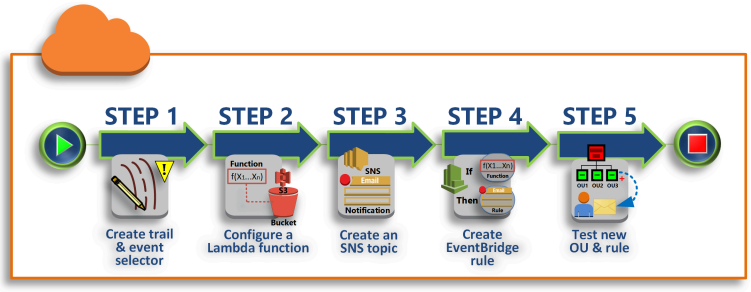
Anda sekarang dapat masuk sebagai pengguna di salah satu akun anggota dan mencoba melakukan berbagai AWS tindakan:

- Jika Anda masuk sebagai pengguna di akun pengelolaan, maka Anda dapat melakukan operasi apa pun yang diizinkan oleh kebijakan izin IAM Anda. SCP tidak mempengaruhi setiap pengguna atau peran dalam akun pengelolaan, terlepas dari root atau OU di mana akun itu berada.
- Jika Anda masuk sebagai pengguna di akun 22222222222222, Anda dapat melakukan tindakan apa pun yang diizinkan oleh daftar izinkan. AWS Organizationsmenolak upaya apa pun untuk melakukan tindakan di layanan apa pun yang tidak ada dalam daftar izin. Juga, AWS Organizations menyangkal setiap upaya untuk melakukan salah satu tindakan CloudTrail konfigurasi.
- Jika Anda masuk sebagai pengguna di akun 333333333333, maka Anda dapat melakukan tindakan apa pun yang diizinkan oleh daftar diizinkan dan tidak diblokir oleh daftar ditolak. AWS Organizations menolak setiap upaya untuk melakukan tindakan yang tidak ada dalam kebijakan daftar diizinkan dan tindakan apa pun yang ada dalam kebijakan daftar ditolak. Juga, AWS Organizations menyangkal setiap upaya untuk melakukan salah satu tindakan CloudTrail konfigurasi.

Tutorial: Pantau perubahan penting pada organisasi Anda dengan Amazon EventBridge

Tutorial ini menunjukkan cara mengkonfigurasi Amazon EventBridge, sebelumnya Amazon CloudWatch Events, untuk memantau organisasi Anda untuk perubahan. Anda mulai dengan mengonfigurasi aturan yang dipicu ketika pengguna mengaktifkan operasi AWS Organizations tertentu. Selanjutnya, Anda mengonfigurasi Amazon EventBridge untuk menjalankan AWS Lambda fungsi saat aturan dipicu, dan Anda mengonfigurasi Amazon SNS untuk mengirim email dengan detail tentang acara tersebut.

Ilustrasi berikut menunjukkan langkah-langkah utama dari tutorial tersebut.



[Langkah 1: Mengonfigurasi jejak dan pemilih peristiwa]

Membuat log, yang disebut jejak, di AWS CloudTrail. Anda mengonfigurasinya untuk menangkap semua panggilan API.

[Langkah 2: Mengonfigurasi fungsi Lambda]

Buat fungsi AWS Lambda yang mencatat detail tentang peristiwa ke bucket S3.

[Langkah 3: Buat topik Amazon SNS yang mengirimkan email ke pelanggan]

Buat topik Amazon SNS yang mengirimkan email ke pelanggannya, dan kemudian Anda berlangganan sendiri untuk topik tersebut.

[Langkah 4: Buat EventBridge aturan Amazon]

Buat aturan yang memberi tahu Amazon EventBridge untuk meneruskan detail panggilan API yang ditentukan ke fungsi Lambda dan ke pelanggan topik SNS.

[Langkah 5: Uji EventBridge aturan Amazon Anda]

Uji aturan baru Anda dengan menjalankan salah satu operasi yang dipantau. Dalam tutorial ini, operasi yang dipantau sedang membuat sebuah unit organisasi (OU). Anda melihat entri log yang dibuat fungsi Lambda, dan Anda melihat email yang dikirim Amazon SNS ke pelanggan.

> **Kiat**
>
> Anda juga dapat menggunakan tutorial ini sebagai panduan dalam mengonfigurasi operasi serupa, seperti mengirim notifikasi email saat pembuatan akun selesai. Karena pembuatan akun adalah operasi tak serempak, maka Anda tidak akan mendapatkan notifikasi secara default setelah selesai. Untuk informasi selengkapnya tentang penggunaan AWS CloudTrail dan Amazon EventBridge denganAWS Organizations, lihat[Pencatatan dan pemantauan di AWS Organizations].

Prasyarat

Tutorial ini mengasumsikan hal berikut:

- Anda dapat masuk ke AWS Management Console sebagai pengguna IAM dari akun pengelolaan di organisasi Anda. Pengguna IAM harus memiliki izin untuk membuat dan mengonfigurasi log in CloudTrail, fungsi di Lambda, topik di Amazon SNS, dan aturan di Amazon. EventBridge Untuk informasi selengkapnya tentang pemberian izin tersebut, lihat Pengelolaan Akses di Panduan Pengguna IAM, atau panduan untuk layanan yang ingin Anda konfigurasi akses-nya.
- Anda memiliki akses ke bucket Amazon Simple Storage Service (Amazon S3) yang sudah ada (atau Anda memiliki izin untuk membuat bucket) untuk menerima log yang Anda konfigurasikan CloudTrail pada langkah 1.

> **Important**
>
> Saat ini, AWS Organizations di-host hanya di Wilayah US East (N. Virginia) (meskipun tersedia secara global). Untuk melakukan langkah-langkah di tutorial ini, Anda harus mengonfigurasi AWS Management Console untuk menggunakan wilayah tersebut.

Langkah 1: Mengonfigurasi jejak dan pemilih peristiwa

Pada langkah ini, Anda masuk ke akun pengelolaan dan mengonfigurasi log (disebut jejak) di AWS CloudTrail. Anda juga mengonfigurasi pemilih peristiwa di jejak untuk menangkap semua panggilan API baca/tulis sehingga Amazon EventBridge memiliki panggilan untuk dipicu.

Untuk membuat jejak

1. Masuk AWS sebagai administrator akun manajemen organisasi dan kemudian buka CloudTrail konsol dihttps://console.aws.amazon.com/cloudtrail/.
2. Pada bilah navigasi yang ada di sudut kanan atas konsol, pilih opsi Wilayah US East (N. Virginia). Jika Anda memilih wilayah lain, AWS Organizations tidak muncul sebagai opsi di pengaturan EventBridge konfigurasi Amazon, dan CloudTrail tidak menangkap informasi tentangnyaAWS Organizations.
3. Di panel navigasi, pilih Jejak.
4. Pilih Buat jejak.

5. Untuk Nama jejak, masukkan **`My-Test-Trail`**.
6. Lakukan salah satu opsi berikut untuk menentukan di CloudTrail mana akan mengirimkan lognya:

   - Jika Anda perlu membuat bucket, pilih Create new S3 bucket dan kemudian, untuk Trail log bucket dan folder, masukkan nama untuk bucket baru.

     > **Note**
     >
     > Nama bucket S3 harus unik secara global.

   - Jika Anda sudah memiliki bucket, pilih Use existing S3 bucket lalu pilih nama bucket dari bucket list S3.
7. Pilih Selanjutnya.
8. Pada halaman Pilih peristiwa log, di bagian Manajemen peristiwa, pilih Baca dan Tulis.
9. Pilih Selanjutnya.
10. Tinjau pilihan Anda dan pilih Buat jejak.

Amazon EventBridge memungkinkan Anda memilih dari beberapa cara berbeda untuk mengirim peringatan saat aturan alarm cocok dengan panggilan API yang masuk. Tutorial ini menunjukkan dua metode: mengaktifkan fungsi Lambda yang dapat mencatat log panggilan API dan mengirim informasi ke topik Amazon SNS yang mengirimkan email atau pesan teks ke pelanggan topik ini. Dalam dua langkah berikutnya, Anda membuat komponen yang Anda butuhkan: fungsi Lambda, dan topik Amazon SNS.

Langkah 2: Mengonfigurasi fungsi Lambda

Pada langkah ini, Anda membuat fungsi Lambda yang mencatat aktivitas API yang dikirim kepadanya oleh EventBridge aturan Amazon yang Anda konfigurasikan nanti.

Untuk membuat fungsi Lambda yang mencatat peristiwa Amazon EventBridge

1. Membuka AWS Lambda konsol di https://console.aws.amazon.com/lambda/.
2. Jika Anda baru mengenal Lambda, pilih Mulai Sekarang di halaman selamat datang; jika tidak, pilih Buat fungsi.
3. Pada halaman Buat fungsi, pilih Gunakan cetak biru.

4. Dari kotak pencarian Cetak biru, masukkan **`hello`** untuk filter dan pilih cetak biru hello-world.
5. Pilih Konfigurasi.
6. Di halaman Informasi Basic, lakukan hal berikut:

   a. Untuk nama fungsi Lambda, masukkan **`LogOrganizationEvents`** di kotak teks Nama.

   b. Untuk Peran, pilih Buat peran baru dengan izin Lambda dasar. Peran ini memberikan izin fungsi Lambda Anda untuk mengakses data yang dibutuhkan dan menulis log outputnya.
7. Edit kode fungsi Lambda, seperti yang ditunjukkan pada contoh berikut.

```
console.log('Loading function');

exports.handler = async (event, context) => {
    console.log('LogOrganizationsEvents');
    console.log('Received event:', JSON.stringify(event, null, 2));
    return event.key1;  // Echo back the first key value
    // throw new Error('Something went wrong');
};
```

   Kode sampel ini mencatat peristiwa dengan string penanda **`LogOrganizationEvents`** yang diikuti oleh string JSON yang membentuk peristiwa.
8. Pilih Buat fungsi.

Langkah 3: Buat topik Amazon SNS yang mengirimkan email ke pelanggan

Pada langkah ini, Anda membuat topik Amazon SNS yang mengirimkan email informasi kepada pelanggannya. Anda menjadikan topik ini sebagai target EventBridge aturan Amazon yang Anda buat nanti.

Untuk membuat topik Amazon SNS untuk mengirim email ke para pelanggan

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/v3/.
2. Di panel navigasi, pilih Topik.
3. Pilih Buat topik baru.

   a. Untuk Nama topik, masukkan **`OrganizationsCloudWatchTopic`**.

   b. Untuk Nama tampilan, masukkan **`OrgsCWEvnt`**.

   c. Pilih Buat topik.

4. Sekarang Anda bisa membuat langganan untuk topik ini. Pilih ARN untuk topik yang baru saja Anda buat.
5. Pilih Buat berlangganan.

    a. Pada halaman Buat langganan, untuk Protokol, pilih Email.

    b. Untuk Titik Akhir, masukkan alamat email Anda.

    c. Pilih Buat langganan. AWS mengirimkan email ke alamat email yang Anda tentukan pada langkah sebelumnya. Tunggu sampai email tersebut tiba, lalu pilih Konfirmasi langganan pada tautan email untuk memverifikasi bahwa Anda berhasil menerima email.

    d. Lalu, kembali ke konsol tersebut dan segarkan halaman. Pesan Konfirmasi menunggu hilang dan sekarang digantikan oleh ID langganan yang berlaku.

Langkah 4: Buat EventBridge aturan Amazon

Sekarang setelah fungsi Lambda yang diperlukan ada di akun Anda, Anda membuat EventBridge aturan Amazon yang memanggilnya saat kriteria dalam aturan terpenuhi.

Untuk membuat EventBridge aturan

1. Buka EventBridge konsol Amazon dihttps://console.aws.amazon.com/events/.
2. Setel konsol ke Wilayah AS Timur (Virginia N.) atau informasi tentang Organizations tidak tersedia. Pada bilah navigasi yang ada di sudut kanan atas konsol, pilih opsi Wilayah US East (N. Virginia).
3. Untuk petunjuk cara membuat aturan, lihat Memulai Amazon EventBridge di panduan EventBridge pengguna Amazon.

Langkah 5: Uji EventBridge aturan Amazon Anda

Pada langkah ini, Anda membuat unit organisasi (OU) dan mengamati EventBridge aturan Amazon, membuat entri log, dan mengirim email kepada diri Anda sendiri dengan detail tentang acara tersebut.

AWS Management Console

Untuk membuat sebuah OU

1. Buka konsol AWS Organizations ke halaman Akun AWS.

2. Pilih kotak centang

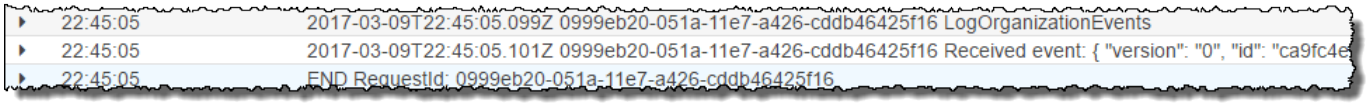
   ☑

   OU Root, pilih Tindakan, dan kemudian di bawah Unit organisasi, pilih Buat baru.

3. Untuk nama OU, masukkan **`TestCWEOU`** lalu pilih Buat unit organisasi.

Untuk melihat entri EventBridge log

1. Buka CloudWatch konsol dihttps://console.aws.amazon.com/cloudwatch/.
2. Di halaman navigasi, pilih Log.
3. Di bawah Grup Log, pilih grup yang terkait dengan fungsi Lambda Anda: /aws/lambda/. LogOrganizationEvents
4. Setiap grup berisi satu atau lebih pengaliran, dan harus ada satu grup untuk hari ini. Pilih itu.
5. Lihat log. Anda akan melihat baris yang serupa dengan yang berikut.



6. Pilih baris tengah entri untuk melihat teks JSON lengkap dari peristiwa yang diterima. Anda dapat melihat semua detail permintaan API di potongan `requestParameters` dan `responseElements` dari keluaran tersebut.

```
2017-03-09T22:45:05.101Z 0999eb20-051a-11e7-a426-cddb46425f16 Received event:
{
    "version": "0",
    "id": "123456-EXAMPLE-GUID-123456",
    "detail-type": "AWS API Call via CloudTrail",
    "source": "aws.organizations",
    "account": "123456789012",
    "time": "2017-03-09T22:44:26Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "eventVersion": "1.04",
        "userIdentity": {
            ...
        },
        "eventTime": "2017-03-09T22:44:26Z",
        "eventSource": "organizations.amazonaws.com",
        "eventName": "CreateOrganizationalUnit",
```

```
        "awsRegion": "us-east-1",
        "sourceIPAddress": "192.168.0.1",
        "userAgent": "AWS Organizations Console, aws-internal/3",
        "requestParameters": {
            "parentId": "r-exampleRootId",
            "name": "TestCWEOU"
        },
        "responseElements": {
            "organizationalUnit": {
                "name": "TestCWEOU",
                "id": "ou-exampleRootId-exampleOUId",
                "arn": "arn:aws:organizations::1234567789012:ou/o-exampleOrgId/ou-
exampleRootId-exampeOUId"
            }
        },
        "requestID": "123456-EXAMPLE-GUID-123456",
        "eventID": "123456-EXAMPLE-GUID-123456",
        "eventType": "AwsApiCall"
    }
}
```

7. Periksa akun email Anda untuk mendapatkan pesan dari OrgsCWEvnt (nama tampilan topik Amazon SNS Anda). Badan email berisi keluaran teks JSON yang sama seperti entri log yang ditampilkan di langkah sebelumnya.

Bersihkan: Hapus sumber daya yang tidak Anda butuhkan lagi

Untuk menghindari biaya yang ditimbulkan, Anda harus menghapus sumber daya AWS yang Anda buat sebagai bagian dari tutorial ini yang tidak ingin Anda simpan.

Untuk membersihkan lingkungan AWS Anda

1. Gunakan CloudTrail konsol untuk menghapus jejak bernama **`My-Test-Trail`** yang Anda buat di langkah 1.
2. Jika Anda membuat bucket Amazon S3 pada langkah 1, gunakan Konsol Amazon S3 untuk menghapusnya.
3. Gunakan Konsol Lambda untuk menghapus fungsi bernama **`LogOrganizationEvents`** yang Anda buat di langkah 2.
4. Gunakan Konsol Amazon SNS untuk menghapus topik Amazon SNS bernama **`OrganizationsCloudWatchTopic`** yang Anda buat di langkah 3.

5. Gunakan CloudWatch konsol untuk menghapus EventBridge aturan bernama **`OrgsMonitorRule`** yang Anda buat di langkah 4.
6. Akhirnya, gunakan Konsol Organizations untuk menghapus OU bernama **`TestCWEOU`** yang Anda buat pada langkah 5.

Selesai. Dalam tutorial ini, Anda dikonfigurasi EventBridge untuk memantau organisasi Anda untuk perubahan. Anda telah mengonfigurasi aturan yang dipicu ketika pengguna mengaktifkan operasi AWS Organizations tertentu. Aturan tersebut menjalankan fungsi Lambda yang mencatat peristiwa dan mengirim email yang berisi detail tentang peristiwa tersebut.

Praktik terbaik untuk manajemen multi-akun

Ikuti rekomendasi ini untuk membantu memandu Anda menyiapkan dan mengelola lingkungan multi-akun diAWS Organizations.

Topik

Mengelola akun Anda dalam satu organisasi

Kami menyarankan untuk membuat satu organisasi dan mengelola semua akun Anda dalam organisasi ini. Organisasi adalah batas keamanan yang memungkinkan Anda menjaga konsistensi di seluruh akun di lingkungan Anda. Anda dapat menerapkan kebijakan atau konfigurasi tingkat layanan secara terpusat di seluruh akun dalam organisasi. Jika Anda ingin mengaktifkan kebijakan yang konsisten, visibilitas pusat, dan kontrol terprogram di seluruh lingkungan multi-akun Anda, ini paling baik dicapai dalam satu organisasi.

Gunakan kata sandi yang kuat untuk pengguna root

Kami menyarankan agar Anda menggunakan kata sandi yang kuat dan unik. Banyak pengelola kata sandi dan algoritme dan alat pembuatan kata sandi yang kuat yang dapat membantu Anda mencapai tujuan ini. Untuk informasi selengkapnya, lihat Mengubah kata sandi untuk Pengguna root akun AWS. Gunakan kebijakan keamanan informasi bisnis Anda untuk mengelola penyimpanan jangka panjang dan akses ke kata sandi untuk pengguna root. Kami menyarankan agar Anda menyimpan kata sandi dalam sistem pengelola kata sandi atau setara yang memenuhi persyaratan keamanan organisasi Anda. Untuk menghindari membuat ketergantungan melingkar, jangan menyimpan kata sandi pengguna root dengan alat yang bergantung pada layanan AWS yang Anda masuki dengan akun yang dilindungi. Metode apa pun yang Anda pilih, kami menyarankan agar Anda memprioritaskan ketahanan dan berpotensi mempertimbangkan untuk meminta beberapa aktor untuk mengotorisasi akses ke brankas ini untuk perlindungan yang ditingkatkan. Setiap akses ke kata sandi atau lokasi penyimpanannya harus dicatat dan dilakukan monitoring. Untuk rekomendasi kata sandi pengguna root tambahan, lihat Praktik terbaik pengguna Root untuk Anda Akun AWS.

Dokumentasikan proses untuk menggunakan kredensial pengguna root

Dokumentasikan pelaksanaan proses penting saat dilakukan untuk memastikan Anda memiliki catatan individu yang terlibat dalam setiap langkah. Untuk mengelola kata sandi, sebaiknya gunakan pengelola kata sandi terenkripsi yang aman. Juga penting untuk menyediakan dokumentasi tentang pengecualian dan kejadian tak terduga yang mungkin terjadi. Untuk informasi selengkapnya, lihat Memecahkan masalah AWS Management Console proses masuk di Panduan Pengguna AWS Masuk dan Tugas yang memerlukan kredensi pengguna root di Panduan Pengguna IAM.

Uji dan validasi bahwa Anda terus memiliki akses ke pengguna root dan bahwa nomor telepon kontak beroperasi setidaknya setiap triwulanan. Ini membantu untuk menegaskan bisnis bahwa proses tersebut bekerja dan bahwa Anda dapat mempertahankan akses ke pengguna root. Hal ini juga menunjukkan bahwa orang yang bertanggung jawab untuk akses root memahami langkah-langkah yang harus mereka melakukan agar proses tersebut berhasil. Untuk meningkatkan waktu respons dan keberhasilan, penting untuk memastikan bahwa semua personel yang terlibat dalam suatu proses memahami dengan tepat apa yang harus mereka lakukan jika akses diperlukan.

Aktifkan kredensi pengguna root Anda

Kami menyarankan agar Anda mengaktifkan beberapa perangkat autentikasi multi-faktor (MFA) ke pengguna Akun AWS root dan pengguna IAM di perangkat Anda. Akun AWS Ini memungkinkan Anda meningkatkan bilah keamanan di Anda Akun AWS dan menyederhanakan pengelolaan akses ke pengguna yang sangat istimewa, seperti pengguna Akun AWS root. Untuk memenuhi kebutuhan pelanggan yang berbeda, AWS mendukung tiga jenis perangkat MFA untuk IAM, termasuk kunci keamanan FIDO, aplikasi otentikator virtual, dan token perangkat keras satu kali kata sandi (TOTP) berbasis waktu.

Setiap jenis authenticator memiliki sifat fisik dan keamanan yang sedikit berbeda yang paling cocok untuk kasus penggunaan yang berbeda. Kunci keamanan FIDO2 menawarkan tingkat jaminan tertinggi dan tahan phishing. Segala bentuk MFA menawarkan postur keamanan yang lebih kuat daripada otentikasi hanya kata sandi, dan kami sangat menyarankan Anda menambahkan beberapa bentuk MFA ke akun Anda. Pilih jenis perangkat yang paling sesuai dengan persyaratan keamanan dan operasional Anda.

Jika Anda memilih perangkat bertenaga baterai untuk autentikator utama Anda, seperti token perangkat keras TOTP, pertimbangkan juga mendaftarkan autentikator yang tidak bergantung pada baterai sebagai mekanisme cadangan. Memeriksa fungsionalitas perangkat secara teratur dan menggantinya sebelum tanggal kedaluwarsa juga penting untuk menjaga akses tanpa gangguan. Apa pun jenis perangkat yang Anda pilih, sebaiknya daftarkan setidaknya dua perangkat (IAM mendukung hingga delapan perangkat MFA per pengguna) untuk meningkatkan ketahanan Anda terhadap kehilangan atau kegagalan perangkat.

Ikuti kebijakan keamanan informasi organisasi Anda untuk penyimpanan perangkat MFA. Kami menyarankan Anda menyimpan perangkat MFA secara terpisah dari kata sandi terkait. Hal ini memastikan bahwa akses ke kata sandi dan perangkat MFA membutuhkan sumber daya (orang, data dan alat) yang berbeda. Pemisahan ini menambahkan lapisan perlindungan ekstra terhadap akses yang tidak sah. Kami juga menyarankan agar Anda mencatat dan memantau akses apa pun ke perangkat MFA atau lokasi penyimpanannya. Ini membantu mendeteksi dan menanggapi akses yang tidak sah.

Untuk informasi lebih lanjut, lihat Mengamankan pengguna root Anda dengan autentikasi multi-faktor (MFA) di Panduan Pengguna IAM. Untuk petunjuk tentang mengaktifkan MFA, lihat Menggunakan autentikasi multi-faktor (MFA) AWS di dan Mengaktifkan perangkat MFA bagi pengguna di. AWS

Terapkan kendali untuk memantau akses ke kredensial pengguna root

Akses ke kredensial pengguna root harus berupa suatu peristiwa yang sangat jarang. Buat peringatan menggunakan alat seperti Amazon EventBridge untuk mengumumkan login dan penggunaan kredensi pengguna root akun manajemen. Peringatan ini harus mencakup, namun tidak boleh terbatas pada, alamat email yang digunakan untuk pengguna root itu sendiri. Peringatan ini harus signifikan dan sulit dilewatkan. Sebagai contoh, lihat Monitor dan beri tahu tentang Aktivitas pengguna root Akun AWS. Verifikasi bahwa personil yang menerima peringatan tersebut memahami cara memvalidasi bahwa akses pengguna root diharapkan, dan bagaimana melakukan ekskalasi jika mereka percaya bahwa insiden keamanan sedang berlangsung. Untuk informasi selengkapnya, lihat Melaporkan Email Mencurigakan atau Pelaporan Kerentanan. Atau, Anda dapat menghubungi AWS untuk bantuan dan panduan tambahan.

Tetap perbarui nomor telepon kontak

Untuk memulihkan akses ke AndaAkun AWS, sangat penting untuk memiliki nomor telepon kontak yang valid dan aktif yang memungkinkan Anda menerima pesan teks atau panggilan. Sebaiknya gunakan nomor telepon khusus untuk memastikan bahwa AWS dapat menghubungi Anda untuk tujuan dukungan dan pemulihan akun. Anda dapat dengan mudah melihat dan mengelola nomor telepon akun Anda melalui AWS Management Console atau Account Management API.

Ada berbagai cara untuk mendapatkan nomor telepon khusus yang memastikan AWS dapat menghubungi Anda. Kami sangat menyarankan agar Anda mendapatkan kartu SIM khusus dan telepon fisik. Simpan telepon dan SIM jangka panjang dengan aman untuk menjamin nomor telepon tetap tersedia untuk pemulihan akun. Juga pastikan tim yang bertanggung jawab atas tagihan seluler memahami pentingnya nomor ini, meskipun tetap tidak aktif untuk waktu yang lama. Penting untuk menjaga kerahasiaan nomor telepon ini dalam organisasi Anda untuk perlindungan tambahan.

Dokumentasikan nomor telepon di halaman konsol Informasi AWS Kontak, dan bagikan detailnya dengan tim tertentu yang harus mengetahuinya di organisasi Anda. Pendekatan ini membantu meminimalkan risiko yang terkait dengan mentransfer nomor telepon ke SIM yang berbeda. Simpan telepon sesuai dengan kebijakan keamanan informasi yang ada. Namun, jangan menyimpan telepon di lokasi yang sama dengan informasi kredensial terkait lainnya. Setiap akses ke kata sandi atau lokasi penyimpanannya harus dicatat dan dilakukan monitoring. Jika nomor telepon yang terkait dengan akun berubah, terapkan proses untuk memperbarui nomor telepon dalam dokumentasi Anda yang ada.

Gunakan alamat email grup untuk akun root

Gunakan alamat email yang dikelola oleh bisnis Anda. Gunakan alamat email yang meneruskan pesan yang diterima langsung ke grup pengguna. Dalam hal AWS harus menghubungi pemilik akun, misalnya, untuk mengkonfirmasi akses, maka pesan email didistribusikan ke beberapa pihak. Pendekatan ini membantu mengurangi risiko keterlambatan dalam menanggapi, bahkan jika individu sedang berlibur, sakit, atau meninggalkan bisnis.

Beban kerja kelompok berdasarkan tujuan bisnis dan bukan struktur pelaporan

Kami menyarankan Anda mengisolasi lingkungan dan data beban kerja produksi di bawah OU yang berorientasi pada beban kerja tingkat atas. OU Anda harus didasarkan pada serangkaian kontrol umum daripada mencerminkan struktur pelaporan perusahaan Anda. Selain OU produksi, kami menyarankan Anda menentukan satu atau lebih OU non-produksi yang berisi akun dan lingkungan beban kerja yang digunakan untuk mengembangkan dan menguji beban kerja. Untuk panduan tambahan, lihat Mengatur OU yang berorientasi pada beban kerja.

Gunakan beberapa akun untuk mengatur beban kerja Anda

An Akun AWS menyediakan keamanan alami, akses, dan batas penagihan untuk AWS sumber daya Anda. Ada manfaat menggunakan beberapa akun karena memungkinkan Anda mendistribusikan kuota tingkat akun dan batas tingkat permintaan API, dan manfaat tambahan yang tercantum di sini. Kami menyarankan Anda menggunakan sejumlah akun dasar di seluruh organisasi, seperti akun untuk keamanan, pencatatan, dan infrastruktur. Untuk akun beban kerja, Anda harus memisahkan beban kerja produksi dari beban kerja pengujian/pengembangan di akun terpisah.

Aktifkan AWS layanan di tingkat organisasi menggunakan konsol layanan atau operasi API/CLI

Sebagai praktik terbaik, kami merekomendasikan untuk mengaktifkan atau menonaktifkan layanan apa pun yang ingin Anda integrasikan AWS Organizations menggunakan konsol layanan itu, atau operasi API/setara perintah CLI. Dengan menggunakan metode ini, AWS layanan dapat melakukan semua langkah inisialisasi yang diperlukan untuk organisasi Anda, seperti membuat sumber daya yang diperlukan dan membersihkan sumber daya saat menonaktifkan layanan. AWS Account

Managementadalah satu-satunya layanan yang memerlukan penggunaan AWS Organizations Konsol atau API untuk mengaktifkan. Untuk meninjau daftar layanan yang terintegrasi denganAWS Organizations, LihatAWS Layanan yang dapat Anda gunakan dengan AWS Organizations.

Gunakan alat penagihan untuk melacak biaya dan mengoptimalkan penggunaan sumber daya

Saat mengelola organisasi, Anda mendapatkan tagihan konsolidasi yang mencakup semua biaya dari akun di organisasi Anda. Untuk pengguna bisnis yang memerlukan akses ke visibilitas biaya, Anda dapat memberikan peran di akun manajemen dengan izin hanya-baca terbatas untuk meninjau alat penagihan dan biaya. Misalnya, Anda dapat membuat kumpulan izin yang menyediakan akses ke laporan penagihan, atau menggunakan AWS Cost Explorer Service (alat untuk melihat tren biaya dari waktu ke waktu), dan layanan efisiensi biaya seperti Amazon S3 Storage Lens dan Compute Optimizer. AWS

Rencanakan strategi penandaan dan penegakan tag di seluruh sumber daya organisasi Anda

Saat akun dan beban kerja Anda berskala, tag dapat menjadi fitur yang berguna untuk pelacakan biaya, kontrol akses, dan organisasi sumber daya. Untuk menandai strategi penamaan, ikuti panduan dalam Menandai sumber daya Anda AWS. Selain sumber daya, Anda dapat membuat tag di root organisasi, akun, OU, dan kebijakan. Lihat strategi Membangun penandaan Anda untuk informasi tambahan.

Praktik terbaik untuk akun manajemen

Ikuti rekomendasi ini untuk membantu melindungi keamanan akun manajemen di AWS Organizations. Rekomendasi ini berasumsi bahwa Anda juga mematuhi Praktik terbaik menggunakan pengguna root saja untuk tugas-tugas yang benar-benar mensyaratkannya.

Topik

- Membatasi siapa yang memiliki akses ke akun manajemen
- Tinjau dan lacak siapa yang memiliki akses
- Gunakan akun manajemen hanya untuk tugas-tugas yang memerlukan akun manajemen

- Hindari penerapan beban kerja ke akun manajemen organisasi
- Mendelegasikan tanggung jawab di luar akun manajemen untuk desentralisasi

Membatasi siapa yang memiliki akses ke akun manajemen

Akun manajemen adalah kunci untuk semua tugas administratif yang disebutkan seperti manajemen akun, kebijakan, integrasi dengan AWS layanan lain, penagihan konsolidasi, dan sebagainya. Oleh karena itu, Anda harus membatasi dan membatasi akses ke akun manajemen hanya untuk pengguna admin yang membutuhkan hak untuk membuat perubahan pada organisasi.

Tinjau dan lacak siapa yang memiliki akses

Untuk memastikan bahwa Anda mempertahankan akses ke akun manajemen, tinjau secara berkala personel dalam bisnis Anda yang memiliki akses ke alamat email, kata sandi, MFA, dan nomor telepon yang terkait dengannya. Selaraskan tinjauan Anda dengan prosedur bisnis yang ada. Tambahkan ulasan bulanan atau triwulanan informasi ini untuk memverifikasi bahwa hanya orang yang benar yang memiliki akses. Pastikan bahwa proses untuk memulihkan atau me-reset akses ke kredensial pengguna root tidak bergantung pada setiap individu tertentu untuk menyelesaikannya. Semua proses harus membahas tentang kemungkinan orang tidak tersedia.

Gunakan akun manajemen hanya untuk tugas-tugas yang memerlukan akun manajemen

Kami merekomendasikan bahwa Anda menggunakan akun manajemen dan pengguna dan perannya untuk tugas-tugas yang harus dilakukan hanya oleh akun tersebut. Simpan semua perangkat AWS Sumber daya dalam Lainnya Akun AWS dalam organisasi dan menjaga mereka keluar dari akun manajemen. Salah satu alasan penting untuk menjaga sumber daya Anda di akun lain adalah karena layanan kontrol kebijakan (SCP) Organizations tidak bekerja untuk membatasi setiap pengguna atau peran dalam akun manajemen. Memisahkan sumber daya Anda dari akun manajemen Anda juga membantu Anda memahami tagihan pada faktur Anda.

Hindari penerapan beban kerja ke akun manajemen organisasi

Operasi istimewa dapat dilakukan dalam akun manajemen organisasi, dan SCP tidak berlaku untuk akun manajemen. Itu sebabnya Anda harus membatasi sumber daya cloud dan data yang terkandung dalam akun manajemen hanya untuk yang harus dikelola di akun manajemen.

Mendelegasikan tanggung jawab di luar akun manajemen untuk desentralisasi

Jika memungkinkan, kami merekomendasikan untuk mendelegasikan tanggung jawab dan layanan di luar akun manajemen. Berikan izin kepada tim Anda di akun mereka sendiri untuk mengelola kebutuhan organisasi, tanpa memerlukan akses ke akun manajemen. Selain itu, Anda dapat mendaftarkan beberapa administrator yang didelegasikan untuk layanan yang mendukung fungsi ini seperti AWS Service Catalog untuk berbagi perangkat lunak di seluruh organisasi, atau AWS CloudFormation StackSets untuk membuat dan menerapkan tumpukan.

Untuk informasi selengkapnya, lihat Arsitektur Referensi Keamanan, Mengatur AWS Lingkungan Anda Menggunakan Beberapa Akun, dan AWS Layanan yang dapat Anda gunakan dengan AWS Organizations untuk saran tentang mendaftarkan akun anggota sebagai administrator yang didelegasikan untuk berbagai AWS layanan. Untuk informasi selengkapnya tentang menyiapkan admin yang didelegasikan, lihat Mengaktifkan akun admin yang didelegasikan untuk dan. AWS Account Management Administrator yang didelegasikan untuk AWS Organizations

Praktik terbaik untuk akun anggota

Ikuti rekomendasi ini untuk membantu melindungi keamanan akun anggota di organisasi Anda. Rekomendasi ini berasumsi bahwa Anda juga mematuhi Praktik terbaik menggunakan pengguna root saja untuk tugas-tugas yang benar-benar mensyaratkannya.

Topik

- Tentukan nama akun dan atribut
- Skalakan lingkungan dan penggunaan akun Anda secara efisien
- Gunakan SCP untuk membatasi apa yang dapat dilakukan pengguna root di akun anggota Anda

Tentukan nama akun dan atribut

Untuk akun anggota Anda, gunakan struktur penamaan dan alamat email yang mencerminkan penggunaan akun. Misalnya, `Workloads+fooA+dev@domain.com` untuk`WorkloadsFooADev`, `Workloads+fooB+dev@domain.com` untuk`WorkloadsFooBDev`. Jika Anda memiliki tag khusus yang ditentukan untuk organisasi Anda, sebaiknya Anda menetapkan tag tersebut pada akun yang mencerminkan penggunaan akun, pusat biaya, lingkungan, dan proyek. Ini membuatnya lebih mudah untuk mengidentifikasi, mengatur, dan mencari akun.

Skalakan lingkungan dan penggunaan akun Anda secara efisien

Saat Anda menskalakan, sebelum membuat akun baru, pastikan akun untuk kebutuhan serupa belum ada, untuk menghindari duplikasi yang tidak perlu. Akun AWSharus didasarkan pada persyaratan akses umum. Jika Anda berencana untuk menggunakan kembali akun, seperti akun sandbox atau yang setara, kami sarankan Anda membersihkan sumber daya atau beban kerja yang tidak dibutuhkan dari akun, tetapi menyimpan akun untuk penggunaan di masa mendatang.

Sebelum menutup akun, perhatikan bahwa mereka tunduk pada batas kuota penutupan akun. Untuk informasi selengkapnya, lihat Kuota untuk AWS Organizations. Pertimbangkan untuk menerapkan proses pembersihan untuk menggunakan kembali akun alih-alih menutupnya dan membuat yang baru jika memungkinkan. Dengan cara ini, Anda akan menghindari biaya yang timbul dari menjalankan sumber daya, dan mencapai batas CloseAccount API.

Gunakan SCP untuk membatasi apa yang dapat dilakukan pengguna root di akun anggota Anda

Kami merekomendasikan bahwa Anda membuat kebijakan kontrol layanan (SCP) dalam organisasi dan melampirkannya ke root organisasi sehingga berlaku untuk semua akun anggota. Untuk informasi selengkapnya, lihat Mengamankan kredensi pengguna root akun Organizations Anda.

Anda dapat menolak semua tindakan root kecuali tindakan root saja tertentu yang harus Anda lakukan di akun anggota Anda. Misalnya, SCP berikut mencegah pengguna root di akun anggota mana pun melakukan panggilan API AWS layanan apa pun kecuali “Memperbarui kebijakan bucket S3 yang salah dikonfigurasi dan menolak akses ke semua prinsipal” (salah satu tindakan yang memerlukan kredensi root). Untuk informasi selengkapnya, lihat Tugas yang memerlukan kredensi pengguna root di Panduan Pengguna IAM.

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

    "Statement": [

        {

            "Effect": "Deny",

            "NotAction":[

            "s3:GetBucketPolicy",
```

```
            "s3:PutBucketPolicy",

            "s3:DeleteBucketPolicy"

                 ],

            "Resource": "*",

            "Condition": {
"StringLike": { "aws:PrincipalArn": "arn:aws:iam::*:root" }

            }

       }

   ]
}
```

Dalam sebagian besar keadaan, setiap tugas administratif dapat dilakukan oleh AWS Identity and Access Management (IAM) role dalam akun anggota yang memiliki izin administrator yang relevan. Peran tersebut harus memiliki kendali sesuai yang diterapkan untuk membatasi, log, dan memantau aktivitas.

Membuat dan mengelola organisasi

Anda dapat melakukan tugas-tugas berikut menggunakan konsol AWS Organizations atau dengan menjalankan perintah AWS Command Line Interface (AWS CLI) atau operasi API AWS SDK:

- Buat organisasi. Buat organisasi Anda dengan akun saat ini sebagai akun pengelolaannya. Buat akun anggota di organisasi Anda, dan undang akun lain untuk bergabung di organisasi Anda.
- Aktifkan semua fitur di organisasi Anda. Mengaktifkan semua fitur adalah cara yang lebih diutamakan untuk menggunakan AWS Organizations. Saat Anda membuat organisasi, Anda memiliki pilihan untuk mengaktifkan semua fitur atau subset fitur untuk tagihan terkonsolidasi. Mengaktifkan semua fitur merupakan default, dan ini mencakup fitur Tagihan Terkonsolidasi.

  Dengan semua fitur diaktifkan, Anda dapat menggunakan fitur pengelolaan akun lanjutan yang tersedia di AWS Organizations seperti Kebijakan Kontrol Layanan (SCP). SCP menawarkan kontrol pusat atas izin maksimum yang tersedia untuk semua akun di organisasi Anda, membantu Anda menjaga akun Anda agar tetap dalam pedoman kontrol akses organisasi Anda.
- Lihat detail tentang organisasi Anda. Lihat detail organisasi Anda beserta akarnya, unit organisasi (UO), dan akun-akunnya.
- Hapus organisasi. Hapus organisasi saat Anda tidak lagi membutuhkannya.

> **Note**
>
> Prosedur di bagian ini menentukan izin minimum yang diperlukan untuk melaksanakan tugas. Prosedur tersebut biasanya berlaku untuk API atau akses ke alat baris perintah. Melaksanakan tugas di konsol mungkin memerlukan izin tambahan. Misalnya, Anda dapat memberikan izin baca-saja kepada semua pengguna di organisasi Anda, dan kemudian memberikan izin lain yang memungkinkan pengguna terpilih untuk melakukan tugas tertentu.

Membuat organisasi

Anda dapat membuat organisasi yang dimulai dengan Akun AWS Anda sebagai akun pengelolaan. Saat Anda membuat organisasi, Anda dapat memilih apakah organisasi men-support semua fitur (direkomendasikan) atau hanya fitur tagihan terkonsolidasi.

Setelah membuat organisasi, Anda dapat menambahkan akun ke organisasi Anda dengan cara berikut dari akun pengelolaan:

- Buat Akun AWS lain yang secara otomatis ditambahkan ke organisasi Anda sebagai akun anggota
- Setelah memverifikasi alamat email Anda, undang Akun AWS yang sudah ada untuk bergabung dengan organisasi Anda sebagai akun anggota

Buat organisasi

Anda dapat membuat sebuah organisasi dengan menggunakan AWS Management Console atau menggunakan perintah dari AWS CLI atau salah satu dari API SDK.

> **Izin minimum**
>
> Untuk membuat organisasi dengan Akun AWS Anda saat ini, Anda harus memiliki izin berikut ini:
>
> - `organizations:CreateOrganization`
> - `iam:CreateServiceLinkedRole`
>
> Anda dapat membatasi izin ini hanya pada `organizations.amazonaws.com` layanan prinsipal.

AWS Management Console

Untuk membuat organisasi

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Secara default, organisasi dibuat dengan semua fitur diaktifkan. Namun, Anda dapat memilih salah satu dari langkah-langkah berikut:
   - Untuk membuat organisasi dengan semua fitur diaktifkan, pada halaman pendahuluan, pilih Buat organisasi.

- Untuk membuat organisasi dengan fitur Tagihan Terkonsolidasi saja, pada halaman pengenalan dan di bawah Buat organisasi, pilih Fitur tagihan terkonsolidasi, dan kemudian di kotak dialog konfirmasi, pilih Buat organisasi.

Jika Anda secara tidak sengaja memilih pilihan yang salah, Anda bisa langsung menuju ke halaman Pengaturan, dan kemudian pilih Hapus organisasi dan mulai dari awal.

3. Organisasi yang dibuat dan halaman Akun AWS muncul. Satu-satunya akun yang ada adalah akun pengelolaan Anda, dan saat ini disimpan di unit organisasi akar (OU).

   Jika diperlukan, Organizations secara otomatis mengirimkan email verifikasi ke alamat terkait dengan akun pengelolaan Anda. Mungkin ada waktu tunda sebelum Anda menerima email verifikasi. Verifikasi alamat email Anda dalam waktu 24 jam. Untuk informasi lebih lanjut, lihat Verifikasi alamat email. Anda dapat membuat akun untuk mengembangkan organisasi tanpa memverifikasi alamat email akun pengelolaan. Namun, untuk mengundang akun yang ada, Anda harus terlebih dahulu menyelesaikan verifikasi email.

   > **Note**
   >
   > Jika akun ini sebelumnya memverifikasi alamat emailnya, maka verifikasi tersebut tidak akan terjadi lagi saat Anda menggunakan akun tersebut untuk membuat organisasi.

AWS CLI & AWS SDKs

Untuk membuat organisasi

Anda dapat menggunakan salah satu perintah berikut untuk membuat organisasi:

- AWS CLI: create-organization

  Contoh berikut membuat sebuah organisasi dan membuat Akun AWS yang saat ini masuk menjadi akun pengelolaan untuk organisasi.

```
$ aws organizations create-organization
{
    "Organization": {
        "Id": "o-aa111bb222",
        "Arn": "arn:aws:organizations::123456789012:organization/o-aa111bb222",
```

```
        "FeatureSet": "ALL",
        "MasterAccountArn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
        "MasterAccountId": "123456789012",
        "MasterAccountEmail": "admin@example.com",
        "AvailablePolicyTypes": [  ...DEPRECATED - DO NOT USE ... ]
    }
}
```

> **Important**
>
> Bidang `AvailablePolicyTypes` tidak lagi digunakan dan tidak berisi informasi yang akurat tentang kebijakan yang diaktifkan di organisasi Anda. Untuk melihat daftar akurat dan lengkap jenis kebijakan yang benar-benar diaktifkan untuk organisasi, gunakan perintah`ListRoots`, seperti yang dijelaskan di bagian AWS CLI dalam bagian berikut.

- AWSSDK: CreateOrganization

Sekarang Anda dapat menambahkan akun tambahan ke organisasi Anda sebagai berikut:

- Untuk membuat Akun AWS yang secara otomatis menjadi bagian dari organisasi AWS Anda, lihat Membuat akun anggota di organisasi Anda.
- Untuk mengundang akun yang ada ke organisasi Anda, lihat Mengundang Akun AWS untuk bergabung dengan organisasi Anda.

Verifikasi alamat email

Setelah Anda membuat organisasi dan sebelum Anda dapat mengundang akun untuk bergabung, Anda harus memverifikasi bahwa Anda memiliki alamat email yang disediakan untuk akun pengelolaan di organisasi.

Saat Anda membuat organisasi, jika akun pengelolaan belum diverifikasi sebelumnya, maka AWS secara otomatis mengirimkan email verifikasi ke alamat email yang ditentukan. Mungkin ada waktu tunda sebelum Anda menerima email verifikasi.

Dalam waktu 24 jam, ikuti petunjuk di email untuk memverifikasi alamat email Anda.

Jika Anda tidak memverifikasi alamat email Anda dalam waktu 24 jam, maka Anda dapat mengirim ulang permintaan verifikasi sehingga Anda dapat mengundang Akun AWS lain ke organisasi Anda.

Jika Anda tidak menerima email verifikasi, periksa apakah alamat email Anda sudah benar dan, jika perlu, ubah alamat email Anda.

- Untuk mengetahui alamat email yang dikaitkan dengan akun pengelolaan Anda, lihat Melihat detail organisasi dari akun pengelolaan.
- Untuk mengubah alamat email yang terkait dengan akun pengelolaan Anda, lihat Mengelola Akun AWS di Panduan Pengguna AWS Billing.

AWS Management Console

Untuk mengirim ulang permintaan verifikasi

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Arahkan ke halaman Pengaturan dan kemudian pilih Kirim permintaan verifikasi. Opsi ini hanya ada jika akun pengelolaan tidak diverifikasi.
3. Verifikasi alamat email Anda dalam waktu 24 jam.

   Setelah memverifikasi alamat email, Anda dapat mengundang Akun AWS lain ke organisasi Anda. Untuk informasi lebih lanjut, lihat Mengundang Akun AWS untuk bergabung dengan organisasi Anda.

Jika Anda mengubah alamat email akun pengelolaan, maka status akun tersebut akan dikembalikan ke "email belum diverifikasi", dan Anda harus menyelesaikan proses verifikasi untuk alamat email baru Anda.

> **Note**
>
> Jika Anda mengundang akun untuk bergabung dengan organisasi sebelum mengubah alamat email akun pengelolaan dan undangan tersebut belum diterima, maka akun tersebut tidak dapat diterima hingga Anda memverifikasi alamat email baru dari akun pengelolaan tersebut. Gunakan prosedur sebelumnya untuk mengirim ulang permintaan verifikasi. Setelah menyelesaikan proses dengan menanggapi email, akun yang diundang dapat menerima undangan tersebut.

Mengaktifkan semua fitur di organisasi Anda

AWS Organizations memiliki dua set fitur yang tersedia:

- Semua fitur — Set fitur ini adalah cara pilihan untuk bekerja dengan AWS Organizations, dan mencakup fitur Tagihan Terkonsolidasi. Saat Anda membuat organisasi, mengaktifkan semua fitur adalah default. Dengan semua fitur diaktifkan, Anda dapat menggunakan fitur pengelolaan akun tingkat lanjut yang tersedia di AWS Organizations seperti Integrasi dengan layanan AWS yang didukung dan kebijakan pengelolaan organisasi.
- Fitur tagihan terkonsolidasi — Semua organisasi mendukung subset fitur ini, yang menyediakan alat pengelolaan dasar yang dapat digunakan untuk mengelola akun di organisasi secara terpusat.

Jika Anda membuat organisasi dengan fitur tagihan terkonsolidasi saja, nanti Anda dapat mengaktifkan semua fitur. Halaman ini menjelaskan proses mengaktifkan semua fitur.

Sebelum mengaktifkan semua fitur

Sebelum mengubah dari organisasi yang mendukung hanya fitur tagihan konsolidasi untuk organisasi yang mendukung semua fitur, perhatikan hal berikut:

- Saat Anda mulai proses untuk mengaktifkan semua fitur, AWS Organizations mengirim permintaan ke setiap akun anggota yang Anda diundang untuk bergabung dengan organisasi Anda. Setiap akun yang diundang harus setuju mengaktifkan semua fitur dengan menerima permintaan. Hanya dengan begitu Anda dapat menyelesaikan proses untuk mengaktifkan semua fitur di organisasi Anda. Jika akun menolak permintaan, Anda harus menghapus akun dari organisasi Anda atau mengirim ulang permintaan. Permintaan harus diterima sebelum Anda dapat menyelesaikan proses untuk mengaktifkan semua fitur. Akun yang Anda dibuat dengan menggunakan AWS Organizations tidak mendapatkan permintaan karena akun tersebut tidak perlu menyetujui kendali tambahan.
- Anda dapat tetap mengundang akun ke organisasi sambil mengaktifkan semua fitur. Pemilik akun yang diundang diberitahu dengan undangan tersebut apakah mereka bergabung dengan organisasi dengan tagihan terkonsolidasi saja, atau dengan semua fitur diaktifkan.
  - Jika Anda mengundang akun selama proses untuk mengaktifkan semua fitur, undangan menyatakan bahwa organisasi mereka bergabung meminta semua fitur diaktifkan. Jika Anda membatalkan proses untuk mengaktifkan semua fitur sebelum akun menerima undangan, undangan tersebut dibatalkan. Anda harus mengundang akun lagi untuk menjadi anggota organisasi dengan fitur tagihan terkonsolidasi saja.

  - Jika Anda mengundang akun dan undangan belum diterima sebelum Anda memulai proses untuk mengaktifkan semua fitur, maka undangan itu akan dibatalkan karena undangan tersebut menyatakan bahwa organisasi hanya memiliki fitur tagihan terkonsolidasi. Anda harus mengundang lagi akun tersebut untuk menjadi anggota organisasi dengan semua fitur diaktifkan.
- Anda juga dapat terus membuat akun di organisasi. Proses tersebut tidak terpengaruh oleh perubahan ini.
- AWS Organizations memverifikasi bahwa setiap akun anggota memiliki peran tertaut layanan bernama `AWSServiceRoleForOrganizations`. Peran ini wajib dilakukan di semua akun untuk mengaktifkan semua fitur. Jika Anda menghapus peran di akun yang diundang, menerima undangan untuk mengaktifkan semua fitur membuat ulang peran. Jika Anda menghapus peran di akun yang dibuat menggunakan AWS Organizations, maka akun yang menerima undangan tersebut secara khusus membuat peran tersebut. Semua undangan ini harus diterima bagi organisasi untuk menyelesaikan proses mengaktifkan semua fitur.
- Karena mengaktifkan semua fitur memungkinkan untuk menggunakan SCP, pastikan administrator akun Anda memahami pengaruh melampirkan SCP ke organisasi, unit organisasi, atau akun. SCP dapat membatasi apa yang pengguna dan bahkan administrator dapat lakukan di akun yang terpengaruh. Misalnya, akun pengelolaan menerapkan SCP yang dapat mencegah akun anggota meninggalkan organisasi.
- Akun pengelolaan tidak terpengaruh oleh SCP. Anda tidak dapat membatasi apa yang dapat dilakukan pengguna dan peran dalam akun pengelolaan dengan menerapkan SCP. SCP hanya mempengaruhi akun anggota.
- Migrasi dari fitur tagihan terkonsolidasi ke semua fitur adalah satu arah. Anda tidak dapat mengalihkan organisasi dengan semua fitur yang diaktifkan kembali ke fitur tagihan terkonsolidasi saja.
- (Tidak direkomendasikan) Jika organisasi Anda hanya mengaktifkan fitur tagihan terkonsolidasi, maka administrator akun anggota dapat memilih untuk menghapus peran tertaut layanan bernama `AWSServiceRoleForOrganizations`. Jika nanti Anda memilih untuk mengaktifkan semua fitur dalam sebuah organisasi, peran ini diperlukan dan dibuat ulang di semua akun sebagai bagian dari penerimaan undangan untuk mengaktifkan semua fitur. Untuk informasi lebih lanjut tentang cara AWS Organizations menggunakan peran ini, lihat AWS Organizations dan peran tertaut layanan.

Memulai proses untuk mengaktifkan semua fitur

Saat masuk ke akun pengelolaan organisasi Anda, Anda dapat memulai proses untuk mengaktifkan semua fitur. Untuk melakukan ini, selesaikan langkah-langkah berikut.

> **Izin minimum**
>
> Untuk mengaktifkan semua fitur di organisasi Anda, Anda harus memiliki izin berikut:
>
> - `organizations:EnableAllFeatures`
> - `organizations:DescribeOrganization` — hanya diperlukan bila menggunakan konsol Organizations

AWS Management Console

Untuk meminta akun anggota yang diundang untuk menyetujui untuk mengaktifkan semua fitur dalam organisasi

1. Masuk konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Pengaturan pilih Mulai proses untuk mengaktifkan semua fitur.
3. Pada halaman Aktifkan semua fitur, akui Anda memahami bahwa Anda tidak dapat kembali ke fitur tagihan terkonsolidasi saja setelah Anda beralih dengan memilih Mulai proses untuk mengaktifkan semua fitur.

   AWS Organizations mengirimkan permintaan ke setiap akun yang diundang (bukan dibuat) di organisasi yang meminta persetujuan untuk mengaktifkan semua fitur dalam organisasi. Jika Anda memiliki akun yang dibuat menggunakan AWS Organizations dan administrator akun anggota menghapus peran tertaut layanan bernama `AWSServiceRoleForOrganizations`, maka AWS Organizations akan mengirimkan akun tersebut permintaan untuk membuat ulang peran.

   Konsol menampilkan daftar Status persetujuan permintaan untuk akun yang diundang.

   > **Tip**
   >
   > Untuk kembali ke halaman ini nanti, buka laman Pengaturan dan di bagian Permintaan dikirim tanggal, pilih Tinjau status.

4. Laman Aktifkan semua fitur menunjukkan status permintaan saat ini untuk setiap akun dalam organisasi. Akun yang telah menyetujui permintaan menunjukkan status DITERIMA. Akun yang belum disetujui menampilkan status BUKA.

AWS CLI & AWS SDKs

Untuk meminta akun anggota yang diundang untuk menyetujui untuk mengaktifkan semua fitur dalam organisasi

Anda dapat menggunakan salah satu perintah berikut untuk mengaktifkan semua fitur di organisasi:

- AWS CLI: enable-all-features

  Perintah berikut memulai proses untuk mengaktifkan semua fitur dalam organisasi.

```
$ aws organizations enable-all-features
{
    "Handshake": {
        "Id": "h-79d8f6f114ee4304a5e55397eEXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-79d8f6f114ee4304a5e55397eEXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ],
        "State": "REQUESTED",
        "RequestedTimestamp": "2020-11-19T16:21:46.995000-08:00",
        "ExpirationTimestamp": "2021-02-17T16:21:46.995000-08:00",
        "Action": "ENABLE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "o-a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ]
    }
}
```

  Output menunjukkan detail jabat tangan yang harus disetujui oleh akun anggota yang diundang.

- AWSSDK: EnableAllFeatures

> **Catatan**
>
> - Hitungan mundur 90 hari dimulai saat permintaan dikirim ke akun anggota. Semua akun harus menyetujui permintaan dalam jangka waktu tersebut atau permintaan kedaluwarsa. Jika permintaan kedaluwarsa, semua permintaan yang terkait dengan upaya ini dibatalkan, dan Anda harus mulai kembali dengan langkah 2.
> - Setelah Anda membuat permintaan untuk mengaktifkan semua fitur, undangan akun yang tidak diterima yang ada akan dibatalkan.
> - Selama proses migrasi semua fitur, Anda masih dapat memulai undangan akun baru dan membuat akun baru.

Setelah semua akun yang diundang dalam organisasi menyetujui permintaan mereka, Anda dapat menyelesaikan proses dan mengaktifkan semua fitur. Anda juga dapat segera menyelesaikan proses jika organisasi Anda tidak memiliki akun anggota yang diundang. Untuk menyelesaikan proses, lanjutkan dengan Menyelesaikan proses untuk mengaktifkan semua fitur.

Menyetujui permintaan untuk mengaktifkan semua fitur atau membuat ulang peran tertaut layanan

Saat masuk ke salah satu akun anggota yang diundang organisasi, Anda dapat menyetujui permintaan dari akun pengelolaan. Jika akun Anda awalnya diundang untuk bergabung dengan organisasi, maka undangan bertujuan untuk mengaktifkan semua fitur dan secara implisit menyertakan persetujuan untuk membuat ulang peran `AWSServiceRoleForOrganizations`, jika diperlukan. Jika akun Anda dibuat menggunakan AWS Organizations dan Anda menghapus peran tertaut layanan `AWSServiceRoleForOrganizations`, maka Anda menerima undangan hanya untuk membuat ulang peran. Untuk melakukan ini, selesaikan langkah-langkah berikut.

> **Important**
>
> Jika Anda mengaktifkan semua fitur, akun manajemen di organisasi dapat menerapkan kontrol berbasis kebijakan pada akun anggota Anda. Kendali ini dapat membatasi apa yang

pengguna dan bahkan apa yang dapat Anda lakukan sebagai administrator di akun Anda. Pembatasan tersebut dapat mencegah akun Anda keluar dari organisasi.

Izin minimum

Untuk menyetujui permintaan untuk mengaktifkan semua fitur untuk akun anggota Anda, Anda harus memiliki izin berikut:

- `organizations:AcceptHandshake`
- `organizations:DescribeOrganization` — hanya diperlukan bila menggunakan konsol Organizations
- `organizations:ListHandshakesForAccount`— hanya diperlukan bila menggunakan konsol Organizations
- `iam:CreateServiceLinkedRole` — hanya diperlukan jika peran `AWSServiceRoleForOrganizations` harus dibuat ulang di akun anggota

AWS Management Console

Untuk menyetujui permintaan untuk mengaktifkan semua fitur dalam organisasi

1. Masuk ke konsol AWS Organizations di konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak direkomendasikan) di akun anggota.
2. Baca apa artinya menerima permintaan untuk semua fitur dalam organisasi bagi akun Anda, lalu pilih Terima. Halaman terus menunjukkan proses sebagai belum selesai sampai semua akun dalam organisasi menerima permintaan dan administrator akun pengelolaan menyelesaikan proses.

AWS CLI & AWS SDKs

Untuk menyetujui permintaan untuk mengaktifkan semua fitur dalam organisasi

Untuk menyetujui permintaan tersebut, Anda harus menerima jabat tangan dengan `"Action": "APPROVE_ALL_FEATURES"`.

- AWS CLI:

- terima-jabat tangan
- list-handshakes-for-account

Contoh berikut menunjukkan cara mendaftar jabat tangan yang tersedia untuk akun Anda. Nilai `"Id"` di baris keempat dari output adalah nilai yang Anda butuhkan untuk perintah berikutnya.

```
$ aws organizations list-handshakes-for-account
{
    "Handshakes": [
        {
            "Id": "h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
            "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
approve_all_features/h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
            "Parties": [
                {
                    "Id": "a1b2c3d4e5",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "111122223333",
                    "Type": "ACCOUNT"
                }
            ],
            "State": "OPEN",
            "RequestedTimestamp": "2020-11-19T16:35:24.824000-08:00",
            "ExpirationTimestamp": "2021-02-17T16:35:24.035000-08:00",
            "Action": "APPROVE_ALL_FEATURES",
            "Resources": [
                {
                    "Value": "c440da758cab44068cdafc812EXAMPLE",
                    "Type": "PARENT_HANDSHAKE"
                },
                {
                    "Value": "o-aa111bb222",
                    "Type": "ORGANIZATION"
                },
                {
                    "Value": "111122223333",
                    "Type": "ACCOUNT"
                }
            ]
        }
    ]
```

```
}
```

Contoh berikut menggunakan Id jabat tangan dari perintah sebelumnya untuk menerima jabat tangan itu.

```
$ aws organizations accept-handshake --handshake-id h-
a2d6ecb7dbdc4540bc788200aEXAMPLE
{
    "Handshake": {
        "Id": "h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
approve_all_features/h-a2d6ecb7dbdc4540bc788200aEXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "111122223333",
                "Type": "ACCOUNT"
            }
        ],
        "State": "ACCEPTED",
        "RequestedTimestamp": "2020-11-19T16:35:24.824000-08:00",
        "ExpirationTimestamp": "2021-02-17T16:35:24.035000-08:00",
        "Action": "APPROVE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "c440da758cab44068cdafc812EXAMPLE",
                "Type": "PARENT_HANDSHAKE"
            },
            {
                "Value": "o-aa111bb222",
                "Type": "ORGANIZATION"
            },
            {
                "Value": "111122223333",
                "Type": "ACCOUNT"
            }
        ]
    }
}
```

- AWS SDK:
  - list-handshakes-for-account
  - AcceptHandshake

Menyelesaikan proses untuk mengaktifkan semua fitur

Semua akun anggota yang diundang harus menyetujui permintaan untuk mengaktifkan semua fitur. Jika tidak ada akun anggota yang diundang dalam organisasi, halaman Aktifkan semua kemajuan fitur menunjukkan banner hijau bahwa Anda dapat menyelesaikan proses.

> **Izin minimum**
>
> Untuk menyelesaikan proses untuk mengaktifkan semua fitur untuk organisasi, Anda harus memiliki izin berikut:
>
> - `organizations:AcceptHandshake`
> - `organizations:ListHandshakesForOrganization`
> - `organizations:DescribeOrganization` — hanya diperlukan bila menggunakan konsol Organizations

AWS Management Console

Untuk menyelesaikan proses untuk mengaktifkan semua fitur

1. Masuk konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Pengaturan, jika semua akun yang diundang menerima permintaan untuk mengaktifkan semua fitur, maka kotak hijau akan muncul di bagian atas halaman untuk memberi tahu Anda. Dalam kotak hijau, pilih Menuju penyelesaian.
3. Pada halaman Aktifkan semua fitur, pilih Selesaikan, dan kemudian di kotak dialog konfirmasi, pilih Selesaikan lagi.
4. Organisasi sekarang memiliki semua fitur yang diaktifkan.

AWS CLI & AWS SDKs

Untuk menyelesaikan proses untuk mengaktifkan semua fitur

Menyelesaikan prosesnya, Anda harus menerima jabat tangan dengan `"Action": "ENABLE_ALL_FEATURES"`.

- AWS CLI:
  - list-handshakes-for-organization
  - terima-jabat tangan

```
$ aws organizations list-handshakes-for-organization
{
    "Handshakes": [
        {
            "Id": "h-43a871103e4c4ee399868fbf2EXAMPLE",
            "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-43a871103e4c4ee399868fbf2EXAMPLE",
            "Parties": [
                {
                    "Id": "a1b2c3d4e5",
                    "Type": "ORGANIZATION"
                }
            ],
            "State": "OPEN",
            "RequestedTimestamp": "2020-11-20T08:41:48.047000-08:00",
            "ExpirationTimestamp": "2021-02-18T08:41:48.047000-08:00",
            "Action": "ENABLE_ALL_FEATURES",
            "Resources": [
                {
                    "Value": "o-aa111bb222",
                    "Type": "ORGANIZATION"
                }
            ]
        }
    ]
}
```

Contoh berikut menunjukkan cara mencantumkan jabat tangan yang tersedia untuk organisasi. Nilai `"Id"` di baris keempat dari output adalah nilai yang Anda butuhkan untuk perintah berikutnya.

```
$ aws organizations accept-handshake \
    --handshake-id h-43a871103e4c4ee399868fbf2EXAMPLE
{
    "Handshake": {
        "Id": "h-43a871103e4c4ee399868fbf2EXAMPLE",
        "Arn": "arn:aws:organizations::123456789012:handshake/o-aa111bb222/
enable_all_features/h-43a871103e4c4ee399868fbf2EXAMPLE",
        "Parties": [
            {
                "Id": "a1b2c3d4e5",
                "Type": "ORGANIZATION"
            }
        ],
        "State": "ACCEPTED",
        "RequestedTimestamp": "2020-11-20T08:41:48.047000-08:00",
        "ExpirationTimestamp": "2021-02-18T08:41:48.047000-08:00",
        "Action": "ENABLE_ALL_FEATURES",
        "Resources": [
            {
                "Value": "o-aa111bb222",
                "Type": "ORGANIZATION"
            }
        ]
    }
}
```

- AWS SDK:
  - AcceptHandshake
  - AcceptHandshake

Langkah selanjutnya:

- Aktifkan jenis kebijakan yang ingin Anda gunakan. Setelah itu, Anda dapat melampirkan kebijakan untuk mengelola akun di organisasi Anda. Untuk informasi lebih lanjut, lihat Mengelola kebijakan di AWS Organizations.
- Aktifkan integrasi dengan layanan yang didukung. Untuk informasi lebih lanjut, lihat Menggunakan AWS Organizations dengan layanan AWS lainnya.

Melihat detail tentang organisasi Anda

Anda dapat melakukan tugas-tugas berikut untuk melihat detail tentang elemen organisasi Anda.

Topik

Melihat detail organisasi dari akun pengelolaan

Saat Anda masuk ke akun pengelolaan organisasi di konsol AWS Organizations, Anda dapat melihat detail organisasi.

> **Izin minimum**
>
> Untuk melihat detail organisasi, Anda harus memiliki izin berikut:
>
> - `organizations:DescribeOrganization`

AWS Management Console

Untuk melihat detail untuk organisasi Anda

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Arahkan ke halaman Pengaturan. Halaman ini menampilkan detail tentang organisasi, termasuk ID organisasi serta nama akun serta alamat e-mail yang ditetapkan ke akun pengelolaan organisasi.

AWS CLI & AWS SDKs

Untuk melihat detail untuk organisasi Anda

Anda dapat menggunakan salah satu perintah berikut untuk melihat detail organisasi:

- AWS CLI: describe-organizations

  Contoh berikut menunjukkan informasi yang termasuk dalam keluaran dari perintah ini.

```
$ aws organizations describe-organization
{
    "Organization": {
        "Id": "o-aa111bb222",
        "Arn": "arn:aws:organizations::123456789012:organization/o-aa111bb222",
        "FeatureSet": "ALL",
        "MasterAccountArn": "arn:aws:organizations::128716708097:account/o-
aa111bb222/123456789012",
        "MasterAccountId": "123456789012",
        "MasterAccountEmail": "admin@example.com",
        "AvailablePolicyTypes": [ ...DEPRECATED - DO NOT USE... ]
    }
}
```

  Important

  Bidang `AvailablePolicyTypes` tidak lagi digunakan dan tidak berisi informasi yang akurat tentang kebijakan yang diaktifkan di organisasi Anda. Untuk melihat daftar akurat dan lengkap jenis kebijakan yang benar-benar diaktifkan untuk organisasi, gunakan perintah`ListRoots`, seperti yang dijelaskan di bagian AWS CLI dalam bagian berikut.

- AWSSDK: DescribeOrganization

Saat Anda melihat detail wadah akar

Saat Anda masuk ke akun pengelolaan organisasi di AWS Organizationskonsol, Anda dapat melihat detail wadah akar.

Izin minimum

Untuk melihat detail akar, Anda harus memiliki izin berikut:

- `organizations:DescribeOrganization` (hanya konsol)

- `organizations:ListRoots`

Akar adalah kontainer paling atas dalam hirarki unit organisasi (OU) dan umumnya berperilaku sebagai OU. Namun, sebagai kontainer di bagian paling atas hirarki, perubahan akar mempengaruhi setiap OU lain dan setiap Akun AWS dalam organisasi.

AWS Management Console

Untuk melihat detail akar

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Arahkan ke halaman Akun AWS, dan pilih OU Akar (namanya, bukan tombol radio).
3. Halaman detail Akar akan muncul dan menampilkan detail akar.

AWS CLI & AWS SDKs

Untuk melihat detail akar

Anda dapat menggunakan salah satu perintah berikut untuk melihat detail akar:

- AWS CLI: list-roots

  Contoh berikut menunjukkan bagaimana untuk mengambil detail akar, termasuk yang jenis kebijakannya saat ini diaktifkan dalam organisasi:

```
$ aws organizations list-roots
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": [
                {
                    "Type": "BACKUP_POLICY",
                    "Status": "ENABLED"
                }
```

```
            ]
        }
    ]
}
```

- AWSSDK: ListRoots

Melihat detail dari sebuah OU

Saat Anda masuk ke akun pengelolaan organisasi di konsol AWS Organizations, Anda dapat melihat detail OU di organisasi Anda.

> **Izin minimum**
>
> Untuk melihat detail unit organisasi (OU), Anda harus memiliki izin berikut:
>
> - `organizations:DescribeOrganizationalUnit`
> - `organizations:DescribeOrganization` — hanya diperlukan bila menggunakan konsol Organizations
> - `organizations:ListOrganizationsUnitsForParent`— hanya diperlukan bila menggunakan konsol Organizations
> - `organizations:ListRoots` — hanya diperlukan bila menggunakan konsol Organizations

AWS Management Console

Untuk melihat detail OU

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Akun AWS, pilih nama OU (bukan tombol radio) yang ingin Anda periksa. Jika OU yang Anda inginkan adalah anak dari OU lain, maka pilih ikon segitiga di sebelah OU induknya untuk memperluas dan melihat OU di tingkat berikutnya dalam hirarki. Ulangi sampai Anda menemukan OU yang Anda inginkan.

   Kotak Detail unit organisasi menunjukkan informasi tentang OU.

AWS CLI & AWS SDKs

Untuk melihat detail OU

Anda dapat menggunakan perintah berikut untuk melihat detail OU:

- AWS CLI, AWS SDK:
  - daftar-akar
  - daftar-anak-anak
  - describe-organizational-unit

Contoh berikut menunjukkan cara menemukan ID di OU menggunakan AWS CLI. Anda menemukan ID OU dengan melintasi hirarki dimulai dengan perintah `list-roots` dan kemudian melakukan `list-children` pada akar dan lakukan berulang pada masing-masing anak-anaknya sampai Anda menemukan yang Anda inginkan.

```
$ aws organizations list-roots
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": []
        }
    ]
}
$ aws organizations list-children --parent-id r-a1b2 --child-type
 ORGANIZATIONAL_UNIT
{
    "Children": [
        {
            "Id": "ou-a1b2-f6g7h111",
            "Type": "ORGANIZATIONAL_UNIT"
        }
    ]
}
```

Setelah Anda memiliki ID OU, contoh berikut menunjukkan bagaimana untuk mengambil detail tentang OU.

```
$ aws organizations describe-organizational-unit --organizational-unit-id ou-a1b2-
f6g7h111
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h111",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h111",
        "Name": "Production-Apps"
    }
}
```

- AWS SDK:
  - ListRoots
  - ListChildren
  - DescribeOrganizationalUnit

Melihat detail sebuah akun

Saat Anda masuk ke akun pengelolaan organisasi di konsol AWS Organizations, Anda dapat melihat detail tentang akun Anda.

> **Izin minimum**
>
> Untuk melihat detail Akun AWS, Anda harus memiliki izin berikut:
>
> - `organizations:DescribeAccount`
> - `organizations:DescribeOrganization` — hanya diperlukan bila menggunakan konsol Organizations
> - `organizations:ListAccounts` — hanya diperlukan bila menggunakan konsol Organizations

AWS Management Console

Untuk melihat detail Akun AWS

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Arahkan ke halaman Akun AWS dan pilih nama akun (bukan tombol radio) yang ingin Anda periksa. Jika akun yang Anda inginkan adalah anak dari OU, Anda mungkin harus memilih ikon segitiga  di sebelah OU untuk memperluasnya dan melihat anak-anaknya. Ulangi sampai Anda menemukan akunnya.

   Kotak Detail akun menunjukkan informasi tentang akun.

AWS CLI & AWS SDKs

Untuk melihat detail Akun AWS

Anda dapat menggunakan perintah berikut untuk melihat detail akun:

- AWS CLI:
  - list-accounts — mencantumkan detail Semua akun dalam organisasi
  - describe-account — mencantumkan detail hanya akun yang ditentukan

  Kedua perintah tersebut mengembalikan detail yang sama untuk setiap akun termasuk dalam responsnya.

  Contoh berikut menunjukkan cara mengambil detail tentang akun tertentu.

```
$ aws organizations describe-account --account-id 123456789012

{
    "Account": {
        "Id": "123456789012",
        "Arn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
        "Email": "admin@example.com",
        "Name": "Example.com Organization's Management Account",
```

```
        "Status": "ACTIVE",
        "JoinedMethod": "INVITED",
        "JoinedTimestamp": "2020-11-20T09:04:20.346000-08:00"
    }
}
```

- AWS SDK:
  - ListAccounts
  - DescribeAccount

Melihat detail kebijakan

Saat Anda masuk ke akun pengelolaan organisasi di konsol AWS Organizations, Anda dapat melihat detail tentang kebijakan Anda.

> **Izin minimum**
>
> Untuk melihat detail kebijakan, Anda harus memiliki izin berikut:
>
> - `organizations:DescribePolicy`
> - `organizations:ListPolicies`

AWS Management Console

Untuk melihat detail kebijakan

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Lakukan salah satu hal berikut:
   - Arahkan ke halaman Kebijakan, kemudian pilih jenis kebijakan untuk kebijakan yang ingin Anda periksa.
   - Arahkan ke halaman Akun AWS, lalu buka OU atau akun tempat kebijakan tersebut dilampirkan. Akhirnya, pilih tab Kebijakan untuk melihat daftar kebijakan terlampir.
3. Pilih nama kebijakan (bukan tombol radio).

Pada halaman Detail untuk kebijakan, Anda dapat melihat semua informasi tentang kebijakan, termasuk teks kebijakan JSON, dan daftar OU dan akun yang dilampiri dengan kebijakan tersebut.

AWS CLI & AWS SDKs

Untuk melihat detail kebijakan

Anda dapat menggunakan salah satu perintah berikut untuk melihat detail kebijakan:

- AWS CLI:
  - daftar-kebijakan
  - describe-policy — mencantumkan detail kebijakan yang ditentukan saja

Contoh berikut menunjukkan bagaimana cara menemukan ID kebijakan dari kebijakan yang ingin Anda periksa. Anda harus menentukan jenis kebijakan, dan perintah akan mengembalikan semua kebijakan dari jenis kebijakan itu saja.

```
$ aws organizations list-policies --filter BACKUP_POLICY
{
    "Policies": [
        {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "test-backup-policy",
            "Description": "test-policy-description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        }
    ]
}
```

Responsnya mencakup semua detail kecuali dokumen kebijakan JSON.

Contoh berikut menunjukkan bagaimana cara mengambil detail dari kebijakan yang ditentukan saja, termasuk dokumen kebijakan JSON.

```
$ aws organizations describe-policy --policy-id p-i9j8k7l6m5
{
```

```
    "Policies": [
        {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "test-backup-policy",
            "Description": "test-policy-description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"plans\":{\"My-Backup-Plan\":{\"regions\":{\"@@assign\":
[\"us-west-2\"]},\"rules\":{\"My-Backup-Rule\"
                    :{\"target_backup_vault_name\":{\"@@assign\":\"My-Primary-
Backup-Vault\"}}},\"selections\":{\"tags\":{
                    \"My-Backup-Plan-Resource-Assignment\":{\"iam_role_arn\":
{\"@@assign\":\"arn:aws:iam::$account:role/
                    My-Backup-Role\"},\"tag_key\":{\"@@assign\":\"Stage\"},
\"tag_value\":{\"@@assign\":[\"Production\"]}}}}}}"
    ]
}
```


- AWS SDK:
  - ListPolicies
  - DescribePolicy

Menghapus organisasi

Saat tidak membutuhkan organisasi Anda, Anda dapat menghapusnya. Menghapus organisasi tidak menutup akun manajemen, melainkan menghapus akun manajemen dari organisasi dan menghapus organisasi itu sendiri. Akun manajemen sebelumnya menjadi mandiri Akun AWS yang tidak lagi dikelola olehAWS Organizations. Anda kemudian memiliki tiga pilihan: Anda dapat terus menggunakannya sebagai akun yang berdiri sendiri, Anda dapat menggunakannya untuk membuat organisasi yang berbeda, atau Anda dapat menerima undangan dari organisasi lain untuk menambahkan akun ke organisasi tersebut sebagai akun anggota.

Important

- Jika Anda menghapus organisasi, Anda tidak dapat memulihkannya. Jika Anda telah membuat kebijakan apa pun di dalam organisasi, kebijakan tersebut juga akan terhapus dan Anda tidak dapat memulihkannya.
- Anda dapat menghapus organisasi hanya setelah menghapus semua akun anggota dari organisasi. Jika Anda membuat beberapa akun anggota dengan menggunakan AWS Organizations, Anda mungkin diblokir untuk menghapus akun tersebut. Anda dapat menghapus akun anggota hanya jika memiliki semua informasi yang diperlukan untuk beroperasi sebagai Akun AWS yang berdiri sendiri. Untuk informasi lebih lanjut tentang cara menyediakan informasi dan kemudian menghapus akun, lihat Tinggalkan organisasi dari akun anggota Anda.
- Jika Anda menutup akun anggota sebelum menghapusnya dari organisasi, akun tersebut akan masuk status 'ditangguhkan' selama jangka waktu tertentu dan Anda tidak dapat menghapus akun dari organisasi hingga akhirnya ditutup. Ini dapat memakan waktu hingga 90 hari dan dapat mencegah Anda menghapus organisasi hingga semua akun anggota ditutup sepenuhnya.

Saat Anda menghapus akun pengelolaan dari organisasi dengan menghapus organisasi, penghapusan dapat mempengaruhi akun dengan cara berikut:

- Akun bertanggung jawab untuk hanya membayar biaya sendiri dan tidak lagi bertanggung jawab atas biaya yang dikeluarkan oleh akun lain.
- Integrasi dengan layanan lain mungkin dinonaktifkan. Misalnya, AWS IAM Identity Center mengharuskan organisasi untuk beroperasi, jadi jika Anda menghapus akun dari organisasi yang mendukung IAM Identity Center, pengguna di akun tersebut tidak dapat lagi menggunakan layanan tersebut.

Akun pengelolaan organisasi tidak akan terpengaruh oleh kebijakan kontrol layanan (SCP), sehingga tidak ada perubahan izin setelah SCP tidak lagi tersedia.

Topik

- Menghapus organisasi

Menghapus organisasi

Gunakan prosedur berikut untuk menghapus organisasi yang mengembalikan akun manajemen sebelumnya ke mandiri Akun AWS yang tidak lagi dikelola oleh. AWS Organizations

> **Izin minimum**
>
> Untuk menghapus organisasi, Anda harus masuk sebagai pengguna atau peran dalam akun manajemen, dan Anda harus memiliki izin berikut:
>
> - `organizations:DeleteOrganization`
> - `organizations:DescribeOrganization` — hanya diperlukan bila menggunakan konsol Organizations

AWS Management Console

Untuk menghapus organisasi

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Sebelum Anda dapat menghapus organisasi, Anda harus terlebih dahulu menghapus semua akun dari organisasi. Untuk informasi lebih lanjut, lihat Menghapus akun anggota dari organisasi Anda.
3. Buka Pengaturan halaman, dan kemudian pilih Hapus organisasi.
4. Di kotak dialog konfirmasi Hapus organisasi, masukkan ID organisasi yang ditampilkan pada baris di atas kotak teks. Lalu, pilih Hapus organisasi.

> **Important**
>
> Operasi ini tidak menutup akun manajemen tetapi mengembalikannya ke mandiriAkun AWS. Untuk menutup akun, ikuti langkah-langkah diMenutup akun anggota di organisasi Anda.

AWS CLI & AWS SDKs

Untuk menghapus organisasi

Gunakan salah satu perintah berikut untuk menghapus organisasi:

- AWS CLI: delete-organization

  Contoh berikut menghapus organisasi untuk Akun AWS yang kredensialnya digunakan adalah akun pengelolaan.

  ```
  $ aws organizations delete-organization
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWSSDK: DeleteOrganization

Mengelola Akun AWS di organisasi Anda

Sebuah organisasi adalah kumpulan Akun AWS yang Anda kelola bersama. Anda dapat melakukan tugas berikut untuk mengelola akun yang merupakan bagian dari organisasi Anda:

- Tinjau detail akun di organisasi Anda. Anda dapat melihat nomor ID unik akun, Amazon Resource Name (ARN), dan kebijakan yang terlampir pada nama sumber daya itu.
- Ekspor daftar semua Akun AWS di organisasi Anda. Anda dapat mengunduh file.csv yang berisi detail akun untuk setiap akun dalam organisasi Anda.
- Undang Akun AWS yang ada untuk bergabung dengan organisasi Anda. Buat undangan, kelola undangan yang telah Anda buat, dan terima atau tolak undangan.
- Buat Akun AWS sebagai bagian dari organisasi Anda. Buat dan akses sebuah Akun AWS yang secara otomatis menjadi bagian dari organisasi Anda.
- Perbarui kontak alternatif di organisasi Anda. Perbarui kontak alternatif untuk Akun AWS s Anda di organisasi Anda.
- Hapus Akun AWS dari organisasi Anda. Sebagai administrator di akun pengelolaan, hapus akun anggota yang tidak ingin Anda kelola lagi dari organisasi Anda. Sebagai administrator dari sebuah akun anggota, hapus akun Anda dari organisasinya. Jika akun pengelolaan telah melampirkan kebijakan ke akun anggota, Anda dapat diblokir untuk menghapus akun Anda.
- Hapus (atau tutup) Akun AWS. Saat Anda tidak lagi membutuhkan Akun AWS, Anda dapat menutup akun untuk mencegah penggunaan atau akrual biaya apa pun.

Dampak berada di organisasi

- Apa dampaknya pada Akun AWS yang bergabung dengan organisasi?
- Apa dampaknya pada Akun AWS yang Anda buat dalam suatu organisasi?

Dampak pada Akun AWS yang bergabung di suatu organisasi?

Saat Anda mengundang Akun AWS untuk bergabung pada organisasi, dan pemilik akun menerima undangan tersebut, AWS Organizations secara otomatis melakukan perubahan berikut di akun anggota baru:

- AWS Organizations membuat panggilan peran yang tertaut layanan yang disebut `AWSServiceRoleForOrganizations`. Akun harus memiliki peran ini jika organisasi Anda mendukung semua fitur. Anda dapat menghapus peran jika organisasi hanya mendukung kumpulan fitur tagihan terkonsolidasi. Jika Anda menghapus peran dan selanjutnya mengaktifkan semua fitur di organisasi, AWS Organizations membuat ulang peran untuk akun.
- Anda mungkin memiliki berbagai kebijakan yang dilampirkan ke akar organisasi atau OU yang berisi akun. Jika Anda melakukannya, kebijakan tersebut langsung berlaku bagi semua pengguna dan peran dalam akun yang diundang.
- Anda dapat mengaktifkan kepercayaan layanan untuk layanan AWS lain untuk organisasi Anda. Bila Anda melakukannya, layanan yang tepercaya tersebut dapat membuat peran tertaut layanan atau melakukan tindakan di setiap akun anggota dalam organisasi, termasuk akun yang diundang.

> **Note**
>
> Untuk akun anggota yang diundang, AWS Organizations tidak secara otomatis membuat peran OrganizationAccountAccessRoleIAM. Peran ini memberikan pengguna di akun pengelolaan akses administratif ke akun anggota. Jika Anda ingin mengaktifkan tingkat kontrol administratif tersebut ke akun yang diundang, maka Anda dapat menambahkan peran secara manual. Untuk informasi lebih lanjut, lihat Membuat akun anggota yang diundang OrganizationAccountAccessRole .

Anda dapat mengundang suatu akun untuk bergabung dengan organisasi yang hanya mengaktifkan fitur tagihan terkonsolidasi. Jika nantinya Anda ingin mengaktifkan semua fitur untuk organisasi, akun yang diundang harus menyetujui perubahan tersebut.

Apa dampaknya pada Akun AWS yang Anda buat di sebuah organisasi?

Saat Anda membuat Akun AWS di organisasi Anda, AWS Organizations secara otomatis membuat perubahan berikut ke akun anggota baru:

- AWS Organizations membuat panggilan peran yang tertaut layanan yang disebut `AWSServiceRoleForOrganizations`. Akun harus memiliki peran ini jika organisasi Anda mendukung semua fitur. Anda dapat menghapus peran jika organisasi hanya mendukung kumpulan fitur tagihan terkonsolidasi. Jika Anda menghapus peran dan selanjutnya mengaktifkan semua fitur di organisasi, AWS Organizations membuat ulang peran untuk akun.

- AWS Organizationsmenciptakan peran OrganizationAccountAccessRoleIAM. Peran ini memberikan akses akun pengelolaan ke akun anggota baru. Meskipun peran ini dapat dihapus, kami sarankan Anda tidak menghapusnya sehingga peran tersebut tersedia sebagai opsi pemulihan.
- Jika Anda memiliki kebijakan yang terlampir pada akar pohon OU, kebijakan itu langsung berlaku bagi semua pengguna dan peran dalam akun yang dibuat. Akun baru ditambahkan ke akar OU secara default.
- Jika Anda telah mengaktifkan kepercayaan layanan untuk layanan AWS lain untuk organisasi Anda, layanan tepercaya tersebut dapat membuat peran tertaut layanan atau melakukan tindakan di akun anggota mana pun di organisasi, termasuk akun yang Anda buat.

Mengundang Akun AWS untuk bergabung dengan organisasi Anda

Setelah membuat organisasi dan memverifikasi bahwa Anda memiliki alamat email yang terkait dengan akun manajemen, Anda dapat mengundang yang ada Akun AWS untuk bergabung dengan organisasi Anda.

Saat Anda mengundang akun, AWS Organizations kirimkan undangan ke pemilik akun, yang memutuskan apakah akan menerima atau menolak undangan tersebut. Anda dapat menggunakan AWS Organizations konsol untuk memulai dan mengelola undangan yang Anda kirim ke akun lain. Anda dapat mengirim undangan ke akun lain hanya dari akun pengelolaan organisasi Anda.

> **Note**
>
> Riwayat penagihan dan laporan untuk semua akun tetap berada di akun pembayar di Organisasi. Sebelum memindahkan akun ke Organisasi baru, unduh tagihan apa pun dan laporkan riwayat untuk akun anggota mana pun yang ingin Anda simpan. Ini mungkin termasuk Laporan Biaya dan Penggunaan, Laporan Penagihan Terperinci, atau laporan yang dihasilkan oleh Cost Explorer Service.

Jika Anda adalah administrator Akun AWS, Anda juga dapat menerima atau menolak undangan dari suatu organisasi. Jika Anda menerima, maka akun Anda menjadi anggota organisasi tersebut. Akun Anda hanya dapat bergabung dengan satu organisasi, jadi jika Anda menerima beberapa undangan untuk bergabung, maka Anda hanya dapat menerima satu.

Saat akun menerima undangan untuk bergabung dengan organisasi, akun manajemen organisasi menjadi bertanggung jawab atas semua biaya yang timbul oleh akun anggota baru. Metode pembayaran yang dilampirkan pada akun anggota tidak lagi digunakan. Sebagai gantinya, metode pembayaran yang dilampirkan pada akun pengelolaan organisasi membayar semua biaya yang diperoleh oleh akun anggota.

Ketika akun yang diundang bergabung dengan organisasi Anda, dan organisasi Anda dalam mode Semua fitur, akun manajemen memiliki akses administratif penuh dan kontrol atas akun anggota yang diundang. Namun, tidak seperti akun yang dibuat, peran `OrganizationAccountAccessRole` IAM tidak secara otomatis dibuat di akun anggota dengan izin untuk diasumsikan oleh akun manajemen. Untuk membuat dan mengonfigurasi ini setelah akun yang diundang menjadi anggota, ikuti langkah-langkahnyaMembuat akun anggota yang diundang OrganizationAccountAccessRole .

> **Note**
>
> Saat Anda membuat akun di organisasi alih-alih mengundang akun yang ada untuk bergabung, AWS Organizations secara otomatis membuat peran IAM (dinamai secara `OrganizationAccountAccessRole` default) yang dapat Anda gunakan untuk memberi pengguna di administrator akun manajemen akses ke akun yang dibuat.

AWS Organizations secara otomatis membuat peran terkait layanan di akun anggota yang diundang untuk mendukung integrasi antara AWS Organizations dan layanan lainnya AWS . Untuk informasi selengkapnya, lihat AWS Organizations dan peran tertaut layanan.

Untuk jumlah undangan yang dapat Anda kirim per hari, lihat Nilai maksimum dan minimum. Undangan yang diterima tidak dihitung masuk dalam kuota ini. Segera setelah satu undangan diterima, Anda dapat mengirim undangan lain pada hari yang sama. Setiap undangan harus ditanggapi dalam waktu 15 hari, atau kedaluwarsa.

Undangan yang dikirim ke akun dihitung masuk kuota akun di organisasi Anda. Hitungan dipulihkan jika akun yang diundang menurun, akun pengelolaan membatalkan undangan, atau undangan kedaluwarsa.

Untuk membuat akun yang secara otomatis menjadi bagian dari organisasi Anda, lihat Membuat akun anggota di organisasi Anda.

Important

Karena kendala penagihan, Anda Akun AWS hanya dapat mengundang dari AWS penjual yang sama (dalam kasus AWS India) dan AWS partisi sebagai akun manajemen.

- Semua akun dalam suatu organisasi harus berasal dari penjual catatan yang sama dengan akun manajemen jika akun manajemen organisasi Anda dibuat oleh Amazon Web Services India Private Limited ("AWS India") (sebelumnya dikenal sebagai Amazon Internet Services Private Limited). Misalnya, sebagai AWS penjual di India, Anda hanya dapat mengundang akun AWS India lainnya ke organisasi Anda. Anda tidak dapat menggabungkan akun AWS India atau dari AWS penjual lain.
- Semua akun dalam suatu organisasi harus berasal dari AWS partisi yang sama dengan akun manajemen. Akun di Wilayah AWS partisi komersial tidak dapat berada di organisasi dengan akun dari partisi Wilayah China atau akun di partisi AWS GovCloud (US) Regions.

Mengirim undangan ke Akun AWS

Untuk mengundang akun ke organisasi, Anda harus terlebih dahulu memverifikasi bahwa Anda memiliki alamat email yang tertaut dengan akun pengelolaan. Untuk informasi lebih lanjut, lihat Verifikasi alamat email. Setelah Anda memverifikasi alamat email, lakukan langkah-langkah berikut untuk mengundang akun ke organisasi Anda.

Izin minimum

Untuk mengundang seorang Akun AWS untuk bergabung dengan organisasi Anda, Anda harus memiliki izin berikut:

- `organizations:DescribeOrganization` (konsol saja)
- `organizations:InviteAccountToOrganization`

AWS Management Console

Untuk mengundang akun lain untuk bergabung dengan organisasi Anda

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Jika Anda sudah memverifikasi alamat email Anda AWS, lewati langkah ini.

   Jika belum memverifikasi alamat email, ikuti petunjuk di email verifikasi dalam waktu 24 jam setelah Anda membuat organisasi. Mungkin ada waktu tunda sebelum Anda menerima pesan email verifikasi. Anda tidak dapat mengundang akun untuk bergabung dengan organisasi hingga Anda memverifikasi alamat email Anda.
3. Arahkan ke halaman Akun AWS, dan pilih Tambahkan akun AWS .
4. Pada halaman Tambahkan Akun AWS, pilih Undang akun AWS yang ada.
5. Pada AWS halaman Undang yang sudah ada, untuk alamat Email atau ID akun yang Akun AWS akan diundang masukkan alamat email yang terkait dengan akun yang akan diundang, atau nomor ID akunnya.
6. (Opsional) Untuk Pesan yang akan disertakan dalam pesan email undangan, masukkan teks apa pun yang ingin Anda sertakan dalam undangan email kepada pemilik akun yang diundang.
7. (Opsional) Pada bagian Tambahkan tag, tentukan satu atau beberapa tag yang secara otomatis diterapkan ke akun setelah administrator menerima undangan. Untuk melakukan ini, pilih Tambahkan tag dan kemudian masukkan nilai kunci dan nilai opsional. Membiarkan nilai kosong akan mengaturnya menjadi string kosong; itu bukan `null`. Anda dapat melampirkan hingga 50 tag ke Akun AWS.
8. Pilih Kirim undangan.

   > **Important**
   >
   > Jika Anda menerima pesan bahwa Anda telah melampaui kuota akun untuk organisasi atau bahwa Anda tidak dapat menambahkan akun karena organisasi Anda masih menginisialisasi, hubungi AWS Support.
9. Konsol tersebut mengalihkan Anda ke halaman Undangan di mana Anda dapat melihat semua undangan yang terbuka dan diterima di sini. Undangan yang baru saja Anda buat muncul di bagian atas daftar dengan statusnya diatur ke BUKA.

AWS Organizations mengirim undangan ke alamat email pemilik akun yang Anda undang ke organisasi. Pesan email ini menyertakan tautan ke AWS Organizations konsol, tempat pemilik akun dapat melihat detailnya dan memilih untuk menerima atau menolak undangan. Atau, pemilik akun yang diundang dapat melewati pesan email, langsung ke AWS Organizations konsol, melihat undangan, dan menerima atau menolaknya.

Undangan ke akun ini segera dihitung terhadap jumlah maksimum akun yang dapat Anda miliki di organisasi Anda. AWS Organizations tidak menunggu hingga akun menerima undangan. Jika akun yang diundang menolak, maka akun pengelolaan membatalkan undangan. Jika akun yang diundang tidak merespons dalam jangka waktu yang ditentukan, undangan akan kedaluwarsa. Dalam kedua kasus, undangan tidak lagi dihitung masuk dalam kuota Anda.

AWS CLI & AWS SDKs

Untuk mengundang akun lain untuk bergabung dengan organisasi Anda

Anda dapat menggunakan salah satu perintah berikut untuk mengundang akun lain untuk bergabung dengan organisasi Anda:

- AWS CLI: invite-account-to-organization

```
$ aws organizations invite-account-to-organization \
    --target '{"Type": "EMAIL", "Id": "juan@example.com"}' \
    --notes "This is a request for Juan's account to join Bill's organization."
{
    "Handshake": {
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "ExpirationTimestamp": 1482952459.257,
        "Id": "h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                 "Type": "ORGANIZATION"
            },
            {
                 "Id": "juan@example.com",
                 "Type": "EMAIL"
```

```
            }
        ],
        "RequestedTimestamp": 1481656459.257,
        "Resources": [
            {
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@amazon.com"
                    },
                    {
                         "Type": "MASTER_NAME",
                         "Value": "Management Account"
                    },
                    {
                         "Type": "ORGANIZATION_FEATURE_SET",
                         "Value": "FULL"
                    }
                ],
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid"
            },
            {
                "Type": "EMAIL",
                "Value": "juan@example.com"
            }
        ],
        "State": "OPEN"
    }
}
```


- AWS SDK: InviteAccountToOrganization

Mengelola undangan tertunda untuk organisasi Anda

Saat masuk ke akun pengelolaan, Anda dapat melihat semua Akun AWS di organisasi Anda dan batalkan undangan yang tertunda (terbuka). Untuk melakukan ini, selesaikan langkah-langkah berikut.

> **Izin minimum**
>
> Untuk mengelola undangan tertunda untuk organisasi Anda, Anda harus memiliki izin berikut:

- `organizations:DescribeOrganization` — hanya diperlukan bila menggunakan konsol Organizations
- `organizations:ListHandshakesForOrganization`
- `organizations:CancelHandshake`

AWS Management Console

Untuk melihat atau membatalkan undangan yang dikirim dari organisasi Anda ke akun lain

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Arahkan ke halaman Undangan.

   Halaman ini menampilkan semua undangan yang dikirim dari organisasi Anda dan statusnya saat ini.

   > **Note**
   >
   > Undangan yang diterima, dibatalkan, dan ditolak akan tetap muncul dalam daftar selama 30 hari. Setelah itu, mereka akan dihapus dan tidak lagi muncul dalam daftar.

3. Pilih tombol radio  yang ada di samping undangan yang ingin Anda batalkan, lalu pilih Batalkan undangan. Jika tombol radio berwarna abu-abu, maka undangan itu tidak dapat dibatalkan.

   Status undangan berubah dari TERBUKA menjadi DIBATALKAN.

   AWS mengirim pesan email ke pemilik akun yang menyatakan bahwa Anda membatalkan undangan. Akun tidak lagi dapat bergabung dengan organisasi kecuali Anda mengirim undangan baru.

AWS CLI & AWS SDKs

Untuk melihat atau membatalkan undangan yang dikirim dari organisasi Anda ke akun lain

Anda dapat menggunakan perintah berikut untuk melihat atau membatalkan undangan:

- AWS CLI: list-handshakes-for-organization, batalkan-jabat tangan
- Contoh berikut menunjukkan undangan yang dikirim oleh organisasi ini ke akun lain.

```
$ aws organizations list-handshakes-for-organization
{
    "Handshakes": [
        {
            "Action": "INVITE",
            "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
            "ExpirationTimestamp": 1482952459.257,
            "Id": "h-examplehandshakeid111",
            "Parties": [
                {
                    "Id": "o-exampleorgid",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "juan@example.com",
                    "Type": "EMAIL"
                }
            ],
            "RequestedTimestamp": 1481656459.257,
            "Resources": [
                {
                    "Resources": [
                        {
                            "Type": "MASTER_EMAIL",
                            "Value": "bill@amazon.com"
                        },
                        {
                            "Type": "MASTER_NAME",
                            "Value": "Management Account"
                        },
                        {
                            "Type": "ORGANIZATION_FEATURE_SET",
                            "Value": "FULL"
                        }
                    ],
                    "Type": "ORGANIZATION",
                    "Value": "o-exampleorgid"
```

```
                },
                {
                    "Type": "EMAIL",
                    "Value": "juan@example.com"
                },
                {
                    "Type":"NOTES",
                    "Value":"This is an invitation to Juan's account to join
 Bill's organization."
                }
            ],
            "State": "OPEN"
        },
        {
            "Action": "INVITE",
            "State":"ACCEPTED",
            "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
            "ExpirationTimestamp": 1.471797437427E9,
            "Id": "h-examplehandshakeid222",
            "Parties": [
                {
                    "Id": "o-exampleorgid",
                    "Type": "ORGANIZATION"
                },
                {
                    "Id": "anika@example.com",
                    "Type": "EMAIL"
                }
            ],
            "RequestedTimestamp": 1.469205437427E9,
            "Resources": [
                {
                    "Resources": [
                        {
                            "Type":"MASTER_EMAIL",
                             "Value":"bill@example.com"
                        },
                        {
                            "Type":"MASTER_NAME",
                            "Value":"Management Account"
                        }
                    ],
                    "Type":"ORGANIZATION",
```

```
                    "Value":"o-exampleorgid"
                },
                {
                    "Type":"EMAIL",
                    "Value":"anika@example.com"
                },
                {
                    "Type":"NOTES",
                    "Value":"This is an invitation to Anika's account to join
 Bill's organization."
                }
            ]
        }
    ]
}
```

Contoh berikut menunjukkan cara membatalkan undangan ke akun.

```
$ aws organizations cancel-handshake --handshake-id h-examplehandshakeid111
{
    "Handshake": {
        "Id": "h-examplehandshakeid111",
        "State":"CANCELED",
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "susan@example.com",
                "Type": "EMAIL"
            }
        ],
        "Resources": [
            {
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid",
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
```

```
                        "Value": "bill@example.com"
                    },
                    {
                        "Type": "MASTER_NAME",
                        "Value": "Management Account"
                    },
                    {
                        "Type": "ORGANIZATION_FEATURE_SET",
                        "Value": "CONSOLIDATED_BILLING"
                    }
                ]
            },
            {
                "Type": "EMAIL",
                "Value": "anika@example.com"
            },
            {
                "Type": "NOTES",
                "Value": "This is a request for Susan's account to join Bob's
 organization."
            }
        ],
        "RequestedTimestamp": 1.47008383521E9,
        "ExpirationTimestamp": 1.47137983521E9
    }
}
```

- AWS SDK: ListHandshakesForOrganization, CancelHandshake

Menerima atau menolak undangan dari organisasi

Anda Akun AWS mungkin menerima undangan untuk bergabung dengan organisasi. Anda dapat menerima atau menolak undangan. Untuk melakukan ini, selesaikan langkah-langkah berikut.

> **Note**
>
> Status akun dengan organisasi memengaruhi biaya dan data penggunaan yang terlihat:
>
> - Jika akun anggota meninggalkan organisasi dan menjadi akun mandiri, maka akun tidak lagi memiliki akses ke data biaya dan penggunaan dari rentang waktu ketika akun menjadi anggota organisasi. Akun hanya memiliki akses ke data yang dihasilkan sebagai akun mandiri.

- Jika akun anggota meninggalkan organisasi A untuk bergabung dengan organisasi B, maka akun tidak lagi memiliki akses ke data biaya dan penggunaan dari rentang waktu ketika akun masih menjadi anggota organisasi A. Akun memiliki akses hanya ke data yang dihasilkan sebagai anggota organisasi B.
- Jika akun bergabung kembali ke organisasi di mana sebelumnya ia menjadi bagian darinya, maka akun tersebut akan kembali mendapatkan akses ke data biaya dan penggunaan historis.

Note

Hanya akun anggota dan akun mandiri yang dapat menerima atau menolak undangan untuk bergabung dengan organisasi. Jika undangan dikirim ke akun anggota, akun tersebut harus meninggalkan organisasi saat ini sebelum menerima undangan. Jika undangan dikirim ke akun manajemen yang sudah menjadi bagian dari AWS Organisasi, akun tersebut tidak akan dapat menerima undangan sampai mereka menghapus semua akun anggota dari organisasi mereka dan menghapus organisasi tersebut.

Izin minimum

Untuk menerima atau menolak undangan untuk bergabung dengan AWS organisasi, Anda harus memiliki izin berikut:

- `organizations:ListHandshakesForAccount`— Diperlukan untuk melihat daftar undangan di konsol. AWS Organizations
- `organizations:AcceptHandshake`.
- `organizations:DeclineHandshake`.
- `iam:CreateServiceLinkedRole`— Diperlukan hanya ketika menerima undangan memerlukan pembuatan peran terkait layanan di akun anggota untuk mendukung integrasi dengan layanan lain. AWS Untuk informasi selengkapnya, lihat AWS Organizations dan peran tertaut layanan.

AWS Management Console

Untuk menerima atau menolak undangan

1. Undangan untuk bergabung dengan organisasi akan dikirim ke alamat email pemilik akun. Jika Anda adalah pemilik akun dan menerima pesan email undangan, ikuti petunjuk dalam undangan email atau buka konsol AWS Organizations di peramban Anda, lalu pilih Undangan, atau langsung menuju halaman Undangan akun anggota.
2. Jika diminta, masuk ke akun yang diundang sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar akun (tidak disarankan).
3. Halaman Undangan akun anggota menampilkan undangan terbuka akun Anda untuk bergabung dengan organisasi.

   Pilih Terima undangan atau Tolak undangan, sesuai keadaan.

   - Jika Anda memilih Terima undangan di langkah sebelumnya, konsol tersebut akan mengarahkan Anda ke Gambaran umum organisasi berisi detail tentang organisasi yang kini akun Anda menjadi anggotanya. Anda dapat melihat ID organisasi dan alamat email pemilik.

     > **Note**
     >
     > Undangan yang diterima akan tetap muncul dalam daftar selama 30 hari. Setelah itu, mereka akan dihapus dan tidak lagi muncul dalam daftar.

     AWS Organizations secara otomatis membuat peran terkait layanan di akun anggota baru untuk mendukung integrasi antara AWS Organizations dan layanan lainnya AWS . Untuk informasi selengkapnya, lihat AWS Organizations dan peran tertaut layanan.

     AWS mengirim pesan email ke pemilik akun manajemen organisasi yang menyatakan bahwa Anda menerima undangan tersebut. Ia juga mengirim pesan email ke pemilik akun anggota yang menyatakan bahwa akun sekarang menjadi anggota organisasi.
   - Jika Anda memilih Menolak pada langkah sebelumnya, maka akun Anda tetap berada di halaman Undangan akun anggota yang mencantumkan undangan tertunda lainnya.

     AWS mengirim pesan email ke pemilik akun manajemen organisasi yang menyatakan bahwa Anda menolak undangan.

> **Note**
>
> Undangan yang ditolak akan tetap muncul dalam daftar selama 30 hari. Setelah itu, mereka akan dihapus dan tidak lagi muncul dalam daftar.

AWS CLI & AWS SDKs

Untuk menerima atau menolak undangan

Anda dapat menggunakan perintah berikut untuk menerima atau menolak undangan:

- AWS CLI: accept-handshake, decline-handshake

  Contoh berikut menunjukkan cara menerima undangan untuk bergabung ke sebuah organisasi.

```
$ aws organizations accept-handshake --handshake-id h-examplehandshakeid111
{
    "Handshake": {
        "Action": "INVITE",
        "Arn": "arn:aws:organizations::111111111111:handshake/o-exampleorgid/
invite/h-examplehandshakeid111",
        "RequestedTimestamp": 1481656459.257,
        "ExpirationTimestamp": 1482952459.257,
        "Id": "h-examplehandshakeid111",
        "Parties": [
            {
                "Id": "o-exampleorgid",
                "Type": "ORGANIZATION"
            },
            {
                "Id": "juan@example.com",
                "Type": "EMAIL"
            }
        ],
        "Resources": [
            {
                "Resources": [
                    {
                        "Type": "MASTER_EMAIL",
                        "Value": "bill@amazon.com"
                    },
```

```
                    {
                        "Type": "MASTER_NAME",
                        "Value": "Management Account"
                    },
                    {
                        "Type": "ORGANIZATION_FEATURE_SET",
                         "Value": "ALL"
                    }
                ],
                "Type": "ORGANIZATION",
                "Value": "o-exampleorgid"
            },
            {
                "Type": "EMAIL",
                "Value": "juan@example.com"
            }
        ],
        "State": "ACCEPTED"
    }
}
```

Contoh berikut menunjukkan cara menolak undangan untuk bergabung ke sebuah organisasi.

- AWS SDK: AcceptHandshake, DeclineHandshake

Membuat akun anggota di organisasi Anda

Halaman ini menjelaskan cara membuat Akun AWS dalam organisasi Anda diAWS Organizations. Untuk mempelajari tentang memulai AWS dan membuat satu Akun AWS, lihat Memulai Pusat Sumber Daya.

Sebuah organisasi adalah kumpulan Akun AWS yang Anda kelola secara terpusat. Anda dapat melakukan prosedur berikut untuk mengelola akun yang merupakan bagian dari organisasi Anda:

- Membuat Akun AWS yang merupakan bagian dari organisasi Anda
- Mengakses akun anggota yang memiliki peran akses akun pengelolaan

Important

- Bila Anda membuat akun anggota di organisasi Anda, AWS Organizations secara otomatis membuat AWS Identity and Access Management (IAM) role `OrganizationAccountAccessRole` dalam akun anggota yang memungkinkan pengguna dan role dalam akun manajemen untuk melakukan kontrol administratif penuh atas akun anggota. Peran ini tunduk pada setiap kebijakan kontrol layanan (SCP) yang berlaku untuk akun anggota.

  AWS Organizationsjuga secara otomatis menambahkan kebijakan terkelola dengan `OrganizationAccountAccessRole` peran ke akun anggota. Hal ini memungkinkan kontrol terpusat, sehingga setiap akun tambahan yang dilampirkan pada kebijakan terkelola yang sama akan diperbarui secara otomatis setiap kali kebijakan diperbarui. Sebelumnya, akun baru yang dibuat dalam organisasi mendapat kebijakan inline yang ditambahkan yang hanya diterapkan ke akun tunggal itu. Untuk mempelajari selengkapnya tentang kebijakan sebaris dan terkelola, lihat Kebijakan terkelola dan kebijakan sebaris di Panduan Pengguna IAM.

  AWS Organizations juga secara otomatis membuat peran tertaut layanan bernama `AWSServiceRoleForOrganizations` yang memungkinkan integrasi dengan pilihan layanan AWS. Anda harus mengkonfigurasi layanan lain untuk memungkinkan integrasi. Untuk informasi lebih lanjut, lihat AWS Organizations dan peran tertaut layanan.
- Jika organisasi ini dikelola dengan AWS Control Tower, lalu buat akun Anda dengan menggunakan account factory AWS Control Tower di konsol AWS Control Tower atau API. Jika Anda membuat akun di Organizations, maka akun tersebut tidak terdaftar dengan AWS Control Tower. Untuk informasi selengkapnya, lihat Mengacu pada Sumber Daya di luar AWS Control Tower dalam Panduan Pengguna AWS Control Tower.

Note

Akun AWS yang Anda buat sebagai bagian dari organisasi tidak secara otomatis berlangganan email pemasaran AWS. Untuk mengikutsertakan akun Anda sehingga menerima email pemasaran, lihat https://pages.awscloud.com/communication-preferences.

Membuat Akun AWS yang merupakan bagian dari organisasi Anda

Setelah Anda masuk ke akun manajemen organisasi, Anda dapat membuat akun anggota yang secara otomatis menjadi bagian dari organisasi Anda. Bila Anda membuat akun menggunakan prosedur berikut, AWS Organizations secara otomatis menyalin informasi kontak utama berikut dari akun manajemen ke akun anggota baru:

- nomor telepon
- Nama perusahaan
- URL Situs Web
- Alamat

Ini juga menyalin bahasa komunikasi dan informasi Marketplace (vendor akun di beberapaWilayah AWS) dari akun manajemen.

> **Note**
>
> AWStidak secara otomatis mengumpulkan semua informasi yang diperlukan akun anggota untuk beroperasi sebagai akun mandiri. Jika Anda perlu menghapus akun anggota dari organisasi dan menjadikannya akun mandiri, Anda harus memberikan informasi tersebut untuk akun tersebut sebelum Anda dapat menghapusnya. Untuk informasi selengkapnya, lihat Tinggalkan organisasi dari akun anggota Anda.

> **Izin minimum**
>
> Untuk membuat akun anggota di organisasi Anda, Anda harus memiliki izin berikut:
>
> - `organizations:CreateAccount`
> - `organizations:DescribeOrganization` — hanya diperlukan saat menggunakan konsol Organizations
> - `iam:CreateServiceLinkedRole` (diberikan kepada prinsipal `organizations.amazonaws.com` untuk mengaktifkan pembuatan peran tertaut layanan yang diperlukan di akun anggota).

AWS Management Console

Untuk membuat Akun AWS yang secara otomatis menjadi bagian dari organisasi Anda

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Akun AWS, pilih Tambahkan Akun AWS.
3. Pada halaman TambahkanAkun AWS, pilih Buat Akun AWS (dipilih secara default).
4. Pada halaman Buat Akun AWS, untuk nama Akun AWS, masukkan nama yang ingin Anda tetapkan untuk akun. Nama ini membantu Anda membedakan akun tersebut dari semua akun lain dalam organisasi dan terpisah dari IAM alias atau nama email pemilik.
5. Untuk Alamat email pemilik akun, masukkan alamat email pemilik akun. Alamat email ini tidak dapat dikaitkan dengan Akun AWS yang lain karena itu menjadi kredensial nama pengguna untuk pengguna akar akun.
6. (Opsional) Tentukan nama yang akan ditetapkan ke IAM role yang dibuat secara otomatis di akun baru. Peran ini memberikan akun pengelolaan organisasi izin untuk mengakses akun anggota yang baru dibuat. Jika Anda tidak menentukan nama, AWS Organizations akan memberikan peran tersebut dengan nama default dari `OrganizationAccountAccessRole`. Kami sarankan Anda menggunakan nama default di semua akun Anda agar konsisten.

   > **Important**
   >
   > Ingat nama peran ini. Anda membutuhkannya nanti untuk memberikan akses ke akun baru untuk pengguna dan peran di akun manajemen.

7. (Opsional) Di bagian Tag, tambahkan satu atau beberapa tag ke akun baru dengan memilih Tambahkan tag lalu masukkan kunci dan nilai opsional. Membiarkan nilai kosong akan mengaturnya menjadi string kosong; itu bukan `null`. Anda dapat melampirkan hingga 50 tag ke akun.
8. Pilih Buat Akun AWS.

   - Jika Anda mendapatkan kesalahan yang menunjukkan bahwa Anda melampaui kuota akun untuk organisasi, lihat Saya menerima pesan "kuota terlampaui" saat mencoba menambahkan akun ke organisasi saya.

- Jika Anda mengalami kesalahan yang menunjukkan bahwa Anda tidak dapat menambahkan akun karena organisasi Anda masih menginisialisasi, tunggu satu jam dan coba lagi.
- Anda juga dapat memeriksa log AWS CloudTrail untuk informasi tentang apakah pembuatan akun berhasil. Untuk informasi lebih lanjut, lihat Pencatatan dan pemantauan di AWS Organizations.
- Jika kesalahan berlanjut, kontak AWS Support.

Halaman Akun AWS akan muncul, dengan akun baru Anda ditambahkan ke daftar.

9. Setelah akun ada dan memiliki IAM role yang memberikan akses administrator ke pengguna di akun pengelolaan, Anda dapat mengakses akun dengan mengikuti langkah-langkah dalam Mengakses akun anggota di organisasi Anda.

> **Note**
>
> Saat Anda membuat akun, AWS Organizations awalnya menetapkan kata sandi yang panjang (64 karakter) dan kompleks yang dihasilkan secara acak ke pengguna akar. Anda tidak dapat mengambil kata sandi awal ini. Untuk mengakses akun sebagai pengguna akar untuk pertama kalinya, Anda harus melalui proses pemulihan kata sandi. Untuk informasi lebih lanjut, lihat Mengakses akun anggota sebagai pengguna akar.

AWS CLI & AWS SDKs

Untuk membuat Akun AWS yang secara otomatis menjadi bagian dari organisasi Anda

Anda dapat menggunakan salah satu perintah berikut untuk membuat akun:

- AWS CLI: create-account

```
$ aws organizations create-account \
    --email susan@example.com \
    --account-name "Production Account"
{
        "CreateAccountStatus": {
                "State": "IN_PROGRESS",
                "Id": "car-examplecreateaccountrequestid111"
        }
```

```
}
```

Anda kemudian dapat memeriksa status pembuatan akun dengan perintah berikut.

```
$ aws organizations describe-create-account-status \
    --create-account-request-id car-examplecreateaccountrequestid111
{
  "CreateAccountStatus": {
    "State": "SUCCEEDED",
    "AccountId": "555555555555",
    "AccountName": "Production account",
    "RequestedTimestamp": 1470684478.687,
    "CompletedTimestamp": 1470684532.472,
    "Id": "car-examplecreateaccountrequestid111"
  }
}
```

- AWSSDK: CreateAccount

Mengakses akun anggota di organisasi Anda

Saat Anda membuat akun di organisasi, selain pengguna root,AWS Organizations secara otomatis membuat IAM role yang secara default diberi nama `OrganizationAccountAccessRole`. Anda dapat menentukan nama yang berbeda saat membuatnya, namun sebaiknya Anda menamainya secara konsisten di semua akun Anda. Kami merujuk ke peran dalam panduan ini dengan nama default. AWS Organizationstidak membuat pengguna atau peran lain. Untuk mengakses akun di organisasi Anda, Anda harus menggunakan salah satu metode berikut:

- Saat Anda membuat Akun AWS, Anda memulai dengan satu identitas masuk yang memiliki akses penuh ke semua Layanan AWS dan sumber daya di akun tersebut. Identitas ini disebut pengguna root Akun AWS dan diakses dengan cara masuk menggunakan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari Anda. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar tugas lengkap yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM. Untuk rekomendasi keamanan pengguna root tambahan, lihat Praktik terbaik pengguna Root untuk Anda Akun AWS.
- Jika Anda membuat akun dengan menggunakan alat yang disediakan sebagai bagian dari AWS Organizations, Anda dapat mengakses akun dengan menggunakan peran yang telah dikonfigurasi

bernama `OrganizationAccountAccessRole` yang ada di semua akun baru yang Anda buat dengan cara ini. Untuk informasi selengkapnya, lihat Mengakses akun anggota yang memiliki peran akses akun pengelolaan.

- Jika Anda mengundang akun yang ada untuk bergabung dengan organisasi Anda dan akun tersebut menerima undangan, Anda kemudian dapat memilih untuk membuat IAM role yang memungkinkan akun pengelolaan mengakses akun anggota yang diundang. Peran ini dimaksudkan agar identik dengan peran yang ditambahkan secara otomatis ke akun yang dibuat dengan AWS Organizations. Untuk membuat peran ini, lihat Membuat akun anggota yang diundang OrganizationAccountAccessRole . Setelah membuat peran, Anda dapat mengaksesnya menggunakan langkah-langkah di Mengakses akun anggota yang memiliki peran akses akun pengelolaan.
- Gunakan AWS IAM Identity Centerdan aktifkan akses tepercaya untuk IAM Identity Center denganAWS Organizations. Hal ini memungkinkan pengguna untuk masuk ke portal AWS akses dengan kredensi perusahaan mereka dan mengakses sumber daya di akun manajemen atau akun anggota yang ditugaskan.

  Untuk informasi selengkapnya, lihat Izin multi-akun di AWS IAM Identity CenterPanduan Pengguna. Untuk informasi tentang menyiapkan akses tepercaya untuk Pusat Identitas IAM, lihatAWS IAM Identity Center dan AWS Organizations.

> **Izin minimum**
>
> Untuk mengakses Akun AWS dari akun lain di organisasi Anda, Anda harus memiliki izin berikut:
>
> - `sts:AssumeRole` — Elemen `Resource` harus diatur ke tanda bintang (*) atau nomor ID akun dengan pengguna yang perlu mengakses akun anggota baru

Mengakses akun anggota sebagai pengguna akar

Saat Anda membuat akun baru, AWS Organizations awalnya akan menetapkan kata sandi untuk pengguna akar yang terdiri dari minimal 64 karakter. Semua karakter yang dihasilkan secara acak tanpa jaminan pada penampilan rangkaian karakter tertentu. Anda tidak dapat mengambil kata sandi awal ini. Untuk mengakses akun sebagai pengguna akar untuk pertama kalinya, Anda harus melalui proses pemulihan kata sandi. Untuk informasi selengkapnya, lihat Saya lupa kata sandi pengguna root untuk saya Akun AWS di Panduan Pengguna AWS Masuk.

Catatan

- Sebagai praktik terbaik, kami menyarankan agar Anda tidak menggunakan pengguna akar untuk mengakses akun Anda kecuali untuk membuat pengguna dan peran lain dengan izin yang lebih terbatas. Setelah itu, masuk sebagai salah satu pengguna atau peran tersebut.
- Kami juga menyarankan Anda mengaktifkan otentikasi multi-faktor (MFA) pada pengguna root. Setel ulang kata sandi, dan tetapkan perangkat MFA ke pengguna akar.
- Jika Anda membuat akun anggota di organisasi dengan alamat email yang salah, maka Anda tidak dapat masuk ke akun sebagai pengguna akar. Kontak Penagihan dan Support AWS untuk mendapatkan bantuan.

Membuat akun anggota yang diundang OrganizationAccountAccessRole

Secara default, jika Anda membuat akun anggota sebagai bagian dari organisasi, AWS secara otomatis membuat peran dalam akun yang memberikan izin administrator untuk pengguna IAM di akun pengelolaan yang dapat mengambil peran tersebut. Secara default, peran diberi nama `OrganizationAccountAccessRole`. Untuk informasi lebih lanjut, lihat Mengakses akun anggota yang memiliki peran akses akun pengelolaan.

Namun, akun anggota yang Anda undang untuk bergabung dengan organisasi Anda tidak secara otomatis mendapatkan peran administrator yang dibuat. Anda harus melakukannya secara manual, seperti yang ditunjukkan dalam prosedur berikut. Hal ini pada dasarnya menduplikasi peran secara otomatis yang disiapkan untuk akun yang dibuat. Kami menyarankan agar Anda menggunakan nama yang sama, `OrganizationAccountAccessRole`, untuk peran Anda yang dibuat secara manual untuk konsistensi dan kemudahan mengingatnya.

AWS Management Console

Untuk membuat peran administrator AWS Organizations di akun anggota

1. Masuk ke konsol IAM dan di https://console.aws.amazon.com/iam/. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak disarankan) di akun anggota. Pengguna atau peran harus memiliki izin untuk membuat peran dan kebijakan IAM.
2. Di konsol IAM, navigasikan ke Peran dan kemudian pilih Buat peran.
3. Pilih Akun AWS, lalu pilih Lainnya Akun AWS.

4. Masukkan 12 digit nomor ID akun dari akun manajemen yang ingin Anda berikan akses administrator. Di bawah Opsi, harap perhatikan hal berikut:

   - Untuk peran ini, karena akun adalah internal perusahaan Anda, maka Anda harus tidak memilih Minta ID eksternal. Untuk informasi selengkapnya tentang opsi ID eksternal, lihat Kapan saya harus menggunakan ID eksternal? di Panduan Pengguna IAM.
   - Jika Anda telah mengaktifkan dan mengonfigurasi MFA, maka Anda dapat memilih untuk meminta autentikasi menggunakan perangkat MFA. Untuk informasi selengkapnya tentang MFA, lihat Menggunakan otentikasi multi-faktor (MFA) AWS di Panduan Pengguna IAM.

5. Pilih Berikutnya.
6. Pada halaman Tambahkan izin, pilih kebijakan AWS terkelola bernama, `AdministratorAccess` lalu pilih Berikutnya.
7. Pada halaman Nama, tinjau, dan buat, tentukan nama peran dan deskripsi opsional. Kami menyarankan agar Anda menggunakan `OrganizationAccountAccessRole`, agar konsisten dengan nama default yang ditetapkan ke peran di akun baru. Untuk melakukan perubahan Anda, pilih Buat peran.
8. Peran baru Anda akan muncul di daftar peran yang tersedia. Pilih nama peran baru untuk melihat detailnya, perhatikan dengan baik URL tautan yang disediakan. Berikan URL ini kepada pengguna di akun anggota yang perlu mengakses peran tersebut. Perhatikan juga ARN Peran karena Anda akan membutuhkannya di langkah 15.
9. Masuk ke konsol IAM dan di https://console.aws.amazon.com/iam/. Kali ini, masuk sebagai pengguna di akun pengelolaan yang memiliki izin untuk membuat kebijakan dan menetapkan kebijakan untuk pengguna atau grup.
10. Arahkan ke Kebijakan, lalu pilih Buat kebijakan.
11. Untuk Layanan, pilih STS.
12. Untuk Tindakan, mulai ketik **`AssumeRole`** di Filter dan pilih kotak centang di sampingnya saat muncul.
13. Di bawah Sumber Daya, pastikan Spesifik dipilih dan kemudian pilih Tambahkan ARN.
14. Masukkan nomor ID akun anggota AWS, lalu masukkan nama peran yang Anda buat sebelumnya di langkah 1–8. Pilih Tambahkan ARN.
15. Jika Anda memberikan izin untuk mengambil peran di beberapa akun anggota, ulangi langkah 14 dan 15 untuk setiap akun.
16. Pilih Berikutnya.

17. Pada halaman Tinjau dan buat, masukkan nama untuk kebijakan baru, lalu pilih Buat kebijakan untuk menyimpan perubahan.
18. Pilih Grup pengguna di panel navigasi lalu pilih nama grup (bukan kotak centang) yang ingin Anda gunakan untuk mendelegasikan administrasi akun anggota.
19. Pilih tab Izin.
20. Pilih Tambahkan izin, pilih Lampirkan kebijakan, lalu pilih kebijakan yang Anda buat di langkah 11—18.

Pengguna yang merupakan anggota grup yang dipilih sekarang dapat menggunakan URL yang Anda ambil di langkah 9 untuk mengakses peran dari setiap akun anggota. Mereka dapat mengakses akun anggota ini dengan cara yang sama seperti jika mengakses akun yang Anda buat di organisasi. Untuk informasi selengkapnya tentang penggunaan peran untuk mengelola akun anggota, lihat Mengakses akun anggota yang memiliki peran akses akun pengelolaan.

Mengakses akun anggota yang memiliki peran akses akun pengelolaan

Ketika Anda membuat akun anggota menggunakan konsol AWS Organizations, AWS Organizations secara otomatis membuat IAM role bernama `OrganizationAccountAccessRole` pada akun. Peran ini memiliki izin administratif penuh di akun anggota. Ruang lingkup akses untuk peran ini mencakup semua prinsip dalam akun manajemen, sehingga peran tersebut dikonfigurasi untuk memberikan akses ke akun manajemen organisasi. Anda dapat membuat peran yang sama untuk akun anggota yang diundang dengan mengikuti langkah-langkah di Membuat akun anggota yang diundang OrganizationAccountAccessRole . Untuk menggunakan peran ini untuk mengakses akun anggota, Anda harus masuk sebagai pengguna dari akun pengelolaan yang memiliki izin untuk mengambil peran tersebut. Untuk mengkonfigurasi izin ini, lakukan prosedur berikut. Kami merekomendasikan agar Anda memberikan izin ke grup bukan pengguna untuk kemudahan pemeliharaan.

AWS Management Console

Untuk memberikan izin kepada anggota grup IAM di akun pengelolaan untuk mengakses peran

1. Masuk ke konsol IAM di https://console.aws.amazon.com/iam/ dengan pengguna Anda yang memiliki izin administrator di akun pengelolaan. Hal ini diperlukan untuk mendelegasikan izin ke grup IAM pengguna yang akan mengakses peran dalam akun anggota itu.
2. Mulailah dengan membuat kebijakan terkelola yang Anda butuhkan nanti di ???.

Pada panel navigasi, pilih Kebijakan, lalu pilih Buat kebijakan.

3. Pada tab Editor Visual, pilih Pilih layanan, ketik **`STS`** di kotak pencarian untuk mem-filter daftar, lalu pilih kotak centang opsi STS.
4. Di bagian Tindakan, ketik **`assume`** kotak pencarian untuk memfilter daftar, lalu pilih AssumeRoleopsi.
5. Di bagian Sumber Daya, pilih Spesifik, pilih Tambahkan ARN, lalu ketik nomor akun anggota dan nama peran yang Anda buat di bagian sebelumnya (kami sarankan untuk menamainya`OrganizationAccountAccessRole`).
6. Pilih Tambahkan ARN saat kotak dialog menampilkan ARN yang benar.
7. (Opsional) Jika Anda ingin mewajibkan autentikasi multi faktor (MFA), atau membatasi akses ke peran dari rentang alamat IP tertentu, maka perluas bagian syarat Permintaan, dan pilih opsi yang ingin Anda terapkan.
8. Pilih Berikutnya.
9. Pada halaman Tinjau dan buat, masukkan nama untuk kebijakan baru. Sebagai contoh : **`GrantAccessToOrganizationAccountAccessRole`**. Anda juga dapat menambahkan deskripsi opsional.
10. Pilih Buat kebijakan untuk menyimpan kebijakan terkelola baru Anda.
11. Setelah kebijakan tersedia, Anda dapat melampirkannya ke grup.

    Di panel navigasi, pilih Grup pengguna lalu pilih nama grup (bukan kotak centang) yang anggotanya ingin Anda dapat mengambil peran di akun anggota. Jika perlu, Anda dapat membuat grup baru.
12. Pilih tab Izin, pilih Tambahkan izin, lalu pilih Lampirkan kebijakan.
13. (Opsional) Dalam kotak Pencarian, Anda dapat mulai mengetik nama kebijakan Anda untuk mem-filter daftar sampai Anda dapat melihat nama kebijakan Anda yang baru saja dibuat di Step 2 melalui Step 10. Anda juga dapat memfilter semua kebijakan AWS terkelola dengan memilih Semua jenis dan kemudian memilih Customer managed.
14. Centang kotak di samping kebijakan Anda, lalu pilih Lampirkan kebijakan.

Pengguna IAM yang merupakan anggota grup sekarang memiliki izin untuk beralih ke peran baru di konsol AWS Organizations dengan menggunakan prosedur berikut.

AWS Management Console

Untuk beralih ke peran akun anggota

Saat menggunakan peran, pengguna memiliki izin administrator di akun anggota baru. Instruksikan pengguna IAM Anda yang merupakan anggota grup untuk melakukan hal berikut untuk beralih ke peran baru.

1. Dari sudut kanan atas konsol AWS Organizations, pilih tautan yang berisi nama masuk Anda saat ini dan kemudian pilih Beralih Peran.
2. Masukkan nomor ID akun dan nama peran yang disediakan administrator.
3. Untuk Nama Tampilan, masukkan teks yang ingin Anda tampilkan di bilah navigasi di sudut kanan atas di tempat nama pengguna Anda saat Anda menggunakan peran tersebut. Anda dapat memilih warna secara opsional.
4. Pilih Ganti Peran. Sekarang semua tindakan yang Anda lakukan akan dilakukan dengan izin yang diberikan untuk peran yang Anda beralih padanya. Anda tidak lagi memiliki izin yang terkait dengan pengguna IAM asli Anda sampai Anda beralih kembali.
5. Setelah selesai melakukan tindakan yang memerlukan izin peran, Anda dapat beralih kembali ke pengguna IAM normal. Pilih nama peran di sudut kanan atas (apa pun yang Anda tentukan sebagai Nama Tampilan) lalu pilih Kembali ke. ***`UserName`***

Sumber daya tambahan

- Untuk informasi selengkapnya tentang pemberian izin untuk beralih peran, lihat Memberikan izin pengguna untuk beralih peran di Panduan Pengguna IAM.
- Untuk informasi selengkapnya tentang penggunaan peran yang telah diberikan izin untuk diasumsikan, lihat Beralih ke peran (konsol) di Panduan Pengguna IAM.
- Untuk tutorial tentang penggunaan peran untuk akses lintas akun, lihat Tutorial: Mendelegasikan akses Akun AWS menggunakan peran IAM dalam Panduan Pengguna IAM.
- Untuk informasi tentang menutup Akun AWS, lihat Menutup akun anggota di organisasi Anda.

Mengekspor Akun AWS detail untuk organisasi Anda

DenganAWS Organizations, pengguna akun manajemen dan administrator yang didelegasikan untuk organisasi dapat mengekspor file.csv dengan semua detail akun dalam organisasi.

Akibatnya, administrator organisasi dapat dengan mudah melihat akun dan memfilter berdasarkan status:`ACTIVE`,`SUSPENDED`, atau`PENDING`. Jika organisasi Anda memiliki banyak akun, opsi pengunduhan file.csv menyediakan cara mudah untuk melihat dan mengurutkan detail akun dalam spreadsheet.

Sebelumnya, satu-satunya cara untuk melihat akun adalah dengan melihat hierarki akun atau tampilan daftar di konsol. AWS Organizations

> **Note**
>
> Hanya kepala sekolah di akun manajemen yang dapat mengunduh daftar akun.

Mengekspor daftar semua Akun AWS di organisasi Anda

Saat masuk ke akun manajemen organisasi, Anda bisa mendapatkan daftar semua akun yang merupakan bagian dari organisasi Anda sebagai file.csv. Daftar ini berisi detail akun individual; namun, daftar tersebut tidak menentukan unit organisasi (OU) milik akun tersebut.

File.csv berisi informasi berikut untuk setiap akun:

- ID Akun - Pengidentifikasi akun numerik. Contoh: 123456789012
- ARN - Nama Sumber Daya Amazon untuk akun. Misalnya: `arn:aws:organizations::123456789012account/o-o1gb0d1234/123456789012`
- Email - Alamat email yang terkait dengan akun. Contoh: marymajor@example.com
- Nama - Nama akun yang disediakan oleh pembuat akun. Misalnya: akun pengujian tahap
- Status - Status akun dalam organisasi. Nilai bisa`PENDING`, `ACTIVE` atau`SUSPENDED`.
- Metode bergabung - Menentukan bagaimana akun dibuat. Nilai bisa `INVITED` atau`CREATED`.
- Bergabung timestamp - Tanggal dan waktu akun bergabung dengan organisasi.

> **Izin minimum**
>
> Untuk mengekspor file.csv dengan semua akun anggota di organisasi Anda, Anda harus memiliki izin berikut:
>
> - `organizations:DescribeOrganization`

- `organizations:ListAccounts`

AWS Management Console

Untuk mengekspor file.csv untuk semua Akun AWS di organisasi

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pilih Tindakan, lalu Akun AWSpilih Ekspor daftar akun. Spanduk biru di bagian atas halaman menunjukkan “Ekspor sedang berlangsung!”
3. Ketika file sudah siap, spanduk berubah menjadi hijau dan menunjukkan: “Unduh sudah siap!” Pilih Unduh CSV. File `Organization_accounts_information.csv` diunduh ke perangkat Anda.

AWS CLI & AWS SDKs

Satu-satunya cara untuk mengekspor file.csv dengan detail akun adalah dengan menggunakan file. AWS Management Console Anda tidak dapat mengekspor file.csv daftar akun menggunakan file. AWS CLI

Menghapus akun anggota dari organisasi Anda

Bagian dari mengelola akun dalam suatu organisasi adalah menghapus akun anggota yang tidak lagi Anda butuhkan. Menghapus akun anggota tidak menutup akun, melainkan menghapus akun anggota dari organisasi. Akun mantan anggota menjadi mandiri Akun AWS yang tidak lagi dikelola olehAWS Organizations. Setelah itu, akun tidak lagi tunduk pada kebijakan apa pun dan bertanggung jawab atas pembayaran tagihannya sendiri. Akun manajemen organisasi tidak lagi dikenakan biaya untuk setiap biaya yang timbul oleh akun setelah dihapus dari organisasi.

Untuk informasi tentang menghapus akun pengelolaan, lihat Menghapus organisasi.

Topik

- Pertimbangan sebelum menghapus akun dari organisasi
- Menghapus akun anggota dari organisasi Anda
- Tinggalkan organisasi dari akun anggota Anda

Pertimbangan sebelum menghapus akun dari organisasi

Sebelum Anda menghapus akun, penting untuk mempertimbangkan hal-hal berikut:

- Anda dapat menghapus akun dari organisasi Anda hanya jika akun tersebut memiliki informasi yang diperlukan untuk beroperasi sebagai akun mandiri. Saat Anda membuat akun di organisasi menggunakan AWS Organizations konsol, API, atau AWS CLI perintah, semua informasi yang diperlukan dari akun mandiri tidak dikumpulkan secara otomatis. Untuk setiap akun yang ingin Anda buat menjadi akun mandiri, Anda harus memilih paket support, menyediakan dan memverifikasi informasi kontak yang diperlukan, dan menyediakan metode pembayaran saat ini. AWS menggunakan metode pembayaran untuk mengenakan biaya untuk setiap aktivitas AWS (bukan Tingkat Gratis AWS) yang bisa ditagih yang terjadi saat akun tidak dilampirkan ke organisasi. Untuk menghapus akun yang belum memiliki informasi ini, ikuti langkah-langkahnyaTinggalkan organisasi dari akun anggota Anda.
- Untuk menghapus akun yang Anda buat di organisasi, Anda harus menunggu hingga setidaknya tujuh hari setelah akun dibuat. Akun yang diundang tidak dikenakan periode tunggu ini.
- Saat ini akun berhasil meninggalkan organisasi, pemilik Akun AWS menjadi bertanggung jawab untuk semua biaya AWS yang ditambahkan, dan metode pembayaran akun digunakan. Akun pengelolaan organisasi tidak lagi bertanggung jawab.
- Akun yang ingin Anda hapus tidak boleh menjadi akun administrator yang didelegasikan untuk layanan AWS apapun yang diaktifkan untuk organisasi Anda. Jika akun administrator didelegasikan, maka Anda harus terlebih dahulu mengubah akun administrator yang didelegasikan ke akun lain yang tersisa dalam organisasi. Untuk informasi selengkapnya tentang cara menonaktifkan atau mengubah akun administrator yang didelegasikan untuk suatu AWS layanan, lihat dokumentasi untuk layanan tersebut.
- Bahkan setelah penghapusan akun yang dibuat (akun yang dibuat menggunakan konsol AWS Organizations atau API `CreateAccount`) dari dalam suatu organisasi, (i) akun yang dibuat diatur oleh persyaratan yang ada dalam perjanjian antara akun pengelolaan yang membuat akun tersebut dengan kami, dan (ii) akun pengelolaan yang membuat akun tersebut tetap bertanggung jawab secara bersama dan secara terpisah atas tindakan yang dilakukan oleh akun yang dibuatnya. Perjanjian pelanggan dengan kami, serta hak dan kewajiban berdasarkan perjanjian tersebut, tidak dapat dialihkan atau ditransfer tanpa ada persetujuan sebelumnya dari kami. Untuk mendapatkan persetujuan kami, Hubungi AWS.
- Ketika akun anggota meninggalkan organisasi, akun itu tidak lagi memiliki akses ke data biaya dan penggunaan dari rentang waktu ketika akun masih menjadi anggota organisasi. Namun demikian,

akun pengelolaan organisasi masih dapat mengakses data. Jika akun tersebut bergabung kembali ke organisasi, maka akun tersebut dapat mengakses data itu lagi.

- Ketika akun anggota meninggalkan sebuah organisasi, semua tag yang dilampirkan ke akun akan dihapus.
- Saat Anda menghapus akun anggota dari organisasi, peran IAM apa pun yang dibuat untuk mengaktifkan akses oleh akun manajemen organisasi tidak akan dihapus secara otomatis. Jika Anda ingin menghentikan akses ini dari akun manajemen organisasi sebelumnya, Anda harus menghapus peran IAM secara manual. Untuk informasi tentang menghapus peran, lihat Menghapus peran atau profil instans dalam Panduan Pengguna IAM.

Efek menghapus akun dari sebuah organisasi

Bila Anda menghapus akun dari sebuah organisasi, tidak ada perubahan langsung yang akan terjadi pada akun. Namun, efek tidak langsung berikut ini akan terjadi:

- Akun sekarang bertanggung jawab untuk membayar biaya sendiri dan harus memiliki metode pembayaran yang valid yang dilampirkan pada akun.
- Prinsipal utama dalam akun tidak lagi terpengaruh oleh kebijakan yang diterapkan dalam organisasi. Ini berarti bahwa pembatasan yang diberlakukan oleh SCP hilang, dan pengguna serta peran dalam akun mungkin memiliki lebih banyak izin daripada sebelumnya. Jenis kebijakan organisasi lainnya tidak dapat lagi ditegakkan atau diproses.
- Jika Anda menggunakan kunci syarat `aws:PrincipalOrgID` apapun untuk membatasi akses hanya ke pengguna dan peran dari Akun AWS di organisasi Anda, maka Anda harus meninjau, dan mungkin memperbarui kebijakan ini sebelum menghapus akun anggota. Jika Anda tidak memperbarui kebijakan, maka kemudian pengguna dan peran di akun dapat kehilangan akses ke sumber daya saat akun meninggalkan organisasi.
- Integrasi dengan layanan lain mungkin dinonaktifkan. Jika Anda menghapus akun dari organisasi yang memiliki integrasi dengan AWS, maka pengguna di akun tersebut tidak dapat lagi menggunakan layanan tersebut.

Menghapus akun anggota dari organisasi Anda

Saat masuk ke akun pengelolaan organisasi, Anda dapat menghapus akun anggota dari organisasi yang tidak lagi diperlukan. Untuk melakukannya, selesaikan prosedur berikut. Prosedur ini hanya berlaku untuk akun anggota. Untuk menghapus akun pengelolaan, Anda harus menghapus organisasi.

Note

Jika akun anggota dihapus dari organisasi, maka akun anggota tersebut tidak akan lagi tercakup oleh perjanjian organisasi. Administrator akun pengelolaan harus menyampaikan hal ini ke akun anggota sebelum menghapus akun anggota dari organisasi, sehingga akun anggota dapat menempatkan perjanjian baru jika diperlukan. Daftar perjanjian organisasi aktif dapat dilihat di konsol AWS Artifact yang ada di halaman Perjanjian Organisasi AWS Artifact.

Izin minimum

Untuk menghapus satu atau beberapa akun anggota dari organisasi, Anda harus masuk sebagai pengguna atau peran di akun manajemen dengan izin berikut:

- `organizations:DescribeOrganization` — hanya diperlukan bila menggunakan konsol Organizations
- `organizations:RemoveAccountFromOrganization`

Jika Anda memilih untuk masuk sebagai pengguna atau peran di akun anggota di langkah 5, maka pengguna atau peran tersebut harus memiliki izin berikut:

- `organizations:DescribeOrganization` — hanya diperlukan bila menggunakan konsol Organizations.
- `organizations:LeaveOrganization` — Perhatikan bahwa administrator organisasi dapat menerapkan kebijakan ke akun yang menghapus izin ini, sehingga akan mencegah Anda menghapus akun dari organisasi.
- Jika Anda masuk sebagai pengguna IAM dan akun tidak memiliki informasi pembayaran, pengguna harus memiliki salah satu `aws-portal:ModifyBilling` dan `aws-portal:ModifyPaymentMethods` izin (jika akun belum bermigrasi ke izin berbutir halus) ATAU `payments:CreatePaymentInstrument` dan `payments:UpdatePaymentPreferences` izin (jika akun telah bermigrasi ke izin berbutir halus). Selain itu, akun anggota harus mengaktifkan akses pengguna IAM ke penagihan. Jika ini belum diaktifkan, lihat Mengaktifkan Akses ke Konsol Manajemen Penagihan dan Biaya di Panduan Pengguna AWS Billing.

AWS Management Console

Untuk menghapus akun anggota dari organisasi Anda

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Akun AWS, temukan dan pilih kotak centang
   yang ada di samping setiap akun anggota yang ingin Anda hapus dari organisasi Anda. Anda dapat membuka hirarki OU atau mengaktifkan Lihat Akun AWS Saja untuk melihat daftar datar akun tanpa struktur OU. Jika Anda memiliki banyak akun, Anda mungkin harus memilih Muat lebih banyak akun di 'ou-nama' di bagian bawah daftar untuk menemukan semua akun yang ingin Anda pindahkan.

   Pada halaman Akun AWS, temukan dan pilih nama akun anggota yang ingin dihapus dari organisasi Anda. Anda mungkin harus memperluas OU (pilih) untuk menemukan akun yang Anda inginkan.
3. Pilih Tindakan, lalu di bawah Akun AWS, pilih Hapus dari organisasi.
4. Dalam Hapus akun 'account-name' (# account-id-num) dari organisasi? kotak dialog, pilih Hapus akun.
5. Jika AWS Organizations gagal untuk menghapus satu atau beberapa akun, hal itu biasanya karena Anda belum memberikan semua informasi yang diperlukan kepada akun tersebut untuk beroperasi sebagai akun mandiri. Lakukan langkah-langkah berikut ini:

   a. Masuk ke akun yang gagal. Sebaiknya Anda masuk ke akun anggota dengan memilih Salin tautan, lalu menempelkannya ke bilah alamat jendela peramban penyamaran baru. Jika Anda tidak menggunakan jendela penyamaran, maka Anda akan keluar dari akun pengelolaan dan tidak dapat membuka kembali ke kotak dialog ini.

   b. Peramban membawa Anda langsung ke proses pendaftaran untuk menyelesaikan langkah-langkah yang hilang untuk akun ini. Selesaikan semua langkah yang disajikan. Langkah-lamgkah tersebut mungkin mencakup yang berikut ini:

      - Memberikan informasi kontak
      - Memberikan metode pembayaran yang valid
      - Memverifikasi nomor telepon

- Memilih opsi paket support

c. Setelah Anda menyelesaikan langkah pendaftaran terakhir, AWS secara otomatis mengalihkan peramban Anda ke konsol AWS Organizations untuk akun anggota. Pilih Meninggalkan organisasi, dan kemudian konfirmasikan pilihan Anda di kotak dialog konfirmasi. Anda diarahkan ke halaman Memulai di konsol AWS Organizations, di mana Anda dapat melihat undangan tertunda untuk akun Anda untuk bergabung dengan organisasi lain.

d. Menghapus IAM role yang memberikan akses ke akun Anda dari organisasi.

> **Important**
>
> Jika akun Anda dibuat di Organizations, maka Organisasi secara otomatis membuat IAM role di akun yang mengaktifkan akses oleh akun pengelolaan organisasi. Jika akun diundang untuk bergabung, maka Organizations tidak akan secara otomatis membuat peran seperti itu, tetapi Anda atau administrator lain mungkin telah membuatnya untuk mendapatkan manfaat yang sama. Dalam kedua kasus di atas, bila Anda menghapus akun dari organisasi, peran tersebut tidak akan dihapus secara otomatis. Jika Anda ingin menghentikan akses ini dari akun pengelolaan organisasi sebelumnya, maka Anda harus secara manual menghapus IAM role ini. Untuk informasi tentang menghapus peran, lihat Menghapus peran atau profil instans dalam Panduan Pengguna IAM.

AWS CLI & AWS SDKs

Untuk menghapus akun anggota dari organisasi Anda

Anda dapat menggunakan salah satu perintah berikut untuk menghapus akun anggota:

- AWS CLI: remove-account-from-organization

```
$ aws organizations remove-account-from-organization \
    --account-id 123456789012
```

Perintah ini tidak menghasilkan output saat berhasil.

- AWSSDK: RemoveAccountFromOrganization

Setelah akun anggota dihapus dari organisasi, pastikan untuk menghapus peran IAM yang memberikan akses ke akun Anda dari organisasi.

> **Important**
>
> Jika akun Anda dibuat di Organizations, maka Organisasi secara otomatis membuat IAM role di akun yang mengaktifkan akses oleh akun pengelolaan organisasi. Jika akun diundang untuk bergabung, maka Organizations tidak akan secara otomatis membuat peran seperti itu, tetapi Anda atau administrator lain mungkin telah membuatnya untuk mendapatkan manfaat yang sama. Dalam kedua kasus di atas, bila Anda menghapus akun dari organisasi, peran tersebut tidak akan dihapus secara otomatis. Jika Anda ingin menghentikan akses ini dari akun pengelolaan organisasi sebelumnya, maka Anda harus secara manual menghapus IAM role ini. Untuk informasi tentang menghapus peran, lihat Menghapus peran atau profil instans dalam Panduan Pengguna IAM.

Akun anggota dapat menghapus diri mereka sendiri dengan cuti organisasi sebagai gantinya. Untuk informasi selengkapnya, lihat Tinggalkan organisasi dari akun anggota Anda.

Tinggalkan organisasi dari akun anggota Anda

Saat masuk ke akun anggota, Anda dapat menghapus akun tersebut dari organisasinya. Untuk melakukannya, selesaikan prosedur berikut. Prosedur ini hanya berlaku untuk akun anggota. Akun pengelolaan tidak dapat meninggalkan organisasi menggunakan teknik ini. Untuk menghapus akun pengelolaan, Anda harus menghapus organisasi.

> **Note**
>
> Status akun dengan organisasi memengaruhi biaya dan data penggunaan yang terlihat:
>
> - Jika akun anggota meninggalkan organisasi dan menjadi akun mandiri, maka akun tidak lagi memiliki akses ke data biaya dan penggunaan dari rentang waktu ketika akun menjadi anggota organisasi. Akun hanya memiliki akses ke data yang dihasilkan sebagai akun mandiri.
> - Jika akun anggota meninggalkan organisasi A untuk bergabung dengan organisasi B, maka akun tidak lagi memiliki akses ke data biaya dan penggunaan dari rentang waktu ketika akun masih menjadi anggota organisasi A. Akun memiliki akses hanya ke data yang dihasilkan sebagai anggota organisasi B.

- Jika akun bergabung kembali ke organisasi di mana sebelumnya ia menjadi bagian darinya, maka akun tersebut akan kembali mendapatkan akses ke data biaya dan penggunaan historis.

Important

Jika Anda meninggalkan organisasi, Anda tidak lagi tercakup oleh perjanjian organisasi yang disetujui atas nama Anda oleh akun pengelolaan organisasi. Anda dapat melihat daftar perjanjian organisasi ini di konsol AWS Artifact pada halaman Perjanjian OrganisasiAWS Artifact. Sebelum meninggalkan organisasi, Anda harus menentukan (dengan bantuan tim legal, privasi, atau kepatuhan Anda jika diperlukan) apakah perlu bagi Anda untuk memiliki perjanjian(-perjanjian) baru.

Izin minimum

Untuk meninggalkan AWS, Anda harus memiliki izin berikut:

- `organizations:DescribeOrganization` — hanya diperlukan bila menggunakan konsol Organizations.
- `organizations:LeaveOrganization` — Perhatikan bahwa administrator organisasi dapat menerapkan kebijakan ke akun yang menghapus izin ini, sehingga akan mencegah Anda menghapus akun dari organisasi.
- Jika Anda masuk sebagai pengguna IAM dan akun tidak memiliki informasi pembayaran, pengguna harus memiliki salah satu `aws-portal:ModifyBilling` dan `aws-portal:ModifyPaymentMethods` izin (jika akun belum bermigrasi ke izin berbutir halus) ATAU `payments:CreatePaymentInstrument` dan `payments:UpdatePaymentPreferences` izin (jika akun telah bermigrasi ke izin berbutir halus). Selain itu, akun anggota harus mengaktifkan akses pengguna IAM ke penagihan. Jika ini belum diaktifkan, lihat Mengaktifkan Akses ke Konsol Manajemen Penagihan dan Biaya di Panduan Pengguna AWS Billing.

AWS Management Console

Untuk meninggalkan organisasi dari akun anggota Anda

1. Masuk ke konsol AWS Organizations di konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak direkomendasikan) di akun anggota.

   Secara default, Anda tidak memiliki akses ke kata sandi pengguna akar di akun anggota yang dibuat menggunakan AWS Organizations. Jika diperlukan, pulihkan sandi pengguna akar dengan mengikuti langkah-langkah di Mengakses akun anggota sebagai pengguna akar.
2. Pada halaman Dasbor Organisasi, pilih Tinggalkan organisasi ini.
3. Dalam Konfirmasi meninggalkan organisasi? kotak dialog, pilih Tinggalkan organisasi. Saat diminta, konfirmasikan pilihan Anda untuk menghapus akun. Setelah dikonfirmasi, Anda akan diarahkan ke halaman Memulai AWS Organizations konsol, di mana Anda dapat melihat undangan yang tertunda untuk akun Anda untuk bergabung dengan organisasi lain.

   Jika Anda melihat pesan Anda belum dapat meninggalkan organisasi, akun Anda tidak memiliki semua informasi yang diperlukan untuk beroperasi sebagai akun mandiri. Jika ini masalahnya, lanjutkan ke langkah berikutnya.
4. Jika Konfirmasi meninggalkan organisasi? kotak dialog menampilkan pesan Anda belum dapat meninggalkan organisasi, pilih tautan Lengkapi langkah pendaftaran akun.
5. Pada AWS halaman Daftar, masukkan semua informasi yang diperlukan agar ini menjadi akun mandiri. Ini mungkin termasuk jenis informasi berikut:

   - Nama dan alamat kontak
   - Metode pembayaran yang valid
   - Verifikasi nomor telepon
   - Opsi paket Support
6. Ketika Anda melihat kotak dialog yang menyatakan bahwa proses pendaftaran selesai, pilih Meninggalkan organisasi.

   Sebuah kotak dialog konfirmasi kemudian muncul. Konfirmasikan pilihan Anda untuk menghapus akun. Anda diarahkan ke halaman Memulai di konsol AWS Organizations, di mana Anda dapat melihat undangan tertunda untuk akun Anda untuk bergabung dengan organisasi lain.
7. Menghapus IAM role yang memberikan akses ke akun Anda dari organisasi.

> **Important**
>
> Jika akun Anda dibuat di Organizations, maka Organisasi secara otomatis membuat IAM role di akun yang mengaktifkan akses oleh akun pengelolaan organisasi. Jika akun diundang untuk bergabung, maka Organizations tidak akan secara otomatis membuat peran seperti itu, tetapi Anda atau administrator lain mungkin telah membuatnya untuk mendapatkan manfaat yang sama. Dalam kedua kasus di atas, bila Anda menghapus akun dari organisasi, peran tersebut tidak akan dihapus secara otomatis. Jika Anda ingin menghentikan akses ini dari akun pengelolaan organisasi sebelumnya, maka Anda harus secara manual menghapus IAM role ini. Untuk informasi tentang menghapus peran, lihat Menghapus peran atau profil instans dalam Panduan Pengguna IAM.

AWS CLI & AWS SDKs

Untuk meninggalkan organisasi sebagai akun anggota

Anda dapat menggunakan salah satu perintah berikut untuk meninggalkan sebuah organisasi:

- AWS CLI: leave-organization

  Contoh berikut menyebabkan akun yang kredensialnya digunakan untuk menjalankan perintah untuk meninggalkan organisasi.

  ```
  $ aws organizations leave-organization
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWSSDK: LeaveOrganization

Setelah akun anggota meninggalkan organisasi, pastikan untuk menghapus peran IAM yang memberikan akses ke akun Anda dari organisasi.

> **Important**
>
> Jika akun Anda dibuat di Organizations, maka Organisasi secara otomatis membuat IAM role di akun yang mengaktifkan akses oleh akun pengelolaan organisasi. Jika akun

diundang untuk bergabung, maka Organizations tidak akan secara otomatis membuat peran seperti itu, tetapi Anda atau administrator lain mungkin telah membuatnya untuk mendapatkan manfaat yang sama. Dalam kedua kasus di atas, bila Anda menghapus akun dari organisasi, peran tersebut tidak akan dihapus secara otomatis. Jika Anda ingin menghentikan akses ini dari akun pengelolaan organisasi sebelumnya, maka Anda harus secara manual menghapus IAM role ini. Untuk informasi tentang menghapus peran, lihat Menghapus peran atau profil instans dalam Panduan Pengguna IAM.

Akun anggota juga dapat dihapus oleh pengguna di akun manajemen dengan remove-account-from-organizationsebagai gantinya. Untuk informasi selengkapnya, lihat Menghapus akun anggota dari organisasi Anda.

Menutup akun anggota di organisasi Anda

Jika Anda tidak lagi memerlukan akun anggota di organisasi Anda, Anda dapat menutupnya dari AWS Organizations konsol mengikuti petunjuk di bagian ini. Anda hanya dapat menutup akun anggota menggunakan AWS Organizations konsol jika organisasi Anda dalam mode Semua fitur.

Anda juga dapat menutup Akun AWS langsung dari halaman Akun di AWS Management Console setelah masuk sebagai pengguna root. Untuk step-by-step petunjuk, lihat Menutup Akun AWS di Panduan Manajemen AWS Akun.

Untuk menutup akun manajemen, lihatMenutup akun manajemen di organisasi Anda.

Cara menutup akun anggota

Saat masuk ke akun manajemen organisasi, Anda dapat menutup akun anggota yang merupakan bagian dari organisasi Anda. Untuk melakukan ini, selesaikan langkah-langkah berikut.

Important

Sebelum Anda menutup akun anggota Anda, kami sangat menyarankan Anda meninjau pertimbangan dan memahami dampaknya untuk menutup akun. Untuk informasi selengkapnya, lihat Apa yang perlu Anda ketahui sebelum menutup akun dan Apa yang diharapkan setelah menutup akun di Panduan Manajemen AWS Akun.

AWS Management Console

Untuk menutup akun anggota dari AWS Organizations konsol

1. Masuk ke konsol AWS Organizations tersebut.
2. Pada Akun AWShalaman, temukan dan pilih nama akun anggota yang ingin Anda tutup. Anda dapat menavigasi hierarki OU, atau melihat daftar datar akun tanpa struktur OU.
3. Pilih Tutup di sebelah nama akun di bagian atas halaman. Organizations dalam mode penagihan Konsolidasi tidak akan dapat melihat tombol Tutup di konsol. Untuk menutup akun dalam mode penagihan konsolidasi, ikuti langkah-langkah di tab Akun mandiri dari Cara menutup akun Anda di Panduan Manajemen AWS Akun.
4. Pilih setiap kotak centang untuk mengetahui semua laporan penutupan akun yang diperlukan.
5. Masukkan ID akun anggota, lalu pilih Tutup akun.

> **Note**
>
> Setiap akun anggota yang Anda tutup akan menampilkan `SUSPENDED` label di sebelah nama akunnya di AWS Organizations konsol.

Untuk menutup akun anggota dari halaman Akun

Secara opsional, Anda dapat menutup akun AWS anggota langsung dari halaman Akun di. AWS Management Console Untuk step-by-step panduan, ikuti petunjuk di Close an Akun AWS in the AWS Account Management Guide.

AWS CLI & AWS SDKs

Untuk menutup sebuah Akun AWS

Anda dapat menggunakan salah satu perintah berikut untuk menutup AWS akun:

- AWS CLI: tutup akun

```
$ aws organizations close-account \
    --account-id 123456789012
```

Perintah ini tidak menghasilkan output saat berhasil.

- AWS SDK: CloseAccount

Melindungi akun anggota dari penutupan

Jika Anda ingin melindungi akun anggota dari penutupan yang tidak disengaja, Anda dapat membuat kebijakan IAM untuk menentukan akun mana yang dibebaskan dari penutupan. Setiap akun anggota yang dilindungi dengan kebijakan ini tidak dapat ditutup. Ini tidak dapat dicapai dengan SCP, karena mereka tidak mempengaruhi kepala sekolah di akun manajemen.

Anda dapat membuat kebijakan IAM yang menolak penutupan akun dengan salah satu dari dua cara:

- Secara eksplisit mencantumkan setiap akun yang ingin Anda lindungi dalam kebijakan dengan memasukkan elemen `arn` dalam`Resource`. Untuk melihat contoh, lihatMencegah akun anggota yang tercantum dalam kebijakan ini agar tidak ditutup.
- Tandai akun individu untuk mencegahnya ditutup. Gunakan kunci kondisi global `aws:ResourceTag` tag dalam kebijakan Anda untuk mencegah akun dengan tag ditutup. Untuk mempelajari cara menandai akun, lihat Menandai sumber daya Organizations. Untuk melihat contoh, lihatMencegah akun anggota dengan tag agar tidak ditutup .

Contoh kebijakan IAM yang mencegah penutupan akun anggota

Contoh kode berikut menunjukkan dua metode berbeda yang dapat Anda gunakan untuk membatasi akun anggota agar tidak menutup akun mereka.

Mencegah akun anggota dengan tag agar tidak ditutup

Anda dapat melampirkan kebijakan berikut ke identitas di akun manajemen Anda. Kebijakan ini mencegah prinsipal di akun manajemen menutup akun anggota yang ditandai dengan kunci kondisi global `aws:ResourceTag` tag, kunci, dan nilai `AccountType` tag. `Critical`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PreventCloseAccountForTaggedAccts",
            "Effect": "Deny",
            "Action": "organizations:CloseAccount",
            "Resource": "*",
```

```
            "Condition": {
                "StringEquals": {"aws:ResourceTag/AccountType": "Critical"}
            }
        }
    ]
}
```

Mencegah akun anggota yang tercantum dalam kebijakan ini agar tidak ditutup

Anda dapat melampirkan kebijakan berikut ke identitas di akun manajemen Anda. Kebijakan ini mencegah prinsipal di akun manajemen menutup akun anggota yang secara eksplisit ditentukan dalam elemen. `Resource`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PreventCloseAccount",
            "Effect": "Deny",
            "Action": "organizations:CloseAccount",
            "Resource": [
                "arn:aws:organizations::555555555555:account/
o-12345abcdef/123456789012",
                "arn:aws:organizations::555555555555:account/
o-12345abcdef/123456789014"
            ]
        }
    ]
}
```

Menutup akun manajemen di organisasi Anda

Untuk menutup akun manajemen di organisasi Anda, Anda harus terlebih dahulu menutup atau menghapus semua akun anggota di organisasi. Tindakan menutup akun manajemen juga menghapus contoh AWS Organizations dan kebijakan apa pun yang Anda buat di dalam organisasi tersebut setelah periode pasca-penutupan berakhir.

Cara menutup akun manajemen

Gunakan prosedur berikut untuk menutup akun manajemen.

> **Important**
>
> Sebelum Anda menutup akun manajemen Anda, kami sangat menyarankan agar Anda meninjau pertimbangan dan memahami dampaknya untuk menutup akun. Untuk informasi selengkapnya, lihat Apa yang perlu Anda ketahui sebelum menutup akun Anda dan Apa yang diharapkan setelah Anda menutup akun Anda di Panduan Manajemen AWS Akun.

AWS Management Console

Untuk menutup akun manajemen dari halaman Akun

> **Note**
>
> Anda tidak dapat menutup akun manajemen langsung dari AWS Organizations konsol.

1. Masuk ke AWS Management Console sebagai pengguna root untuk akun manajemen yang ingin Anda tutup. Anda tidak dapat menutup akun saat masuk sebagai pengguna atau peran IAM.
2. Verifikasi bahwa tidak ada akun anggota aktif yang tersisa di organisasi Anda. Untuk melakukan ini, buka AWS Organizations konsol, dan pastikan semua akun anggota ditampilkan di `Suspended` sebelah nama akun mereka. Jika Anda memiliki akun anggota yang masih aktif, Anda harus mengikuti panduan yang diberikan Menutup akun anggota di organisasi Anda sebelum Anda dapat melanjutkan ke langkah berikutnya.
3. Pada bilah navigasi di sudut kanan atas, pilih nama atau nomor akun Anda, lalu pilih Akun.
4. Pada halaman Akun, gulir ke bagian bawah halaman ke bagian Tutup akun. Baca dan pastikan Anda memahami proses penutupan akun.
5. Pilih tombol Tutup akun untuk memulai proses penutupan akun.
6. Dalam beberapa menit, Anda akan menerima konfirmasi email bahwa akun Anda telah ditutup.

AWS CLI & AWS SDKs

Tugas ini tidak didukung di AWS CLI atau oleh operasi API dari salah satu AWS SDK. Anda dapat melakukan tugas ini hanya dengan menggunakan AWS Management Console.

Memperbarui kontak alternatif di organisasi

Anda dapat memperbarui kontak alternatif untuk akun dalam Organizations Anda menggunakan konsolAWS Organisasi, atau secara terprogram menggunakanAWS CLI atauAWS SDK. Untuk mempelajari cara memperbarui kontak alternatif, lihat Mengakses atau memperbarui kontak alternatif di Referensi ManajemenAWS Akun.

Memperbarui informasi kontak utama di organisasi

Anda dapat memperbarui informasi kontak utama untuk akun dalam Organizations Anda menggunakan konsolAWS Organisasi, atau secara terprogram menggunakanAWS CLI atauAWS SDK. Untuk mempelajari cara memperbarui informasi kontak utama, lihat Mengakses atau memperbarui kontak akun utama di Referensi ManajemenAWS Akun.

Mengaktifkan pembaruanWilayah AWS di organisasi Anda

Anda dapat memperbarui diaktifkanWilayah AWS untuk account dalam organisasi Anda menggunakanAWS Organizations konsol. Untuk mempelajari cara memperbarui diaktifkanWilayah AWS, lihat MenentukanWilayah AWS akun yang dapat digunakan dalam Referensi ManajemenAWS Akun.

Mengelola kebijakan di AWS Organizations

Kebijakan dalam AWS Organizations memungkinkan Anda untuk menerapkan jenis manajemen tambahan ke Akun AWS dalam organisasi Anda. Anda dapat menggunakan kebijakan saat semua fitur diaktifkan di organisasi Anda.

AWS Organizations Konsol menampilkan status diaktifkan atau dinonaktifkan untuk setiap jenis kebijakan. Pada tab Mengatur akun, pilih `Root` di panel navigasi yang ada di sebelah kiri. Panel detail yang ada di sisi kanan layar menampilkan semua jenis kebijakan yang tersedia. Daftar tersebut menunjukkan mana yang diaktifkan dan yang dinonaktifkan dalam root organisasi tersebut. Jika opsi untuk Mengaktifkan sebuah tipe tersedia, maka tipe tersebut saat ini dinonaktifkan. Jika opsi untuk Menonaktifkan sebuah tipe tersedia, maka tipe tersebut saat ini diaktifkan.

Tipe kebijakan

Organizations menawarkan tipe kebijakan pada dua kategori luas berikut ini:

Kebijakan otorisasi

Kebijakan otorisasi membantu Anda untuk mengelola keamanan Akun AWS di organisasi Anda.

- Kebijakan Kontrol Layanan (SCP) menawarkan kontrol pusat atas izin maksimum yang tersedia untuk semua akun di organisasi Anda.

Kebijakan pengelolaan

Kebijakan manajemen memungkinkan Anda mengonfigurasi dan mengelola AWS layanan dan fitur-fiturnya secara terpusat.

- Kebijakan menolak layanan Kecerdasan Buatan (AI) memungkinkan Anda untuk mengendalikan pengumpulan data pada layanan AI AWS di seluruh akun organisasi Anda.
- Kebijakan Backup membantu Anda mengelola dan menerapkan rencana cadangan secara terpusat ke AWS sumber daya di seluruh akun organisasi Anda.
- Kebijakan tag membantu Anda menstandarisasi tag yang dilampirkan ke AWS sumber daya di akun organisasi Anda.

Tabel berikut merangkum beberapa karakteristik dari masing-masing jenis kebijakan. Untuk karakteristik tambahan tentang jenis kebijakan ini, lihatKuota untuk AWS Organizations.

Tipe kebijakan	Mempengaruhi akun pengelolaan	Jumlah maksimum yang dapat Anda lampirkan pada root, OU, atau akun	Ukuran maksimum	Men-support melihat kebijakan efektif pada OU atau akun
SCP	 T	5	5120 karakter	 Tidak
kebijakan menolak layanan AI	 Y	5	2500 karakter	 Ya
Kebijakan Backup	 Y	10	10.000 karakter	 Ya
Kebijakan tag	 Y	10	10.000 karakter	 Ya

Menggunakan kebijakan di organisasi Anda

- Mengaktifkan dan menonaktifkan jenis kebijakan
- Mendapatkan informasi tentang kebijakan organisasi Anda
- Administrator yang didelegasikan untuk AWS Organizations
- Kebijakan pengelolaan
- Kebijakan Pengendalian Layanan (SCPs)

Mengaktifkan dan menonaktifkan jenis kebijakan

Mengaktifkan jenis kebijakan

Sebelum Anda dapat membuat dan melampirkan kebijakan ke organisasi Anda, Anda harus mengaktifkan jenis kebijakan tersebut untuk digunakan. Mengaktifkan jenis kebijakan adalah tugas satu kali pada root organisasi. Anda dapat mengaktifkan jenis kebijakan hanya dari akun pengelolaan organisasi.

Izin minimum

Untuk mengaktifkan sebuah jenis kebijakan, Anda memerlukan izin untuk menjalankan tindakan-tindakan berikut:

- `organizations:EnablePolicyType`
- `organizations:DescribeOrganization` — hanya diperlukan bila menggunakan konsol Organizations
- `organizations:ListRoots` — hanya diperlukan bila menggunakan konsol Organizations

AWS Management Console

Untuk mengaktifkan sebuah jenis kebijakan

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Kebijakan, pilih nama jenis kebijakan yang ingin Anda aktifkan.
3. Pada halaman jenis kebijakan, pilih Aktifkan ***jenis kebijakan***.

   Halaman tersebut diganti dengan daftar kebijakan yang tersedia dari jenis yang ditentukan.

AWS CLI & AWS SDKs

Untuk mengaktifkan sebuah jenis kebijakan

Anda dapat menggunakan salah satu perintah berikut untuk mengaktifkan sebuah jenis kebijakan:

- AWS CLI: enable-policy-type

  Contoh berikut menunjukkan cara mengaktifkan kebijakan backup untuk organisasi Anda. Perhatikan bahwa Anda harus menentukan ID root organisasi Anda.

```
$ aws organizations enable-policy-type \
    --root-id r-a1b2 \
    --policy-type BACKUP_POLICY
{
    "Root": {
        "Id": "r-a1b2",
        "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
        "Name": "Root",
        "PolicyTypes": [
            {
                "Type": "BACKUP_POLICY",
                "Status": "ENABLED"
            }
        ]
    }
}
```

  Daftar `PolicyTypes` dalam output sekarang menyertakan jenis kebijakan yang ditentukan dengan `Status` dari `ENABLED`.

- AWSSDK: EnablePolicyType

Menonaktifkan sebuah jenis kebijakan

Jika Anda tidak ingin menggunakan jenis kebijakan tertentu di organisasi Anda, maka Anda dapat menonaktifkan jenis kebijakan tersebut untuk mencegah penggunaan yang tidak disengaja. Anda dapat menonaktifkan jenis kebijakan dari akun pengelolaan organisasi saja.

Important

- Bila Anda menonaktifkan jenis kebijakan, semua kebijakan jenis yang ditentukan secara otomatis dilepaskan dari semua entitas di root organisasi. Kebijakan tidak dihapus.
- (Jenis kebijakan kontrol layanan kebijakan saja) Jika Anda mengaktifkan kembali jenis kebijakan SCP nanti, maka semua entitas dalam organisasi root awalnya hanya dilampirkan ke SCP `FullAWSAccess` default saja. Lampiran SCP untuk entitas hilang

ketika SCP dinonaktifkan dalam organisasi tersebut. Jika nanti Anda ingin mengaktifkan kembali SCP, maka Anda harus melampirkannya kembali ke root organisasi, OU, dan akun, sesuai keadaan.

Izin minimum

Untuk menonaktifkan SCP, Anda memerlukan izin untuk menjalankan tindakan-tindakan berikut:

- `organizations:DisablePolicyType`
- `organizations:DescribeOrganization` — hanya diperlukan bila menggunakan konsol Organizations
- `organizations:ListRoots` — hanya diperlukan bila menggunakan konsol Organizations

AWS Management Console

Untuk menonaktifkan sebuah jenis kebijakan

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Kebijakan, pilih nama jenis kebijakan yang ingin Anda nonaktifkan.
3. Pada halaman jenis kebijakan, pilih Nonaktifkan ***jenis kebijakan***.
4. Di kotak dialog konfirmasi, masukkan kata **`disable`**, lalu pilih Nonaktifkan.

   Daftar kebijakan yang tersedia dari jenis tertentu menghilang.

AWS CLI & AWS SDKs

Untuk menonaktifkan sebuah jenis kebijakan

Anda dapat menggunakan salah satu perintah berikut untuk menonaktifkan sebuah jenis kebijakan:

- AWS CLI: disable-policy-type

Contoh berikut menunjukkan cara menonaktifkan kebijakan backup untuk organisasi Anda. Perhatikan bahwa Anda harus menentukan ID root organisasi Anda.

```
$ aws organizations disable-policy-type \
    --root-id r-a1b2 \
    --policy-type BACKUP_POLICY
{
    "Root": {
        "Id": "r-a1b2",
        "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
        "Name": "Root",
        "PolicyTypes": []
    }
}
```

Daftar `PolicyTypes` dalam output tidak lagi menyertakan jenis kebijakan tertentu.

- AWSSDK: DisablePolicyType

Mendapatkan informasi tentang kebijakan organisasi Anda

Bagian ini menjelaskan berbagai cara untuk mendapatkan detail tentang kebijakan di organisasi Anda. Prosedur ini berlaku untuk semua jenis kebijakan. Anda harus mengaktifkan sebuah jenis kebijakan pada root organisasi sebelum Anda dapat melampirkan jenis kebijakan tersebut ke entitas apa pun di root organisasi tersebut.

Mencantumkan semua kebijakan

Izin minimum

Untuk mencantumkan kebijakan dalam organisasi Anda, Anda harus memiliki izin berikut:

- `organizations:ListPolicies`

Anda dapat melihat kebijakan di organisasi Anda di AWS Management Console atau dengan menggunakan sebuah perintah AWS Command Line Interface (AWS CLI) atau operasi SDK AWS.

AWS Management Console

Untuk mencantumkan semua kebijakan di organisasi Anda

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Kebijakan, pilih nama jenis kebijakan yang ingin Anda cantumkan.

   Jika jenis kebijakan tertentu diaktifkan, maka konsol akan menampilkan daftar semua jenis kebijakan yang saat ini tersedia dalam organisasi.
3. Kembali ke halaman Kebijakan dan ulangi untuk setiap jenis kebijakan.

AWS CLI & AWS SDKs

Untuk mencantumkan semua kebijakan di organisasi Anda

Anda dapat menggunakan salah satu perintah berikut untuk mencantumkan kebijakan dalam sebuah organisasi:

- AWS CLI: daftar-kebijakan

  Contoh berikut menunjukkan cara mendapatkan daftar dari semua kebijakan kontrol layanan di organisasi Anda. Anda harus menentukan jenis kebijakan yang ingin Anda lihat. Ulangi perintah untuk setiap jenis kebijakan yang ingin Anda sertakan.

```
$ aws organizations list-policies \
    --filter SERVICE_CONTROL_POLICY
{
    "Policies": [
        {
            "Id": "p-FullAWSAccess",
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": true
        }
    ]
```

```
}
```

- AWSSDK: ListPolicies

Mencantumkan kebijakan kebijakan yang dilampirkan pada root, OU, atau akun

> **Izin minimum**
>
> Untuk daftar kebijakan yang dilampirkan ke akar, unit organisasi (OU), atau akun dalam organisasi Anda, Anda harus memiliki izin berikut:
>
> - `organizations:ListPoliciesForTarget` dengan elemen `Resource` dalam pernyataan kebijakan yang sama yang menyertakan Amazon Resource Name (ARN) dari target yang ditentukan (atau "*")

AWS Management Console

Untuk daftar semua kebijakan yang dilampirkan secara langsung ke root, OU, atau akun tertentu

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Akun AWS, pilih nama root, OU, atau akun yang kebijakannya ingin Anda lihat. Anda mungkin harus memperluas OU (pilih ▶) untuk menemukan OU yang Anda inginkan.
3. Pada halaman Root, OU, atau akun, pilih tab Kebijakan.

   Tab Kebijakan menampilkan semua kebijakan yang dilampirkan ke root, OU, atau akun, yang dikelompokkan dalam grup berdasarkan jenis kebijakan.

AWS CLI & AWS SDKs

Untuk daftar semua kebijakan yang dilampirkan secara langsung ke root, OU, atau akun tertentu

Anda dapat menggunakan salah satu perintah berikut untuk mencantumkan kebijakan yang dilampirkan ke sebuah entitas:

- AWS CLI: list-policies-for-target

  Contoh berikut mencantumkan semua kebijakan kontrol layanan yang dilampirkan pada OU tertentu. Anda harus menentukan ID dari root, OU, atau akun, dan jenis kebijakan yang ingin Anda cantumkan.

```
$ aws organizations list-policies-for-target \
    --target-id ou-a1b2-f6g7h222 \
    --filter SERVICE_CONTROL_POLICY
{
    "Policies": [
        {
            "Id": "p-FullAWSAccess",
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": true
        }
    ]
}
```

- AWSSDK: ListPoliciesForTarget

Mencantumkan semua root, OU, dan akun yang terlampir kebijakan padanya

> **Izin minimum**
>
> Untuk mencantumkan entitas yang padanya kebijakan terlampir, Anda harus memiliki izin berikut:
>
> - `organizations:ListTargetsForPolicy` dengan elemen `Resource` dalam pernyataan kebijakan yang sama yang mencakup ARN dari kebijakan yang ditentukan (atau "*")

AWS Management Console

Untuk mencantumkan semua root, OU, dan akun yang mempunyai kebijakan terlampir yang ditentukan

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Kebijakan, pilih jenis kebijakan, lalu pilih nama kebijakan yang lampirannya ingin Anda periksa.
3. Pilih tab Target, untuk menampilkan tabel dari setiap root, OU, dan akun yang mempunyai kebijakan terlampir yang dipilih.

AWS CLI & AWS SDKs

Untuk mencantumkan semua root, OU, dan akun yang mempunyai kebijakan terlampir yang ditentukan

Anda dapat menggunakan salah satu perintah berikut untuk mecantumkan entitas yang memiliki sebuah kebijakan:

- AWS CLI: list-targets-for-policy

  Contoh berikut menunjukkan semua lampiran ke root, OU, dan akun untuk kebijakan tertentu.

```
$ aws organizations list-targets-for-policy \
    --policy-id p-FullAWSAccess
{
    "Targets": [
        {
            "TargetId": "ou-a1b2-f6g7h111",
            "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h111",
            "Name": "testou2",
            "Type": "ORGANIZATIONAL_UNIT"
        },
        {
            "TargetId": "ou-a1b2-f6g7h222",
            "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
            "Name": "testou1",
```

```
            "Type": "ORGANIZATIONAL_UNIT"
        },
        {
            "TargetId": "123456789012",
            "Arn": "arn:aws:organizations::123456789012:account/o-
aa111bb222/123456789012",
            "Name": "My Management Account (bisdavid)",
            "Type": "ACCOUNT"
        },
        {
            "TargetId": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "Type": "ROOT"
        }
    ]
}
```

- AWSSDK: ListTargetsForPolicy

Mendapatkan detail tentang sebuah kebijakan

> **Izin minimum**
>
> Untuk menampilkan detail kebijakan, Anda harus memiliki izin berikut:
>
> - `organizations:DescribePolicy` dengan elemen `Resource` dalam pernyataan kebijakan yang sama yang mencakup ARN dari kebijakan yang ditentukan (atau "*")

AWS Management Console

Untuk mendapatkan detail tentang sebuah kebijakan

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Kebijakan, pilih jenis kebijakan yang ingin Anda periksa, dan kemudian pilih nama kebijakan tersebut.

Halaman kebijakan tersebut akan menampilkan informasi yang tersedia tentang kebijakan, termasuk ARN, deskripsi, dan target terlampir.

- Tab Daftar isi menunjukkan isi kebijakan saat ini dalam format JSON.
- Tab Target menampilkan daftar root, OU, dan akun yang padanya kebijakan dilampirkan.
- Tab Tag menunjukkan tag yang dilampirkan ke kebijakan. Catatan: Tab tag tidak tersedia untuk kebijakan terkelola AWS.

Untuk mengedit kebijakan, pilih Edit Kebijakan. Karena setiap jenis kebijakan memiliki persyaratan pengeditan yang berbeda, lihat petunjuk untuk membuat dan memperbarui kebijakan dari jenis kebijakan yang Anda tentukan.

AWS CLI & AWS SDKs

Untuk mendapatkan detail tentang sebuah kebijakan

Anda dapat menggunakan salah satu perintah berikut untuk mendapatkan detail tentang sebuah kebijakan:

- AWS CLI: describe-policy

Contoh berikut menampilkan detail untuk kebijakan yang ditentukan.

```
$ aws organizations describe-policy \
    --policy-id p-FullAWSAccess
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-FullAWSAccess",
            "Arn": "arn:aws:organizations::aws:policy/service_control_policy/p-
FullAWSAccess",
            "Name": "FullAWSAccess",
            "Description": "Allows access to every operation",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": true
        },
        "Content": "{\n  \"Version\": \"2012-10-17\",\n  \"Statement\": [\n    {\n
      \"Effect\": \"Allow\",\n      \"Action\": \"*\",\n      \"Resource\": \"*
\"\n    }\n  ]\n}"
```

```
    }
}
```

- AWSSDK: DescribePolicy

Administrator yang didelegasikan untuk AWS Organizations

Kami menyarankan Anda menggunakan akun AWS Organizations manajemen dan penggunanya dan perannya hanya untuk tugas-tugas yang harus dilakukan oleh akun itu. Kami juga menyarankan agar Anda menyimpan AWS sumber daya Anda di akun anggota lain di organisasi dan menjauhkannya dari akun manajemen. Ini karena fitur keamanan seperti Organizations Service Control Policies (SCPs) tidak membatasi pengguna atau peran dalam akun manajemen.

Dari akun manajemen organisasi, Anda dapat mendelegasikan manajemen kebijakan untuk Organizations ke akun anggota tertentu untuk melakukan tindakan kebijakan yang secara default hanya tersedia untuk akun manajemen.

Membuat atau memperbarui kebijakan delegasi berbasis sumber daya

Dari akun manajemen, buat atau perbarui kebijakan delegasi berbasis sumber daya untuk organisasi Anda dan tambahkan pernyataan yang menentukan akun anggota mana yang dapat melakukan tindakan pada kebijakan. Anda dapat menambahkan beberapa pernyataan dalam kebijakan untuk menunjukkan kumpulan izin yang berbeda ke akun anggota.

Izin minimum

Untuk membuat atau memperbarui kebijakan delegasi berbasis sumber daya, Anda memerlukan izin untuk menjalankan tindakan berikut:

- `organizations:PutResourcePolicy`
- `organizations:DescribeResourcePolicy`

Selain itu, Anda harus memberikan peran dan pengguna di akun administrator yang didelegasikan izin IAM yang sesuai untuk tindakan yang diperlukan. Tanpa izin IAM, diasumsikan bahwa prinsipal panggilan tidak memiliki izin yang diperlukan untuk mengelola kebijakan. AWS Organizations

AWS Management Console

Tambahkan pernyataan ke kebijakan delegasi berbasis sumber daya dalam AWS Management Console menggunakan salah satu metode berikut:

- Kebijakan JSON — Tempelkan dan sesuaikan contoh kebijakan delegasi berbasis sumber daya untuk digunakan di akun Anda, atau ketik dokumen kebijakan JSON Anda sendiri di editor JSON.
- Editor visual - Buat kebijakan delegasi baru di editor visual, yang memandu Anda dalam membuat kebijakan delegasi tanpa harus menulis sintaks JSON.

Menggunakan editor kebijakan JSON untuk membuat atau memperbarui kebijakan delegasi

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pilih Pengaturan.
3. Di AWS Organizations bagian Administrator yang didelegasikan, pilih Delegasi untuk membuat kebijakan delegasi Organizations. Untuk memperbarui kebijakan delegasi yang ada, pilih Edit.
4. Ketik atau tempel dokumen kebijakan JSON. Untuk detail bahasa kebijakan IAM, lihat Referensi kebijakan JSON IAM.
5. Selesaikan peringatan keamanan, kesalahan, atau peringatan umum yang dihasilkan selama validasi kebijakan, lalu pilih Buat kebijakan untuk menyimpan pekerjaan Anda.

Gunakan editor visual untuk membuat atau memperbarui kebijakan delegasi

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pilih Pengaturan.
3. Di AWS Organizations bagian Administrator yang didelegasikan, pilih Delegasi untuk membuat kebijakan delegasi Organizations. Untuk memperbarui kebijakan delegasi yang ada, pilih Edit.
4. Pada halaman kebijakan Buat Delegasi, pilih Tambahkan pernyataan baru.

5. Atur Efek ke`Allow`.
6. Tambahkan `Principal` untuk menentukan akun anggota yang ingin Anda delegasikan. Untuk detail tentang sintaks, lihat. Contoh kebijakan delegasi berbasis sumber daya
7. Dari daftar Tindakan, pilih tindakan yang ingin Anda delegasikan. Anda dapat menggunakan tindakan Filter untuk mempersempit pilihan.
8. Untuk menentukan apakah akun anggota yang didelegasikan dapat melampirkan kebijakan ke root organisasi atau unit organisasi (OU), tetapkan`Resources`. Anda juga harus memilih `policy` sebagai jenis sumber daya. Untuk detail tambahan, lihatContoh kebijakan delegasi berbasis sumber daya. Anda dapat menentukan sumber daya dengan cara berikut:
   - Pilih Tambahkan sumber daya dan buat Nama Sumber Daya Amazon (ARN) dengan mengikuti petunjuk di kotak dialog.
   - Daftar ARN sumber daya secara manual di editor. Untuk informasi selengkapnya tentang sintaks ARN, lihat Amazon Resource Name (ARN) di Panduan Referensi Umum. AWS Untuk informasi tentang penggunaan ARN dalam elemen sumber daya kebijakan, lihat elemen kebijakan IAM JSON: Resource.
9. Pilih Tambahkan kondisi untuk menentukan kondisi lain, termasuk jenis kebijakan yang ingin Anda delegasikan. Pilih kondisi kondisi kunci, Tag key, Qualifier, dan Operator, dan kemudian ketik a**`Value`**. Untuk detail tambahan, lihat Contoh kebijakan delegasi berbasis sumber daya. Setelah selesai, pilih Tambahkan kondisi. Untuk informasi selengkapnya tentang elemen Kondisi, lihat elemen kebijakan IAM JSON: Kondisi dalam referensi kebijakan IAM JSON.
10. Untuk menambahkan lebih banyak blok izin, pilih Tambahkan pernyataan baru. Untuk setiap blok, ulangi langkah 5 hingga 9.
11. Selesaikan peringatan keamanan, kesalahan, atau peringatan umum yang dihasilkan selama validasi kebijakan, lalu pilih Buat kebijakan untuk menyimpan pekerjaan Anda.

AWS CLI & AWS SDKs

Membuat atau memperbarui kebijakan delegasi

Anda dapat menggunakan perintah berikut untuk membuat atau memperbarui kebijakan delegasi:

- AWS CLI: put-resource-policy

  Contoh berikut membuat atau memperbarui kebijakan delegasi.

```
$ aws organizations put-resource-policy --content
```

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Fully_manage_backup_policies",
            "Effect": "Allow",
            "Principal": {
                "AWS": "135791357913"
            }
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:CreatePolicy",
                "organizations:DescribePolicy",
                "organizations:UpdatePolicy",
                "organizations:DeletePolicy",
                "organizations:AttachPolicy",
                "organizations:DetachPolicy"
            ],
            "Resource": [
                "arn:aws:organizations::246802468024:root/o-abcdef/r-pqrstu",
                "arn:aws:organizations::246802468024:ou/o-abcdef/*",
                "arn:aws:organizations::246802468024:account/o-abcdef/*",
                "arn:aws:organizations::246802468024:organization/policy/
backup_policy/*",
            ],
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [
                        "BACKUP_POLICY"
                    ]
                }
            }
        }
    ]
}
```

- AWS SDK: PutResourcePolicy

Tindakan kebijakan delegasi yang didukung

Tindakan berikut didukung untuk kebijakan delegasi:

- AttachPolicy
- CreatePolicy
- DeletePolicy
- DescribeAccount
- DescribeCreateAccountStatus
- DescribeEffectivePolicy
- DescribeHandshake
- DescribeOrganization
- DescribeOrganizationalUnit
- DescribePolicy
- DescribeResourcePolicy
- DetachPolicy
- DisablePolicyType
- EnablePolicyType
- ListAccounts
- ListAccountsForParent
- ListAWSServiceAccessForOrganization
- ListChildren
- ListCreateAccountStatus
- ListDelegatedAdministrators
- ListDelegatedServicesForAccount
- ListHandshakesForAccount
- ListHandshakesForOrganization
- ListOrganizationalUnitsForParent
- ListParents
- ListPolicies
- ListPoliciesForTarget
- ListRoots
- ListTagsForResource

- `ListTargetsForPolicy`
- `TagResource`
- `UntagResource`
- `UpdatePolicy`

Kunci kondisi yang didukung

Hanya kunci kondisi yang didukung oleh yang AWS Organizations dapat digunakan untuk kebijakan delegasi. Untuk informasi selengkapnya, lihat Kunci kondisi untuk AWS Organizations Referensi Otorisasi Layanan.

Melihat kebijakan delegasi berbasis sumber daya

Dari akun manajemen, lihat kebijakan delegasi berbasis sumber daya organisasi Anda untuk memahami administrator yang didelegasikan yang memiliki akses untuk mengelola jenis kebijakan mana.

> **Izin minimum**
>
> Untuk melihat kebijakan delegasi berbasis sumber daya, Anda memerlukan izin untuk menjalankan tindakan berikut:. `organizations:DescribeResourcePolicy`

AWS Management Console

Untuk melihat kebijakan delegasi

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pilih Pengaturan.
3. Di AWS Organizations bagian Administrator yang didelegasikan, gulir untuk melihat kebijakan delegasi lengkap.

AWS CLI & AWS SDKs

Melihat kebijakan delegasi

Anda dapat menggunakan perintah berikut untuk melihat kebijakan delegasi:

- AWS CLI: describe-resource-policy

  Contoh berikut mengambil kebijakan.

  ```
  $ aws organizations describe-resource-policy
  ```

- AWS SDK: DescribeResourcePolicy

Menghapus kebijakan delegasi berbasis sumber daya

Jika Anda tidak perlu lagi mendelegasikan pengelolaan kebijakan di organisasi, Anda dapat menghapus kebijakan delegasi berbasis sumber daya dari akun manajemen organisasi.

> **Important**
>
> Jika Anda menghapus kebijakan delegasi berbasis sumber daya, Anda tidak dapat memulihkannya.

> **Izin minimum**
>
> Untuk menghapus kebijakan delegasi berbasis sumber daya, Anda memerlukan izin untuk menjalankan tindakan berikut:. `organizations:DeleteResourcePolicy`

AWS Management Console

Untuk menghapus kebijakan delegasi

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pilih Pengaturan.
3. Di AWS Organizations bagian Administrator yang didelegasikan untuk, pilih Hapus.
4. Di kotak dialog Hapus konfirmasi kebijakan, ketik**`delete`**. Kemudian, pilih Hapus kebijakan.

AWS CLI & AWS SDKs

Menghapus kebijakan delegasi

Anda dapat menggunakan perintah berikut untuk menghapus kebijakan delegasi:

- AWS CLI: delete-resource-policy

  Contoh berikut menghapus kebijakan.

  ```
  $ aws organizations delete-resource-policy
  ```

- AWS SDK: DeleteResourcePolicy

Contoh kebijakan delegasi berbasis sumber daya

Contoh kode berikut menunjukkan bagaimana Anda dapat menggunakan kebijakan delegasi berbasis sumber daya.

Contoh

- Contoh: Melihat organisasi, OU, akun, dan kebijakan
- Contoh: Izin terkonsolidasi untuk mengelola kebijakan cadangan organisasi

Contoh: Melihat organisasi, OU, akun, dan kebijakan

Sebelum mendelegasikan pengelolaan kebijakan, Anda harus mendelegasikan izin untuk menavigasi struktur organisasi dan melihat unit organisasi (oU), akun, dan kebijakan yang melekat padanya.

Contoh ini menunjukkan bagaimana Anda dapat menyertakan izin ini dalam kebijakan delegasi berbasis sumber daya untuk akun anggota, *`AccountId`*.

> **Important**
>
> Sebaiknya Anda menyertakan izin hanya untuk tindakan minimum yang diperlukan seperti yang ditunjukkan dalam contoh, meskipun dimungkinkan untuk mendelegasikan tindakan hanya-baca Organizations apa pun menggunakan kebijakan ini.

Kebijakan delegasi ini memberi izin yang diperlukan untuk menyelesaikan tindakan dariAWS API atauAWS CLI. Untuk menggunakan kebijakan delegasi ini, ganti teksAWS placeholder *AccountId*dengan informasi Anda sendiri. Kemudian, ikuti petunjuk diAdministrator yang didelegasikan untuk AWS Organizations.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*"
    }
  ]
}
```

Contoh: Izin terkonsolidasi untuk mengelola kebijakan cadangan organisasi

Contoh ini menunjukkan cara membuat kebijakan delegasi berbasis sumber daya yang memungkinkan akun manajemen mendelegasikan izin penuh yang diperlukan untuk mengelola kebijakan pencadangan dalam organisasi, termasuk,,, dan `delete` tindakan `create` `readupdate`,

serta tindakan kebijakan. `attach` `detach` Untuk memahami pentingnya setiap tindakan, sumber daya, dan kondisi, lihatContoh kebijakan delegasi berbasis sumber daya.

> **Important**
>
> Kebijakan ini memungkinkan administrator yang didelegasikan untuk melakukan tindakan tertentu pada kebijakan yang dibuat oleh akun mana pun di organisasi, termasuk akun manajemen.

Contoh kebijakan delegasi ini memberikan izin yang diperlukan untuk menyelesaikan tindakan secara terprogram dari API atau. AWS AWS CLI Untuk menggunakan kebijakan delegasi ini, ganti teks AWS placeholder untuk *`MemberAccountId`*,, *`ManagementAccountIdOrganizationId`*, dan *`RootId`*dengan informasi Anda sendiri. Kemudian, ikuti petunjuk masukAdministrator yang didelegasikan untuk AWS Organizations.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
```

```
      ],
      "Resource": "*",
      "Condition": {
        "StringLikeIfExists": {
          "organizations:PolicyType": "BACKUP_POLICY"
        }
      }
    },
    {
      "Sid": "DelegatingAllActionsForBackupPolicies",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:CreatePolicy",
        "organizations:UpdatePolicy",
        "organizations:DeletePolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "organizations:EnablePolicyType",
        "organizations:DisablePolicyType"
      ],
      "Resource": [
        "arn:aws:organizations::ManagementAccountId:root/o-OrganizationId/r-RootId",
        "arn:aws:organizations::ManagementAccountId:ou/o-OrganizationId/*",
        "arn:aws:organizations::ManagementAccountId:account/o-OrganizationId/*",
        "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/
backup_policy/*"
      ]
    }
  ]
}
```

Kebijakan pengelolaan

Kebijakan pengelolaan memungkinkan Anda mengonfigurasi dan mengelola secara terpusat layanan dan fitur AWS mereka. Bagaimana kebijakan tersebut memengaruhi OU dan akun yang mewarisinya tergantung pada jenis kebijakan manajemen yang Anda terapkan. AWS Organizations Tinjau topik di bagian ini untuk memahami istilah dan konsep yang relevan tentang kebijakan manajemen.

Topik

- Memahami warisan kebijakan manajemen
- Kebijakan berhenti berlangganan layanan AI
- Kebijakan Backup
- Kebijakan tag

Memahami warisan kebijakan manajemen

> **Note**
>
> Informasi di bagian ini tidak berlaku untuk SCP karena SCP mengelola mengizinkan dan menolak tindakan IAM. Meskipun SCP dilampirkan ke root, OU, dan akun, memungkinkan tindakan memerlukan `allow` pernyataan eksplisit dalam SCP di setiap tingkat dari root melalui setiap OU di jalur langsung ke akun (termasuk akun target itu sendiri). Untuk informasi selengkapnya tentang cara kerja SCP dalam AWS Organizations hierarki, lihat. Evaluasi SCP

Anda dapat melampirkan kebijakan manajemen ke entitas organisasi (root organisasi, unit organisasi (OU), atau akun) di organisasi Anda:

- Saat Anda melampirkan kebijakan manajemen ke root organisasi, semua OU dan akun di organisasi mewarisi kebijakan tersebut.
- Saat Anda melampirkan kebijakan manajemen ke OU tertentu, akun yang secara langsung berada di bawah OU tersebut atau OU anak mana pun mewarisi kebijakan tersebut.
- Ketika Anda melampirkan kebijakan manajemen ke akun tertentu, itu hanya memengaruhi akun itu.

Karena Anda dapat melampirkan kebijakan manajemen ke beberapa tingkatan dalam organisasi, akun dapat mewarisi beberapa kebijakan.

Bagian ini menjelaskan bagaimana kebijakan induk dan kebijakan anak diproses menjadi kebijakan efektif untuk sebuah akun.

Topik

- Terminologi pewarisan
- Sintaksis kebijakan dan pewarisan untuk jenis kebijakan pengelolaan
- Operator pewarisan

- Contoh warisan

Terminologi pewarisan

Topik ini menggunakan istilah-istilah berikut ketika membahas pewarisan kebijakan manajemen.

Warisan kebijakan

Interaksi berbagai kebijakan yang ada di tingkat yang berbeda dari suatu organisasi, bergerak dari akar tingkat atas organisasi, turun melalui hirarki unit organisasi (OU) ke masing-masing akun.

Anda dapat melampirkan kebijakan ke akar organisasi, OU, masing-masing akun, dan kombinasi dari entitas organisasi ini. Warisan kebijakan mengacu pada kebijakan manajemen yang melekat pada akar organisasi atau OU. Semua akun yang merupakan anggota root organisasi atau OU di mana kebijakan manajemen dilampirkan mewarisi kebijakan itu.

Misalnya, ketika kebijakan manajemen dilampirkan ke akar organisasi, semua akun dalam organisasi mewarisi kebijakan itu. Hal itu karena semua akun dalam suatu organisasi selalu berada di bawah akar organisasi. Ketika Anda melampirkan kebijakan untuk OU tertentu, akun yang langsung di bawah OU atau anak OU akan mewarisi kebijakan itu. Karena Anda dapat melampirkan kebijakan ke beberapa tingkatan dalam organisasi, akun mungkin mewarisi beberapa dokumen kebijakan untuk satu jenis kebijakan.

Kebijakan orang tua

Kebijakan yang dilampirkan lebih tinggi di pohon organisasi daripada kebijakan yang dilampirkan pada entitas yang lebih rendah di pohon organisasi tersebut.

Misalnya, jika Anda melampirkan kebijakan manajemen A ke root organisasi, itu hanya kebijakan. Jika Anda juga melampirkan kebijakan B untuk OU di bawah akar itu, maka kebijakan A adalah kebijakan induk dari kebijakan B. Kebijakan B adalah kebijakan anak dari kebijakan A. Kebijakan A dan kebijakan B bergabung untuk membuat kebijakan tag efektif untuk akun yang ada di OU.

Kebijakan anak

Kebijakan yang dilampirkan pada tingkat yang lebih rendah di pohon organisasi daripada kebijakan induk.

Kebijakan yang efektif

Akhirnya, dokumen kebijakan tunggal yang menentukan aturan yang berlaku untuk akun. Kebijakan efektif adalah agregasi kebijakan apa pun yang diwarisi akun, ditambah kebijakan apa

pun yang secara langsung dilampirkan pada akun. Sebagai contoh, kebijakan tag memungkinkan Anda melihat kebijakan tag efektif yang berlaku untuk salah satu akun Anda. Untuk informasi lebih lanjut, lihat Melihat kebijakan tag efektif.

Operator warisan

Operator yang mengontrol bagaimana warisan kebijakan bergabung menjadi satu kebijakan efektif tunggal. Operator-operator ini dianggap sebagai fitur lanjutan. Penulis kebijakan yang berpengalaman dapat menggunakannya untuk membatasi perubahan yang dapat dibuat oleh kebijakan anak dan bagaimana pengaturan dalam kebijakan bergabung. Untuk informasi selengkapnya, lihat Operator pewarisan.

Sintaksis kebijakan dan pewarisan untuk jenis kebijakan pengelolaan

Bagaimana tepatnya kebijakan memengaruhi OU dan akun yang mewarisinya tergantung pada jenis kebijakan manajemen yang Anda pilih. Jenis kebijakan pengelolaan meliputi:

- Kebijakan opt-out layanan Artificial Intelligence (AI)
- Kebijakan Backup
- Kebijakan tag

Sintaks untuk jenis kebijakan manajemen termasuk Operator pewarisan, yang memungkinkan Anda menentukan dengan perincian halus elemen apa dari kebijakan induk yang diterapkan dan elemen apa yang dapat diganti atau dimodifikasi saat diwarisi oleh OU dan akun anak.

Kebijakan efektif adalah seperangkat aturan yang diwarisi dari akar organisasi dan OU bersama dengan aturan yang langsung dilampirkan pada akun tersebut. Kebijakan efektif menentukan seperangkat aturan akhir yang berlaku untuk akun. Anda dapat melihat kebijakan efektif untuk akun yang mencakup efek dari semua operator pewarisan dalam kebijakan yang diterapkan. Untuk informasi selengkapnya, lihat Melihat kebijakan tag efektif.

Operator pewarisan

Operator pewarisan mengontrol bagaimana warisan kebijakan dan kebijakan akun bergabung menjadi sebuah kebijakan efektif dari akun tersebut. Operator ini mencakup operator pengaturan nilai dan operator kontrol anak.

Bila Anda menggunakan editor visual dalam konsol AWS Organizations, Anda dapat menggunakan operator `@@assign` saja. Operator-operator lain dianggap sebagai fitur lanjutan. Untuk menggunakan

operator yang lain, Anda harus secara manual menulis kebijakan JSON. Penulis kebijakan yang berpengalaman dapat menggunakan operator pewarisan untuk mengontrol nilai-nilai apa yang diterapkan pada kebijakan efektif dan membatasi perubahan apa yang dapat dibuat kebijakan anak.

Operator pengaturan nilai

Anda dapat menggunakan operator pengaturan nilai berikut untuk mengontrol bagaimana kebijakan Anda berinteraksi dengan kebijakan induknya:

- `@@assign` — Menimpa pengaturan kebijakan yang diwariskan dengan pengaturan yang ditentukan. Jika pengaturan yang ditentukan tidak diwariskan, operator ini menambahkannya ke kebijakan efektif. Operator ini dapat berlaku untuk pengaturan kebijakan apa pun dari jenis apa pun.
  - Untuk pengaturan bernilai tunggal, operator ini menggantikan nilai yang diwariskan dengan nilai yang ditentukan.
  - Untuk pengaturan multi-nilai (array JSON), operator ini menghapus nilai-nilai yang diwariskan dan menggantikannya dengan nilai-nilai yang ditentukan oleh kebijakan ini.
- `@@append` — Menambahkan pengaturan yang ditentukan (tanpa menghapus apapun) ke pengaturan yang diwariskan. Jika pengaturan yang ditentukan tidak diwariskan, operator ini menambahkannya ke kebijakan efektif. Anda dapat menggunakan operator ini hanya dengan pengaturan multi-nilai.
  - Operator ini menambahkan nilai yang ditentukan untuk setiap nilai dalam array yang diwariskan.
- `@@remove` — Menghapus pengaturan warisan yang ditentukan dari kebijakan efektif, jika ada. Anda dapat menggunakan operator ini hanya dengan pengaturan multi-nilai.
  - Operator ini hanya menghapus nilai-nilai yang ditentukan dari array nilai yang diwarisi dari kebijakan induk. Nilai-nilai lain dapat tetap ada dalam array dan dapat diwariskan oleh kebijakan anak.

Operator kontrol anak

Menggunakan operator kontrol anak adalah opsional. Anda dapat menggunakan operator `@@operators_allowed_for_child_policies` untuk mengontrol pengaturan nilai kebijakan anak yang dapat digunakan. Anda dapat mengizinkan semua operator, beberapa operator tertentu, atau tidak ada operator yang diizinkan. Secara default, semua operator (`@@all`) diizinkan.

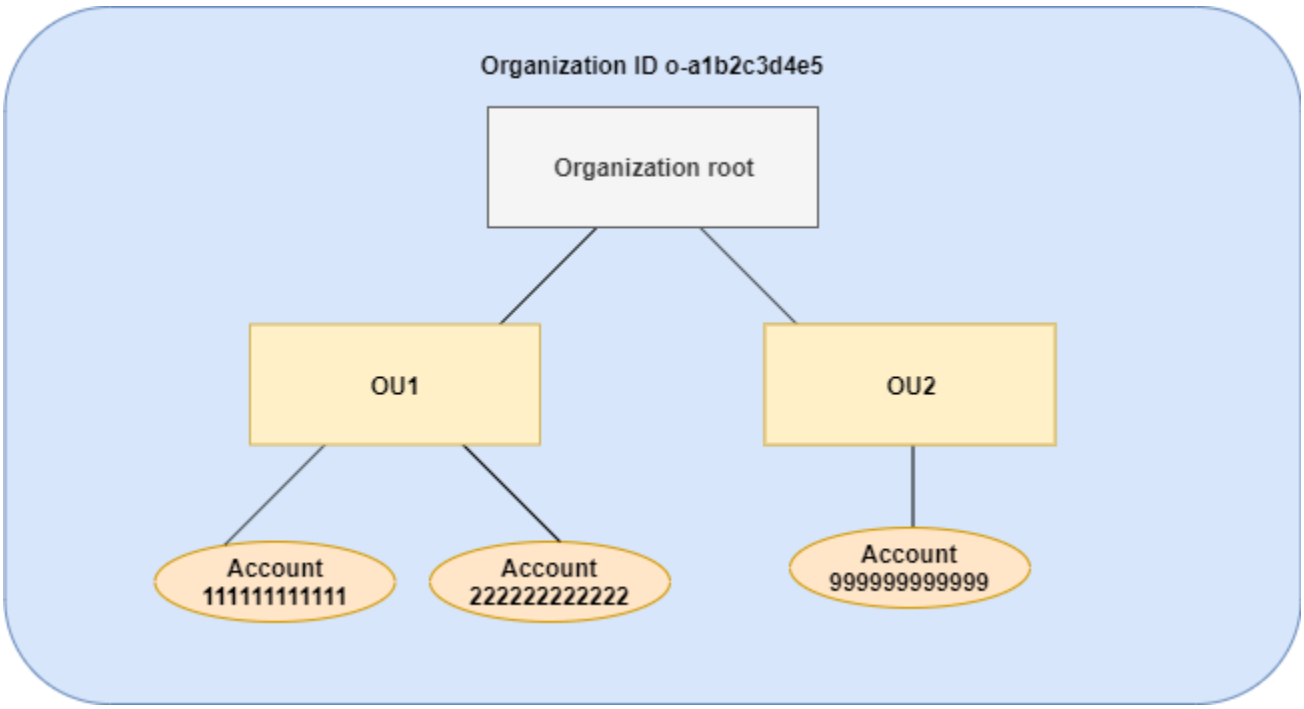
- `"@@operators_allowed_for_child_policies":["@@all"]` — OU anak dan akun dapat menggunakan operator apa pun dalam kebijakan. Secara default, semua operator diizinkan dalam kebijakan anak.
- `"@@operators_allowed_for_child_policies":["@@assign", "@@append", "@@remove"]` — OU anak dan akun hanya dapat menggunakan operator tertentu dalam kebijakan anak. Anda dapat menentukan satu atau beberapa operator pengaturan nilai pada operator kontrol anak ini.
- `"@@operators_allowed_for_child_policies":["@@none"]` — OU anak dan akun tidak dapat menggunakan operator dalam kebijakan. Anda dapat menggunakan operator ini untuk secara efektif mengunci nilai-nilai yang didefinisikan dalam kebijakan induk sehingga kebijakan anak tidak dapat menambahkan, menambah, atau menghapus nilai-nilai tersebut.

> **Note**
>
> Jika operator kontrol anak yang diwariskan membatasi penggunaan operator, Anda tidak dapat membalikkan aturan tersebut dalam kebijakan anak. Jika Anda menyertakan operator kontrol anak dalam kebijakan induk, maka mereka membatasi operator pengaturan nilai di semua kebijakan anak.

Contoh warisan

Contoh ini menunjukkan cara kerja pewarisan kebijakan dengan menunjukkan bagaimana kebijakan tag induk dan anak digabungkan ke kebijakan tag efektif untuk sebuah akun.

Contoh berikut mengasumsikan bahwa Anda memiliki struktur organisasi yang ditunjukkan pada diagram berikut.



Contoh

- Contoh 1: Izinkan kebijakan anak untuk menimpa hanya nilai tag
- Contoh 2: Menambahkan nilai-nilai baru untuk tag yang diwariskan
- Contoh 3: Hapus nilai dari tag yang diwariskan
- Contoh 4: Membatasi perubahan kebijakan anak
- Contoh 5: Konflik dengan operator kontrol anak
- Contoh 6: Konflik dengan penambahan nilai pada tingkat hirarki yang sama

Contoh 1: Izinkan kebijakan anak untuk menimpa hanya nilai tag

Kebijakan tag berikut mendefinisikan kunci tag `CostCenter` dan dua nilai yang dapat diterima, `Development` dan `Support`. Jika Anda melampirkannya ke akar organisasi, kebijakan tag berlaku untuk semua akun di organisasi tersebut.

Kebijakan A — Kebijakan tag akar organisasi

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
```

```
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

Misalnya Anda ingin pengguna di OU1 menggunakan nilai tag yang berbeda untuk sebuah kunci, dan Anda ingin menegakkan kebijakan tag untuk jenis sumber daya tertentu. Karena kebijakan A tidak menentukan operator kontrol anak mana yang diizinkan, semua operator diperbolehkan. Anda dapat menggunakan operator `@@assign` dan membuat kebijakan tag seperti berikut untuk melampirkan ke OU1.

Kebijakan B - Kebijakan tag OU1

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Sandbox"
                ]
            },
            "enforced_for": {
                "@@assign": [
                    "redshift:*",
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

Menentukan operator `@@assign` untuk tag menyebabkan hal berikut ketika kebijakan A dan kebijakan B bergabung untuk membentuk kebijakan tag efektif untuk sebuah akun:

- Kebijakan B menimpa dua nilai tag yang ditentukan dalam kebijakan induk, yakni kebijakan A. Hasilnya adalah bahwa `Sandbox` menjadi nilai satu-satunya yang patuh untuk kunci tag `CostCenter`.
- Penambahan `enforced_for` menentukan bahwa tag `CostCenter` harus menjadi nilai tag yang ditentukan pada semua sumber daya Amazon Redshift dan tabel Amazon DynamoDB.

Seperti yang ditunjukkan dalam diagram, OU1 mencakup dua akun: 111111111111 dan 222222222222.

Kebijakan tag efektif yang dihasilkan untuk akun 111111111111 dan 222222222222

> **Note**
>
> Anda tidak dapat langsung menggunakan konten kebijakan efektif yang ditampilkan sebagai isi dari kebijakan baru. Sintaksis tidak menyertakan operator yang diperlukan untuk mengontrol penggabungan dengan kebijakan anak dan kebijakan induk lainnya. Tampilan dari sebuah kebijakan efektif dimaksudkan hanya untuk memahami hasil penggabungan.

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Sandbox"
            ],
            "enforced_for": [
                "redshift:*",
                "dynamodb:table"
            ]
        }
    }
}
```

Contoh 2: Menambahkan nilai-nilai baru untuk tag yang diwariskan

Mungkin ada kasus di mana Anda ingin semua akun di organisasi Anda menentukan kunci tag dengan daftar pendek nilai yang dapat diterima. Untuk akun di satu OU, Anda mungkin ingin mengizinkan nilai tambahan yang hanya akun tersebut dapat menentukan kapan membuat sumber

daya. Contoh ini menentukan bagaimana melakukannya dengan menggunakan operator `@@append`. Operator `@@append` adalah fitur lanjutan.

Seperti contoh 1, contoh ini dimulai dengan kebijakan A untuk kebijakan tag akar organisasi.

Kebijakan A — Kebijakan tag akar organisasi

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

Untuk contoh ini, lampirkan kebijakan C ke OU2. Perbedaan dalam contoh ini adalah bahwa menggunakan operator `@@append` dalam kebijakan C menambahkan ke, bukan menimpa, daftar nilai yang dapat diterima dan aturan `enforced_for`.

Kebijakan C - Kebijakan tag OU2 untuk menambahkan nilai

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@append": [
                    "Marketing"
                ]
            },
            "enforced_for": {
                "@@append": [
                    "redshift:*",
```

```
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

Melampirkan kebijakan C ke OU2 memiliki efek berikut ketika kebijakan A dan kebijakan C bergabung untuk membentuk kebijakan tag efektif untuk sebuah akun:

- Karena kebijakan C menyertakan operator `@@append`, ia memungkinkan untuk menambahkan ke, bukan menimpa, daftar nilai tag yang dapat diterima yang ditentukan dalam Kebijakan A.
- Seperti dalam kebijakan B, penambahan `enforced_for` menentukan bahwa tag `CostCenter` harus digunakan sebagai nilai tag yang ditentukan pada semua sumber daya Amazon Redshift dan tabel Amazon DynamoDB. Menimpa (`@@assign`) dan menambahkan (`@@append`) memiliki efek yang sama jika kebijakan induk tidak menyertakan operator kontrol anak yang membatasi apa yang dapat ditentukan kebijakan anak.

Seperti yang ditunjukkan dalam diagram, OU2 mencakup satu akun: 999999999999. Kebijakan A dan kebijakan C bergabung untuk membuat kebijakan tag efektif untuk akun 999999999999.

Kebijakan tag yang efektif untuk akun 999999999999

> **Note**
>
> Anda tidak dapat langsung menggunakan konten kebijakan efektif yang ditampilkan sebagai isi dari kebijakan baru. Sintaksis tidak menyertakan operator yang diperlukan untuk mengontrol penggabungan dengan kebijakan anak dan kebijakan induk lainnya. Tampilan dari sebuah kebijakan efektif dimaksudkan hanya untuk memahami hasil penggabungan.

```
{
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Development",
                "Support",
                "Marketing"
```

```
            ],
            "enforced_for": [
                "redshift:*",
                "dynamodb:table"
            ]
        }
    }
}
```

Contoh 3: Hapus nilai dari tag yang diwariskan

Mungkin ada kasus di mana kebijakan tag yang dilampirkan ke organisasi mendefinisikan nilai tag lebih dari yang Anda inginkan untuk digunakan sebuah akun. Contoh ini menjelaskan cara merevisi kebijakan tag menggunakan operator `@@remove`. `@@remove` adalah fitur lanjutan.

Seperti contoh lainnya, contoh ini dimulai dengan kebijakan A untuk kebijakan tag akar organisasi.

Kebijakan A — Kebijakan tag akar organisasi

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "Development",
                    "Support"
                ]
            }
        }
    }
}
```

Untuk contoh ini, lampirkan kebijakan D ke akun 999999999999.

Kebijakan D - Kebijakan tag Akun 999999999999 untuk menghapus nilai

```
{
    "tags": {
        "costcenter": {
            "tag_key": {
```

```
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@remove": [
                    "Development",
                    "Marketing"
                ],
                "enforced_for": {
                    "@@remove": [
                        "redshift:*",
                        "dynamodb:table"
                    ]
                }
            }
        }
    }
}
```

Melampirkan kebijakan D ke akun 999999999999 memiliki efek berikut ketika kebijakan A, kebijakan C, dan kebijakan D bergabung untuk membentuk kebijakan tag efektif:

- Dengan asumsi Anda melakukan semua contoh sebelumnya, kebijakan B, C, dan C adalah kebijakan anak A. Kebijakan B hanya dilampirkan pada OU1, sehingga tidak berpengaruh pada akun 9999999999999.
- Untuk akun 9999999999999, satu-satunya nilai yang dapat diterima untuk kunci tag `CostCenter` adalah `Support`.
- Kepatuhan tidak ditegakkan untuk kunci tag `CostCenter`.

Kebijakan tag efektif baru untuk akun 99999999999999

> **Note**
>
> Anda tidak dapat langsung menggunakan konten kebijakan efektif yang ditampilkan sebagai isi dari kebijakan baru. Sintaksis tidak menyertakan operator yang diperlukan untuk mengontrol penggabungan dengan kebijakan anak dan kebijakan induk lainnya. Tampilan dari sebuah kebijakan efektif dimaksudkan hanya untuk memahami hasil penggabungan.

```
{
```

```
    "tags": {
        "costcenter": {
            "tag_key": "CostCenter",
            "tag_value": [
                "Support"
            ]
        }
    }
}
```

Jika nanti Anda menambahkan lebih banyak akun ke OU2, kebijakan tag efektifnya akan berbeda dengan akun 999999999999. Hal itu karena kebijakan D yang lebih ketat hanya dilampirkan pada tingkat akun, dan bukan ke OU.

Contoh 4: Membatasi perubahan kebijakan anak

Mungkin ada kasus di mana Anda ingin membatasi perubahan dalam kebijakan anak. Contoh ini menjelaskan bagaimana melakukan hal itu dengan menggunakan operator kontrol anak.

Contoh ini dimulai dengan sebuah kebijakan tag akar organisasi baru dan mengasumsikan bahwa kebijakan tag belum dilampirkan ke entitas organisasi.

Kebijakan E — Kebijakan tag akar organisasi untuk membatasi perubahan kebijakan anak

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "Project"
            },
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append"],
                "@@assign": [
                    "Maintenance",
                    "Escalations"
                ]
            }
        }
    }
}
```

Ketika Anda melampirkan kebijakan E ke akar organisasi, kebijakan tersebut akan mencegah kebijakan anak mengubah kunci tag `Project`. Namun, kebijakan anak dapat menimpa atau menambahkan nilai tag.

Misalnya Anda kemudian melampirkan kebijakan F berikut ke sebuah OU.

Kebijakan F - Kebijakan tag OU

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "PROJECT"
            },
            "tag_value": {
                "@@append": [
                    "Escalations - research"
                ]
            }
        }
    }
}
```

Menggabungkan kebijakan E dan kebijakan F memiliki efek berikut pada akun OU:

- Kebijakan F adalah kebijakan anak untuk Kebijakan E.
- Kebijakan F mencoba untuk mengubah perlakuan kasus, tetapi tidak bisa. Itu karena kebijakan E menyertakan operator `"@@operators_allowed_for_child_policies": ["@@none"]` untuk kunci tag.
- Namun, kebijakan F dapat menambahkan nilai tag untuk kunci tersebut. Itu karena kebijakan E menyertakan `"@@operators_allowed_for_child_policies": ["@@append"]` untuk nilai tag.

Kebijakan efektif untuk akun di OU

> **Note**
>
> Anda tidak dapat langsung menggunakan konten kebijakan efektif yang ditampilkan sebagai isi dari kebijakan baru. Sintaksis tidak menyertakan operator yang diperlukan untuk

mengontrol penggabungan dengan kebijakan anak dan kebijakan induk lainnya. Tampilan dari sebuah kebijakan efektif dimaksudkan hanya untuk memahami hasil penggabungan.

```
{
    "tags": {
        "project": {
            "tag_key": "Project",
            "tag_value": [
                "Maintenance",
                "Escalations",
                "Escalations - research"
            ]
        }
    }
}
```

Contoh 5: Konflik dengan operator kontrol anak

Operator kontrol anak dapat ada dalam kebijakan tag yang dilampirkan pada tingkat yang sama dalam hirarki organisasi. Ketika itu terjadi, persimpangan operator diizinkan digunakan ketika kebijakan bergabung untuk membentuk kebijakan efektif untuk akun.

Asumsikan kebijakan G dan kebijakan H sudah dilampirkan ke akar organisasi.

Kebijakan G - Kebijakan tag akar organisasi 1

```
{
    "tags": {
        "project": {
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append"],
                "@@assign": [
                    "Maintenance"
                ]
            }
        }
    }
}
```

Kebijakan H — Kebijakan tag akar organisasi 2

```
{
    "tags": {
        "project": {
            "tag_value": {
                "@@operators_allowed_for_child_policies": ["@@append", "@@remove"]
            }
        }
    }
}
```

Dalam contoh ini, satu kebijakan di akar organisasi mendefinisikan bahwa nilai untuk kunci tag saja yang dapat ditambahkan. Kebijakan lain yang dilampirkan pada akar organisasi memungkinkan kebijakan anak untuk menambahkan dan menghapus nilai. Persimpangan dua izin ini digunakan untuk kebijakan anak. Hasilnya adalah kebijakan anak dapat menambahkan nilai, tetapi tidak menghapus nilai. Oleh karena itu, kebijakan anak dapat menambahkan nilai ke daftar nilai tag tetapi tidak dapat menghapus nilai `Maintenance`.

Contoh 6: Konflik dengan penambahan nilai pada tingkat hirarki yang sama

Anda dapat melampirkan beberapa kebijakan tag ke setiap entitas organisasi. Ketika Anda melakukannya, kebijakan tag yang dilampirkan ke entitas organisasi yang sama mungkin menyertakan informasi yang bertentangan. Kebijakan dievaluasi berdasarkan urutan saat mereka dilampirkan pada entitas organisasi. Untuk mengubah kebijakan mana yang dievaluasi terlebih dahulu, Anda dapat melepaskan kebijakan dan kemudian melampirkannya kembaliitu.

Asumsikan kebijakan J dilampirkan ke akar organisasi terlebih dahulu, dan kemudian kebijakan K dilampirkan ke akar organisasi.

Kebijakan J — Kebijakan tag pertama yang dilampirkan ke root organisasi

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "PROJECT"
            },
            "tag_value": {
                "@@append": ["Maintenance"]
            }
        }
    }
```

```
}
```

Kebijakan K — Kebijakan tag kedua yang dilampirkan ke root organisasi

```
{
    "tags": {
        "project": {
            "tag_key": {
                "@@assign": "project"
            }
        }
    }
}
```

Dalam contoh ini, kunci tag `PROJECT` digunakan dalam kebijakan tag efektif karena kebijakan itulah yang ditetapkan dilampirkan pada akar organisasi terlebih dahulu.

Kebijakan JK — Kebijakan tag efektif untuk akun

Kebijakan efektif untuk akun adalah sebagai berikut.

> **Note**
>
> Anda tidak dapat langsung menggunakan konten kebijakan efektif yang ditampilkan sebagai isi dari kebijakan baru. Sintaksis tidak menyertakan operator yang diperlukan untuk mengontrol penggabungan dengan kebijakan anak dan kebijakan induk lainnya. Tampilan dari sebuah kebijakan efektif dimaksudkan hanya untuk memahami hasil penggabungan.

```
{
    "tags": {
        "project": {
            "tag_key": "PROJECT",
            "tag_value": [
                "Maintenance"
            ]
        }
    }
}
```

Kebijakan berhenti berlangganan layanan AI

AWSLayanan kecerdasan buatan (AI), seperti Amazon Rekognition, Amazon, CodeWhisperer Amazon Transcribe, dan Contact Lens for Amazon Connect, dapat menyimpan dan menggunakan konten pelanggan yang diproses oleh layanan tersebut untuk pengembangan dan peningkatan berkelanjutan layanan lainnya. AWS Sebagai AWS pelanggan, Anda dapat memilih untuk tidak menyimpan konten Anda atau digunakan untuk peningkatan layanan.

> **Note**
>
> AWSLayanan kecerdasan buatan (AI) mungkin perlu menyimpan konten Anda untuk menyediakan layanan, bahkan jika Anda memilih untuk tidak AWS menggunakan data Anda untuk peningkatan layanan. Untuk informasi selengkapnya, lihat dokumentasi untuk layanan AI yang Anda gunakan.

Alih-alih mengkonfigurasi pengaturan ini secara individu untuk setiap Akun AWS yang digunakan organisasi, Anda dapat mengkonfigurasi kebijakan organisasi yang memberlakukan pilihan pengaturan di semua akun yang merupakan anggota organisasi. Anda dapat memilih untuk menolak penyimpanan konten dan penggunaan untuk layanan AI individual, atau untuk semua layanan tercakup sekaligus. Anda dapat meminta kebijakan efektif yang berlaku untuk setiap akun untuk melihat efek dari pilihan pengaturan Anda.

> **Important**
>
> - Ketika Anda menentukan pilihan berlangganan atau berhenti berlangganan untuk layanan, pengaturan tersebut bersifat global dan diterapkan ke semua Wilayah AWS. Pengaturan nilai dari dalam satu Wilayah AWS bereplikasi ke semua Wilayah lainnya.
> - Saat Anda berhenti berlangganan penggunaan konten oleh layanan AI AWS, layanan tersebut menghapus semua konten historis terkait yang dibagikan dengan AWS sebelum Anda mengatur pilihan. Penghapusan ini harus dibatasi pada data yang disimpan yang tidak diperlukan untuk menyediakan fungsi layanan.

Memulai kebijakan berhenti berlangganan layanan AI

Ikuti langkah-langkah ini untuk mulai menggunakan kebijakan berhenti berlangganan layanan Artificial Intelligence (AI).

1. Aktifkan kebijakan berhenti berlangganan layanan AI untuk organisasi Anda.
2. Membuat kebijakan berhenti berlangganan layanan AI.
3. Lampirkan kebijakan berhenti berlangganan layanan AI ke akar, OU, atau akun organisasi Anda.
4. Melihat kebijakan berhenti berlangganan gabungan layanan AI yang berlaku untuk akun.

Untuk semua langkah ini, Anda masuk sebagai pengguna (IAM) AWS Identity and Access Management, mengambil IAM role, atau masuk sebagai pengguna akar (tidak direkomendasikan) di akun manajemen organisasi.

Informasi lainnya

- Pelajari sintaks kebijakan untuk kebijakan opt-out layanan AI dan lihat contoh kebijakan

Membuat, memperbarui, dan menghapus kebijakan berhenti berlangganan layanan AI

Dalam topik ini:

- Setelah Anda mengaktifkan kebijakan berhenti berlangganan layanan AI untuk organisasi Anda, Anda dapat memuat kebijakan.
- Bila persyaratan berhenti berlangganan And berubah, Anda dapat memperbarui kebijakan yang ada.
- Bila Anda tidak lagi memerlukan kebijakan dan setelah melepaskannya dari semua unit organisasi (OU) dan akun, Anda dapat menghapusnya.

Membuat kebijakan berhenti berlangganan layanan AI

> **Izin minimum**
>
> Untuk membuat kebijakan berhenti berlangganan layanan AI, Anda perlu izin untuk melakukan tindakan-tindakan berikut:
>
> - `organizations:CreatePolicy`

AWS Management Console

Untuk membuat kebijakan berhenti berlangganan layanan AI

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada laman Kebijakan berhenti berlangganan layanan AI, pilih Buat kebijakan.
3. Pada laman Buat kebijakan berhenti berlangganan layanan AI baru, masukkan Nama kebijakan dan Deskripsi kebijakan opsional.
4. (Opsional) Anda dapat menambahkan satu tag atau lebih ke kebijakan tersebut dengan memilih Tambahkan tag dan kemudian masukkan kunci dan nilai opsional. Membiarkan nilai kosong akan mengaturnya menjadi string kosong; itu bukan `null`. Anda dapat melampirkan hingga 50 tag ke kebijakan. Untuk informasi lebih lanjut, lihat Penandaan pada sumber daya AWS Organizations.
5. Masukkan atau tempel teks kebijakan di tab JSON. Untuk informasi tentang sintaks kebijakan berhenti berlangganan layanan AI, lihat Sintaks dan contoh kebijakan berhenti berlangganan layanan AI. Untuk contoh kebijakan yang dapat Anda gunakan sebagai titik awal, lihat Sintaks dan contoh kebijakan berhenti berlangganan layanan AI.
6. Setelah selesai mengedit kebijakan, pilih Buat kebijakan di sudut kanan bawah laman.

AWS CLI & AWS SDKs

Untuk membuat kebijakan berhenti berlangganan layanan AI

Anda dapat menggunakan salah satu hal berikut untuk membuat kebijakan tag:

- AWS CLI: create-policy

1. Buat kebijakan berhenti berlangganan layanan AI seperti berikut, dan simpan dalam file teks. Perhatikan bahwa "`optOut`" dan "`optIn`" peka huruf besar dan kecil.

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
```

```
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

Kebijakan berhenti berlangganan layanan AI ini menetapkan bahwa semua akun yang terpengaruh oleh kebijakan dapat berhenti berlangganan semua layanan AI kecuali untuk Amazon Rekognition.

2. Impor file kebijakan JSON untuk membuat kebijakan baru di organisasi. Dalam contoh ini, file JSON sebelumnya dinamai `policy.json`.

```
$ aws organizations create-policy \
    --type AISERVICES_OPT_OUT_POLICY \
    --name "MyTestPolicy" \
    --description "My test policy" \
    --content file://policy.json
{
    "Policy": {
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":{\"@@assign
\":\"optOut\"}},\"rekognition\":{\"opt_out_policy\":{\"@@assign\":\"optIn
\"}}}}",
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5"
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Description": "My test policy",
            "Name": "MyTestPolicy",
            "Type": "AISERVICES_OPT_OUT_POLICY"
        }
    }
}
```

- AWSSDK: CreatePolicy

Apa yang harus dilakukan selanjutnya

Setelah membuat kebijakan berhenti berlangganan layanan AI, Anda dapat memberlakukan pilihan berhenti berlangganan. Untuk melakukannya, Anda dapat melampirkan kebijakan untuk akar organisasi, unit organisasi (UO), Akun AWS dalam organisasi Anda, atau kombinasi semua ini.

Membuat kebijakan berhenti berlangganan layanan AI

> **Izin minimum**
>
> Untuk memperbarui kebijakan berhenti berlangganan layanan AI, Anda harus memiliki izin untuk melakukan tindakan-tindakan berikut:
>
> - `organizations:UpdatePolicy` dengan elemen `Resource` dalam pernyataan kebijakan yang sama yang mencakup ARN kebijakan yang ditentukan (atau "*")
> - `organizations:DescribePolicy` dengan elemen `Resource` dalam pernyataan kebijakan yang sama yang menyertakan Amazon Resource Name (ARN) dari kebijakan yang ditentukan (atau "*")

AWS Management Console

Untuk membuat kebijakan berhenti berlangganan layanan AI

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada laman Kebijakan berhenti berlangganan layanan AI, pilih nama kebijakan yang ingin Anda perbarui.
3. Pada laman detail kebijakan, pilih Edit kebijakan.
4. Anda dapat memasukkan Nama kebijakan, Deskripsi kebijakan, atau edit teks kebijakan JSON. Untuk informasi tentang sintaks kebijakan berhenti berlangganan layanan AI, lihat Sintaks dan contoh kebijakan berhenti berlangganan layanan AI. Untuk contoh kebijakan yang dapat Anda gunakan sebagai titik awal, lihat Sintaks dan contoh kebijakan berhenti berlangganan layanan AI.
5. Setelah selesai memperbarui kebijakan, pilih Simpan perubahan.

AWS CLI & AWS SDKs

Untuk memperbarui kebijakan

Anda dapat menggunakan salah satu hal berikut untuk memperbarui kebijakan:

- AWS CLI: update-policy

  Contoh berikut mengubah nama kebijakan berhenti berlangganan layanan AI.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":
  ....TRUNCATED FOR BREVITY...   :{\"@@assign\":\"optIn\"}}}}"
    }
}
```

  Contoh berikut menambahatau mengubah deskripsi untuk kebijakan berhenti berlangganan layanan AI.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "AISERVICES_OPT_OUT_POLICY",
            "AwsManaged": false
        },
```

```
        "Content": "{\"services\":{\"default\":{\"opt_out_policy\":
  ....TRUNCATED FOR BREVITY...   :{\"@@assign\":\"optIn\"}}}}"
    }
}
```

Contoh berikut mengubah dokumen kebijakan JSON yang dilampirkan pada kebijakan berhenti berlangganan layanan AI. Dalam contoh ini, konten diambil dari file bernama `policy.json` dengan teks berikut:

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "comprehend": {
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
aiservices_opt_out_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "AISERVICES_OPT_OUT_POLICY",
```

```
            "AwsManaged": false
        },
         "Content": "{\n\"services\": {\n\"default\": {\n\"   ....TRUNCATED FOR
 BREVITY....    ": \"optIn\"\n}\n}\n}\n"}
}
```

- AWSSDK: UpdatePolicy

Untuk mengedit tag yang dilampirkan pada kebijakan memilih berhenti berlangganan layanan AI

Saat Anda masuk ke akun manajemen organisasi Anda, Anda dapat menambah atau menghapus tag yang dilampirkan pada kebijakan berhenti berlangganan layanan AI. Untuk informasi lebih lanjut tentang penandaan, lihat Penandaan pada sumber daya AWS Organizations.

Izin minimum

Untuk mengedit tag yang dilampirkan pada kebijakan berhenti berlangganan layanan AI di organisasi AWS Anda, Anda harus memiliki izin berikut:

- `organizations:DescribeOrganization`– hanya diperlukan bila menggunakan konsol Organizations
- `organizations:DescribePolicy`– hanya diperlukan bila menggunakan konsol Organizations
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

Untuk mengedit tag yang dilampirkan pada kebijakan berhenti berlangganan layanan AI

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada laman Kebijakan berhenti berlangganan layanan AI, pilih nama kebijakan dengan tag yang ingin Anda edit.
3. Pada laman detail kebijakan yang dipilih, pilih tab Tag, dan kemudian pilih Kelola tag.
4. Anda dapat melakukan salah satu tindakan berikut di laman ini:

- Edit nilai untuk tag dengan memasukkan nilai baru menggantikan yang lama. Anda tidak dapat memodifikasi kunci. Untuk mengubah kunci, Anda harus menghapus tag dengan kunci yang lama dan menambahkan tag dengan kunci yang baru.
- Hapus tag yang ada dengan memilih Hapus.
- Tambahkan kunci tag dan pasangan nilai baru. Pilih Tambahkan tag, lalu masukkan nama kunci baru dan nilai opsional dalam kotak yang disediakan. Jika Anda membiarkan kotak Nilai kosong, nilai-nya adalah string kosong; itu bukan `null`.

5. Pilih Simpan perubahan setelah Anda melakukan semua penambahan, penghapusan, dan pengeditan yang ingin Anda buat.

AWS CLI & AWS SDKs

Untuk mengedit tag yang dilampirkan pada kebijakan berhenti berlangganan layanan AI

Anda dapat menggunakan salah satu perintah berikut untuk mengedit tag yang dilampirkan pada kebijakan berhenti berlangganan layanan AI:

- AWS CLI: tag-resource dan untag-resource
- AWS SDK: TagResourcedan UntagResource

Membuat kebijakan berhenti berlangganan layanan AI

Saat masuk ke akun pengelolaan organisasi, Anda dapat menghapus kebijakan yang tidak diperlukan lagi di organisasi.

Sebelum Anda dapat menghapus kebijakan, Anda harus melepasnya terlebih dahulu dari semua entitas terlampir.

Izin minimum

Untuk menghapus kebijakan, Anda harus memiliki izin untuk melakukan tindakan berikut:

- `organizations:DescribePolicy` (konsol saja — untuk menavigasi ke kebijakan)
- `organizations:DeletePolicy`

AWS Management Console

Untuk menghapus kebijakan berhenti berlangganan layanan AI

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada laman Kebijakan berhenti berlangganan layanan AI, pilih nama kebijakan yang ingin Anda hapus.
3. Anda harus melepaskan kebijakan yang ingin Anda hapus dari semua akar, OU, dan akun. Pilih tab Target, pilih tombol radio yang ada di samping setiap root, OU, atau akun yang ditampilkan di daftar Target, dan kemudian pilih Lepaskan. Dalam kotak dialog konfirmasi, pilih Lepaskan. Ulangi sampai Anda menghapus semua target.
4. Pilih Hapus di bagian atas halaman.
5. Pada kotak dialog konfirmasi, masukkan nama kebijakan, dan kemudian pilih Hapus.

AWS CLI & AWS SDKs

Untuk menghapus kebijakan berhenti berlangganan layanan AI

Anda dapat menggunakan salah satu dari berikut ini untuk menghapus kebijakan:

- AWS CLI: hapus-kebijakan

  Contoh berikut menghapus kebijakan yang ditentukan. Ia berfungsi hanya jika kebijakan tidak dilampirkan pada root, OU, atau akun apa pun.

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWSSDK: DeletePolicy

Melampirkan dan melepaskan kebijakan berhenti berlangganan layanan AI

Anda dapat menggunakan kebijakan berhenti berlangganan layanan Kecerdasan Buatan (AI) di seluruh organisasi serta di unit organisasi (OU) dan masing-masing akun. Kebijakan berhenti berlangganan layanan AI yang berlaku tergantung pada elemen organisasi yang Anda lampirkan ke:

- Saat Anda melampirkan kebijakan berhenti berlangganan layanan AI ke akar organisasi Anda, kebijakan ini berlaku untuk semua anggota OU dan akun akar.
- Ketika Anda melampirkan kebijakan berhenti berlangganan layanan AI ke OU, kebijakan tersebut berlaku untuk akun yang ada di OU atau salah satu OU anak. Akun tersebut juga tunduk pada kebijakan apa pun yang dilampirkan pada akar organisasi.
- Ketika Anda melampirkan kebijakan berhenti berlangganan layanan AI ke akun, kebijakan tersebut hanya berlaku untuk akun tersebut. Akun ini juga tunduk pada kebijakan yang dilampirkan pada akar organisasi dan OU apa pun yang dimiliki akun tersebut.

Agregasi kebijakan berhenti berlangganan layanan AI yang diwarisi akun dari akar dan OU induk, serta kebijakan apa pun yang secara langsung dilampirkan pada akun, adalah kebijakan efektif. Untuk informasi selengkapnya tentang bagaimana kebijakan digabung ke kebijakan efektif, lihat Memahami warisan kebijakan manajemen.

Izin minimum

Untuk melampirkan kebijakan berhenti berlangganan layanan AI, Anda harus memiliki izin untuk melakukan tindakan berikut:

- `organizations:AttachPolicy`

AWS Management Console

Anda dapat melampirkan kebijakan berhenti berlangganan layanan AI dengan menavigasi ke kebijakan atau akar, OU, atau akun yang Anda ingin lampiri dengan kebijakan.

Untuk melampirkan kebijakan opt-out layanan AI dengan menavigasi ke akar, OU, atau akun

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Akun AWS, buka dan lalu pilih nama root, OU, atau akun yang ingin Anda lampirkan kebijakan padanya. Anda mungkin harus memperluas OU (pilih ▶) untuk menemukan OU atau akun yang Anda inginkan.

3. Di tab Kebijakan, dalam entri untuk Kebijakan berhenti berlangganan layanan AI, pilih Lampirkan.
4. Temukan kebijakan yang Anda inginkan dan pilih Lampirkan kebijakan.

   Daftar kebijakan berhenti berlangganan layanan AI terlampir di tab Kebijakan diperbarui sehingga menyertakan tambahan baru. Perubahan kebijakan berlaku segera.

Untuk melampirkan kebijakan berhenti berlangganan layanan AI dengan menavigasi ke akar, OU, atau akun

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada laman Kebijakan berhenti berlangganan layanan AI, pilih nama kebijakan yang ingin Anda lampirkan.
3. Di tab Target, pilih Lampirkan.
4. Pilih tombol radio yang ada di samping root, OU, atau akun yang ingin Anda lampirkan kebijakan padanya. Anda mungkin harus memperluas OU (pilih ▶) untuk menemukan OU atau akun yang Anda inginkan.
5. Pilih Lampirkan kebijakan.

   Daftar kebijakan berhenti berlangganan layanan AI terlampir di tab Target diperbarui sehingga menyertakan tambahan baru. Perubahan kebijakan berlaku segera.

AWS CLI & AWS SDKs

Lampirkan kebijakan berhenti berlangganan layanan AI ke akar, OU, atau akun organisasi Anda.

Anda dapat menggunakan salah satu perintah berikut untuk melampirkan kebijakan berhenti berlangganan layanan AI:

- AWS CLI: attach-policy

  Contoh berikut melampirkan kebijakan ke OU.

```
$ aws organizations attach-policy \
    --target-id ou-a1b2-f6g7h222 \
```

```
    --policy-id p-i9j8k7l6m5
```

Perintah ini tidak menghasilkan output bila berhasil.

- AWSSDK: AttachPolicy

Perubahan kebijakan langsung berlaku.

Melepaskan kebijakan berhenti berlangganan layanan AI

Saat masuk ke akun manajemen organisasi, Anda dapat melepaskan kebijakan berhenti berlanggan layanan AI dari akar organisasi, OU, atau akun yang dilampirinya. Setelah Anda melepaskan kebijakan berhenti berlangganan layanan AI dari sebuah entitas, kebijakan tersebut tidak lagi berlaku untuk akun yang sebelumnya dipengaruhi oleh entitas yang sekarang dilepas. Untuk melepaskan kebijakan, lakukan langkah-langkah berikut.

Izin minimum

Untuk melepaskan kebijakan berhenti berlangganan layanan AI dari akar organisasi, OU, atau akun, Anda harus memiliki izin untuk melakukan tindakan-tindakan berikut:

- `organizations:DetachPolicy`

AWS Management Console

Anda dapat melepasan kebijakan berhenti berlangganan layanan AI dengan menavigasi ke kebijakan atau akar, OU, atau akun yang Anda ingin kebijakannya dilepaskan.

Untuk melampirkan kebijakan berhenti berlangganan layanan AI dengan menavigasi ke akar, OU, atau akun yang dilampirinya

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Akun AWS navigasi ke akar, OU, atau akun yang ingin Anda lepaskan kebijakan darinya. Anda mungkin harus memperluas OU (pilih ▶) untuk menemukan OU atau akun yang Anda inginkan. Pilih nama Akar, OU, atau akun.

3. Pada tab Kebijakan, pilih tombol radio yang ada di samping kebijakan berhenti berlangganan layanan AI yang ingin Anda lepaskan, dan kemudian pilih Lepaskan.
4. Di kotak dialog konfirmasi, pilih Lepaskan kebijakan.

   Daftar kebijakan berhenti berlangganan layanan AI terlampir diperbarui. Perubahan kebijakan berlaku segera.

Untuk melepaskan kebijakan berhenti berlangganan layanan AI dengan menavigasi ke kebijakan

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada laman Kebijakan berhenti berlangganan layanan AI, pilih nama kebijakan yang ingin Anda lepaskan dari akar, OU, atau akun.
3. Pada tab Target, pilih tombol radio yang ada di sebelah akar, OU, atau akun yang kebijakannya ingin Anda lepaskan. Anda mungkin harus memperluas OU (pilih ▶) untuk menemukan OU atau akun yang Anda inginkan.
4. Pilih Lepaskan.
5. Dalam kotak dialog konfirmasi, pilih Lepaskan.

   Daftar kebijakan berhenti berlangganan layanan AI terlampir diperbarui. Perubahan kebijakan berlaku segera.

AWS CLI & AWS SDKs

Untuk melepaskan kebijakan berhenti berlangganan layanan AI dari akar organisasi, OU, atau akun

Anda dapat menggunakan salah satu perintah berikut untuk melampirkan kebijakan berhenti berlangganan layanan AI:

- AWS CLI: detach-policy

  Contoh berikut melepaskan kebijakan dari OU.

```
$ aws organizations detach-policy \
    --target-id ou-a1b2-f6g7h222 \
```

```
    --policy-id p-i9j8k7l6m5
```

Perintah ini tidak menghasilkan output saat berhasil.

- AWSSDK: DetachPolicy

Perubahan kebijakan langsung berlaku.

Melihat kebijakan berhenti berlangganan layanan AI yang efektif

Tentukan kebijakan berhenti berlanganan layanan Kecerdasan Buatan (AI) yang efektif untuk akun di organisasi Anda.

Apa kebijakan berhenti berlangganan layanan AI yang efektif?

kebijakan berhenti berlangganan layanan AI yang efektif menentukan aturan akhir yang berlaku untuk Akun AWS. Ini adalah agregasi dari setiap kebijakan berhenti berlangganan layanan AI yang diwarisi akun, ditambah kebijakan berhenti berlangganan layanan AI yang secara langsung dilampirkan pada akun. Bila Anda melampirkan kebijakan berhenti berlangganan layanan AI ke akar organisasi, kebijakan tersebut berlaku untuk semua akun di organisasi Anda. Ketika Anda melampirkan kebijakan berhenti berlangganan layanan AI ke OU, maka kebijakan tag tersebut akan berlaku untuk semua akun yang ada di OU tersebut. Bila Anda melampirkan kebijakan secara langsung ke akun, kebijakan tersebut hanya berlaku untuk akun Akun AWS tersebut.

Misalnya, kebijakan berhenti berlangganan layanan AI yang dilampirkan ke akar organisasi dapat menentukan bahwa semua akun di organisasi berhenti berlangganan penggunaan konten oleh semua layanan machine learning AWS. Sebuah layanan kebijakan berhenti berlangganan layanan AI terpisah yang dilampirkan langsung ke satu akun anggota menentukan bahwa ia memilih untuk menggunakan konten hanya untuk Amazon Rekognition. Kombinasi kebijakan berhenti berlangganan layanan AI ini terdiri atas kebijakan berhenti berlangganan layanan AI yang efektif. Hasilnya adalah bahwa semua akun dalam organisasi berhenti berlangganan semua layanan AWS, dengan pengecualian satu akun yang memilih untuk berlangganan Amazon Rekognition.

Untuk informasi tentang bagaimana kebijakan digabungkan ke kebijakan efektif akhir, lihat Memahami warisan kebijakan manajemen.

Pelajari cara melihat kebijakan berhenti berlangganan layanan AI yang efektif.

Anda dapat melihat kebijakan berhenti berlangganan layanan AI yang efektif untuk akun dari AWS Management Console, API AWS, atau AWS Command Line Interface.

Izin minimum

Untuk melihat kebijakan berhenti berlangganan layanan AI yang efektif untuk akun, Anda harus memiliki izin untuk melakukan tindakan-tindakan berikut:

- `organizations:DescribeEffectivePolicy`
- `organizations:DescribeOrganization` – hanya diperlukan bila menggunakan konsol Organizations

AWS Management Console

Untuk melihat kebijakan berhenti berlangganan layanan AI yang efektif untuk akun.

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada laman Akun AWS, pilih nama akun yang ingin Anda lihat kebijakan berhenti berlangganan layanan AI darinya yang efektif. Anda mungkin harus memperluas OU (pilih ▶) untuk menemukan akun yang Anda inginkan.
3. Pada tab Kebijakan, di bagian Kebijakan berhenti berlangganan layanan AI, pilih Lihat kebijakan AI yang efektif untuk Akun AWS ini.

   Konsol menampilkan kebijakan efektif yang diterapkan pada akun yang ditentukan.

   Note

   Anda tidak dapat menyalin dan menempelkan kebijakan yang efektif dan menggunakannya sebagai JSON untuk kebijakan berhenti berlangganan layanan AI lain tanpa perubahan signifikan. Dokumen kebijakan berhenti berlangganan layanan AI harus mencakup operator warisan yang menentukan bagaimana setiap pengaturan digabung menjadi kebijakan akhir yang efektif.

AWS CLI & AWS SDKs

Untuk melihat kebijakan berhenti berlangganan layanan AI yang efektif untuk akun.

Anda dapat menggunakan salah satu hal berikut untuk melihat kebijakan berhenti berlangganan layanan AI yang efektif:

- AWS CLI: describe-effective-policy

  Contoh berikut menunjukkan kebijakan berhenti berlangganan layanan AI yang efektif untuk akun.

```
$ aws organizations describe-effective-policy \
    --policy-type AISERVICES_OPT_OUT_POLICY \
    --target-id 123456789012
{
    "EffectivePolicy": {
        "PolicyContent": "{\"services\":{\"comprehend\":{\"opt_out_policy\":
\"optOut\"},   ....TRUNCATED FOR BREVITY....   "opt_out_policy\":\"optIn\"}}}",
        "LastUpdatedTimestamp": "2020-12-09T12:58:53.548000-08:00",
        "TargetId": "123456789012",
        "PolicyType": "AISERVICES_OPT_OUT_POLICY"
    }
}
```

- AWSSDK: DescribeEffectivePolicy

Sintaks dan contoh kebijakan berhenti berlangganan layanan AI

Topik ini menjelaskan sintaks kebiajakanan berhenti berlangganan layanan Kecerdasan Buatan (AI) dan memberikan contoh.

Kebijakan berhenti berlangganan layanan AI

Kebijakan berhenti berlangganan layanan AI adalah file plaintext yang terstruktur sesuai dengan aturan JSON. Sintaks untuk kebijakan berhenti berlangganan layanan AI tersebut mengikuti sintaks untuk jenis kebijakan manajemen. Untuk pembahasan lengkap tentang sintaks itu, lihat Memahami warisan kebijakan manajemen. Topik ini berfokus pada penerapan sintaks umum untuk persyaratan spesifik jenis kebijakan berhenti berlangganan layanan AI.

> **Important**
>
> Kapitalisasi nilai-nilai yang dibahas di bagian ini penting. Masukkan nilai dengan huruf besar dan kecil seperti yang ditunjukkan dalam topik ini. Kebijakan tidak bekerja jika Anda menggunakan kapitalisasi yang tidak terduga.

Kebijakan berikut menunjukkan sintaks kebijakan berhenti berlangganan layanan AI dasar. Jika contoh ini dilampirkan langsung ke akun, akun tersebut akan secara eksplisit berhenti berlangganan satu layanan dan memilih untuk berlangganan ke akun lain. Layanan lain dapat berlangganan atau berhenti berlangganan berdasarkan kebijakan yang diwarisi dari tingkatan yang lebih tinggi (kebijakan OU atau akar).

```
{
    "services": {
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "lex": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

Bayangkan contoh kebijakan berikut yang dilampirkan pada akar organisasi. Ini menetapkan default untuk organisasi untuk berhenti berlangganan semua layanan AI. Ini secara otomatis mencakup layanan AI apa pun yang tidak dikecualikan secara eksplisit, termasuk layanan AI apa pun yang mungkin disebarkan AWS di masa depan. Anda dapat melampirkan kebijakan anak untuk OU atau langsung ke akun untuk menimpa pengaturan ini untuk setiap layanan AI kecuali Amazon Comprehend. Entri kedua dalam contoh berikut menggunakan atur `@@operators_allowed_for_child_policies` ke `none` untuk mencegahnya ditimpa. Entri ketiga dalam contoh membuat pembebasan organisasi luas untuk Amazon Rekognition. Ini berlangganan di seluruh organisasi untuk layanan tersebut, tetapi kebijakan tidak memungkinkan kebijakan anak menimpa jika sesuai.

```
{
    "services": {
        "default": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "comprehend": {
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        },
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

Sintaks kebijakan berhenti berlangganan semua layanan AI mencakup elemen-elemen berikut:

- Elemen `services`. Kebijakan berhenti berlangganan semua layanan AI diidentifikasi berdasarkan nama tetap ini sebagai elemen yang mengandung JSON terluar.

  Kebijakan berhenti berlangganan semua layanan AI dapat memiliki satu atau lebih pernyataan di bawah elemen `services`. Setiap pasangan kunci berisi elemen berikut:

  - Kunci nama layanan yang mengidentifikasi layanan AWS AI. Nama-nama kunci berikut adalah nilai yang valid untuk bidang ini:
    - **`default`** – mewakili semua layanan AI yang saat ini tersedia dan secara implisit dan otomatis mencakup setiap layanan AI yang mungkin ditambahkan di masa mendatang.
    - `awssupplychain`
    - `chimesdkvoiceanalytics`
    - `cloudwatch`
    - `codeguruprofiler`
    - `codewhisperer`
    - `comprehend`

- `connectamd`
- `connectoptimization`
- `contactlens`
- `datazone`
- `entityresolution`
- `frauddetector`
- `glue`
- `guardduty`
- `lex`
- `polly`
- `q`
- `quicksightq`
- `rekognition`
- `securitylake`
- `textract`
- `transcribe`
- `translate`

Setiap pernyataan kebijakan yang diidentifikasi oleh kunci nama layanan dapat berisi unsur-unsur berikut:

- Kunci `opt_out_policy`. Kunci ini harus ada. Ini adalah satu-satunya kunci yang dapat Anda tempatkan di bawah kunci nama layanan.

  Kunci `opt_out_policy` dapat berisi saja dari operator `@@assign` dengan salah satu nilai berikut:

  - `optOut` – Anda memilih berhenti berlangganan penggunaan konten untuk layanan AI yang ditentukan.
  - `optIn` – Anda memilih berhenti berlangganan penggunaan konten untuk layanan AI yang ditentukan.

> **Catatan**
>
> - Anda tidak dapat menggunakan operator warisan `@@append` dan `@@remove` dalam kebijakan berhenti berlangganan layanan AI.
> - Anda tidak dapat menggunakan operator `@@enforced_for` dalam kebijakan berhenti berlangganan layanan AI.

- Pada tingkat apa pun, Anda dapat menentukan operator `@@operators_allowed_for_child_policies` untuk mengontrol kebijakan anak yang dapat dilakukan untuk menimpa pengaturan yang diberlakukan oleh kebijakan induk. Anda dapat menentukan salah satu nilai berikut:
  - `@@assign` – kebijakan anak dari kebijakan ini dapat menggunakan operator `@@assign` untuk menimpa nilai yang diwariskan dengan nilai yang berbeda.
  - `@@none` – kebijakan anak dari kebijakan ini tidak dapat mengubah nilainya.

  Perilaku `@@operators_allowed_for_child_policies` tergantung pada di mana Anda menempatkannya. Anda dapat menggunakan lokasi berikut:
  - Di bawah kunci `services` – mengontrol apakah kebijakan anak dapat menambah atau mengubah daftar layanan dalam kebijakan efektif.
  - Di bawah kunci untuk layanan AI tertentu atau kunci `default` - mengontrol apakah kebijakan anak dapat menambah atau mengubah daftar kunci di bawah entri khusus ini.
  - Di bawah kunci `opt_out_policies` untuk layanan tertentu – mengontrol apakah kebijakan anak hanya dapat mengubah pengaturan untuk layanan khusus ini.

Sintaks dan contoh kebijakan berhenti berlangganan layanan AI

Contoh kebijakan berikut untuk tujuan informasi saja.

Contoh 1: Berhenti berlangganan semua layanan AI untuk semua akun di organisasi

Contoh berikut menunjukkan kebijakan yang dapat dilampirkan ke akar organisasi Anda untuk berhenti berlangganan layanan AI untuk akun di organisasi Anda.

> **Tip**
>
> Jika Anda menyalin contoh berikut menggunakan tombol salin di sudut kanan atas contoh, salinan tidak termasuk nomor baris. Sudah siap untuk ditempelkan.

```
    | {
    |     "services": {
[1] |         "@@operators_allowed_for_child_policies": ["@@none"],
    |         "default": {
[2] |             "@@operators_allowed_for_child_policies": ["@@none"],
    |             "opt_out_policy": {
[3] |                 "@@operators_allowed_for_child_policies": ["@@none"],
    |                 "@@assign": "optOut"
    |             }
    |         }
    |     }
    | }
```

- [1] – `"@@operators_allowed_for_child_policies": ["@@none"]` yang berada di bawah `services` mencegah kebijakan anak apa pun dari menambahkan setiap bagian baru untuk layanan individual selain bagian `default` yang sudah ada. `Default` adalah placeholder yang mewakili "semua layanan AI".
- [2] – `"@@operators_allowed_for_child_policies": ["@@none"]` yang berada di bawah `default` mencegah setiap kebijakan anak menambahkan setiap bagian baru selain bagian `opt_out_policy` bagian yang sudah ada.
- [3] – `"@@operators_allowed_for_child_policies": ["@@none"]` yang berada di bawah `opt_out_policy` mencegah kebijakan anak mengubah nilai `optOut` mengatur atau menambah pengaturan tambahan.

Contoh 2: Tetapkan pengaturan default organisasi untuk semua layanan, tetapi izinkan kebijakan anak menimpa pengaturan untuk layanan individual

Contoh kebijakan berikut mengatur default seluruh organisasi untuk semua layanan AI. Nilai untuk `default` mencegah kebijakan anak dari mengubah nilai `optOut` untuk layanan `default`, placeholder untuk semua layanan AI. Jika kebijakan ini diterapkan sebagai kebijakan induk dengan melampirkan ke akar atau OU, kebijakan anak masih dapat mengubah pengaturan berhenti berlangganan untuk layanan individual, seperti yang ditunjukkan pada kebijakan kedua.

- Karena tidak ada `"@@operators_allowed_for_child_policies": ["@@none"]` di bawah kunci `services`, kebijakan anak dapat menambahkan bagian baru untuk layanan individu.
- `"@@operators_allowed_for_child_policies": ["@@none"]` yang berada di bawah `default` mencegah setiap kebijakan anak menambahkan setiap bagian baru selain bagian `opt_out_policy` yang sudah ada.
- `"@@operators_allowed_for_child_policies": ["@@none"]` yang berada di bawah `opt_out_policy` mencegah kebijakan anak mengubah nilai `optOut` mengatur atau menambah pengaturan tambahan.

Kebijakan induk opt-out layanan UserAI root organisasi

```
{
    "services": {
        "default": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "opt_out_policy": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@assign": "optOut"
            }
        }
    }
}
```

Kebijakan contoh berikut mengasumsikan bahwa kebijakan contoh sebelumnya dilampirkan ke akar organisasi atau OU induk, dan bahwa Anda melampirkan contoh ini ke akun yang dipengaruhi oleh kebijakan induk. Ini menimpa pengaturan berhenti berlangganan default dan secara eksplisit berlangganan layanan Amazon Lex saja.

Layanan AI memilih keluar kebijakan anak

```
{
    "services": {
        "lex": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
        }
    }
}
```

Kebijakan efektif yang dihasilkan untuk Akun AWS ini adalah bahwa akun hanya memilih Amazon Lex, dan memilih keluar dari semua layanan AWS AI lainnya karena pengaturan `default` opt-out yang diwariskan dari kebijakan induk.

Contoh 3: Tentukan kebijakan berhenti berlangganan layanan AI di seluruh organisasi untuk satu layanan

Contoh berikut menunjukkan kebijakan berhenti berlangganan layanan AI yang menentukan pengaturan `optOut` untuk satu layanan AI. Jika kebijakan ini dilampirkan ke akar organisasi, ini mencegah kebijakan anak dari menimpa pengaturan `optOut` untuk satu layanan ini. Layanan lain tidak ditangani dengan kebijakan ini, tetapi dapat dipengaruhi oleh kebijakan anak di OU atau akun lain.

```
{
    "services": {
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optOut",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        }
    }
}
```

Kebijakan Backup

AWS Backup memungkinkan Anda untuk membuat paket backup yang menentukan cara mencadangkan sumber daya AWS. Aturan dalam paket tersebut mencakup berbagai pengaturan, seperti frekuensi backup, jendela waktu di mana backup terjadi, Wilayah AWS yang berisi sumber daya yang akan di-backup dan vault di mana backup akan disimpan. Anda kemudian dapat menerapkan paket backup ke grup sumber AWS yang diidentifikasi dengan menggunakan tag. Anda juga harus mengidentifikasi AWS Identity and Access Management (IAM) role yang memberikan AWS Backup izin untuk melakukan operasi backup atas nama Anda.

Kebijakan Backup di AWS Organizations menggabungkan semua potongan itu ke dalam dokumen teks JSON. Anda dapat melampirkan kebijakan bakcup untuk salah satu elemen dalam struktur organisasi Anda, seperti root, unit organisasi (OU), dan masing-masing akun. Organizations menerapkan aturan warisan untuk menggabungkan kebijakan di root organisasi, OU induk, atau dilampirkan pada akun. Hal ini menghasilkan kebijakan backup efektif untuk setiap akun. Kebijakan efektif ini menginstruksikan AWS Backup cara mencadangkan sumber daya AWS secara otomatis.

Kebijakan Backup memberi Anda kontrol terperinci atas pencadangan sumber daya Anda di tingkat apa pun yang dibutuhkan organisasi Anda. Sebagai contoh, Anda dapat menentukan dalam kebijakan yang terlampir pada root organisasi bahwa semua tabel Amazon DynamoDB harus dicadangkan. Kebijakan tersebut dapat mencakup frekuensi backup default. Anda kemudian dapat melampirkan kebijakan backup untuk OU yang akan menimpa frekuensi backup sesuai dengan persyaratan masing-masing OU. Sebagai contoh, OU `Developers` mungkin menentukan frekuensi backup sekali per minggu, sedangkan OU `Production` menentukan sekali per hari.

Anda dapat membuat kebijakan backup parsial yang secara individual mencakup hanya sebagian dari informasi yang diperlukan untuk berhasil melakukan pencadangan sumber daya Anda. Anda dapat melampirkan kebijakan ini ke bagian yang berbeda dari pohon organisasi, seperti root atau OU induk, dengan maksud agar kebijakan parsial tersebut diwarisi oleh OU dan akun di tingkat rendah. Ketika Organizations menggabungkan semua kebijakan untuk akun dengan menggunakan aturan warisan, kebijakan efektif yang dihasilkan harus memiliki semua elemen yang diperlukan. Jika tidak, AWS Backup menganggap kebijakan tidak valid dan tidak membuat backup sumber daya yang terpengaruh.

> **Important**
>
> AWS Backup hanya dapat melakukan backup dengan sukses ketika dipanggil oleh kebijakan efektif lengkap yang memiliki semua elemen yang diperlukan.
> Meskipun strategi kebijakan parsial seperti yang dijelaskan sebelumnya dapat bekerja, namun jika kebijakan efektif untuk akun tidak lengkap, maka hal itu akan mengakibatkan kesalahan atau sumber daya tidak berhasil dicadangkan. Sebagai strategi alternatif, pertimbangkan untuk mengharuskan semua kebijakan backup harus lengkap dan valid sendiri. Gunakan nilai default yang diberikan oleh kebijakan yang dilampirkan lebih tinggi dalam hirarki, dan menimpa mereka jika diperlukan dalam kebijakan anak dengan menyertakan operator kontrol warisan anak.

Paket backup yang efektif untuk setiap Akun AWS dalam organisasi akan muncul di konsol AWS Backup sebagai paket tetap untuk akun tersebut. Anda bisa melihatnya, tapi tidak bisa mengubahnya.

Saat AWS Backup memulai melakukan backup berdasarkan rencana backup yang dibuat kebijakan, Anda dapat melihat status tugas backup di konsol AWS Backup. Pengguna di akun anggota dapat melihat status dan kesalahan untuk tugas backup di akun anggota tersebut. Jika Anda juga mengaktifkan akses layanan tepercaya dengan AWS Backup, pengguna di akun pengelolaan

organisasi dapat melihat status dan kesalahan untuk semua tugas backup dalam organisasi. Untuk informasi selengkapnya, lihat Mengaktifkan pengelolaan lintas akun di Panduan Developer AWS Backup.

Memulai kebijakan backup

Ikuti langkah berikut untuk mulai menggunakan kebijakan backup.

1. Pelajari tentang izin yang harus Anda miliki untuk melakukan tugas kebijakan backup.
2. Pelajari tentang beberapa praktik terbaik yang kami sarankan saat menggunakan kebijakan backup.
3. Mengaktifkan kebijakan backup untuk organisasi Anda.
4. Membuat kebijakan backup.
5. Melampirkan kebijakan backup ke root organisasi Anda, OU, atau akun.
6. Melihat kebijakan backup efektif gabungan yang berlaku untuk akun.

Untuk semua langkah-langkah ini, Anda masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna root (tidak disarankan) di akun manajemen organisasi.

Informasi lainnya

- Pelajari sintaks kebijakan cadangan dan lihat contoh kebijakan

Prasyarat dan izin untuk mengelola kebijakan backup

Halaman ini menjelaskan prasyarat dan izin yang diperlukan untuk mengelola kebijakan backup di AWS Organizations.

Topik

- Prasyarat untuk mengelola kebijakan backup
- Izin untuk mengelola kebijakan backup

Prasyarat untuk mengelola kebijakan backup

Untuk mengelola kebijakan backup di organisasi memerlukan hal-hal berikut ini:

- Organisasi Anda harus mengaktifkan semua fitur.

- Anda harus masuk ke akun pengelolaan organisasi Anda.
- Pengguna atau peran AWS Identity and Access Management (IAM) harus memiliki izin yang tercantum di bagian berikut.

Izin untuk mengelola kebijakan backup

Contoh kebijakan IAM berikut menyediakan izin untuk mengelola semua aspek kebijakan backup dalam sebuah organisasi.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageBackupPolicies",
            "Effect": "Allow",
            "Action": [
                "organizations:AttachPolicy",
                "organizations:CreatePolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeAccount",
                "organizations:DescribeCreateAccountStatus",
                "organizations:DescribeEffectivePolicy",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribePolicy",
                "organizations:DetachPolicy",
                "organizations:DisableAWSServiceAccess",
                "organizations:DisablePolicyType",
                "organizations:EnableAWSServiceAccess",
                "organizations:EnablePolicyType",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListCreateAccountStatus",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListPolicies",
                "organizations:ListPoliciesForTarget",
                "organizations:ListRoots",
                "organizations:ListTargetsForPolicy",
                "organizations:UpdatePolicy"
            ],
```

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

Untuk informasi selengkapnya tentang kebijakan IAM dan izin, lihat Panduan Pengguna IAM.

Praktik terbaik untuk menggunakan kebijakan backup

AWS merekomendasikan praktik terbaik berikut untuk menggunakan kebijakan backup.

Memutuskan strategi kebijakan backup

Anda dapat membuat kebijakan backup dalam potongan yang tidak lengkap yang diwariskan dan digabung untuk membuat kebijakan lengkap untuk masing-masing akun anggota. Jika Anda melakukan ini, Anda berisiko berakhir dengan kebijakan efektif yang tidak lengkap jika Anda membuat perubahan pada satu tingkat tanpa mempertimbangkan dengan hati-hati dampak perubahan pada semua akun di bawah tingkat tersebut. Untuk mencegah hal ini, kami merekomendasikan agar Anda sebaliknya memastikan bahwa kebijakan backup yang Anda terapkan di semua tingkat sudah lengkap dengan sendirinya. Perlakukan kebijakan induk sebagai kebijakan default yang dapat diganti dengan pengaturan yang ditentukan dalam kebijakan anak. Dengan begitu, meskipun kebijakan anak tidak ada, namun kebijakan yang diwariskan sudah lengkap dan menggunakan nilai default. Anda dapat mengontrol pengaturan yang dapat ditambahkan ke, diubah, atau dihapus oleh kebijakan anak dengan menggunakan operator warisan kontrol anak.

Validasi perubahan pada pemeriksaan kebijakan backup Anda menggunakan **`GetEffectivePolicy`**

Setelah Anda membuat perubahan ke kebijakan backup, periksa kebijakan efektif untuk akun perwakilan di bawah tingkat di mana Anda membuat perubahan. Anda dapat melihat kebijakan efektif dengan menggunakan AWS Management Console, atau dengan menggunakan operasi API GetEffectivePolicy atau salah satu varian SDK AWS CLI atau AWS. Pastikan bahwa perubahan yang Anda buat memiliki dampak yang diinginkan pada kebijakan efektif.

Mulai dengan sederhana dan buat perubahan kecil

Untuk menyederhanakan debugging, mulai dengan kebijakan sederhana dan buat perubahan satu item pada satu waktu. Validasi perilaku dan dampak dari setiap perubahan sebelum membuat perubahan berikutnya. Pendekatan ini mengurangi jumlah variabel yang harus Anda hitung ketika kesalahan atau hasil yang tidak terduga tidak terjadi.

Menyimpan salinan backup Anda di Wilayah AWS dan akun lain di organisasi Anda

Untuk meningkatkan posisi pemulihan bencana Anda, Anda dapat menyimpan salinan backup Anda.

- Wilayah yang berbeda — Jika anda menyimpan salinan backup dalam Wilayah AWS tambahan, Anda membantu melindungi backup dari kerusakan yang tidak disengaja atau penghapusan di Wilayah asli. Gunakan bagian `copy_actions` dari kebijakan untuk menentukan vault dalam satu Wilayah atau lebih dari akun yang sama di mana paket backup berjalan. Untuk melakukannya, identifikasi akun dengan menggunakan variabel `$account` ketika Anda menentukan ARN dari ruang penyimpanan backup untuk menyimpan salinan backup. `$account` secara otomatis diganti pada waktu aktif dengan ID akun di mana kebijakan backup sedang berjalan.
- Akun yang berbeda — Jika anda menyimpan salinan backup dalam Akun AWS tambahan, Anda menambahkan penghalang keamanan yang membantu melindungi dari aktor jahat yang membahayakan salah satu akun Anda. Gunakan bagian `copy_actions` dari kebijakan untuk menentukan vault dalam satu akun atau lebih di organisasi Anda, terpisah dari akun di mana paket backup berjalan. Untuk melakukannya, identifikasi akun dengan menggunakan nomor ID akun sebenarnya ketika Anda menentukan ARN ruang penyimpanan backup untuk menyimpan salinan backup.

Batasi jumlah paket per kebijakan

Kebijakan yang berisi beberapa paket lebih rumit dalam pemecahan masalahnya karena jumlah output yang lebih besar yang harus divalidasi semuanya. Sebaliknya, miliki kebijakan yang masing-masing berisi satu dan satu-satunya paket backup untuk menyederhanakan debugging dan pemecahan masalah. Anda kemudian dapat menambahkan kebijakan tambahan dengan paket lain untuk memenuhi persyaratan lainnya. Pendekatan ini membantu menjaga agar setiap masalah paket terisolasi untuk satu kebijakan, dan mencegah masalah tersebut agar tidak mempersulit pemecahan masalah dengan kebijakan lain dan paketnya.

Gunakan set tumpukan untuk membuat ruang penyimpanan backup dan IAM role yang diperlukan

Gunakan integrasi set tumpukan AWS CloudFormation dengan Organizations untuk secara otomatis membuat ruang penyimpanan backup yang diperlukan dan AWS Identity and Access Management (IAM) role di setiap akun anggota di organisasi Anda. Anda dapat membuat set tumpukan yang mencakup sumber daya yang Anda inginkan secara otomatis tersedia di setiap Akun AWS di organisasi Anda. Pendekatan ini memungkinkan Anda untuk menjalankan paket backup Anda dengan jaminan bahwa dependensinya sudah terpenuhi. Untuk informasi lebih lanjut, lihat Membuat Set Tumpukan dengan Izin Dikelola Sendiri di Panduan Pengguna AWS CloudFormation.

Periksa hasil Anda dengan meninjau backup pertama yang dibuat di masing-masing akun

Ketika Anda membuat perubahan pada kebijakan, periksa backup berikutnya yang dibuat setelah perubahan itu untuk memastikan perubahan memiliki dampak yang diinginkan. Langkah ini lebih dari sekedar melihat kebijakan efektif dan memastikan bahwa AWS Backup menafsirkan kebijakan Anda dan menerapkan paket backup sesuai keinginan Anda.

Membuat, memperbarui, dan menghapus kebijakan backup

Dalam topik ini:

- Setelah Anda mengaktifkan kebijakan backup untuk organisasi Anda, Anda dapat membuat kebijakan.
- Bila persyaratan backup berubah, Anda dapat memperbarui kebijakan yang ada.
- Bila Anda tidak lagi memerlukan kebijakan dan setelah melepaskannya dari semua unit organisasi (OU) dan akunmaka , Anda dapat menghapusnya.

Membuat kebijakan backup

> **Izin minimum**
>
> Untuk membuat kebijakan backup, Anda perlu izin untuk menjalankan tindakan-tindakan berikut:
>
> - `organizations:CreatePolicy`

AWS Management Console

Anda dapat membuat kebijakan backup di AWS Management Console dengan menggunakan salah satu dari dua cara berikut:

- Editor visual yang memungkinkan Anda memilih opsi dan menghasilkan teks kebijakan JSON untuk Anda.
- Editor teks yang memungkinkan Anda langsung membuat teks kebijakan JSON sendiri.

Editor visual membuat prosesnya mudah, namun membatasi fleksibilitas Anda. Ini adalah cara yang bagus untuk membuat kebijakan pertama Anda dan merasa nyaman menggunakannya.

Setelah Anda memahami cara kerjanya dan mulai dibatasi oleh apa yang disediakan editor visual, Anda dapat menambahkan fitur lanjutan ke kebijakan Anda dengan mengedit teks kebijakan JSON sendiri. Editor visual hanya menggunakan operator pengaturan-nilai @@assign, dan tidak menyediakan akses apa pun ke operator kontrol anak. Anda dapat menambahkan operator kontrol anak hanya jika Anda mengedit teks kebijakan JSON secara manual.

Untuk membuat kebijakan backup

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Kebijakan Backup, pilih Buat Kebijakan.
3. Pada halaman Bua kebijakan, masukkan Nama kebijakan dan Deskripsi kebijakan opsional.
4. (Opsional) Anda dapat menambahkan satu tag atau lebih ke kebijakan tersebut dengan memilih Tambahkan tag dan kemudian masukkan kunci dan nilai opsional. Membiarkan nilai kosong akan mengaturnya menjadi string kosong; itu bukan `null`. Anda dapat melampirkan hingga 50 tag ke kebijakan. Untuk informasi lebih lanjut tentang penandaan, lihat Penandaan pada sumber daya AWS Organizations.
5. Anda dapat membangun kebijakan dengan menggunakan Editor visual seperti yang diterangkan dalam prosedur ini. Anda juga dapat memasukkan atau menempelkan teks kebijakan di tab JSON. Untuk informasi tentang sintaksis kebijakan backup, lihat Sintaksis kebijakan Backup dan contoh.

   Jika Anda memilih untuk menggunakan Editor visual, pilih opsi backup yang sesuai untuk skenario Anda. Sebuah paket backup terdiri dari tiga bagian. Untuk informasi selengkapnya tentang elemen-elemen paket backup ini, lihat Membuat paket backup dan Menetapkan sumber daya di Panduan Developer AWS Backup.

   a. Detail umum paket Backup

      - Nama paket Backup dapat terdiri dari alfanumerik, tanda hubung, dan karakter garis bawah saja.
      - Anda harus memilih setidaknya satu Wilayah paket Backup dari daftar. Paket ini dapat mencadangkan sumber daya hanya dalam Wilayah AWS pilihan.

   b. Satu atau lebih aturan backup yang menentukan bagaimana dan kapan AWS Backup beroperasi. Setiap aturan backup mendefinisikan item berikut:

- Jadwal yang mencakup frekuensi backup dan jendela waktu di mana backup dapat terjadi.
- Nama ruang penyimpanan backup yang akan digunakan. Nama ruang penyimpanan Backup dapat terdiri dari alfanumerik, tanda hubung, dan karakter garis bawah saja. Ruang penyimpanan backup harus ada sebelum paket dapat berhasil dijalankan. Buat ruang penyimpanan menggunakan konsol AWS Backup atau perintah AWS CLI.
- (Opsional) Satu atau lebih Salin ke wilayah berlaku untuk juga menyalin backup ke ruang penyimpanan di Wilayah AWS lainnya.
- Satu pasangan kunci dan nilai tag atau lebih yang akan dilampirkan ke titik pemulihan backup dibuat setiap kali paket backup ini berjalan.
- Opsi siklus hidup yang menentukan kapan backup beralih ke penyimpanan dingin, dan saat backup habis masa berlakunya.

Pilih Tambahkan aturan untuk menambahkan setiap aturan yang Anda butuhkan pada paket.

Untuk informasi lebih lanjut tentang aturan backup, lihat Aturan Backup di Panduan Developer AWS Backup.

c. Sebuah tugas sumber daya yang menentukan sumber daya mana yang harus di-backup oleh AWS Backup dengan paket ini. Tugas ini dibuat dengan menentukan pasangan tag yang digunakan AWS Backup untuk menemukan dan mencocokkan sumber daya
   - Nama tugas sumber daya dapat terdiri dari alfanumerik, tanda hubung, dan karakter garis bawah saja.
   - Tentukan IAM role untuk AWS Backup yang akan digunakan untuk melakukan backup dengan namanya.

     Dalam konsol tersebut, Anda tidak menentukan seluruh Amazon Resource Name (ARN). Anda harus menyertakan nama peran dan prefiks-nya yang menentukan jenis peran. Prefiks biasanya `role` atau `service-role`, dan mereka terpisah dari nama peran dengan garis miring ('/'). Misalnya, Anda dapat memasukkan `role/MyRoleName` atau `service-role/MyManagedRoleName`. Ini kemudian dikonversi ke ARN penuh untuk Anda ketika disimpan dalam JSON mendasari.

> **Important**
>
> IAM role yang ditentukan harus sudah ada di akun yang padanya kebijakan diterapkan. Jika tidak, paket backup mungkin berhasil memulai tugas backup, tetapi tugas backup tersebut akan gagal.

- Tentukan satu atau lebih pasangan Kunci tag sumber daya dan Nilai tag untuk mengidentifikasi sumber daya yang ingin Anda backup. Jika ada lebih dari satu nilai tag, pisahkan nilai-nilai tersebut dengan koma.

Pilih Tambahkan tugas untuk menambahkan setiap tugas sumber daya dikonfigurasi ke paket backup.

Untuk informasi lebih lanjut, lihat Menetapkan Sumber Daya untuk Paket Backup di Panduan Developer AWS Backup.

6. Setelah selesai membuat kebijakan, pilih Buat kebijakan. Kebijakan tersebut muncul di daftar kebijakan backup yang tersedia.

AWS CLI & AWS SDKs

Untuk membuat kebijakan backup

Anda menggunakan salah satu hal berikut untuk membuat kebijakan backup:

- AWS CLI: buat-kebijakan

Buat paket backup sebagai teks JSON yang mirip dengan berikut ini, dan simpan dalam file teks. Untuk aturan lengkap untuk sintaksis, lihat Sintaksis kebijakan Backup dan contoh.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-
north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 5/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "complete_backup_window_minutes": { "@@assign": "10080" },
```

```
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "180" },
                        "delete_after_days": { "@@assign": "270" }
                    },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "10" },
                                "delete_after_days": { "@@assign": "100" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                        "tag_key": { "@@assign": "dataType" },
                        "tag_value": { "@@assign": [ "PII" ] }
                    }
                }
            }
        }
    }
}
```

Paket backup ini menetapkan bahwa AWS Backup harus membuat backup dari semua sumber daya di Akun AWS terdampak yang ada di Wilayah AWS yang ditentukan dan yang memiliki tag `dataType` dengan nilai `PII`.

Selanjutnya, impor paket backup file kebijakan JSON untuk membuat kebijakan backup baru dalam organisasi. Perhatikan ID kebijakan pada akhir ARN kebijakan dalam keluaran.

```
$ aws organizations create-policy \
    --name "MyBackupPolicy" \
    --type BACKUP_POLICY \
    --description "My backup policy" \
```

```
    --content file://policy.json{
    "Policy": {
        "PolicySummary": {
            "Arn": "arn:aws:organizations::o-aa111bb222:policy/backup_policy/p-
i9j8k7l6m5",
            "Description": "My backup policy",
            "Name": "MyBackupPolicy",
            "Type": "BACKUP_POLICY"
        }
        "Content": "...a condensed version of the JSON policy document you
 provided in the file...",
    }
}
```

- AWSSDK: CreatePolicy

Apa yang harus dilakukan selanjutnya

Setelah membuat kebijakan backup, Anda dapat menerapkan kebijakan Anda. Untuk melakukannya, Anda dapat lampirkan kebijakan untuk organisasi root, unit organisasi (UO), Akun AWS dalam organisasi Anda, atau kombinasi dari entitas organisasi.

Memperbarui kebijakan backup

Saat masuk ke akun pengelolaan organisasi Anda, Anda dapat mengedit kebijakan yang memerlukan perubahan di organisasi Anda.

Izin minimum

Untuk memperbarui kebijakan backup, Anda harus memiliki izin untuk menjalankan tindakan-tindakan berikut:

- `organizations:UpdatePolicy` dengan elemen `Resource` dalam pernyataan kebijakan yang sama yang mencakup ARN dari kebijakan yang akan diperbarui (atau "*")
- `organizations:DescribePolicy` dengan elemen `Resource` dalam pernyataan kebijakan yang sama yang mencakup ARN dari kebijakan yang akan diperbarui (atau "*")

AWS Management Console

Untuk memperbarui kebijakan backup

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Kebijakan Backup, pilih nama kebijakan yang ingin Anda perbarui.
3. Pilih Sunting kebijakan.
4. Anda dapat memasukkan Nama kebijakan, Deskripsi kebijakan baru. Anda dapat mengubah konten kebijakan dengan menggunakan Editor visual atau dengan secara langsung mengedit JSON.
5. Setelah selesai memperbarui kebijakan, pilih Simpan perubahan.

AWS CLI & AWS SDKs

Untuk memperbarui kebijakan backup

Anda dapat menggunakan salah satu yang berikut ini untuk memperbarui kebijakan backup:

- AWS CLI: update-policy

  Contoh berikut mengganti nama kebijakan backup.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
    }
```

```
}
```

Contoh berikut menambahkan atau mengubah deskripsi untuk kebijakan backup.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
       "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
    }
}
```

Contoh berikut mengubah dokumen kebijakan JSON yang dilampirkan ke kebijakan backup. Dalam contoh ini, konten diambil dari file bernama `policy.json` dengan teks berikut:

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { "@@assign": [ "ap-northeast-2", "us-east-1", "eu-
north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 5/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "complete_backup_window_minutes": { "@@assign": "10080" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "180" },
                        "delete_after_days": { "@@assign": "270" }
                    },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "copy_actions": {
```

```
                        "arn:aws:backup:us-east-1:$account:backup-vault:secondary-
vault": {
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "10" },
                                "delete_after_days": { "@@assign": "100" }
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "datatype": {
                            "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                            "tag_key": { "@@assign": "dataType" },
                            "tag_value": { "@@assign": [ "PII" ] }
                        }
                    }
                }
            }
    }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
backup_policy/p-i9j8k7l6m5",
            "Name": "Renamed policy",
            "Description": "My new description",
            "Type": "BACKUP_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"plans\":{\"TestBackupPlan\":{\"regions\":{\"@@assign\":
  ....TRUNCATED FOR BREVITY....   "@@assign\":[\"Yes\"]}}}}}}"
}
```

- AWSSDK: UpdatePolicy

Mengedit tag yang dilampirkan ke kebijakan backup

Saat masuk ke akun pengelolaan organisasi Anda, Anda dapat menambahkan atau menghapus tag yang dilampirkan ke kebijakan backup. Untuk informasi lebih lanjut tentang penandaan, lihat Penandaan pada sumber daya AWS Organizations.

Izin minimum

Untuk mengedit tag yang dilampirkan ke kebijakan backup di organisasi AWS Anda, Anda harus memiliki izin berikut:

- `organizations:DescribeOrganization` (konsol saja — untuk menavigasi ke kebijakan)
- `organizations:DescribePolicy` (konsol saja — untuk menavigasi ke kebijakan)
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

Untuk mengedit tag yang dilampirkan ke kebijakan backup

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Halaman Kebijakan Backup
3. Pilih nama kebijakan dengan tag yang ingin Anda edit.

   Halaman detail kebijakan akan muncul.
4. Di bagian tab Tanda, pilih Kelola tanda.
5. Anda dapat melakukan salah satu tindakan berikut di halaman ini:

   - Edit nilai untuk tag dengan memasukkan nilai baru menggantikan yang lama. Anda tidak dapat memodifikasi kunci. Untuk mengubah kunci, Anda harus menghapus tag dengan kunci yang lama dan menambahkan tag dengan kunci yang baru.

- Hapus tag yang ada dengan memilih Hapus.
- Tambahkan kunci tag dan pasangan nilai baru. Pilih Tambahkan tag, lalu masukkan nama kunci baru dan nilai opsional dalam kotak yang disediakan. Jika Anda membiarkan kotak Nilai kosong, nilai-nya adalah string kosong; itu bukan `null`.

6. Pilih Simpan perubahan setelah Anda melakukan semua penambahan, penghapusan, dan pengeditan yang ingin Anda buat.

AWS CLI & AWS SDKs

Untuk mengedit tag yang dilampirkan ke kebijakan backup

Anda dapat menggunakan salah satu perintah berikut untuk mengedit tag yang dilampirkan ke kebijakan backup:

- AWS CLI: tag-resource dan untag-resource
- AWS SDK: TagResourcedan UntagResource

Menghapus kebijakan backup

Saat masuk ke akun pengelolaan organisasi Anda, Anda dapat menghapus kebijakan yang tidak diperlukan lagi di organisasi Anda.

Sebelum Anda dapat menghapus kebijakan, Anda harus melepasnya terlebih dahulu dari semua entitas terlampir.

Izin minimum

Untuk menghapus kebijakan tag, Anda harus memiliki izin untuk menjalankan tindakan berikut:

- `organizations:DeletePolicy` dengan elemen `Resource` dalam pernyataan kebijakan yang sama yang mencakup ARN dari kebijakan yang akan dihapus (atau "*")

AWS Management Console

Untuk menghapus kebijakan backup

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Kebijakan Backup, pilih nama kebijakan yang ingin Anda hapus.
3. Anda harus terlebih dahulu melepaskan kebijakan backup yang ingin Anda hapus dari semua root, OU, dan akun. Pilih tab Target, pilih tombol radio yang ada di samping setiap root, OU, atau akun yang ditampilkan di daftar Target, dan kemudian pilih Lepaskan. Dalam kotak dialog konfirmasi, pilih Lepaskan. Ulangi sampai Anda menghapus semua target.
4. Pilih Hapus di bagian atas halaman.
5. Pada kotak dialog konfirmasi, masukkan nama kebijakan, dan kemudian pilih Hapus.

AWS CLI & AWS SDKs

Untuk menghapus kebijakan backup

Anda dapat menggunakan salah satu hal berikut untuk menghapus kebijakan:

- AWS CLI: hapus-kebijakan

  Contoh berikut menghapus kebijakan yang ditentukan. Ia berfungsi hanya jika kebijakan tidak dilampirkan pada root, OU, atau akun apa pun.

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  Perintah ini tidak menghasilkan output saat berhasil.

- AWSSDK: DeletePolicy

Melampirkan dan melepaskan kebijakan backup

Anda dapat menggunakan kebijakan backup di seluruh organisasi serta pada unit organisasi (OU) dan masing-masing akun. Ingatlah hal-hal berikut ini:

- Saat Anda melampirkan kebijakan backup ke root organisasi, kebijakan ini berlaku untuk semua anggota OU dan akun milik root.
- Ketika Anda melampirkan kebijakan backup ke OU, kebijakan tersebut berlaku untuk akun yang ada di OU atau salah satu anak OU. Akun tersebut juga tunduk pada kebijakan apa pun yang dilampirkan ke root organisasi.
- Ketika Anda melampirkan kebijakan backup ke akun, kebijakan tersebut hanya berlaku untuk akun tersebut. Akun ini juga tunduk pada kebijakan yang dilampirkan pada root organisasi dan OU apa pun yang dimiliki akun tersebut.

Agregasi kebijakan backup apa pun yang diwarisi akun dari root dan OU induk, serta kebijakan apa pun yang secara langsung dilampirkan pada akun, adalah kebijakan efektif. Untuk informasi selengkapnya tentang bagaimana kebijakan digabung ke kebijakan efektif, lihat Memahami warisan kebijakan manajemen.

Melampirkan kebijakan backup

Saat masuk ke akun pengelolaan organisasi, Anda dapat melampirkan kebijakan backup ke root organisasi, OU, atau langsung ke akun.

> Izin minimum
>
> Untuk melampirkan kebijakan backup, Anda harus memiliki izin untuk menjalankan tindakan-tindakan berikut:
>
> - `organizations:AttachPolicy`

AWS Management Console

Anda dapat melampirkan kebijakan backup dengan menavigasi ke kebijakan atau root, OU, atau akun yang ingin Anda lampirkan.

Untuk melampirkan kebijakan backup dengan menavigasi ke root, OU, atau akun

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Akun AWS, buka dan lalu pilih nama root, OU, atau akun yang ingin Anda lampirkan kebijakan padanya. Anda mungkin harus memperluas OU (pilih

untuk menemukan OU atau akun yang Anda inginkan.

3. Di tab Kebijakan, dalam entri untuk Kebijakan Backup, pilih Lampirkan.
4. Temukan kebijakan yang Anda inginkan dan pilih Lampirkan kebijakan.

   Daftar kebijakan backup terlampir pada tab Kebijakan diperbarui untuk menyertakan tambahan baru. Perubahan kebijakan langsung berlaku.

Untuk melampirkan kebijakan backup dengan menavigasi ke kebijakan

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Kebijakan Backup, pilih nama kebijakan yang ingin Anda lampirkan.
3. Di tab Target, pilih Lampirkan.
4. Pilih tombol radio yang ada di samping root, OU, atau akun yang ingin Anda lampirkan kebijakan padanya. Anda mungkin harus memperluas OU (pilih) untuk menemukan OU atau akun yang Anda inginkan.
5. Pilih Pasang kebijakan.

   Daftar kebijakan backup terlampir pada tab Target diperbarui untuk menyertakan tambahan baru. Perubahan kebijakan langsung berlaku.

AWS CLI & AWS SDKs

Untuk melampirkan kebijakan backup ke root organisasi, OU, atau akun

Anda dapat menggunakan salah satu perintah berikut untuk melampirkan kebijakan backup:

- AWS CLI: attach-policy

```
$ aws organizations attach-policy \
    --target-id 123456789012 \
    --policy-id p-i9j8k7l6m5
```

- AWSSDK: AttachPolicy

Perubahan kebijakan langsung berlaku.

Melepaskan kebijakan backup

Ketika Anda masuk ke akun pengelolaan organisasi Anda, Anda dapat melepaskan kebijakan backup dari root organisasi, OU, atau akun yang melampirkan kebijakan tersebut. Setelah Anda melepaskan kebijakan backup dari sebuah entitas, kebijakan tersebut tidak lagi berlaku untuk akun yang sebelumnya dipengaruhi oleh entitas yang sekarang terlepas. Untuk melepaskan kebijakan, lakukan langkah-langkah berikut.

Izin minimum

Untuk melepaskan kebijakan backup dari root organisasi, OU, atau akun, Anda harus memiliki izin untuk menjalankan tindakan berikut:

- `organizations:DetachPolicy`

AWS Management Console

Anda dapat melepaskan kebijakan backup dengan menavigasi ke kebijakan atau root, OU, atau akun yang Anda ingin lepaskan kebijakannya.

Untuk melepaskan kebijakan backup dengan menavigasi ke root, OU, atau akun yang melampirkannya

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Akun AWS navigasi ke akar, OU, atau akun yang ingin Anda lepaskan kebijakan darinya. Anda mungkin harus memperluas OU (pilih ▶) untuk menemukan OU atau akun yang Anda inginkan. Pilih nama Root, OU, atau akun.
3. Pada tab Kebijakan, pilih tombol radio yang ada di samping kebijakan backup yang ingin Anda lepaskan, dan kemudian pilih Lepaskan.
4. Dalam kotak dialog konfirmasi, pilih Lepaskan kebijakan.

   Daftar kebijakan backup terlampir sudah diperbarui. Perubahan kebijakan langsung berlaku.

Untuk melepaskan kebijakan backup dengan menavigasi ke kebijakan

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Kebijakan Backup, pilih nama kebijakan yang ingin Anda lepaskan dari root, OU, atau akun.
3. Pada tab Target, pilih tombol radio yang ada di sebelah root, OU, atau akun yang ingin Anda lepaskan kebijakan darinya. Anda mungkin harus memperluas OU (pilih ▶) untuk menemukan OU atau akun yang Anda inginkan.
4. Pilih Lepaskan.
5. Dalam kotak dialog konfirmasi, pilih Lepaskan.

   Daftar kebijakan backup terlampir sudah diperbarui. Perubahan kebijakan langsung berlaku.

AWS CLI & AWS SDKs

Untuk melepaskan kebijakan backup dari root organisasi, OU, atau akun

Anda dapat menggunakan salah satu perintah berikut untuk melepaskan kebijakan backup:

- AWS CLI: detach-policy

  Contoh berikut melepaskan kebijakan dari OU.

```
$ aws organizations detach-policy \
    --target-id ou-a1b2-f6g7h222 \
    --policy-id p-i9j8k7l6m5
```

  Perintah ini tidak menghasilkan keluaran saat berhasil.

- AWSSDK: DetachPolicy

Perubahan kebijakan langsung berlaku.

Melihat kebijakan backup yang efektif

Anda dapat melihat kebijakan backup efektif untuk akun dari Konsol Manajemen AWS, API AWS, atau Antarmuka Baris Perintah AWS. Bagian berikut memberikan gambaran singkat tentang kebijakan backup efektif, termasuk contohnya.

Apa itu kebijakan backup efektif?

Kebijakan backup yang efektif menentukan pengaturan paket backup akhir yang berlaku untuk Akun AWS. Ia adalah agregasi dari setiap kebijakan backup yang diwarisi akun, ditambah kebijakan backup yang secara langsung dilampirkan ke akun. Bila Anda melampirkan kebijakan backup ke root organisasi, kebijakan tersebut berlaku untuk semua akun di organisasi Anda. Ketika Anda melampirkan kebijakan backup untuk unit organisasi (OU), kebijakan itu berlaku untuk semua akun dan OU yang dimiliki OU tersebut. Bila Anda melampirkan kebijakan secara langsung ke akun, kebijakan tersebut hanya berlaku untuk satu Akun AWS tersebut.

Sebagai contoh, kebijakan backup yang dilampirkan ke root organisasi mungkin menentukan apakah semua akun dalam organisasi membuat backup dari semua tabel Amazon DynamoDB dengan frekuensi backup default sekali per minggu. Sebuah kebijakan backup terpisah yang dilampirkan langsung ke satu akun anggota dengan informasi penting dalam tabel dapat menimpa frekuensi dengan nilai sekali per hari. Kombinasi kebijakan backup ini terdiri dari kebijakan backup efektif. Kebijakan backup efektif ini ditentukan untuk setiap akun dalam organisasi secara individual. Dalam contoh ini, hasilnya adalah bahwa semua akun dalam organisasi membuat backup dari tabel DynamoDB mereka sekali per minggu, dengan pengecualian satu akun yang membuat backup tabel per hari.

Untuk informasi tentang bagaimana kebijakan backup digabungkan ke kebijakan backup efektif akhir, lihat Memahami warisan kebijakan manajemen.

Melihat kebijakan backup yang efektif

Anda dapat melihat kebijakan backup efektif untuk akun dengan menggunakan AWS Management Console, API AWS, atau AWS Command Line Interface.

> **Izin minimum**
>
> Untuk melihat kebijakan backup efektif untuk sebuah akun, Anda harus memiliki izin untuk menjalankan tindakan berikut:
>
> - `organizations:DescribeEffectivePolicy`

- `organizations:DescribeOrganization` — hanya diperlukan bila menggunakan konsol Organizations

AWS Management Console

Untuk melihat kebijakan backup efektif untuk sebuah akun

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Akun AWS, pilih nama akun yang ingin Anda lihat kebijakan backup efektif-nya. Anda mungkin harus memperluas OU (pilih ▶) untuk menemukan akun yang Anda inginkan.
3. Pada tab Kebijakan, di Kebijakan Backup, pilih Lihat kebijakan backup efektif untuk Akun AWS.

   Konsol menampilkan kebijakan efektif yang diterapkan pada akun yang ditentukan.

   > **Note**
   >
   > Anda tidak dapat menyalin dan menempelkan kebijakan efektif dan menggunakannya sebagai JSON untuk kebijakan backup lain tanpa ada perubahan signifikan. Dokumen kebijakan backup harus menyertakan Operator warisan yang menentukan bagaimana setiap pengaturan digabung ke kebijakan efektif akhir.

AWS CLI & AWS SDKs

Untuk melihat kebijakan backup efektif untuk sebuah akun

Anda dapat menggunakan salah satu perintah berikut untuk melihat kebijakan backup efektif:

- AWS CLI: describe-effective-policy

  Contoh berikut menampilkan detail sebuah kebijakan backup.

```
$ aws organizations describe-effective-policy \
```

```
--policy-type BACKUP_POLICY \
--target-id 123456789012{
    "EffectivePolicy": {
        "LastUpdatedTimestamp": "2020-06-22T14:31:50.748000-07:00",
        "TargetId": "123456789012",
        "PolicyType": "BACKUP_POLICY",
        "PolicyContent": "{\"plans\":{\"pii_backup_plan\":{\"regions\":[\"ap-
northeast-2\",\"us-east-1\",\"eu-north-1\"],\
"selections\":{\"tags\":{\"datatype\":{\"iam_role_arn\":\"arn:aws:iam::
$account:role/MyIamRole\",\"tag_value\":[\"PII\"],\
"tag_key\":\"dataType\"}}},\"rules\":{\"hourly\":{\"complete_backup_window_minutes
\":\"10080\",\"target_backup_vault_name\
":\"FortKnox\",\"start_backup_window_minutes\":\"480\",\"schedule_expression\":
\"cron(0 5/1 ? * * *)\",\"lifecycle\":{\"mo
ve_to_cold_storage_after_days\":\"180\",\"delete_after_days\":\"270\"},
\"copy_actions\":{\"arn:aws:backup:us-east-1:$accou
nt:backup-vault:secondary-vault\":{\"lifecycle\":
{\"move_to_cold_storage_after_days\":\"10\",\"delete_after_days\":\"100\"
}}}}}}}"
    }
}
```

- AWSSDK: DescribeEffectivePolicy

Menggunakan AWS CloudTrail acara untuk memantau kebijakan pencadangan di organisasi Anda

Anda dapat menggunakan AWS CloudTrail peristiwa untuk memantau kapan kebijakan cadangan dibuat, diperbarui, atau dihapus dari akun apa pun di AWS organisasi Anda, atau bila ada rencana pencadangan organisasi yang tidak valid. Untuk informasi selengkapnya, lihat Mencatat peristiwa pengelolaan lintas akun di Panduan AWS Backup Pengembang.

Sintaksis kebijakan Backup dan contoh

Halaman ini menjelaskan sintaksis kebijakan backup dan memberikan contohnya.

Sintaksis untuk kebijakan backup

Kebijakan backup adalah file plaintext yang terstruktur sesuai dengan aturan JSON. Sintaksis untuk kebijakan backup mengikuti sintaksis untuk semua jenis kebijakan pengelolaan. Untuk pembahasan lengkap tentang sintaksis itu, lihat Sintaksis kebijakan dan warisan untuk jenis kebijakan pengelolaan. Topik ini berfokus pada penerapan sintaksis umum untuk persyaratan khusus jenis kebijakan backup.

Sebagian besar kebijakan backup adalah paket backup dan aturannya. Sintaks untuk rencana cadangan dalam kebijakan AWS Organizations cadangan secara struktural identik dengan sintaks yang digunakan oleh AWS Backup, tetapi nama kuncinya berbeda. Dalam deskripsi nama kunci kebijakan di bawah ini, masing-masing menyertakan nama kunci AWS Backup paket yang setara. Untuk informasi selengkapnya tentang AWS Backup paket, lihat CreateBackupPlandi PanduanAWS Backup Pengembang.

> **Note**
>
> Saat menggunakan JSON, nama kunci duplikat akan ditolak. Jika Anda ingin menyertakan beberapa paket, aturan, atau pilihan dalam satu kebijakan, pastikan nama setiap kunci unik.

Agar lengkap dan fungsional, kebijakan backup yang efektif harus menyertakan lebih dari sekedar paket backup dengan jadwal dan peraturannya. Kebijakan juga harus mengidentifikasi Wilayah AWS dan sumber daya yang akan dicadangkan, dan peran AWS Identity and Access Management (IAM) yang AWS Backup dapat digunakan untuk melakukan pencadangan.

Kebijakan fungsional lengkap berikut menunjukkan sintaksis kebijakan backup basic. Jika contoh ini dilampirkan langsung ke akun, AWS Backup akan mencadangkan semua sumber daya untuk akun tersebut di `us-east-1` dan `eu-north-1` Wilayah yang memiliki tag `dataType` dengan nilai salah satu `PII` atau`RED`. Ia men-support sumber daya tersebut setiap hari pada 5:00 AM hingga `My_Backup_Vault` dan juga menyimpan salinan di `My_Secondary_Vault`. Kedua ruang penyimpanan tersebut berada di akun yang sama dengan sumber daya. Ia juga menyimpan salinan backup dalam `My_Tertiary_Vault` dalam akun yang berbeda, yang ditentukan secara eksplisit. Brankas harus sudah ada di masing-masing yang ditentukan Wilayah AWS untuk masing-masing Akun AWS yang menerima kebijakan yang efektif. Jika salah satu sumber daya yang di-backup adalah instans EC2, maka support untuk Microsoft Volume Shadow Copy Service (VSS) diaktifkan untuk melakukan backup pada instans tersebut. Backup menerapkan tag `Owner:Backup` ke setiap titik pemulihan.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "rules": {
                "My_Hourly_Rule": {
                    "schedule_expression": {"@@assign": "cron(0 5 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "60"},
                    "complete_backup_window_minutes": {"@@assign": "604800"},
```

```
                    "enable_continuous_backup": {"@@assign": false},
                    "target_backup_vault_name": {"@@assign": "My_Backup_Vault"},
                    "recovery_point_tags": {
                        "Owner": {
                            "tag_key": {"@@assign": "Owner"},
                            "tag_value": {"@@assign": "Backup"}
                        }
                    },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {"@@assign": "180"},
                        "delete_after_days": {"@@assign": "270"}
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-west-2:$account:backup-
vault:My_Secondary_Vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-west-2:$account:backup-
vault:My_Secondary_Vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "180"},
                                "delete_after_days": {"@@assign": "270"}
                            }
                        },
                        "arn:aws:backup:us-east-1:$account:backup-
vault:My_Tertiary_Vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
east-1:111111111111:backup-vault:My_Tertiary_Vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "180"},
                                "delete_after_days": {"@@assign": "270"}
                            }
                        }
                    }
                }
            },
            "regions": {
                "@@append": [
                    "us-east-1",
                    "eu-north-1"
                ]
            },
```

```
            "selections": {
                "tags": {
                    "My_Backup_Assignment": {
                        "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/
MyIamRole"},
                        "tag_key": {"@@assign": "dataType"},
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {
                    "windows_vss": {"@@assign": "enabled"}
                }
            },
            "backup_plan_tags": {
                "stage": {
                    "tag_key": {"@@assign": "Stage"},
                    "tag_value": {"@@assign": "Beta"}
                }
            }
        }
    }
}
```

Sintaksis kebijakan Backup mencakup komponen-komponen berikut:

- Variabel `$account` - Dalam string teks tertentu dalam kebijakan, Anda dapat menggunakan variabel `$account` untuk mewakili Akun AWSsaat ini. Ketika AWS Backup menjalankan rencana dalam kebijakan yang efektif, secara otomatis mengganti variabel ini dengan saat ini Akun AWS di mana kebijakan efektif dan rencananya berjalan.

  > **Important**
  >
  > Anda dapat menggunakan variabel `$account` hanya dalam elemen kebijakan yang dapat mencakup Amazon Resource Name (ARN), seperti variabel yang menentukan ruang

penyimpanan backup untuk menyimpan backup dalam, atau IAM role dengan izin untuk melakukan backup.

Misalnya, berikut ini mensyaratkan bahwa vault bernama `My_Vault` ada di setiap kebijakan Akun AWS yang berlaku.

```
arn:aws:backup:us-west-2:$account:vault:My_Vault"
```

Kami menyarankan Anda menggunakan kumpulan AWS CloudFormation tumpukan dan integrasinya dengan Organizations untuk secara otomatis membuat dan mengonfigurasi vault cadangan dan peran IAM untuk setiap akun anggota di organisasi. Untuk informasi lebih lanjut, lihat Membuat set tumpukan dengan izin dikelola sendiri di Panduan PenggunaAWS CloudFormation .

- Operator warisan - Kebijakan Backup dapat menggunakan kedua operator warisan, operator pengaturan nilai dan operator kontrol anak.
- `plans`

  Pada tingkat atas, kunci kebijakan adalah kunci `plans`. Kebijakan backup harus selalu dimulai dengan nama kunci tetap ini di bagian atas file kebijakan. Anda dapat memiliki satu atau beberapa paket backup berdasarkan kunci ini.
- Setiap paket berdasarkan kunci tingkat atas `plans` memiliki nama kunci yang terdiri dari nama paket backup yang ditetapkan oleh pengguna. Dalam contoh sebelumnya, nama paket backup adalah `PII_Backup_Plan`. Anda dapat memiliki beberapa paket dalam kebijakan, masing-masing dengan `rules`, `regions`, `selections`, dan `tags`.

  Nama kunci rencana cadangan ini dalam kebijakan cadangan memetakan nilai `BackupPlanName` kunci dalam AWS Backup rencana.

  Setiap paket dapat berisi elemen-elemen berikut:

  - `rules` — Kunci ini berisi kumpulan aturan. Setiap aturan diterjemahkan ke tugas terjadwal, dengan waktu mulai dan jendela di mana untuk membuat backup sumber daya diidentifikasi oleh elemen `selections` dan `regions` dalam kebijakan backup efektif.
  - `regions`— Kunci ini berisi daftar array Wilayah AWS yang sumber dayanya dapat didukung oleh kebijakan ini.

- `selections` — Kunci ini berisi satu atau lebih kumpulan sumber daya (dalam `regions` tertentu) yang di-backup oleh `rules`.
- `advanced_backup_settings` — Kunci ini berisi pengaturan khusus untuk backup yang berjalan pada sumber daya tertentu.
- `backup_plan_tags` — Ini menentukan tag yang dilampirkan ke paket backup itu sendiri.

- `rules`

  Kunci kebijakan `rules` memetakan ke kunci `Rules` dalam paket AWS Backup . Anda dapat memiliki satu atau beberapa aturan berdasarkan kunci `rules`. Setiap aturan menjadi tugas terjadwal untuk melakukan backup sumber daya yang dipilih.

  Setiap aturan berisi kunci yang namanya adalah nama aturan. Pada contoh sebelumnya, nama aturannya adalah "My_Hourly_Rule". Nilai dari kunci aturan tersebut adalah kumpulan dari elemen aturan berikut:

  - `schedule_expression`— Kunci kebijakan ini memetakan `ScheduleExpression` kunci ke kunci dalam suatu AWS Backup rencana.

    Menentukan waktu mulai backup. Kunci ini berisi operator nilai `@@assign` warisan dan nilai string dengan ekspresi CRON yang menentukan kapan AWS Backup akan memulai pekerjaan cadangan. Format umum dari string CRON adalah: "cron ()". Masing-masing adalah nomor atau wildcard. Misalnya, `cron(0 5 ? * 1,3,5 *)` memulai backup pada pukul 5 pagi setiap hari Senin, Rabu, dan Jumat. `cron(0 0/1 ? * * *)` memulai backup setiap jam pada jamnya, setiap hari dalam seminggu.

  - `target_backup_vault_name`— Kunci kebijakan ini memetakan `TargetBackupVaultName` kunci ke kunci dalam suatu AWS Backup rencana.

    Menentukan nama ruang penyimpanan backup di mana backup akan disimpan. Anda membuat nilai dengan menggunakan AWS Backup. Kunci ini berisi operator nilai warisan `@@assign` dan nilai string dengan nama ruang penyimpanan.

    > **Important**
    >
    > Vault harus sudah ada saat paket backup diluncurkan untuk pertama kalinya. Kami menyarankan Anda menggunakan kumpulan AWS CloudFormation tumpukan dan integrasinya dengan Organizations untuk secara otomatis membuat dan mengonfigurasi vault cadangan dan peran IAM untuk setiap akun anggota di organisasi. Untuk informasi

lebih lanjut, lihat Membuat set tumpukan dengan izin dikelola sendiri di Panduan PenggunaAWS CloudFormation .

- `start_backup_window_minutes`— Kunci kebijakan ini memetakan `StartWindowMinutes` kunci ke kunci dalam suatu AWS Backup rencana.

  (Opsional) Menentukan jumlah menit untuk menunggu sebelum membatalkan tugas yang tidak berhasil memulai. Kunci ini berisi operator nilai warisan `@@assign` dan nilai dengan jumlah integer menit.

- `complete_backup_window_minutes` — Kunci kebijakan ini memetakan ke kunci `CompletionWindowMinutes` dalam paket AWS Backup .

  (Opsional) Menentukan jumlah menit setelah tugas backup berhasil dimulai sebelum ia harus selesai atau dibatalkan oleh AWS Backup. Kunci ini berisi operator nilai warisan `@@assign` dan nilai dengan jumlah integer menit.

- `enable_continuous_backup`— Kunci kebijakan ini memetakan `EnableContinuousBackup` kunci ke kunci dalam suatu AWS Backup rencana.

  (Opsional) Menentukan apakah AWS Backup membuat backup terus menerus. `True`menyebabkan AWS Backup membuat cadangan berkelanjutan yang mampu point-in-time memulihkan (PITR). `False`(atau tidak ditentukan) menyebabkan AWS Backup membuat cadangan snapshot.

  > **Note**
  >
  > Karena backup diaktifkan-PITR dapat dipertahankan selama maksimum 35 hari, Anda harus memilih `False` atau tidak menentukan nilai jika Anda mengatur dengan salah satu opsi berikut:
  >
  > - Atur `delete_after_days` hingga lebih besar dari 35.
  > - Atur `move_to_cold_storage_after_days` ke nilai apapun.

  Untuk informasi selengkapnya tentang pencadangan berkelanjutan, lihat oint-in-time pemulihan P di PanduanAWS Backup Pengembang.

- `lifecycle`— Kunci kebijakan ini memetakan `Lifecycle` kunci ke kunci dalam suatu AWS Backup rencana.

(Opsional) Menentukan kapan AWS Backup transisi cadangan ini ke cold storage dan kapan kedaluwarsa.

- `move_to_cold_storage_after_days` — Kunci kebijakan ini memetakan `MoveToColdStorageAfterDays` kunci ke kunci dalam suatu AWS Backup rencana.

  Menentukan jumlah hari setelah backup terjadi sebelum AWS Backup memindahkan titik pemulihan ke penyimpanan dingin. Kunci ini berisi operator nilai warisan `@@assign` dan nilai dengan angka integer hari.

- `delete_after_days`— Kunci kebijakan ini memetakan `DeleteAfterDays` kunci ke kunci dalam suatu AWS Backup rencana.

  Menentukan jumlah hari setelah backup terjadi sebelum AWS Backup menghapus titik pemulihan. Kunci ini berisi operator nilai warisan `@@assign` dan nilai dengan angka integer hari. Jika Anda mengalihkan backup ke penyimpanan dingin, maka ia harus berada di sana minimal 90 hari, sehingga nilai ini harus minimal 90 hari lebih besar dari nilai `move_to_cold_storage_after_days`.

- `copy_actions`— Kunci kebijakan ini memetakan `CopyActions` kunci ke kunci dalam suatu AWS Backup rencana.

  (Opsional) Menentukan yang AWS Backup harus menyalin cadangan ke satu atau lebih lokasi tambahan. Setiap lokasi salinan backup dijelaskan sebagai berikut:

  - Kunci yang namanya mengidentifikasi tindakan penyalinan ini secara unik. Pada saat ini, nama kunci harus Amazon Resource Name (ARN) dari ruang penyimpanan backup. Kunci ini berisi dua entri.

    - `target_backup_vault_arn` — Kunci kebijakan ini memetakan ke kunci `DestinationBackupVaultArn` dalam paket AWS Backup .

      (Opsional) Menentukan brankas tempat AWS Backup menyimpan salinan cadangan tambahan. Nilai kunci ini berisi operator nilai warisan `@@assign` dan ARN ruang penyimpanan.

      - Untuk mereferensikan vault tempat kebijakan pencadangan berjalan, gunakan `$account` variabel di ARN sebagai pengganti nomor ID akun. Akun AWS Saat AWS Backup menjalankan paket cadangan, secara otomatis akan mengganti variabel dengan nomor ID akun Akun AWS tempat kebijakan dijalankan. Hal ini memungkinkan backup untuk berjalan dengan benar ketika kebijakan backup berlaku untuk lebih dari satu akun dalam organisasi.

- Untuk me-referensi ruang penyimpanan dalam Akun AWS yang berbeda di organisasi yang sama, gunakan nomor ID akun aktual di ARN.

> **Important**
>
> - Jika kunci ini hilang, maka semua versi huruf kecil ARN dalam nama kunci induk akan digunakan. Karena ARN adalah sensitif huruf besar kecil, maka string ini mungkin tidak cocok dengan ARN sebenarnya dari kesalahan dan paket akan gagal. Untuk alasan ini, kami sarankan Anda selalu menyediakan kunci dan nilai ini.
> - Ruang penyimpanan backup yang ingin Anda salin backup-nya harus sudah ada saat pertama kali Anda meluncurkan paket backup. Kami menyarankan agar Anda menggunakan set tumpukan AWS CloudFormation dan integrasinya dengan Organizations untuk secara otomatis membuat dan mengonfigurasi ruang penyimpanan backup dan IAM role untuk setiap akun anggota dalam organisasi. Untuk informasi lebih lanjut, lihat Membuat set tumpukan dengan izin dikelola sendiri di Panduan PenggunaAWS CloudFormation .

- `lifecycle`— Kunci kebijakan ini memetakan `Lifecycle` kunci di bawah `CopyAction` kunci dalam AWS Backup rencana.

  (Opsional) Menentukan kapan AWS Backup transisi salinan cadangan ini ke cold storage dan kapan kedaluwarsa.

  - `move_to_cold_storage_after_days` — Kunci kebijakan ini memetakan ke kunci `MoveToColdStorageAfterDays` dalam paket AWS Backup .

    Menentukan jumlah hari setelah backup terjadi sebelum AWS Backup memindahkan titik pemulihan ke cold storage. Kunci ini berisi operator nilai warisan `@@assign` dan nilai dengan angka integer hari.

  - `delete_after_days` — Kunci kebijakan ini memetakan ke kunci `DeleteAfterDays` dalam paket AWS Backup .

    Menentukan jumlah hari setelah backup terjadi sebelum AWS Backup menghapus titik pemulihan. Kunci ini berisi operator nilai warisan `@@assign` dan nilai dengan angka integer hari. Jika Anda mengalihkan backup ke penyimpanan dingin, maka ia harus berada di sana minimal 90 hari, sehingga nilai ini harus minimal 90 hari lebih besar dari nilai `move_to_cold_storage_after_days`.

- `recovery_point_tags`— Kunci kebijakan ini memetakan `RecoveryPointTags` kunci ke kunci dalam suatu AWS Backup rencana.

  (Opsional) Menentukan tag yang AWS Backup melekat pada setiap cadangan yang dibuat dari rencana ini. Nilai kunci ini berisi satu elemen berikut atau lebih:

  - Sebuah pengidentifikasi untuk pasangan nama dan nilai kunci ini. Nama ini untuk setiap elemen di `recovery_point_tags` adalah nama kunci tag dalam semua huruf kecil, bahkan jika `tag_key` memiliki perlakuan kasus yang berbeda. Pengidentifikasi ini tidak peka huruf besar kecil. Pada contoh sebelumnya, pasangan kunci ini diidentifikasi dengan nama `0wner`. Setiap pasangan kunci berisi elemen berikut:

    - `tag_key` — Menentukan nama kunci tag untuk dilampirkan ke paket backup. Kunci ini berisi operator nilai warisan `@@assign` dan nilai string. Nilai ini memedulikan huruf besar atau huruf kecil.

    - `tag_value` — Menentukan nilai yang melekat pada paket backup dan terkait dengan `tag_key`. Kunci ini berisi salah satu operator nilai warisan, dan satu nilai atau lebih untuk mengganti, menambahkan, atau menghapus dari kebijakan efektif. Nilai ini peka huruf besar kecil.

- `regions`

  Kunci `regions` kebijakan menentukan mana Wilayah AWS yang AWS Backup melihat ke dalam untuk menemukan sumber daya yang cocok dengan kondisi dalam `selections` kunci. Kunci ini berisi salah satu operator nilai warisan dan satu atau lebih nilai string untuk Wilayah AWS kode, misalnya:`["us-east-1", "eu-north-1"]`.

- `selections`

  Kunci kebijakan `selections` menentukan sumber daya yang di-backup oleh aturan paket dalam kebijakan ini. Kunci ini kira-kira sesuai dengan BackupSelectionobjek di AWS Backup. Sumber daya yang ditentukan oleh kueri untuk pencocokan nama dan nilai kunci tag. Kunci `selections` berisi satu kunci di bawahnya — `tags`.

  - `tags` — Menentukan tag yang mengidentifikasi sumber daya, dan IAM role yang memiliki izin untuk meng-kueri sumber daya dan mem-backup-nya. Nilai kunci ini berisi satu elemen berikut atau lebih:

    - Sebuah pengidentifikasi untuk elemen tag ini. Pengidentifikasi ini di bawah `tags` adalah nama kunci tag dalam semua huruf kecil, bahkan jika tag untuk kueri memiliki perlakuan kasus yang berbeda. Pengidentifikasi ini tidak peka huruf besar kecil. Pada contoh sebelumnya, satu

elemen diidentifikasi dengan nama `My_Backup_Assignment`. Setiap pengidentifikasi di bawah `tags` berisi elemen-elemen berikut:

- `iam_role_arn` — Menentukan IAM role yang memiliki izin untuk mengakses sumber daya yang diidentifikasi oleh kueri tag di Wilayah AWS yang ditentukan oleh kunci `regions`. Nilai ini berisi operator nilai `@@assign` warisan dan nilai string yang berisi ARN peran. AWS Backup menggunakan peran ini untuk menanyakan dan menemukan sumber daya dan untuk melakukan pencadangan.

  Anda dapat menggunakan variabel `$account` di ARN di tempat nomor ID akun. Ketika paket cadangan dijalankan AWS Backup, secara otomatis akan mengganti variabel dengan nomor ID akun aktual Akun AWS tempat kebijakan dijalankan.

  > **Important**
  >
  > Peran tersebut harus sudah ada ketika Anda meluncurkan paket backup pertama kali. Kami menyarankan Anda menggunakan kumpulan AWS CloudFormation tumpukan dan integrasinya dengan Organizations untuk secara otomatis membuat dan mengonfigurasi vault cadangan dan peran IAM untuk setiap akun anggota di organisasi. Untuk informasi lebih lanjut, lihat Membuat set tumpukan dengan izin dikelola sendiri di Panduan PenggunaAWS CloudFormation .

- `tag_key` — Menentukan nama kunci tag yang akan dicari. Kunci ini berisi operator nilai warisan `@@assign` dan nilai string. Nilai ini memedulikan huruf besar atau huruf kecil.
- `tag_value`— Menentukan nilai yang harus dikaitkan dengan nama kunci yang cocok`tag_key`. AWS Backup termasuk sumber daya dalam cadangan hanya jika keduanya `tag_key` dan `tag_value` cocok. Kunci ini berisi salah satu operator nilai warisan, dan satu nilai atau lebih untuk mengganti, menambahkan, atau menghapus dari kebijakan efektif. Nilai ini peka huruf besar kecil.

- `advanced_backup_settings` — Menentukan pengaturan untuk skenario backup tertentu. Kunci ini berisi satu atau beberapa pengaturan. Setiap pengaturan adalah string objek JSON dengan elemen-elemen berikut:
  - Nama kunci objek - Sebuah string yang menentukan jenis sumber daya yang padanya pengaturan lanjutan berikut berlaku.
  - Nilai objek — Sebuah string objek JSON yang berisi satu atau beberapa pengaturan backup spesifik untuk jenis sumber daya yang terkait.

Pada saat ini, satu-satunya pengaturan backup lanjutan yang didukung memungkinkan backup Microsoft Volume Shadow Copy Service (VSS) untuk Windows atau SQL Server yang berjalan pada instans Amazon EC2. Nama kunci harus jenis sumber daya `"ec2"`, dan nilai-nya menentukan bahwa support `"windows_vss"` adalah `enabled` atau `disabled` untuk backup yang dilakukan pada instans Amazon EC2. Untuk informasi lebih lanjut tentang fitur ini, lihat Membuat Backup Windows yang Diaktifkan VSS di Panduan DeveloperAWS Backup .

```
"advanced_backup_settings": {
    "ec2": {
        "windows_vss": {
            "@@assign": "enabled"
        }
    }
}
```

- `backup_plan_tags` — Menentukan tag yang dilampirkan ke paket backup itu sendiri. Ini tidak memengaruhi tag yang ditentukan dalam aturan atau pilihan apa pun.

  (Opsional) Anda dapat melampirkan tag ke paket backup Anda. Nilai kunci ini adalah kumpulan elemen.

  Nama kunci untuk setiap elemen di `backup_plan_tags` adalah nama kunci tag dengan huruf kecil semua, bahkan jika tag untuk kueri memiliki perlakuan kasus yang berbeda. Pengidentifikasi ini tidak peka huruf besar kecil. Nilai untuk masing-masing entri ini terdiri dari kunci berikut:

  - `tag_key` — Menentukan nama kunci tag untuk dilampirkan ke paket backup. Kunci ini berisi operator nilai warisan `@@assign` dan nilai string. Nilai ini peka huruf besar kecil.
  - `tag_value` — Menentukan nilai yang melekat pada paket backup dan terkait dengan `tag_key`. Kunci ini berisi operator nilai warisan `@@assign` dan nilai string. Nilai ini peka huruf besar kecil.

Contoh kebijakan Backup

Contoh kebijakan backup berikut adalah untuk tujuan informasi saja. Dalam beberapa contoh berikut, format spasi kosong JSON mungkin dikompresi untuk menghemat ruang.

Contoh 1: Kebijakan yang ditetapkan ke simpul induk

Contoh berikut menunjukkan kebijakan backup yang ditetapkan ke salah satu simpul induk akun.

Kebijakan Induk — Kebijakan ini dapat dilampirkan ke root organisasi, atau ke OU yang merupakan induk dari semua akun yang dimaksud.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@assign": [
                    "ap-northeast-2",
                    "us-east-1",
                    "eu-north-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {
                        "@@assign": "cron(0 5/1 ? * * *)"
                    },
                    "start_backup_window_minutes": {
                        "@@assign": "480"
                    },
                    "complete_backup_window_minutes": {
                        "@@assign": "10080"
                    },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": {
                            "@@assign": "180"
                        },
                        "delete_after_days": {
                            "@@assign": "270"
                        }
                    },
                    "target_backup_vault_name": {
                        "@@assign": "FortKnox"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:$account:backup-
vault:secondary_vault"
                            },
                            "lifecycle": {
```

```
                                "move_to_cold_storage_after_days": {
                                    "@@assign": "30"
                                },
                                "delete_after_days": {
                                    "@@assign": "120"
                                }
                            }
                        },
                        "arn:aws:backup:us-west-1:111111111111:backup-
vault:tertiary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
west-1:111111111111:backup-vault:tertiary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {
                                    "@@assign": "30"
                                },
                                "delete_after_days": {
                                    "@@assign": "120"
                                }
                            }
                        }                   }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": {
                            "@@assign": "arn:aws:iam::$account:role/MyIamRole"
                        },
                        "tag_key": {
                            "@@assign": "dataType"
                        },
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            },
            "advanced_backup_settings": {
```

```
                "ec2": {
                    "windows_vss": {
                        "@@assign": "enabled"
                    }
                }
            }
        }
    }
}
```

Jika tidak ada kebijakan lain yang diwarisi atau dilampirkan ke akun, kebijakan efektif yang diberikan di setiap yang berlaku Akun AWS terlihat seperti contoh berikut. Ekspresi CRON menyebabkan backup berjalan sekali dalam satu jam pada jamnya. ID akun 123456789012 akan menjadi ID akun aktual untuk setiap akun.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-east-1",
                "ap-northeast-3",
                "eu-north-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "to_delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
                            "lifecycle": {
                                "to_delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180"
                            }
                        },
```

```
                        "arn:aws:backup:us-west-1:111111111111:vault:tertiary_vault": {
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-
west-1:111111111111:vault:tertiary_vault"
                            },
                            "lifecycle": {
                                "to_delete_after_days": "28",
                                "move_to_cold_storage_after_days": "180"
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "datatype": {
                            "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
                            "tag_key": "dataType",
                            "tag_value": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                },
                "advanced_backup_settings": {
                    "ec2": {
                        "windows_vss": "enabled"
                    }
                }
            }
        }
}
```

Contoh 2: Sebuah kebijakan induk digabung dengan sebuah kebijakan anak

Dalam contoh berikut, kebijakan induk yang diwariskan dan kebijakan anak diwariskan atau langsung dilampirkan pada Akun AWS penggabungan untuk membentuk kebijakan yang efektif.

Kebijakan Induk — Kebijakan ini dapat dilampirkan ke root organisasi atau ke OU induk.

```
{
    "plans": {
       "PII_Backup_Plan": {
```

```
            "regions": { "@@append":[ "us-east-1", "ap-northeast-3", "eu-north-1" ] },
            "rules": {
                "Hourly": {
                    "schedule_expression": { "@@assign": "cron(0 0/1 ? * * *)" },
                    "start_backup_window_minutes": { "@@assign": "60" },
                    "target_backup_vault_name": { "@@assign": "FortKnox" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "28" },
                        "to_delete_after_days": { "@@assign": "180" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "28" },
                                "to_delete_after_days": { "@@assign": "180" }
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "datatype": {
                            "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyIamRole" },
                            "tag_key": { "@@assign": "dataType" },
                            "tag_value": { "@@assign": [ "PII", "RED" ] }
                        }
                    }
                }
            }
        }
}
```

Kebijakan anak — Kebijakan ini dapat dilampirkan langsung ke akun atau ke OU di tingkat di bawahnya di mana kebijakan induk dilampirkan.

```
{
```

```
    "plans": {
       "Monthly_Backup_Plan": {
            "regions": {
                "@@append":[ "us-east-1", "eu-central-1" ] },
            "rules": {
                "Monthly": {
                    "schedule_expression": { "@@assign": "cron(0 5 1 * ? *)" },
                    "start_backup_window_minutes": { "@@assign": "480" },
                    "target_backup_vault_name": { "@@assign": "Default" },
                    "lifecycle": {
                        "move_to_cold_storage_after_days": { "@@assign": "30" },
                        "to_delete_after_days": { "@@assign": "365" }
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:Default" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": { "@@assign":
 "30" },
                                "to_delete_after_days": { "@@assign": "365" }
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "MonthlyDatatype": {
                        "iam_role_arn": { "@@assign": "arn:aws:iam::$account:role/
MyMonthlyBackupIamRole" },
                        "tag_key": { "@@assign": "BackupType" },
                        "tag_value": { "@@assign": [ "MONTHLY", "RED" ] }
                    }
                }
            }
        }
    }
}
```

Menghasilkan kebijakan efektif — Kebijakan efektif yang diterapkan pada akun yang berisi dua paket, masing-masing dengan seperangkat aturan dan seperangkat sumber daya sendiri untuk menerapkan aturan.

```
{
    "plans": {
       "PII_Backup_Plan": {
            "regions": [ "us-east-1", "ap-northeast-3", "eu-north-1" ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "to_delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault" : {
                            "target_backup_vault_arn" : {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:secondary_vault"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "28",
                                "to_delete_after_days": "180"
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "datatype": {
                            "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                            "tag_key": "dataType",
                            "tag_value": [ "PII", "RED" ]
                        }
                    }
                }
            },
            "Monthly_Backup_Plan": {
                "regions": [ "us-east-1", "eu-central-1" ],
```

```
            "rules": {
                "monthly": {
                    "schedule_expression": "cron(0 5 1 * ? *)",
                    "start_backup_window_minutes": "480",
                    "target_backup_vault_name": "Default",
                    "lifecycle": {
                        "to_delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:Default" : {
                            "target_backup_vault_arn": {
                                "@@assign" : "arn:aws:backup:us-east-1:
$account:vault:Default"
                            },
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "30",
                                "to_delete_after_days": "365"
                            }
                        }
                    }
                },
                "selections": {
                    "tags": {
                        "monthlydatatype": {
                            "iam_role_arn": "arn:aws:iam::&ExampleAWSAccountNo3;:role/
MyMonthlyBackupIamRole",
                            "tag_key": "BackupType",
                            "tag_value": [ "MONTHLY", "RED" ]
                        }
                    }
                }
            }
        }
}
```

Contoh 3: Kebijakan induk mencegah perubahan oleh kebijakan anak

Pada contoh berikut, kebijakan induk yang diwariskan menggunakan operator kontrol anak untuk menegakkan semua pengaturan dan mencegahnya diubah atau ditimpa oleh kebijakan anak.

Kebijakan Induk — Kebijakan ini dapat dilampirkan ke root organisasi atau ke OU induk. Kehadiran `"@@operators_allowed_for_child_policies": ["@@none"]` di setiap simpul kebijakan berarti bahwa kebijakan anak tidak dapat membuat perubahan dalam bentuk apapun pada paket. Kebijakan anak juga tidak dapat menambahkan paket tambahan untuk kebijakan efektif. Kebijakan ini menjadi kebijakan efektif untuk setiap OU dan akun di bawah OU yang padanya kebijakan tersebut dilampirkan.

```
{
    "plans": {
        "@@operators_allowed_for_child_policies": ["@@none"],
        "PII_Backup_Plan": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "regions": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "@@append": [
                    "us-east-1",
                    "ap-northeast-3",
                    "eu-north-1"
                ]
            },
            "rules": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "Hourly": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "schedule_expression": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "cron(0 0/1 ? * * *)"
                    },
                    "start_backup_window_minutes": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "60"
                    },
                    "target_backup_vault_name": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "@@assign": "FortKnox"
                    },
                    "lifecycle": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "move_to_cold_storage_after_days": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "28"
                        },
                        "to_delete_after_days": {
```

```
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "180"
                        }
                    },
                    "copy_actions": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "target_backup_vault_arn": {
                                "@@assign": "arn:aws:backup:us-east-1:
$account:vault:secondary_vault",
                                "@@operators_allowed_for_child_policies": ["@@none"]
                            },
                            "lifecycle": {
                                "@@operators_allowed_for_child_policies": ["@@none"],
                                "to_delete_after_days": {
                                    "@@operators_allowed_for_child_policies":
 ["@@none"],
                                    "@@assign": "28"
                                },
                                "move_to_cold_storage_after_days": {
                                    "@@operators_allowed_for_child_policies":
 ["@@none"],
                                    "@@assign": "180"
                                }
                            }
                        }
                    }
                }
            },
            "selections": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "tags": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "datatype": {
                        "@@operators_allowed_for_child_policies": ["@@none"],
                        "iam_role_arn": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "arn:aws:iam::$account:role/MyIamRole"
                        },
                        "tag_key": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": "dataType"
                        },
```

```
                        "tag_value": {
                            "@@operators_allowed_for_child_policies": ["@@none"],
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            },
            "advanced_backup_settings": {
                "@@operators_allowed_for_child_policies": ["@@none"],
                "ec2": {
                    "@@operators_allowed_for_child_policies": ["@@none"],
                    "windows_vss": {
                        "@@assign": "enabled",
                        "@@operators_allowed_for_child_policies": ["@@none"]
                    }
                }
            }
        }
    }
}
```

Menghasilkan kebijakan efektif — Jika ada kebijakan backup anak apapun, mereka akan diabaikan dan kebijakan induk menjadi kebijakan efektif.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-east-1",
                "ap-northeast-3",
                "eu-north-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/1 ? * * *)",
                    "start_backup_window_minutes": "60",
                    "target_backup_vault_name": "FortKnox",
                    "lifecycle": {
                        "to_delete_after_days": "2",
                        "move_to_cold_storage_after_days": "180"
```

```
                    },
                    "copy_actions": {
                        "target_backup_vault_arn": "arn:aws:backup:us-
east-1:123456789012:vault:secondary_vault",
                        "lifecycle": {
                            "move_to_cold_storage_after_days": "28",
                            "to_delete_after_days": "180"
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::123456789012:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            },
            "advanced_backup_settings": {
                "ec2": {"windows_vss": "enabled"}
            }
        }
    }
}
```

Contoh 4: Kebijakan induk mencegah perubahan ke sebuah paket backup oleh kebijakan anak

Pada contoh berikut, kebijakan induk yang diwariskan menggunakan operator kontrol anak untuk menegakkan pengaturan untuk paket tunggal dan mencegahnya diubah atau ditimpa oleh kebijakan anak. Kebijakan anak masih dapat menambahkan paket tambahan.

Kebijakan Induk — Kebijakan ini dapat dilampirkan ke root organisasi atau ke OU induk. Contoh ini mirip dengan contoh sebelumnya dengan semua operator warisan anak diblokir, kecuali pada `plans` tingkat atas. Pengaturan `@@append` pada tingkat yang memungkinkan kebijakan anak untuk menambahkan paket lain untuk kumpulan dalam kebijakan efektif. Setiap perubahan pada paket yang diwariskan masih diblokir.

Bagian dalam paket dipotong untuk kejelasan.

```
{
    "plans": {
        "@@operators_allowed_for_child_policies": ["@@append"],
        "PII_Backup_Plan": {
            "@@operators_allowed_for_child_policies": ["@@none"],
            "regions": { ... },
            "rules": { ... },
            "selections": { ... }
        }
    }
}
```

Kebijakan anak — Kebijakan ini dapat dilampirkan langsung ke akun atau ke OU di tingkat di bawahnya di mana kebijakan induk dilampirkan. Kebijakan anak ini menentukan paket baru.

Bagian dalam paket dipotong untuk kejelasan.

```
{
    "plans": {
        "MonthlyBackupPlan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { … }
        }
    }
}
```

Menghasilkan kebijakan efektif — Kebijakan efektif menyertakan kedua paket tersebut.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { ... }
        },
        "MonthlyBackupPlan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { … }
        }
    }
```

```
}
```

Contoh 5: Kebijakan anak menimpa pengaturan di kebijakan induk

Pada contoh berikut, kebijakan anak menggunakan operator pengaturan nilai untuk menimpa beberapa pengaturan yang diwarisi dari kebijakan induk.

Kebijakan Induk — Kebijakan ini dapat dilampirkan ke root organisasi atau ke OU induk. Setiap pengaturan dapat ditimpa oleh kebijakan anak karena perilaku default, dengan tidak adanya operator kontrol anak yang mencegah hal itu, maka itu akan memungkinkan kebijakan anak untuk `@@assign`, `@@append`, atau `@@remove`. Kebijakan induk berisi semua elemen yang diperlukan untuk paket backup yang valid, sehingga ia berhasil mencadangkan sumber daya Anda jika diwariskan sebagaimana adanya.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@append": [
                    "us-east-1",
                    "ap-northeast-3",
                    "eu-north-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {"@@assign": "cron(0 0/1 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "60"},
                    "target_backup_vault_name": {"@@assign": "FortKnox"},
                    "lifecycle": {
                        "to_delete_after_days": {"@@assign": "2"},
                        "move_to_cold_storage_after_days": {"@@assign": "180"}
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:t2": {
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:vault:t2"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": {"@@assign": "28"},
                                "to_delete_after_days": {"@@assign": "180"}
                            }
                        }
```

```
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": {"@@assign": "arn:aws:iam::$account:role/
MyIamRole"},
                        "tag_key": {"@@assign": "dataType"},
                        "tag_value": {
                            "@@assign": [
                                "PII",
                                "RED"
                            ]
                        }
                    }
                }
            }
        }
    }
}
```

Kebijakan anak — Kebijakan anak hanya mencakup pengaturan yang harus berbeda dari kebijakan induk yang diwariskan. Harus ada kebijakan induk yang diwariskan yang menyediakan pengaturan lain yang diperlukan ketika digabungkan ke kebijakan efektif. Jika tidak, kebijakan backup efektif berisi paket backup yang tidak valid dan tidak membuat mencadangkan sumber daya Anda seperti yang diharapkan.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": {
                "@@assign": [
                    "us-west-2",
                    "eu-central-1"
                ]
            },
            "rules": {
                "Hourly": {
                    "schedule_expression": {"@@assign": "cron(0 0/2 ? * * *)"},
                    "start_backup_window_minutes": {"@@assign": "80"},
                    "target_backup_vault_name": {"@@assign": "Default"},
                    "lifecycle": {
```

```
                        "move_to_cold_storage_after_days": {"@@assign": "30"},
                        "to_delete_after_days": {"@@assign": "365"}
                    }
                }
            }
        }
    }
}
```

Menghasilkan kebijakan efektif — Kebijakan efektif mencakup pengaturan dari kedua kebijakan, dengan pengaturan yang disediakan oleh kebijakan anak yang menimpa pengaturan yang diwarisi dari induk. Dalam contoh ini, perubahan berikut terjadi:

- Daftar Wilayah diganti dengan daftar yang sama sekali berbeda. Jika Anda ingin menambahkan Wilayah ke daftar warisan, gunakan `@@append`, bukan `@@assign` dalam kebijakan anak.
- AWS Backup melakukan setiap jam, bukan setiap jam.
- AWS Backup memungkinkan 80 menit untuk pencadangan dimulai, bukan 60 menit.
- AWS Backup menggunakan lemari `Default` besi alih-alih. `FortKnox`
- Siklus hidup diperpanjang baik untuk transfer backup ke penyimpanan dingin atau pun penghapusan di akhir.

```
{
    "plans": {
        "PII_Backup_Plan": {
            "regions": [
                "us-west-2",
                "eu-central-1"
            ],
            "rules": {
                "hourly": {
                    "schedule_expression": "cron(0 0/2 ? * * *)",
                    "start_backup_window_minutes": "80",
                    "target_backup_vault_name": "Default",
                    "lifecycle": {
                        "to_delete_after_days": "365",
                        "move_to_cold_storage_after_days": "30"
                    },
                    "copy_actions": {
                        "arn:aws:backup:us-east-1:$account:vault:secondary_vault": {
```

```
                            "target_backup_vault_arn": {"@@assign": "arn:aws:backup:us-
east-1:$account:vault:secondary_vault"},
                            "lifecycle": {
                                "move_to_cold_storage_after_days": "28",
                                "to_delete_after_days": "180"
                            }
                        }
                    }
                }
            },
            "selections": {
                "tags": {
                    "datatype": {
                        "iam_role_arn": "arn:aws:iam::$account:role/MyIamRole",
                        "tag_key": "dataType",
                        "tag_value": [
                            "PII",
                            "RED"
                        ]
                    }
                }
            }
        }
    }
}
```

Kebijakan tag

Anda dapat menggunakan kebijakan tanda untuk mempertahankan tanda yang konsisten, termasuk penanganan kasus pilihan atas kunci tag dan nilai tag.

Apa itu tag?

Tag adalah label atribut kustom yang Anda tetapkan atau yang AWS tetapkan ke sumber daya AWS. Setiap tanda memiliki dua bagian:

- Sebuah kunci tag (misalnya, `CostCenter`, `Environment`, atau `Project`). Kunci tag peka huruf besar dan kecil.
- Bidang opsional yang dikenal sebagai nilai tag (misalnya, `111122223333` atau `Production`). Mengabaikan nilai tag sama dengan menggunakan sebuah string kosong. Seperti kunci tag, nilai tag peka terhadap huruf besar dan kecil.

Sisa halaman ini menjelaskan kebijakan tag. Untuk informasi lebih lanjut tentang penandaan, lihat sumber-sumber berikut ini:

- Untuk informasi umum tentang penandaan, termasuk konvensi penamaan dan penggunaan, lihat Panduan Pengguna AWSSumber Daya Penandaan.
- Untuk daftar layanan yang men-support penggunaan tag, lihat Referensi API Penandaan Resource Groups.
- Untuk informasi tentang penggunaan tag untuk mengkategorikan sumber daya, lihat Whitepaper Praktik Terbaik untuk Menandai AWS Sumber Daya.
- Untuk informasi tentang penandaan sumber daya Organizations, lihat Penandaan pada sumber daya AWS Organizations.
- Untuk informasi tentang menandai sumber daya di AWS layanan lain, lihat dokumentasi untuk layanan tersebut.

Apa itu kebijakan tag?

Kebijakan tag adalah jenis kebijakan yang dapat membantu Anda menstandardisasi tag di seluruh sumber daya yang ada di akun organisasi Anda. Dalam kebijakan tag, Anda menetapkan aturan penandaan yang berlaku untuk sumber daya saat ditandai.

Sebagai contoh, kebijakan tag dapat menentukan ketika tag `CostCenter` harus terlampir pada sebuah sumber, ia harus menggunakan perlakuan kasus dan nilai tag yang ditentukan kebijakan tag tersebut. Kebijakan tag juga dapat menentukan apakah operasi penandaan yang tak sesuai pada jenis sumber daya tertentu ditegakkan. Dengan kata lain, permintaan penandaan yang tidak sesuai pada jenis sumber daya yang ditentukan dicegah untuk diselesaikan. Sumber daya atau tag yang tak ditandai yang tidak didefinisikan dalam kebijakan tag tidak akan dievaluasi demi kepatuhan terhadap kebijakan tag.

Menggunakan kebijakan tag melibatkan kerjasama dengan berbagai layanan AWS:

- Gunakan AWS Organizations untuk mengelola kebijakan tag. Ketika Anda masuk ke akun pengelolaan organisasi, Anda menggunakan Organizations untuk mengaktifkan fitur kebijakan tag. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna root (tidak direkomendasikan) di akun pengelolaan organisasi. Kemudian Anda dapat membuat kebijakan tag dan melampirkannya ke entitas organisasi untuk memberlakukan aturan penandaan tersebut.

- Gunakan AWS Resource Groups untuk mengelola kepatuhan dengan kebijakan tag. Saat masuk ke sebuah akun dalam organisasi, Anda menggunakan Resource Groups untuk menemukan tag yang tak sesuai pada sumber daya di akun tersebut. Anda dapat memperbaiki tag yang tak sesuai di layanan AWS di mana Anda membuat sumber daya tersebut.

  Jika Anda masuk dengan akun pengelolaan di organisasi, Anda dapat melihat informasi kepatuhan semua akun organisasi Anda.

Kebijakan tag hanya tersedia di organisasi yang mengaktifkan semua fitur. Untuk informasi lebih lanjut mengenai apa yang diperlukan untuk menggunakan kebijakan tag, lihat Prasyarat dan izin untuk mengelola kebijakan tag.

> **Important**
>
> Untuk memulai kebijakan tag, AWS sangat menganjurkan agar Anda mengikuti contoh alur kerja yang dijelaskan di Memulai kebijakan tag sebelum beralih ke kebijakan tag yang lebih lanjut. Sebaiknya Anda pahami dampak dari melampirkan kebijakan tag yang sederhana ke satu akun sebelum memperluas kebijakan tag ke seluruh OU atau organisasi. Sangat penting untuk memahami dampak kebijakan tag sebelum Anda menegakkan kepatuhan dengan kebijakan tag apa pun. Tabel pada halaman Memulai kebijakan tag juga menyediakan tautan ke instruksi untuk tugas terkait kebijakan yang lebih lanjut.

Prasyarat dan izin untuk mengelola kebijakan tag

Halaman ini menjelaskan prasyarat dan izin yang diperlukan untuk mengelola kebijakan tag di AWS Organizations.

Topik

- Prasyarat untuk mengelola kebijakan tag
- Izin untuk mengelola kebijakan tag

Prasyarat untuk mengelola kebijakan tag

Menggunakan kebijakan tag memerlukan hal-hal berikut:

- Organisasi Anda harus mengaktifkan semua fitur.

- Anda harus masuk ke akun pengelolaan organisasi Anda.
- Anda memerlukan izin yang tercantum dalam Izin untuk mengelola kebijakan tag.

Untuk mengevaluasi kepatuhan terhadap kebijakan tag, Anda menggunakan AWS Resource Groups. Untuk informasi tentang persyaratan untuk mengevaluasi kepatuhan, lihat Prasyarat dan Izin di Panduan Pengguna AWS Resource Groups.

Izin untuk mengelola kebijakan tag

Contoh kebijakan IAM berikut menyediakan izin untuk mengelola kebijakan tag.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ManageTagPolicies",
            "Effect": "Allow",
            "Action": [
                "organizations:ListPoliciesForTarget",
                "organizations:ListTargetsForPolicy",
                "organizations:DescribeEffectivePolicy",
                "organizations:DescribePolicy",
                "organizations:ListRoots",
                "organizations:DisableAWSServiceAccess",
                "organizations:DetachPolicy",
                "organizations:DeletePolicy",
                "organizations:DescribeAccount",
                "organizations:DisablePolicyType",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListPolicies",
                "organizations:ListAccountsForParent",
                "organizations:ListAccounts",
                "organizations:EnableAWSServiceAccess",
                "organizations:ListCreateAccountStatus",
                "organizations:DescribeOrganization",
                "organizations:UpdatePolicy",
                "organizations:EnablePolicyType",
                "organizations:DescribeOrganizationalUnit",
                "organizations:AttachPolicy",
                "organizations:ListParents",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:CreatePolicy",
```

```
                "organizations:DescribeCreateAccountStatus"
            ],
            "Resource": "*"
        }
    ]
}
```

Untuk informasi selengkapnya tentang Kebijakan IAM dan izin, lihat Panduan Pengguna IAM.

Praktik terbaik untuk menggunakan kebijakan tag

AWS merekomendasikan praktik terbaik berikut untuk menggunakan kebijakan tag.

Tentukan strategi kapitalisasi tag

Tentukan bagaimana Anda ingin memanfaatkan tag dan secara konsisten menerapkan strategi tersebut di semua jenis sumber daya. Misalnya, putuskan apakah akan menggunakan `Costcenter`, `costcenter`, atau `CostCenter` dan menggunakan kesepakatan yang sama untuk semua tag. Untuk hasil yang konsisten dalam laporan kepatuhan, hindari penggunaan tag yang serupa dengan perlakuan kasus yang tidak konsisten. Strategi ini akan membantu Anda menentukan kebijakan tag untuk organisasi Anda.

Gunakan alur kerja yang direkomendasikan

Mulai dari kecil dengan membuat kebijakan tag yang sederhana. Kemudian lampirkan ke akun anggota yang dapat Anda gunakan untuk tujuan pengujian. Gunakan alur kerja yang dijelaskan di Memulai kebijakan tag.

Menentukan aturan penandaan

Hal ini akan tergantung pada kebutuhan organisasi Anda. Sebagai contoh, Anda mungkin ingin menentukan bahwa ketika tag `CostCenter` dilampirkan ke AWS Secrets Manager rahasia, maka ia harus menggunakan perlakuan kasus yang ditentukan. Buat kebijakan tag yang menentukan tag yang patuh dan melampirkannya ke entitas organisasi di mana Anda ingin aturan penandaan tersebut berlaku.

Mengedukasi administrator akun

Saat Anda siap memperluas penggunaan kebijakan tag, berikan edukasi pada administrator akun mengenai hal-hal berikut:

- Sampaikan strategi pemberian tag Anda.
- Tekankan bahwa administrator perlu menggunakan tag pada jenis sumber daya tertentu.

  Hal ini penting, karena sumber daya yang tak ditandai tidak menunjukkan sebagai tag yang tidak patuh dalam hasil kepatuhan.
- Berikan panduan untuk memeriksa kepatuhan terhadap kebijakan tag. Instruksikan administrator untuk menemukan dan memperbaiki tag yang tidak patuh pada sumber daya di akun mereka menggunakan prosedur yang dijelaskan di Mengevaluasi Kepatuhan untuk sebuah Akun di Panduan Pengguna AWS Resource Groups. Biarkan mereka tahu seberapa sering Anda ingin mereka memeriksa kepatuhan.

Gunakan kehati-hatian dalam menegakkan kepatuhan

Menegakkan kepatuhan dapat mencegah pengguna yang ada di akun organisasi Anda menandai sumber daya yang mereka butuhkan. Meninjau informasi di Memahami penegakan. Lihat juga alur kerja yang dijelaskan di Memulai kebijakan tag.

Pertimbangkan untuk membuat SCP untuk mengatur pagar di sekitar permintaan pembuatan sumber daya

Sumber daya yang tidak pernah memiliki tag yang dilampirkan padanya tidak ditampilkan sebagai sumber daya tidak patuh dalam laporan. Administrator akun masih dapat membuat sumber daya yang tak ditandai. Dalam beberapa kasus, Anda dapat menggunakan kebijakan kontrol layanan (SCP) untuk mengatur pagar di sekitar permintaan pembuatan sumber daya. Sebagai contoh SCP, lihat Mengharuskan tag pada sumber daya yang dibuat tertentu. Untuk mempelajari apakahAWSlayanan mendukung pengendalian akses menggunakan tag, lihatAWSLayanan yang Bekerja dengan IAMdiPanduan Pengguna IAM. Cari layanan yang memiliki Ya di kolom Otorisasi berdasarkan tag. Pilih nama layanan untuk melihat dokumentasi otorisasi dan kontrol akses untuk layanan tersebut.

Memulai kebijakan tag

Menggunakan kebijakan tag melibatkan bekerja dengan beberapa AWS layanan. Untuk memulai, tinjau halaman berikut. Kemudian ikuti alur kerja di halaman ini untuk mengetahui kebijakan tag dan efeknya.

- Prasyarat dan izin untuk mengelola kebijakan tag
- Praktik terbaik untuk menggunakan kebijakan tag

Menggunakan kebijakan tag untuk pertama kalinya

Ikuti langkah berikut untuk mulai menggunakan kebijakan tag untuk pertama kalinya.

Tugas	Akun untuk masuk ke	AWS konsol layanan untuk digunakan
Langkah 1: Aktifkan kebijakan tag untuk organisasi Anda.	Akun pengelolaan organisasi.[1]	AWS Organizations
Langkah 2: Membuat kebijakan tag. Pastikan kebijakan tag pertama Anda sederhana . Masukkan satu kunci tag dalam kasus perlakuan yang ingin Anda gunakan dan biarkan semua pilihan lain pada pengaturan default-nya.	Akun pengelolaan organisasi.[1]	AWS Organizations
Langkah 3: Lampirkan kebijakan tag ke akun anggota tunggal yang dapat Anda gunakan untuk pengujian. Anda harus masuk ke akun ini pada langkah berikutnya.	Akun pengelolaan organisasi.[1]	AWS Organizations
Langkah 4: Buat beberapa sumber daya dengan tag yang patuh dan beberapa dengan tag yang tidak patuh.	Akun anggota yang sedang Anda gunakan untuk tujuan pengujian.	AWS Layanan apa pun yang Anda merasa nyaman. Misalnya, Anda dapat menggunakan AWS Secrets Manager dan ikuti prosedur di Membuat Rahasia Basic untuk membuat rahasia dengan rahasia yang patuh dan tidak patuh.

Tugas	Akun untuk masuk ke	AWS konsol layanan untuk digunakan
Langkah 5: Lihat kebijakan tag efektif dan evaluasi status kepatuhan akun.	Akun anggota yang sedang Anda gunakan untuk tujuan pengujian.	Resource Groups dan AWS layanan tempat sumber daya dibuat. Jika Anda membuat sumber daya dengan tag patuh dan tidak patuh, maka Anda akan melihat tag yang tidak patuh dalam hasil.
Langkah 6: Ulangi proses pencarian dan perbaikan masalah kepatuhan sampai sumber daya yang ada dalam akun pengujian patuh dengan kebijakan tag Anda.	Akun anggota yang sedang Anda gunakan untuk tujuan pengujian.	Resource Groups dan AWS layanan tempat sumber daya dibuat.
Kapan saja, Anda dapat mengevaluasi kepatuhan di seluruh organisasi.	Akun pengelolaan organisasi.[1]	Resource Groups

[1] Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna root (tidak direkomendasikan) di akun pengelolaan organisasi.

Memperluas penggunaan kebijakan tag

Anda dapat melakukan tugas-tugas berikut dalam urutan apapun untuk memperluas penggunaan kebijakan tag Anda.

Tugas lanjutan	Akun untuk masuk ke	AWS konsol layanan untuk digunakan
Membuat kebijakan tag lanjutan.	Akun pengelolaan organisasi.[1]	AWS Organizations

Tugas lanjutan	Akun untuk masuk ke	AWS konsol layanan untuk digunakan
Ikuti proses yang sama seperti untuk pengguna pertama kali, tapi coba tugas yang lain. Misalnya, tentukan kunci atau nilai tambahan atau tentukan perlakuan kasus yang berbeda untuk kunci tag. Anda dapat menggunak an informasi di Memahami warisan kebijakan manajemen dan Sintaks kebijakan tag untuk membuat kebijakan tag yang lebih detail.		
Lampirkan kebijakan tag ke akun tambahan atau OU. Periksa kebijakan tag efektif untuk akun setelah Anda melampirkan lebih banyak kebijakan untuk akun tersebut atau ke OU di mana akun menjadi anggota.	Akun pengelolaan organisasi.[1]	AWS Organizations
Buat SCP untuk mengharus kan tag ketika ada yang menciptakan sumber daya baru. Sebagai contoh, lihat Mengharuskan tag pada sumber daya yang dibuat tertentu.	Akun pengelolaan organisasi.[1]	AWS Organizations

Tugas lanjutan	Akun untuk masuk ke	AWS konsol layanan untuk digunakan
Lanjutkan untuk mengevaluasi status kepatuhan akun terhadap kebijakan tag efektif saat ada perubahan. Perbaiki tag tidak patuh.	Akun anggota dengan kebijakan tag efektif.	Resource Groups dan AWS layanan tempat sumber daya dibuat.
Evaluasi kepatuhan di seluruh organisasi.	Akun pengelolaan organisasi.[1]	Resource Groups

[1] Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna root (tidak direkomendasikan) di akun pengelolaan organisasi.

Menegakkan kebijakan tag untuk pertama kalinya

Untuk menerapkan kebijakan tag untuk pertama kalinya, ikuti alur kerja yang mirip dengan menggunakan kebijakan tag untuk pertama kalinya dan gunakan akun pengujian.

> **Warning**
>
> Gunakan kehati-hatian dalam menegakkan kepatuhan. Pastikan bahwa Anda memahami efek menggunakan kebijakan tag dan ikuti alur kerja yang direkomendasikan. Uji bagaimana penegakan bekerja pada sebuah akun pengujian sebelum memperluasnya ke akun lainnya. Jika tidak, Anda dapat mencegah pengguna di akun organisasi Anda dari menandai sumber daya yang mereka butuhkan. Untuk informasi lebih lanjut, lihat Memahami penegakan.

Tugas penegakan	Akun untuk masuk ke	AWS konsol layanan untuk digunakan
Langkah 1: Membuat kebijakan tag. Pastikan kebijakan tag pertama yang Anda tegakkan sederhana. Masukkan satu	Akun pengelolaan organisasi.[1]	AWS Organizations

Tugas penegakan	Akun untuk masuk ke	AWS konsol layanan untuk digunakan
kunci tag dalam perlakuan kasus yang ingin Anda gunakan, dan pilih opsi Mencegah operasi yang tidak patuh untuk tag ini. Kemudian tentukan satu jenis sumber daya untuk menegakkannya. Melanjutkan dengan contoh kami sebelumnya, Anda dapat memilih untuk menegakka nnya pada rahasia Secrets Manager.		
Langkah 2: Lampirkan kebijakan tag ke sebuah akun uji.	Akun pengelolaan organisasi.[1]	AWS Organizations
Langkah 3: Coba buat beberapa sumber daya dengan tag yang patuh dan beberapa dengan tag yang tidak patuh. Anda seharusnya tidak diizinkan untuk membuat tag pada sumber daya dari jenis yang ditentukan dalam kebijakan tag dengan tag yang tidak sesuai.	Akun anggota yang sedang Anda gunakan untuk tujuan pengujian.	AWS Layanan apa pun yang Anda merasa nyaman. Misalnya, Anda dapat menggunakan AWS Secrets Manager dan ikuti prosedur di Membuat Rahasia Basic untuk membuat rahasia dengan rahasia yang patuh dan tidak patuh.
Langkah 4: Evaluasi status kepatuhan akun terhadap kebijakan tag efektif dan koreksi tag yang tidak patuh.	Akun anggota yang sedang Anda gunakan untuk tujuan pengujian.	Resource Groups dan AWS layanan tempat sumber daya dibuat.

Tugas penegakan	Akun untuk masuk ke	AWS konsol layanan untuk digunakan
Langkah 5: Ulangi proses pencarian dan perbaikan masalah kepatuhan sampai sumber daya yang ada dalam akun pengujian patuh dengan kebijakan tag Anda.	Akun anggota yang sedang Anda gunakan untuk tujuan pengujian.	Resource Groups dan AWS layanan tempat sumber daya dibuat.
Kapan saja, Anda dapat mengevaluasi kepatuhan di seluruh organisasi.	Akun pengelolaan organisasi.[1]	Resource Groups

[1] Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna root (tidak direkomendasikan) di akun pengelolaan organisasi.

Membuat, memperbarui, dan menghapus kebijakan tag

Dalam topik ini:

- Setelah Anda mengaktifkan kebijakan tag untuk organisasi Anda, Anda dapat membuat sebuah kebijakan.
- Bila persyaratan penandaan berubah, Anda dapat memperbarui kebijakan yang ada.
- Bila Anda tidak lagi memerlukan kebijakan dan setelah melepaskannya dari semua unit organisasi (OU) dan akun, Anda dapat menghapusnya.

> **Important**
>
> Sumber daya yang tidak diberi tag tidak akan muncul sebagai tag tidak patuh dalam hasil.

Membuat kebijakan tag

> **Izin minimum**
>
> Untuk membuat kebijakan tag, Anda memerlukan izin untuk menjalankan tindakan-tindakan berikut:
>
> - `organizations:CreatePolicy`

Anda dapat membuat kebijakan tag di AWS Management Console dengan salah satu dari dua cara berikut:

- Editor visual yang memungkinkan Anda memilih opsi dan menghasilkan teks kebijakan JSON untuk Anda.
- Editor teks yang memungkinkan Anda langsung membuat teks kebijakan JSON sendiri.

Editor visual membuat prosesnya mudah, namun membatasi fleksibilitas Anda. Ini adalah cara yang bagus untuk membuat kebijakan pertama Anda dan merasa nyaman menggunakannya. Setelah Anda memahami cara kerjanya dan mulai dibatasi oleh apa yang disediakan editor visual, Anda dapat menambahkan fitur lanjutan ke kebijakan Anda dengan mengedit teks kebijakan JSON sendiri. Editor visual hanya menggunakan operator pengaturan-nilai @@assign, dan tidak menyediakan akses apa pun ke operator kontrol anak. Anda dapat menambahkan operator kontrol anak hanya jika Anda mengedit teks kebijakan JSON secara manual.

AWS Management Console

Untuk membuat kebijakan tag

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Kebijakan tag, pilih Buat Kebijakan.
3. Pada halaman Bua kebijakan, masukkan Nama kebijakan dan Deskripsi kebijakan opsional.
4. (Opsional) Anda dapat menambahkan satu tag atau lebih ke objek kebijakan itu sendiri. Tag tersebut bukan bagian dari kebijakan. Untuk melakukan ini, pilih Tambahkan tag dan kemudian masukkan nilai kunci dan nilai opsional. Membiarkan nilai kosong akan mengaturnya menjadi string kosong; itu bukan `null`. Anda dapat melampirkan hingga 50

tag ke kebijakan. Untuk informasi lebih lanjut, lihat Penandaan pada sumber daya AWS Organizations.

5. Anda dapat membangun kebijakan tag dengan menggunakan Editor visual seperti yang diterangkan dalam prosedur ini. Anda juga dapat mengetik atau menempelkan kebijakan tag di tab JSON. Untuk informasi selengkapnya tentang sintaks kebijakan tag, lihat Sintaks kebijakan tag.

   Untuk Kunci tag baru 1, tentukan nama kunci tag yang akan ditambahkan.

6. Untuk Kepatuhan kapitalisasi kunci tag, biarkan opsi ini dihapus (default) untuk menentukan bahwa kebijakan tag induk yang diwariskan, jika ada, harus menentukan perlakuan kasus untuk kunci tag tersebut.

   Aktifkan opsi ini jika Anda ingin mengamanatkan kapitalisasi khusus untuk kunci tag dengan menggunakan kebijakan ini. Jika Anda memilih pilihan ini, kapitalisasi yang Anda tentukan untuk Kunci Tag akan mengganti perlakuan kasus yang ditentukan dalam kebijakan induk yang diwariskan.

   Jika kebijakan induk tidak ada dan Anda tidak mengaktifkan opsi ini, hanya kunci tag di semua karakter huruf kecil yang dianggap sesuai. Untuk informasi selengkapnya tentang warisan dari kebijakan induk, lihat Memahami warisan kebijakan manajemen.

   > **Tip**
   >
   > Pertimbangkan untuk menggunakan kebijakan tag contoh yang ditampilkan di Contoh 1: Tentukan kasus kunci tag di seluruh organisasi sebagai panduan dalam membuat kebijakan tag yang menentukan kunci tag dan perlakuan kasusnya. Lampirkan kebijakan tag ke organisasi root. Kemudian, Anda dapat membuat dan melampirkan kebijakan tag tambahan ke OU atau akun untuk membuat aturan penandaan tambahan.

7. Untuk kepatuhan nilai tag, aktifkan opsi ini jika Anda ingin menambahkan nilai yang diizinkan untuk kunci tag ini dengan nilai apapun yang diwarisi dari kebijakan induk.

   Secara default, opsi ini dihapus, yang berarti bahwa hanya nilai-nilai yang didefinisikan dalam dan diwarisi dari kebijakan induk yang dianggap patuh. Jika kebijakan induk tidak ada dan Anda tidak menentukan nilai tag maka nilai apapun (termasuk tidak ada nilai sama sekali) akan dianggap patuh.

Untuk memperbarui daftar nilai tag yang dapat diterima, pilih Tentukan nilai yang diizinkan untuk kunci tag ini lalu pilih Tentukan nilai. Saat diminta, masukkan nilai baru (satu nilai per kotak), dan kemudian pilih Simpan perubahan.

8. Untuk Mencegah operasi tidak patuh untuk tag ini, sebaiknya biarkan opsi ini dihapus (default) kecuali jika Anda berpengalaman menggunakan kebijakan tag. Pastikan Anda telah meninjau rekomendasi di Memahami penegakan, dan uji secara menyeluruh. Jika tidak, Anda dapat mencegah pengguna di akun organisasi Anda dari menandai sumber daya yang mereka butuhkan.

   Jika Anda ingin menerapkan kepatuhan dengan kunci tag ini, pilih kotak centang dan kemudian Tentukan jenis sumber daya. Saat diminta, pilih jenis sumber daya untuk disertakan dalam kebijakan. Lalu pilih Simpan perubahan.

   > **Important**
   >
   > Ketika Anda memilih opsi ini, setiap operasi yang memanipulasi tag untuk sumber daya dari jenis tertentu hanya akan berhasil jika hasil operasi dalam tag patuh dengan kebijakan.

9. (Opsional) Untuk menambahkan kunci tag lain ke kebijakan tag ini, pilih Tambahkan kunci tag. Kemudian lakukan langkah 6–9 untuk menentukan kunci tag.
10. Setelah selesai membuat kebijakan tag, pilih Simpan perubahan.

AWS CLI & AWS SDKs

Untuk membuat kebijakan tag

Anda dapat menggunakan salah satu hal berikut untuk membuat kebijakan tag:

- AWS CLI: buat-kebijakan

  Anda dapat menggunakan editor teks apa pun untuk membuat sebuah kebijakan tag. Gunakan sintaks JSON dan simpan kebijakan tag sebagai file dengan nama dan ekstensi di lokasi yang Anda pilih. Kebijakan tag dapat terdiri dari maksimum 2.500 karakter, termasuk spasi. Untuk informasi selengkapnya tentang sintaks kebijakan tag, lihat Sintaks kebijakan tag.

Untuk membuat kebijakan tag

1. Membuat kebijakan tag dalam file teks yang terlihat serupa dengan berikut ini:

   Isi dari `testpolicy.json`:

   ```
   {
       "tags": {
           "CostCenter": {
               "tag_key": {
                   "@@assign": "CostCenter"
               }
           }
       }
   }
   ```

   Kebijakan tag ini menentukan kunci tag `CostCenter`. Tag dapat menerima nilai apapun atau bahkan tanpa nilai. Kebijakan seperti ini berarti bahwa sumber daya yang memiliki CostCenter tag yang dilampirkan dengan atau tanpa nilai sesuai.

2. Membuat kebijakan yang berisi konten kebijakan dari file. Spasi kosong ekstra dalam keluaran telah dipotong agar lebih mudah dibaca.

   ```
   $ aws organizations create-policy \
       --name "MyTestTagPolicy" \
       --description "My Test policy" \
       --content file://testpolicy.json \
       --type TAG_POLICY
   {
       "Policy": {
           "PolicySummary": {
               "Id": "p-a1b2c3d4e5",
               "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
   tag_policy/p-a1b2c3d4e5",
               "Name": "MyTestTagPolicy",
               "Description": "My Test policy",
               "Type": "TAG_POLICY",
               "AwsManaged": false
           },
           "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign
   \":\"CostCenter\"\n}\n}\n}\n}\n\n"
       }
   ```

```
}
```

- AWSSDK: CreatePolicy

Apa yang harus dilakukan selanjutnya

Setelah membuat kebijakan tag, Anda dapat menerapkan aturan penandaan. Untuk melakukannya, lampirkan kebijakan untuk organisasi root, unit organisasi (UO), Akun AWS dalam organisasi Anda, atau kombinasi dari entitas organisasi.

Memperbarui kebijakan tag

> **Izin minimum**
>
> Untuk memperbarui kebijakan tag, Anda harus memiliki izin untuk menjalankan tindakan-tindakan berikut:
>
> - `organizations:UpdatePolicy` dengan elemen `Resource` dalam pernyataan kebijakan yang sama yang mencakup ARN dari kebijakan yang ditentukan (atau "*")
> - `organizations:DescribePolicy` dengan elemen `Resource` dalam pernyataan kebijakan yang sama yang mencakup ARN dari kebijakan yang ditentukan (atau "*")

AWS Management Console

Untuk memperbarui kebijakan tag

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Kebijakan tag halaman halaman, pilih kebijakan tag yang ingin Anda perbarui.
3. Pilih Edit kebijakan.
4. Anda dapat memasukkan Nama kebijakan, Deskripsi kebijakan baru. Anda dapat mengubah konten kebijakan dengan menggunakan Editor visual atau dengan mengedit JSON.
5. Setelah selesai memperbarui kebijakan tag, pilih Simpan perubahan.

AWS CLI & AWS SDKs

Untuk memperbarui kebijakan

Anda dapat menggunakan salah satu hal berikut untuk memperbarui kebijakan:

- AWS CLI: update-policy

  Contoh berikut mengganti nama kebijakan tag.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "Renamed tag policy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
        "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":
\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

  Contoh berikut menambahkan atau mengubah deskripsi untuk kebijakan tag.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new tag policy description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Description": "My new tag policy description",
            "Type": "TAG_POLICY",
            "AwsManaged": false
```

```
        },
       "Content": "{\n\"tags\":{\n\"CostCenter\":{\n\"tag_key\":{\n\"@@assign\":
\"CostCenter\"\n}\n}\n}\n}\n\n"
    }
}
```

Contoh berikut mengubah dokumen kebijakan JSON yang dilampirkan pada kebijakan memilih keluar layanan AI. Dalam contoh ini, konten diambil dari file bernama `policy.json` dengan teks berikut:

```
{
  "tags": {
    "Stage": {
      "tag_key": {
        "@@assign": "Stage"
      },
      "tag_value": {
        "@@assign": [
          "Production",
          "Test"
        ]
      }
    }
  }
}
```

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --content file://policy.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
tag_policy/p-i9j8k7l6m5",
            "Name": "Renamed tag policy",
            "Description": "My new tag policy description",
            "Type": "TAG_POLICY",
            "AwsManaged": false
        },
```

```
        "Content": "{\"tags\":{\"Stage\":{\"tag_key\":{\"@@assign\":\"Stage
\"},\"tag_value\":{\"@@assign\":[\"Production\",\"Test\"]},\"enforced_for\":
{\"@@assign\":[\"ec2:instance\"]}}}}"
}
```

- AWSSDK: UpdatePolicy

Mengedit tag yang dilampirkan pada kebijakan tag

Saat Anda masuk ke akun pengelolaan organisasi Anda, Anda dapat menambahkan atau menghapus tag yang dilampirkan pada kebijakan tag. Caranya, lakukan langkah-langkah berikut.

Izin minimum

Untuk mengedit tag yang dilampirkan pada kebijakan tag di organisasi AWS Anda, Anda harus memiliki izin berikut:

- `organizations:DescribeOrganization` (konsol saja — untuk menavigasi ke kebijakan)
- `organizations:DescribePolicy` (konsol saja — untuk menavigasi ke kebijakan)
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

Untuk mengedit tag yang dilampirkan pada kebijakan memilih keluar layanan AI

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Kebijakan tag halaman halaman, pilih nama kebijakan dengan tag yang ingin Anda edit.
3. Pada halaman detail kebijakan yang dipilih, pilih tab Tag, dan kemudian pilih Kelola tag.
4. Anda dapat melakukan salah satu tindakan berikut di laman ini:

- Edit nilai untuk tag dengan memasukkan nilai baru menggantikan yang lama. Anda tidak dapat memodifikasi kunci. Untuk mengubah kunci, Anda harus menghapus tag dengan kunci yang lama dan menambahkan tag dengan kunci yang baru.
- Hapus tag yang ada dengan memilih Hapus.
- Tambahkan kunci tag dan pasangan nilai baru. Pilih Tambahkan tag, lalu masukkan nama kunci baru dan nilai opsional dalam kotak yang disediakan. Jika Anda membiarkan kotak Nilai kosong, nilai-nya adalah string kosong; itu bukan `null`.

5. Pilih Simpan perubahan setelah Anda melakukan semua penambahan, penghapusan, dan pengeditan yang ingin Anda buat.

AWS CLI & AWS SDKs

Untuk mengedit tag yang dilampirkan pada kebijakan tag

Anda dapat menggunakan salah satu perintah berikut untuk mengedit tag yang dilampirkan pada kebijakan tag:

- AWS CLI: tag-resource dan untag-resource
- AWSSDK: TagResourcedan UntagResource

Menghapus kebijakan tag

Saat masuk ke akun pengelolaan organisasi Anda, Anda dapat menghapus kebijakan yang tidak diperlukan lagi di organisasi Anda.

Sebelum Anda dapat menghapus kebijakan, Anda harus melepasnya terlebih dahulu dari semua entitas terlampir.

Izin minimum

Untuk menghapus kebijakan tag, Anda harus memiliki izin untuk menjalankan tindakan berikut:

- `organizations:DeletePolicy`

AWS Management Console

Untuk menghapus kebijakan tag

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2.
3. Pada halaman Kebijakan tag halaman halaman, pilih kebijakan tag yang ingin Anda hapus.
4. Anda harus melepaskan kebijakan yang ingin Anda hapus dari semua root, OU, dan akun. Pilih tab Target, pilih tombol radio yang ada di samping setiap root, OU, atau akun yang ditampilkan di daftar Target, dan kemudian pilih Lepaskan. Dalam kotak dialog konfirmasi, pilih Lepaskan.
5. Pilih Hapus di bagian atas halaman.
6. Pada kotak dialog konfirmasi, masukkan nama kebijakan, dan kemudian pilih Hapus.

AWS CLI & AWS SDKs

Untuk menghapus kebijakan tag

Anda dapat menggunakan salah satu hal berikut untuk menghapus kebijakan:

- AWS CLI: hapus-kebijakan

  Contoh berikut menghapus kebijakan yang ditentukan. Ia berfungsi hanya jika kebijakan tidak dilampirkan pada root, OU, atau akun apa pun.

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWSSDK: DeletePolicy

Memasang dan pelepasan kebijakan tag

Anda dapat menggunakan kebijakan tag di seluruh organisasi serta pada unit organisasi (OU) dan masing-masing akun.

- Saat Anda melampirkan kebijakan tag ke organisasi root, kebijakan tag berlaku untuk semua anggota OU dan akun root tersebut.
- Ketika Anda melampirkan kebijakan tag ke OU, kebijakan tag berlaku untuk akun yang ada di OU tersebut. Akun tersebut juga tunduk pada kebijakan tag apa pun yang dilampirkan ke root organisasi.
- Ketika Anda melampirkan kebijakan tag ke akun, kebijakan tag berlaku pada akun tersebut. Selain itu, akun tersebut tunduk pada kebijakan tag yang dilampirkan pada root organisasi, ditambah kebijakan tag yang dilampirkan pada OU di mana akun tersebut menjadi bagiannya.

Agregasi kebijakan tag apa pun yang diwarisi akun, ditambah kebijakan tag apa pun yang langsung dilampirkan pada akun adalah kebijakan tag efektif. Untuk informasi selengkapnya, lihat Memahami warisan kebijakan manajemen.

Important

Sumber daya yang tidak diberi tag tidak akan muncul sebagai tag tidak patuh dalam hasil.

Izin minimum

Untuk melampirkan kebijakan tag, Anda harus memiliki izin untuk menjalankan tindakan berikut:

- `organizations:AttachPolicy`

AWS Management Console

Anda dapat melampirkan kebijakan tag dengan menavigasi ke kebijakan atau ke root, OU, atau akun yang ingin Anda lampirkan kebijakan padanya.

Untuk melampirkan kebijakan tag dengan menavigasi ke root, OU, atau akun

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Akun AWS, buka dan lalu pilih nama root, OU, atau akun yang ingin Anda lampirkan kebijakan padanya. Anda mungkin harus memperluas OU (pilih

untuk menemukan OU atau akun yang Anda inginkan.

3. Di tab Kebijakan, dalam entri untuk Kebijakan tag, pilih Lampirkan.
4. Temukan kebijakan yang Anda inginkan dan pilih Lampirkan kebijakan.

   Daftar kebijakan tag terlampir pada tab Kebijakan sudah diperbarui dan mencakup tambahan baru. Perubahan kebijakan langsung berlaku.

Untuk melampirkan kebijakan tag dengan menavigasi ke kebijakan

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Kebijakan tag, pilih nama kebijakan yang ingin Anda lampirkan.
3. Di tab Target, pilih Lampirkan.
4. Pilih tombol radio yang ada di samping root, OU, atau akun yang ingin Anda lampirkan kebijakan padanya. Anda mungkin harus memperluas OU (pilih untuk menemukan OU atau akun yang Anda inginkan.
5. Pilih Pasang kebijakan.

   Daftar kebijakan tag terlampir pada tab Target sudah diperbarui dan mencakup tambahan baru. Perubahan kebijakan langsung berlaku.

AWS CLI & AWS SDKs

Untuk melampirkan kebijakan tag ke root organisasi, OU, atau akun

Anda dapat menggunakan salah satu hal berikut untuk melampirkan kebijakan tag:

- AWS CLI: attach-policy

  Prosedur berikut menunjukkan cara melampirkan kebijakan tag yang baru saja Anda buat ke sebuah akun pengujian.

  - Lampirkan kebijakan tag ke akun pengujian Anda dengan menjalankan sebuah perintah seperti berikut ini:

```
$ aws organizations attach-policy \
    --target-id <account-id> \
    --policy-id p-a1b2c3d4e5
```

Perintah ini tidak akan memberikan keluaran apa pun jika berhasil.

- AWSSDK: AttachPolicy

Perubahan kebijakan langsung berlaku.

Apa yang harus dilakukan selanjutnya

Setelah melampirkan kebijakan tag, Anda dapat mengetahui seberapa patuh sumber daya Anda dengan kebijakan tag tersebut. Untuk melakukan ini, gunakan konsol Resource Groups. Untuk informasi, lihat Mengevaluasi Kepatuhan Akun di Panduan Pengguna AWS Resource Groups.

Melepaskan kebijakan tag

Saat masuk ke akun pengelolaan organisasi, Anda dapat melepaskan kebijakan tag dari root organisasi, OU, atau akun yang melampirkan kebijakan tag tersebut. Setelah Anda melepaskan kebijakan tag dari sebuah entitas, kebijakan tersebut tidak lagi berlaku untuk akun yang terpengaruh oleh entitas yang sekarang telah melepaskan kebijakan tersebut. Untuk melepaskan kebijakan, lakukan langkah-langkah berikut.

Izin minimum

Untuk melepaskan kebijakan tag dari root organisasi, OU, atau akun, Anda harus memiliki izin untuk menjalankan tindakan-tindakan berikut:

- `organizations:DetachPolicy`

AWS Management Console

Anda dapat melepaskan kebijakan tag dengan menavigasi ke kebijakan atau root, OU, atau akun yang ingin Anda lepaskan kebijakan darinya.

Untuk melepaskan kebijakan tag dengan menavigasi ke root, OU, atau akun yang melampirkan kebijakan tersebut

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Akun AWS navigasi ke akar, OU, atau akun yang ingin Anda lepaskan kebijakan darinya. Anda mungkin harus memperluas OU (pilih ▸) untuk menemukan OU atau akun yang Anda inginkan. Pilih nama Root, OU, atau akun.
3. Pada tab Kebijakan, pilih tombol radio di samping kebijakan tag yang ingin Anda lepaskan, kemudian pilih Lepaskan.
4. Dalam kotak dialog konfirmasi, pilih Lepaskan kebijakan.

   Daftar kebijakan tag terlampir telah diperbarui. Perubahan kebijakan langsung berlaku.

Untuk melepaskan kebijakan tag dengan menavigasi ke kebijakan

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Kebijakan tag, pilih nama kebijakan yang ingin Anda lepaskan dari root, OU, atau akun.
3. Pada tab Target, pilih tombol radio yang ada di sebelah root, OU, atau akun yang ingin Anda lepaskan kebijakan darinya. Anda mungkin harus memperluas OU (pilih ▸) untuk menemukan OU atau akun yang Anda inginkan.
4. Pilih Lepaskan.
5. Dalam kotak dialog konfirmasi, pilih Lepaskan.

   Daftar kebijakan tag terlampir telah diperbarui. Perubahan kebijakan langsung berlaku.

AWS CLI & AWS SDKs

Untuk melepaskan kebijakan tag dari root organisasi, OU, atau akun

Anda dapat menggunakan salah satu hal berikut untuk melepaskan kebijakan tag:

- AWS CLI: detach-policy
- AWSSDK: DetachPolicy

Perubahan kebijakan langsung berlaku.

Melihat kebijakan tag efektif

Sebelum Anda mulai memeriksa status kepatuhan untuk sumber daya yang ditandai di akun, sebaiknya tentukan kebijakan tag efektif untuk sebuah akun terlebih dahulu.

Apa itu kebijakan tag efektif?

kebijakan tag efektif menentukan aturan penandaan yang berlaku untuk sebuah akun. Ini adalah agregasi dari setiap kebijakan tag yang diwarisi akun, ditambah kebijakan tag yang langsung dilampirkan pada akun tersebut. Bila Anda melampirkan kebijakan tag ke root organisasi, maka kebijakan tag tersebut akan berlaku untuk semua akun di organisasi Anda. Ketika Anda melampirkan kebijakan tag ke sebuah OU, maka kebijakan tag tersebut akan berlaku untuk akun yang ada dalam OU tersebut.

Sebagai contoh, kebijakan tag yang dilampirkan ke root organisasi dapat menentukan tag `CostCenter` dengan empat nilai patuh. Kebijakan tag terpisah yang dilampirkan ke akun dapat membatasi kunci `CostCenter` pada dua dari empat nilai patuh saja. Kombinasi dari kebijakan tag ini terdiri dari kebijakan tag efektif. Hasilnya adalah bahwa hanya dua dari empat nilai tag patuh yang didefinisikan dalam kebijakan tag root organisasi yang patuh untuk akun tersebut.

Untuk informasi dan contoh lanjutan tentang seberapa efektif kebijakan tag yang dihasilkan, lihat Memahami warisan kebijakan manajemen.

Cara melihat kebijakan tag efektif

Anda dapat melihat kebijakan tag efektif untuk akun dari AWS Management Console, API AWS, atau AWS Command Line Interface.

> **Izin minimum**
>
> Untuk melihat kebijakan tag efektif untuk akun, Anda harus memiliki izin untuk menjalankan tindakan-tindakan berikut:
>
> - `organizations:DescribeEffectivePolicy`

- `organizations:DescribeOrganization`

AWS Management Console

Melihat kebijakan tag efektif untuk sebuah akun

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Akun AWS, pilih nama akun yang ingin Anda lihat kebijakan tag efektif-nya. Anda mungkin harus memperluas OU (pilih ▶) untuk menemukan akun yang Anda inginkan.
3. Pada tab Kebijakan, di bagian Kebijakan tag, pilih Lihat kebijakan tag efektif untuk Akun AWS.

   Konsol menampilkan kebijakan efektif yang diterapkan pada akun yang ditentukan.

   > **Note**
   >
   > Anda tidak dapat menyalin dan menempelkan kebijakan efektif dan menggunakannya sebagai JSON untuk kebijakan tag lain tanpa perubahan signifikan. Dokumen kebijakan tag harus mencakup operator warisan yang menentukan bagaimana setiap pengaturan digabung ke kebijakan efektif akhir.

AWS CLI & AWS SDKs

Melihat kebijakan tag efektif untuk sebuah akun

Anda dapat menggunakan salah satu hal berikut untuk melihat kebijakan tag efektif:

- AWS CLI: describe-effective-policy

  Untuk menentukan aturan penandaan apa yang diwarisi oleh atau dilampirkan ke akun, jalankan berikut dari akun dan simpan hasilnya ke file:

```
$ aws organizations describe-effective-policy \
```

```
    --policy-type TAG_POLICY
{
    "EffectivePolicy": {
        "PolicyContent": "{\"tags\":{\"costcenter\":{\"tag_value\":[\"*\"],
\"tag_key\":\"CostCenter\"}}}",
        "LastUpdatedTimestamp": "2020-06-09T08:34:25.103000-07:00",
        "TargetId": "123456789012",
        "PolicyType": "TAG_POLICY"
    }
}
```

Jika kebijakan tag dilampirkan ke akun serta root-nya atau OU apa pun, maka kombinasi dari semua kebijakan yang diwariskan akan menentukan kebijakan tag efektif akun. Dalam kasus ini, menjalankan `describe-effective-policy` dari akun akan mengembalikan konten gabungan dari semua kebijakan tag dalam hirarki akun.

- AWSSDK: DescribeEffectivePolicy

Menggunakan Amazon EventBridge untuk memantau tag yang tidak sesuai

Anda dapat menggunakan Amazon EventBridge, sebelumnya Amazon CloudWatch Events, untuk memantau kapan tag yang tidak sesuai diperkenalkan. Dalam peristiwa contoh berikut ini, nilai `"false"` untuk `tag-policy-compliant` menunjukkan bahwa tag baru tidak patuh dengan kebijakan tag efektif.

```
{
  "detail-type": "Tag Change on Resource",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa"
  ],
  "detail": {
    "changed-tag-keys": [
      "a-new-key"
    ],
    "service": "ec2",
    "resource-type": "instance",
    "version": 3,
    "tag-policy-compliant": "false",
    "tags": {
      "a-new-key": "tag-value-on-new-key-just-added"
    }
```

```
  }
}
```

Anda dapat berlangganan peristiwa dan menentukan string atau pola untuk memantau. Untuk informasi selengkapnya EventBridge, lihat Panduan EventBridge Pengguna Amazon.

Memahami penegakan

Kebijakan tag dapat menentukan apakah operasi penandaan yang tak sesuai pada jenis sumber daya tertentu ditegakkan. Dengan kata lain, permintaan penandaan yang tidak sesuai pada jenis sumber daya yang ditentukan dicegah untuk diselesaikan.

> **Important**
>
> Penegakan tidak berpengaruh pada sumber daya yang dibuat tanpa tag.

Untuk menegakkan kepatuhan terhadap kebijakan tag, lakukan salah satu hal berikut saat Anda membuat kebijakan tag:

- Dari tab Editor visual, pilih Cegah operasi yang tidak patuh untuk tag ini.
- Dari tab JSON, gunakan bidang `enforced_for`. Untuk informasi tentang sintaks kebijakan tag, lihat Sintaks dan contoh kebijakan tag.

Ikuti praktik terbaik berikut untuk menerapkan kepatuhan terhadap kebijakan tag:

- Gunakan kehati-hatian dalam menegakkan kepatuhan — Pastikan Anda memahami efek penggunaan kebijakan tag, dan ikuti alur kerja yang disarankan yang dijelaskan di Memulai kebijakan tag. Uji bagaimana penegakan bekerja pada sebuah akun pengujian sebelum memperluasnya ke akun lainnya. Jika tidak, Anda dapat mencegah pengguna di akun organisasi Anda dari menandai sumber daya yang mereka butuhkan.
- Ketahui jenis sumber daya apa yang dapat Anda tegakkan — Anda hanya dapat menegakkan kepatuhan terhadap kebijakan tag pada jenis sumber daya yang didukung. Jenis sumber daya yang men-support penegakan kepatuhan tercantum saat Anda menggunakan editor visual untuk membangun kebijakan tag.
- Memahami interaksi dengan beberapa layanan — Beberapa AWS layanan memiliki pengelompokan sumber daya seperti kontainer yang secara otomatis membuat sumber daya untuk

Anda, dan tag dapat menyebar dari sumber daya di satu layanan ke layanan lainnya. Misalnya, tag pada grup Amazon EC2 Auto Scaling dan klaster Amazon EMR dapat secara otomatis menyebarkan dengan instans Amazon EC2 yang terkandung. Anda mungkin memiliki kebijakan tag untuk Amazon EC2 yang lebih ketat daripada grup Auto Scaling atau klaster EMR. Jika Anda mengaktifkan penegakan, maka kebijakan tag mencegah sumber daya agar tidak ditandai dan dapat memblokir penskalaan dan penyediaan yang dinamis.

Bagian berikut menunjukkan bagaimana Anda dapat menemukan sumber daya tidak patuh, dan memperbaikinya agar patuh.

Menemukan sumber daya tidak patuh untuk sebuah akun

Untuk setiap akun, Anda bisa mendapatkan informasi tentang sumber daya yang tidak patuh. Anda harus menjalankan perintah ini dari setiap WIlayah di mana akun tersebut memiliki sumber daya.

Untuk menemukan sumber daya yang tidak sesuai untuk akun dengan kebijakan tag, jalankan perintah berikut untuk menyimpan hasil ke file:

```
$ aws resourcegroupstaggingapi get-resources  --region us-east-1 \
    --include-compliance-details \
    --exclude-compliant-resources > outputfile.txt
```

Memperbaiki tag tidak patuh dalam sumber daya

Setelah menemukan tag tidak patuh, lakukan perbaikan menggunakan salah satu metode berikut. Anda harus masuk ke akun yang memiliki sumber daya dengan tag yang tidak patuh:

- Gunakan konsol atau menandai operasi API AWS layanan yang membuat sumber daya yang tidak sesuai.
- Gunakan AWS Resource Groups TagResourcesdan UntagResourcesoperasi untuk menambahkan tag yang sesuai dengan kebijakan efektif atau untuk menghapus tag yang tidak sesuai.

Menemukan dan memperbaiki masalah ke-tidak-patuhan tambahan

Menemukan dan memperbaiki masalah kepatuhan adalah proses yang berulang. Ulangi langkah-langkah di dua bagian sebelumnya hingga sumber daya yang Anda rawat patuh dengan kebijakan tag Anda.

Membuat laporan kepatuhan di seluruh organisasi

Kapan saja, Anda dapat membuat laporan yang mencantumkan semua sumber daya yang ditandai di Akun AWS seluruh organisasi Anda. Laporan ini menunjukkan apakah setiap sumber daya patuh dengan kebijakan tag efektif. Perlu diketahui bahwa perubahan yang Anda buat pada kebijakan tag atau sumber daya memerlukan waktu hingga 48 jam untuk tercermin dalam laporan kepatuhan di seluruh organisasi. Sebagai contoh, anggaplah bahwa Anda memiliki kebijakan tag yang mendefinisikan tag standar baru untuk jenis sumber daya. Jenis sumber daya itu yang tidak memiliki tag ini akan ditampilkan sebagai patuh dalam laporan hingga 48 jam.

Anda dapat membuat laporan dari akun pengelolaan organisasi Anda di Wilayah `us-east-1`, dengan ketentuan bahwa akun memiliki akses ke bucket Amazon S3. Bucket harus memiliki kebijakan bucket terlampir seperti yang ditunjukkan di Kebijakan Bucket Amazon S3 untuk Menyimpan Laporan. Untuk membuat laporan, jalankan perintah berikut:

```
$ aws resourcegroupstaggingapi get-compliance-summary --region us-east-1
{
    "SummaryList": [
        {
            "LastUpdated": "2020-06-09T18:40:46Z",
            "NonCompliantResources": 0
        }
    ]
}
```

Anda dapat membuat satu laporan dalam satu waktu.

Laporan ini dapat memakan waktu lama untuk diselesaikan. Anda dapat memeriksa status dengan menjalankan perintah berikut:

```
$ aws resourcegroupstaggingapi describe-report-creation --region us-east-1
{
    "Status": "SUCCEEDED"
}
```

Setelah perintah di atas mengembalikan `SUCCEEDED`, Anda dapat membuka laporan dari bucket Amazon S3.

Layanan dan jenis sumber daya yang men-support penegakan

Layanan dan jenis sumber daya berikut mendukung penegakan kebijakan tag:

Nama layanan	Jenis sumber daya	Sintaks JSON
Amazon API Gateway	• Kunci API • Nama domain • Operasi REST API • Tahapan	• `"apigateway:apikeys"` • `"apigateway:domainnames"` • `"apigateway:restapis"` • `"apigateway:restapis/stages"`
AWS Amplify	• Komponen • Tema	• `"amplifyuibuilder:app/environment/components"` • `"amplifyuibuilder:app/environment/themes"`
AWS AppConfig	• Aplikasi • Profil Konfigurasi • Deployment • Strategi Penerapan • Environment	• `"appconfig:application"` • `"appconfig:application/configurationprofile"` • `"appconfig:application/environment/deployment"` • `"appconfig:deploymentstrategy"` • `"appconfig:application/environment"`
AWS App Mesh	• Semua • Rute gerbang • Mesh • Rute • Gerbang virtual • Simpul virtual • Router virtual • Layanan virtual	• `"appmesh:*"` • `"appmesh:mesh/virtualGateway/gatewayRoute"` • `"appmesh:mesh"` • `"appmesh:mesh/virtualRouter/route"` • `"appmesh:mesh/virtualGateway"` • `"appmesh:mesh/virtualNode"` • `"appmesh:mesh/virtualRouter"` • `"appmesh:mesh/virtualService"`
Amazon Athena	• Semua • Workgroup	• `"athena:*"` • `"athena:workgroup"`

Nama layanan	Jenis sumber daya	Sintaks JSON
AWS Audit Manager	• Penilaian • Kerangka Penilaian • Kontrol	• `"auditmanager:assessment "` • `"auditmanager:assessmentFramework "` • `"auditmanager:control "`
AWS Backup	• Paket Backup • Vault • Gateway • Visor Hiper • VM	• `"backup:backup-plan"` • `"backup:backup-vault"` • `"backup-gateway:gateway"` • `"backup-gateway:hypervisor"` • `"backup-gateway:vm"`
AWS Batch	• Pekerjaan • Ketentuan Tugas • Antrean Tugas	• `"batch:job"` • `"batch:job-definition"` • `"batch:job-queue"`
AWS BugBust	• Peristiwa	• `"bugbust:event"`
AWS Certificate Manager	• Semua • Sertifikat • Otoritas Sertifikat Swasta	• `"acm:*"` • `"acm:certificate"` • `"acm-pca:certificate-authority"`
Amazon Chime	• Instans Aplikasi • Channel • Pipa Media • Rapat • Aplikasi Media SIP • Instans Aplikasi Pengguna • Konektor Suara	• `"chime:app-instance"` • `"chime:app-instance/channel"` • `"chime:media-pipeline"` • `"chime:meeting"` • `"chime:sma"` • `"chime:app-instance/user"` • `"chime:vc"`

Nama layanan	Jenis sumber daya	Sintaks JSON
AWS Clean Rooms	• Kolaborasi • Tabel yang Dikonfigurasi • Keanggotaan • Asosiasi Tabel yang Dikonfigurasi	• `"cleanrooms:collaboration"` • `"cleanrooms:configuredtable"` • `"cleanrooms:membership"` • `"cleanrooms:membership/configuredtableassociation"`
AWS Cloud9	• Environment	• `"cloud9:environment"`
Amazon CloudFront	• Semua • Distribusi • Distribusi streaming	• `"cloudfront:*"` • `"cloudfront:distribution"` • `"cloudfront:streaming-distribution"`
AWS CloudTrail	• Semua • Trail	• `"cloudtrail:*"` • `"cloudtrail:trail"`
Amazon CloudWatch	• Semua • Alarm • Aturan Wawasan Kontributor • Aliran Metrik	• `"cloudwatch:*"` • `"cloudwatch:alarm"` • `"cloudwatch:insight-rule"` • `"cloudwatch:metric-stream"`
Monitor CloudWatch Internet Amazon	• Memantau	• `"internetmonitor:monitor"`
CloudWatch Log Amazon	• Tujuan • Grup log	• `"logs:destination"` • `"logs:log-group"`
Manajer Akses CloudWatch Observabilitas Amazon	• Tautan • Wastafel	• `"oam:link"` • `"oam:sink"`

Nama layanan	Jenis sumber daya	Sintaks JSON
AWS CodeBuild	• Semua • Proyek	• `"codebuild:*"` • `"codebuild:project"`
Amazon CodeCatalyst	• Koneksi	• `"codecatalyst:connections"`
AWS CodeCommit	• Semua • Repositori	• `"codecommit:*"` • `"codecommit:repository"`
AWS CodePipeline	• Semua • Jenis tindakan • Alur • Webhook	• `"codepipeline:*"` • `"codepipeline:actiontype"` • `"codepipeline:pipeline"` • `"codepipeline:webhook"`
Identitas Amazon Cognito	• Semua • Kolam identitas	• `"cognito-identity:*"` • `"cognito-identity:identitypool"`
Kolam pengguna Amazon Cognito	• Semua • Kolam pengguna	• `"cognito-idp:*"` • `"cognito-idp:userpool"`
Amazon Comprehend	• Semua • Pengklasifikasi dokumen • Pengenal entitas	• `"comprehend:*"` • `"comprehend:document-classifier"` • `"comprehend:entity-recognizer"`
AWS Config	• Semua • Otorisasi agregasi • Agregator Config • Aturan Config	• `"config:*"` • `"config:aggregation-authorization"` • `"config:config-aggregator"` • `"config:config-rule"`
CodeGuru Peninjau Amazon	• Asosiasi	• `"codeguru-reviewer:association"`

Nama layanan	Jenis sumber daya	Sintaks JSON
CodeGuru Keamanan Amazon	• Scan	• `"codeguru-security:scans"`
CodeConnections	• Koneksi • Host	• `"codestar-connections:connection"` • `"codestar-connections:host"`
Amazon Connect	• Kontak Flow • Asosiasi Integrasi • Antrean • Connect Cepat • Profil Routing • Pengguna	• `"connect:instance/contact-flow"` • `"connect:instance/integration-association"` • `"connect:instance/queue"` • `"connect:instance/transfer-destination"` • `"connect:instance/routing-profile"` • `"connect:instance/agent"`
Kebijaksanaan Amazon Connect	• Asisten • Asosiasi • Daftar isi • Basis Pengetahuan • Sesi	• `"wisdom:assistant"` • `"wisdom:association"` • `"wisdom:content"` • `"wisdom:knowledge-base"` • `"wisdom:session"`
AWS Database Migration Service	• Semua • Titik akhir • ES • Rep • Subgrp • Tugas	• `"dms:*"` • `"dms:endpoint"` • `"dms:es"` • `"dms:rep"` • `"dms:subgrp"` • `"dms:task"`

Nama layanan	Jenis sumber daya	Sintaks JSON
Amazon Data Lifecycle Manager	• Kebijakan	• `"dlm:policy"`
AWS Dioda	• Pemetaan	• `"diode-messaging:mapping"`
AWS Direct Connect	• Semua • Dxcon • Dxlag • Dxvif	• `"directconnect:*"` • `"directconnect:dxcon"` • `"directconnect:dxlag"` • `"directconnect:dxvif"`
Amazon DynamoDB	• Semua • Tabel	• `"dynamodb:*"` • `"dynamodb:table"`
Amazon EC2	• Pencadangan kapasitas • Armada reservasi kapasitas • Gateway pembawa	• `"ec2:capacity-reservation"` • `"ec2:capacity-reservation-fleet"` • `"ec2:carrier-gateway"`
	• Titik akhir VPN klien • Kolam CoIP • Gateway pelanggan	• `"ec2:client-vpn-endpoint"` • `"ec2:coip-pool"` • `"ec2:customer-gateway"`
	• Tuan rumah khusus • Opsi DHCP • Gateway internet khusus egress	• `"ec2:dedicated-host"` • `"ec2:dhcp-options"` • `"ec2:egress-only-internet-gateway"`
	• IP elastis • Jendela acara • Armada	• `"ec2:elastic-ip"` • `"ec2:instance-event-window"` • `"ec2:fleet"`

Nama layanan	Jenis sumber daya	Sintaks JSON
	• Citra FPGA • Reservasi host • Citra	• `"ec2:fpga-image"` • `"ec2:host-reservation"` • `"ec2:image"`
	• Instans • Gateway internet • Manajer Alamat IP	• `"ec2:instance"` • `"ec2:internet-gateway"` • `"ec2:ipam"`
	• Pool Manajer Alamat IP • Lingkup Manajer Alamat IP • Kolam IPv4	• `"ec2:ipam-pool"` • `"ec2:ipam-scope"` • `"ec2:ipv4pool-ec2"`
	• Pasangan Kunci • Templat peluncuran • Tabel Rute Gerbang Lokal	• `"ec2:key-pair"` • `"ec2:launch-template"` • `"ec2:local-gateway-route-table"`
	• Tabel Rute Gerbang Lokal Asosiasi Grup Antarmuka Virtual • Tabel Rute Gerbang Lokal Asosiasi VPC • Gateway NAT	• `"ec2:local-gateway-route-table-virtual-interface-group-association"` • `"ec2:local-gateway-route-table-vpc-association"` • `"ec2:natgateway"`
	• ACL Jaringan • Antarmuka jaringan • Lingkup Akses Wawasan Jaringan	• `"ec2:network-acl"` • `"ec2:network-interface"` • `"ec2:network-insights-access-scope"`

Nama layanan	Jenis sumber daya	Sintaks JSON
	• Analisis Lingkup Akses Wawasan Jaringan • Analisis Wawasan Jaringan • Jalur Wawasan Jaringan	• `"ec2:network-insights-access-scope-analysis"` • `"ec2:network-insights-analysis"` • `"ec2:network-insights-path"`
	• Grup Penempatan • Daftar Awalan • Ganti Tugas Volume Root	• `"ec2:placement-group"` • `"ec2:prefix-list"` • `"ec2:replace-root-volume-task"`
	• Instans Cadangan • Tabel rute • Grup keamanan	• `"ec2:reserved-instances"` • `"ec2:route-table"` • `"ec2:security-group"`
	• Snapshot • Permintaan Instans Spot • Subnet	• `"ec2:snapshot"` • `"ec2:spot-instances-request"` • `"ec2:subnet"`
	• Reservasi CIDR Subnet • Filter Traffic Mirror • Sesi Traffic Mirror	• `"ec2:subnet-cidr-reservation"` • `"ec2:traffic-mirror-filter"` • `"ec2:traffic-mirror-session"`
	• Target Traffic Mirror • Transit Gateway • Lampiran Transit Gateway	• `"ec2:traffic-mirror-target"` • `"ec2:transit-gateway"` • `"ec2:transit-gateway-attachment"`

Nama layanan	Jenis sumber daya	Sintaks JSON
	• Transit Gateway Connect Peer • Domain Multicast Transit Gateway • Tabel Kebijakan Transit Gateway	• `"ec2:transit-gateway-connect-peer"` • `"ec2:transit-gateway-multicast-domain"` • `"ec2:transit-gateway-policy-table"`
	• Tabel Rute Transit Gateway • Titik Akhir Akses Terverifikasi • Grup Akses Terverifikasi	• `"ec2:transit-gateway-route-table"` • `"ec2:verified-access-endpoint"` • `"ec2:verified-access-group"`
	• Instans Akses Terverifikasi • Penyedia Kepercayaan Akses Terverifikasi • Volume	• `"ec2:verified-access-instance"` • `"ec2:verified-access-trust-provider"` • `"ec2:volume"`
	• Log Aliran VPC • VPC • VPC endpoint	• `"ec2:vpc-flow-log"` • `"ec2:vpc"` • `"ec2:vpc-endpoint"`
	• Layanan VPC endpoint • Koneksi peering VPC • Koneksi VPN • Gateway VPN	• `"ec2:vpc-endpoint-service"` • `"ec2:vpc-peering-connection"` • `"ec2:vpn-connection"` • `"ec2:vpn-gateway"`

Nama layanan	Jenis sumber daya	Sintaks JSON
Tempat Sampah Daur Ulang Amazon EC2	• Aturan	• `"rbin:rule"`
AWS Elastic Beanstalk	• Aplikasi • Versi aplikasi • Templat konfigurasi • Platform	• `"elasticbeanstalk:application"` • `"elasticbeanstalk:applicationversion"` • `"elasticbeanstalk:configurationtemplate"` • `"elasticbeanstalk:platform"`
Amazon Elastic Container Registry	• Repositori	• `"ecr:repository"`
Amazon Elastic Container Service	• Penyedia Kapasitas • Klaster • Layanan • Definisi Tugas • Set tugas	• `"ecs:capacity-provider"` • `"ecs:cluster"` • `"ecs:service"` • `"ecs:task-definition"` • `"ecs:task-set"`
Amazon Elastic File System	• Semua • Sistem file	• `"elasticfilesystem:*"` • `"elasticfilesystem:file-system"`
Amazon Elastic Inference	• Akselerator	• `"elastic-inference:elastic-inference-accelerator"`
Amazon Elastic Kubernetes Service	• Klaster	• `"eks:cluster"`
Pencarian Elastis Amazon	• Domain	• `"es:domain"`
Amazon EMR	• Klaster • Editor	• `"elasticmapreduce:cluster"` • `"elasticmapreduce:editor"`

Nama layanan	Jenis sumber daya	Sintaks JSON
Amazon EMR Tanpa Server	• Aplikasi	• `"emr-serverless:applications"`
AWS Resolusi Entitas	• Alur Kerja Pencocokan • Pemetaan Skema	• `"entityresolution:matchingworkflow"` • `"entityresolution:schemamapping"`
Amazon ElastiCache	• Klaster	• `"elasticache:cluster"`
Amazon EventBridge	• Semua • Bus peristiwa • Aturan	• `"events:*"` • `"events:event-bus"` • `"events:rule"`
EventBridge Pipa Amazon	• Pipa	• `"pipes:pipe"`
EventBridge Penjadwal Amazon	• Jadwal Grup	• `"scheduler:schedule-group"`
Amazon Fraud Detector	• Detektor • Versi detektor • Model • Aturan • Variabel	• `"frauddetector:detector"` • `"frauddetector:detector-version"` • `"frauddetector:model"` • `"frauddetector:rule"` • `"frauddetector:variable"`
Akselerator Global Amazon	• Akselerator	• `"globalaccelerator:accelerator"`

Nama layanan	Jenis sumber daya	Sintaks JSON
Penyeimbang Beban Elastis	• Semua • Listener • Aturan Pendengar • Penyeimbang beban • Grup target	• `"elasticloadbalancing:*"` • `"elasticloadbalancing:listener"` • `"elasticloadbalancing:listener-rule"` • `"elasticloadbalancing:loadbalancer"` • `"elasticloadbalancing:targetgroup"`
Amazon FSx	• Semua • Backup • Sistem file	• `"fsx:*"` • `"fsx:backup"` • `"fsx:file-system"`
Amazon GuardDuty	• Detektor • Filter • Set IP • Set Intel Ancaman	• `"guardduty:detector"` • `"guardduty:detector/filter"` • `"guardduty:detector/ipset"` • `"guardduty:detector/threatintelset"`
AWS HealthLake	• Penyimpanan data	• `"healthlake:datastore  "`

Nama layanan	Jenis sumber daya	Sintaks JSON
AWS HealthOmics	• Toko Anotasi • Versi Toko Anotasi • Toko Referensi • Referensi • Jalankan . • Jalankan Grup • Toko Urutan • Baca Set • Toko Varian • Alur kerja	• `"omics:annotationStore"` • `"omics:annotationStore/version"` • `"omics:referenceStore"` • `"omics:referenceStore/reference"` • `"omics:run"` • `"omics:runGroup"` • `"omics:sequenceStore"` • `"omics:sequenceStore/readSet"` • `"omics:variantStore"` • `"omics:workflow"`
Amazon Inspector	• Filter	• `"inspector2:filter "`
AWS Identity and Access Management	• Profil Instance • MFA • Penyedia OIDC • Kebijakan • Penyedia SALL • Sertifikat Server	• `"iam:instance-profile"` • `"iam:mfa"` • `"iam:oidc-provider"` • `"iam:policy"` • `"iam:saml-provider"` • `"iam:server-certificate"`
AWS IoT Analytics	• Semua • Saluran • Set data • Penyimpanan data • Alur	• `"iotanalytics:*"` • `"iotanalytics:channel"` • `"iotanalytics:dataset"` • `"iotanalytics:datastore"` • `"iotanalytics:pipeline"`
AWS IoT Events	• Semua • Model detektor • Input	• `"iotevents:*"` • `"iotevents:detectorModel"` • `"iotevents:input"`

Nama layanan	Jenis sumber daya	Sintaks JSON
AWS IoT Fleet Hub	• Aplikasi	• `"iotfleethub:application"`
AWS IoT SiteWise	• Aset • Model Aset	• `"iotsitewise:asset"` • `"iotsitewise:asset-model  "`
AWS IoT Greengrass	• Penyebaran Massal • Definisi Konektor • Definisi Inti • Definisi Perangkat • Definisi Fungsi • Definisi Logger • Definisi Sumber Daya • Definisi Langganan	• `"greengrass:bulk"` • `"greengrass:connectorsDefinition"` • `"greengrass:coresDefinition"` • `"greengrass:devicesDefinition"` • `"greengrass:functionsDefinition"` • `"greengrass:loggersDefinition"` • `"greengrass:resourcesDefinition"` • `"greengrass:subscriptionsDefinition"`
AWS Key Management Service	• Semua • Kunci	• `"kms:*"` • `"kms:key"`
Amazon Kinesis	• Semua • Aplikasi	• `"kinesisanalytics:*"` • `"kinesisanalytics:application"`
Amazon Data Firehose	• Semua • Aliran pengiriman	• `"firehose:*"` • `"firehose:deliverystream"`
AWS Lambda	• Semua • Fungsi	• `"lambda:*"` • `"lambda:function"`
Amazon Macie	• Pengidentifikasi Data Kustom	• `"macie2:custom-data-identifier"`
Amazon MediaStore	• Kontainer	• `"mediastore:container"`

Nama layanan	Jenis sumber daya	Sintaks JSON
Amazon MQ	• Pialang • Konfigurasi	• `"mq:broker"` • `"mq:configuration"`
Firewall Jaringan Amazon	• firewall • Kebijakan Firewall • Grup Aturan Stateful • Kelompok Aturan Tanpa Kewargane garaan	• `"network-firewall:firewall"` • `"network-firewall:firewall-policy"` • `"network-firewall:stateful-rulegroup"` • `"network-firewall:stateless-rulegroup"`
Amazon Tanpa OpenSearch Server	• Koleksi	• `"aoss:collection"`
AWS Organizations	• Akun • Unit Organisasi • Kebijakan • root	• `"organizations:account"` • `"organizations:ou"` • `"organizations:policy"` • `"organizations:root"`
Amazon Pinpoint SMS Voice V2	• Set Konfigurasi • Daftar Keluar • Nomor Telepon • Kolam • Id Pengirim	• `"sms-voice:configuration-set"` • `"sms-voice:opt-out-list"` • `"sms-voice:phone-number"` • `"sms-voice:pool"` • `"sms-voice:sender-id"`

Nama layanan	Jenis sumber daya	Sintaks JSON
Amazon RDS	• Grup parameter klaster • Titik akhir klaster • Langganan peristiwa • Grup opsi DB • Grup parameter DB • Proksi DB • Titik akhir proxy DB • Instans DB pesanan • Grup keamanan DB • Grup subnet DB • Grup target	• `"rds:cluster-pg"` • `"rds:cluster-endpoint"` • `"rds:es"` • `"rds:og"` • `"rds:pg"` • `"rds:db-proxy"` • `"rds:db-proxy-endpoint"` • `"rds:ri"` • `"rds:secgrp"` • `"rds:subgrp"` • `"rds:target-group"`
Amazon Redshift	• Semua • Klaster • Grup DB • Nama DB • Pengguna DB • Langganan peristiwa • Sertifikat klien HSM • Konfigurasi HSM • Grup parameter • Snapshot • Pemberian salinan snapshot • Jadwal snapshot • Grup subnet	• `"redshift:*"` • `"redshift:cluster"` • `"redshift:dbgroup"` • `"redshift:dbname"` • `"redshift:dbuser"` • `"redshift:eventsubscription"` • `"redshift:hsmclientcertificate"` • `"redshift:hsmconfiguration"` • `"redshift:parametergroup"` • `"redshift:snapshot"` • `"redshift:snapshotcopygrant"` • `"redshift:snapshotschedule"` • `"redshift:subnetgroup"`

Nama layanan	Jenis sumber daya	Sintaks JSON
Amazon Redshift Tanpa Server	• Namespace • Workgroup	• `"redshift-serverless:namespace"` • `"redshift-serverless:workgroup"`
AWS Resource Access Manager	• Semua • Berbagi sumber daya	• `"ram:*"` • `"ram:resource-share"`
AWS Resource Groups	• Semua • Grup	• `"resource-groups:*"` • `"resource-groups:group"`
Amazon Route 53	• Zona yang di-hosting	• `"route53:hostedzone"`
Amazon Route 53 Resolver	• Semua • Titik akhir penyelesai • Aturan penyelesai	• `"route53resolver:*"` • `"route53resolver:resolver-endpoint"` • `"route53resolver:resolver-rule"`
Amazon S3	• Bucket • Lensa Penyimpanan • Grup Lensa Penyimpanan	• `"s3:bucket"` • `"s3:storage-lens"` • `"s3:storage-lens-group"`

Nama layanan	Jenis sumber daya	Sintaks JSON
Amazon SageMaker	• Config Gambar Aplikasi • Artifact • Konteks • Tugas pelatihan • Tugas pengolahan • Grup paket model • UI tugas manusia • Model Package • Tindakan • Alur • Eksperimen • Definisi Aliran • Proyek	• `"sagemaker:app-image-config"` • `"sagemaker:artifact"` • `"sagemaker:context"` • `"sagemaker:training-job"` • `"sagemaker:processing-job "` • `"sagemaker:model-package-group"` • `"sagemaker:human-task-ui"` • `"sagemaker:model-package"` • `"sagemaker:action"` • `"sagemaker:pipeline"` • `"sagemaker:experiment"` • `"sagemaker:flow-definition"` • `"sagemaker:project"`
AWS Secrets Manager	• Semua • Rahasia	• `"secretsmanager:*"` • `"secretsmanager:secret"`
AWS Danau Keamanan	• Data Danau • Pelanggan	• `"securitylake:data-lake"` • `"securitylake:subscriber"`
AWS Service Catalog	• Aplikasi • Grup Atribut • Portofolio • Produk	• `"servicecatalog:applications"` • `"servicecatalog:attribute-groups "` • `"catalog:portfolio "` • `"catalog:product "`
Amazon Simple Notification Service (SNS)	• Topik	• `"sns:topic"`

Nama layanan	Jenis sumber daya	Sintaks JSON
Amazon Simple Queue Service (SQS)	• Antrean	• `"sqs:queue"`
Amazon States Language	• Semua • Aktifitas • Mesin Negara	• `"states:*"` • `"states:activity "` • `"states:stateMachine  "`
AWS Step Functions	• Aktivitas	• `"states:activity"`
AWS Storage Gateway	• Semua • Gateway • Bagikan • Tape • Volume	• `"storagegateway:*"` • `"storagegateway:gateway"` • `"storagegateway:share"` • `"storagegateway:tape"` • `"storagegateway:gateway/volume"`
AWS Systems Manager	• Asosiasi • Eksekusi otomatisasi • Dokumen • Periode Pemeliharaan • Instans terkelola • Item operasional • Dasar patch • Sesi • Kontak	• `"ssm:association"` • `"ssm:automation-execution"` • `"ssm:document"` • `"ssm:maintenancewindow"` • `"ssm:managed-instance"` • `"ssm:opsitem"` • `"ssm:patchbaseline"` • `"ssm:session"` • `"ssm-contacts:contact"`
Amazon Textract	• Adaptor • Versi	• `"textract:adapters"` • `"textract:adapters/versions"`

Nama layanan	Jenis sumber daya	Sintaks JSON
AWS Transfer Family	• Server • Pengguna • Alur kerja	• `"transfer:server"` • `"transfer:user"` • `"transfer:workflow"`
Amazon Diarsitek sikan dengan Baik	• Beban kerja	• `"wellarchitected:workload"`
AWS Wickr	• Jaringan	• `"wickr:network"`
Amazon WorkSpaces	• Semua • Alias Koneksi • Direktori • WorkSpace • WorkSpaces bundel • WorkSpaces gambar • WorkSpaces Grup IP	• `"workspaces:*"` • `"workspaces:connectionalias"` • `"workspaces:directory"` • `"workspaces:workspace"` • `"workspaces:workspacebundle"` • `"workspaces:workspaceimage"` • `"workspaces:workspaceipgroup"`
Amazon WorkLink	• Armada	• `"worklink:fleet"`

Sintaks dan contoh kebijakan tag

Halaman ini menjelaskan sintaks kebijakan tag dan memberikan contoh.

Sintaks kebijakan tag

Kebijakan tag adalah file plaintext yang terstruktur sesuai dengan aturan JSON. Sintaks untuk kebijakan tag tersebut mengikuti sintaks untuk jenis kebijakan pengelolaan. Untuk pembahasan lengkap tentang sintaks itu, lihat Memahami warisan kebijakan manajemen. Topik ini berfokus pada penerapan sintaks umum untuk persyaratan spesifik jenis kebijakan tag.

Kebijakan tag berikut menunjukkan sintaks kebijakan tag basic:

```
{
```

```
    "tags": {
        "costcenter": {
            "tag_key": {
                "@@assign": "CostCenter"
            },
            "tag_value": {
                "@@assign": [
                    "100",
                    "200"
                ]
            },
            "enforced_for": {
                "@@assign": [
                    "secretsmanager:*"
                ]
            }
        }
    }
}
```

Sintaks kebijakan tag mencakup elemen-elemen berikut:

- Nama kunci bidang `tags`. Kebijakan tag selalu dimulai dengan nama kunci tetap ini. Ini adalah baris teratas dalam contoh kebijakan di atas.
- Sebuah kunci kebijakan yang secara unik mengidentifikasi pernyataan kebijakan. Ini harus sesuai dengan nilai untuk kunci tag, kecuali untuk perlakuan kasus. Berbeda dengan kunci tag (dijelaskan selanjutnya), nilai kebijakan tidak peka huruf besar kecil.

  Dalam contoh ini, `costcenter` adalah kunci kebijakan.
- Setidaknya satu kunci tag yang menentukan kunci tag yang diperbolehkan dengan kapitalisasi yang Anda ingin dipatuhi oleh sumber daya. Jika penanganan kasus tidak didefinisikan, maka huruf kecil adalah perlakuan kasus default untuk kunci tag. Nilai untuk kunci tag harus sesuai dengan nilai untuk kunci kebijakan. Tapi karena nilai kunci kebijakan sensitif huruf besar kecil, maka kapitalisasi-nya bisa berbeda.

  Dalam contoh ini, `CostCenter` adalah kunci tag. Ini adalah perlakuan kasus yang diperlukan untuk kepatuhan dengan kebijakan tag. Sumber daya dengan perlakuan kasus alternatif untuk kunci tag ini tidak patuh dengan kebijakan tag.

  Anda dapat menentukan beberapa kunci tag dalam kebijakan tag.

- (Opsional) Daftar satu atau lebih nilai tag yang dapat diterima untuk kunci tag. Jika kebijakan tag tidak menentukan nilai tag untuk kunci tag tersebut, maka nilai apapun (termasuk tidak ada nilai sama sekali) akan dianggap patuh.

  Dalam contoh ini, nilai yang dapat diterima untuk kunci tag `CostCenter` adalah `100` dan `200`.

- (Opsional) Sebuah opsi `enforced_for` yang menunjukkan apakah akan mencegah operasi penandaan tidak patuh pada layanan tertentu dan sumber daya. Di konsol tersebut, ini adalah opsi Mencegah operasi tidak patuh untuk tag ini di editor visual untuk membuat kebijakan tag. Nilai pengaturan default untuk opsi ini adalah null.

  Contoh tag kebijakan menetapkan bahwa semua sumber daya AWS Secrets Manager harus memiliki tag ini.

  > ⚠ Warning
  >
  > Anda hanya harus mengubah opsi ini dari pengaturan default-nya jika Anda berpengalaman menggunakan kebijakan tag. Jika tidak, Anda dapat mencegah pengguna di akun organisasi Anda dari membuat sumber daya yang mereka butuhkan.

- Operator yang menentukan bagaimana kebijakan tag bergabung dengan kebijakan tag lain dalam pohon organisasi untuk membuat kebijakan tag efektif. Dalam contoh ini, `@@assign` digunakan untuk menetapkan string ke `tag_key`, `tag_value`, dan `enforced_for`. Untuk informasi selengkapnya tentang operator, lihat Operator pewarisan.
- — Anda dapat menggunakan wildcard `*` dalam nilai tag dan bidang `enforced_for`.
  - Anda dapat menggunakan satu wildcard saja untuk setiap nilai tag. Misalnya, `*@example.com` diperbolehkan, tapi `*@*.com` tidak.
  - Untuk `enforced_for`, Anda dapat menggunakan `<service>:*` dengan beberapa layanan untuk memungkinkan penegakan untuk semua sumber daya untuk layanan tersebut. Untuk daftar layanan dan jenis sumber daya yang men-support `enforced_for`, lihat Layanan dan jenis sumber daya yang men-support penegakan.

    Anda tidak dapat menggunakan wildcard untuk menentukan semua layanan atau menentukan sumber daya untuk semua layanan.

Contoh kebijakan tag

Contoh kebijakan tag berikut adalah untuk tujuan informasi saja.

> **Note**
>
> Sebelum Anda mencoba menggunakan kebijakan tag contoh ini dalam organisasi Anda, perhatikan hal berikut:
>
> - Pastikan Anda telah mengikuti alur kerja yang direkomendasikan untuk memulai kebijakan tag.
> - Anda harus hati-hati dalam meninjau dan menyesuaikan kebijakan tag ini untuk kebutuhan unik Anda.
> - Semua karakter dalam kebijakan tag Anda tunduk pada ukuran maksimum. Contoh dalam panduan ini menunjukkan kebijakan tag yang diformat dengan spasi kosong ekstra untuk meningkatkan keterbacaannya. Namun, untuk menghemat ruang jika ukuran kebijakan Anda mendekati ukuran maksimum, maka Anda dapat menghapus spasi kosong. Contoh spasi kosong termasuk karakter spasi dan jeda baris yang berada di luar tanda kutip.
> - Sumber daya yang tidak diberi tag tidak akan muncul sebagai tag tidak patuh dalam hasil.

Contoh 1: Tentukan kasus kunci tag di seluruh organisasi

Contoh berikut menunjukkan kebijakan tag yang hanya mendefinisikan dua kunci tag dan kapitalisasi yang Anda inginkan agar akun dalam organisasi Anda menjadi standardisasi.

Kebijakan A — kebijakan tag akar organisasi

```
{
    "tags": {
        "CostCenter": {
            "tag_key": {
                "@@assign": "CostCenter",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        },
        "Project": {
            "tag_key": {
                "@@assign": "Project",
                "@@operators_allowed_for_child_policies": ["@@none"]
            }
        }
    }
}
```

Kebijakan tag ini mendefinisikan dua kunci tag: `CostCenter` dan `Project`. Melampirkan kebijakan tag ini pada root organisasi memiliki efek berikut:

- Semua akun dalam organisasi Anda akan mewarisi kebijakan tag ini.
- Semua akun dalam organisasi Anda harus menggunakan perlakuan kasus yang ditetapkan untuk kepatuhan. Sumber daya dengan tag `CostCenter` dan `Project` adalah patuh. Sumber daya dengan perlakuan kasus alternatif untuk kunci tag (misalnya, `costcenter`, `Costcenter`, atau `COSTCENTER`) adalah tidak patuh.
- Garis `@@operators_allowed_for_child_policies": ["@@none"]` mengunci kunci tag. Kebijakan tag yang dilampirkan di bagian bawah pohon organisasi (kebijakan anak) tidak dapat menggunakan pengaturan nilai operator untuk mengubah kunci tag, termasuk perlakuan kasus.
- Seperti semua kebijakan tag, Sumber daya atau tag yang tak ditandai yang tidak didefinisikan dalam kebijakan tag tidak akan dievaluasi demi kepatuhan terhadap kebijakan tag.

AWS merekomendasikan bahwa Anda menggunakan contoh ini sebagai panduan dalam menciptakan kebijakan tag yang sama untuk tag kunci yang ingin Anda gunakan. Lampirkan kebijakan tag ke organisasi root. Kemudian buat kebijakan tag yang serupa dengan contoh berikutnya, yang hanya mendefinisikan nilai yang dapat diterima saja untuk kunci tag yang didefinisikan tersebut.

Langkah berikutnya: Tentukan nilai

Asumsikan bahwa Anda melampirkan kebijakan tag sebelumnya ke root organisasi. Selanjutnya, Anda dapat membuat kebijakan tag seperti berikut ini dan melampirkannya pada akun. Kebijakan ini mendefinisikan nilai yang dapat diterima untuk kunci tag `CostCenter` dan `Project`.

Kebijakan B — kebijakan tag akun

```
{
    "tags": {
        "CostCenter": {
            "tag_value": {
                "@@assign": [
                    "Production",
                    "Test"
                ]
            }
        },
        "Project": {
```

```
            "tag_value": {
                "@@assign": [
                    "A",
                    "B"
                ]
            }
        }
    }
}
```

Jika Anda melampirkan kebijakan A ke root organisasi dan kebijakan B pada akun, maka kebijakan tersebut bergabung untuk membuat kebijakan tag efektif berikut ini untuk akun tersebut:

Kebijakan A+Kebijakan B = kebijakan tag efektif untuk akun

```
{
    "tags": {
        "Project": {
            "tag_value": [
                "A",
                "B"
            ],
            "tag_key": "Project"
        },
        "CostCenter": {
            "tag_value": [
                "Production",
                "Test"
            ],
            "tag_key": "CostCenter"
        }
    }
}
```

Untuk informasi lebih lanjut tentang warisan kebijakan, termasuk contoh bagaimana operator warisan bekerja dan contoh kebijakan tag efektif, lihat Memahami warisan kebijakan manajemen.

Contoh 2: Mencegah penggunaan kunci tag

Untuk mencegah penggunaan kunci tag, Anda dapat melampirkan kebijakan tag seperti berikut pada entitas organisasi.

Kebijakan contoh ini menetapkan bahwa tidak ada nilai yang dapat diterima untuk kunci tag `Color`. Hal ini juga menetapkan bahwa tidak ada operator yang diizinkan dalam kebijakan tag anak. Oleh karena itu, setiap tag `Color` pada sumber daya pada akun yang terpengaruh dianggap tidak patuh. Namun, `enforced_for` sebenarnya mencegah akun yang terpengaruh dari penandaan tabel Amazon DynamoDB dengan tag `Color` saja.

```
{
    "tags": {
        "Color": {
            "tag_key": {
                "@@operators_allowed_for_child_policies": [
                    "@@none"
                ],
                "@@assign": "Color"
            },
            "tag_value": {
                "@@operators_allowed_for_child_policies": [
                    "@@none"
                ],
                "@@assign": []
            },
            "enforced_for": {
                "@@assign": [
                    "dynamodb:table"
                ]
            }
        }
    }
}
```

Wilayah yang Didukung

Fitur kebijakan tag tersedia di Wilayah berikut:

Nama wilayah	Parameter wilayah
Wilayah AS Timur (Virginia N.) [1]	**us-east-1**
Wilayah US East (Ohio)	us-east-2
Wilayah US West (N California)	us-west-1

Nama wilayah	Parameter wilayah
Wilayah US West (Oregon)	`us-west-2`
Wilayah Africa (Cape Town)[2]	`af-south-1`
Wilayah Asia Pacific (Hong Kong)[2]	`ap-east-1`
Wilayah Asia Pasifik (Mumbai)	`ap-south-1`
Asia Pasifik (Haiderabad) [2]	`ap-south-2`
Wilayah Asia Pacific (Tokyo)	`ap-northeast-1`
Wilayah Asia Pasifik (Seoul)	`ap-northeast-2`
Wilayah Asia Pasifik (Osaka)	`ap-northeast-3`
Wilayah Asia Pasifik (Singapura)	`ap-southeast-1`
Wilayah Asia Pacific (Sydney)	`ap-southeast-2`
Wilayah Asia Pasifik (Jakarta) [2]	`ap-southeast-3`
Asia Pasifik (Melbourne) [2]	`ap-southeast-4`
Kanada Barat (Calgary) [2]	`ca-west-1`
Wilayah Kanada (Pusat)	`ca-central-1`
Wilayah Eropa (Frankfurt)	`eu-central-1`
Wilayah Eropa (Zurich) [2]	`eu-central-2`
Wilayah Eropa (Milan)	`eu-south-1`
Eropa (Spanyol) [2]	`eu-south-2`
Wilayah Eropa (Irlandia)	`eu-west-1`
Wilayah Eropa (London)	`eu-west-2`

Nama wilayah	Parameter wilayah
Wilayah Eropa (Paris)	`eu-west-3`
Wilayah Eropa (Stockholm)	`eu-north-1`
Wilayah Timur Tengah (UEA) [2]	`me-central-1`
Wilayah Middle East (Bahrain)[2]	`me-south-1`
Wilayah South America (Sao Paulo)	`sa-east-1`
Israel (Tel Aviv) [2]	`il-central-1`

[1]Anda harus menentukan **`us-east-1`** Wilayah saat memanggil operasi Organizations berikut:

- DeletePolicy
- DisablePolicyType
- EnablePolicyType
- Setiap operasi lain pada akar organisasi, seperti ListRoots.

Anda juga harus menentukan **`us-east-1`** Wilayah saat memanggil operasi API Penandaan Resource Groups berikut yang merupakan bagian dari fitur kebijakan tag:

- DescribeReportCreation
- GetComplianceSummary
- GetResources
- StartReportCreation

> **Note**
>
> Untuk mengevaluasi kepatuhan organisasi dengan kebijakan tag, Anda juga harus memiliki akses ke bucket Amazon S3 di Wilayah US East (N. Virginia) untuk penyimpanan laporan. Untuk informasi selengkapnya, lihat kebijakan bucket Amazon S3 untuk penyimpanan laporan di Panduan Pengguna AWS Sumber Daya Penandaan.

[2]Kawasan ini harus diaktifkan secara manual. Untuk mempelajari lebih lanjut tentang mengaktifkan dan menonaktifkan Wilayah AWS, lihat Menentukan Wilayah AWS akun yang dapat digunakan dalam Panduan Referensi ManajemenAWS Akun. Konsol Resource Groups tidak tersedia di Wilayah ini.

Kebijakan Pengendalian Layanan (SCPs)

Kebijakan kontrol layanan (SCP) adalah jenis kebijakan organisasi yang dapat Anda gunakan untuk mengelola izin dalam organisasi Anda. SCP menawarkan kontrol pusat atas izin maksimum yang tersedia untuk pengguna IAM dan peran IAM di organisasi Anda. SCP membantu Anda memastikan akun tetap berada dalam pedoman kontrol akses organisasi Anda. SCP hanya tersedia dalam organisasi yang mengaktifkan semua fitur. SCP tidak tersedia jika organisasi Anda hanya mengaktifkan fitur tagihan terkonsolidasi. Untuk petunjuk tentang cara mengaktifkan SCP, lihat Mengaktifkan dan menonaktifkan jenis kebijakan.

SCP tidak memberikan izin kepada pengguna IAM dan peran IAM di organisasi Anda. Tidak ada izin yang diberikan oleh SCP. SCP mendefinisikan pagar pembatas izin, atau menetapkan batasan, pada tindakan yang dapat dilakukan oleh pengguna IAM dan peran IAM di organisasi Anda. Untuk memberikan izin, administrator harus melampirkan kebijakan untuk mengontrol akses, seperti kebijakan berbasis identitas yang dilampirkan ke pengguna IAM dan peran IAM, serta kebijakan berbasis sumber daya yang dilampirkan ke sumber daya di akun Anda. Izin efektif adalah persimpangan logis antara apa yang diizinkan oleh SCP dan apa yang diizinkan oleh identitas dan kebijakan berbasis sumber daya.

> **Important**
>
> SCP tidak memengaruhi pengguna atau peran dalam akun pengelolaan. SCP tersebut hanya mempengaruhi akun anggota di organisasi Anda.

Topik di halaman ini

- Membuat, memperbarui, dan menghapus kebijakan kontrol layanan
- Melampirkan dan melepaskan kebijakan kontrol layanan
- Evaluasi SCP
- Sintaksis SCP
- Contoh kebijakan kontrol layanan

Pengujian efek SCP

AWS sangat menyarankan agar Anda tidak melampirkan SCP ke akar organisasi Anda tanpa menguji secara menyeluruh dampak kebijakan terhadap akun. Sebaliknya, buat OU yang dapat Anda gunakan sebagai tempat untuk memindahkan akun Anda ke sana satu per satu, atau setidaknya dalam jumlah kecil, untuk memastikan bahwa Anda tidak mengunci pengguna dari layanan utama dengan tidak sengaja. Salah satu cara untuk menentukan apakah layanan digunakan oleh akun adalah dengan memeriksa layanan data terakhir yang diakses di IAM. Cara lain adalah dengan AWS CloudTrail menggunakan log penggunaan layanan di tingkat API.

> **Note**
>
> Anda tidak boleh menghapus AWSAccess kebijakan Lengkap kecuali Anda memodifikasi atau menggantinya dengan kebijakan terpisah dengan tindakan yang diizinkan, jika tidak semua AWS tindakan dari akun anggota akan gagal.

Ukuran maksimum SCP

Semua karakter dalam hitungan SCP Anda terhadap ukuran maksimum-nya. Contoh dalam panduan ini menunjukkan SCP yang diformat dengan spasi kosong ekstra untuk meningkatkan keterbacaannya. Namun, untuk menghemat ruang jika ukuran kebijakan Anda mendekati ukuran maksimum, maka Anda dapat menghapus spasi kosong, seperti spasi karakter dan baris putus yang berada di luar tanda kutip.

> **Tip**
>
> Gunakan editor visual untuk membangun SCP Anda. Ia secara otomatis menghilangkan spasi kosong.

Melampirkan SCP ke berbagai tingkatan dalam organisasi

Untuk penjelasan rinci tentang cara kerja SCP, lihatEvaluasi SCP.

Efek SCP pada izin

SCP mirip dengan kebijakan izin AWS Identity and Access Management (IAM) dan menggunakan sintaks yang hampir sama. Namun, SCP tidak pernah memberikan izin. Sebagai gantinya, SCP adalah kebijakan JSON yang menentukan izin maksimum untuk pengguna IAM dan peran IAM di organisasi Anda. Untuk informasi selengkapnya, lihat: Logika evaluasi Kebijakan di Panduan Pengguna IAM.

- SCP hanya mempengaruhi pengguna dan peran IAM yang dikelola oleh akun yang merupakan bagian dari organisasi. SCP tidak mempengaruhi kebijakan berbasis sumber daya secara langsung. Mereka juga tidak memengaruhi pengguna atau peran dari akun di luar organisasi. Sebagai contoh, pertimbangkan bucket Amazon S3 yang dimiliki oleh akun A dalam sebuah organisasi. Kebijakan bucket (kebijakan berbasis sumber daya) memberikan akses ke pengguna dari akun B di luar organisasi. Akun A memiliki SCP terlampir. SCP itu tidak berlaku untuk pengguna luar di akun B. SCP hanya berlaku untuk pengguna yang dikelola oleh akun A dalam organisasi itu.
- SCP membatasi izin untuk pengguna dan peran IAM dalam akun anggota, termasuk pengguna akun anggota. Setiap akun hanya memiliki izin yang diizinkan oleh setiap induk di atasnya. Jika izin diblokir pada tingkat manapun yang ada di atas akun, baik secara implisit (dengan tidak disertakan dalam pernyataan kebijakan `Allow`) atau secara eksplisit (dengan dimasukkan dalam `Deny`), pengguna atau peran dalam akun yang terpengaruh tidak dapat menggunakan izin tersebut, meskipun administrator akun melampirkan kebijakan IAM `AdministratorAccess` dengan izin */* untuk pengguna.
- SCP tersebut hanya mempengaruhi akun anggota di organisasi. Mereka tidak berpengaruh pada pengguna atau peran dalam akun pengelolaan.
- Pengguna dan peran masih harus diberikan izin dengan kebijakan izin IAM yang sesuai. Pengguna tanpa kebijakan izin IAM tidak memiliki akses, bahkan jika SCP yang berlaku mengizinkan semua layanan dan semua tindakan.
- Jika pengguna atau peran memiliki kebijakan izin IAM yang memberikan akses pada tindakan yang juga diizinkan oleh SCP yang berlaku, maka pengguna atau peran dapat melakukan tindakan tersebut.

- Jika pengguna atau peran memiliki kebijakan izin IAM yang memberikan akses pada tindakan yang tidak diizinkan atau secara eksplisit ditolak oleh SCP yang berlaku, maka pengguna atau peran tidak dapat melakukan tindakan tersebut.
- SCP mempengaruhi semua pengguna dan peran dalam akun terlampir, termasuk pengguna akar. Satu-satunya pengecualian adalah yang diterangkan dalam Tugas dan entitas yang tidak dibatasi oleh SCP.
- SCP tidak mempengaruhi peran terkait layanan. Peran terkait layanan memungkinkan AWS layanan lain untuk diintegrasikan AWS Organizations dan tidak dapat dibatasi oleh SCP.
- Saat Anda menonaktifkan jenis kebijakan SCP di root, semua SCP secara otomatis terlepas dari semua AWS Organizations entitas di root tersebut. AWS Organizations entitas termasuk unit organisasi, organisasi, dan akun. Jika Anda mengaktifkan kembali SCP di sebuah akar, maka akar itu kembali ke kebijakan `FullAWSAccess` default saja yang secara otomatis dilampirkan ke semua entitas di akar. Lampiran SCP apa pun ke entitas AWS Organizations sebelum SCP dinonaktifkan hilang dan tidak dapat dipulihkan secara otomatis, meskipun Anda dapat melampirkannya kembali secara manual.
- Jika batas izin (fitur IAM lanjutan) dan SCP ada, maka batas tersebut, SCP, dan kebijakan berbasis identitas semuanya harus mengizinkan tindakan.

Menggunakan data akses untuk meningkatkan SCP

Saat masuk dengan kredenal akun manajemen, Anda dapat melihat data layanan yang terakhir diakses untuk AWS Organizations entitas atau kebijakan di AWS Organizationsbagian konsol IAM. Anda juga dapat menggunakan AWS Command Line Interface (AWS CLI) atau AWS API di IAM untuk mengambil data layanan yang terakhir diakses. Data ini mencakup informasi tentang layanan yang memungkinkan pengguna IAM dan peran dalam AWS Organizations akun terakhir mencoba untuk mengakses dan kapan. Anda dapat menggunakan informasi ini untuk mengidentifikasi izin yang tidak digunakan sehingga Anda dapat menyempurnakan SCP Anda agar lebih mematuhi prinsip hak istimewa terkecil.

Misalnya, Anda mungkin memiliki daftar penolakan SCP yang melarang akses ke tiga AWS layanan. Semua layanan yang tidak tercantum di pernyataan `Deny` SCP diperbolehkan. Layanan data yang terakhir diakses di IAM memberi tahu Anda AWS layanan mana yang diizinkan oleh SCP tetapi tidak pernah digunakan. Dengan informasi tersebut, Anda dapat memperbarui SCP untuk menolak akses ke layanan yang tidak Anda butuhkan.

Untuk informasi selengkapnya, lihat topik berikut di Panduan Pengguna IAM:

- Melihat Layanan Organizations Data Terakhir yang Diakses untuk Organizations
- Menggunakan Data untuk Memperbaiki Izin untuk Unit Organisasi

Tugas dan entitas yang tidak dibatasi oleh SCP

Anda tidak dapat menggunakan SCP untuk membatasi tugas berikut:

- Setiap tindakan yang dilakukan oleh akun pengelolaan
- Tindakan apa pun yang dilakukan menggunakan izin yang dilampirkan pada peran yang terkait layanan
- Mendaftar untuk paket support Korporasi sebagai pengguna akar
- Ubah level AWS dukungan sebagai pengguna root
- Menyediakan fungsionalitas penandatangan tepercaya untuk konten CloudFront pribadi
- Konfigurasikan DNS terbalik untuk server email Amazon Lightsail dan instans Amazon EC2 sebagai pengguna root
- Tugas pada beberapa layanan AWS terkait:
  - Alexa Top Sites
  - Alexa Web Information Service
  - Amazon Mechanical Turk
  - API Pemasaran Produk Amazon

Membuat, memperbarui, dan menghapus kebijakan kontrol layanan

Saat masuk ke akun pengelolaan organisasi Anda, Anda dapat membuat dan memperbarui kebijakan kontrol layanan (SCP). Anda membuat SCP dengan membangun pernyataan yang menolak atau mengizinkan akses ke layanan dan tindakan yang Anda tentukan.

Konfigurasi default untuk bekerja dengan SCP adalah dengan menggunakan strategi "daftar blok" di mana semua tindakan secara implisit diperbolehkan kecuali untuk tindakan yang Anda ingin blokir dengan membuat pernyataan yang menolak akses. Dengan pernyataan Deny, Anda dapat menentukan sumber daya dan syarat untuk pernyataan dan menggunakan NotActionelemen. Untuk pernyataan izinkan, Anda dapat menentukan layanan dan tindakan saja. Untuk informasi selengkapnya tentang pernyataan yang menolak akses dan mengizinkan akses, lihat Evaluasi SCP.

> **Tip**
>
> Anda dapat menggunakan data layanan terakhir diakses di IAM sebagai titik data untuk memperbarui SCP Anda untuk membatasi akses hanya ke layanan AWS yang Anda butuhkan. Untuk informasi selengkapnya, lihat: Melihat Data Layanan Organizations Terakhir Diakses untuk Organizations di Panduan Pengguna IAM.

Dalam topik ini:

- Setelah Anda mengaktifkan kebijakan kontrol layanan untuk organisasi Anda, Anda dapat memuat kebijakan.
- Bila persyaratan SCP berubah, Anda dapat memperbarui kebijakan yang ada.
- Bila Anda tidak lagi memerlukan kebijakan dan setelah melepaskannya dari semua unit organisasi (OU) dan akunmaka , Anda dapat menghapusnya.

Membuat SCP

> **Izin minimum**
>
> Untuk membuat SCP, Anda memerlukan izin untuk menjalankan tindakan berikut:
>
> - `organizations:CreatePolicy`

AWS Management Console

Untuk membuat kebijakan kontrol layanan

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Kebijakan kontrol layanan, pilih Buat kebijakan.
3. Pada halaman halaman Membuat kebijakan kontrol layanan baru, masukkan Nama kebijakan dan Deskripsi kebijakan opsional.
4. (Opsional) Tambahkan satu tag atau lebih dengan memilih Tambahkan tag dan kemudian masukkan kunci dan nilai opsional. Membiarkan nilai kosong akan mengaturnya menjadi

string kosong; itu bukan `null`. Anda dapat melampirkan hingga 50 tag ke kebijakan. Untuk informasi lebih lanjut, lihat Penandaan pada sumber daya AWS Organizations.

> **Note**
>
> Dalam sebagian besar langkah-langkah yang mengikuti, kita membahas penggunaan kontrol di sisi kanan editor JSON untuk membangun kebijakan, elemen demi elemen. Atau, Anda dapat, kapan saja, cukup memasukkan teks di editor JSON yang ada di sisi kiri jendela. Anda dapat langsung mengetik, atau menggunakan salin dan tempel.

5. Untuk membangun kebijakan, langkah berikutnya berbeda-beda tergantung pada apakah Anda ingin menambahkan pernyataan yang menolak atau memungkinkan akses. Untuk informasi selengkapnya, lihat Evaluasi SCP. Jika Anda menggunakan `Deny` pernyataan, Anda memiliki kontrol tambahan karena Anda dapat membatasi akses ke sumber daya tertentu, menentukan syarat untuk kapan SCP berlaku, dan menggunakan elemen. NotAction Untuk detail tentang sintaksis, lihat Sintaksis SCP.

   Untuk menambahkan pernyataan yang menolak akses:

   a. Di sebelah kanan Edit panel pernyataan editor, di bawah Tambahkan tindakan, pilih AWS layanan.

      Ketika Anda memilih opsi yang ada di sebelah kanan, editor JSON diperbarui untuk menampilkan kebijakan JSON yang sesuai di sebelah kiri.

   b. Setelah Anda memilih layanan, daftar yang berisi tindakan yang tersedia untuk layanan tersebut akan terbuka. Anda dapat memilih Semua tindakan, atau pilih satu atau beberapa tindakan individual yang ingin Anda tolak.

      JSON di sebelah kiri memperbarui untuk menyertakan tindakan yang Anda pilih.

      > **Note**
      >
      > Jika Anda memilih tindakan individu dan kemudian juga kembali dan juga memilih Semua tindakan, maka entri yang diharapkan untuk *`servicename`*`/*` ditambahkan ke JSON, tetapi tindakan individu yang sebelumnya Anda pilih dibiarkan di JSON dan tidak dihapus.

c. Jika ingin menambahkan tindakan dari layanan tambahan, Anda dapat memilih Semua layanan di bagian atas kotak Pernyataan, dan kemudian ulangi dua langkah sebelumnya sesuai kebutuhan.

d. Tentukan sumber daya untuk menyertakan dalam pernyataan.

- Di samping Tambahkan sumber daya, pilih Tambah.
- Di Menambahkan sumber daya, pilih layanan yang sumber daya-nya ingin Anda kontrol dari daftar. Anda dapat memilih hanya dari antara layanan-layanan yang Anda pilih pada langkah sebelumnya.
- Di bawah Jenis sumber daya, pilih jenis sumber daya yang ingin Anda kontrol.
- Akhirnya, selesaikan Amazon Resource Name (ARN) di Sumber Daya ARN untuk mengidentifikasi sumber daya tertentu yang Anda inginkan untuk mengontrol akses. Anda harus mengganti semua placeholder yang dikelilingi oleh kurung kurawal `{}`. Anda dapat menentukan kartu liar (*) di mana sintaksis ARN jenis sumber daya tersebut diizinkan. Lihat dokumentasi untuk jenis sumber daya tertentu untuk informasi tentang di mana Anda dapat menggunakan kartu liar.
- Simpan penambahan Anda ke kebijakan dengan memilih Menambahkan sumber daya. Elemen `Resource` dalam JSON mencerminkan penambahan atau perubahan. Elemen Sumber Daya wajib diisi.

> **Tip**
>
> Jika Anda ingin menentukan semua sumber daya untuk layanan yang dipilih, pilih opsi Semua sumber daya dalam daftar, atau edit pernyataan `Resource` secara langsung di JSON untuk membaca `"Resource":"*"`.

e. (Opsional) Untuk menentukan syarat yang membatasi kapan pernyataan kebijakan berlaku, di samping Tambahkan syarat, pilih Tambah.

- Kunci syarat — Dari daftar Anda dapat memilih kunci syarat yang tersedia untuk semua layanan AWS (misalnya, `aws:SourceIp`) atau kunci khusus layanan untuk hanya salah satu layanan yang Anda pilih untuk pernyataan ini.
- Pengualifikasi — (Opsional) Jika Anda memberikan beberapa nilai untuk syarat (tergantung pada kunci syarat yang ditentukan), Anda dapat menentukan kualifikasi untuk menguji permintaan terhadap nilai-nilai.

- Default — Menguji nilai tunggal dalam permintaan terhadap nilai kunci syarat dalam kebijakan. Syarat tersebut akan memberikan hasil BETUL jika setiap nilai kunci dalam permintaan tersebut sesuai dengan setidaknya satu nilai dalam kebijakan. Jika kebijakan menentukan lebih dari satu nilai maka mereka diperlakukan sebagai uji "atau", dan syarat akan memberikan hasil BETUL jika nilai permintaan cocok dengan salah satu nilai kebijakan.
- Untuk setiap nilai dalam permintaan — Ketika permintaan dapat memiliki beberapa nilai, opsi ini menguji apakah paling tidak satu nilai permintaan sesuai dengan setidaknya satu nilai kunci syarat dalam kebijakan. Syarat memberikan hasil BETUL jika salah satu nilai kunci dalam permintaan sesuai dengan salah satu nilai syarat dalam kebijakan. Jika tidak ada kunci yang cocok atau kumpulan data nol, kondisi akan memberikan hasil salah.
- Untuk setiap nilai dalam permintaan — Ketika permintaan dapat memiliki beberapa nilai, opsi ini menguji apakah setiap nilai permintaan sesuai dengan setidaknya satu nilai kunci syarat dalam kebijakan. Syarat tersebut akan memberikan hasil benar jika setiap nilai kunci dalam permintaan tersebut sesuai dengan setidaknya satu nilai dalam kebijakan. Syarat ini juga akan memberikan hasil benar jika tidak ada kunci dalam permintaan, atau jika nilai kunci menghasilkan kumpulan data nol, seperti string kosong.

- Operator — Operator menentukan jenis perbandingan yang akan dibuat. Pilihan yang disajikan tergantung pada jenis data kunci syarat. Misalnya, kunci syarat global `aws:CurrentTime` memungkinkan Anda memilih dari salah satu operator perbandingan tanggal, atau `Null`, yang dapat Anda gunakan untuk menguji apakah nilai hadir dalam permintaan.

  Untuk operator syarat apa pun kecuali `Null` tes, Anda dapat memilih IfExistsopsi.
- Nilai — (Opsional) Tentukan satu atau beberapa nilai yang ingin Anda uji permintaannya.

Pilih Tambahkan syarat.

Untuk informasi selengkapnya tentang kunci syarat, lihat Elemen Kebijakan IAM JSON: Syarat di Panduan Pengguna IAM.

f. (Opsional) Untuk menggunakan elemen `NotAction` untuk menolak akses ke semua tindakan kecuali yang ditentukan, ganti `Action` di panel kiri dengan `NotAction`, hanya

setelah elemen `"Effect": "Deny",`. Untuk informasi selengkapnya, lihat Elemen Kebijakan IAM: NotAction di Panduan Pengguna IAM.

6. Untuk menambahkan pernyataan yang mengizinkan akses:

   a. Dalam editor JSON di sebelah kiri, ubah baris `"Effect": "Deny"` ke `"Effect": "Allow"`.

      Ketika Anda memilih opsi yang ada di sebelah kanan, editor JSON diperbarui untuk menampilkan kebijakan JSON yang sesuai di sebelah kiri.

   b. Setelah Anda memilih layanan, daftar yang berisi tindakan yang tersedia untuk layanan tersebut akan terbuka. Anda dapat memilih Semua tindakan, atau pilih satu atau beberapa tindakan individual yang ingin Anda izinkan.

      JSON di sebelah kiri memperbarui untuk menyertakan tindakan yang Anda pilih.

      > **Note**
      >
      > Jika Anda memilih tindakan individu dan kemudian juga kembali dan juga memilih Semua tindakan, maka entri yang diharapkan untuk *servicename*`:*` ditambahkan ke JSON, tetapi tindakan individu yang sebelumnya Anda pilih dibiarkan di JSON dan tidak dihapus.

   c. Jika ingin menambahkan tindakan dari layanan tambahan, Anda dapat memilih Semua layanan di bagian atas kotak Pernyataan, dan kemudian ulangi dua langkah sebelumnya sesuai kebutuhan.

7. (Opsional) Untuk menambahkan pernyataan lain pada kebijakan, pilih Menambahkan pernyataan dan gunakan editor visual untuk membuat pernyataan berikutnya.

8. Setelah selesai menambahkan pernyataan, pilih Buat kebijakan untuk menyimpan SCP yang telah selesai.

SCP baru Anda muncul dalam daftar kebijakan organisasi. Sekarang Anda dapat melampirkan SCP Anda ke akar, OU, atau akun.

AWS CLI & AWS SDKs

Untuk membuat kebijakan kontrol layanan

Anda dapat menggunakan salah satu perintah berikut untuk membuat SCP:

- AWS CLI: create-policy

  Contoh berikut mengasumsikan bahwa Anda memiliki sebuah file bernama `Deny-IAM.json` dengan teks kebijakan JSON di dalamnya. Ia menggunakan file tersebut untuk membuat kebijakan kontrol layanan baru.

```
$ aws organizations create-policy \
    --content file://Deny-IAM.json \
    --description "Deny all IAM actions" \
    --name DenyIAMSCP \
    --type SERVICE_CONTROL_POLICY
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "DenyIAMSCP",
            "Description": "Deny all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
         "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

- AWSSDK: CreatePolicy

> **Note**
>
> SCP tidak berlaku pada akun pengelolaan dan dalam beberapa situasi lainnya. Untuk informasi lebih lanjut, lihat Tugas dan entitas yang tidak dibatasi oleh SCP.

Memperbarui SCP

Bila Anda masuk ke akun pengelolaan organisasi Anda, Anda dapat mengganti nama atau mengubah konten kebijakan. Mengubah konten SCP akan langsung mempengaruhi setiap pengguna, grup, dan peran dalam semua akun terlampir.

Izin minimum

Untuk memperbarui SCP, Anda memerlukan izin untuk menjalankan tindakan-tindakan berikut:

- `organizations:UpdatePolicy` dengan elemen `Resource` dalam pernyataan kebijakan yang sama yang mencakup ARN dari kebijakan yang ditentukan (atau "*")
- `organizations:DescribePolicy` dengan elemen `Resource` dalam pernyataan kebijakan yang sama yang mencakup ARN dari kebijakan yang ditentukan (atau "*")

AWS Management Console

Untuk memperbarui kebijakan

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Kebijakan kontrol layanan, pilih nama kebijakan yang ingin Anda perbarui.
3. Pada halaman detail kebijakan, pilih Edit kebijakan.
4. Membuat salah satu atau semua perubahan berikut:
   - Anda dapat mengubah nama kebijakan dengan memasukkan nama baru di Nama kebijakan.
   - Anda dapat mengubah deskripsi dengan memasukkan teks baru di Deskripsi kebijakan.
   - Anda dapat mengedit teks kebijakan dengan mengedit kebijakan dalam format JSON yang ada di panel kiri. Atau, Anda dapat memilih pernyataan di editor di sebelah kanan, dan juga mengubah elemennya dengan menggunakan kontrol. Untuk detail selengkapnya tentang setiap kontrol, lihat bagian Membuat prosedur SCP sebelumnya dalam topik ini.
5. Setelah Anda selesai, pilih Simpan perubahan.

AWS CLI & AWS SDKs

Untuk memperbarui kebijakan

Anda dapat menggunakan salah satu perintah berikut untuk memperbarui kebijakan:

- AWS CLI: update-policy

  Contoh berikut mengganti nama kebijakan.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --name "MyRenamedPolicy"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "Blocks all IAM actions",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
}
```

  Contoh berikut menambahkan atau mengubah deskripsi untuk kebijakan tag.

```
$ aws organizations update-policy \
    --policy-id p-i9j8k7l6m5 \
    --description "My new policy description"
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"Statement1\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*\"]}]}"
    }
```

```
}
```

Contoh berikut mengubah dokumen kebijakan SCP dengan menentukan file yang berisi teks kebijakan JSON baru.

```
$ aws organizations update-policy \
    --policy-id p-zlfw1r64
    --content file://MyNewPolicyText.json
{
    "Policy": {
        "PolicySummary": {
            "Id": "p-i9j8k7l6m5",
            "Arn": "arn:aws:organizations::123456789012:policy/o-aa111bb222/
service_control_policy/p-i9j8k7l6m5",
            "Name": "MyRenamedPolicy",
            "Description": "My new policy description",
            "Type": "SERVICE_CONTROL_POLICY",
            "AwsManaged": false
        },
        "Content": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Sid\":
\"AModifiedPolicy\",\"Effect\":\"Deny\",\"Action\":[\"iam:*\"],\"Resource\":[\"*
\"]}]}"
    }
}
```

- AWSSDK: UpdatePolicy

Untuk informasi selengkapnya

Untuk informasi lebih lanjut tentang membuat SCP, lihat topik berikut:

- Contoh kebijakan kontrol layanan
- Sintaksis SCP

Mengedit tag yang dilampirkan ke SCP

Bila Anda masuk ke akun pengelolaan organisasi Anda, Anda dapat menambahkan atau menghapus tag yang dilampirkan ke SCP. Untuk informasi lebih lanjut tentang penandaan, lihat Penandaan pada sumber daya AWS Organizations.

Izin minimum

Untuk mengedit tag yang dilampirkan ke SCP di perangkat organisasi AWS Anda, Anda harus memiliki izin berikut:

- `organizations:DescribeOrganization` — hanya diperlukan bila menggunakan konsol Organizations
- `organizations:DescribePolicy` — hanya diperlukan bila menggunakan konsol Organizations
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

Untuk mengedit tag yang dilampirkan ke SCP

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Kebijakan kontrol layanan, pilih nama kebijakan dengan tag yang ingin Anda edit.
3. Pada halaman detail kebijakan, pilih tag Tag, dan kemudian pilihKelola tag.
4. Membuat salah satu atau semua perubahan berikut:
   - Ubah nilai tag dengan memasukkan nilai baru mengganti yang lama. Anda tidak dapat mengubah kunci tag secara langsung. Untuk mengubah kunci, Anda harus menghapus tag dengan kunci yang lama dan kemudian menambahkan tag dengan kunci yang baru.
   - Hapus tag yang ada dengan memilih Hapus.
   - Tambahkan kunci tag dan pasangan nilai baru. Pilih Tambahkan tag, lalu masukkan nama kunci baru dan nilai opsional dalam kotak yang disediakan. Jika Anda membiarkan kotak Nilai kosong, nilai-nya adalah string kosong; itu bukan `null`.
5. Setelah Anda selesai, pilih Simpan perubahan.

AWS CLI & AWS SDKs

Untuk mengedit tag yang dilampirkan ke SCP

Anda dapat menggunakan salah satu perintah berikut untuk mengedit tag yang dilampirkan pada SCP:

- AWS CLI: tag-resource dan untag-resource
- AWSSDK: TagResourcedan UntagResource

Menghapus SCP

Saat masuk ke akun pengelolaan organisasi, Anda dapat menghapus kebijakan yang tidak diperlukan lagi di organisasi.

> **Catatan**
>
> - Sebelum Anda dapat menghapus kebijakan, Anda harus melepasnya terlebih dahulu dari semua entitas terlampir.
> - Anda tidak dapat menghapus SCP terkelola AWS seperti SCP bernama `FullAWSAccess`.

> **Izin minimum**
>
> Untuk menghapus SCP, Anda memerlukan izin untuk menjalankan tindakan berikut:
>
> - `organizations:DeletePolicy`

AWS Management Console

Untuk menghapus SCP

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Kebijakan kontrol layanan, pilih nama SCP yang ingin Anda hapus.

3. Anda harus melepaskan kebijakan yang ingin Anda hapus dari semua root, OU, dan akun. Pilih tab Target, pilih tombol radio yang ada di samping setiap root, OU, atau akun yang ditampilkan di daftar Target, dan kemudian pilih Lepaskan. Dalam kotak dialog konfirmasi, pilih Lepaskan. Ulangi sampai Anda menghapus semua target.
4. Pilih Hapus di bagian atas halaman.
5. Pada kotak dialog konfirmasi, masukkan nama kebijakan, dan kemudian pilih Hapus.

AWS CLI & AWS SDKs

Untuk menghapus SCP

Anda dapat menggunakan salah satu perintah berikut untuk menghapus kebijakan:

- AWS CLI: delete-policy

  Contoh berikut menghapus SCP yang ditentukan.

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWSSDK: DeletePolicy

Melampirkan dan melepaskan kebijakan kontrol layanan

Saat masuk ke akun pengelolaan organisasi, Anda dapat melampirkan kebijakan kontrol layanan (SCP) yang sebelumnya Anda buat. Anda dapat melampirkan SCP ke akar organisasi, untuk unit organisasi (OU), atau langsung ke akun. Untuk melampirkan SCP, selesaikan langkah-langkah berikut.

> **Izin minimum**
>
> Untuk melampirkan SCP ke akar, OU, atau akun, Anda memerlukan izin untuk menjalankan tindakan-tindakan berikut:

- `organizations:AttachPolicy` dengan elemen `Resource` dalam pernyataan kebijakan yang sama yang menyertakan "*" atau Amazon Resource Name (ARN) dari kebijakan tertentu dan ARN akar, OU, atau akun yang ingin Anda lampiri kebijakan

AWS Management Console

Anda dapat melampirkan SCP dengan menavigasi ke kebijakan atau akar, OU, atau akun yang Anda ingin lampiri dengan kebijakan.

Untuk melampirkan SCP dengan menavigasi ke akar, OU, atau akun

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Akun AWS, buka dan pilih kotak centang di samping akar, OU, atau akun yang ingin Anda lampiri SCP. Anda mungkin harus memperluas OU (pilih ▶) untuk menemukan OU atau akun yang Anda inginkan.
3. Di tab Kebijakan, dalam entri untuk Kebijakan kontrol layanan, pilih Lampirkan.
4. Temukan kebijakan yang Anda inginkan dan pilih Lampirkan kebijakan.

   Daftar SCP terlampir pada tab Kebijakan sudah diperbarui dan mencakup tambahan baru. Perubahan kebijakan akan langsung berlaku, mempengaruhi izin IAM pengguna dan peran dalam akun terlampir atau semua akun di bawah akar terlampir atau OU.

Untuk melampirkan SCP dengan menavigasi ke kebijakan

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Kebijakan kontrol layanan, pilih nama kebijakan yang ingin Anda lampirkan.
3. Di tab Target, pilih Lampirkan.
4. Pilih tombol radio yang ada di samping root, OU, atau akun yang ingin Anda lampirkan kebijakan padanya. Anda mungkin harus memperluas OU (pilih

untuk menemukan OU atau akun yang Anda inginkan.

5. Pilih Pasang kebijakan.

   Daftar SCP terlampir pada tab Target sudah diperbarui dan mencakup tambahan baru. Perubahan kebijakan akan langsung berlaku, mempengaruhi izin IAM pengguna dan peran dalam akun terlampir atau semua akun di bawah akar terlampir atau OU.

AWS CLI & AWS SDKs

Untuk melampirkan SCP dengan menavigasi ke akar, OU, atau akun

Anda dapat menggunakan salah satu perintah berikut untuk melampirkan SCP:

- AWS CLI: attach-policy

  Contoh berikut melampirkan SCP ke OU.

```
$ aws organizations attach-policy \
    --policy-id p-i9j8k7l6m5 \
    --target-id ou-a1b2-f6g7h222
```

  Perintah ini tidak menghasilkan output saat berhasil.

- AWS SDK: AttachPolicy

Perubahan kebijakan akan langsung berlaku, mempengaruhi izin IAM pengguna dan peran dalam akun terlampir atau semua akun di bawah akar terlampir atau OU.

Melepaskan SCP dari akar organisasi, OU, atau akun

Ketika Anda masuk ke akun pengelolaan organisasi Anda, Anda dapat melepaskan SCP dari akar organisasi, OU, atau akun yang melampirkannya. Setelah Anda melepaskan SCP dari entitas, SCP tersebut tidak lagi berlaku untuk pengguna IAM dan peran IAM mana pun yang terpengaruh oleh entitas yang sekarang terpisah. Untuk melepaskan SCP, selesaikan langkah-langkah berikut.

> **Note**
>
> Anda tidak dapat melepaskan SCP terakhir dari akar, OU, atau akun. Harus ada setidaknya satu SCP yang dilampirkan pada setiap akar, OU, dan akun setiap saat.

> **Izin minimum**
>
> Untuk melepaskan SCP dari akar, OU, atau akun, Anda memerlukan izin untuk menjalankan tindakan-tindakan berikut:
>
> - `organizations:DetachPolicy`

AWS Management Console

Anda dapat melepaskan SCP dengan menavigasi ke kebijakan atau ke root, OU, atau akun yang ingin Anda lepaskan dari kebijakan tersebut.

Untuk melepaskan SCP dengan menavigasi ke akar, OU, atau akun yang dilampiri SCP

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Akun AWS navigasi ke akar, OU, atau akun yang ingin Anda lepaskan kebijakan darinya. Anda mungkin harus memperluas OU (pilih ▸) untuk menemukan OU atau akun yang Anda inginkan. Pilih nama Root, OU, atau akun.
3. Pada tab Kebijakan, pilih tombol radio di samping SCP yang ingin Anda lepaskan, kemudian pilih Lepaskan.
4. Dalam kotak dialog konfirmasi, pilih Lepaskan kebijakan.

   Daftar SCP yang dilampirkan sudah diperbarui. Perubahan kebijakan yang disebabkan oleh pelepasan SCP langsung berlaku. Sebagai contoh, memisahkan SCP akan langsung mempengaruhi izin pengguna dan peran IAM dalam akun yang sebelumnya dilampiri SCP atau akun di bawah akar organisasi atau OU yang sebelumnya dilampiri SCP.

Untuk melepaskan SCP dengan menavigasi ke kebijakan

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Kebijakan kontrol layanan, pilih nama kebijakan yang ingin Anda lepaskan dari akar, OU, atau akun.
3. Pada tab Target, pilih tombol radio yang ada di sebelah root, OU, atau akun yang ingin Anda lepaskan kebijakan darinya. Anda mungkin harus memperluas OU (pilih ▶) untuk menemukan OU atau akun yang Anda inginkan.
4. Pilih Lepaskan.
5. Dalam kotak dialog konfirmasi, pilih Lepaskan.

   Daftar SCP yang dilampirkan sudah diperbarui. Perubahan kebijakan yang disebabkan oleh pelepasan SCP langsung berlaku. Sebagai contoh, memisahkan SCP akan langsung mempengaruhi izin pengguna dan peran IAM dalam akun yang sebelumnya dilampiri SCP atau akun di bawah akar organisasi atau OU yang sebelumnya dilampiri SCP.

AWS CLI & AWS SDKs

Untuk melepaskan SCP dari akar, OU, atau akun

Anda dapat menggunakan salah satu perintah berikut untuk melepaskan SCP:

- AWS CLI: detach-policy

  Contoh berikut melepaskan SCP yang ditentukan dari OU ditentukan.

```
$ aws organizations detach-policy \
    --policy-id p-i9j8k7l6m5 \
    --target-id ou-a1b2-f6g7h222
```

- AWS SDK: DetachPolicy

Perubahan kebijakan akan langsung berlaku, mempengaruhi izin IAM pengguna dan peran dalam akun terlampir atau semua akun di bawah akar terlampir atau OU

Evaluasi SCP

> **Note**
>
> Informasi di bagian ini tidak berlaku untuk jenis kebijakan pengelolaan, termasuk kebijakan penolakan layanan AI, kebijakan backup, atau kebijakan tag. Untuk informasi selengkapnya, lihat Memahami warisan kebijakan manajemen.

Karena Anda dapat melampirkan beberapa kebijakan kontrol layanan (SCP) pada tingkat yang berbedaAWS Organizations, memahami bagaimana SCP dievaluasi dapat membantu Anda menulis SCP yang menghasilkan hasil yang tepat.

Topik

- Bagaimana SCP bekerja dengan Izinkan
- Bagaimana SCP bekerja dengan Deny
- Strategi untuk menggunakan SCP

Bagaimana SCP bekerja dengan Izinkan

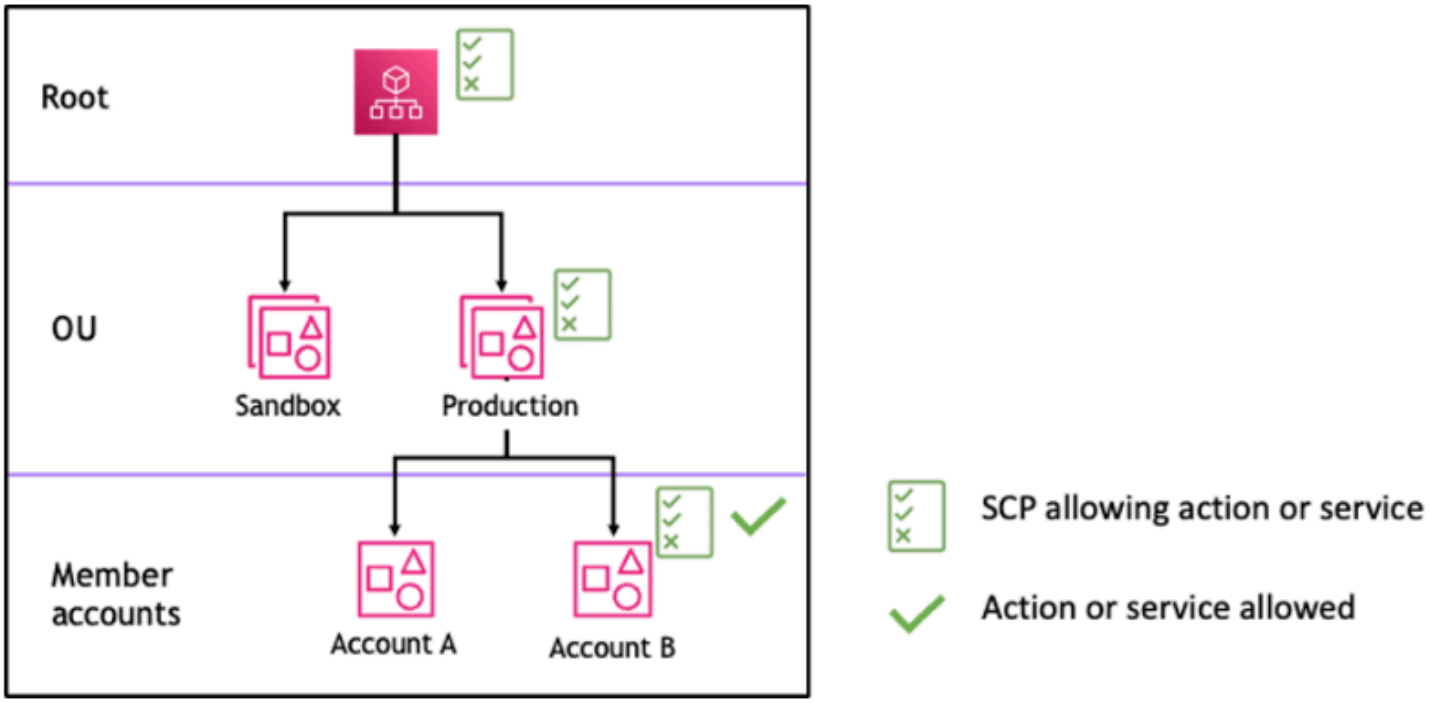
Agar izin diizinkan untuk akun tertentu, harus ada **`Allow`**pernyataan eksplisit di setiap tingkat dari root melalui setiap OU di jalur langsung ke akun (termasuk akun target itu sendiri). Inilah sebabnya mengapa ketika Anda mengaktifkan SCP, AWS Organizations melampirkan kebijakan SCP AWS terkelola bernama Full AWSAccess yang memungkinkan semua layanan dan tindakan. Jika kebijakan ini dihapus dan tidak diganti di tingkat organisasi mana pun, semua OU dan akun di bawah tingkat itu akan diblokir untuk mengambil tindakan apa pun.

Sebagai contoh, mari kita telusuri skenario yang ditunjukkan pada gambar 1 dan 2. Agar izin atau layanan diizinkan di Akun B, SCP yang mengizinkan izin atau layanan harus dilampirkan ke Root, OU Produksi, dan Akun B itu sendiri.

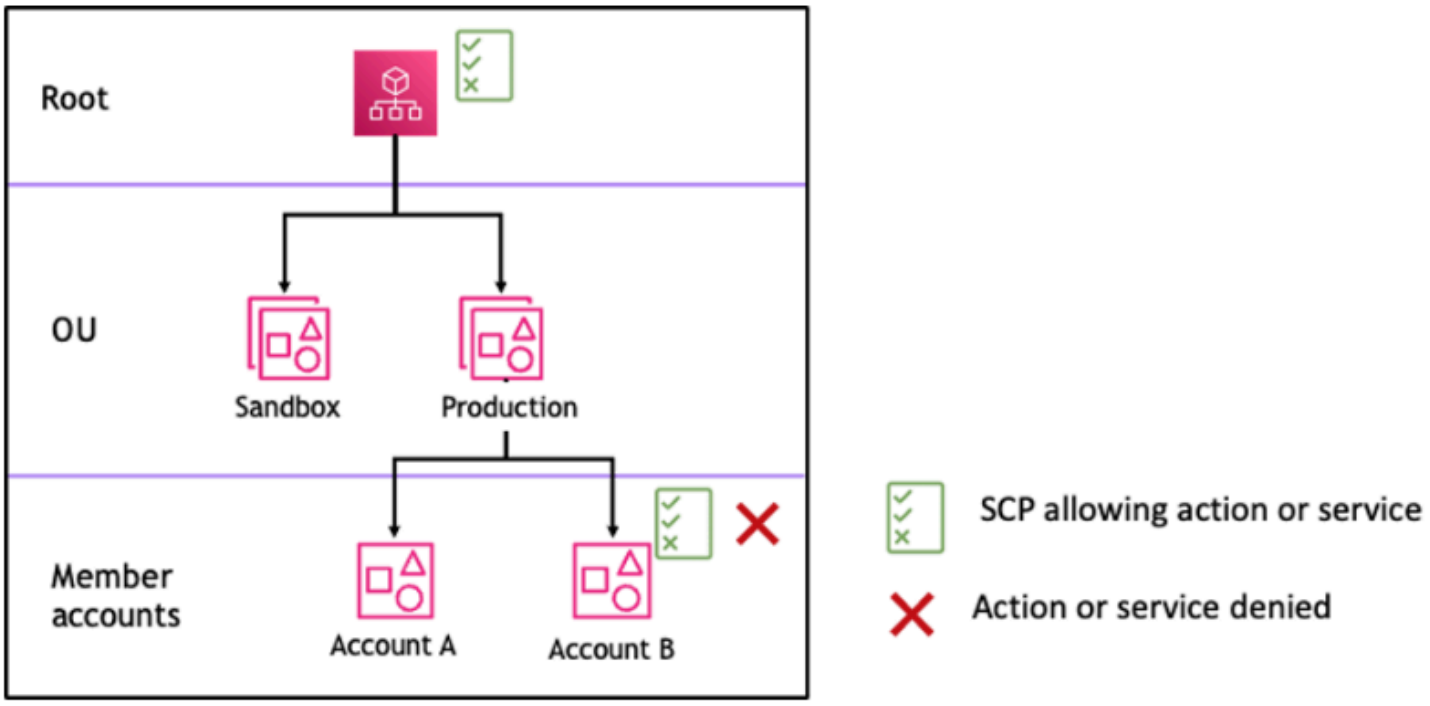
Evaluasi SCP mengikuti deny-by-default model, yang berarti bahwa izin apa pun yang tidak diizinkan secara eksplisit di SCP ditolak. Jika pernyataan izin tidak ada di SCP di salah satu tingkat seperti Root, Produksi OU atau Akun B, akses ditolak.

Catatan

- `Allow`Pernyataan dalam SCP memungkinkan `Resource` elemen untuk hanya memiliki entri. `"*"`
- Sebuah pernyataan `Allow` di SCP tidak dapat memiliki `Condition` elemen sama sekali.



Gambar 1: Contoh struktur organisasi dengan *`Allow`* pernyataan terlampir di Root, Production OU dan Account B

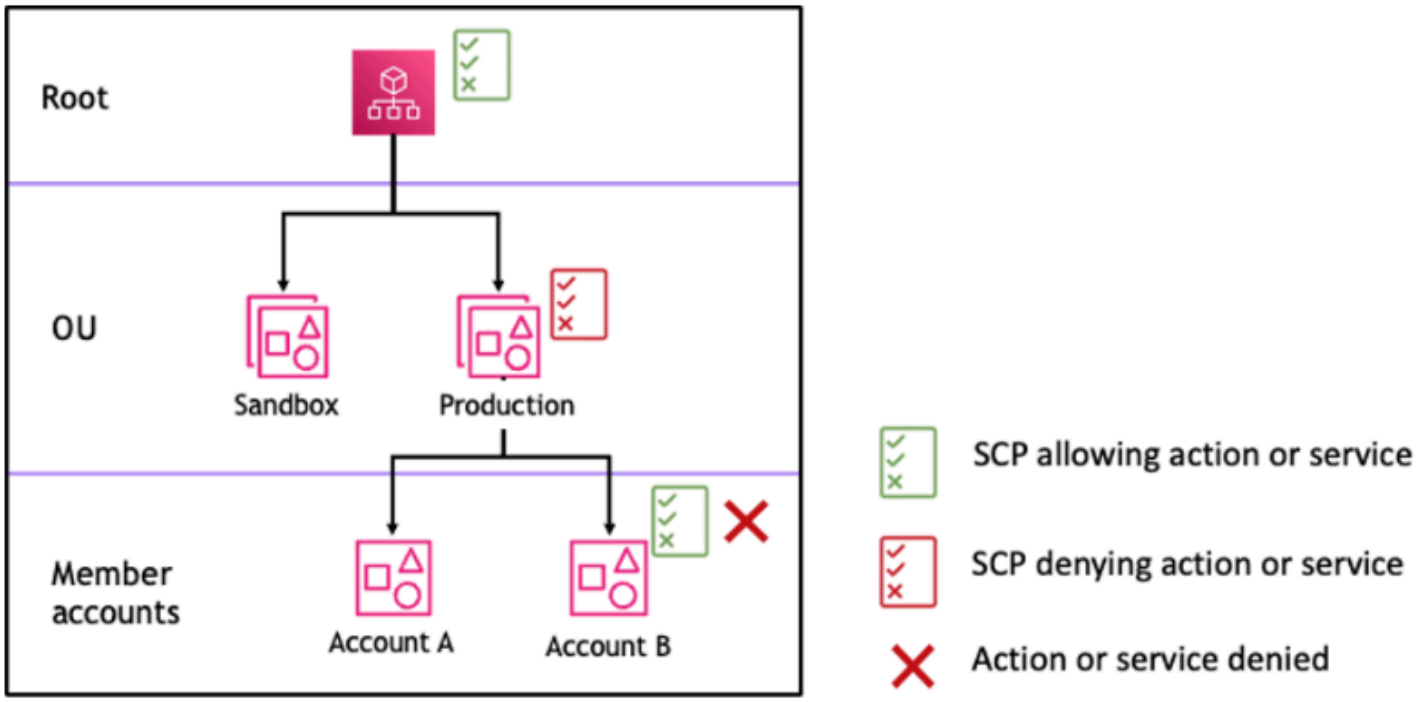


Gambar 2: Contoh struktur organisasi dengan *`Allow`* pernyataan yang hilang di Produksi OU dan dampaknya pada Akun B

Bagaimana SCP bekerja dengan Deny

Agar izin ditolak untuk akun tertentu, SCP apa pun dari root melalui setiap OU di jalur langsung ke akun (termasuk akun target itu sendiri) dapat menolak izin itu.

Sebagai contoh, katakanlah ada SCP yang melekat pada OU Produksi yang memiliki `Deny` pernyataan eksplisit yang ditentukan untuk layanan tertentu. Ada juga SCP lain yang dilampirkan ke Root dan Akun B yang secara eksplisit memungkinkan akses ke layanan yang sama, seperti yang ditunjukkan pada Gambar 3. Akibatnya, baik Akun A dan Akun B akan ditolak aksesnya ke layanan karena kebijakan penolakan yang dilampirkan pada tingkat mana pun dalam organisasi dievaluasi untuk semua OU dan akun anggota di bawahnya.



Gambar 3: Contoh struktur organisasi dengan *Deny* pernyataan terlampir di Produksi OU dan dampaknya pada Akun B

Strategi untuk menggunakan SCP

Saat menulis SCP, Anda dapat menggunakan kombinasi `Allow` dan `Deny` pernyataan untuk memungkinkan tindakan dan layanan yang dimaksudkan di organisasi Anda. `Deny`pernyataan adalah cara yang ampuh untuk menerapkan pembatasan yang seharusnya benar untuk bagian yang lebih luas dari organisasi atau OU Anda karena ketika mereka diterapkan di root atau tingkat OU mereka mempengaruhi semua akun di bawahnya.

Misalnya, Anda dapat menerapkan kebijakan menggunakan ke [Mencegah akun anggota keluar dari organisasi](#) tingkat root, yang akan efektif untuk semua akun di organisasi. Pernyataan tolak juga mendukung elemen kondisi yang dapat membantu untuk membuat pengecualian.

> **Tip**
>
> Anda dapat menggunakan [Data layanan terakhir diakses](#) di [IAM](#) untuk memperbarui SCP Anda untuk membatasi akses hanya ke layanan AWS yang Anda butuhkan. Untuk informasi selengkapnya, lihat: [Melihat Data Layanan Organizations Terakhir Diakses untuk Organizations](#) di Panduan Pengguna IAM.

AWS Organizationsmelampirkan SCP AWS terkelola bernama Full AWSAccess ke setiap root, OU, dan akun saat dibuat. Kebijakan ini mengizinkan semua layanan dan tindakan. Anda dapat mengganti Full AWSAccess dengan kebijakan yang hanya mengizinkan satu set layanan sehingga AWS layanan baru tidak diizinkan kecuali secara eksplisit diizinkan dengan memperbarui SCP. Misalnya, jika organisasi Anda hanya ingin mengizinkan penggunaan subset layanan di lingkungan Anda, Anda dapat menggunakan `Allow` pernyataan untuk hanya mengizinkan layanan tertentu.

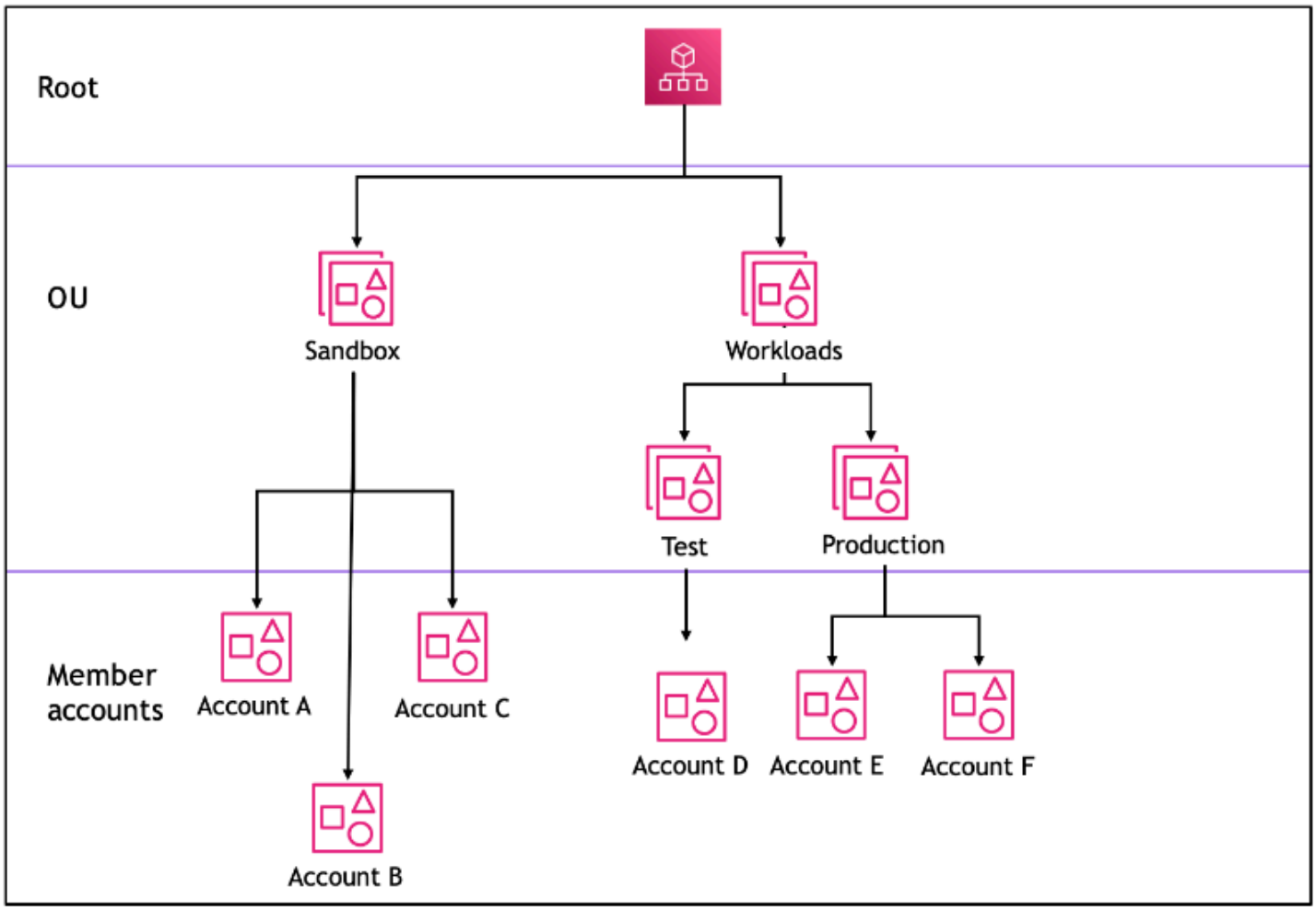
```
{
"Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
        }
    ]
}
```

Kebijakan yang menggabungkan dua pernyataan mungkin terlihat seperti contoh berikut, yang mencegah akun anggota meninggalkan organisasi dan memungkinkan penggunaan AWS layanan yang diinginkan. Administrator organisasi dapat melepaskan kebijakan Lengkap dan melampirkan AWSAccess kebijakan ini sebagai gantinya.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
```

```
            "Action":"organizations:LeaveOrganization",
            "Resource": "*"
        }
    ]
}
```

Sekarang, pertimbangkan contoh struktur organisasi berikut untuk memahami bagaimana Anda dapat menerapkan beberapa SCP pada tingkat yang berbeda dalam suatu organisasi.



Tabel berikut menunjukkan kebijakan efektif di Sandbox OU.

Skenario	SCP di Root	SCP di Sandbox OU	SCP di Akun A	Kebijakan yang dihasilkan di Akun A	Kebijakan yang dihasilkan di Akun B dan Akun C
1	AWSAkses penuh	AWSAkses penuh+tolak akses S3	AWSAkses penuh+tolak akses EC2	Tidak ada S3, tidak ada akses EC2	Tidak ada akses S3
2	AWSAkses penuh	Izinkan akses Amazon Elastic Compute Cloud (Amazon EC2)	Izinkan akses EC2	Memungkinkan akses EC2 saja	Memungkinkan akses EC2 saja
3	Tolak akses S3	Izinkan akses S3	AWSAkses penuh	Tidak ada akses layanan	Tidak ada akses layanan

Tabel berikut menunjukkan kebijakan efektif dalam Beban Kerja OU.

Skenario	SCP di Root	SCP di Beban Kerja OU	SCP dan Uji OU	Kebijakan yang dihasilkan di Akun D	Kebijakan yang dihasilkan di Produksi OU, Akun E dan Akun F
1	AWSAkses penuh	AWSAkses penuh	AWSAkses penuh+tolak akses EC2	Tidak ada akses EC2	AWSAkses penuh

Skenario	SCP di Root	SCP di Beban Kerja OU	SCP dan Uji OU	Kebijakan yang dihasilkan di Akun D	Kebijakan yang dihasilkan di Produksi OU, Akun E dan Akun F
2	AWSAkses penuh	AWSAkses penuh	Izinkan akses EC2	Izinkan akses EC2	AWSAkses penuh
3	Tolak akses S3	AWSAkses penuh	Izinkan akses S3	Tidak ada akses layanan	Tidak ada akses layanan

Sintaksis SCP

Kebijakan kontrol layanan (SCP) menggunakan sintaks serupa dengan kebijakan izin AWS Identity and Access Management (IAM) dan kebijakan berbasis sumber daya (seperti kebijakan bucket Amazon S3). Untuk informasi selengkapnya tentang kebijakan IAM dan sintaksisnya, lihat Gambaran Umum Kebijakan IAM dalam Panduan Pengguna IAM.

SCP adalah file plaintext yang terstruktur sesuai dengan aturan JSON. Ia menggunakan elemen-elemen yang dijelaskan dalam topik ini.

> **Note**
>
> Semua karakter dalam hitungan SCP Anda terhadap ukuran maksimum-nya. Contoh dalam panduan ini menunjukkan SCP yang diformat dengan spasi kosong ekstra untuk meningkatkan keterbacaannya. Namun, untuk menghemat ruang jika ukuran kebijakan Anda mendekati ukuran maksimum, maka Anda dapat menghapus spasi kosong, seperti spasi karakter dan baris putus yang berada di luar tanda kutip.

Untuk informasi umum tentang SCP, lihat Kebijakan Pengendalian Layanan (SCPs).

Ringkasan elemen

Tabel berikut merangkum elemen kebijakan yang dapat Anda gunakan di SCP. Beberapa elemen kebijakan hanya tersedia di SCP yang menolak tindakan. Kolom Efek didukung mencantumkan jenis efek yang dapat Anda gunakan dengan setiap elemen kebijakan di SCP.

Elemen	Tujuan	Efek didukung
Versi	Menentukan aturan sintaksis bahasa yang digunakan untuk memproses kebijakan.	`Allow`, `Deny`
Pernyataan	Berfungsi sebagai kontainer untuk elemen kebijakan. Anda dapat memiliki beberapa pernyataan di SCP.	`Allow`, `Deny`
ID Pernyataan (Sid)	(Opsional) Menyediakan nama yang ramah untuk pernyataa	`Allow`, `Deny`

Elemen	Tujuan	Efek didukung
	n tersebut.	
Efek	Menentukan apakah pernyataan SCP mengizinkan atau menolak akses ke pengguna dan peran IAM dalam akun.	`Allow`, `Deny`
Aksi	Menentukan AWS layanan dan tindakan yang SCP memungkinkan atau menyangkal.	`Allow`, `Deny`

Elemen	Tujuan	Efek didukung
NotAction	Menentukan AWS layanan dan tindakan yang dikecualikan dari SCP. Digunakan sebagai pengganti dari elemen `Action`.	`Deny`
Sumber	Menentukan AWS sumber daya yang berlaku SCP.	`Deny`
Kondisi	Menentukan syarat ketika pernyataan ini berlaku.	`Deny`

Bagian berikut memberikan informasi lebih lanjut dan contoh bagaimana elemen kebijakan digunakan dalam SCP.

Elemen **`Version`**

Setiap SCP harus menyertakan elemen `Version` dengan nilai `"2012-10-17"`. Ini adalah nilai versi yang sama sebagai versi terbaru dari kebijakan izin IAM.

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

Untuk informasi selengkapnya, lihat Elemen Kebijakan IAM JSON: Versi dalam Panduan Pengguna IAM.

Elemen **`Statement`**

SCP terdiri dari satu atau beberapa elemen `Statement`. Anda hanya dapat memiliki satu kata kunci `Statement` dalam kebijakan, tetapi nilai dapat berupa array JSON dari pernyataan (diapit oleh karakter [ ]).

Contoh berikut menunjukkan pernyataan tunggal yang terdiri dari satu elemen `Effect`, `Action`, dan `Resource`.

```
    "Statement": {
        "Effect": "Allow",
        "Action": "*",
        "Resource": "*"
    }
```

Contoh berikut mencakup dua pernyataan sebagai daftar array dalam satu elemen `Statement`. Pernyataan pertama mengizinkan semua tindakan, sedangkan yang kedua menolak tindakan EC2. Hasilnya adalah bahwa administrator di akun dapat mendelegasikan izin kecuali izin dari Amazon Elastic Compute Cloud (Amazon EC2).

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "ec2:*",
            "Resource": "*"
        }
```

```
    ]
```

Untuk informasi selengkapnya, lihat Elemen kebijakan IAM JSON: Pernyataan dalam Panduan Pengguna IAM.

Elemen ID pernyataan (**`Sid`**)

`Sid` adalah pengidentifikasi opsional yang Anda berikan untuk pernyataan kebijakan. Anda dapat menetapkan nilai `Sid` untuk setiap pernyataan dalam rangkaian pernyataan. Dalam contoh berikut, SCP menunjukkan sampel `Sid`.

```
{
    "Statement": {
        "Sid": "AllowsAllActions",
        "Effect": "Allow",
        "Action": "*",
        "Resource": "*"
    }
}
```

Untuk informasi selengkapnya, lihat Elemen Kebijakan IAM JSON: Id dalam Panduan Pengguna IAM.

Elemen **`Effect`**

Setiap pernyataan harus berisi satu elemen `Effect`. Nilai dapat berupa `Allow` atau `Deny`, salah satu. Ia mempengaruhi setiap tindakan yang tercantum dalam pernyataan yang sama.

Untuk informasi selengkapnya, lihat Elemen Kebijakan IAM JSON: Efek dalam Panduan Pengguna IAM.

`"Effect": "Allow"`

Contoh berikut menunjukkan SCP dengan pernyataan yang berisi elemen `Effect` dengan nilai `Allow` yang mengizinkan pengguna akun untuk melakukan tindakan untuk layanan Amazon S3. Contoh ini berguna dalam sebuah organisasi yang menggunakan strategi daftar izinkan (dimana kebijakan `FullAWSAccess` default-nya telah dilepaskan sehingga izin secara implisit ditolak secara default). Hasilnya adalah bahwa pernyataan mengizinkan izin Amazon S3 untuk akun terlampir:

```
{
    "Statement": {
        "Effect": "Allow",
        "Action": "s3:*",
```

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

Meskipun pernyataan ini menggunakan nilai kata kunci `Allow` yang sama sebagai kebijakan izin IAM, dalam SCP ia tidak benar-benar memberikan izin pengguna untuk melakukan apa pun. Sebagai gantinya, SCP bertindak sebagai filter yang menentukan izin maksimum untuk pengguna IAM dan peran IAM dalam suatu organisasi. Dalam contoh sebelumnya, bahkan jika pengguna di akun memiliki kebijakan terkelola `AdministratorAccess` terlampir, SCP ini membatasi Semua pengguna di akun yang terpengaruh hanya ke tindakan Amazon S3.

`"Effect": "Deny"`

Dalam sebuah pernyataan di mana elemen `Effect` memiliki nilai `Deny`, Anda juga dapat membatasi akses ke sumber daya tertentu atau menentukan syarat ketika SCP berlaku.

Berikut ini menunjukkan contoh bagaimana menggunakan kunci syarat dalam pernyataan tolak.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "ec2:RunInstances",
        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
            "StringNotEquals": {
                "ec2:InstanceType": "t2.micro"
            }
        }
    }
}
```

Pernyataan ini di SCP menetapkan pagar untuk mencegah akun terpengaruh (di mana SCP dilampirkan ke akun itu sendiri atau akar organisasi atau OU yang berisi akun), dari meluncurkan instans Amazon EC2 jika instans Amazon EC2 tidak diatur ke `t2.micro`. Bahkan jika kebijakan IAM yang memungkinkan tindakan ini dilampirkan ke akun, pagar yang dibuat oleh SCP akan mencegahnya.

Elemen **`Action`** dan **`NotAction`**

Setiap pernyataan harus berisi salah satu dari berikut ini:

- Dalam pernyataan mengizinkan dan menolak, sebuah elemen `Action`.
- Dalam pernyataan menolak saja (di mana nilai dari elemen `Effect` adalah `Deny`), sebuah elemen `Action` atau elemen `NotAction`.

Nilai untuk `NotAction` elemen `Action` or adalah daftar (array JSON) string yang mengidentifikasi AWS layanan dan tindakan yang diizinkan atau ditolak oleh pernyataan.

Setiap string terdiri dari singkatan untuk layanan (seperti "s3", "ec2", "iam", atau "organisasi"), dalam semua huruf kecil, diikuti oleh titik dua dan kemudian tindakan dari layanan tersebut. Action dan NotAction peka huruf besar kecil dan harus diketik seperti yang ditunjukkan dalam dokumentasi setiap layanan. Umumnya, mereka semua diketik dengan setiap kata dimulai dengan huruf besar dan sisanya huruf kecil. Sebagai contoh: `"s3:ListAllMyBuckets"`.

Anda juga dapat menggunakan karakter wildcard seperti asterisk (*) atau tanda tanya (?) dalam SCP:

- Gunakan tanda bintang (*) sebagai wildcard untuk mencocokkan beberapa tindakan yang berbagi bagian dari nama. Nilai `"s3:*"` artinya semua tindakan dalam layanan Amazon S3. Nilai `"ec2:Describe*"` cocok hanya dengan tindakan EC2 yang dimulai dengan "Describe".
- Gunakan tanda tanya (?) wildcard untuk mencocokkan satu karakter.

> **Note**
>
> Dalam SCP, karakter wildcard (*) dan (?) dalam `NotAction` elemen `Action` atau dapat digunakan hanya dengan sendirinya atau pada akhir string. Ia tidak dapat muncul di awal atau tengah string. Karena itu, `"servicename:action*"` valid, tapi `"servicename:*action"` dan `"servicename:some*action"` keduanya tidak valid di SCP.

Untuk daftar semua layanan dan tindakan yang mereka dukung dalam kebijakan izin AWS Organizations SCP dan IAM, lihat Tindakan, Sumber Daya, dan Kunci Kondisi untuk AWS Layanan di Panduan Pengguna IAM.

Untuk informasi selengkapnya, lihat IAM JSON Policy Elements: Action dan IAM JSON Policy Elements: NotAction di Panduan Pengguna IAM.

Contoh elemen **`Action`**

Contoh berikut menunjukkan SCP dengan pernyataan yang memungkinkan administrator akun untuk mendelegasikan menjelaskan, mulai, berhenti, dan mengakhiri izin untuk instans EC2 di akun. Ini adalah contoh daftar izinkan, dan berguna ketika kebijakan `Allow *` default tidak dilampirkan sehingga, secara default, izin secara implisit ditolak. Jika kebijakan `Allow *` default masih dilampirkan pada akar, OU, atau akun yang dilampiri dengan kebijakan berikut, kebijakan tidak berpengaruh.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
          "ec2:DescribeInstances", "ec2:DescribeImages", "ec2:DescribeKeyPairs",
          "ec2:DescribeSecurityGroups", "ec2:DescribeAvailabilityZones",
 "ec2:RunInstances",
          "ec2:TerminateInstances", "ec2:StopInstances", "ec2:StartInstances"
        ],
        "Resource": "*"
    }
}
```

Contoh berikut menunjukkan bagaimana Anda dapat menolak akses ke layanan yang Anda ingin tidak gunakan di akun terlampir. Ia mengasumsikan bahwa SCP `"Allow *"` default masih dilampirkan pada semua OU dan akar. Kebijakan contoh ini mencegah administrator akun di akun terlampir mendelegasikan izin untuk layanan IAM, Amazon EC2, dan Amazon RDS. Setiap tindakan dari layanan lain dapat didelegasikan selama tidak ada kebijakan terlampir lain yang menolaknya.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": [ "iam:*", "ec2:*", "rds:*" ],
        "Resource": "*"
    }
}
```

Contoh elemen **`NotAction`**

Contoh berikut menunjukkan bagaimana Anda dapat menggunakan `NotAction` elemen untuk mengecualikan AWS layanan dari efek kebijakan.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LimitActionsInRegion",
      "Effect": "Deny",
      "NotAction": "iam:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "us-west-1"
        }
       }
     }
   ]
}
```

Dengan pernyataan ini, akun yang terpengaruh dibatasi untuk mengambil tindakan dalam yang ditentukan Wilayah AWS, kecuali saat menggunakan tindakan IAM.

Elemen **`Resource`**

Dalam pernyataan di mana elemen `Effect` memiliki nilai `Allow`, Anda dapat menentukan hanya "*" di elemen `Resource` dari sebuah SCP. Anda tidak dapat menentukan sumber daya individual Amazon Resource Name (ARN).

Anda juga dapat menggunakan karakter wildcard seperti asterisk (*) atau tanda tanya (?) dalam elemen sumber daya:

- Gunakan tanda bintang (*) sebagai wildcard untuk mencocokkan beberapa tindakan yang berbagi bagian dari nama.
- Gunakan tanda tanya (?) wildcard untuk mencocokkan satu karakter.

Dalam pernyataan di mana elemen `Effect` memiliki nilai `Deny`, Anda dapat menentukan ARN individu, seperti yang ditunjukkan dalam contoh berikut.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessToAdminRole",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/role-to-deny"
      ]
    }
  ]
}
```

SCP ini membatasi pengguna dan peran IAM dalam akun yang terpengaruh dari membuat perubahan ke IAM role administratif umum yang dibuat di semua akun di organisasi Anda.

Untuk informasi selengkapnya, lihat Elemen kebijakan IAM JSON: Sumber Daya dalam Panduan Pengguna IAM.

Elemen **`Condition`**

Anda dapat menentukan elemen `Condition` dalam pernyataan menolak dalam SCP.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "cloudfront:*",
```

```
                "iam:*",
                "route53:*",
                "support:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                }
            }
        }
    ]
}
```

SCP ini menolak akses ke setiap operasi di luar Wilayah `eu-central-1` dan `eu-west-1`, kecuali untuk tindakan dalam layanan yang terdaftar.

Untuk informasi selengkapnya, lihat Elemen kebijakan IAM JSON: Syarat dalam Panduan Pengguna IAM.

Elemen yang Tidak Didukung

Elemen berikut tidak didukung di SCP:

- `Principal`
- `NotPrincipal`
- `NotResource`

Contoh kebijakan kontrol layanan

Contoh Kebijakan Kontrol Layanan (SCP) yang ditampilkan dalam topik ini hanya untuk tujuan informasi.

> **Sebelum menggunakan contoh-contoh ini**
>
> Sebelum Anda menggunakan SCP contoh ini di organisasi Anda, lakukan hal berikut:
>
> - Tinjau dan sesuaikan SCP dengan cermat berdasarkan kebutuhan unik Anda.

- Benar-benar menguji SCP di lingkungan Anda dengan layanan AWS yang Anda gunakan.

  Contoh kebijakan di bagian ini menunjukkan implementasi dan penggunaan SCP. Contoh-contoh tersebut tidak dimaksudkan untuk ditafsirkan sebagai rekomendasi AWS resmi atau praktik terbaik untuk diimplementasikan persis seperti yang ditunjukkan. Adalah tanggung jawab Anda untuk secara hati-hati menguji setiap kebijakan berbasis penolakan untuk kesesuaiannya untuk menyelesaikan kebutuhan bisnis di lingkungan Anda. Kebijakan kontrol layanan berbasis penolakan dapat secara tidak sengaja membatasi atau memblokir penggunaan AWS kecuali jika Anda menambahkan pengecualian yang diperlukan untuk kebijakan. Untuk contoh pengecualian seperti itu, lihat contoh pertama yang membebaskan layanan global dari aturan yang memblokir akses ke Wilayah AWS yang tidak diinginkan.
- Ingat bahwa SCP memengaruhi setiap pengguna dan peran, termasuk pengguna root, di setiap akun yang dilampirkan.

Tip

Anda dapat menggunakan Data layanan terakhir diakses di IAM untuk memperbarui SCP Anda untuk membatasi akses hanya ke layanan AWS yang Anda butuhkan. Untuk informasi selengkapnya, lihat: Melihat Data Layanan Organizations Terakhir Diakses untuk Organizations di Panduan Pengguna IAM.

Setiap kebijakan berikut adalah contoh dari strategi kebijakan daftar tolak. Kebijakan daftar tolak harus dilampirkan bersama dengan kebijakan lain yang memungkinkan tindakan yang disetujui di akun yang terpengaruh. Misalnya, kebijakan `FullAWSAccess` default memungkinkan penggunaan semua layanan dalam sebuah akun. Kebijakan ini dilampirkan secara default ke akar, semua unit organizational (UO), dan semua akun. Kebijakan tersebut tidak benar-benar memberikan izin; tidak ada SCP yang melakukannya. Sebaliknya, kebijakan tersebut memungkinkan administrator dalam akun tersebut untuk mendelegasikan akses ke tindakan tersebut dengan melampirkan kebijakan izin AWS Identity and Access Management (IAM) standar untuk pengguna, peran, atau grup di akun. Masing-masing kebijakan daftar tolak ini kemudian menimpa kebijakan apapun dengan memblokir akses ke layanan atau tindakan yang ditentukan.

Contoh

- Contoh Umum
  - Menolak akses ke AWS berdasarkan Wilayah AWS yang diminta

- Mencegah VPC apa pun yang belum memiliki akses internet untuk mendapatkannya

Contoh Umum

Menolak akses ke AWS berdasarkan Wilayah AWS yang diminta

SCP ini menolak akses ke setiap operasi di luar WIlayah yang ditentukan. Ganti `eu-central-1` dan `eu-west-1` dengan Wilayah AWS yang ingin Anda gunakan. Ia memberikan pengecualian untuk operasi dalam layanan global yang disetujui. Contoh ini juga menunjukkan bagaimana untuk membebaskan permintaan yang dibuat oleh salah satu dari dua peran administrator yang ditentukan.

> **Note**
>
> Untuk menggunakan Region deny SCP denganAWS Control Tower, lihat Menolak akses ke AWS berdasarkan Wilayah AWS yang diminta.

Kebijakan ini menggunakan `Deny` untuk menolak akses ke semua permintaan untuk operasi yang tidak menargetkan salah satu dari dua wilayah yang disetujui (`eu-central-1` dan `eu-west-1`). NotActionElemen ini memungkinkan Anda untuk mencantumkan layanan yang operasi (atau operasi individu) dibebaskan dari pembatasan ini. Karena layanan global memiliki titik akhir yang secara fisik di-host oleh Wilayah `us-east-1`, mereka harus dibebaskan dengan cara ini. Dengan SCP yang distruktur dengan cara ini, permintaan dibuat untuk layanan global di WIlayah `us-east-1` diperbolehkan jika layanan yang diminta disertakan dalam elemen `NotAction`. Permintaan lain untuk layanan di Wilayah `us-east-1` ditolak oleh kebijakan contoh ini.

> **Note**
>
> Contoh ini mungkin tidak mencakup semuaAWS layanan atau operasi global terbaru. Ganti daftar layanan dan operasi dengan layanan global yang digunakan oleh akun di organisasi Anda.
>
> > **Kiat**
> >
> > Anda dapat melihat data terakhir yang diakses di konsol IAM untuk menentukan layanan global yang digunakan organisasi Anda. Tab Penasihat Akses di halaman

detail untuk pengguna, grup, atau peran IAM menampilkan layanan AWS yang telah digunakan oleh entitas tersebut, diurutkan berdasarkan akses terbaru.

Pertimbangan-pertimbangan

- AWS KMS dan AWS Certificate Manager men-support titik akhir Wilayah. Namun, jika Anda ingin menggunakannya dengan layanan global seperti Amazon CloudFront Anda harus memasukkannya dalam daftar pengecualian layanan global dalam SCP contoh berikut. Layanan global seperti Amazon CloudFront biasanya membutuhkan akses keAWS KMS dan ACM di wilayah yang sama, yang untuk layanan global adalah Wilayah US East (N. Virginia) (N. Virginia) (`us-east-1`).
- Secara default, AWS STS adalah layanan global dan harus disertakan dalam daftar pengecualian layanan global. Namun, Anda dapat mengaktifkan AWS STS untuk menggunakan titik akhir Wilayah, bukan titik akhir global tunggal. Jika Anda melakukan ini, Anda dapat menghapus STS dari daftar pengecualian layanan global di SCP contoh berikut. Untuk informasi selengkapnya, lihat Mengelola AWS STS di sebuah Wilayah AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "a4b:*",
                "acm:*",
                "aws-marketplace-management:*",
                "aws-marketplace:*",
                "aws-portal:*",
                "budgets:*",
                "ce:*",
                "chime:*",
                "cloudfront:*",
                "config:*",
                "cur:*",
                "directconnect:*",
```

```
                "ec2:DescribeRegions",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeVpnGateways",
                "fms:*",
                "globalaccelerator:*",
                "health:*",
                "iam:*",
                "importexport:*",
                "kms:*",
                "mobileanalytics:*",
                "networkmanager:*",
                "organizations:*",
                "pricing:*",
                "route53:*",
                "route53domains:*",
                "route53-recovery-cluster:*",
                "route53-recovery-control-config:*",
                "route53-recovery-readiness:*",
                "s3:GetAccountPublic*",
                "s3:ListAllMyBuckets",
                "s3:ListMultiRegionAccessPoints",
                "s3:PutAccountPublic*",
                "shield:*",
                "sts:*",
                "support:*",
                "trustedadvisor:*",
                "waf-regional:*",
                "waf:*",
                "wafv2:*",
                "wellarchitected:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
```

```
                }
            }
        }
    ]
}
```

Mencegah pengguna dan peran IAM membuat perubahan tertentu

SCP ini membatasi pengguna dan peran IAM dari membuat perubahan pada IAM role tertentu yang Anda buat di semua akun di organisasi Anda.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessToASpecificRole",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/name-of-role-to-deny"
      ]
    }
  ]
}
```

Mencegah pengguna dan peran IAM membuat perubahan yang ditentukan, dengan pengecualian untuk peran admin tertentu

SCP ini dibangun pada contoh sebelumnya untuk membuat pengecualian untuk administrator. Ia mencegah pengguna dan peran IAM dalam akun yang terpengaruh membuat perubahan pada IAM

role administratif umum yang dibuat di semua akun di organisasi Anda kecuali untuk administrator yang menggunakan peran tertentu.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessWithException",
      "Effect": "Deny",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
      ],
      "Resource": [
        "arn:aws:iam::*:role/name-of-role-to-deny"
      ],
      "Condition": {
        "StringNotLike": {
          "aws:PrincipalARN":"arn:aws:iam::*:role/name-of-admin-role-to-allow"
        }
      }
    }
  ]
}
```

Mewajibkan MFA untuk melakukan tindakan API

Gunakan SCP seperti berikut untuk mengharuskan autentikasi multi-faktor (MFA) diaktifkan sebelum pengguna atau peran IAM dapat melakukan tindakan. Dalam contoh ini, tindakan tersebut adalah untuk menghentikan instans Amazon EC2.

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

```
    {
      "Sid": "DenyStopAndTerminateWhenMFAIsNotPresent",
      "Effect": "Deny",
      "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*",
      "Condition": {"BoolIfExists": {"aws:MultiFactorAuthPresent": false}}
    }
  ]
}
```

Memblokir akses layanan untuk pengguna akar

Kebijakan berikut membatasi semua akses ke tindakan tertentu untuk pengguna akar dalam akun anggota. Jika Anda ingin mencegah akun Anda menggunakan kredensial akar dengan cara tertentu, tambahkan tindakan Anda sendiri ke kebijakan ini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RestrictEC2ForRoot",
      "Effect": "Deny",
      "Action": [
        "ec2:*"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::*:root"
          ]
        }
      }
    }
  ]
}
```

Mencegah akun anggota keluar dari organisasi

Kebijakan berikut memblokir penggunaan operasi`LeaveOrganization` API sehingga administrator akun anggota tidak dapat menghapus akun mereka dari organisasi.

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

Contoh SCP untuk Amazon CloudWatch

Contoh dalam kategori ini

- Mencegah pengguna menonaktifkan CloudWatch atau mengubah konfigurasinya

Mencegah pengguna menonaktifkan CloudWatch atau mengubah konfigurasinya

Operator CloudWatch tingkat bawah harus memantau dasbor dan alarm. Namun, operator tidak harus dapat menghapus atau mengubah dasbor atau alarm yang mungkin dimasukkan ke dalam tempatnya oleh orang senior. SCP ini mencegah pengguna atau peran dalam akun yang terpengaruh menjalankan salah satu perintah CloudWatch yang dapat menghapus atau mengubah dasbor atau alarm Anda.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudwatch:DeleteAlarms",
        "cloudwatch:DeleteDashboards",
        "cloudwatch:DisableAlarmActions",
        "cloudwatch:PutDashboard",
```

```
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:SetAlarmState"
      ],
      "Resource": "*"
    }
  ]
}
```

Contoh SCP untuk AWS Config

Contoh dalam kategori ini

- Mencegah pengguna menonaktifkan AWS Config atau mengubah aturannya

Mencegah pengguna menonaktifkan AWS Config atau mengubah aturannya

SCP ini mencegah pengguna atau peran dalam akun yang terpengaruh dari menjalankan operasi AWS Config yang dapat menonaktifkan AWS Config atau mengubah aturan atau pemicunya.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "config:DeleteConfigRule",
        "config:DeleteConfigurationRecorder",
        "config:DeleteDeliveryChannel",
        "config:StopConfigurationRecorder"
      ],
      "Resource": "*"
    }
  ]
}
```

Contoh SCP untuk Amazon Elastic Compute Cloud (Amazon EC2)

Contoh dalam kategori ini

- Mengharuskan instans Amazon EC2 untuk menggunakan jenis tertentu
- Mencegah peluncuran instans EC2 tanpa IMDSv2
- Mencegah penonaktifan enkripsi Amazon EBS default

Mengharuskan instans Amazon EC2 untuk menggunakan jenis tertentu

Dengan SCP ini, setiap instans yang meluncurkan tidak menggunakan jenis instans `t2.micro` akan ditolak.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RequireMicroInstanceType",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "ec2:InstanceType": "t2.micro"
        }
      }
    }
  ]
}
```

Mencegah peluncuran instans EC2 tanpa IMDSv2

Kebijakan berikut membatasi semua pengguna meluncurkan instans EC2 tanpa IMDSv2.

```
[
   {
      "Effect":"Deny",
      "Action":"ec2:RunInstances",
      "Resource":"arn:aws:ec2:*:*:instance/*",
      "Condition":{
         "StringNotEquals":{
            "ec2:MetadataHttpTokens":"required"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"ec2:RunInstances",
      "Resource":"arn:aws:ec2:*:*:instance/*",
```

```
      "Condition":{
         "NumericGreaterThan":{
            "ec2:MetadataHttpPutResponseHopLimit":"3"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"*",
      "Resource":"*",
      "Condition":{
         "NumericLessThan":{
            "ec2:RoleDelivery":"2.0"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"ec2:ModifyInstanceMetadataOptions",
      "Resource":"*"
   }
]
```

Kebijakan berikut membatasi semua pengguna dari meluncurkan instans EC2 tanpa IMDSv2 tetapi memungkinkan identitas IAM tertentu untuk memodifikasi opsi metadata instans.

```
[
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:MetadataHttpTokens": "required"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "NumericGreaterThan": {
```

```
        "ec2:MetadataHttpPutResponseHopLimit": "3"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NumericLessThan": {
        "ec2:RoleDelivery": "2.0"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:ModifyInstanceMetadataOptions",
    "Resource": "*",
    "Condition": {
      "StringNotLike": {
        "aws:PrincipalARN": [
          "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
        ]
      }
    }
  }
]
```

Mencegah penonaktifan enkripsi Amazon EBS default

Kebijakan berikut membatasi semua pengguna untuk menonaktifkan Enkripsi Amazon EBS default.

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:DisableEbsEncryptionByDefault"
  ],
  "Resource": "*"
}
```

Contoh SCP untuk Amazon GuardDuty

Contoh dalam kategori ini

- Mencegah pengguna menonaktifkan GuardDuty atau memodifikasi konfigurasinya

Mencegah pengguna menonaktifkan GuardDuty atau memodifikasi konfigurasinya

SCP ini mencegah pengguna atau peran dalam akun yang terpengaruh menonaktifkan GuardDuty atau mengubah konfigurasinya, baik secara langsung sebagai perintah atau melalui konsol. Secara efektif memungkinkan akses baca-saja ke informasi dan sumber daya GuardDuty.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "guardduty:AcceptInvitation",
                "guardduty:ArchiveFindings",
                "guardduty:CreateDetector",
                "guardduty:CreateFilter",
                "guardduty:CreateIPSet",
                "guardduty:CreateMembers",
                "guardduty:CreatePublishingDestination",
                "guardduty:CreateSampleFindings",
                "guardduty:CreateThreatIntelSet",
                "guardduty:DeclineInvitations",
                "guardduty:DeleteDetector",
                "guardduty:DeleteFilter",
                "guardduty:DeleteInvitations",
                "guardduty:DeleteIPSet",
                "guardduty:DeleteMembers",
                "guardduty:DeletePublishingDestination",
                "guardduty:DeleteThreatIntelSet",
                "guardduty:DisassociateFromMasterAccount",
                "guardduty:DisassociateMembers",
                "guardduty:InviteMembers",
                "guardduty:StartMonitoringMembers",
                "guardduty:StopMonitoringMembers",
                "guardduty:TagResource",
                "guardduty:UnarchiveFindings",
                "guardduty:UntagResource",
                "guardduty:UpdateDetector",
                "guardduty:UpdateFilter",
                "guardduty:UpdateFindingsFeedback",
                "guardduty:UpdateIPSet",
```

```
                "guardduty:UpdatePublishingDestination",
                "guardduty:UpdateThreatIntelSet"
            ],
            "Resource": "*"
        }
    ]
}
```

Contoh SCP untuk AWS Resource Access Manager

Contoh dalam kategori ini

- Mencegah berbagi eksternal
- Mengizinkan akun tertentu untuk hanya berbagi jenis sumber daya yang ditentukan
- Mencegah berbagi dengan organisasi atau unit organisasi (OU)
- Izinkan berbagi hanya dengan pengguna dan peran IAM tertentu

Mencegah berbagi eksternal

Contoh SCP berikut mencegah pengguna membuat berbagi sumber daya saham yang memungkinkan berbagi dengan pengguna dan peran IAM yang bukan bagian dari organisasi.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:UpdateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "ram:RequestedAllowsExternalPrincipals": "true"
                }
            }
        }
    ]
}
```

Mengizinkan akun tertentu untuk hanya berbagi jenis sumber daya yang ditentukan

SCP berikut memungkinkan akun 111111111111 dan 222222222222 untuk membuat berbagi sumber daya yang membagikan daftar prefiks, dan untuk meng-associate daftar prefiks dengan berbagi sumber daya yang ada.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "OnlyNamedAccountsCanSharePrefixLists",
            "Effect": "Deny",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalAccount": [
                        "111111111111",
                        "222222222222"
                    ]
                },
                "StringEquals": {
                    "ram:RequestedResourceType": "ec2:PrefixList"
                }
            }
        }
    ]
}
```

Mencegah berbagi dengan organisasi atau unit organisasi (OU)

SCP berikut mencegah pengguna membuat berbagi sumber daya yang membagikan sumber daya dengan Organisasi atau OU AWS.

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

```
                "ram:CreateResourceShare",
                "ram:AssociateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringLike": {
                    "ram:Principal": [
                        "arn:aws:organizations::*:organization/*",
                        "arn:aws:organizations::*:ou/*"
                    ]
                }
            }
        }
    ]
}
```

Izinkan berbagi hanya dengan pengguna dan peran IAM tertentu

Contoh SCP berikut memungkinkan pengguna untuk berbagi sumber daya dengan hanya organisasi `o-12345abcdef`, unit organisasi `ou-98765fedcba`, dan akun `111111111111` saja.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "ram:Principal": [
                        "arn:aws:organizations::123456789012:organization/
o-12345abcdef",
                        "arn:aws:organizations::123456789012:ou/o-12345abcdef/
ou-98765fedcba",
                        "111111111111"
                    ]
                }
            }
        }
```

```
    ]
}
```

Pengendali Pemulihan Pemulihan Aplikasi

Contoh dalam kategori ini

- Cegah pengguna memperbarui status kontrol perutean Route 53 ARC

Cegah pengguna memperbarui status kontrol perutean Route 53 ARC

Operator ARC tingkat bawah harus memantau dasbor dan melihat informasi Route 53 ARC. Namun, operator tidak boleh memperbarui kontrol routing untuk gagal atas aplikasi dari satuWilayah AWS ke yang lain, sebagai operator senior mungkin diizinkan untuk. SCP ini mencegah pengguna atau peran dalam akun yang terpengaruh menjalankan operasi Route 53 ARC yang memperbarui kontrol perute Route 53.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAll",
            "Effect": "Deny",
            "Action": [
                "route53-recovery-cluster:UpdateRoutingControlState",
                "route53-recovery-cluster:UpdateRoutingControlStates"
            ],
            "Resource": "*",
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

Contoh SCP untuk Amazon S3

Contoh dalam kategori ini

- Mencegah unggahan objek tak terenkripsi Amazon S3

Mencegah unggahan objek tak terenkripsi Amazon S3

Kebijakan berikut membatasi semua pengguna untuk mengunggah objek yang tidak dienkripsi ke bucket S3.

```
{
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "*",
  "Condition": {
    "Null": {
      "s3:x-amz-server-side-encryption": "true"
    }
  }
}
```

Kebijakan berikut membatasi semua pengguna untuk mengunggah objek yang tidak terenkripsi ke bucket S3 dan juga memberlakukan jenis enkripsi tertentu (baik AES256 atau aws:kms) untuk unggahan objek dalam bucket mereka.

```
[
  {
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "*",
    "Condition": {
      "Null": {
        "s3:x-amz-server-side-encryption": "true"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "*",
    "Condition": {
```

```
      "StringNotEquals": {
        "s3:x-amz-server-side-encryption": "AES256"
      }
    }
  }
]
```

Contoh SCP untuk penandaan sumber daya

Contoh dalam kategori ini

- Mengharuskan tag pada sumber daya yang dibuat tertentu
- Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal utama yang berwenang

Mengharuskan tag pada sumber daya yang dibuat tertentu

SCP berikut mencegah pengguna IAM dan peran dalam akun yang terpengaruh membuat jenis sumber daya tertentu jika permintaan tidak menyertakan tag tertentu.

> **Important**
>
> Ingatlah untuk menguji kebijakan berbasis tolak dengan layanan yang Anda gunakan di lingkungan Anda. Contoh berikut adalah blok sederhana menciptakan rahasia yang tidak diberi tag atau menjalankan instans Amazon EC2 yang tidak diberi tag, dan tidak termasuk pengecualian.
> Kebijakan contoh berikut ini tidak kompatibel dengan AWS CloudFormation seperti tertulis, karena layanan yang menciptakan rahasia dan menandainya sebagai dua langkah terpisah. Kebijakan contoh ini secara efektif memblokir AWS CloudFormation dari menciptakan rahasia sebagai bagian dari tumpukan, karena tindakan seperti itu akan menghasilkan, namun secara singkat, rahasia yang tidak ditandai seperti yang diharuskan.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyCreateSecretWithNoProjectTag",
      "Effect": "Deny",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "*",
```

```
      "Condition": {
        "Null": {
          "aws:RequestTag/Project": "true"
        }
      }
    },
    {
      "Sid": "DenyRunInstanceWithNoProjectTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/Project": "true"
        }
      }
    },
    {
      "Sid": "DenyCreateSecretWithNoCostCenterTag",
      "Effect": "Deny",
      "Action": "secretsmanager:CreateSecret",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:RequestTag/CostCenter": "true"
        }
      }
    },
    {
      "Sid": "DenyRunInstanceWithNoCostCenterTag",
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
      ],
      "Condition": {
        "Null": {
          "aws:RequestTag/CostCenter": "true"
        }
      }
```

```
    }
  ]
}
```

Untuk daftar semua layanan dan tindakan yang mereka support baik di kebijakan izin SCP AWS Organizations dan IAM, lihat Tindakan, Sumber Daya, Kunci Syarat untuk Layanan AWS di Panduan Pengguna IAM.

Mencegah tag agar tidak dimodifikasi kecuali oleh prinsipal utama yang berwenang

SCP berikut menunjukkan bagaimana kebijakan dapat memungkinkan hanya prinsipal utama yang berwenang untuk memodifikasi tag yang melekat pada sumber daya Anda. Ini adalah bagian penting dari penggunaan kontrol akses berbasis atribut (attribute-based access control/ABAC) sebagai bagian dari strategi keamanan cloud AWS Anda. Kebijakan ini memungkinkan pemanggil untuk memodifikasi tag hanya pada sumber daya di mana tag otorisasi (dalam contoh ini, `access-project`) sama persis dengan tag otorisasi yang sama yang dilampirkan pada pengguna atau peran yang membuat permintaan. Kebijakan ini juga mencegah pengguna yang berwenang mengubah nilai dari tag yang digunakan untuk otorisasi. Prinsipal utama yang memanggil harus memiliki tag otorisasi untuk membuat perubahan sekaligus.

Kebijakan ini hanya memblokir pengguna yang tidak sah agar tidak mengubah tag. Pengguna yang diotorisasi yang tidak diblokir oleh kebijakan ini harus masih memiliki kebijakan IAM terpisah yang secara eksplisit memberikan izin `Allow` pada API penandaan yang relevan. Sebagai contoh, jika pengguna Anda memiliki kebijakan administrator dengan `Allow */*` (izinkan semua layanan dan semua operasi), maka hasil kombinasi pada pengguna administrator yang diizinkan untuk mengubah hanya tag yang memiliki nilai tag otorisasi yang cocok dengan nilai tag otorisasi yang dilampirkan pada prinsipal utama pengguna. Hal ini karena `Deny` eksplisit dalam kebijakan ini menimpa `Allow` eksplisit dalam kebijakan administrator.

> **Important**
>
> Contoh ini bukan solusi kebijakan yang lengkap dan tidak boleh digunakan seperti yang ditunjukkan di sini. Contoh ini dimaksudkan hanya untuk menggambarkan bagian dari strategi ABAC dan harus disesuaikan dan diuji untuk lingkungan produksi.
> Untuk kebijakan lengkap dengan analisis detail tentang cara kerjanya, lihat Mengamankan tag sumber daya yang digunakan untuk otorisasi dengan menggunakan kebijakan kontrol layanan di AWS Organizations

Ingatlah untuk menguji kebijakan berbasis tolak dengan layanan yang Anda gunakan di lingkungan Anda.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModifyTagsIfResAuthzTagAndPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "ec2:ResourceTag/access-project": "${aws:PrincipalTag/access-
project}",
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "Null": {
                    "ec2:ResourceTag/access-project": false
                }
            }
        },
        {
            "Sid": "DenyModifyResAuthzTagIfPrinTagDontMatch",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestTag/access-project": "${aws:PrincipalTag/access-
project}",
```

```
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "access-project"
                    ]
                }
            }
        },
        {
            "Sid": "DenyModifyTagsIfPrinTagNotExists",
            "Effect": "Deny",
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::123456789012:role/org-admins/iam-
admin"
                },
                "Null": {
                    "aws:PrincipalTag/access-project": true
                }
            }
        }
    ]
}
```

Contoh SCP untuk Amazon Virtual Private Cloud (Amazon VPC)

Contoh dalam kategori ini

- Mencegah pengguna menghapus log alur Amazon VPC
- Mencegah VPC apa pun yang belum memiliki akses internet untuk mendapatkannya

Mencegah pengguna menghapus log alur Amazon VPC

SCP ini mencegah pengguna atau peran dalam akun yang terpengaruh menghapus log alur Amazon Elastic Compute Cloud (Amazon EC2) atau grup CloudWatch logs atau log pengaliran.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:DeleteFlowLogs",
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream"
      ],
      "Resource": "*"
    }
  ]
 }
```

Mencegah VPC apa pun yang belum memiliki akses internet untuk mendapatkannya

SCP ini mencegah pengguna atau peran dalam akun yang terpengaruh mengubah konfigurasi Virtual Private Cloud (VPC) Amazon EC2 Anda untuk memberi mereka akses langsung ke internet. Ia tidak memblokir akses langsung yang ada atau akses yang merutekan melalui lingkungan jaringan lokal on premise Anda.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ec2:AttachInternetGateway",
        "ec2:CreateInternetGateway",
        "ec2:CreateEgressOnlyInternetGateway",
        "ec2:CreateVpcPeeringConnection",
        "ec2:AcceptVpcPeeringConnection",
        "globalaccelerator:Create*",
        "globalaccelerator:Update*"
      ],
      "Resource": "*"
```

```
    }
  ]
}
```

Mengelola unit organisasi

Anda dapat menggunakan unit organisasi (OU) untuk mengelompokkan akun bersama-sama untuk mengelola sebagai satu unit. Ini sangat menyederhanakan pengelolaan akun Anda. Misalnya, Anda dapat melampirkan kontrol berbasis kebijakan untuk OU, dan semua akun dalam OU secara otomatis mewarisi kebijakan. Anda dapat membuat beberapa OU dalam satu organisasi, dan Anda dapat membuat OU dalam OU lainnya. Setiap OU dapat berisi beberapa akun, dan Anda dapat memindahkan akun dari satu OU ke yang lain. Namun, nama OU harus unik dalam OU induk atau akar.

> **Note**
>
> Ada satu akar dalam organisasi, yang AWS Organizations menciptakan untuk Anda ketika Anda pertama kali mengatur organisasi Anda.

Topik

Anda juga dapat meninjau semua OU di seluruh organisasi Anda. Untuk informasi selengkapnya, lihat Melihat detail OU.

Menavigasi akar dan hirarki OU

Untuk menavigasi ke OU yang berbeda atau ke akar saat memindahkan akun atau melampirkan kebijakan, Anda dapat menggunakan tampilan "pohon" default.

AWS Management Console

Untuk menavigasi organisasi sebagai 'pohon'

1. Masuklah ke konsolAWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada Akun AWShalaman, di bagian atas bagian Organisasi, pilih sakelar Hierarki (bukan Daftar).
3. Pohon awalnya muncul yang menunjukkan akar, hanya menampilkan tingkat pertama OU anak dan akun. Untuk memperluas pohon untuk menampilkan level yang lebih dalam, pilih ikon perluas ( ) di sebelah entitas induk mana pun. Untuk mengurangi kekacauan dan runtuh cabang pohon, pilih ikon runtuh ( ) di sebelah entitas induk yang diperluas.
4. Pilih nama OU atau akar untuk melihat rincian dan melakukan operasi tertentu. Atau, Anda dapat memilih tombol radio di samping nama, dan melakukan operasi tertentu pada entitas tersebut di menu Tindakan.

Anda juga dapat melihat daftar hanya akun di organisasi Anda dalam bentuk tabel, tanpa harus terlebih dahulu menavigasi ke OU untuk menemukan mereka. Dalam tampilan ini Anda tidak dapat melihat salah satu OU atau memanipulasi kebijakan yang dilampirkan padanya.

AWS Management Console

Untuk melihat organisasi sebagai daftar datar akun tanpa hirarki

1. Masuklah ke konsolAWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada Akun AWShalaman, di bagian atas bagian Organisasi, pilih ikon sakelar Lihat Akun AWS saja untuk menyalakannya.
3. Daftar akun ditampilkan tanpa hirarki apa pun.

Membuat OU

Saat masuk ke akun pengelolaan organisasi Anda, Anda dapat membuat OU di akar organisasi Anda. OU dapat dibuat nest hingga kedalaman lima tingkat . Untuk membuat OU, selesaikan langkah berikut.

Important

Jika organisasi ini dikelola AWS Control Tower, buat OU Anda dengan AWS Control Tower konsol atau API. Jika Anda membuat OU di Organizations, maka OU tersebut tidak terdaftar AWS Control Tower. Untuk informasi lebih lanjut, lihat Mengacu pada Sumber Daya di luar AWS Control Tower di Panduan PenggunaAWS Control Tower .

Izin minimum

Untuk membuat OU di akar di organisasi Anda, Anda harus memiliki izin berikut:

- `organizations:DescribeOrganization` – hanya diperlukan bila menggunakan konsol Organizations
- `organizations:CreateOrganizationalUnit`

AWS Management Console

Untuk membuat OU

1. Masuklah ke konsolAWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Arahkan ke laman Akun AWS.

   Konsol menampilkan OU Akar dan isinya. Pertama kali Anda mengunjungi Akar, konsol menampilkan semua Akun AWS Anda di tampilan tingkat atas. Jika Anda sebelumnya membuat OU dan pindah akun ke dalamnya, konsol hanya menampilkan OU tingkat atas dan akun yang belum Anda pindah ke OU.
3. (Opsional) Jika Anda ingin membuat OU di dalam OU yang sudah ada, navigasikan ke OU anak dengan memilih nama (bukan kotak centang) OU anak, atau dengan memilih opsi

di samping OU dalam tampilan pohon sampai Anda melihat yang Anda inginkan, dan lalu memilih namanya.

4. Ketika Anda telah memilih OU induk yang benar pada hirarki, pada menu Tindakan, di bawah Unit Organisasi, pilih Buat baru
5. Di kotak dialog Buat unit organisasi, masukkan nama OU yang ingin Anda buat.
6. (Opsional) Tambahkan satu atau lebih tag dengan memilih Tambahkan tag dan kemudian memasukkan kunci dan nilai opsional. Membiarkan nilai kosong akan mengaturnya ke string kosong; itu tidak `null`. Anda dapat melampirkan hingga 50 tag ke OU.
7. Akhirnya, pilih Buat unit organisasi.

OU baru Anda muncul di dalam induk. Anda sekarang dapat memindahkan akun ke OU ini atau melampirkan kebijakan padanya.

AWS CLI & AWS SDKs

Untuk membuat OU

Anda dapat menggunakan salah satu perintah berikut untuk membuat OU:

- AWS CLI: create-organizational-unit

  Untuk membuat OU, Anda harus terlebih dahulu menemukan identitas akar atau OU yang Anda inginkan menjadi induk dari OU baru.

  Untuk menemukan identitas akar, gunakan perintah list-roots. Untuk menemukan identitas OU, gunakan list-children untuk menavigasi ke OU yang Anda inginkan.

  Contoh berikut menunjukkan bagaimana menemukan identitas akar, dan kemudian menemukan identitas OU di bawah akar. Perintah terakhir menunjukkan cara membuat OU baru di OU yang ditemukan.

```
$ aws organizations list-roots
{
    "Roots": [
        {
            "Id": "r-a1b2",
            "Arn": "arn:aws:organizations::123456789012:root/o-aa111bb222/r-a1b2",
            "Name": "Root",
            "PolicyTypes": []
```

```
        }
    ]
}
$ aws organizations list-children \
    --parent-id r-a1b2 \
    --child-type ORGANIZATIONAL_UNIT
{
    "Children": [
        {
            "Id": "ou-a1b2-f6g7h111",
            "Type": "ORGANIZATIONAL_UNIT"
        }
    ]
}
$ aws organizations create-organizational-unit \
    --parent-id ou-a1b2-f6g7h111 \
    --name New-Child-OU
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h222",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
        "Name": "New-Child-OU"
    }
}
```

- AWS SDK: CreateOrganizationalUnit

Mengubah nama OU

Saat masuk ke akun pengelolaan organisasi Anda, Anda dapat mengganti nama OU. Untuk melakukan ini, selesaikan langkah-langkah berikut.

> **Izin minimum**
>
> Untuk mengganti nama OU dalam root di AWS organisasi Anda, Anda harus memiliki izin berikut:
>
> - `organizations:DescribeOrganization` – hanya diperlukan bila menggunakan konsol Organizations
> - `organizations:UpdateOrganizationalUnit`

AWS Management Console

Untuk mengubah nama OU

1. Masuklah ke konsolAWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada laman Akun AWS, navigasikan ke OU yang ingin Anda ubah namanya, dan lakukan salah satu langkah berikut:

   - Pilih
     
     tombol radio di samping OU yang ingin Anda ubah namanya. Kemudian, pada menu Tindakan, di bawah Unit organisasi, pilih Ubah nama.
   - Pilih nama OU, untuk mengakses laman detail OU. Lalu, di bagian atas laman pilih Ubah nama.
3. Di kotak dialog Ubah nama unit organisasi, masukkan nama baru, dan kemudian pilih Simpan perubahan.

AWS CLI & AWS SDKs

Untuk mengubah nama OU

Anda dapat menggunakan salah satu perintah berikut untuk mengubah nama OU:

- AWS CLI: update-organizational-unit

  Contoh berikut menunjukkan cara mengubah nama OU.

```
$ aws organizations update-organizational-unit \
    --organizational-unit-id ou-a1b2-f6g7h222 \
    --name "Renamed-OU"
{
    "OrganizationalUnit": {
        "Id": "ou-a1b2-f6g7h222",
        "Arn": "arn:aws:organizations::123456789012:ou/o-aa111bb222/ou-a1b2-
f6g7h222",
        "Name": "Renamed-OU"
    }
```

```
}
```

- AWS SDK: UpdateOrganizationalUnit

Mengedit tag yang dilampirkan ke OU

Saat masuk ke akun manajemen organisasi, Anda dapat menambahkan atau menghapus tag yang dilampirkan ke OU. Untuk melakukan ini, selesaikan langkah-langkah berikut.

> **Izin minimum**
>
> Untuk mengedit tag yang dilampirkan ke OU dalam root di AWS organisasi Anda, Anda harus memiliki izin berikut:
>
> - `organizations:DescribeOrganization` – hanya diperlukan bila menggunakan konsol Organizations
> - `organizations:DescribeOrganizationalUnit`– hanya diperlukan bila menggunakan konsol Organizations
> - `organizations:TagResource`
> - `organizations:UntagResource`

AWS Management Console

Untuk mengedit tag yang dilampirkan ke OU

1. Masuklah ke konsolAWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada laman Akun AWS, navigasikan ke dan pilih nama OU yang tagnya ingin Anda edit.
3. Pada laman detail OU, pilih tab Tag, dan kemudian pilih Kelola tag.
4. Anda dapat melakukan salah satu tindakan berikut di tab ini:
   - Edit nilai untuk tag dengan memasukkan nilai baru menggantikan yang lama. Anda tidak dapat memodifikasi kunci tag. Untuk mengubah kunci, Anda harus menghapus tag dengan kunci yang lama dan menambahkan tag dengan kunci baru.
   - Hapus tag yang ada dengan memilih Hapus di samping tag yang ingin Anda hapus.

- Tambahkan kunci tag dan pasangan nilai baru. Pilih Tambahkan tag, lalu masukkan nama kunci baru dan nilai opsional dalam kotak yang disediakan. Jika Anda membiarkan kotak Nilai kosong, nilai-nya adalah string kosong; itu bukan `null`.

5. Pilih Simpan perubahan setelah Anda membuat semua penambahan, penghapusan, dan pengeditan yang ingin Anda buat.

AWS CLI & AWS SDKs

Untuk mengedit tag yang dilampirkan ke OU

Anda dapat menggunakan salah satu perintah berikut untuk mengubah tag yang dilampirkan pada OU:

- AWS CLI: tag-resource dan untag-resource

  Contoh berikut melampirkan `"Department"="12345"` tag pada OU. Perhatikan bahwa `Key` and `Value` peka huruf besar dan kecil.

  ```
  $ aws organizations tag-resource \
      --resource-id ou-a1b2-f6g7h222 \
      --tags Key=Department,Value=12345
  ```

  Perintah ini tidak menghasilkan output bila berhasil.

  Contoh berikut menghapus tag `Department` dari OU.

  ```
  $ aws organizations untag-resource \
      --resource-id ou-a1b2-f6g7h222 \
      --tag-keys Department
  ```

  Perintah ini tidak menghasilkan output saat berhasil.

- AWS SDK: TagResourcedan UntagResource

Memindahkan akun ke OU atau antara akar dan OU

Ketika Anda masuk ke akun pengelolaan organisasi Anda, Anda dapat memindahkan akun di organisasi Anda dari akar ke OU, dari satu OU ke yang lain, atau kembali ke akar dari OU. Menempatkan akun di dalam OU membuatnya tunduk pada kebijakan yang dilampirkan pada OU

induk dan OU apa pun di induk rantai sampai ke akar. Jika akun tidak ada di OU, akun tersebut hanya tunduk pada kebijakan yang dilampirkan langsung ke akar dan kebijakan apa pun yang dilampirkan langsung ke akun. Untuk memindahkan akun, selesaikan langkah-langkah berikut.

> **Izin minimum**
>
> Untuk memindahkan akun ke lokasi baru di hirarki OU, Anda harus memiliki izin berikut:
>
> - `organizations:DescribeOrganization` – hanya diperlukan bila menggunakan konsol Organizations
> - `organizations:MoveAccount`

AWS Management Console

Untuk memindahkan beberapa akun ke OU

1. Masuklah ke konsolAWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada laman Akun AWS, temukan akun atau beberapa akun yang ingin Anda pindahkan. Anda dapat menavigasi hirarki OU atau mengaktifkan Melihat Akun AWS saja untuk melihat daftar datar akun tanpa struktur OU. Jika Anda memiliki banyak akun, Anda mungkin harus memilih Muat lebih banyak akun di 'ou-nama' di bagian bawah daftar untuk menemukan semua yang ingin Anda pindahkan.
3. Pilih
   ☑
   kotak centang di samping nama setiap akun yang ingin Anda pindahkan.
4. Pada menu Tindakan, di bawah Akun AWS, pilih Memindahkan.
5. Di kotak dialog Akun AWSPindahkan, navigasikan ke dan kemudian pilih OU atau akar yang akunnya ingin Anda pindahkan , dan kemudian pilih Akun AWSPindah.

AWS CLI & AWS SDKs

Untuk memindahkan sebuah akun ke OU

Anda dapat menggunakan salah satu perintah berikut untuk memindahkan akun:

- AWS CLI: move-account

  Contoh berikut memindahkan Akun AWS dari root ke OU. Perhatikan bahwa Anda harus menentukan ID dari wadah sumber dan tujuan kontainer.

  ```
  $ aws organizations move-account \
      --account-id 111122223333 \
      --source-parent-id r-a1b2 \
      --destination-parent-id ou-a1b2-f6g7h111
  ```

  Perintah ini tidak menghasilkan output saat berhasil.

- AWS SDK: MoveAccount

Menghapus OU

Saat masuk ke akun pengelolaan organisasi, Anda dapat menghapus OU yang tidak Anda perlukan lagi.

Anda harus terlebih dahulu memindahkan semua akun dari OU dan OU anak, dan kemudian Anda dapat menghapus OU anak.

> **Izin minimum**
>
> Untuk menghapus OU, Anda harus memiliki izin berikut:
>
> - `organizations:DescribeOrganization` – hanya diperlukan bila menggunakan konsol Organizations
> - `organizations:DeleteOrganizationalUnit`

AWS Management Console

Untuk menghapus OU

1. Masuklah ke konsolAWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.

2. Pada laman Akun AWS, temukan OU yang ingin Anda hapus dan pilih
   ☑
   kotak centang di samping nama masing-masing OU.
3. Pilih Tindakan, dan kemudian di bawah Unit organisasi, pilih Hapus.
4. Untuk mengonfirmasi bahwa Anda ingin menghapus OU, masukkan nama OU (jika Anda memilih untuk menghapus hanya satu) atau kata 'hapus' (jika Anda memilih lebih dari satu), dan lalu pilih Hapus.

   AWS Organizations menghapus OU dan menghapusnya dari daftar.

AWS CLI & AWS SDKs

Untuk menghapus OU

Anda dapat menggunakan perintah berikut untuk menghapus OU:

- AWS CLI: delete-organizational-unit

  Contoh berikut menunjukkan cara menghapus OU.

  ```
  $ aws organizations delete-organizational-unit \
      --organizational-unit-id ou-a1b2-f6g7h222
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWS SDK: DeleteOrganizationalUnit

Penandaan pada sumber daya AWS Organizations

Tag adalah label atribut khusus yang Anda tambahkan ke sumber daya AWS untuk membuatnya lebih mudah dalam melakukan identifikasi, pengelolaan, dan mencari sumber daya. Setiap tag memiliki dua bagian:

- Kunci tag (misalnya, `CostCenter`, `Environment`, atau `Project`). Kunci tag dapat memiliki panjang hingga 128 karakter dan peka huruf besar kecil.
- Nilai tag (misalnya, `111122223333` atau`Production`). Nilai tag dapat memiliki panjang hingga 256 karakter, dan seperti kunci tag, peka huruf besar kecil. Anda dapat mengatur nilai tanda menjadi sebuah string kosong, tetapi Anda tidak dapat mengatur nilai tanda menjadi nol. Mengabaikan nilai tag sama dengan menggunakan rangkaian kosong.

Untuk informasi lebih lanjut tentang karakter apa yang diizinkan dalam kunci atau nilai tag, lihat Parameter tag dari API Tag di Referensi API Penandaan Resource Groups.

Anda dapat menggunakan tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya. Untuk informasi selengkapnya, lihat Praktik Terbaik untuk Menandai AWS Sumber Daya.

> **Tip**
>
> Gunakan kebijakan tag untuk membantu menstandardisasi penerapan tag di seluruh sumber daya yang ada di akun organisasi Anda.

Saat ini, AWS Organizations men-support operasi penandaan berikut ketika Anda masuk ke akun pengelolaan:

- Anda dapat menambahkan tag ke sumber daya organisasi berikut:
  - Akun AWS
  - Unit organisasi
  - Root organisasi
  - Kebijakan

Anda dapat menambahkan tag pada waktu-waktu berikut:

- Saat Anda membuat sumber daya — Tentukan tag baik di konsol Organizations, atau gunakan parameter `Tags` dengan salah satu operasi API `Create`. Hal ini tidak berlaku untuk root organisasi.
- Setelah Anda membuat sumber daya — Gunakan konsol Organizations, atau panggil operasi `TagResource`.

Anda dapat melihat tag pada salah satu sumber daya yang bisa ditandai di AWS Organizations dengan menggunakan konsol atau dengan memanggil operasi `ListTagsForResource`.

Anda dapat menghapus tag dari sebuah sumber daya dengan menentukan kunci yang akan dihapus dengan menggunakan konsol atau dengan memanggil operasi `UntagResource`.

Menggunakan tanda

Tag membantu Anda mengatur sumber daya di organisasi Anda dengan memungkinkan Anda mengelompokkannya berdasarkan kategori apa pun yang berguna bagi Anda. Misalnya, Anda dapat menetapkan tag "Departemen" yang melacak departemen yang memiliki. Anda dapat menetapkan tag "Lingkungan" untuk melacak apakah sumber daya tertentu merupakan bagian dari lingkungan alfa, beta, gamma, atau lingkungan produksi Anda.

Anda juga dapat menggunakan tag untuk:

- Menegakkan standar penandaan pada sumber daya Anda.
- Kontrol siapa yang dapat mengakses sumber daya Anda.

Menambahkan, memperbarui, dan menghapus tag

Saat Anda masuk ke akun pengelolaan organisasi Anda, Anda dapat menambahkan tag ke sumber daya yang ada di organisasi Anda.

Menambahkan tanda ke sumber daya saat Anda membuatnya

> **Izin minimum**
>
> Untuk menambahkan tanda ke sebuah sumber daya saat Anda membuatnya, Anda memerlukan izin berikut:

- Izin untuk membuat sumber daya dengan jenis tertentu
- `organizations:TagResource`
- `organizations:ListTagsForResource` — hanya diperlukan bila menggunakan konsol Organizations

Anda dapat menyertakan kunci dan nilai-nilai tag yang dilampirkan pada sumber daya berikut saat Anda membuatnya.

- Akun AWS
  - Akun yang dibuat
  - Akun yang diundang
- Unit organisasi (OU)
- Kebijakan
  - Kebijakan opt-out layanan AI
  - Kebijakan Backup
  - Kebijakan kontrol layanan
  - Kebijakan tag

Root organisasi dibuat ketika awal Anda membuat organisasi, sehingga Anda hanya dapat menambahkan tag padanya sebagai sumber daya yang ada.

Menambahkan atau memperbarui tag untuk sumber daya yang ada

Anda juga dapat menambahkan tag baru atau memperbarui nilai tag yang dilampirkan pada sumber daya yang ada.

Izin minimum

Untuk menambah atau memperbarui tag ke sumber daya yang ada di organisasi Anda, Anda memerlukan izin berikut:

- `organizations:TagResource`
- `organizations:ListTagsForResource` — hanya diperlukan bila menggunakan konsol Organizations

Untuk menghapus tag dari sumber daya yang ada di organisasi Anda, Anda memerlukan izin berikut:

- `organizations:UntagResource`

AWS Management Console

Untuk menambahkan, memperbarui, atau menghapus tag untuk sumber daya yang ada

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Arahkan ke dan pilih akun, Root, OU, atau kebijakan, dan klik namanya untuk membuka halaman detailnya.
3. Di bagian tab Tanda, pilih Kelola tanda.
4. Anda dapat menambahkan tag baru, mengubah nilai tag yang ada, atau menghapus tag.

   Untuk menambahkan tag, pilih Tambahkan tag, dan masukkan Kunci, dan secara opsional, Nilai untuk tag tersebut.

   Untuk menghapus sebuah tag, pilih Hapus.

   Kunci dan nilai tag sensitif huruf besar dan kecil. Gunakan kapitalisasi yang ingin Anda standarisasi. Anda juga harus mematuhi setiap persyaratan kebijakan tag yang berlaku.
5. Ulangi langkah-langkah sebelumnya sebanyak yang Anda butuhkan.
6. Pilih Simpan perubahan.

AWS CLI & AWS SDKs

Menambahkan atau memperbarui tag untuk sumber daya yang ada

Anda dapat menggunakan salah satu perintah berikut untuk menambahkan tag ke sumber daya yang dapat diberi tag dalam organisasi Anda:

- AWS CLI: tag-resource
- AWSSDK: TagResource

Untuk menghapus tag dari sumber daya yang ada di organisasi Anda

Anda dapat menggunakan salah satu perintah berikut untuk menghapus tag:

- AWS CLI: untag-resource
- AWSSDK: UntagResource

Menggunakan AWS Organizations dengan layanan AWS lainnya

Anda dapat menggunakan akses terpercaya untuk mengaktifkan layanan AWS yang Anda tentukan, yang disebut Layanan terpercaya, untuk melakukan tugas di organisasi Anda dan akunnya atas nama Anda. Ini melibatkan pemberian izin ke layanan tepercaya tetapi tidak memengaruhi izin untuk pengguna atau peran. Bila Anda mengaktifkan akses, layanan terpercaya dapat membuat IAM role yang disebut Peran yang terhubung dengan layanan di setiap akun di organisasi Anda kapan pun peran tersebut diperlukan. Peran tersebut memiliki kebijakan izin yang memungkinkan layanan terpercaya untuk melakukan tugas-tugas yang dijelaskan dalam layanan dokumentasi. Hal ini memungkinkan Anda untuk menentukan pengaturan dan rincian konfigurasi yang Anda ingin layanan terpercaya tersebut untuk mempertahankan akun organisasi Anda atas nama Anda. Layanan terpercaya hanya menciptakan peran terkait layanan ketika diperlukan untuk melakukan tindakan pengelolaan pada akun, dan tidak harus di semua akun organisasi.

Important

Kami sangat menyarankan bahwa, ketika opsi tersedia, Anda mengaktifkan dan menonaktifkan akses tepercaya dengan hanya menggunakan konsol layanan tepercaya, atau setara operasi API AWS CLI atau API. Hal ini memungkinkan layanan terpercaya melakukan inisialisasi yang diperlukan ketika mengaktifkan akses terpercaya, seperti membuat sumber daya yang diperlukan dan setiap pembersihan sumber daya yang diperlukan ketika menonaktifkan akses terpercaya.

Untuk informasi tentang cara mengaktifkan atau menonaktifkan akses layanan terpercaya ke organisasi Anda menggunakan layanan terpercaya, lihat Pelajari selengkapnya tautan di bawah kolom Mendukung Akses Tepercaya di AWS Layanan yang dapat Anda gunakan dengan AWS Organizations.

Jika Anda menonaktifkan akses dengan menggunakan konsol Organizations, perintah CLI, atau operasi API, hal ini menyebabkan tindakan berikut terjadi:

- Layanan tidak lagi dapat membuat peran yang terkait dengan layanan dalam akun di organisasi Anda. Ini berarti bahwa layanan tersebut tidak dapat menjalankan operasi atas nama Anda pada akun baru apa pun di organisasi Anda. Layanan masih dapat melakukan operasi di akun lama sampai layanan menyelesaikan pembersihannya dari AWS Organizations.

- Layanan tidak lagi dapat melakukan tugas di akun anggota dalam organisasi, kecuali operasi tersebut secara eksplisit diizinkan oleh kebijakan IAM yang dilampirkan pada peran Anda. Ini mencakup agregasi data apa pun dari akun anggota ke akun manajemen, atau ke sebuah akun administrator yang didelegasikan, jika relevan.
- Beberapa layanan mendeteksi ini dan membersihkan data atau sumber daya yang tersisa yang terkait dengan integrasi, sementara layanan lain berhenti mengakses organisasi tetapi meninggalkan data riwayat dan konfigurasi apa pun di tempat untuk mendukung kemungkinan pengaktifan kembali integrasi.

Sebaliknya, menggunakan konsol layanan lain atau perintah untuk menonaktifkan integrasi memastikan bahwa layanan lain dapat membersihkan sumber daya yang diperlukan hanya untuk integrasi. Bagaimana layanan membersihkan sumber daya dalam akun organisasi tergantung pada layanan tersebut. Untuk informasi lebih lanjut, lihat dokumentasi untuk layanan AWS lain.

Izin yang diperlukan untuk mengaktifkan akses terpercaya

Akses terpercaya memerlukan izin untuk dua layanan: AWS Organizations dan layanan terpercaya. Untuk mengaktifkan akses terpercaya, pilih salah satu skenario berikut ini:

- Jika Anda memiliki kredensial dengan izin di kedua AWS Organizations dan layanan terpercaya, aktifkan akses dengan menggunakan alat (konsol atau AWS CLI) yang disediakan oleh layanan terpercaya. Hal ini memungkinkan layanan untuk mengaktifkan akses terpercaya di AWS Organizations atas nama Anda dan untuk membuat sumber daya apa pun yang diperlukan agar layanan dapat beroperasi di organisasi Anda.

  Izin minimum untuk kredensial ini adalah sebagai berikut:

  - `organizations:EnableAWSServiceAccess`. Anda juga dapat menggunakan kunci kondisi `organizations:ServicePrincipal` dengan operasi ini untuk membatasi permintaan yang operasi tersebut membuat daftar nama utama layanan disetujui. Untuk informasi lebih lanjut, lihat Kunci syarat.
  - `organizations:ListAWSServiceAccessForOrganization` — Yang diperlukan jika Anda menggunakan konsol AWS Organizations.
  - Izin minimum yang diperlukan oleh layanan terpercaya tergantung pada layanan. Untuk informasi lebih lanjut, lihat dokumentasi layanan terpercaya.

- Jika satu orang memiliki kredensial dengan izin di AWS Organizations tetapi orang lain memiliki mandat dengan izin di layanan terpercaya, lakukan langkah-langkah berikut dalam urutan berikut:

  1. Orang yang memiliki mandat dengan izin di AWS Organizations harus menggunakan konsol AWS Organizations, AWS CLI, atau SDK AWS untuk mengaktifkan akses terpercaya untuk layanan terpercaya. Ini memberikan izin ke layanan lain untuk melakukan konfigurasi yang diperlukan dalam organisasi ketika langkah berikut (langkah 2) dilakukan.

     Izin AWS Organizations minimum adalah sebagai berikut:

     - `organizations:EnableAWSServiceAccess`
     - `organizations:ListAWSServiceAccessForOrganization` — Yang diperlukan hanya jika Anda menggunakan konsol AWS Organizations

     Untuk langkah-langkah untuk mengaktifkan akses terpercaya di AWS Organizations, lihat Bagaimana mengaktifkan atau menonaktifkan akses terpercaya.

  2. Orang yang memiliki mandat dengan izin dalam layanan terpercaya memungkinkan bahwa layanan untuk bekerja dengan AWS Organizations. Ini menginstruksikan layanan untuk melakukan inisialisasi yang diperlukan, seperti membuat sumber daya yang diperlukan untuk layanan terpercaya untuk beroperasi dalam organisasi. Untuk informasi lebih lanjut, lihat instruksi khusus layanan di AWS Layanan yang dapat Anda gunakan dengan AWS Organizations.

Izin yang diperlukan untuk menonaktifkan akses terpercaya

Bila Anda tidak lagi ingin mengizinkan layanan terpercaya beroperasi pada organisasi Anda atau akunnya, pilih salah satu skenario berikut ini.

> **Important**
>
> Menonaktifkan akses layanan terpercaya tidak mencegah pengguna dan peran dengan izin yang sesuai dari penggunaan layanan tersebut. Untuk sepenuhnya memblokir pengguna dan peran dari mengakses AWS layanan, Anda dapat menghapus izin IAM yang memberikan akses tersebut, atau Anda dapat menggunakan kebijakan kontrol layanan (SCP) di. AWS Organizations
> Anda dapat menerapkan SCP hanya ke akun anggota. SCP tidak berlaku untuk akun manajemen. Kami menyarankan Anda untuk tidak menjalankan layanan di akun manajemen.

Sebagai gantinya, jalankan di akun anggota tempat Anda dapat mengontrol keamanan dengan menggunakan SCP.

- Jika Anda memiliki kredensial dengan izin di kedua AWS Organizations dan layanan terpercaya, nonaktifkan akses dengan menggunakan alat (konsol atau AWS CLI) yang disediakan oleh layanan terpercaya. Layanan kemudian membersihkan dengan menghapus sumber daya yang tidak lagi diperlukan dan dengan menonaktifkan akses terpercaya untuk layanan di AWS Organizations atas nama Anda.

  Izin minimum untuk kredensial ini adalah sebagai berikut:

  - `organizations:DisableAWSServiceAccess`. Anda juga dapat menggunakan kunci kondisi `organizations:ServicePrincipal` dengan operasi ini untuk membatasi permintaan yang operasi tersebut membuat daftar nama utama layanan disetujui. Untuk informasi lebih lanjut, lihat Kunci syarat.
  - `organizations:ListAWSServiceAccessForOrganization` — Yang diperlukan jika Anda menggunakan konsol AWS Organizations.
  - Izin minimum yang diperlukan oleh layanan terpercaya tergantung pada layanan. Untuk informasi lebih lanjut, lihat dokumentasi layanan terpercaya.
- Jika kredensials dengan izin di AWS Organizations bukan kredensial dengan izin di layanan terpercaya, lakukan langkah-langkah berikut dalam urutan sebagai berikut:
  1. Orang dengan izin di layanan terpercaya pertama menonaktifkan akses menggunakan layanan tersebut. Ini menginstruksikan layanan terpercaya untuk membersihkan dengan menghapus sumber daya yang diperlukan untuk akses terpercaya. Untuk informasi lebih lanjut, lihat instruksi khusus layanan di AWS Layanan yang dapat Anda gunakan dengan AWS Organizations.
  2. Orang dengan izin di AWS Organizations kemudian dapat menggunakan konsol AWS Organizations, AWS CLI, atau SDK AWS untuk menonaktifkan akses untuk layanan terpercaya. Ini akan menghapus izin untuk layanan terpercaya dari organisasi dan akunnya.

     Izin AWS Organizations minimum adalah sebagai berikut:

     - `organizations:DisableAWSServiceAccess`
     - `organizations:ListAWSServiceAccessForOrganization` — Yang diperlukan hanya jika Anda menggunakan konsol AWS Organizations

     Untuk langkah-langkah untuk menonaktifkan akses terpercaya di AWS Organizations, lihat Bagaimana mengaktifkan atau menonaktifkan akses terpercaya.

Bagaimana mengaktifkan atau menonaktifkan akses terpercaya

Jika Anda memiliki izin hanya untuk AWS Organizations dan Anda ingin mengaktifkan atau menonaktifkan akses terpercaya ke organisasi Anda atas nama administrator layanan AWS, gunakan prosedur berikut.

Important

Kami sangat menyarankan bahwa, ketika opsi tersedia, Anda mengaktifkan dan menonaktifkan akses tepercaya dengan hanya menggunakan konsol layanan tepercaya, atau setara operasi API AWS CLI atau API. Hal ini memungkinkan layanan terpercaya melakukan inisialisasi yang diperlukan ketika mengaktifkan akses terpercaya, seperti membuat sumber daya yang diperlukan dan setiap pembersihan sumber daya yang diperlukan ketika menonaktifkan akses terpercaya.

Untuk informasi tentang cara mengaktifkan atau menonaktifkan akses layanan terpercaya ke organisasi Anda menggunakan layanan terpercaya, lihat Pelajari selengkapnya tautan di bawah kolom Mendukung Akses Tepercaya di AWS Layanan yang dapat Anda gunakan dengan AWS Organizations.

Jika Anda menonaktifkan akses dengan menggunakan konsol Organizations, perintah CLI, atau operasi API, hal ini menyebabkan tindakan berikut terjadi:

- Layanan tidak lagi dapat membuat peran yang terkait dengan layanan dalam akun di organisasi Anda. Ini berarti bahwa layanan tersebut tidak dapat menjalankan operasi atas nama Anda pada akun baru apa pun di organisasi Anda. Layanan masih dapat melakukan operasi di akun lama sampai layanan menyelesaikan pembersihannya dari AWS Organizations.
- Layanan tidak lagi dapat melakukan tugas di akun anggota dalam organisasi, kecuali operasi tersebut secara eksplisit diizinkan oleh kebijakan IAM yang dilampirkan pada peran Anda. Ini mencakup agregasi data apa pun dari akun anggota ke akun manajemen, atau ke sebuah akun administrator yang didelegasikan, jika relevan.
- Beberapa layanan mendeteksi ini dan membersihkan data atau sumber daya yang tersisa yang terkait dengan integrasi, sementara layanan lain berhenti mengakses organisasi tetapi meninggalkan data riwayat dan konfigurasi apa pun di tempat untuk mendukung kemungkinan pengaktifan kembali integrasi.

Sebaliknya, menggunakan konsol layanan lain atau perintah untuk menonaktifkan integrasi memastikan bahwa layanan lain dapat membersihkan sumber daya yang diperlukan hanya

untuk integrasi. Bagaimana layanan membersihkan sumber daya dalam akun organisasi tergantung pada layanan tersebut. Untuk informasi lebih lanjut, lihat dokumentasi untuk layanan AWS lain.

AWS Management Console

Bagaimana mengaktifkan akses layanan terpercaya

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk layanan yang ingin Anda aktifkan, dan pilih namanya.
3. Pilih Aktifkan akses terpercaya.
4. Di kotak dialog konfirmasi, centang kotak untuk Menampilkan opsi untuk mengaktifkan akses terpercaya, masukkan **`enable`** dalam kotak, dan kemudian pilih Aktifkan akses terpercaya.
5. Jika Anda mengaktifkan akses, beritahu administrator layanan AWS yang lain bahwa mereka sekarang dapat mengaktifkan layanan lain untuk bekerja dengan AWS Organizations.

Cara menonaktifkan akses layanan terpercaya

1. Masuk ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk layanan yang ingin Anda menonaktifkan, dan pilih namanya.
3. Tunggu sampai administrator layanan lain memberitahu Anda bahwa layanan dinonaktifkan dan bahwa sumber dayanya telah dibersihkan.
4. Di kotak dialog konfirmasi, masukkan **`disable`** dalam kotak, dan kemudian pilih Menonaktifkan akses terpercaya.

AWS CLI, AWS API

Untuk mengaktifkan atau menonaktifkan akses terpercaya

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk mengaktifkan atau menonaktifkan akses layanan terpercaya:

- AWS CLI: AWS organisasi enable-aws-service-access
- AWS CLI: AWS organisasi disable-aws-service-access
- AWSAPI: Aktifkan AWSServiceAccess
- AWSAPI: Nonaktifkan AWSServiceAccess

AWS Organizations dan peran tertaut layanan

AWS Organizations menggunakan Peran yang terhubung dengan IAM untuk mengaktifkan layanan terpercaya untuk melakukan tugas atas nama Anda di akun anggota organisasi Anda. Bila Anda mengonfigurasi layanan terpercaya dan memberikan otorisasi kepadanya untuk diintegrasikan dengan organisasi Anda, layanan tersebut dapat meminta AWS Organizations membuat peran tertaut layanan di akun anggotanya. Layanan tepercaya melakukan ini secara asinkron sesuai kebutuhan dan tidak harus di semua akun di organisasi secara bersamaan. Peran tertaut layanan memiliki izin IAM yang telah ditetapkan sebelumnya yang memungkinkan layanan terpercaya untuk melakukan hanya tugas tertentu dalam akun tersebut. Secara umum, AWS mengelola semua peran tertaut layanan, yang berarti bahwa Anda biasanya tidak dapat mengubah peran atau kebijakan yang dilampirkan.

Agar semua ini dapat dilakukan, bila Anda membuat akun di organisasi atau menerima undangan untuk bergabung dengan akun yang ada ke organisasi, AWS Organizations ketentuan akun anggota dengan peran tertaut layanan yang bernama `AWSServiceRoleForOrganizations`. Hanya layanan AWS Organizations itu sendiri dapat mengambil peran ini. Peran tersebut memiliki izin yang memungkinkan AWS Organizations untuk membuat peran tertaut layanan untuk layanan AWS. Peran tertaut layanan ini hadir di semua organisasi.

Meskipun kami tidak merekomendasikannya, jika organisasi Anda hanya telah mengaktifkan fitur penagihan gabungan, peran tertaut layanan yang bernama `AWSServiceRoleForOrganizations` tidak pernah digunakan, dan Anda dapat menghapusnya. Jika nanti Anda ingin mengaktifkan semua fitur di organisasi Anda, peran tersebut diperlukan, dan Anda harus memulihkannya. Pemeriksaan berikut terjadi ketika Anda memulai proses untuk mengaktifkan semua fitur:

- Untuk setiap akun anggota yang diundang untuk bergabung organisasi — Administrator akun menerima permintaan untuk menyetujui untuk mengaktifkan semua fitur. Agar berhasil menyetujui permintaan tersebut, administrator harus memiliki kedua izin

`organizations:AcceptHandshake` dan `iam:CreateServiceLinkedRole` jika peran yang ditautkan dengan layanan (`AWSServiceRoleForOrganizations`) belum ada. Jika peran `AWSServiceRoleForOrganizations` sudah ada, administrator hanya membutuhkan izin `organizations:AcceptHandshake` untuk menyetujui permintaan tersebut. Ketika administrator menyetujui permintaan tersebut, AWS Organizations membuat peran tertaut layanan jika belum ada.

- Untuk setiap akun anggota yang dibuat dalam organisasi — Administrator akun menerima permintaan untuk membuat ulang peran tertaut layanan tersebut. (Administrator akun anggota tidak menerima permintaan untuk mengaktifkan semua fitur karena administrator akun manajemen (sebelumnya dikenal sebagai "akun master") dianggap sebagai pemilik akun anggota yang dibuat.) AWS Organizations membuat peran tertaut layanan ketika administrator akun anggota menyetujui permintaan tersebut. Administrator harus memiliki kedua izin `organizations:AcceptHandshake` dan `iam:CreateServiceLinkedRole` untuk berhasil menerima jabat tangan.

Setelah Anda mengaktifkan semua fitur di organisasi Anda, Anda tidak lagi dapat menghapus peran tertaut layanan `AWSServiceRoleForOrganizations` dari akun mana pun.

> **Important**
>
> SCP AWS Organizations tidak pernah mempengaruhi peran tertaut layanan. Peran ini dibebaskan dari pembatasan SCP.

AWS Layanan yang dapat Anda gunakan dengan AWS Organizations

Dengan AWS Organizations Anda dapat melakukan aktivitas manajemen akun dalam skala besar dengan mengkonsolidasikan beberapa Akun AWS ke dalam satu organisasi. Mengkonsolidasikan akun menyederhanakan cara Anda menggunakan layanan lain AWS . Anda dapat memanfaatkan layanan manajemen multi-akun yang tersedia AWS Organizations dengan AWS layanan tertentu untuk melakukan tugas di semua akun yang menjadi anggota organisasi Anda.

Tabel berikut mencantumkan AWS layanan yang dapat Anda gunakan AWS Organizations, dan manfaat menggunakan setiap layanan pada tingkat organisasi.

Akses tepercaya — Anda dapat mengaktifkan AWS layanan yang kompatibel untuk melakukan operasi Akun AWS di semua organisasi Anda. Untuk informasi selengkapnya, lihat Menggunakan AWS Organizations dengan layanan AWS lainnya.

Administrator yang didelegasikan untuk AWS AWS layanan — Layanan yang kompatibel dapat mendaftarkan akun AWS anggota di organisasi sebagai administrator untuk akun organisasi dalam layanan tersebut. Untuk informasi selengkapnya, lihat Administrator yang didelegasikan untuk AWS layanan yang bekerja dengan Organisasi.

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
AWS Account Management Kelola detail dan metadata untuk semua untuk organisasi Akun AWS Anda.	Anda dapat membuat, memperbarui, dan menghapus informasi kontak alternatif untuk semua akun di organisasi Anda.	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya	
AWS Application Migration Service AWS Application Migration	Anda dapat mengelola migrasi skala	 Ya	 Ya Pelajari selengkapnya	

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
Service memungkinkan perusahaan untuk lift-and-shift ke AWS sejumlah besar server fisik, virtual, atau cloud tanpa masalah kompatibilitas, gangguan kinerja, atau jendela cutover yang panjang.	besar di beberapa akun.	Pelajari selengkapnya		
AWS Artifact Unduh laporan kepatuhan AWS keamanan seperti laporan ISO dan PCI.	Anda dapat menerima perjanjian atas nama semua akun dalam organisasi Anda.	 Ya Pelajari selengkapnya	 Tidak	

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
AWS Audit Manager Otomatiskan koleksi bukti yang berkelanjutan untuk membantu Anda meng-audit penggunaan layanan cloud Anda.	Terus audit AWS penggunaan Anda di beberapa akun di organisasi Anda untuk menyederhanakan cara Anda menilai risiko dan kepatuhan.	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya	

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan
AWS Backup Kelola dan pantau backup di semua akun di organisasi Anda.	Anda dapat mengonfigurasi dan mengelola paket backup untuk seluruh organisasi, atau untuk grup akun di unit organisasi (OU). Anda dapat secara terpusat memantau backup untuk semua akun Anda.	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan
AWS Billing and Cost Management Memberikan ikhtisar data manajemen keuangan AWS cloud Anda dan untuk membantu Anda membuat keputusan yang lebih cepat dan lebih tepat.	Memungkinkan data alokasi biaya terpisah untuk mengambil AWS Organizations informasi, jika berlaku, dan mengumpulkan data telemetri untuk layanan data alokasi biaya terpisah yang telah Anda pilih.	 Ya Pelajari selengkapnya	 Tidak

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
	Untuk informasi lebih lanjut, lihat Apa itu AWS Billing and Cost Management? dalam panduan pengguna Billing and Cost Management.			

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
AWS CloudFormation Stackset Buat, perbarui, atau hapus tumpukan di beberapa akun dan Wilayah dengan satu operasi.	Pengguna di akun pengelolaan atau akun administrator yang didelegasikan dapat membuat set tumpukan dengan izin terkelola layanan yang men-deploy instans tumpukan ke akun di organisasi Anda.	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya	

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
AWS CloudTrail Aktifkan tata kelola, kepatuhan, serta audit operasional dan risiko akun Anda.	Pengguna di akun manajemen atau akun administrator yang didelegasikan dapat membuat jejak organisasi atau penyimpanan data peristiwa yang mencatat semua peristiwa untuk semua akun di organisasi.	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya	

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan
AWS Compute Optimizer Dapatkan rekomendasi pengoptimalan AWS komputasi.	Anda dapat menganalisis semua sumber daya yang ada di akun organisasi Anda untuk mendapatkan rekomendasi optimalisasi. Untuk informasi selengkapnya, lihat Akun yang Didukung oleh Compute Optimizer di	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
	Panduan Pengguna AWS Compute Optimizer.			

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan
AWS Config Nilai, audit, dan evaluasi konfigurasi sumber daya AWS Anda.	Anda bisa mendapatkan tampilan status kepatuhan di seluruh organisasi. Anda juga dapat menggunakan operasi AWS Config API untuk mengelola AWS Config aturan dan paket kesesuaian Akun AWS di seluruh organisasi Anda.	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya: Aturan Config Paket kesesuaian Agregasi data multi-wilayah multi-akun

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
	Anda dapat menggunakan akun administrator yang didelegasikan untuk mengumpulkan data konfigurasi dan kepatuhan sumber daya dari semua akun anggota organisasi di AWS Organizations. Untuk informasi selengkapnya, lihat Daftarkan administrator yang			

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
	didelegasikan di Panduan Developer AWS Config .			

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan
AWS Control Tower Siapkan dan atur sebuah lingkungan AWS multi-akun yang patuh dan aman.	Anda dapat mengatur landing zone, lingkungan multi-akun untuk semua AWS sumber daya Anda. Lingkungan ini mencakup organisasi dan entitas organisasi. Anda dapat menggunakan lingkungan ini untuk menegakka	 Ya Pelajari selengkapnya	 Tidak

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
	n peraturan kepatuhan pada semua Anda Akun AWS. Untuk informasi selengkapnya, lihat Cara AWS Control Tower dan Kelola Akun Melalui AWS Organizations di Panduan AWS Control Tower Pengguna.			

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan
Hub Optimisasi Biaya AWS Kumpulkan rekomendasi biaya di seluruh produk AWS pengoptimalan.	Anda dapat dengan mudah mengidentifikasi, memfilter, dan mengumpulkan rekomendasi pengoptimalan AWS biaya di seluruh akun AWS Organizations anggota dan AWS Wilayah Anda. Untuk informasi selengkapnya, lihat	 Ya Pelajari lebih lanjut	 Tidak

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
	Pusat Pengoptimalan Biaya di panduan pengguna Hub Pengoptimalan Biaya.			

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
Detektif Amazon Hasilkan visualisasi dari data log Anda untuk menganalisis, menyelidiki, dan dengan cepat mengidentifikasi akar penyebab temuan keamanan atau aktivitas yang mencurigakan.	Anda dapat mengintegrasikan Amazon Detective AWS Organizations untuk memastikan bahwa grafik perilaku Detektif Anda memberikan visibilitas ke dalam aktivitas untuk semua akun organisasi Anda.	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya	

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan
DevOpsGuru Amazon Menganalisis data operasional dan metrik aplikasi dan peristiwa untuk mengidentifikasi perilaku yang menyimpang dari pola operasi normal. Pengguna diberi tahu ketika DevOps Guru mendeteksi masalah operasional atau risiko.	Anda dapat mengintegrasikan dengan AWS Organizations mengelola wawasan dari semua akun di seluruh organisasi Anda. Anda mendelegasikan administrator untuk melihat, mengurutkan, dan memfilter wawasan dari semua	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
	akun untuk mendapatkan kesehatan seluruh organisasi dari semua aplikasi yang dipantau.			

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan
AWS Directory Service Siapkan dan jalankan direktori di AWS Cloud atau sambungkan AWS sumber daya Anda dengan Microsoft Active Directory lokal yang ada.	Anda dapat mengintegrasikan AWS Directory Service dengan AWS Organizations berbagi direktori tanpa batas di beberapa akun dan VPC apa pun di Wilayah.	 Ya Pelajari selengkapnya	 Tidak

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
Amazon EventBridge Pantau AWS sumber daya Anda dan aplikasi yang Anda jalankan AWS secara real time.	Anda dapat mengaktifkan berbagi semua EventBridge acara Amazon, sebelumnya Amazon CloudWatch Events, di semua akun di organisasi Anda. Untuk informasi selengkapnya, lihat Mengirim dan menerima EventBridge peristiwa Amazon	 Tida	 Tidak	

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
	antara Akun AWS di Panduan EventBridge Pengguna Amazon.			
AWS Firewall Manager Konfigurasikan dan kelola aturan firewall untuk aplikasi web di seluruh akun dan aplikasi Anda secara terpusat.	Anda dapat mengonfigurasi dan mengelola AWS WAF aturan secara terpusat di seluruh akun di organisasi Anda.	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya	

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
Amazon GuardDuty GuardDuty adalah layanan pemantauan keamanan berkelanjutan yang menganalisis dan memproses informasi dari berbagai sumber data. Ini menggunakan umpan intelijen ancaman dan machine learning untuk mengidentifikasi aktivitas yang tidak terduga dan berpotensi tidak sah dan berbahaya dalam	Anda dapat menunjuk akun anggota untuk melihat dan mengelola GuardDuty semua akun di organisasi Anda. Menambahkan akun anggota secara otomatis memungkinkan GuardDuty akun-akun tersebut di yang dipilih Wilayah	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya	

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
lingkungan AWS .	AWS. Anda juga dapat mengotomatiskan GuardDuty aktivasi untuk akun baru yang ditambahkan ke organisasi Anda. Untuk informasi selengkapnya, lihat GuardDuty dan Organizations di Panduan GuardDuty Pengguna Amazon.			

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
AWS Health Dapatkan visibilitas ke peristiwa yang mungkin memengaruhi kinerja sumber daya atau masalah ketersediaan untuk AWS layanan.	Anda dapat menggabungkan AWS Health peristiwa di seluruh akun di organisasi Anda.	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya	

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
AWS Identity and Access Management Kontrol akses ke AWS sumber daya dengan aman.	Anda dapat menggunakan data yang terakhir diakses dengan layanan di IAM untuk membantu Anda lebih memahami aktivitas AWS di seluruh organisasi Anda. Anda dapat menggunakan data ini untuk membuat dan memperbarui	 Tida	 Tidak	

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
	Kebijakan Kontrol Layanan (SCP) yang membatasi akses ke hanya AWS yang digunakan akun organisasi Anda. Sebagai contoh, lihat Menggunakan Data untuk Memperbaiki Izin untuk Unit Organisasi di Panduan Pengguna IAM.			

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan
Penganalisis Akses IAM Analisis kebijakan berbasis sumber daya di AWS lingkungan Anda untuk mengidentifikasi kebijakan apa pun yang memberikan akses ke prinsipal di luar zona kepercayaan Anda.	Anda dapat menetapkan akun anggota untuk menjadi administrator untuk Penganalisis Akses IAM. Untuk informasi lebih lanjut, lihat Mengaktifkan Penganalisis Akses di Panduan Pengguna IAM.	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
Amazon Inspector Secara otomatis memindai AWS beban kerja Anda untuk mencari kerentanan untuk menemukan instans Amazon EC2 dan gambar kontainer yang berada di Amazon ECR untuk mencari kerentanan perangkat lunak dan paparan jaringan yang tidak diinginkan.	Delegasikan administrator untuk mengaktifkan atau menonaktifkan pemindaian akun anggota, melihat data temuan gabungan dari seluruh organisasi, membuat dan mengelola aturan penindasan. Untuk informasi selengkap	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya	

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
	nya, lihat Mengelola beberapa akun dengan AWS Organizations di Panduan Pengguna Amazon Inspector.			
AWS License Manager Sederhanakan proses membawa lisensi perangkat lunak ke cloud.	Anda dapat mengaktifkan penemuan lintas akun sumber daya komputasi di seluruh organisasi Anda.	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya	

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
Amazon Macie Menemukan dan mengklasifikasikan konten penting bisnis Anda menggunakan machine learning untuk membantu Anda memenuhi persyaratan keamanan dan privasi data. Ini terus mengevaluasi konten Anda yang disimpan di Amazon S3 dan memberitahu Anda tentang potensi masalah.	Anda dapat mengonfigurasi Amazon Macie untuk semua akun di organisasi Anda untuk mendapatkan tampilan konsolidasi semua data Anda di Amazon S3, di semua akun dari akun administrator Macie yang	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya	

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
	ditunjuk. Anda dapat mengonfigurasi Macie untuk secara otomatis melindungi sumber daya di akun baru seiring pertumbuhan organisasi Anda. Anda diberi tahu untuk memulihkan kebijakan misconfiguration di S3 bucket di seluruh			

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan
	organisasi Anda.		
AWS Marketplace Katalog digital yang dikurasi yang dapat Anda gunakan untuk menemukan, membeli, menyebarkan, dan mengelola perangkat lunak, data, dan layanan pihak ketiga yang Anda butuhkan untuk membangun solusi dan menjalankan bisnis Anda.	Anda dapat membagikan lisensi untuk AWS Marketplace langganan dan pembelian di seluruh akun di organisasi Anda.	 Ya Pelajari selengkapnya	 Tidak

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
AWS Marketplace Marketplace Pribadi Memberi Anda katalog luas produk yang tersedia di AWS Marketplace, bersama dengan kontrol spesifik produk tersebut.	Memungkinkan Anda membuat beberapa pengalaman pasar pribadi yang terkait dengan seluruh organisasi Anda, satu atau lebih OU, atau satu atau beberapa akun di organisasi Anda, masing-masing dengan rangkaian produk yang disetujui	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya	

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
	sendiri. AWS Administrator Anda juga dapat menerapkan branding perusahaan ke setiap pengalaman pasar pribadi dengan logo, pesan, dan skema warna perusahaan atau tim Anda.			

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan
AWS Manajer Jaringan Memungkinkan Anda mengelola jaringan inti AWS Cloud WAN dan jaringan AWS Transit Gateway secara terpusat di seluruh AWS akun, Wilayah, dan lokasi lokal.	Anda dapat mengelola dan memantau jaringan global Anda secara terpusat dengan gateway transit dan sumber daya terlampirnya di beberapa AWS akun dalam organisasi Anda.	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
Pengembang Amazon Q Amazon Q Developer adalah asisten percakapan yang didukung kecerdasan buatan (AI) generatif yang dapat membantu Anda memahami, membangun, memperluas, dan mengoperasikan AWS aplikasi.	Versi langganan berbayar Amazon Q Developer memerlukan integrasi Organizations.	 Ya Pelajari selengkapnya	 Tidak	

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan
AWS Resource Access Manager Bagikan AWS sumber daya tertentu yang Anda miliki dengan akun lain.	Anda dapat berbagi sumber daya dalam organisasi Anda tanpa bertukar undangan tambahan. Sumber daya yang dapat Anda bagikan meliputi Aturan Route 53 Resolver, pencadangan kapasitas sesuai permintaan, dan	 Ya Pelajari selengkapnya	 Tidak

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
	banyak lagi. Untuk informasi tentang pencadangan kapasitas berbagi, lihat Panduan Pengguna Amazon EC2 untuk Instans Linux atau Panduan Pengguna Amazon EC2 untuk Instans Windows. Untuk daftar			

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
	sumber daya yang dapat dibagikan, lihat Sumber Daya yang dapat dibagikan di Panduan Pengguna AWS RAM .			
Penjelajah Sumber Daya AWS Jelajahi sumber daya Anda menggunakan pengalaman seperti mesin pencari internet.	Aktifkan pencarian multi-akun.	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya	

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan
AWS Security Hub Lihat status keamanan Anda AWS dan periksa lingkungan Anda terhadap standar industri keamanan dan praktik terbaik.	Anda dapat secara otomatis mengaktifkan Security Hub untuk semua akun organisasi Anda, termasuk akun baru saat mereka ditambahkan. Hal ini meningkatkan cakupan pemeriksaan dan temuan Security Hub, yang memberikan	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
	gambaran yang lebih akurat tentang keseluruhan postur keamanan Anda.			

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
Lensa Penyimpanan Amazon S3 Dapatkan visibilitas metrik penggunaan dan aktivitas penyimpanan Amazon S3 Anda dengan rekomendasi yang dapat ditindaklanjuti untuk mengoptimalkan penyimpanan.	Konfigurasikan Amazon S3 Storage Lens untuk mendapatkan visibilitas ke instans Amazon S3 storage Lens, serta rekomendasi untuk semua akun anggota di organisasi Anda.	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya	

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan
Danau Keamanan Amazon Amazon Security Lake memusatkan data keamanan dari sumber cloud, lokal, dan kustom ke dalam data lake yang disimpan di akun Anda.	Buat data lake yang mengumpulkan log dan peristiwa di seluruh akun Anda.	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
AWS Service Catalog Buat dan kelola katalog layanan IT yang disetujui untuk digunakan pada AWS.	Anda dapat berbagi portofolio dan menyalin produk di seluruh akun dengan lebih mudah, tanpa berbagi ID portofolio.	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya	

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan
Service Quotas Lihat dan kelola layanan Kuota, yang juga disebut sebagai batas, Anda dari lokasi pusat.	Anda dapat membuat templat permintaan kuota untuk secara otomatis meminta peningkatan kuota ketika akun di organisasi Anda dibuat.	 Ya Pelajari selengkapnya	 Tidak

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
AWS IAM Identity Center Berikan akses masuk tunggal untuk semua akun dan aplikasi cloud Anda.	Pengguna dapat masuk ke portal AWS akses dengan kredensi perusahaan dan mengakses sumber daya di akun manajemen atau akun anggota yang ditetapkan.	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya	

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan
AWS Systems Manager Aktifkan visibilitas dan kontrol sumber AWS daya Anda.	Anda dapat menyinkronkan data operasi Akun AWS di seluruh organisasi Anda dengan menggunakan Systems Manager Explorer. Anda dapat mengelola perubahan templat, persetujuan, dan pelaporan untuk semua akun anggota	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
	di organisasi Anda dari akun administrator yang didelegasikan dengan menggunakan Manajer Perubahan Systems Manager.			

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan
Kebijakan tag Gunakan tag terstandarisasi di seluruh sumber daya di akun organisasi Anda.	Anda dapat membuat kebijakan tag untuk menentukan aturan penandaan untuk sumber daya dan jenis sumber daya tertentu dan melampirkan kebijakan tersebut ke unit organisasi dan akun untuk menerapkan aturan tersebut.	 Ya Pelajari selengkapnya	 Tidak

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
AWS Trusted Advisor Trusted Advisor memeriksa AWS lingkungan Anda dan membuat rekomendasi ketika ada peluang untuk menghemat uang, untuk meningkatkan ketersediaan dan kinerja sistem, atau untuk membantu menutup kesenjangan keamanan.	Jalankan Trusted Advisor pemeriksaan untuk semua yang Akun AWS ada di organisasi Anda.	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya	

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
AWS Well-Architected Tool AWS Well-Architected Tool Ini membantu Anda mendokumentasikan keadaan beban kerja Anda dan membandingkannya dengan praktik terbaik AWS arsitektur terbaru.	Memungkinkan pelanggan keduanya AWS WA Tool dan Organizations untuk menyederhanakan proses berbagi AWS WA Tool sumber daya dengan anggota lain dari organisasi mereka.	 Ya Pelajari selengkapnya	 Tidak	

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan
Manajer Alamat IP VPC Amazon (IPAM) IPAM adalah fitur VPC yang memudahkan Anda merencanakan, melacak, dan memantau alamat IP untuk AWS beban kerja Anda.	Pantau penggunaan alamat IP di seluruh organisasi Anda dan bagikan kumpulan alamat IP di seluruh akun anggota.	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya

AWS layanan	Manfaat menggunakan dengan AWS Organizations	Mendukung akses tepercaya	Mendukung administrator yang didelegasikan	
Penganalisis Reachability VPC Amazon Reachability Analyzer adalah alat analisis konfigurasi yang memungkinkan Anda melakukan pengujian konektivitas antara sumber daya sumber dan sumber daya tujuan di cloud pribadi virtual (VPC) Anda.	Lacak jalur di seluruh akun di organisasi Anda.	 Ya Pelajari selengkapnya	 Ya Pelajari selengkapnya	

AWS Account Management dan AWS Organizations

AWS Account Managementmembantu Anda mengelola informasi akun dan metadata untuk semua yang ada Akun AWS di organisasi Anda. Anda dapat mengatur, memodifikasi, atau menghapus informasi kontak alternatif untuk setiap akun anggota organisasi Anda. Untuk informasi

selengkapnya, lihat Menggunakan AWS Account Management di organisasi Anda di Panduan AWS Account Management Pengguna.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan AWS Account Management dengan AWS Organizations.

Untuk mengaktifkan akses tepercaya dengan Manajemen Akun

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Manajemen Akun memerlukan akses tepercaya AWS Organizations sebelum Anda dapat menetapkan akun anggota untuk menjadi administrator yang didelegasikan untuk layanan ini untuk organisasi Anda.

Anda dapat mengaktifkan akses terpercaya hanya menggunakan alat Organizations.

Anda dapat mengaktifkan akses terpercaya dengan menggunakan konsol AWS Organizations, dengan menjalankan perintah AWS CLI, atau dengan memanggil operasi API di salah satu SDK AWS.

AWS Management Console

Untuk mengaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk AWS Account Management, pilih nama layanan, dan kemudian Mengaktifkan akses terpercaya.
3. Di kotak dialog konfirmasi, aktifkan Menampilkan opsi untuk mengaktifkan akses terpercaya, masukkan **`enable`** dalam kotak, dan kemudian pilih Mengaktifkan akses terpercaya.
4. Jika Anda adalah administrator hanya AWS Organizations, beritahu administrator AWS Account Management bahwa mereka sekarang dapat mengaktifkan layanan tersebut menggunakan konsolnya untuk bekerja dengan AWS Organizations.

AWS CLI, AWS API

Untuk mengaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk mengaktifkan atau mengaktifkan akses layanan terpercaya:

- AWS CLI: enable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk mengaktifkan AWS Account Management sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal account.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.

- AWSAPI: Aktifkan AWSServiceAccess

Untuk menonaktifkan akses tepercaya dengan Manajemen Akun

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Hanya administrator di akun pengelolaan AWS Organizations yang dapat menonaktifkan akses terpercaya dengan AWS Account Management.

Anda dapat menonaktifkan akses terpercaya hanya menggunakan alat Organizations.

Anda dapat menonaktifkan akses terpercaya dengan menggunakan konsol AWS Organizations, dengan menjalankan perintah AWS CLI, atau dengan memanggil operasi API Organizations di salah satu SDK AWS.

AWS Management Console

Untuk menonaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk AWS Account Management dan kemudian pilih nama layanan.
3. Pilih Menonaktifkan akses terpercaya.

4. Di kotak dialog konfirmasi, masukkan **`disable`** dalam kotak, dan kemudian pilih Menonaktifkan akses terpercaya.
5. Jika Anda adalah administrator hanya AWS Organizations, beritahu administrator AWS Account Management bahwa mereka sekarang dapat menonaktifkan layanan tersebut menggunakan konsolnya untuk bekerja dengan AWS Organizations.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk menonaktifkan akses layanan terpercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan AWS Account Management sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal account.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWSAPI: Nonaktifkan AWSServiceAccess

Mengaktifkan akun administrator yang didelegasikan untuk Manajemen Akun

Saat Anda menetapkan akun anggota sebagai administrator yang didelegasikan untuk organisasi, pengguna dan peran dari akun yang ditunjuk dapat mengelola Akun AWS metadata untuk akun anggota lain di organisasi. Jika Anda tidak mengaktifkan akun admin yang didelegasikan, maka tugas ini hanya dapat dilakukan oleh akun manajemen organisasi. Ini membantu Anda memisahkan manajemen organisasi dari pengelolaan detail akun Anda.

> Izin minimum
>
> Hanya pengguna atau peran dalam akun manajemen Organisasi yang dapat mengonfigurasi akun anggota sebagai administrator yang didelegasikan untuk Manajemen Akun di organisasi

Untuk petunjuk umum tentang cara mengonfigurasi kebijakan delegasi, lihatMembuat atau memperbarui kebijakan delegasi berbasis sumber daya.

AWS CLI, AWS API

Jika Anda ingin mengonfigurasi akun administrator yang didelegasikan menggunakan CLI AWS atau salah satu dari SDK AWS, Anda dapat menggunakan perintah berikut:

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal account.amazonaws.com
```

- AWSSDK: Hubungi `RegisterDelegatedAdministrator` operasi Organizations dan nomor ID akun anggota dan identifikasi prinsipal layanan akun `account.amazonaws.com` sebagai parameter.

AWS Application Migration Service (Layanan Migrasi Aplikasi) dan AWS Organizations

AWS Application Migration Service menyederhanakan, mempercepat, dan mengurangi biaya migrasi aplikasi ke aplikasi. AWS Dengan mengintegrasikan dengan Organizations, Anda dapat menggunakan fitur tampilan global untuk mengelola migrasi skala besar di beberapa akun. Untuk informasi selengkapnya, lihat Menyiapkan Anda AWS Organizations di panduan pengguna Layanan Migrasi Aplikasi.

Gunakan informasi berikut untuk membantu Anda AWS Application Migration Service berintegrasi AWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat di akun pengelolaan organisasi Anda bila Anda mengaktifkan akses terpercaya. Peran ini memungkinkan Layanan Migrasi Aplikasi untuk melakukan operasi yang didukung dalam akun organisasi Anda di organisasi Anda.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses tepercaya antara Layanan Migrasi Aplikasi dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

- `AWSServiceRoleForApplicationMigrationService`

Prinsipal layanan yang digunakan oleh Layanan Migrasi Aplikasi

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran terkait layanan yang digunakan oleh Layanan Migrasi Aplikasi memberikan akses ke prinsip layanan berikut:

- `mgn.amazonaws.com`

Mengaktifkan akses tepercaya dengan Layanan Migrasi Aplikasi

Saat mengaktifkan akses tepercaya dengan Layanan Migrasi Aplikasi, Anda dapat menggunakan fitur tampilan global, yang memungkinkan Anda mengelola migrasi skala besar di beberapa akun. Tampilan global memberikan visibilitas dan kemampuan untuk melakukan tindakan spesifik pada server sumber, aplikasi, dan gelombang di AWS akun yang berbeda. Untuk informasi selengkapnya, lihat Menyiapkan AWS Organizations Anda di panduan AWS Application Migration Service pengguna.

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Anda dapat mengaktifkan akses tepercaya menggunakan AWS Application Migration Service konsol atau AWS Organizations konsol.

> **Important**
>
> Kami sangat menyarankan bahwa bila memungkinkan, Anda menggunakan AWS Application Migration Service konsol atau alat untuk mengaktifkan integrasi dengan Organizations. Ini memungkinkan AWS Application Migration Service melakukan konfigurasi apa pun yang diperlukan, seperti membuat sumber daya yang dibutuhkan oleh layanan. Lanjutkan dengan langkah-langkah ini hanya jika Anda tidak dapat mengaktifkan integrasi menggunakan alat yang disediakan oleh AWS Application Migration Service. Untuk informasi lebih lanjut, lihat catatan ini.
>
> Jika Anda mengaktifkan akses tepercaya dengan menggunakan AWS Application Migration Service konsol atau alat, maka Anda tidak perlu menyelesaikan langkah-langkah ini.

Anda dapat mengaktifkan akses tepercaya dengan menggunakan AWS Organizations konsol, dengan menjalankan AWS CLI perintah, atau dengan memanggil operasi API di salah satu AWS SDK.

AWS Management Console

Untuk mengaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk AWS Application Migration Service, pilih nama layanan, dan kemudian Mengaktifkan akses terpercaya.
3. Di kotak dialog konfirmasi, aktifkan Menampilkan opsi untuk mengaktifkan akses terpercaya, masukkan **`enable`** dalam kotak, dan kemudian pilih Mengaktifkan akses terpercaya.
4. Jika Anda hanya administrator AWS Organizations, beri tahu administrator AWS Application Migration Service bahwa mereka sekarang dapat mengaktifkan layanan itu menggunakan konsolnya untuk bekerja dengannya AWS Organizations.

AWS CLI, AWS API

Untuk mengaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan AWS CLI perintah atau operasi API berikut untuk mengaktifkan akses layanan tepercaya:

- AWS CLI: enable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk mengaktifkan AWS Application Migration Service sebagai layanan tepercaya dengan Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal mgn.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWS API: Aktifkan AWSServiceAccess

Menonaktifkan akses tepercaya dengan Layanan Migrasi Aplikasi

Hanya administrator di akun manajemen Organizations yang dapat menonaktifkan akses tepercaya dengan Layanan Migrasi Aplikasi.

Anda dapat menonaktifkan akses tepercaya menggunakan AWS Organizations alat AWS Application Migration Service atau alat.

> **Important**
>
> Kami sangat menyarankan bahwa bila memungkinkan, Anda menggunakan AWS Application Migration Service konsol atau alat untuk menonaktifkan integrasi dengan Organizations. Ini memungkinkan AWS Application Migration Service melakukan pembersihan apa pun yang diperlukan, seperti menghapus sumber daya atau peran akses yang tidak lagi diperlukan oleh layanan. Lanjutkan dengan langkah-langkah ini hanya jika Anda tidak dapat menonaktifkan integrasi menggunakan alat yang disediakan oleh AWS Application Migration Service.
> Jika Anda menonaktifkan akses tepercaya dengan menggunakan AWS Application Migration Service konsol atau alat maka Anda tidak perlu menyelesaikan langkah-langkah ini.

Anda dapat menonaktifkan akses tepercaya dengan menggunakan AWS Organizations konsol, dengan menjalankan AWS CLI perintah Organizations, atau dengan memanggil operasi Organizations API di salah satu AWS SDK.

AWS Management Console

Untuk menonaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk AWS Application Migration Service dan kemudian pilih nama layanan.
3. Pilih Menonaktifkan akses terpercaya.
4. Di kotak dialog konfirmasi, masukkan **`disable`** dalam kotak, dan kemudian pilih Menonaktifkan akses terpercaya.

5. Jika Anda hanya administrator AWS Organizations, beri tahu administrator AWS Application Migration Service bahwa mereka sekarang dapat menonaktifkan layanan itu menggunakan konsol atau alatnya agar tidak berfungsi AWS Organizations.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan AWS CLI perintah atau operasi API berikut untuk menonaktifkan akses layanan tepercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan AWS Application Migration Service sebagai layanan tepercaya dengan Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal mgn.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.

- AWS API: Nonaktifkan AWSServiceAccess

Mengaktifkan akun administrator yang didelegasikan untuk Layanan Migrasi Aplikasi

Ketika Anda menetapkan akun anggota sebagai administrator yang didelegasikan untuk organisasi, pengguna dan peran dari akun tersebut dapat melakukan tindakan administratif untuk Layanan Migrasi Aplikasi yang hanya dapat dilakukan oleh pengguna atau peran dalam akun manajemen organisasi. Ini membantu Anda memisahkan manajemen organisasi dari manajemen Layanan Migrasi Aplikasi. Untuk informasi selengkapnya, lihat Menyiapkan Anda AWS Organizations di panduan pengguna Layanan Migrasi Aplikasi.

Izin minimum

Hanya pengguna atau peran dalam akun manajemen Organizations yang dapat mengonfigurasi akun anggota sebagai administrator yang didelegasikan untuk Layanan Migrasi Aplikasi di organisasi

AWS CLI, AWS API

Jika Anda ingin mengonfigurasi akun administrator yang didelegasikan menggunakan AWS CLI atau salah AWS satu SDK, Anda dapat menggunakan perintah berikut:

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal mgn.amazonaws.com
```

- AWS SDK: Panggil `RegisterDelegatedAdministrator` operasi Organizations dan nomor ID akun anggota dan identifikasi layanan akun `mgn.amazonaws.com` sebagai parameter.

Menonaktifkan administrator yang didelegasikan untuk Layanan Migrasi Aplikasi

Hanya administrator di akun manajemen Organizations yang dapat menghapus administrator yang didelegasikan untuk Layanan Migrasi Aplikasi. Anda dapat menghapus administrator yang didelegasikan menggunakan operasi Organizations `DeregisterDelegatedAdministrator` CLI atau SDK.

AWS Artifact dan AWS Organizations

AWS Artifact adalah layanan yang memungkinkan Anda mengunduh laporan kepatuhan AWS keamanan seperti laporan ISO dan PCI. Dengan menggunakan AWS Artifact, pengguna di akun manajemen organisasi dapat secara otomatis menerima perjanjian atas nama semua akun anggota dalam suatu organisasi, bahkan ketika laporan dan akun baru ditambahkan. Pengguna akun anggota dapat melihat dan mengunduh perjanjian. Untuk informasi selengkapnya, lihat Mengelola perjanjian untuk beberapa akun di AWS Artifak di AWS Artifact Panduan Pengguna.

Gunakan informasi berikut untuk membantu Anda AWS Artifact berintegrasi AWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat di akun pengelolaan organisasi Anda bila Anda mengaktifkan akses terpercaya. Peran ini memungkinkan AWS Artifact untuk melakukan operasi yang didukung dalam akun organisasi Anda di organisasi Anda.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses terpercaya antara AWS Artifact dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

Meskipun Anda dapat menghapus atau mengubah peran ini jika Anda menghapus akun anggota dari organisasi, kami tidak merekomendasikannya.

Memodifikasi peran tidak disarankan karena dapat menyebabkan masalah keamanan seperti wakil lintas layanan yang bingung. Untuk mempelajari lebih lanjut tentang perlindungan terhadap wakil yang bingung, lihat Pencegahan wakil lintas layanan di Panduan AWS Artifact Pengguna.

- `AWSServiceRoleForArtifact`

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran terkait layanan yang digunakan oleh AWS Artifact memberikan akses ke prinsipal layanan berikut:

- `artifact.amazonaws.com`

Mengaktifkan akses terpercaya dengan AWS Artifact

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Anda dapat mengaktifkan akses terpercaya hanya menggunakan alat Organizations.

Anda dapat mengaktifkan akses tepercaya dengan menggunakan AWS Organizations konsol, dengan menjalankan AWS CLI perintah, atau dengan memanggil operasi API di salah satu AWS SDK.

AWS Management Console

Untuk mengaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk AWS Artifact, pilih nama layanan, dan kemudian Mengaktifkan akses terpercaya.
3. Di kotak dialog konfirmasi, aktifkan Menampilkan opsi untuk mengaktifkan akses terpercaya, masukkan **`enable`** dalam kotak, dan kemudian pilih Mengaktifkan akses terpercaya.

4. Jika Anda hanya administrator AWS Organizations, beri tahu administrator AWS Artifact bahwa mereka sekarang dapat mengaktifkan layanan itu menggunakan konsolnya untuk bekerja dengannya AWS Organizations.

AWS CLI, AWS API

Untuk mengaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan AWS CLI perintah atau operasi API berikut untuk mengaktifkan akses layanan tepercaya:

- AWS CLI: enable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk mengaktifkan AWS Artifact sebagai layanan tepercaya dengan Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal artifact.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWS API: Aktifkan AWSServiceAccess

Menonaktifkan akses terpercaya dengan AWS Artifact

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Hanya administrator di akun AWS Organizations manajemen yang dapat menonaktifkan akses tepercaya dengan AWS Artifact.

Anda dapat menonaktifkan akses terpercaya hanya menggunakan alat Organizations.

AWS Artifact membutuhkan akses tepercaya AWS Organizations untuk bekerja dengan perjanjian organisasi. Jika Anda menonaktifkan akses tepercaya AWS Organizations saat Anda menggunakan AWS Artifact untuk perjanjian organisasi, itu berhenti berfungsi karena tidak dapat mengakses organisasi. Perjanjian organisasi apa pun yang Anda terima AWS Artifact tetap ada, tetapi tidak dapat diakses oleh AWS Artifact. AWS Artifact Peran yang AWS Artifact menciptakan tetap ada. Jika Anda kemudian mengaktifkan kembali akses terpercaya, AWS Artifact terus beroperasi seperti sebelumnya, tanpa perlu bagi Anda untuk mengonfigurasi ulang layanan.

Akun mandiri yang dihapus dari organisasi tidak lagi memiliki akses ke perjanjian organisasi.

Anda dapat menonaktifkan akses tepercaya dengan menggunakan AWS Organizations konsol, dengan menjalankan AWS CLI perintah Organizations, atau dengan memanggil operasi Organizations API di salah satu AWS SDK.

AWS Management Console

Untuk menonaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk AWS Artifact dan kemudian pilih nama layanan.
3. Pilih Menonaktifkan akses terpercaya.
4. Di kotak dialog konfirmasi, masukkan **`disable`** dalam kotak, dan kemudian pilih Menonaktifkan akses terpercaya.
5. Jika Anda adalah administrator saja AWS Organizations, beri tahu administrator AWS Artifact bahwa mereka sekarang dapat menonaktifkan layanan itu menggunakan konsol atau alatnya agar tidak berfungsi AWS Organizations.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan AWS CLI perintah atau operasi API berikut untuk menonaktifkan akses layanan tepercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan AWS Artifact sebagai layanan tepercaya dengan Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal artifact.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWS API: Nonaktifkan AWSServiceAccess

AWS Audit Manager dan AWS Organizations

AWS Audit Manager membantu Anda dalam meng-audit AWS Anda secara berkelanjutan untuk menyederhanakan cara Anda menilai risiko dan kepatuhan terhadap peraturan dan standar industri. Audit Manager mengotomatisasi pengumpulan bukti untuk membuatnya lebih mudah untuk menilai apakah kebijakan, prosedur, dan aktivitas Anda beroperasi secara efektif. Ketika saatnya melakukan audit, Audit Manager membantu Anda mengelola tinjauan pemangku kepentingan atas kendali Anda dan membantu Anda membuat laporan siap audit dengan upaya manual yang jauh lebih sedikit.

Ketika Anda mengintegrasikan Audit Manager dengan AWS Organizations, Anda dapat mengumpulkan bukti dari sumber yang lebih luas dengan menyertakan beberapa Akun AWS dari organisasi Anda dalam lingkup penilaian Anda.

Untuk informasi selengkapnya, lihat Mengaktifkan Organizations AWS di Panduan Pengguna Audit Manager.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan AWS Audit Manager dengan AWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat di akun pengelolaan organisasi Anda bila Anda mengaktifkan akses terpercaya. Peran ini memungkinkan Audit Manager untuk menjalankan operasi yang didukung di akun organisasi Anda di organisasi Anda.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses terpercaya antara Audit Manager dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

Untuk informasi selengkapnya tentang bagaimana Audit Manager menggunakan peran ini, lihat Menggunakan peran tertaut layanan di Panduan Pengguna AWS Audit Manager.

- `AWSServiceRoleForAuditManager`

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran tertaut layanan yang digunakan oleh Audit Manager memberikan akses ke prinsipal layanan berikut:

- `auditmanager.amazonaws.com`

Cara mengaktifkan akses terpercaya dengan Audit Manager

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Audit Manager memerlukan akses terpercaya ke AWS Organizations sebelum Anda dapat menetapkan akun anggota menjadi administrator yang didelegasikan untuk organisasi Anda.

Anda dapat mengaktifkan akses terpercaya menggunakan konsol AWS Audit Manager atau konsol AWS Organizations.

> **Important**
>
> Kami sangat merekomendasikan bahwa bila memungkinkan, Anda menggunakan konsol AWS Audit Manager atau alat untuk memungkinkan integrasi dengan Organizations. Hal ini memungkinkan AWS Audit Manager melakukan konfigurasi yang diperlukan, seperti membuat sumber daya yang dibutuhkan oleh layanan. Lanjutkan dengan langkah-langkah ini hanya jika Anda tidak dapat mengaktifkan integrasi integrasi menggunakan alat yang disediakan olehAWS Audit Manager. Untuk informasi selengkapnya, lihat selengkapnya, lihat selengkapnya, lihat selengkapnya, lihat sel
> Jika Anda mengaktifkan akses terpercaya dengan menggunakan konsol AWS Audit Manager atau alat, Anda tidak perlu menyelesaikan langkah-langkah ini.

Untuk mengaktifkan akses terpercaya menggunakan konsol Audit Manager

Untuk instruksi tentang cara mengaktifkan akses terpercaya, lihat Menyiapkan di Panduan Pengguna AWS Audit Manager.

> **Note**
>
> Jika Anda mengonfigurasi administrator yang didelegasikan dengan menggunakan konsol AWS Audit Manager, kemudian AWS Audit Manager secara otomatis memungkinkan akses terpercaya untuk Anda.

Anda dapat mengaktifkan akses terpercaya dengan menjalankan perintah AWS CLI Organizations, atau dengan memanggil operasi API Organizations di salah satu SDK AWS.

AWS CLI, AWS API

Untuk mengaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk mengaktifkan atau mengaktifkan akses layanan terpercaya:

- AWS CLI: enable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk mengaktifkan AWS Audit Manager sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal auditmanager.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.

- AWSAPI: AktifkanAWSServiceAccess

Untuk menonaktifkan akses terpercaya dengan Audit Manager

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Hanya administrator di akun pengelolaan AWS Organizations yang dapat menonaktifkan akses terpercaya dengan AWS Audit Manager.

Anda dapat menonaktifkan akses terpercaya hanya menggunakan alat Organizations.

Anda dapat menonaktifkan akses terpercaya dengan menjalankan perintah AWS CLI Organizations, atau dengan memanggil operasi API Organizations di salah satu SDK AWS.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk menonaktifkan akses layanan terpercaya:

- AWS CLI: disable-aws-service-access

Anda dapat menjalankan perintah berikut untuk menonaktifkan AWS Audit Manager sebagai layanan terpercaya dengan Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal auditmanager.amazonaws.com
```

Perintah ini tidak menghasilkan output saat berhasil.

- AWSAPI: NonaktifkanAWSServiceAccess

Mengaktifkan akun administrator yang didelegasikan untuk Audit Manager

Ketika Anda menetapkan akun anggota untuk menjadi administrator yang didelegasikan untuk organisasi, pengguna dan peran dari akun yang dapat melakukan tindakan administratif untuk Audit Manager yang jika tidak dapat dilakukan hanya oleh pengguna atau peran dalam akun pengelolaan organisasi. Ini membantu Anda untuk memisahkan manajemen organisasi dari manajemen Audit Manager.

> **Izin minimum**
>
> Hanya pengguna atau peran dalam akun pengelolaan Organizations dengan izin berikut dapat mengonfigurasi akun anggota sebagai administrator yang didelegasikan untuk Audit Manager dalam organisasi:
> `audit-manager:RegisterAccount`

Untuk instruksi tentang mengaktifkan akun administrator yang didelegasikan untuk Audit Manager, lihat Menyiapkan di Panduan Pengguna AWS Audit Manager.

Jika Anda mengonfigurasi administrator yang didelegasikan dengan menggunakan konsol AWS Audit Manager, kemudian Audit Manager secara otomatis mengaktifkan akses terpercaya untuk Anda.

AWS CLI, AWS API

Jika Anda ingin mengonfigurasi akun administrator yang didelegasikan menggunakan CLI AWS atau salah satu dari SDK AWS, Anda dapat menggunakan perintah berikut:

- AWS CLI:

```
$  aws audit-manager register-account \
    --delegated-admin-account 123456789012
```

- SDK AWS: Panggil operasi `RegisterAccount` dan sediakan `delegatedAdminAccount` sebagai parameter untuk mendelegasikan akun administrator.

AWS Backup dan AWS Organizations

AWS Backup adalah layanan yang memungkinkan Anda mengelola dan memantau pekerjaan AWS Backup di organisasi Anda. Dengan menggunakan AWS Backup, jika Anda masuk sebagai pengguna di akun pengelolaan organisasi, Anda dapat mengaktifkan perlindungan dan pemantauan backup di seluruh organisasi. Ini membantu Anda untuk mencapai kepatuhan dengan menggunakan kebijakan backup untuk menerapkan secara terpusat AWS Backup ke sumber daya di semua akun di organisasi Anda. Saat Anda menggunakan kedua AWS Backup dan AWS Organizations bersama-sama, Anda bisa mendapatkan manfaat berikut:

Perlindungan

Anda dapat mengaktifkan jenis kebijakan backup di organisasi Anda, lalu membuat kebijakan backup untuk dilampirkan ke root organisasi, OU, atau akun. Kebijakan backup menggabungkan paket AWS Backup dengan detail lain yang diperlukan untuk menerapkan paket secara otomatis ke akun Anda. Kebijakan yang secara langsung dilampirkan ke akun digabungkan dengan kebijakan yang diwariskan dari root organisasi dan OU induk untuk membuat sebuah Kebijakan yang efektif yang berlaku untuk akun. Kebijakan tersebut mencakup ID dari IAM role yang memiliki izin untuk menjalankan AWS Backup pada sumber daya di akun Anda. AWS Backup menggunakan IAM role untuk melakukan backup atas nama Anda sebagaimana yang ditentukan oleh paket backup dalam kebijakan efektif.

Pemantauan

Saat Anda mengaktifkan akses terpercaya untuk AWS Backup di organisasi Anda, Anda dapat menggunakan AWS Backup untuk melihat detail tentang backup, pemulihan, dan menyalin pekerjaan di salah satu akun di organisasi Anda. Untuk informasi selengkapnya, lihat Memantau pekerjaan backup Anda di Panduan Developer AWS Backup.

Untuk informasi selengkapnya tentang AWS Backup, lihat Panduan Developer AWS Backup

Gunakan informasi berikut untuk membantu Anda mengintegrasikan AWS Backup dengan AWS Organizations.

Mengaktifkan akses terpercaya dengan AWS Backup

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Anda dapat mengaktifkan akses terpercaya menggunakan konsol AWS Backup atau konsol AWS Organizations.

> **Important**
>
> Kami sangat merekomendasikan bahwa bila memungkinkan, Anda menggunakan konsol AWS Backup atau alat untuk memungkinkan integrasi dengan Organizations. Hal ini memungkinkan AWS Backup melakukan konfigurasi yang diperlukan, seperti membuat sumber daya yang dibutuhkan oleh layanan. Lanjutkan dengan langkah-langkah ini hanya jika Anda tidak dapat mengaktifkan integrasi menggunakan alat yang disediakan olehAWS Backup. Untuk informasi selengkapnya, lihat catatan ini.
> Jika Anda mengaktifkan akses terpercaya dengan menggunakan konsol AWS Backup atau alat, Anda tidak perlu menyelesaikan langkah-langkah ini.

Untuk mengaktifkan akses terpercaya menggunakan AWS Backup, lihat Mengaktifkan backup dalam beberapa Akun AWS di Panduan Developer AWS Backup.

Menonaktifkan akses terpercaya dengan AWS Backup

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

AWS Backup memerlukan akses terpercaya dengan AWS Organizations untuk mengaktifkan pemantauan pencadangan, pemulihan, dan menyalin pekerjaan di seluruh akun organisasi Anda. Jika Anda menonaktifkan AWS Backup akses terpercaya, Anda kehilangan kemampuan untuk melihat pekerjaan di luar akun saat ini. Parameter peran AWS Backup yang diciptakan oleh AWS Backup tetap. Jika nanti Anda mengaktifkan kembali akses terpercaya, AWS Backup terus beroperasi seperti sebelumnya, tanpa perlu bagi Anda untuk mengonfigurasi ulang layanan.

Anda dapat menonaktifkan akses terpercaya hanya menggunakan alat Organizations.

Anda dapat menonaktifkan akses terpercaya dengan menjalankan perintah AWS CLI Organizations, atau dengan memanggil operasi API Organizations di salah satu SDK AWS.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk menonaktifkan akses layanan terpercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan AWS Backup sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal backup.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.

- AWSAPI: NonaktifkanAWSServiceAccess

Mengaktifkan akun akun akun yang didelegasikan untukAWS Backup

Lihat Administrator yang didelegasikan di PanduanAWS Backup Pengembang.

AWS Billing and Cost Management dan AWS Organizations

AWS Billing and Cost Management menyediakan serangkaian fitur untuk membantu Anda mengatur tagihan, mengambil dan membayar faktur, dan menganalisis, mengatur, merencanakan, dan mengoptimalkan biaya Anda. Saat Anda menggunakan Billing and Cost Management AWS Organizations dengan Anda mengizinkan data alokasi biaya terpisah untuk AWS Organizations mengambil informasi, jika berlaku, dan mengumpulkan data telemetri untuk layanan data alokasi biaya terpisah yang Anda pilih.

Gunakan informasi berikut untuk membantu Anda AWS Billing and Cost Management berintegrasi AWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat di akun pengelolaan organisasi Anda bila Anda mengaktifkan akses terpercaya. Peran ini memungkinkan Billing and Cost Management untuk melakukan operasi yang didukung dalam akun organisasi Anda di organisasi Anda.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses tepercaya antara Billing and Cost Management dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

Untuk informasi selengkapnya, lihat Izin peran terkait layanan untuk Billing and Cost Management di Panduan Pengguna Billing and Cost Management.

- `AWSServiceRoleForSplitCostAllocationData`

Prinsipal layanan yang digunakan oleh Billing and Cost Management

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran terkait layanan yang digunakan oleh Billing and Cost Management memberikan akses ke prinsipal layanan berikut:

Billing and Cost Management menggunakan `billing-cost-management.amazonaws.com` prinsip layanan.

Mengaktifkan akses tepercaya dengan Billing and Cost Management

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Dengan akses tepercaya yang diaktifkan melalui akun manajemen, pelanggan dapat memanfaatkan fitur data alokasi biaya terpisah di bawah Billing and Cost Management. Ketika pelanggan mengaktifkan data alokasi biaya terpisah untuk Amazon Elastic Kubernetes Service dengan Amazon Managed Service for Prometheus, akses tepercaya akan dipanggil untuk membuat peran terkait layanan untuk semua akun anggota dalam Organisasi. Hal ini memungkinkan data alokasi biaya terpisah untuk mengumpulkan data telemetri dari Layanan Terkelola Amazon pelanggan untuk ruang kerja Prometheus dan melakukan alokasi biaya berdasarkan metrik tersebut.

Anda dapat mengaktifkan akses tepercaya dengan menggunakan AWS Organizations konsol, dengan menjalankan AWS CLI perintah, atau dengan memanggil operasi API di salah satu AWS SDK.

AWS Management Console

Untuk mengaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk AWS Billing and Cost Management, pilih nama layanan, dan kemudian Mengaktifkan akses terpercaya.
3. Di kotak dialog konfirmasi, aktifkan Menampilkan opsi untuk mengaktifkan akses terpercaya, masukkan **`enable`** dalam kotak, dan kemudian pilih Mengaktifkan akses terpercaya.
4. Jika Anda hanya administrator AWS Organizations, beri tahu administrator AWS Billing and Cost Management bahwa mereka sekarang dapat mengaktifkan layanan itu menggunakan konsolnya untuk bekerja dengannya AWS Organizations.

AWS CLI, AWS API

Untuk mengaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan AWS CLI perintah atau operasi API berikut untuk mengaktifkan akses layanan tepercaya:

- AWS CLI: enable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk mengaktifkan AWS Billing and Cost Management sebagai layanan tepercaya dengan Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal  billing-cost-management.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWS API: Aktifkan AWSServiceAccess

Menonaktifkan akses tepercaya

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Anda dapat menonaktifkan akses terpercaya hanya menggunakan alat Organizations.

Anda dapat menonaktifkan akses tepercaya dengan menjalankan AWS CLI perintah Organizations, atau dengan memanggil operasi Organizations API di salah satu AWS SDK.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan AWS CLI perintah atau operasi API berikut untuk menonaktifkan akses layanan tepercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan AWS Billing and Cost Management sebagai layanan tepercaya dengan Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal  billing-cost-management.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWS API: Nonaktifkan AWSServiceAccess

AWS CloudFormation dan StackSets AWS Organizations

AWS CloudFormationStackSetsmemungkinkan Anda untuk membuat, memperbarui, atau menghapus tumpukan di beberapa Akun AWS dan Wilayah AWS dengan satu operasi. StackSetsIntegrasi dengan AWS Organizations memungkinkan Anda membuat set tumpukan dengan izin yang dikelola layanan, dengan menggunakan peran terkait layanan yang memiliki izin yang relevan di setiap akun anggota. Ini memungkinkan Anda men-deploy instans tumpukan ke akun anggota di organisasi Anda. Anda tidak perlu membuat AWS Identity and Access Management peran yang diperlukan; StackSets menciptakan IAM role di setiap akun anggota atas nama Anda.

Anda juga dapat memilih untuk mengaktifkan deployment otomatis ke akun yang ditambahkan ke organisasi Anda di masa mendatang. Dengan penerapan auto diaktifkan, peran dan penerapan instans kumpulan tumpukan terkait secara otomatis ditambahkan ke semua akun yang ditambahkan di future ke OU tersebut.

Dengan akses terpercaya antara StackSets Organizations diaktifkan, akun pengelolaan memiliki izin untuk membuat dan mengelola set tumpukan untuk organisasi Anda. Akun manajemen dapat

mendaftar hingga lima akun anggota sebagai administrator yang didelegasikan. Dengan akses terpercaya diaktifkan, administrator yang didelegasikan juga memiliki izin untuk membuat dan mengelola set tumpukan untuk organisasi Anda. Set tumpukan dengan izin terkelola layanan dibuat di akun pengelolaan, termasuk set tumpukan yang dibuat oleh administrator yang didelegasikan.

> **Important**
>
> Administrator yang didelegasikan memiliki izin penuh untuk men-deploy ke akun di organisasi Anda. Akun manajemen tidak dapat membatasi izin administrator yang didelegasikan untuk menyebarkan ke OU tertentu atau untuk melakukan operasi set tumpukan tertentu.

Untuk informasi selengkapnya tentang integrasi StackSets dengan Organizations, lihat Bekerja dengan AWS CloudFormation StackSets di Panduan AWS CloudFormation Pengguna.

Gunakan informasi berikut untuk membantu Anda AWS CloudFormation StackSets berintegrasiAWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat di akun pengelolaan organisasi Anda bila Anda mengaktifkan akses terpercaya. Peran ini memungkinkan Stacksets AWS CloudFormation untuk menjalankan operasi yang didukung dalam akun organisasi Anda di organisasi Anda.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses terpercaya antara Stacksets AWS CloudFormation dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

- Akun manajemen: `AWSServiceRoleForCloudFormationStackSetsOrgAdmin`

Untuk membuat peran terkait layanan `AWSServiceRoleForCloudFormationStackSetsOrgMember` untuk akun anggota di organisasi Anda, Anda harus membuat tumpukan yang ditetapkan di akun manajemen terlebih dahulu. Hal ini menciptakan contoh stack set, yang kemudian menciptakan peran dalam account anggota.

- Akun anggota: `AWSServiceRoleForCloudFormationStackSetsOrgMember`

Untuk detail selengkapnya tentang membuat set tumpukan, lihat Bekerja dengan AWS CloudFormation StackSets di AWS CloudFormationUser Guide.

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran tertaut layanan yang digunakan oleh Stacksets AWS CloudFormation memberikan akses ke prinsipal layanan berikut:

- Akun manajemen: `stacksets.cloudformation.amazonaws.com`

  Anda dapat mengubah atau menghapus peran ini hanya jika Anda menonaktifkan akses terpercaya antara StackSets dan Organizations.
- Akun anggota: `member.org.stacksets.cloudformation.amazonaws.com`

  Anda dapat mengubah atau menghapus peran ini dari akun hanya jika Anda pertama kali menonaktifkan akses terpercaya antara StackSets dan Organizations, atau jika Anda pertama kali menghapus akun dari organisasi target atau unit organisasi (OU).

Mengaktifkan akses terpercaya dengan Stacksets AWS CloudFormation

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Hanya administrator di akun pengelolaan Organizations yang memiliki izin untuk mengaktifkan akses terpercaya dengan layanan AWS. Anda dapat mengaktifkan akses terpercaya menggunakan konsol AWS CloudFormation atau konsol Organizations.

Anda dapat mengaktifkan akses terpercaya hanya menggunakan AWS CloudFormationStackSets.

Untuk mengaktifkan akses terpercaya menggunakan Stacksets AWS CloudFormation konsol, lihat Mengaktifkan Akses Terpercaya dengan AWS Organizations di Panduan Pengguna AWS CloudFormation.

Menonaktifkan akses terpercaya dengan Stacksets AWS CloudFormation

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Hanya administrator di akun pengelolaan Organizations yang memiliki izin untuk menonaktifkan akses terpercaya dengan layanan AWS. Anda dapat menonaktifkan akses terpercaya hanya dengan menggunakan konsol Organizations. Jika Anda menonaktifkan akses terpercaya dengan Organizations saat Anda menggunakanStackSets, semua instans tumpukan yang dibuat sebelumnya dipertahankan. Namun, set tumpukan yang dideploy menggunakan izin peran terkait layanan tidak dapat lagi melakukan deployment ke akun yang dikelola oleh Organizations.

Anda dapat menonaktifkan akses terpercaya menggunakan AWS CloudFormation konsol atau konsol Organizations.

> **Important**
>
> Jika Anda menonaktifkan akses tepercaya secara terprogram (misalnya dengan AWS CLI atau dengan API), ketahuilah bahwa ini akan menghapus izin. Lebih baik menonaktifkan akses tepercaya dengan AWS CloudFormation konsol.

Anda dapat menonaktifkan akses terpercaya dengan menggunakan konsol AWS Organizations, dengan menjalankan perintah AWS CLI, atau dengan memanggil operasi API Organizations di salah satu SDK AWS.

AWS Management Console

Untuk menonaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk AWS CloudFormationStackSetsdan kemudian pilih nama layanan.
3. Pilih Menonaktifkan akses terpercaya.
4. Di kotak dialog konfirmasi, masukkan **`disable`** dalam kotak, dan kemudian pilih Menonaktifkan akses terpercaya.
5. Jika Anda adalah administrator hanyaAWS Organizations, beritahu administrator AWS CloudFormation StackSets bahwa mereka sekarang dapat menonaktifkan layanan tersebut menggunakan konsolnya untuk bekerja denganAWS Organizations.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk menonaktifkan akses layanan terpercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan AWS CloudFormation StackSets sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal stacksets.cloudformation.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWSAPI: Nonaktifkan AWSServiceAccess

Mengaktifkan akun administrator yang didelegasikan untuk Stacksets AWS CloudFormation

Bila Anda menetapkan akun anggota sebagai administrator yang didelegasikan untuk organisasi, pengguna dan peran dari akun tersebut dapat melakukan tindakan administratif untuk Stacksets AWS CloudFormation yang jika tidak dapat dilakukan hanya oleh pengguna atau peran dalam akun pengelolaan organisasi. Ini membantu Anda untuk memisahkan manajemen organisasi dari manajemen Stacksets AWS CloudFormation.

Untuk petunjuk tentang cara menetapkan akun anggota sebagai administrator yang didelegasikan Stacksets AWS CloudFormation dalam organisasi, lihat Daftarkan administrator yang didelegasikan di Panduan Pengguna AWS CloudFormation.

AWS CloudTrail dan AWS Organizations

AWS CloudTrail adalah AWS layanan yang membantu Anda mengaktifkan tata kelola, kepatuhan, dan audit operasional dan risiko Anda. Akun AWSDengan menggunakan AWS CloudTrail, pengguna di akun manajemen dapat membuat jejak organisasi yang mencatat semua peristiwa untuk semua Akun AWS di organisasi itu. Jejak organisasi secara otomatis diterapkan ke semua akun anggota dalam organisasi. Akun anggota dapat melihat jejak organisasi, namun tidak dapat mengubah atau menghapusnya. Secara default, akun anggota tidak memiliki akses ke berkas log untuk jejak

organisasi di bucket Amazon S3. Ini membantu Anda menerapkan dan menegakkan strategi pencatatan peristiwa Anda secara seragam di seluruh akun di organisasi Anda.

Untuk informasi selengkapnya, lihat Membuat Jejak untuk Organisasi di Panduan PenggunaAWS CloudTrail .

Gunakan informasi berikut untuk membantu Anda AWS CloudTrail berintegrasi AWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat di akun pengelolaan organisasi Anda bila Anda mengaktifkan akses terpercaya. Peran ini memungkinkan CloudTrail untuk melakukan operasi yang didukung dalam akun organisasi Anda di organisasi Anda.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses terpercaya antara CloudTrail dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

- `AWSServiceRoleForCloudTrail`

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran terkait layanan yang digunakan oleh CloudTrail memberikan akses ke prinsipal layanan berikut:

- `cloudtrail.amazonaws.com`

Mengaktifkan akses terpercaya dengan CloudTrail

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Jika Anda mengaktifkan akses tepercaya dengan membuat jejak dari AWS CloudTrail konsol, akses tepercaya dikonfigurasi secara otomatis untuk Anda (disarankan). Anda juga dapat mengaktifkan akses tepercaya menggunakan AWS Organizations konsol. Anda harus masuk dengan akun AWS Organizations manajemen Anda untuk membuat jejak organisasi.

Jika Anda memilih untuk membuat jejak organisasi menggunakan AWS CLI atau AWS API, Anda harus mengonfigurasi akses tepercaya secara manual. Untuk informasi selengkapnya, lihat

Mengaktifkan CloudTrail sebagai layanan tepercaya AWS Organizationsdi PanduanAWS CloudTrail Pengguna.

> **Important**
>
> Kami sangat menyarankan bahwa bila memungkinkan, Anda menggunakan AWS CloudTrail konsol atau alat untuk mengaktifkan integrasi dengan Organizations.

Anda dapat mengaktifkan akses tepercaya dengan menjalankan AWS CLI perintah Organizations, atau dengan memanggil operasi Organizations API di salah satu AWS SDK.

AWS CLI, AWS API

Untuk mengaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan AWS CLI perintah atau operasi API berikut untuk mengaktifkan akses layanan tepercaya:

- AWS CLI: enable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk mengaktifkan AWS CloudTrail sebagai layanan tepercaya dengan Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal cloudtrail.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWS API: Aktifkan AWSServiceAccess

Menonaktifkan akses terpercaya dengan CloudTrail

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

AWS CloudTrail membutuhkan akses tepercaya AWS Organizations untuk bekerja dengan jalur organisasi dan penyimpanan data acara organisasi. Jika Anda menonaktifkan akses tepercaya AWS Organizations saat Anda menggunakan AWS CloudTrail, semua jejak organisasi untuk akun anggota akan dihapus karena tidak CloudTrail dapat mengakses organisasi. Semua jejak organisasi

akun manajemen dan penyimpanan data acara organisasi dikonversi ke jalur tingkat akun dan penyimpanan data acara. `AWSServiceRoleForCloudTrail`Peran yang dibuat untuk integrasi antara CloudTrail dan AWS Organizations tetap di akun. Jika Anda mengaktifkan kembali akses tepercaya, tidak CloudTrail akan mengambil tindakan pada jejak yang ada dan penyimpanan data acara. Akun manajemen harus memperbarui jejak tingkat akun dan penyimpanan data acara apa pun untuk menerapkannya ke organisasi.

Untuk mengonversi jejak tingkat akun atau penyimpanan data peristiwa ke jejak organisasi atau penyimpanan data acara organisasi, lakukan hal berikut:

- Dari CloudTrail konsol, perbarui penyimpanan data jejak atau peristiwa dan pilih opsi Aktifkan untuk semua akun di organisasi saya.
- Dari AWS CLI, lakukan hal berikut:
  - Untuk memperbarui jejak, jalankan update-trailperintah dan sertakan `--is-organization-trail` parameternya.
  - Untuk memperbarui penyimpanan data peristiwa, jalankan update-event-data-storeperintah dan sertakan `--organization-enabled` parameternya.

Hanya administrator di akun AWS Organizations manajemen yang dapat menonaktifkan akses tepercaya dengan AWS CloudTrail. Anda dapat menonaktifkan akses tepercaya hanya dengan alat Organizations, menggunakan AWS Organizations konsol, menjalankan perintah Organizations AWS CLI, atau memanggil operasi Organizations API di salah satu SDK. AWS

Anda dapat menonaktifkan akses tepercaya dengan menggunakan AWS Organizations konsol, dengan menjalankan AWS CLI perintah Organizations, atau dengan memanggil operasi Organizations API di salah satu AWS SDK.

AWS Management Console

Untuk menonaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsolAWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk AWS CloudTrail dan kemudian pilih nama layanan.
3. Pilih Menonaktifkan akses terpercaya.

4. Di kotak dialog konfirmasi, masukkan **`disable`** dalam kotak, dan kemudian pilih Menonaktifkan akses terpercaya.
5. Jika Anda hanya administrator AWS Organizations, beri tahu administrator AWS CloudTrail bahwa mereka sekarang dapat menonaktifkan layanan itu menggunakan konsol atau alatnya agar tidak berfungsi AWS Organizations.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan AWS CLI perintah atau operasi API berikut untuk menonaktifkan akses layanan tepercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan AWS CloudTrail sebagai layanan tepercaya dengan Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal cloudtrail.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWS API: Nonaktifkan AWSServiceAccess

Mengaktifkan akun administrator yang didelegasikan untuk CloudTrail

Saat Anda menggunakan CloudTrail Organizations, Anda dapat mendaftarkan akun apa pun di dalam organisasi untuk bertindak sebagai administrator yang CloudTrail didelegasikan untuk mengelola jejak organisasi dan penyimpanan data acara atas nama organisasi. Administrator yang didelegasikan adalah akun anggota dalam organisasi yang dapat melakukan tugas administratif yang sama CloudTrail seperti akun manajemen.

> **Izin minimum**
>
> Hanya administrator di akun manajemen Organizations yang dapat mendaftarkan administrator yang didelegasikan. CloudTrail

Anda dapat mendaftarkan akun administrator yang didelegasikan menggunakan CloudTrail konsol, atau dengan menggunakan operasi Organizations `RegisterDelegatedAdministrator` CLI atau SDK. Untuk mendaftarkan administrator yang didelegasikan menggunakan CloudTrail konsol, lihat Menambahkan administrator yang CloudTrail didelegasikan.

Menonaktifkan administrator yang didelegasikan untuk CloudTrail

Hanya administrator di akun manajemen Organizations yang dapat menghapus administrator yang didelegasikan untuk CloudTrail. Anda dapat menghapus administrator yang didelegasikan menggunakan CloudTrail konsol, atau dengan menggunakan operasi Organizations `DeregisterDelegatedAdministrator` CLI atau SDK. Untuk informasi tentang cara menghapus administrator yang didelegasikan menggunakan CloudTrail konsol, lihat Menghapus administrator yang CloudTrail didelegasikan.

AWS Compute Optimizer dan AWS Organizations

AWS Compute Optimizer adalah layanan yang menganalisis metrik konfigurasi dan pemanfaatan sumber daya AWS Anda. Contoh sumber daya termasuk instans Amazon Elastic Compute Cloud (Amazon EC2) dan Grup Auto Scaling. Compute Optimizer melaporkan apakah sumber daya Anda optimal dan menghasilkan rekomendasi optimasi untuk mengurangi biaya dan meningkatkan kinerja beban kerja Anda. Untuk informasi lebih lanjut tentang Compute Optimizer, lihat Panduan Pengguna AWS Compute Optimizer.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan AWS Compute Optimizer dengan AWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat di akun pengelolaan organisasi Anda bila Anda mengaktifkan akses terpercaya. Peran ini memungkinkan Compute Optimizer untuk melakukan operasi yang didukung dalam akun organisasi Anda di organisasi Anda.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses terpercaya antara Compute Optimizer dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

- `AWSServiceRoleForComputeOptimizer`

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran tertaut layanan yang digunakan oleh Compute Optimizer memberikan akses ke prinsipal layanan berikut:

- `compute-optimizer.amazonaws.com`

Mengaktifkan akses terpercaya dengan Compute Optimizer

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Anda dapat mengaktifkan akses terpercaya menggunakan konsol AWS Compute Optimizer atau konsol AWS Organizations.

> **Important**
>
> Kami sangat merekomendasikan bahwa bila memungkinkan, Anda menggunakan konsol AWS Compute Optimizer atau alat untuk memungkinkan integrasi dengan Organizations. Hal ini memungkinkan AWS Compute Optimizer melakukan konfigurasi yang diperlukan, seperti membuat sumber daya yang dibutuhkan oleh layanan. Lanjutkan dengan langkah-langkah ini hanya jika Anda tidak dapat mengaktifkan integrasi menggunakan alat yang disediakan olehAWS Compute Optimizer. Untuk informasi lebih lanjut, lihatcatatan ini.
> Jika Anda mengaktifkan akses terpercaya dengan menggunakan konsol AWS Compute Optimizer atau alat, Anda tidak perlu menyelesaikan langkah-langkah ini.

Untuk mengaktifkan akses terpercaya menggunakan konsol Compute Optimizer

Anda harus masuk ke konsol Compute Optimizer menggunakan akun pengelolaan organisasi Anda. Pilih ikut atas nama organisasi Anda dengan mengikuti petunjuk di Memilih ikut di Akun Anda di Panduan Pengguna AWS Compute Optimizer.

Anda dapat mengaktifkan akses terpercaya dengan menggunakan konsol AWS Organizations, dengan menjalankan perintah AWS CLI, atau dengan memanggil operasi API di salah satu SDK AWS.

AWS Management Console

Untuk mengaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk AWS Compute Optimizer, pilih nama layanan, dan kemudian Mengaktifkan akses terpercaya.
3. Di kotak dialog konfirmasi, aktifkan Menampilkan opsi untuk mengaktifkan akses terpercaya, masukkan **`enable`** dalam kotak, dan kemudian pilih Mengaktifkan akses terpercaya.
4. Jika Anda adalah administrator hanya AWS Organizations, beritahu administrator AWS Compute Optimizer bahwa mereka sekarang dapat mengaktifkan layanan tersebut menggunakan konsolnya untuk bekerja dengan AWS Organizations.

AWS CLI, AWS API

Untuk mengaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk mengaktifkan atau mengaktifkan akses layanan terpercaya:

- AWS CLI: enable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk mengaktifkan AWS Compute Optimizer sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal compute-optimizer.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.

- AWSAPI:AktifkanAWSServiceAccess

Menonaktifkan akses terpercaya dengan Compute Optimizer

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Hanya administrator di akun pengelolaan AWS Organizations yang dapat menonaktifkan akses terpercaya dengan AWS Compute Optimizer.

Anda dapat menonaktifkan akses terpercaya dengan menjalankan perintah AWS CLI Organizations, atau dengan memanggil operasi API Organizations di salah satu SDK AWS.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk menonaktifkan akses layanan terpercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan AWS Compute Optimizer sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal compute-optimizer.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.

- AWSAPI:NonaktifkanAWSServiceAccess

Mengaktifkan akun administrator yang didelegasikan untuk Compute Optimizer

Ketika Anda menetapkan akun anggota untuk menjadi administrator yang didelegasikan untuk organisasi, pengguna dan peran dari akun yang ditunjuk dapat mengelolaAkun AWSmetadata untuk akun anggota lain di organisasi. Jika Anda tidak mengaktifkan akun admin yang didelegasikan, maka tugas ini hanya dapat dilakukan oleh akun manajemen organisasi. Ini membantu Anda memisahkan manajemen organisasi dari pengelolaan detail akun Anda.

Izin minimum

Hanya pengguna atau peran dalam akun manajemen Organisasi yang dapat mengonfigurasi akun anggota sebagai administrator yang didelegasikan untuk Compute Optimizer di organisasi

Untuk petunjuk tentang mengaktifkan akun administrator yang didelegasikan untuk Compute Optimizer, lihathttps://docs.aws.amazon.com/compute-optimizer/latest/ug/delegate-administrator-account.htmldi dalamAWS Compute OptimizerPanduan Pengguna.

AWS CLI, AWS API

Jika Anda ingin mengonfigurasi akun administrator yang didelegasikan menggunakan CLI AWS atau salah satu dari SDK AWS, Anda dapat menggunakan perintah berikut:

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal compute-optimizer.amazonaws.com
```

- AWSSDK: Hubungi OrganisasiRegisterDelegatedAdministratoroperasi dan nomor ID akun anggota dan mengidentifikasi prinsipal layanan akunaccount.amazonaws.comsebagai parameter.

Menonaktifkan administrator yang didelegasikan untuk Compute Optimizer

Hanya administrator di akun manajemen organisasi yang dapat mengonfigurasi administrator yang didelegasikan untuk Compute Optimizer.

Untuk menonaktifkan akun Compute Optimizer admin yang didelegasikan menggunakan konsol Compute Optimizer, lihathttps://docs.aws.amazon.com/compute-optimizer/latest/ug/delegate-administrator-account.htmldi dalamAWS Compute OptimizerPanduan Pengguna.

Untuk menghapus administrator yang didelegasikan menggunakanAWS AWS CLI, lihatderegister-delegated-administratordi dalamAWS AWS CLIReferensi Perintah.

AWS Config dan AWS Organizations

Agregasi data multi-akun dan multi-wilayah di AWS Config memungkinkan Anda untuk menggabungkan AWS Config data dari beberapa akun dan Wilayah AWS ke dalam satu akun. Agregasi data multi-akun dan multi-wilayah berguna bagi administrator IT pusat untuk memantau kepatuhan terhadap beberapa Akun AWS dalam perusahaan. Agregator adalah jenis sumber daya di AWS Config yang mengumpulkan data AWS Config dari beberapa sumber akun dan Wilayah. Buat agregator di Wilayah tempat Anda ingin melihat agregat AWS Config data. Sementara membuat

agregator, Anda dapat memilih untuk menambahkan baik ID akun individu atau organisasi Anda. Untuk informasi selengkapnya tentang AWS Config, lihat AWS Config Panduan Developer.

Anda juga dapat menggunakan API AWS Config untuk mengelola aturan AWS Config di semua Akun AWS di organisasi Anda. Untuk informasi selengkapnya, lihat Mengaktifkan Aturan AWS Config di Semua Akun di Organisasi Anda di Panduan Developer AWS Config.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan AWS Config dengan AWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut dibuat di akun organisasi Anda saat Anda mengaktifkan akses terpercaya. Peran ini memungkinkan AWS Config untuk menjalankan operasi yang didukung di dalam akun di organisasi Anda.

- `AWSServiceRoleForConfig`

Peran ini dibuat saat Anda mengaktifkan AWS Config di organisasi Anda dengan membuat agregator multi-akun. AWS Config meminta Anda untuk memilih atau membuat peran dan bagi Anda untuk memberikan nama. Tidak ada nama yang dihasilkan secara otomatis.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses terpercaya antara AWS Config dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

Mengaktifkan akses terpercaya dengan AWS Config

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Anda dapat mengaktifkan akses terpercaya menggunakan konsol AWS Config atau konsol AWS Organizations.

> **Important**
>
> Kami sangat merekomendasikan bahwa bila memungkinkan, Anda menggunakan konsol AWS Config atau alat untuk memungkinkan integrasi dengan Organizations. Hal ini memungkinkan AWS Config melakukan konfigurasi yang diperlukan, seperti membuat sumber daya yang dibutuhkan oleh layanan. Lanjutkan dengan langkah-langkah ini hanya

jika Anda tidak dapat mengaktifkan integrasi menggunakan alat yang disediakan olehAWS Config. Untuk informasi selengkapnya, lihat catatan ini.
Jika Anda mengaktifkan akses terpercaya dengan menggunakan konsol AWS Config atau alat, Anda tidak perlu menyelesaikan langkah-langkah ini.

Untuk mengaktifkan akses menggunakan konsol AWS Config

Untuk mengaktifkan akses terpercaya ke AWS Organizations menggunakan AWS Config, buat agregator multi-akun dan tambahkan organisasi. Untuk informasi tentang cara mengonfigurasi agregator multi-akun, lihat Menyiapkan agregator menggunakan konsol di Panduan Developer AWS Config.

Anda dapat mengaktifkan akses terpercaya dengan menggunakan konsol AWS Organizations, dengan menjalankan perintah AWS CLI, atau dengan memanggil operasi API di salah satu SDK AWS.

AWS Management Console

Untuk mengaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk AWS Config, pilih nama layanan, dan kemudian Mengaktifkan akses terpercaya.
3. Di kotak dialog konfirmasi, aktifkan Menampilkan opsi untuk mengaktifkan akses terpercaya, masukkan **`enable`** dalam kotak, dan kemudian pilih Mengaktifkan akses terpercaya.
4. Jika Anda adalah administrator hanya AWS Organizations, beritahu administrator AWS Config bahwa mereka sekarang dapat mengaktifkan layanan tersebut menggunakan konsolnya untuk bekerja dengan AWS Organizations.

AWS CLI, AWS API

Untuk mengaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk mengaktifkan atau mengaktifkan akses layanan terpercaya:

- AWS CLI: enable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk mengaktifkan AWS Config sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal config.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.

- API AWS: AktifkanAWSServiceAccess

Menonaktifkan akses terpercaya dengan AWS Config

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Anda dapat menonaktifkan akses terpercaya hanya menggunakan alat Organizations.

Anda dapat menonaktifkan akses terpercaya dengan menjalankan perintah AWS CLI Organizations, atau dengan memanggil operasi API Organizations di salah satu SDK AWS.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk menonaktifkan akses layanan terpercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan AWS Config sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal config.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.

- API AWS: NonaktifkanAWSServiceAccess

Hub Optimisasi Biaya AWS dan AWS Organizations

Hub Optimisasi Biaya AWS adalah fitur AWS Billing and Cost Management yang membantu Anda mengkonsolidasikan dan memprioritaskan rekomendasi pengoptimalan biaya di seluruh AWS akun AWS dan Wilayah Anda, sehingga Anda bisa mendapatkan hasil maksimal dari pengeluaran Anda. AWS Saat Anda menggunakan Cost Optimization Hub, AWS Organizations Anda dapat dengan mudah mengidentifikasi, memfilter, dan mengumpulkan rekomendasi pengoptimalan AWS biaya di seluruh akun dan AWS Wilayah anggota Organizations Anda.

Untuk informasi selengkapnya, lihat Pusat Pengoptimalan Biaya di Panduan AWS Cost Management Pengguna.

Gunakan informasi berikut untuk membantu Anda Hub Optimisasi Biaya AWS berintegrasi AWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat di akun pengelolaan organisasi Anda bila Anda mengaktifkan akses terpercaya. Peran ini memungkinkan Hub Pengoptimalan Biaya untuk melakukan operasi yang didukung dalam akun organisasi Anda di organisasi Anda.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses tepercaya antara Hub Pengoptimalan Biaya dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

Untuk informasi selengkapnya, lihat Izin peran terkait layanan untuk Hub Pengoptimalan Biaya di Panduan Pengguna..AWS Cost Management

- `AWSServiceRoleForCostOptimizationHub`

Prinsipal layanan yang digunakan oleh Cost Optimization Hub

Hub Pengoptimalan Biaya menggunakan prinsip `cost-optimization-hub.bcm.amazonaws.com` layanan.

Mengaktifkan akses tepercaya dengan Cost Optimization Hub

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Saat Anda memilih untuk menggunakan akun manajemen organisasi dan menyertakan semua akun anggota dalam organisasi, akses tepercaya untuk Hub Pengoptimalan Biaya diaktifkan secara otomatis di akun organisasi Anda.

Anda dapat mengaktifkan akses tepercaya dengan menggunakan AWS Organizations konsol, dengan menjalankan AWS CLI perintah, atau dengan memanggil operasi API di salah satu AWS SDK.

AWS Management Console

Untuk mengaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk Hub Optimisasi Biaya AWS, pilih nama layanan, dan kemudian Mengaktifkan akses terpercaya.
3. Di kotak dialog konfirmasi, aktifkan Menampilkan opsi untuk mengaktifkan akses terpercaya, masukkan **`enable`** dalam kotak, dan kemudian pilih Mengaktifkan akses terpercaya.
4. Jika Anda hanya administrator AWS Organizations, beri tahu administrator Hub Optimisasi Biaya AWS bahwa mereka sekarang dapat mengaktifkan layanan itu menggunakan konsolnya untuk bekerja dengannya AWS Organizations.

AWS CLI, AWS API

Untuk mengaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan AWS CLI perintah atau operasi API berikut untuk mengaktifkan akses layanan tepercaya:

- AWS CLI: enable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk mengaktifkan Hub Optimisasi Biaya AWS sebagai layanan tepercaya dengan Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal cost-optimization-hub.bcm.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.

- AWS API: Aktifkan AWSServiceAccess

Menonaktifkan akses tepercaya

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Anda dapat menonaktifkan akses terpercaya hanya menggunakan alat Organizations.

> **Important**
>
> Jika Anda menonaktifkan akses tepercaya Hub Pengoptimalan Biaya setelah Anda ikut serta, Hub Pengoptimalan Biaya menolak akses ke rekomendasi untuk akun anggota organisasi Anda. Selain itu, akun anggota dalam organisasi tidak ikut serta dalam Hub Pengoptimalan Biaya. Pelajari selengkapnya di Akses tepercaya Hub Pengoptimalan Biaya dan Organizations di Panduan AWS Cost Management Pengguna.

Anda dapat menonaktifkan akses tepercaya dengan menjalankan AWS CLI perintah Organizations, atau dengan memanggil operasi Organizations API di salah satu AWS SDK.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan AWS CLI perintah atau operasi API berikut untuk menonaktifkan akses layanan tepercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan Hub Optimisasi Biaya AWS sebagai layanan tepercaya dengan Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal cost-optimization-hub.bcm.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.

- AWS API: Nonaktifkan AWSServiceAccess

AWS Control Tower dan AWS Organizations

AWS Control Towermenawarkan cara mudah untuk mengatur dan mengatur lingkungan AWS multi-akun, mengikuti praktik terbaik preskriptif. AWS Control Towerorkestrasi memperluas kemampuan. AWS Organizations AWS Control Towermenerapkan kontrol preventif dan detektif (pagar pembatas) untuk membantu menjaga organisasi dan akun Anda dari perbedaan dari praktik terbaik (drift).

AWS Control Towerorkestrasi memperluas kemampuan. AWS Organizations

Untuk informasi selengkapnya, lihat panduan AWS Control Tower pengguna.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan AWS Control Tower dengan AWS Organizations.

Peran yang dibutuhkan untuk integrasi

`AWSControlTowerExecution`Peran harus ada di semua akun yang terdaftar. Ini memungkinkan AWS Control Tower untuk mengelola akun individual Anda dan melaporkan informasi tentang mereka ke akun Audit dan Arsip Log Anda.

Untuk mempelajari lebih lanjut tentang peran yang digunakan olehAWS Control Tower, lihat Cara AWS Control Tower bekerja dengan peran untuk membuat dan mengelola akun dan Menggunakan Kebijakan Berbasis Identitas (Kebijakan IAM) untuk. AWS Control Tower

Prinsipal layanan yang digunakan oleh AWS Control Tower

AWS Control Towermenggunakan prinsip `controltower.amazonaws.com` layanan.

Mengaktifkan akses terpercaya dengan AWS Control Tower

AWS Control Towermenggunakan akses tepercaya untuk mendeteksi penyimpangan untuk kontrol preventif, dan untuk melacak perubahan akun dan OU yang menyebabkan penyimpangan.

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Anda dapat mengaktifkan akses terpercaya hanya menggunakan alat Organizations.

Untuk mengaktifkan akses tepercaya dari konsol Organizations, pilih **`Enable access`** di samping AWS Control Tower.

Anda dapat mengaktifkan akses terpercaya dengan menjalankan perintah AWS CLI Organizations, atau dengan memanggil operasi API Organizations di salah satu SDK AWS.

AWS CLI, AWS API

Untuk mengaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk mengaktifkan atau mengaktifkan akses layanan terpercaya:

- AWS CLI: enable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk mengaktifkan AWS Control Tower sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal controltower.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWSAPI: Aktifkan AWSServiceAccess

Menonaktifkan akses terpercaya dengan AWS Control Tower

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Anda dapat menonaktifkan akses terpercaya hanya menggunakan alat Organizations.

> **Important**
>
> Menonaktifkan AWS Control Tower akses tepercaya menyebabkan penyimpangan di Zona Pendaratan AndaAWS Control Tower. Satu-satunya cara untuk memperbaiki drift adalah dengan menggunakan perbaikan Zona AWS Control Tower Pendaratan. Mengaktifkan kembali akses tepercaya di Organizations tidak memperbaiki penyimpangan. Pelajari lebih lanjut tentang drift di panduan AWS Control Tower pengguna.

Anda dapat menonaktifkan akses terpercaya dengan menjalankan perintah AWS CLI Organizations, atau dengan memanggil operasi API Organizations di salah satu SDK AWS.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk menonaktifkan akses layanan terpercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan AWS Control Tower sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal controltower.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWSAPI: Nonaktifkan AWSServiceAccess

Detektif Amazon danAWS Organizations

Amazon Detective menggunakan data log Anda untuk menghasilkan visualisasi yang memungkinkan Anda menganalisis, menyelidiki, dan mengidentifikasi akar penyebab temuan keamanan atau aktivitas mencurigakan.

MenggunakanAWS Organizationsmemungkinkan Anda untuk memastikan bahwa grafik perilaku Detektif Anda memberikan visibilitas ke aktivitas untuk semua akun organisasi Anda.

Saat Anda memberikan akses tepercaya ke Detektif, layanan Detektif dapat bereaksi secara otomatis terhadap perubahan dalam keanggotaan organisasi. Administrator yang didelegasikan dapat mengaktifkan akun organisasi apa pun sebagai akun anggota dalam grafik perilaku. Detektif juga dapat secara otomatis mengaktifkan akun organisasi baru sebagai akun anggota. Akun organisasi tidak dapat memisahkan diri dari grafik perilaku.

Untuk informasi lebih lanjut, lihatMenggunakan Amazon Detective di organisasi Andadi dalamPanduan Administrasi Detektif Amazon.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan Amazon DetectiveAWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat di akun pengelolaan organisasi Anda bila Anda mengaktifkan akses terpercaya. Peran ini memungkinkan Detektif untuk melakukan operasi yang didukung dalam akun organisasi Anda di organisasi Anda.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses tepercaya antara Detektif dan Organisasi, atau jika Anda menghapus akun anggota dari organisasi.

- `AWSServiceRoleForDetective`

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran terkait layanan yang digunakan oleh Detektif memberikan akses ke prinsip-prinsip layanan berikut:

- `detective.amazonaws.com`

Untuk mengaktifkan akses tepercaya dengan Detektif

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

> **Note**
>
> Saat Anda menunjuk administrator yang didelegasikan untuk Amazon Detective, Detective secara otomatis mengaktifkan akses tepercaya untuk Detective untuk organisasi Anda. Detektif membutuhkan akses tepercaya keAWS Organizationssebelum Anda dapat menunjuk akun anggota untuk menjadi administrator yang didelegasikan untuk layanan ini untuk organisasi Anda.

Anda dapat mengaktifkan akses terpercaya hanya menggunakan alat Organizations.

Anda dapat mengaktifkan akses terpercaya dengan menggunakan konsol AWS Organizations.

AWS Management Console

Untuk mengaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. PadaJasahalaman, menemukan baris untukDetektif Amazon, pilih nama layanan, lalu pilihAktifkan akses tepercaya.
3. Di kotak dialog konfirmasi, aktifkan Menampilkan opsi untuk mengaktifkan akses terpercaya, masukkan **`enable`** dalam kotak, dan kemudian pilih Mengaktifkan akses terpercaya.
4. Jika Anda adalah administrator hanyaAWS Organizations, beri tahu administrator Amazon Detective bahwa mereka sekarang dapat mengaktifkan layanan itu menggunakan konsolnya untuk bekerjaAWS Organizations.

Untuk menonaktifkan akses tepercaya dengan Detektif

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Hanya administrator diAWS Organizationsakun manajemen dapat menonaktifkan akses tepercaya dengan Amazon Detective.

Anda dapat menonaktifkan akses terpercaya hanya menggunakan alat Organizations.

Anda dapat menonaktifkan akses terpercaya dengan menggunakan konsol AWS Organizations.

AWS Management Console

Untuk menonaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. PadaJasahalaman, menemukan baris untukDetektif Amazondan kemudian pilih nama layanan.
3. Pilih Menonaktifkan akses terpercaya.

4. Di kotak dialog konfirmasi, masukkan **`disable`** dalam kotak, dan kemudian pilih Menonaktifkan akses terpercaya.
5. Jika Anda adalah administrator hanyaAWS Organizations, beri tahu administrator Amazon Detective bahwa mereka sekarang dapat menonaktifkan layanan itu menggunakan konsol atau alatnya agar tidak bekerja denganAWS Organizations.

Mengaktifkan akun administrator yang didelegasikan untuk Detektif

Akun administrator yang didelegasikan untuk Detektif adalah akun administrator untuk grafik perilaku Detektif. Administrator yang didelegasikan menentukan akun organisasi mana yang akan diaktifkan dan dinonaktifkan sebagai akun anggota dalam grafik perilaku tersebut. Administrator yang didelegasikan dapat mengonfigurasi Detektif untuk mengaktifkan akun organisasi baru secara otomatis sebagai akun anggota saat ditambahkan ke organisasi. Untuk informasi tentang cara administrator yang didelegasikan mengelola akun organisasi, lihatMengelola akun organisasi sebagai akun anggotadi dalamPanduan Administrasi Detektif Amazon.

Hanya administrator di akun manajemen organisasi yang dapat mengonfigurasi administrator yang didelegasikan untuk Detektif.

Anda dapat menentukan akun administrator yang didelegasikan dari konsol Detektif atau API, atau dengan menggunakan operasi CLI atau SDK Organisasi.

> **Izin minimum**
>
> Hanya pengguna atau peran dalam akun manajemen Organisasi yang dapat mengonfigurasi akun anggota sebagai administrator yang didelegasikan untuk Detektif di organisasi

Untuk mengonfigurasi administrator yang didelegasikan menggunakan konsol Detective atau API, lihatMenunjuk akun administrator Detektif untuk suatu organisasidi dalamPanduan Administrasi Detektif Amazon.

AWS CLI, AWS API

Jika Anda ingin mengonfigurasi akun administrator yang didelegasikan menggunakan CLI AWS atau salah satu dari SDK AWS, Anda dapat menggunakan perintah berikut:

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal detective.amazonaws.com
```

- AWSSDK: Hubungi Organisasi`RegisterDelegatedAdministrator`operasi dan nomor ID akun anggota dan mengidentifikasi prinsipal layanan akun`account.amazonaws.com`sebagai parameter.

Menonaktifkan administrator yang didelegasikan untuk Detektif

Anda dapat menghapus administrator yang didelegasikan menggunakan konsol Detektif atau API, atau dengan menggunakan Organisasi`DeregisterDelegatedAdministrator`Operasi CLI atau SDK. Untuk informasi tentang cara menghapus administrator yang didelegasikan menggunakan Detective console atau API Organizations, lihatMenunjuk akun administrator Detektif untuk suatu organisasidi dalamPanduan Administrasi Detektif Amazon.

AmazonDevOpsGuru danAWS Organizations

AmazonDevOpsGuru menganalisis data operasional dan metrik aplikasi dan peristiwa untuk mengidentifikasi perilaku yang menyimpang dari pola operasi normal. Pengguna diberi tahu kapanDevOpsGuru mendeteksi masalah operasional atau risiko.

MenggunakanDevOpsGuru memungkinkan dukungan multi-akun denganAWS Organizations, sehingga Anda dapat menunjuk akun anggota untuk mengelola wawasan di seluruh organisasi Anda. Administrator yang didelegasikan ini kemudian dapat melihat, mengurutkan, dan memfilter wawasan dari semua akun dalam organisasi Anda untuk mengembangkan pandangan holistik tentang kesehatan semua aplikasi yang dipantau dalam organisasi Anda tanpa perlu penyesuaian tambahan.

Untuk informasi lebih lanjut, lihatPantau akun di seluruh organisasidi dalamAmazonDevOpsPanduan Pengguna Guru.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan AmazonDevOpsGuru denganAWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat di akun pengelolaan organisasi Anda bila Anda mengaktifkan akses terpercaya. Peran ini memungkinkanDevOpsGuru untuk melakukan operasi yang didukung dalam akun organisasi Anda di organisasi Anda.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses tepercaya antaraDevOpsGuru dan Organisasi, atau jika Anda menghapus akun anggota dari organisasi.

- `AWSServiceRoleForDevOpsGuru`

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran terkait layanan yang digunakan olehDevOpsGuru memberikan akses ke prinsip-prinsip layanan berikut:

- `devops-guru.amazonaws.com`

Untuk informasi lebih lanjut, lihatMenggunakan peran terkait layanan untukDevOpsGurudi dalamAmazonDevOpsPanduan Pengguna Guru.

Untuk mengaktifkan akses tepercaya denganDevOpsGuru

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

> **Note**
>
> Saat Anda menunjuk administrator yang didelegasikan untuk AmazonDevOpsGuru,DevOpsGuru secara otomatis memungkinkan akses tepercayaDevOpsGuru untuk organisasi Anda.
> DevOpsGuru membutuhkan akses tepercaya keAWS Organizationssebelum Anda dapat menunjuk akun anggota untuk menjadi administrator yang didelegasikan untuk layanan ini untuk organisasi Anda.

> **Important**
>
> Kami sangat menyarankan jika memungkinkan, Anda menggunakan AmazonDevOpsKonsol guru atau alat untuk mengaktifkan integrasi dengan Organisasi. Hal ini memungkinkan AmazonDevOpsGuru melakukan konfigurasi apa pun yang dibutuhkannya, seperti membuat sumber daya yang dibutuhkan oleh layanan. Lanjutkan dengan langkah-langkah ini hanya jika Anda tidak dapat mengaktifkan integrasi menggunakan alat yang disediakan oleh AmazonDevOpsGuru. Untuk informasi lebih lanjut, lihatcatatan ini.

Anda dapat mengaktifkan akses tepercaya dengan menggunakanAWS Organizationskonsol atauDevOpsKonsol Guru.

AWS Management Console

Untuk mengaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. PadaJasahalaman, menemukan baris untukAmazonDevOpsGuru, pilih nama layanan, lalu pilihAktifkan akses tepercaya.
3. Di kotak dialog konfirmasi, aktifkan Menampilkan opsi untuk mengaktifkan akses terpercaya, masukkan **`enable`** dalam kotak, dan kemudian pilih Mengaktifkan akses terpercaya.
4. Jika Anda adalah administrator hanyaAWS Organizations, beri tahu administrator AmazonDevOpsGuru bahwa mereka sekarang dapat mengaktifkan layanan itu menggunakan konsolnya untuk bekerja denganAWS Organizations.

DevOps Guru console

Untuk mengaktifkan akses layanan tepercaya menggunakanDevOpsKonsol Guru

1. Masuk sebagai administrator di akun manajemen dan bukaDevOpsKonsol Guru:AmazonDevOpsKonsol Guru
2. Pilih Aktifkan akses terpercaya.

Untuk menonaktifkan akses tepercaya denganDevOpsGuru

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Hanya administrator diAWS Organizationsakun manajemen dapat menonaktifkan akses tepercaya dengan AmazonDevOpsGuru.

Anda dapat menonaktifkan akses terpercaya hanya menggunakan alat Organizations.

Anda dapat menonaktifkan akses terpercaya dengan menggunakan konsol AWS Organizations.

AWS Management Console

Untuk menonaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. PadaJasahalaman, menemukan baris untukAmazonDevOpsGurudan kemudian pilih nama layanan.
3. Pilih Menonaktifkan akses terpercaya.
4. Di kotak dialog konfirmasi, masukkan **`disable`** dalam kotak, dan kemudian pilih Menonaktifkan akses terpercaya.
5. Jika Anda adalah administrator hanyaAWS Organizations, beri tahu administrator AmazonDevOpsGuru bahwa mereka sekarang dapat menonaktifkan layanan itu menggunakan konsol atau alat-alatnya untuk bekerja denganAWS Organizations.

Mengaktifkan akun administrator yang didelegasikan untukDevOpsGuru

Akun administrator yang didelegasikan untukDevOpsGuru dapat melihat data wawasan dari semua akun anggota yang onboardedDevOpsGuru dari organisasi. Untuk informasi tentang cara administrator yang didelegasikan mengelola akun organisasi, lihatPantau akun di seluruh organisasidi dalamAmazonDevOpsPanduan Pengguna Guru.

Hanya administrator di akun manajemen organisasi yang dapat mengonfigurasi administrator yang didelegasikanDevOpsGuru.

Anda dapat menentukan akun administrator yang didelegasikan dariDevOpsKonsol Guru, atau dengan menggunakan OrganisasiRegisterDelegatedAdministratorOperasi CLI atau SDK.

> **Izin minimum**
>
> Hanya pengguna atau peran dalam akun manajemen Organisasi yang dapat mengonfigurasi akun anggota sebagai administrator yang didelegasikanDevOpsGuru dalam organisasi

DevOps Guru console

Untuk mengkonfigurasi administrator yang didelegasikan diDevOpsKonsol Guru

1. Masuk sebagai administrator di akun manajemen dan bukaDevOpsKonsol Guru:AmazonDevOpsKonsol Guru
2. Pilih Daftar administrator yang didelegasikan. Anda dapat memilih akun Manajemen atau akun anggota apa pun sebagai admin yang didelegasikan.

AWS CLI, AWS API

Jika Anda ingin mengonfigurasi akun administrator yang didelegasikan menggunakan CLI AWS atau salah satu dari SDK AWS, Anda dapat menggunakan perintah berikut:

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal devops-guru.amazonaws.com
```

- AWSSDK: Hubungi OrganisasiRegisterDelegatedAdministratoroperasi dan nomor ID akun anggota dan mengidentifikasi prinsipal layanan akunaccount.amazonaws.comsebagai parameter.

Menonaktifkan administrator yang didelegasikan untukDevOpsGuru

Anda dapat menghapus administrator yang didelegasikan menggunakanDevOpsKonsol Guru, atau dengan menggunakan OrganisasiDeregisterDelegatedAdministratorOperasi CLI atau SDK. Untuk informasi tentang cara menghapus administrator yang didelegasikan

menggunakanDevOpsKonsol Guru, lihatPantau akun di seluruh organisasidi dalamAmazonDevOpsPanduan Pengguna Guru.

AWS Directory Service dan AWS Organizations

AWS Directory Service untuk Direktori Aktif Microsoft, atau AWS Managed Microsoft AD, memungkinkan Anda menjalankan Microsoft Active Directory (AD) sebagai layanan terkelola. AWS Directory Service memudahkan Anda mengatur dan menjalankan direktori di Cloud AWS atau menghubungkan perangkat AWS dengan Direktori Aktif Microsoft on-premise. AWS Managed Microsoft AD juga terintegrasi erat dengan AWS Organizations untuk memungkinkan berbagi direktori secara mulus di beberapa Akun AWS dan setiap VPC di Wilayah. Untuk informasi selengkapnya, lihat AWS Directory Service Panduan Administrasi.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan AWS Directory Service dengan AWS Organizations.

Mengaktifkan akses terpercaya dengan AWS Directory Service

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Anda dapat mengaktifkan akses terpercaya menggunakan konsol AWS Directory Service atau konsol AWS Organizations.

> **Important**
>
> Kami sangat merekomendasikan bahwa bila memungkinkan, Anda menggunakan konsol AWS Directory Service atau alat untuk memungkinkan integrasi dengan Organizations. Hal ini memungkinkan AWS Directory Service melakukan konfigurasi yang diperlukan, seperti membuat sumber daya yang dibutuhkan oleh layanan. Lanjutkan dengan langkah-langkah ini hanya jika Anda tidak dapat mengaktifkan integrasi menggunakan alat yang disediakan olehAWS Directory Service. Untuk informasi selengkapnya, lihat catatan ini.
> Jika Anda mengaktifkan akses terpercaya dengan menggunakan konsol AWS Directory Service atau alat, Anda tidak perlu menyelesaikan langkah-langkah ini.

Untuk mengaktifkan akses menggunakan konsol AWS Directory Service

Untuk berbagi direktori, yang secara otomatis mengaktifkan akses terpercaya, lihat Bagikan direktori Anda di Panduan Administrasi AWS Directory Service. Untuk step-by-step petunjuknya, lihat Tutorial: Berbagi Direktori Iklan MicrosoftAWS Terkelola Anda.

Anda dapat mengaktifkan akses terpercaya dengan menggunakan konsol AWS Organizations.

AWS Management Console

Untuk mengaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk AWS Directory Service, pilih nama layanan, dan kemudian Mengaktifkan akses terpercaya.
3. Di kotak dialog konfirmasi, aktifkan Menampilkan opsi untuk mengaktifkan akses terpercaya, masukkan **`enable`** dalam kotak, dan kemudian pilih Mengaktifkan akses terpercaya.
4. Jika Anda adalah administrator hanya AWS Organizations, beritahu administrator AWS Directory Service bahwa mereka sekarang dapat mengaktifkan layanan tersebut menggunakan konsolnya untuk bekerja dengan AWS Organizations.

Menonaktifkan akses terpercaya dengan AWS Directory Service

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Jika Anda menonaktifkan akses terpercaya menggunakan AWS Organizations saat anda menggunakan AWS Directory Service, semua direktori bersama sebelumnya terus beroperasi seperti biasa. Namun, Anda tidak dapat lagi berbagi direktori baru dalam organisasi sampai Anda mengaktifkan akses terpercaya lagi.

Anda dapat menonaktifkan akses terpercaya hanya menggunakan alat Organizations.

Anda dapat menonaktifkan akses terpercaya dengan menggunakan konsol AWS Organizations.

AWS Management Console

Untuk menonaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk AWS Directory Service dan kemudian pilih nama layanan.
3. Pilih Menonaktifkan akses terpercaya.
4. Di kotak dialog konfirmasi, masukkan **`disable`** dalam kotak, dan kemudian pilih Menonaktifkan akses terpercaya.
5. Jika Anda adalah administrator hanya AWS Organizations, beritahu administrator AWS Directory Service bahwa mereka sekarang dapat menonaktifkan layanan tersebut menggunakan konsolnya untuk bekerja dengan AWS Organizations.

AWS Firewall Manager dan AWS Organizations

AWS Firewall Manager adalah layanan manajemen keamanan yang Anda gunakan untuk secara terpusat mengonfigurasi dan mengelola aturan firewall dan perlindungan lainnya di seluruh Akun AWS dan aplikasi di organisasi Anda. Menggunakan Firewall Manager, Anda dapat meluncurkan aturan AWS WAF, membuat proteksi AWS Shield Advanced, mengonfigurasi, dan meng-audit grup keamanan Amazon Virtual Private Cloud (Amazon VPC), dan men-deploy AWS Network Firewall. Gunakan Firewall Manager untuk mengatur proteksi Anda sekali saja dan menerapkannya secara otomatis di semua akun dan sumber daya dalam organisasi Anda, bahkan saat sumber daya dan akun baru ditambahkan. Untuk informasi selengkapnya tentang AWS Firewall Manager, lihat Panduan Developer AWS Firewall Manager.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan AWS Firewall Manager dengan AWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat di akun pengelolaan organisasi Anda bila Anda mengaktifkan akses terpercaya. Peran ini memungkinkan Firewall Manager untuk melakukan operasi yang didukung dalam akun organisasi Anda di organisasi Anda.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses terpercaya antara Firewall Manager dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

- `AWSServiceRoleForFMS`

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran tertaut layanan yang digunakan oleh Firewall Manager memberikan akses ke prinsipal layanan berikut:

- `fms.amazonaws.com`

Mengaktifkan akses terpercaya dengan Firewall Manager

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Anda dapat mengaktifkan akses terpercaya menggunakan konsol AWS Firewall Manager atau konsol AWS Organizations.

> **Important**
>
> Kami sangat merekomendasikan bahwa bila memungkinkan, Anda menggunakan konsol AWS Firewall Manager atau alat untuk memungkinkan integrasi dengan Organizations. Hal ini memungkinkan AWS Firewall Manager melakukan konfigurasi yang diperlukan, seperti membuat sumber daya yang dibutuhkan oleh layanan. Lanjutkan dengan langkah-langkah ini ini yang disediakan olehAWS Firewall Manager. Untuk informasi selengkapnya, lihat.
> Jika Anda mengaktifkan akses terpercaya dengan menggunakan konsol AWS Firewall Manager atau alat, Anda tidak perlu menyelesaikan langkah-langkah ini.

Anda harus masuk dengan akun pengelolaan AWS Organizations dan mengonfigurasi account dalam organisasi sebagai akun administrator AWS Firewall Manager. Untuk informasi selengkapnya, lihat, Mengatur Akun Administrator AWS Firewall Manager di Panduan Developer AWS Firewall Manager.

Anda dapat mengaktifkan akses terpercaya dengan menggunakan konsol AWS Organizations, dengan menjalankan perintah AWS CLI, atau dengan memanggil operasi API di salah satu SDK AWS.

AWS Management Console

Untuk mengaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk AWS Firewall Manager, pilih nama layanan, dan kemudian Mengaktifkan akses terpercaya.
3. Di kotak dialog konfirmasi, aktifkan Menampilkan opsi untuk mengaktifkan akses terpercaya, masukkan **`enable`** dalam kotak, dan kemudian pilih Mengaktifkan akses terpercaya.
4. Jika Anda adalah administrator hanya AWS Organizations, beritahu administrator AWS Firewall Manager bahwa mereka sekarang dapat mengaktifkan layanan tersebut menggunakan konsolnya untuk bekerja dengan AWS Organizations.

AWS CLI, AWS API

Untuk mengaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk mengaktifkan atau mengaktifkan akses layanan terpercaya:

- AWS CLI: enable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk mengaktifkan AWS Firewall Manager sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal fms.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWSAPI: AktifkanAWSServiceAccess

Menonaktifkan akses terpercaya dengan Firewall Manager

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Anda dapat menonaktifkan akses terpercaya menggunakan AWS Firewall Manager atau alat AWS Organizations.

> **Important**
>
> Kami sangat merekomendasikan bahwa bila memungkinkan, Anda menggunakan konsol AWS Firewall Manager atau alat untuk menonaktifkan integrasi dengan Organizations. Hal ini memungkinkan AWS Firewall Manager melakukan pembersihan apa pun yang diperlukan, seperti menghapus sumber daya atau peran akses yang tidak lagi diperlukan oleh layanan. Lanjutkan dengan langkah-langkah ini hanya jika Anda tidak dapat menonaktifkan integrasi menggunakan alat yang disediakan oleh AWS Firewall Manager.
> Jika Anda menonaktifkan akses tepercaya dengan menggunakan konsol AWS Firewall Manager atau alat, Anda tidak perlu menyelesaikan langkah-langkah ini.

Untuk menonaktifkan akses terpercaya menggunakan konsol Firewall Manager

Anda dapat mengubah atau mencabut opsi AWS Firewall Manager dengan mengikuti petunjuk di Menetapkan Akun yang Berbeda sebagai Akun Administrator AWS Firewall Manager di Panduan Developer AWS Firewall Manager.

Jika Anda mencabut akun administrator, Anda harus masuk ke AWS Organizations dan tetapkan akun administrator baru untuk AWS Firewall Manager.

Anda dapat menonaktifkan akses terpercaya dengan menggunakan konsol AWS Organizations, dengan menjalankan perintah AWS CLI, atau dengan memanggil operasi API Organizations di salah satu SDK AWS.

AWS Management Console

Untuk menonaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk AWS Firewall Manager dan kemudian pilih nama layanan.
3. Pilih Menonaktifkan akses terpercaya.

4. Di kotak dialog konfirmasi, masukkan **`disable`** dalam kotak, dan kemudian pilih Menonaktifkan akses terpercaya.
5. Jika Anda adalah administrator hanya AWS Organizations, beritahu administrator AWS Firewall Manager bahwa mereka sekarang dapat menonaktifkan layanan tersebut menggunakan konsolnya untuk bekerja dengan AWS Organizations.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk menonaktifkan akses layanan terpercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan AWS Firewall Manager sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal fms.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWSAPI: NonaktifkanAWSServiceAccess

Mengaktifkan akun administrator yang didelegasikan untuk Firewall Manager

Bila Anda menetapkan akun anggota sebagai administrator yang didelegasikan untuk organisasi, pengguna dan peran dari akun tersebut dapat melakukan tindakan administratif untuk Firewall Manager yang jika tidak dapat dilakukan hanya oleh pengguna atau peran dalam akun pengelolaan organisasi. Ini membantu Anda untuk memisahkan manajemen organisasi dari manajemen Firewall Manager.

> **Izin minimum**
>
> Hanya pengguna atau peran dalam akun pengelolaan Organizations yang dapat mengonfigurasi akun anggota sebagai administrator yang didelegasikan untuk Firewall Manager di organisasi.

Untuk petunjuk tentang cara menetapkan akun anggota sebagai administrator Firewall Manager untuk organisasi, lihat Mengatur Akun Administrator AWS Firewall Manager di Panduan Developer AWS Firewall Manager.

Amazon GuardDuty danAWS Organizations

Amazon GuardDuty adalah layanan pemantauan keamanan berkelanjutan yang menganalisis dan memproses berbagai sumber data, menggunakan umpan cerdas ancaman dan machine learning untuk mengidentifikasi aktivitas yang tidak terduga dan berpotensi tidak sah dan berbahaya dalamAWSlingkungan Ini dapat mencakup masalah, seperti eskalasi hak istimewa, penggunaan kredensyal yang terbuka, komunikasi dengan alamat IP berbahaya, URL, atau domain, atau keberadaan malware di instans Amazon Elastic Compute Cloud dan beban kerja kontainer.

Anda dapat membantu menyederhanakan pengelolaan GuardDuty dengan menggunakan Organizations untuk mengelola GuardDuty di semua akun di organisasi Anda.

Untuk informasi selengkapnya, lihatMengelola GuardDuty akun denganAWS Organizationsdi dalamAmazon GuardDuty Panduan Pengguna

Gunakan informasi berikut untuk membantu Anda mengintegrasikan Amazon GuardDuty bersamaAWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat di akun pengelolaan organisasi Anda bila Anda mengaktifkan akses terpercaya. Peran ini memungkinkan GuardDuty untuk melakukan operasi yang didukung dalam akun organisasi Anda di organisasi Anda. Anda dapat menghapus peran hanya jika Anda menonaktifkan akses tepercaya antara GuardDuty dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

- Parameter`AWSServiceRoleForAmazonGuardDuty`peran yang terhubung dengan layanan secara otomatis dibuat di akun yang telah terintegrasi GuardDuty dengan Organizations. Untuk informasi selengkapnya, lihatMengelola GuardDutyakun dengan Organizationsdi dalamAmazon GuardDuty Panduan Pengguna
- Parameter`AmazonGuardDutyMalwareProtectionServiceRolePolicy`peran yang terhubung dengan layanan secara otomatis dibuat di akun yang telah diaktifkan GuardDuty Perlindungan Malware. Untuk informasi selengkapnya, lihatIzin peran terkait layanan untuk GuardDuty Perlindungan Malwaredi dalamAmazon GuardDuty Panduan Pengguna

Prinsipal layanan yang digunakan oleh peran tertaut layanan

- `guardduty.amazonaws.com`, digunakan oleh`AWSServiceRoleForAmazonGuardDuty`peran yang terhubung dengan layanan
- `malware-protection.guardduty.amazonaws.com`, digunakan oleh`AmazonGuardDutyMalwareProtectionServiceRolePolicy`peran yang terhubung dengan layanan

Mengaktifkan akses terpercaya dengan GuardDuty

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Anda dapat mengaktifkan akses terpercaya hanya menggunakan Amazon GuardDuty.

Amazon GuardDuty memerlukan akses terpercaya keAWS Organizationssebelum Anda dapat menetapkan akun anggota menjadi GuardDuty administrator untuk organisasi Anda. Jika Anda mengkonfigurasi administrator yang didelegasikan dengan GuardDuty konsol GuardDuty secara otomatis memungkinkan akses terpercaya untuk Anda.

Namun, jika Anda ingin mengonfigurasi akun administrator yang didelegasikan menggunakanAWS CLIatau salah satuAWSSDK, maka Anda harus secara eksplisit memanggilAktifkanAWSServiceAccessoperasi dan menyediakan layanan utama sebagai parameter. Maka Anda dapat meneleponEnableOrganizationAdminAccountuntuk mendelegasikan GuardDuty akun administrator

Menonaktifkan akses terpercaya dengan GuardDuty

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Anda dapat menonaktifkan akses terpercaya hanya menggunakan alat Organizations.

Anda dapat menonaktifkan akses terpercaya dengan menjalankan perintah AWS CLI Organizations, atau dengan memanggil operasi API Organizations di salah satu SDK AWS.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk menonaktifkan akses layanan terpercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan Amazon GuardDuty sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal guardduty.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.

- API AWS: NonaktifkanAWSServiceAccess

Mengaktifkan akun administrator yang didelegasikan GuardDuty

Bila Anda menetapkan akun anggota sebagai administrator yang didelegasikan untuk organisasi, pengguna dan peran dari akun tersebut dapat melakukan tindakan administratif GuardDuty yang jika tidak dapat dilakukan hanya oleh pengguna atau peran dalam akun pengelolaan organisasi. Ini membantu Anda untuk memisahkan manajemen organisasi dari manajemen GuardDuty.

> **Izin minimum**
>
> Untuk informasi tentang izin yang diperlukan untuk menetapkan akun anggota sebagai administrator yang didelegasikan, lihatIzin yang diperlukan untuk menetapkan administrator yang didelegasikandi dalamAmazon GuardDuty Panduan Pengguna

Untuk menetapkan akun anggota sebagai administrator yang didelegasikan GuardDuty

Lihat Tetapkan administrator yang didelegasikan dan tambahkan akun anggota (konsol) dan Tetapkan administrator yang didelegasikan dan tambahkan akun anggota (API)

AWS Health dan AWS Organizations

AWS Health memberikan visibilitas berkelanjutan ke kinerja sumber daya Anda dan ketersediaan AWS layanan dan akun Anda. AWS Health mengirimkan acara ketika AWS sumber daya dan layanan Anda dipengaruhi oleh masalah atau akan terpengaruh oleh perubahan yang akan datang.

Setelah Anda mengaktifkan tampilan organisasi, pengguna di akun manajemen organisasi dapat menggabungkan AWS Health peristiwa di semua akun di organisasi. Tampilan organisasi hanya menampilkan AWS Health peristiwa yang dikirimkan setelah fitur diaktifkan dan mempertahankannya selama 90 hari.

Anda dapat mengaktifkan tampilan organisasi dengan menggunakan AWS Health konsol, AWS Command Line Interface (AWS CLI), atau AWS Health API.

Untuk informasi selengkapnya, lihat Menggabungkan AWS Health peristiwa di AWS Health Panduan Pengguna.

Gunakan informasi berikut untuk membantu Anda AWS Health berintegrasi AWS Organizations.

Peran terkait layanan untuk integrasi

Peran `AWSServiceRoleForHealth_Organizations` terkait layanan memungkinkan AWS Health untuk melakukan operasi yang didukung dalam akun organisasi Anda di organisasi Anda.

Peran ini dibuat secara otomatis di akun manajemen organisasi Anda saat Anda mengaktifkan akses tepercaya dengan memanggil operasi EnableHealthServiceAccessForOrganizationAPI. Jika tidak, buat peran menggunakan AWS Health konsol, API, atau CLI, seperti yang dijelaskan dalam Membuat peran terkait layanan di Panduan Pengguna IAM.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses tepercaya antara AWS Health dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran terkait layanan yang digunakan oleh AWS Health memberikan akses ke prinsipal layanan berikut:

- `health.amazonaws.com`

Mengaktifkan akses terpercaya dengan AWS Health

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Saat Anda mengaktifkan fitur tampilan organisasi AWS Health, akses tepercaya juga diaktifkan untuk Anda secara otomatis.

Anda dapat mengaktifkan akses tepercaya menggunakan AWS Health konsol atau AWS Organizations konsol.

> **Important**
>
> Kami sangat menyarankan bahwa bila memungkinkan, Anda menggunakan AWS Health konsol atau alat untuk mengaktifkan integrasi dengan Organizations. Ini memungkinkan AWS Health melakukan konfigurasi apa pun yang diperlukan, seperti membuat sumber daya yang dibutuhkan oleh layanan. Lanjutkan dengan langkah-langkah ini hanya jika Anda tidak dapat mengaktifkan integrasi menggunakan alat yang disediakan oleh AWS Health. Untuk informasi lebih lanjut, lihat catatan ini.
> Jika Anda mengaktifkan akses tepercaya dengan menggunakan AWS Health konsol atau alat maka Anda tidak perlu menyelesaikan langkah-langkah ini.

Untuk mengaktifkan akses tepercaya menggunakan AWS Health konsol

Anda dapat mengaktifkan akses tepercaya dengan menggunakan AWS Health dan salah satu opsi berikut:

- Gunakan AWS Health konsol. Untuk informasi selengkapnya, lihat Tampilan organisasi (konsol) di Panduan Pengguna AWS Health .
- Gunakan AWS CLI. Untuk informasi selengkapnya, lihat Tampilan organisasi (CLI) di Panduan Pengguna AWS Health .
- Panggil operasi EnableHealthServiceAccessForOrganizationAPI.

Anda dapat mengaktifkan akses tepercaya dengan menjalankan AWS CLI perintah Organizations, atau dengan memanggil operasi Organizations API di salah satu AWS SDK.

AWS CLI, AWS API

Untuk mengaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan AWS CLI perintah atau operasi API berikut untuk mengaktifkan akses layanan tepercaya:

- AWS CLI: enable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk mengaktifkan AWS Health sebagai layanan tepercaya dengan Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal health.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWS API: Aktifkan AWSServiceAccess

Menonaktifkan akses terpercaya dengan AWS Health

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Setelah menonaktifkan fitur tampilan organisasi, AWS Health berhenti menggabungkan peristiwa untuk semua akun lain di organisasi Anda. Ini juga menonaktifkan akses terpercaya untuk Anda secara otomatis.

Anda dapat menonaktifkan akses tepercaya menggunakan AWS Organizations alat AWS Health atau alat.

> **Important**
>
> Kami sangat menyarankan bahwa bila memungkinkan, Anda menggunakan AWS Health konsol atau alat untuk menonaktifkan integrasi dengan Organizations. Ini memungkinkan AWS Health melakukan pembersihan apa pun yang diperlukan, seperti menghapus sumber daya atau peran akses yang tidak lagi diperlukan oleh layanan. Lanjutkan dengan langkah-langkah ini hanya jika Anda tidak dapat menonaktifkan integrasi menggunakan alat yang disediakan oleh AWS Health.
> Jika Anda menonaktifkan akses tepercaya dengan menggunakan AWS Health konsol atau alat maka Anda tidak perlu menyelesaikan langkah-langkah ini.

Untuk menonaktifkan akses tepercaya menggunakan AWS Health konsol

Anda dapat menonaktifkan akses yang dipercaya dengan salah satu opsi berikut:

- Gunakan AWS Health konsol. Untuk informasi selengkapnya, lihat Menonaktifkan tampilan organisasi (konsol) di Panduan Pengguna AWS Health .
- Gunakan AWS CLI. Untuk informasi selengkapnya, lihat Menonaktifkan tampilan organisasi (CLI) di Panduan Pengguna AWS Health .
- Panggil operasi DisableHealthServiceAccessForOrganizationAPI.

Anda dapat menonaktifkan akses tepercaya dengan menjalankan AWS CLI perintah Organizations, atau dengan memanggil operasi Organizations API di salah satu AWS SDK.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan AWS CLI perintah atau operasi API berikut untuk menonaktifkan akses layanan tepercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan AWS Health sebagai layanan tepercaya dengan Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal health.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWS API: Nonaktifkan AWSServiceAccess

Mengaktifkan akun administrator yang didelegasikan untuk AWS Health

Ketika Anda menetapkan akun anggota sebagai administrator yang didelegasikan untuk organisasi, pengguna dan peran dari akun tersebut dapat melakukan tindakan administratif untuk AWS Health itu hanya dapat dilakukan oleh pengguna atau peran dalam akun manajemen organisasi. Ini membantu Anda memisahkan manajemen organisasi dari manajemen AWS Health.

Untuk menunjuk akun anggota sebagai administrator yang didelegasikan untuk AWS Health

Lihat Mendaftarkan administrator yang didelegasikan untuk tampilan organisasi Anda

Untuk menghapus administrator yang didelegasikan untuk AWS Health

Lihat Menghapus administrator yang didelegasikan dari tampilan organisasi

Inspektur Amazon danAWS Organizations

Amazon Inspector adalah layanan manajemen kerentanan otomatis yang secara terus-menerus memindai Amazon EC2 dan beban kerja kontainer untuk kerentanan perangkat lunak dan eksposur jaringan yang tidak diinginkan.

Menggunakan Amazon Inspector Anda dapat mengelola beberapa akun yang terkait melaluiAWS Organizationshanya dengan mendelegasikan akun administrator untuk Amazon Inspector. Administrator yang didelegasikan mengelola Amazon Inspector untuk organisasi dan diberikan izin khusus untuk melakukan tugas atas nama organisasi Anda seperti:

- Mengaktifkan atau menonaktifkan pemindaian untuk akun anggota
- Melihat data temuan agregat dari seluruh organisasi
- Membuat dan mengelola aturan penindasan

Untuk informasi lebih lanjut, lihatMengelola beberapa akun denganAWS Organizationsdi dalamPanduan Pengguna Inspektur Amazon.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan Amazon Inspector denganAWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat di akun pengelolaan organisasi Anda bila Anda mengaktifkan akses terpercaya. Peran ini memungkinkan Amazon Inspector untuk melakukan operasi yang didukung dalam akun organisasi Anda di organisasi Anda.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses tepercaya antara Amazon Inspector dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

- `AWSServiceRoleForAmazonInspector2`

Untuk informasi lebih lanjut, lihatMenggunakan peran terkait layanan dengan Amazon Inspectordi dalamPanduan Pengguna Inspektur Amazon.

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran terkait layanan yang digunakan oleh Amazon Inspector memberikan akses ke prinsip-prinsip layanan berikut:

- `inspector2.amazonaws.com`

Untuk mengaktifkan akses tepercaya dengan Amazon Inspector

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Amazon Inspector memerlukan akses tepercaya keAWS Organizationssebelum Anda dapat menunjuk akun anggota untuk menjadi administrator yang didelegasikan untuk layanan ini untuk organisasi Anda.

Saat Anda menunjuk administrator yang didelegasikan untuk Amazon Inspector, Amazon Inspector secara otomatis mengaktifkan akses tepercaya untuk Amazon Inspector untuk organisasi Anda.

Namun, jika Anda ingin mengkonfigurasi akun administrator yang didelegasikan menggunakanAWSCLI atau salah satuAWSSDK, maka Anda harus secara eksplisit memanggil`EnableAWSServiceAccess`operasi dan menyediakan layanan utama sebagai parameter. Maka Anda dapat menelepon`EnableDelegatedAdminAccount`untuk mendelegasikan akun administrator Inspektur.

Anda dapat mengaktifkan akses terpercaya dengan menjalankan perintah AWS CLI Organizations, atau dengan memanggil operasi API Organizations di salah satu SDK AWS.

AWS CLI, AWS API

Untuk mengaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk mengaktifkan atau mengaktifkan akses layanan terpercaya:

- AWS CLI: enable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk mengaktifkan Amazon Inspector sebagai layanan tepercaya dengan Organisasi.

```
$ aws organizations enable-aws-service-access \
    --service-principal inspector2.amazonaws.com
```

Perintah ini tidak menghasilkan output saat berhasil.

- AWSAPI:AktifkanAWSServiceAccess

> **Note**
>
> Jika Anda menggunakan`EnableAWSServiceAccess`API, Anda juga perlu menelepon`EnableDelegatedAdminAccount`untuk mendelegasikan akun administrator Inspektur.

Menonaktifkan akses tepercaya dengan Amazon Inspector

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Hanya administrator diAWS Organizationsakun manajemen dapat menonaktifkan akses tepercaya dengan Amazon Inspector.

Anda dapat menonaktifkan akses terpercaya hanya menggunakan alat Organizations.

Anda dapat menonaktifkan akses terpercaya dengan menjalankan perintah AWS CLI Organizations, atau dengan memanggil operasi API Organizations di salah satu SDK AWS.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk menonaktifkan akses layanan terpercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan Amazon Inspector sebagai layanan tepercaya dengan Organisasi.

```
$ aws organizations disable-aws-service-access \
```

```
    --service-principal inspector2.amazonaws.com
```

Perintah ini tidak menghasilkan output saat berhasil.

- AWSAPI:NonaktifkanAWSServiceAccess

Mengaktifkan akun administrator yang didelegasikan untuk Amazon Inspector

Dengan Amazon Inspector, Anda dapat mengelola beberapa akun dalam organisasi menggunakan administrator yang didelegasikan denganAWS Organizationslayanan.

YangAWS Organizationsakun manajemen menunjuk akun dalam organisasi sebagai akun administrator yang didelegasikan untuk Amazon Inspector. Administrator yang didelegasikan mengelola Amazon Inspector untuk organisasi dan diberikan izin khusus untuk melakukan tugas atas nama organisasi Anda seperti: mengaktifkan atau menonaktifkan pemindaian untuk akun anggota, melihat data temuan gabungan dari seluruh organisasi, dan membuat dan mengelola aturan penindasan

Untuk informasi tentang cara administrator yang didelegasikan mengelola akun organisasi, lihatMemahami hubungan antara administrator dan akun anggotadi dalamPanduan Pengguna Inspektur Amazon.

Hanya administrator di akun manajemen organisasi yang dapat mengonfigurasi administrator yang didelegasikan untuk Amazon Inspector.

Anda dapat menentukan akun administrator yang didelegasikan dari konsol atau API Amazon Inspector, atau dengan menggunakan operasi CLI atau SDK Organisasi.

> **Izin minimum**
>
> Hanya pengguna atau peran dalam akun manajemen Organisasi yang dapat mengonfigurasi akun anggota sebagai administrator yang didelegasikan untuk Amazon Inspector di organisasi

Untuk mengonfigurasi administrator yang didelegasikan menggunakan konsol Amazon Inspector, lihatLangkah 1: Aktifkan Amazon Inspector - Lingkungan multi-akundi dalamPanduan Pengguna Inspektur Amazon.

> **Note**
>
> Anda harus meneleponinspector2:enableDelegatedAdminAccountdi setiap wilayah tempat Anda menggunakan Amazon Inspector.

AWS CLI, AWS API

Jika Anda ingin mengonfigurasi akun administrator yang didelegasikan menggunakan CLI AWS atau salah satu dari SDK AWS, Anda dapat menggunakan perintah berikut:

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal inspector2.amazonaws.com
```

- AWSSDK: Hubungi OrganisasiRegisterDelegatedAdministratoroperasi dan nomor ID akun anggota dan mengidentifikasi prinsipal layanan akunaccount.amazonaws.comsebagai parameter.

Menonaktifkan administrator yang didelegasikan untuk Amazon Inspector

Hanya administrator diAWS Organizationsakun manajemen dapat menghapus akun administrator yang didelegasikan dari organisasi.

Anda dapat menghapus administrator yang didelegasikan menggunakan konsol atau API Amazon Inspector, atau dengan menggunakan OrganisasiDeregisterDelegatedAdministratorOperasi CLI atau SDK. Untuk menghapus administrator yang didelegasikan menggunakan konsol Amazon Inspector, lihatMenghapus administrator yang didelegasikandi dalamPanduan Pengguna Inspektur Amazon.

AWS License Manager dan AWS Organizations

AWS License Manager menyederhanakan proses membawa lisensi vendor perangkat lunak ke cloud. Saat Anda membangun infrastruktur cloud diAWS, Anda dapat menghemat biaya dengan menggunakan peluang bring-your-own-license (BYOL) —yaitu, dengan menggunakan kembali inventaris lisensi yang ada untuk digunakan dengan sumber daya cloud. Dengan kendali berbasis aturan pada konsumsi lisensi, administrator dapat menetapkan batas keras atau lunak pada

penyebaran cloud baru dan yang sudah ada, dengan menghentikan penggunaan server yang tidak sesuai sebelum terjadi.

Untuk informasi selengkapnya tentang License Manager, lihat Panduan Pengguna License Manager.

Dengan menautkan License Manager denganAWS Organizations, Anda dapat:

- Aktifkan penemuan lintas akun sumber daya komputasi di seluruh organisasi Anda.
- Lihat dan kelola langganan Linux komersial yang Anda miliki dan jalankanAWS. Untuk informasi selengkapnya, lihat langganan Linux diAWS License Manager.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan AWS License Manager dengan AWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat di akun pengelolaan organisasi Anda saat Anda mengaktifkan akses terpercaya. Peran ini memungkinkan License Manager untuk melakukan operasi yang didukung dalam akun organisasi Anda di organisasi Anda.

Anda dapat menghapus atau mengubah peran hanya jika Anda menonaktifkan akses terpercaya antara License Manager dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

- `AWSLicenseManagerMasterAccountRole`
- `AWSLicenseManagerMemberAccountRole`
- `AWSServiceRoleForAWSLicenseManagerRole`
- `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService`

Untuk informasi selengkapnya, lihat License Manager Lisensi—Peran akun manajemen, License Manager Lisensi—Peran akun Anggota, dan License Manager Lisensi—peran langganan Linux.

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran tertaut layanan yang digunakan oleh License Manager memberikan akses ke prinsipal layanan berikut:

- `license-manager.amazonaws.com`

- `license-manager.member-account.amazonaws.com`
- `license-manager-linux-subscriptions.amazonaws.com`

Mengaktifkan akses terpercaya dengan License Manager

Anda dapat mengaktifkan akses terpercaya hanya menggunakan AWS License Manager.

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Untuk mengaktifkan akses terpercaya dengan License Manager

Anda harus masuk ke konsol License Manager menggunakan perangkat AWS Organizations dan mengaitkannya dengan akun License Manager Anda. Untuk informasi selengkapnya, lihat Pengaturan diAWS License Manager.

Menonaktifkan akses terpercaya dengan License Manager

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Anda dapat menonaktifkan akses terpercaya hanya menggunakan alat Organizations.

Anda dapat menonaktifkan akses terpercaya dengan menjalankanAWS CLI perintah Organizations, atau dengan memanggil operasi API Organizations di salah satuAWS SDK.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk menonaktifkan akses layanan terpercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan AWS License Manager sebagai layanan terpercaya dengan Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal license-manager.amazonaws.com
```

Perintah ini tidak menghasilkan output saat berhasil.

Untuk menonaktifkan akses terpercaya untuk langganan Linux gunakan:

```
$  aws organizations disable-aws-service-access \
    --service-principal license-manager-linux-subscriptions.amazonaws.com
```

- AWSAPI: NonaktifkanAWSServiceAccess

Mengaktifkan akun administrator yang didelegasikan untuk License Manager

Ketika Anda menetapkan akun anggota sebagai administrator yang didelegasikan untuk, pengguna organisasi dan peran dari akun yang dapat melakukan tindakan administratif untuk License Manager yang sebaliknya dapat dilakukan hanya oleh pengguna atau peran dalam akun pengelolaan organisasi. Ini membantu Anda untuk memisahkan manajemen organisasi dari manajemen License Manager.

Untuk mendelegasikan akun anggota sebagai administrator untuk License Manager, ikuti langkah-langkah di Daftarkan administrator yang didelegasikan di Panduan Pengguna License Manager.

Amazon Macie dan AWS Organizations

Amazon Macie adalah layanan keamanan data dan privasi data yang dikelola sepenuhnya yang menggunakan machine learning dan pencocokan pola untuk menemukan, memantau, dan membantu Anda melindungi data sensitif Anda di Amazon Simple Storage Service (Amazon S3). Macie mengotomatisasi penemuan data sensitif, seperti informasi pengenal pribadi (PII) dan kekayaan intelektual, untuk memberi Anda pemahaman yang lebih baik tentang data yang disimpan organisasi Anda di Amazon S3.

Untuk informasi selengkapnya, lihat Mengelola akun Amazon Macie denganAWS Organizations di Panduan Pengguna Amazon Macie.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan Amazon Macie dengan AWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat untuk akun administrator Macie yang didelegasikan oleh organisasi Anda saat Anda mengaktifkan akses terpercaya. Peran ini memungkinkan Macie melakukan operasi yang didukung untuk akun di organisasi Anda.

Anda dapat menghapus peran ini hanya jika Anda menonaktifkan akses terpercaya antara Macie dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

- `AWSServiceRoleRorAmazonMacie`

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran tertaut layanan yang digunakan oleh Macie memberikan akses ke prinsipal layanan berikut:

- `macie.amazonaws.com`

Mengaktifkan akses terpercaya dengan Macie

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Anda dapat mengaktifkan akses terpercaya menggunakan konsol Amazon Macie atau konsol AWS Organizations.

> **Important**
>
> Kami sangat merekomendasikan bahwa bila memungkinkan, Anda menggunakan konsol Amazon Macie atau alat untuk mengaktifkan integrasi dengan Organizations. Ini memungkinkan Amazon Macie melakukan konfigurasi yang membutuhkan, seperti menciptakan sumber daya yang dibutuhkan oleh layanan. Lanjutkan dengan langkah-langkah ini hanya jika Anda tidak dapat mengaktifkan integrasi menggunakan alat yang disediakan oleh Amazon Macie. Untuk informasi lebih lanjut, lihat Catatan lebih lanjut, lihat lebih lanjut, lihat lebih lanjut, lihat
> Jika Anda mengaktifkan akses terpercaya dengan menggunakan konsol Amazon Macie atau alat maka Anda tidak perlu menyelesaikan langkah-langkah ini.

Untuk mengaktifkan akses terpercaya menggunakan konsol Macie

Amazon Macie memerlukan akses terpercaya ke AWS Organizations untuk menetapkan akun anggota sebagai administrator Macie untuk organisasi Anda. Jika Anda mengonfigurasi administrator yang didelegasikan menggunakan konsol manajemen Macie, maka Macie secara otomatis mengaktifkan akses terpercaya untuk Anda.

Untuk informasi selengkapnya, lihat Mengintegrasikan dan mengonfigurasi organisasi di Amazon Macie di Panduan Pengguna Amazon Macie.

Anda dapat mengaktifkan akses terpercaya dengan menjalankan perintah AWS CLI Organizations, atau dengan memanggil operasi API Organizations di salah satu SDK AWS.

AWS CLI, AWS API

Untuk mengaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk mengaktifkan atau mengaktifkan akses layanan terpercaya:

- AWS CLI: enable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk mengaktifkan Amazon Macie sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal macie.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWSAPI: AktifkanAWSServiceAccess

Mengaktifkan akun administrator yang didelegasikan untuk Macie

Ketika Anda menetapkan akun anggota sebagai administrator yang didelegasikan untuk organisasi, pengguna dan peran dari akun tersebut dapat melakukan tindakan administratif untuk Macie yang sebaliknya dapat dilakukan hanya oleh pengguna atau peran dalam akun pengelolaan organisasi. Ini membantu Anda untuk memisahkan manajemen organisasi dari manajemen Macie.

Izin minimum

Hanya pengguna atau peran dalam akun pengelolaan Organizations dengan izin berikut dapat mengonfigurasi akun anggota sebagai administrator yang didelegasikan untuk Macie di organisasi:

- `organizations:EnableAWSServiceAccess`
- `macie:EnableOrganizationAdminAccount`

Untuk menetapkan akun anggota sebagai administrator yang didelegasikan untuk Macie

Amazon Macie memerlukan akses terpercaya ke AWS Organizations untuk menetapkan akun anggota sebagai administrator Macie untuk organisasi Anda. Jika Anda mengonfigurasi administrator yang didelegasikan menggunakan konsol manajemen Macie, maka Macie secara otomatis mengaktifkan akses terpercaya untuk Anda.

Untuk informasi lebih lanjut, lihat https://docs.aws.amazon.com/macie/latest/user/macie-organizations.html#register-delegated-admin

AWS Marketplace dan AWS Organizations

AWS Marketplace adalah katalog digital terkurasi yang dapat Anda gunakan untuk menemukan, membeli, men-deploy, dan mengelola perangkat lunak, data, dan layanan pihak ketiga yang Anda butuhkan untuk membangun solusi dan menjalankan bisnis Anda.

AWS Marketplace membuat dan mengelola lisensi menggunakan AWS License Manager untuk pembelian Anda di AWS Marketplace. Ketika Anda membagikan (memberikan akses ke) lisensi Anda dengan akun lain di organisasi Anda, AWS Marketplace membuat dan mengelola lisensi baru untuk akun tersebut.

Untuk informasi lebih lanjut, lihat Peran tertaut layanan untuk AWS Marketplace dalam Panduan Pembeli AWS Marketplace.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan AWS Marketplace dengan AWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat di akun pengelolaan organisasi Anda bila Anda mengaktifkan akses terpercaya. Peran ini memungkinkan AWS Marketplace untuk menjalankan operasi yang didukung di akun organisasi Anda di organisasi Anda.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses terpercaya antara AWS Marketplace dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

- `AWSServiceRoleForMarketplaceLicenseManagement`

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran tertaut layanan yang digunakan oleh AWS Marketplace memberikan akses ke prinsipal layanan berikut:

- `license-management.marketplace.amazonaws.com`

Mengaktifkan akses terpercaya dengan AWS Marketplace

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Anda dapat mengaktifkan akses terpercaya menggunakan konsol AWS Marketplace atau konsol AWS Organizations.

> **Important**
>
> Kami sangat merekomendasikan bahwa bila memungkinkan, Anda menggunakan konsol AWS Marketplace atau alat untuk memungkinkan integrasi dengan Organizations. Hal ini memungkinkan AWS Marketplace melakukan konfigurasi yang diperlukan, seperti membuat sumber daya yang dibutuhkan oleh layanan. Lanjutkan dengan langkah-langkah ini hanya jika Anda tidak dapat mengaktifkan integrasi menggunakan alat yang disediakan olehAWS Marketplace. Untuk informasi selengkapnya, lihat catatan ini.
> Jika Anda mengaktifkan akses terpercaya dengan menggunakan konsol AWS Marketplace atau alat, Anda tidak perlu menyelesaikan langkah-langkah ini.

Untuk mengaktifkan akses menggunakan konsol AWS Marketplace

Lihat Membuat peran terkait layanan untukAWS Marketplace di PanduanAWS Marketplace Pembeli.

Anda dapat mengaktifkan akses terpercaya dengan menggunakan konsol AWS Organizations, dengan menjalankan perintah AWS CLI, atau dengan memanggil operasi API di salah satu SDK AWS.

AWS Management Console

Untuk mengaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk AWS Marketplace, pilih nama layanan, dan kemudian Mengaktifkan akses terpercaya.
3. Di kotak dialog konfirmasi, aktifkan Menampilkan opsi untuk mengaktifkan akses terpercaya, masukkan **`enable`** dalam kotak, dan kemudian pilih Mengaktifkan akses terpercaya.
4. Jika Anda adalah administrator hanya AWS Organizations, beritahu administrator AWS Marketplace bahwa mereka sekarang dapat mengaktifkan layanan tersebut menggunakan konsolnya untuk bekerja dengan AWS Organizations.

AWS CLI, AWS API

Untuk mengaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk mengaktifkan atau mengaktifkan akses layanan terpercaya:

- AWS CLI: enable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk mengaktifkan AWS Marketplace sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal license-management.marketplace.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.

- AWSAPI: AktifkanAWSServiceAccess

Menonaktifkan akses terpercaya dengan AWS Marketplace

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Anda dapat mengaktifkan akses terpercaya hanya menggunakan alat Organizations.

Anda dapat menonaktifkan akses terpercaya dengan menjalankan perintah AWS CLI Organizations, atau dengan memanggil operasi API Organizations di salah satu SDK AWS.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk menonaktifkan akses layanan terpercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan AWS Marketplace sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal license-management.marketplace.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWSAPI: NonaktifkanAWSServiceAccess

AWS Marketplace Marketplace Pribadi dan AWS Organizations

AWS Marketplace adalah katalog digital yang dikuratori yang dapat Anda gunakan untuk menemukan, membeli, menyebarkan, dan mengelola perangkat lunak, data, dan layanan pihak ketiga yang Anda butuhkan untuk membangun solusi dan menjalankan bisnis Anda. Pasar pribadi memberi Anda katalog luas produk yang tersedia di AWS Marketplace, bersama dengan kontrol penuh atas produk tersebut.

AWS Marketplace Private Marketplace memungkinkan Anda untuk membuat beberapa pengalaman pasar pribadi yang terkait dengan seluruh organisasi Anda, satu atau lebih OU, atau satu atau

beberapa akun di organisasi Anda, masing-masing dengan serangkaian produk yang disetujui sendiri. AWS Administrator Anda juga dapat menerapkan branding perusahaan ke setiap pengalaman pasar pribadi dengan logo, pesan, dan skema warna perusahaan atau tim Anda.

Untuk informasi selengkapnya, lihat Menggunakan peran untuk mengonfigurasi Marketplace Pribadi AWS Marketplacedi PanduanAWS Marketplace Pembeli.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan AWS Marketplace Private Marketplace dengan AWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran terkait layanan berikut dibuat secara otomatis di akun manajemen organisasi Anda saat Anda mengaktifkan akses tepercaya menggunakan konsol AWS Marketplace Marketplace Pribadi. Peran ini memungkinkan Private Marketplace untuk melakukan operasi yang didukung dalam akun organisasi Anda di organisasi Anda. Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses tepercaya antara AWS Marketplace Private Marketplace dan Organizations dan memisahkan semua pengalaman pasar pribadi di organisasi Anda.

Jika Anda mengaktifkan akses tepercaya langsung dari konsol Organizations, CLI, atau SDK, peran terkait layanan tidak dibuat secara otomatis.

- `AWSServiceRoleForPrivateMarketplaceAdmin`

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran terkait layanan yang digunakan oleh Private Marketplace memberikan akses ke prinsip layanan berikut:

- `private-marketplace.marketplace.amazonaws.com`

Mengaktifkan akses tepercaya dengan Private Marketplace

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Anda dapat mengaktifkan akses tepercaya menggunakan konsol AWS Marketplace Private Marketplace atau AWS Organizations konsol.

> **Important**
>
> Kami sangat menyarankan agar jika memungkinkan, Anda menggunakan konsol atau alat AWS Marketplace Private Marketplace untuk mengaktifkan integrasi dengan Organizations. Ini memungkinkan AWS Marketplace Private Marketplace melakukan konfigurasi apa pun yang diperlukan, seperti membuat sumber daya yang dibutuhkan oleh layanan. Lanjutkan dengan langkah-langkah ini hanya jika Anda tidak dapat mengaktifkan integrasi menggunakan alat yang disediakan oleh AWS Marketplace Private Marketplace. Untuk informasi lebih lanjut, lihat catatan ini.
> Jika Anda mengaktifkan akses tepercaya dengan menggunakan konsol atau alat AWS Marketplace Private Marketplace maka Anda tidak perlu menyelesaikan langkah-langkah ini.

Untuk mengaktifkan akses tepercaya menggunakan konsol Private Marketplace

Lihat Memulai Marketplace Pribadi di PanduanAWS Marketplace Pembeli.

Anda dapat mengaktifkan akses tepercaya dengan menggunakan AWS Organizations konsol, dengan menjalankan AWS CLI perintah, atau dengan memanggil operasi API di salah satu AWS SDK.

AWS Management Console

Untuk mengaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsolAWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, cari baris untuk MarketplaceAWS Marketplace Pribadi, pilih nama layanan, lalu pilih Aktifkan akses tepercaya.
3. Di kotak dialog konfirmasi, aktifkan Menampilkan opsi untuk mengaktifkan akses terpercaya, masukkan **`enable`** dalam kotak, dan kemudian pilih Mengaktifkan akses terpercaya.
4. Jika Anda hanya administrator AWS Organizations, beri tahu administrator AWS Marketplace Private Marketplace bahwa mereka sekarang dapat mengaktifkan layanan tersebut menggunakan konsolnya untuk bekerja dengannya AWS Organizations.

AWS CLI, AWS API

Untuk mengaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan AWS CLI perintah atau operasi API berikut untuk mengaktifkan akses layanan tepercaya:

- AWS CLI: enable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk mengaktifkan AWS Marketplace Private Marketplace sebagai layanan tepercaya dengan Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal private-marketplace.marketplace.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWS API: Aktifkan AWSServiceAccess

Menonaktifkan akses tepercaya dengan Private Marketplace

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Anda dapat menonaktifkan akses terpercaya hanya menggunakan alat Organizations.

Anda dapat menonaktifkan akses tepercaya dengan menjalankan AWS CLI perintah Organizations, atau dengan memanggil operasi Organizations API di salah satu AWS SDK.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan AWS CLI perintah atau operasi API berikut untuk menonaktifkan akses layanan tepercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan AWS Marketplace Private Marketplace sebagai layanan tepercaya dengan Organizations.

  ```
  $ aws organizations disable-aws-service-access \
  ```

```
    --service-principal private-marketplace.marketplace.amazonaws.com
```

Perintah ini tidak menghasilkan output saat berhasil.

- AWS API: Nonaktifkan AWSServiceAccess

Mengaktifkan akun administrator yang didelegasikan untuk Private Marketplace

Administrator akun manajemen dapat mendelegasikan izin administratif Marketplace Private ke akun anggota yang ditunjuk yang dikenal sebagai administrator yang didelegasikan. Untuk mendaftarkan akun sebagai administrator yang didelegasikan untuk pasar pribadi, administrator akun manajemen harus memastikan bahwa akses tepercaya dan peran terkait layanan diaktifkan, pilih Daftarkan administrator baru, berikan nomor AWS akun 12 digit, dan pilih Kirim.

Akun manajemen dan akun administrator yang didelegasikan dapat melakukan tugas administratif Marketplace Pribadi, seperti membuat pengalaman, memperbarui pengaturan merek, mengaitkan atau memisahkan audiens, menambah atau menghapus produk, dan menyetujui atau menolak permintaan yang tertunda.

Untuk mengonfigurasi administrator yang didelegasikan menggunakan konsol Marketplace Pribadi, lihat Membuat dan mengelola pasar pribadi di PanduanAWS Marketplace Pembeli.

Anda juga dapat mengonfigurasi administrator yang didelegasikan menggunakan Organizations `RegisterDelegatedAdministrator` API. Untuk informasi selengkapnya, lihat RegisterDelegatedAdministratordi Referensi Perintah Organizations.

Menonaktifkan administrator yang didelegasikan untuk Private Marketplace

Hanya administrator di akun manajemen organisasi yang dapat mengonfigurasi administrator yang didelegasikan untuk Private Marketplace.

Anda dapat menghapus administrator yang didelegasikan menggunakan konsol Marketplace Pribadi atau API, atau dengan menggunakan operasi Organizations `DeregisterDelegatedAdministrator` CLI atau SDK.

Untuk menonaktifkan akun Private Marketplace admin yang didelegasikan menggunakan konsol Marketplace Pribadi, lihat Membuat dan mengelola marketplace pribadi di Panduan AWS Marketplace Pembeli

AWS Manajer Jaringan dan AWS Organizations

Network Manager memungkinkan Anda mengelola jaringan inti AWS Cloud WAN dan jaringan AWS Transit Gateway secara terpusat di seluruh AWS akun, Wilayah, dan lokasi lokal. Dengan dukungan multi-akun, Anda dapat membuat satu jaringan global untuk AWS akun Anda, dan mendaftarkan gateway transit dari beberapa akun ke jaringan global menggunakan konsol Network Manager.

Dengan akses tepercaya antara Network Manager dan Organizations diaktifkan, administrator yang didelegasikan terdaftar dan akun manajemen dapat memanfaatkan peran terkait layanan yang digunakan di akun anggota untuk menjelaskan sumber daya yang dilampirkan ke jaringan global Anda. Dari konsol Network Manager, administrator yang didelegasikan terdaftar dan akun manajemen dapat mengasumsikan peran IAM kustom yang diterapkan di akun anggota: `CloudWatch-CrossAccountSharingRole` untuk pemantauan dan eventing multi-akun, dan untuk akses peran peralihan konsol `IAMRoleForAWSNetworkManagerCrossAccountResourceAccess` untuk melihat dan mengelola sumber daya multi-akun)

> **Important**
>
> - Kami sangat menyarankan menggunakan konsol Network Manager untuk mengelola pengaturan multi-akun (mengaktifkan/menonaktifkan akses tepercaya dan mendaftarkan/membatalkan pendaftaran administrator yang didelegasikan). Mengelola pengaturan ini dari konsol secara otomatis menyebarkan dan mengelola semua peran terkait layanan yang diperlukan dan peran IAM khusus ke akun anggota yang diperlukan untuk akses multi-akun.
> - Saat Anda mengaktifkan akses tepercaya untuk Network Manager di konsol Network Manager, konsol juga mengaktifkan AWS CloudFormation StackSets layanan. Network Manager menggunakan StackSets untuk menerapkan peran IAM kustom yang diperlukan untuk manajemen multi-akun.

Untuk informasi selengkapnya tentang mengintegrasikan Network Manager dengan Organizations, lihat Mengelola beberapa akun di Network Manager dengan AWS Organizations di Panduan Pengguna Amazon VPC.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan AWS Network Manager dengan AWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Saat Anda mengaktifkan akses tepercaya, peran terkait layanan berikut akan dibuat secara otomatis di akun organisasi yang terdaftar. Peran ini memungkinkan Manajer Jaringan untuk melakukan operasi yang didukung dalam akun di organisasi Anda. Jika Anda menonaktifkan akses tepercaya, Manajer Jaringan tidak akan menghapus peran ini dari akun di organisasi Anda. Anda dapat menghapusnya secara manual menggunakan konsol IAM.

Akun manajemen

- `AWSServiceRoleForNetworkManager`
- `AWSServiceRoleForCloudFormationStackSetsOrgAdmin`
- `AWSServiceRoleForCloudWatchCrossAccount`

Akun anggota

- `AWSServiceRoleForNetworkManager`
- `AWSServiceRoleForCloudFormationStackSetsOrgMember`

Saat Anda mendaftarkan akun anggota sebagai administrator yang didelegasikan, peran tambahan berikut secara otomatis dibuat di akun administrator yang didelegasikan:

- `AWSServiceRoleForCloudWatchCrossAccount`

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran terkait layanan hanya dapat diasumsikan oleh prinsip layanan yang disahkan oleh hubungan kepercayaan yang ditentukan untuk peran tersebut.

- Untuk `AWSServiceRoleForNetworkManager service-linked` peran, `networkmanager.amazonaws.com` adalah satu-satunya prinsip layanan yang memiliki akses.
- Untuk peran `AWSServiceRoleForCloudFormationStackSetsOrgMember` terkait layanan, `member.org.stacksets.cloudformation.amazonaws.com` adalah satu-satunya prinsip layanan yang memiliki akses.
- Untuk peran `AWSServiceRoleForCloudFormationStackSetsOrgAdmin` terkait layanan, `stacksets.cloudformation.amazonaws.com` adalah satu-satunya prinsip layanan yang memiliki akses.

- Untuk peran `AWSServiceRoleForCloudWatchCrossAccount` terkait layanan, `cloudwatch-crossaccount.amazonaws.com` adalah satu-satunya prinsip layanan yang memiliki akses.

Menghapus peran ini akan mengganggu fungsionalitas multi-akun untuk Manajer Jaringan.

Mengaktifkan akses tepercaya dengan Network Manager

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Hanya administrator di akun manajemen Organizations yang memiliki izin untuk mengaktifkan akses tepercaya dengan AWS layanan lain. Pastikan untuk menggunakan konsol Network Manager untuk mengaktifkan akses tepercaya, untuk menghindari masalah izin. Untuk informasi selengkapnya, lihat Mengelola beberapa akun di Manajer Jaringan dengan AWS Organizations di Panduan Pengguna Amazon VPC.

Menonaktifkan akses tepercaya dengan Network Manager

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Hanya administrator di akun manajemen Organizations yang memiliki izin untuk menonaktifkan akses tepercaya dengan AWS layanan lain.

> **Important**
>
> Kami sangat menyarankan menggunakan konsol Network Manager untuk menonaktifkan akses tepercaya. Jika Anda menonaktifkan akses tepercaya dengan cara lain, seperti menggunakan AWS CLI, dengan API, atau dengan AWS CloudFormation konsol, peran IAM yang digunakan AWS CloudFormation StackSets dan kustom mungkin tidak dibersihkan dengan benar. Untuk menonaktifkan akses layanan tepercaya, masuk ke konsol Network Manager.

Mengaktifkan akun administrator yang didelegasikan untuk Network Manager

Saat Anda menetapkan akun anggota sebagai administrator yang didelegasikan untuk organisasi, pengguna dan peran dari akun tersebut dapat melakukan tindakan administratif untuk Manajer

Jaringan yang hanya dapat dilakukan oleh pengguna atau peran dalam akun manajemen organisasi. Ini membantu Anda memisahkan manajemen organisasi dari manajemen Manajer Jaringan.

Untuk petunjuk tentang cara menunjuk akun anggota sebagai administrator Manajer Jaringan yang didelegasikan di organisasi, lihat Mendaftarkan administrator yang didelegasikan di Panduan Pengguna Amazon VPC.

Pengembang Amazon Q (Amazon Q) dan AWS Organizations

Amazon Q Developer adalah asisten percakapan yang didukung kecerdasan buatan (AI) generatif yang dapat membantu Anda memahami, membangun, memperluas, dan mengoperasikan AWS aplikasi. Versi langganan berbayar Amazon Q memerlukan integrasi Organizations. Untuk informasi selengkapnya, lihat Pengaturan Akun, Pusat Identitas IAM, dan Organizations di panduan pengguna Amazon Q.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan Amazon Q Developer AWS Organizations.

Peran terkait layanan

Peran `AWSServiceRoleForAmazonQDeveloper` terkait layanan memungkinkan Amazon Q untuk melakukan operasi yang didukung dalam akun organisasi Anda di organisasi Anda. Buat peran menggunakan konsol Amazon Q, API, atau CLI, seperti yang dijelaskan dalam Membuat peran terkait layanan di Panduan Pengguna IAM.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses tepercaya antara Amazon Q dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

Prinsipal layanan yang digunakan oleh Amazon Q

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran terkait layanan yang digunakan oleh Amazon Q memberikan akses ke prinsip layanan berikut:

- `q.amazonaws.com`

Mengaktifkan akses tepercaya dengan Amazon Q

Amazon Q menggunakan akses tepercaya untuk membagikan pengaturan yang dibuat di tingkat Orgs dengan akun anggota. Misalnya, administrator di tingkat Organizations dapat mengaktifkan

Fitur X, dan Fitur X kemudian tersedia untuk semua akun anggota dari organisasi yang sama. Untuk informasi selengkapnya, lihat Menyiapkan Organizations di panduan pengguna Amazon Q Developer.

Anda dapat mengaktifkan akses tepercaya hanya menggunakan Pengembang Amazon Q.

Untuk mengaktifkan akses tepercaya untuk Amazon Q, di konsol Amazon Q, ikuti petunjuk di Langganan di panduan pengguna Pengembang Amazon Q. Pada Langkah 6, pilih Bagikan profil pengaturan dengan akun anggota.

Menonaktifkan akses tepercaya dengan Amazon Q

Anda dapat menonaktifkan akses tepercaya hanya menggunakan alat Pengembang Amazon Q.

Untuk menonaktifkan akses tepercaya untuk Amazon Q, di konsol Amazon Q, ikuti petunjuk di Langganan di panduan pengguna Pengembang Amazon Q. Pada Langkah 6, batalkan pilihan Bagikan profil pengaturan dengan akun anggota.

AWS Resource Access Manager dan AWS Organizations

AWS Resource Access Manager (AWS RAM) memungkinkan Anda untuk berbagi sumber daya AWS yang ditentukan yang Anda miliki dengan lainnya Akun AWS. Ini adalah layanan terpusat yang memberikan pengalaman konsisten untuk berbagi berbagai jenis AWS sumber daya di beberapa akun.

Untuk informasi selengkapnya tentang AWS RAM, lihat Panduan Pengguna AWS RAM.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan AWS Resource Access Manager dengan AWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat di akun pengelolaan organisasi Anda bila Anda mengaktifkan akses terpercaya. Peran ini memungkinkan AWS RAM untuk menjalankan operasi yang didukung di akun organisasi Anda di organisasi Anda.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses terpercaya antara AWS RAM dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

- `AWSServiceRoleForResourceAccessManager`

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran tertaut layanan yang digunakan oleh AWS RAM memberikan akses ke prinsipal layanan berikut:

- `ram.amazonaws.com`

Mengaktifkan akses terpercaya dengan AWS RAM

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Anda dapat mengaktifkan akses terpercaya menggunakan konsol AWS Resource Access Manager atau konsol AWS Organizations.

> **Important**
>
> Kami sangat merekomendasikan bahwa bila memungkinkan, Anda menggunakan konsol AWS Resource Access Manager atau alat untuk memungkinkan integrasi dengan Organizations. Hal ini memungkinkan AWS Resource Access Manager melakukan konfigurasi yang diperlukan, seperti membuat sumber daya yang dibutuhkan oleh layanan. Lanjutkan dengan langkah-langkah ini hanya jika Anda tidak dapat mengaktifkan integrasi menggunakan alat yang disediakan olehAWS Resource Access Manager. Untuk informasi selengkapnya lihat lihat lihat lihat lihat.
> Jika Anda mengaktifkan akses terpercaya dengan menggunakan konsol AWS Resource Access Manager atau alat, Anda tidak perlu menyelesaikan langkah-langkah ini.

Untuk mengaktifkan akses terpercaya menggunakan konsol AWS RAM atau CLI

Lihat Mengaktifkan Berbagi dengan AWS Organizations di Panduan Pengguna AWS RAM.

Anda dapat mengaktifkan akses terpercaya dengan menggunakan konsol AWS Organizations, dengan menjalankan perintah AWS CLI, atau dengan memanggil operasi API di salah satu SDK AWS.

AWS Management Console

Untuk mengaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk AWS Resource Access Manager, pilih nama layanan, dan kemudian Mengaktifkan akses terpercaya.
3. Di kotak dialog konfirmasi, aktifkan Menampilkan opsi untuk mengaktifkan akses terpercaya, masukkan **`enable`** dalam kotak, dan kemudian pilih Mengaktifkan akses terpercaya.
4. Jika Anda adalah administrator hanya AWS Organizations, beritahu administrator AWS Resource Access Manager bahwa mereka sekarang dapat mengaktifkan layanan tersebut menggunakan konsolnya untuk bekerja dengan AWS Organizations.

AWS CLI, AWS API

Untuk mengaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk mengaktifkan atau mengaktifkan akses layanan terpercaya:

- AWS CLI: enable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk mengaktifkan AWS Resource Access Manager sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal ram.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWSAPI: AktifkanAWSServiceAccess

Menonaktifkan akses terpercaya dengan AWS RAM

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Anda dapat menonaktifkan akses terpercaya menggunakan AWS Resource Access Manager atau alat AWS Organizations.

> **Important**
>
> Kami sangat merekomendasikan bahwa bila memungkinkan, Anda menggunakan konsol AWS Resource Access Manager atau alat untuk menonaktifkan integrasi dengan Organizations. Hal ini memungkinkan AWS Resource Access Manager melakukan pembersihan apa pun yang diperlukan, seperti menghapus sumber daya atau peran akses yang tidak lagi diperlukan oleh layanan. Lanjutkan dengan langkah-langkah ini hanya jika Anda tidak dapat menonaktifkan integrasi menggunakan alat yang disediakan oleh AWS Resource Access Manager.
> Jika Anda menonaktifkan akses tepercaya dengan menggunakan konsol AWS Resource Access Manager atau alat, Anda tidak perlu menyelesaikan langkah-langkah ini.

Untuk menonaktifkan akses terpercaya menggunakanAWS Resource Access Manager konsol

Lihat Mengaktifkan Berbagi dengan AWS Organizations di Panduan Pengguna AWS RAM.

Anda dapat menonaktifkan akses terpercaya dengan menggunakan konsol AWS Organizations, dengan menjalankan perintah AWS CLI, atau dengan memanggil operasi API Organizations di salah satu SDK AWS.

AWS Management Console

Untuk menonaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk AWS Resource Access Manager dan kemudian pilih nama layanan.
3. Pilih Menonaktifkan akses terpercaya.
4. Di kotak dialog konfirmasi, masukkan **`disable`** dalam kotak, dan kemudian pilih Menonaktifkan akses terpercaya.

5. Jika Anda adalah administrator hanya AWS Organizations, beritahu administrator AWS Resource Access Manager bahwa mereka sekarang dapat menonaktifkan layanan tersebut menggunakan konsolnya untuk bekerja dengan AWS Organizations.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk menonaktifkan akses layanan terpercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan AWS Resource Access Manager sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ram.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWSAPI: NonaktifkanAWSServiceAccess

Penjelajah Sumber Daya AWS dan AWS Organizations

Penjelajah Sumber Daya AWSadalah layanan pencarian dan penemuan sumber daya. Dengan Resource Explorer, Anda dapat menjelajahi sumber daya Anda, seperti instans Amazon Elastic Compute Cloud, Amazon Kinesis Data Streams, atau tabel Amazon DynamoDB, menggunakan pengalaman seperti mesin pencari internet. Anda dapat mencari sumber daya menggunakan metadata sumber daya seperti nama, tag, dan ID. Resource Explorer bekerja di seluruh AWS Wilayah di akun Anda untuk menyederhanakan beban kerja Lintas wilayah Anda.

Saat mengintegrasikan Resource ExplorerAWS Organizations, Anda dapat mengumpulkan bukti dari sumber yang lebih luas dengan menyertakan beberapa Akun AWS dari organisasi Anda dalam lingkup penilaian Anda.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan Penjelajah Sumber Daya AWS dengan AWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat di akun pengelolaan organisasi Anda bila Anda mengaktifkan akses terpercaya. Peran ini memungkinkan Resource Explorer untuk melakukan operasi yang didukung dalam akun organisasi Anda di organisasi Anda.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses tepercaya antara Resource Explorer dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

Untuk informasi selengkapnya tentang cara Resource Explorer menggunakan peran ini, lihat Menggunakan peran terkait layanan di Panduan Penjelajah Sumber Daya AWSPengguna.

- `AWSServiceRoleForResourceExplorer`

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran terkait layanan yang digunakan oleh Resource Explorer memberikan akses ke prinsip layanan berikut:

- `resource-explorer-2.amazonaws.com`

Untuk mengaktifkan akses tepercaya dengan Penjelajah Sumber Daya AWS

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Resource Explorer memerlukan akses tepercaya AWS Organizations sebelum Anda dapat menetapkan akun anggota untuk menjadi administrator yang didelegasikan untuk organisasi Anda.

Anda dapat mengaktifkan akses tepercaya menggunakan konsol Resource Explorer atau konsol Organizations. Kami sangat menyarankan bahwa bila memungkinkan, Anda menggunakan konsol atau alat Resource Explorer untuk mengaktifkan integrasi dengan Organizations. Hal ini memungkinkan Penjelajah Sumber Daya AWS melakukan konfigurasi yang diperlukan, seperti membuat sumber daya yang dibutuhkan oleh layanan.

Untuk mengaktifkan akses tepercaya menggunakan konsol Resource Explorer

Untuk petunjuk tentang mengaktifkan akses tepercaya, lihat Prasyarat untuk menggunakan Resource Explorer di Panduan Pengguna. Penjelajah Sumber Daya AWS

> **Note**
>
> Jika Anda mengonfigurasi administrator yang didelegasikan dengan menggunakan konsol Penjelajah Sumber Daya AWS, kemudian Penjelajah Sumber Daya AWS secara otomatis memungkinkan akses terpercaya untuk Anda.

Anda dapat mengaktifkan akses terpercaya dengan menjalankan perintah AWS CLI Organizations, atau dengan memanggil operasi API Organizations di salah satu SDK AWS.

AWS CLI, AWS API

Untuk mengaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk mengaktifkan atau mengaktifkan akses layanan terpercaya:

- AWS CLI: enable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk mengaktifkan Penjelajah Sumber Daya AWS sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal resource-explorer-2.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.

- AWSAPI: Aktifkan AWSServiceAccess

Untuk menonaktifkan akses tepercaya dengan Resource Explorer

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Hanya administrator di akun pengelolaan AWS Organizations yang dapat menonaktifkan akses terpercaya dengan Penjelajah Sumber Daya AWS.

Anda dapat menonaktifkan akses terpercaya menggunakan Penjelajah Sumber Daya AWS atau alat AWS Organizations.

> **Important**
>
> Kami sangat merekomendasikan bahwa bila memungkinkan, Anda menggunakan konsol Penjelajah Sumber Daya AWS atau alat untuk menonaktifkan integrasi dengan Organizations. Hal ini memungkinkan Penjelajah Sumber Daya AWS melakukan pembersihan apa pun yang diperlukan, seperti menghapus sumber daya atau peran akses yang tidak lagi diperlukan oleh layanan. Lanjutkan dengan langkah-langkah ini hanya jika Anda tidak dapat menonaktifkan integrasi menggunakan alat yang disediakan oleh Penjelajah Sumber Daya AWS.
> Jika Anda menonaktifkan akses tepercaya dengan menggunakan konsol Penjelajah Sumber Daya AWS atau alat, Anda tidak perlu menyelesaikan langkah-langkah ini.

Anda dapat menonaktifkan akses terpercaya dengan menjalankan perintah AWS CLI Organizations, atau dengan memanggil operasi API Organizations di salah satu SDK AWS.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk menonaktifkan akses layanan terpercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan Penjelajah Sumber Daya AWS sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal resource-explorer-2.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.

- AWSAPI: Nonaktifkan AWSServiceAccess

Mengaktifkan akun administrator yang didelegasikan untuk Resource Explorer

Gunakan akun administrator yang didelegasikan untuk membuat tampilan sumber daya multi-akun dan cakupannya ke unit organisasi atau seluruh organisasi Anda. Anda dapat berbagi tampilan multi-akun dengan akun apa pun di organisasi Anda melalui AWS Resource Access Manager dengan membuat pembagian sumber daya.

> **Izin minimum**
>
> Hanya pengguna atau peran dalam akun manajemen Organizations dengan izin berikut yang dapat mengonfigurasi akun anggota sebagai administrator yang didelegasikan untuk Resource Explorer di organisasi:
> `resource-explorer:RegisterAccount`

Untuk instruksi tentang mengaktifkan akun administrator yang didelegasikan untuk Resource Explorer, lihat Menyiapkan di Penjelajah Sumber Daya AWSPanduan Pengguna.

Jika Anda mengonfigurasi administrator yang didelegasikan menggunakan Penjelajah Sumber Daya AWS konsol, maka Resource Explorer secara otomatis mengaktifkan akses tepercaya untuk Anda.

AWS CLI, AWS API

Jika Anda ingin mengonfigurasi akun administrator yang didelegasikan menggunakan CLI AWS atau salah satu dari SDK AWS, Anda dapat menggunakan perintah berikut:

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal resource-explorer-2.amazonaws.com
```

- AWSSDK: Panggil `RegisterDelegatedAdministrator` operasi Organizations dan nomor ID akun anggota dan identifikasi layanan akun `resource-explorer-2.amazonaws.com` sebagai parameter.

Menonaktifkan administrator yang didelegasikan untuk Resource Explorer

Hanya administrator di akun manajemen Organizations atau di akun administrator yang didelegasikan Resource Explorer yang dapat menghapus administrator yang didelegasikan untuk

Resource Explorer. Anda dapat menonaktifkan akses tepercaya menggunakan operasi Organizations `DeregisterDelegatedAdministrator` CLI atau SDK.

AWS Security Hub dan AWS Organizations

AWS Security Hub memberi Anda pandangan komprehensif tentang keadaan keamanan Anda AWS dan membantu Anda memeriksa lingkungan Anda terhadap standar industri keamanan dan praktik terbaik.

Security Hub mengumpulkan data keamanan dari seluruh Anda Akun AWS, AWS layanan yang Anda gunakan, dan produk mitra pihak ketiga yang didukung. Ini membantu Anda untuk menganalisis tren keamanan Anda dan mengidentifikasi masalah keamanan prioritas tertinggi.

Saat Anda menggunakan Security Hub dan AWS Organizations bersama-sama, Anda dapat secara otomatis mengaktifkan Security Hub untuk semua akun Anda, termasuk akun baru saat ditambahkan. Ini meningkatkan cakupan pemeriksaan dan temuan Security Hub, yang memberikan gambaran yang lebih komprehensif dan akurat tentang keseluruhan postur keamanan Anda.

Untuk informasi selengkapnya tentang Security Hub, lihat Panduan PenggunaAWS Security Hub.

Gunakan informasi berikut untuk membantu Anda AWS Security Hub berintegrasi AWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat di akun pengelolaan organisasi Anda bila Anda mengaktifkan akses terpercaya. Peran ini memungkinkan Security Hub untuk melakukan operasi yang didukung dalam akun organisasi Anda di organisasi Anda.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses terpercaya antara Security Hub dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

- `AWSServiceRoleForSecurityHub`

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran tertaut layanan yang digunakan oleh Security Hub memberikan akses ke prinsipal layanan berikut:

- `securityhub.amazonaws.com`

Mengaktifkan akses terpercaya dengan Security Hub

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Bila Anda menetapkan administrator yang didelegasikan untuk Security Hub, Security Hub secara otomatis memungkinkan akses terpercaya untuk Security Hub di organisasi Anda.

Mengaktifkan akun administrator yang didelegasikan untuk Security Hub

Bila Anda menetapkan akun anggota sebagai administrator yang didelegasikan untuk organisasi, pengguna dan peran dari akun tersebut dapat melakukan tindakan administratif untuk Security Hub yang jika tidak dapat dilakukan hanya oleh pengguna atau peran dalam akun pengelolaan organisasi. Ini membantu Anda untuk memisahkan manajemen organisasi dari manajemen Security Hub.

Untuk informasi, lihat Menetapkan akun administrator Security Hub di Panduan PenggunaAWS Security Hub .

Untuk menetapkan akun anggota sebagai administrator yang didelegasikan untuk Security Hub

1. Masuk ke akun pengelolaan Organizations Anda.
2. Lakukan salah satu tindakan berikut:
   - Jika akun pengelolaan Anda tidak memiliki Security Hub diaktifkan, maka pada konsol Security Hub, pilih Buka Security Hub.
   - Jika akun manajemen Anda mengaktifkan Security Hub, maka pada konsol Security Hub, di bawah Umum pilih Pengaturan.
3. Di bawah Administrator yang didelegasikan, masukkan ID akun.

Amazon S3 Storage Lens dan AWS Organizations

Dengan memberikan Amazon S3 Storage Lens akses tepercaya ke organisasi Anda, Anda mengizinkannya mengumpulkan dan menggabungkan metrik di semua organisasi Anda. Akun AWS S3 Storage Lens melakukan hal ini dengan mengakses daftar akun milik organisasi Anda dan mengumpulkan serta menganalisis penyimpanan dan penggunaan dan metrik aktivitas untuk semuanya.

Untuk informasi selengkapnya, lihat bagian Menggunakan peran tertaut layanan untuk Amazon S3 Storage Lens di Panduan Pengguna Amazon S3 Storage Lens.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan Lensa Penyimpanan Amazon S3 dengan. AWS Organizations

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran terkait layanan berikut dibuat secara otomatis di akun administrator yang didelegasikan organisasi Anda saat Anda mengaktifkan akses tepercaya dan konfigurasi Lensa Penyimpanan telah diterapkan ke organisasi Anda. Peran ini memungkinkan Amazon S3 Storage Lens untuk melakukan operasi yang didukung dalam akun organisasi Anda di organisasi Anda.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses terpercaya antara Amazon S3 Storage Lensa dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

- `AWSServiceRoleForS3StorageLens`

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran tertaut layanan yang digunakan oleh Amazon S3 Storage Lens memberikan akses ke prinsipal layanan berikut:

- `storage-lens.s3.amazonaws.com`

Mengaktifkan akses terpercaya untuk Amazon S3 Storage Lens

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Anda dapat mengaktifkan akses terpercaya menggunakan konsol Amazon S3 Storage Lens atau konsol AWS Organizations .

> **Important**
>
> Kami sangat merekomendasikan bahwa bila memungkinkan, Anda menggunakan konsol Amazon S3 Storage Lens atau alat untuk mengaktifkan integrasi dengan Organizations. Ini

memungkinkan Amazon S3 Storage Lens melakukan konfigurasi apa pun yang dibutuhkan, seperti menciptakan sumber daya yang dibutuhkan oleh layanan. Lanjutkan dengan langkah-langkah ini hanya jika Anda tidak dapat mengaktifkan integrasi menggunakan alat yang disediakan oleh Amazon S3 Storage Lens. Untuk informasi lebih lanjut, lihat catatan ini.
Jika Anda mengaktifkan akses terpercaya dengan menggunakan konsol Amazon S3 Storage Lens atau alat maka Anda tidak perlu menyelesaikan langkah-langkah ini.

Untuk mengaktifkan akses terpercaya menggunakan konsol Amazon S3

Lihat Mengaktifkan akses tepercaya untuk Lensa Penyimpanan S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Anda dapat mengaktifkan akses tepercaya dengan menggunakan AWS Organizations konsol, dengan menjalankan AWS CLI perintah, atau dengan memanggil operasi API di salah satu AWS SDK.

AWS Management Console

Untuk mengaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk Amazon S3 Storage Lens, pilih nama layanan, dan kemudian Mengaktifkan akses terpercaya.
3. Di kotak dialog konfirmasi, aktifkan Menampilkan opsi untuk mengaktifkan akses terpercaya, masukkan **`enable`** dalam kotak, dan kemudian pilih Mengaktifkan akses terpercaya.
4. Jika Anda hanya administrator AWS Organizations, beri tahu administrator Amazon S3 Storage Lens bahwa mereka sekarang dapat mengaktifkan layanan tersebut menggunakan konsolnya untuk bekerja dengannya. AWS Organizations

AWS CLI, AWS API

Untuk mengaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan AWS CLI perintah atau operasi API berikut untuk mengaktifkan akses layanan tepercaya:

- AWS CLI: enable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk mengaktifkan Amazon S3 Storage Lens sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal storage-lens.s3.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWS API: Aktifkan AWSServiceAccess

Menonaktifkan akses terpercaya untuk Amazon S3 Storage Lens

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Anda dapat menonaktifkan akses terpercaya hanya menggunakan alat Amazon S3 Storage Lens.

Anda dapat menonaktifkan akses tepercaya menggunakan konsol Amazon S3, SDK AWS CLI atau salah satu SDK AWS .

Untuk menonaktifkan akses yang dipercaya menggunakan konsol Amazon S3

Lihat Menonaktifkan akses tepercaya untuk Lensa Penyimpanan S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Aktifkan administrator yang didelegasikan untuk Amazon S3 Storage Lens

Bila Anda menetapkan akun anggota sebagai administrator yang didelegasikan untuk organisasi, pengguna dan peran dari akun tersebut dapat melakukan tindakan administratif untuk Amazon S3 Storage Lens yang jika tidak dapat dilakukan hanya oleh pengguna atau peran dalam akun pengelolaan organisasi. Ini membantu Anda untuk memisahkan manajemen organisasi dari manajemen Amazon S3 Storage Lens.

> **Izin minimum**
>
> Hanya pengguna atau peran di akun manajemen Organizations dengan izin berikut yang dapat mengonfigurasi akun anggota sebagai administrator yang didelegasikan untuk Amazon S3 Storage Lens di organisasi: `organizations:RegisterDelegatedAdministrator`

```
    organizations:DeregisterDelegatedAdministrator
```

Amazon S3 Storage Lens mendukung maksimal 5 akun administrator yang didelegasikan di organisasi Anda.

Untuk menetapkan akun anggota sebagai administrator yang didelegasikan untuk Amazon S3 Storage Lens

Anda dapat mendaftarkan administrator yang didelegasikan menggunakan konsol Amazon S3, AWS CLI SDK atau salah satu AWS SDK. Untuk mendaftarkan akun anggota sebagai akun administrator yang didelegasikan untuk organisasi Anda menggunakan konsol Amazon S3, lihat Mendaftarkan administrator yang didelegasikan untuk Lensa Penyimpanan S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Untuk membatalkan pendaftaran administrator yang didelegasikan untuk Amazon S3 Storage Lens

Anda dapat membatalkan pendaftaran administrator yang didelegasikan menggunakan konsol Amazon S3, atau SDK mana pun. AWS CLI AWS Untuk membatalkan pendaftaran administrator yang didelegasikan menggunakan konsol Amazon S3, lihat Membatalkan pendaftaran administrator yang didelegasikan untuk Lensa Penyimpanan S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Danau Keamanan Amazon dan AWS Organizations

Amazon Security Lake memusatkan data keamanan dari sumber cloud, lokal, dan kustom ke dalam data lake yang disimpan di akun Anda. Dengan mengintegrasikan dengan Organizations, Anda dapat membuat data lake yang mengumpulkan log dan peristiwa di seluruh akun Anda. Untuk informasi selengkapnya, lihat Mengelola beberapa akun dengan AWS Organizations di panduan pengguna Amazon Security Lake.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan Amazon Security Lake dengan AWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat di akun pengelolaan organisasi Anda bila Anda mengaktifkan akses terpercaya. Peran ini memungkinkan Amazon Security Lake untuk melakukan operasi yang didukung dalam akun organisasi Anda di organisasi Anda.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses tepercaya antara Amazon Security Lake dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

- `AWSServiceRoleForSecurityLake`

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran terkait layanan yang digunakan oleh Amazon Security Lake memberikan akses ke prinsip layanan berikut:

- `securitylake.amazonaws.com`

Mengaktifkan akses tepercaya dengan Amazon Security Lake

Saat Anda mengaktifkan akses tepercaya dengan Security Lake, Security Lake dapat bereaksi secara otomatis terhadap perubahan keanggotaan organisasi. Administrator yang didelegasikan dapat mengaktifkan pengumpulan AWS log dari layanan yang didukung di akun organisasi mana pun. Untuk informasi selengkapnya, lihat Peran terkait layanan untuk Amazon Security Lake di panduan pengguna Amazon Security Lake.

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Anda dapat mengaktifkan akses terpercaya hanya menggunakan alat Organizations.

Anda dapat mengaktifkan akses tepercaya dengan menggunakan AWS Organizations konsol, dengan menjalankan AWS CLI perintah, atau dengan memanggil operasi API di salah satu AWS SDK.

AWS Management Console

Untuk mengaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.

2. Pada halaman Layanan, cari baris untuk Amazon Security Lake, pilih nama layanan, lalu pilih Aktifkan akses tepercaya.
3. Di kotak dialog konfirmasi, aktifkan Menampilkan opsi untuk mengaktifkan akses terpercaya, masukkan **`enable`** dalam kotak, dan kemudian pilih Mengaktifkan akses terpercaya.
4. Jika Anda hanya administrator AWS Organizations, beri tahu administrator Amazon Security Lake bahwa mereka sekarang dapat mengaktifkan layanan itu menggunakan konsolnya untuk bekerja dengannya AWS Organizations.

AWS CLI, AWS API

Untuk mengaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan AWS CLI perintah atau operasi API berikut untuk mengaktifkan akses layanan tepercaya:

- AWS CLI: enable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk mengaktifkan Amazon Security Lake sebagai layanan tepercaya dengan Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal securitylake.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWS API: Aktifkan AWSServiceAccess

Menonaktifkan akses tepercaya dengan Amazon Security Lake

Hanya administrator di akun manajemen Organizations yang dapat menonaktifkan akses tepercaya dengan Amazon Security Lake.

Anda dapat menonaktifkan akses terpercaya hanya menggunakan alat Organizations.

Anda dapat menonaktifkan akses tepercaya dengan menggunakan AWS Organizations konsol, dengan menjalankan AWS CLI perintah Organizations, atau dengan memanggil operasi Organizations API di salah satu AWS SDK.

AWS Management Console

Untuk menonaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk Amazon Security Lake dan kemudian pilih nama layanan.
3. Pilih Menonaktifkan akses terpercaya.
4. Di kotak dialog konfirmasi, masukkan **`disable`** dalam kotak, dan kemudian pilih Menonaktifkan akses terpercaya.
5. Jika Anda hanya administrator AWS Organizations, beri tahu administrator Amazon Security Lake bahwa mereka sekarang dapat menonaktifkan layanan itu menggunakan konsol atau alatnya agar tidak berfungsi AWS Organizations.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan AWS CLI perintah atau operasi API berikut untuk menonaktifkan akses layanan tepercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan Amazon Security Lake sebagai layanan tepercaya dengan Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal securitylake.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWS API: Nonaktifkan AWSServiceAccess

Mengaktifkan akun administrator yang didelegasikan untuk Amazon Security Lake

Administrator yang didelegasikan Amazon Security Lake menambahkan akun lain di organisasi sebagai akun anggota. Administrator yang didelegasikan dapat mengaktifkan Amazon Security

Lake dan mengonfigurasi pengaturan Amazon Security Lake untuk akun anggota. Administrator yang didelegasikan dapat mengumpulkan log di seluruh organisasi di semua AWS Wilayah tempat Amazon Security Lake diaktifkan (terlepas dari titik akhir Regional yang saat ini Anda gunakan).

Anda juga dapat mengatur administrator yang didelegasikan untuk secara otomatis menambahkan akun baru di organisasi sebagai anggota. Administrator yang didelegasikan Amazon Security Lake memiliki akses ke log dan peristiwa di akun anggota terkait. Dengan demikian, Anda dapat mengatur Amazon Security Lake untuk mengumpulkan data yang dimiliki oleh akun anggota terkait. Anda juga dapat memberikan izin kepada pelanggan untuk mengkonsumsi data yang dimiliki oleh akun anggota terkait.

Untuk informasi selengkapnya, lihat Mengelola beberapa akun dengan AWS Organizations di panduan pengguna Amazon Security Lake.

> **Izin minimum**
>
> Hanya administrator di akun manajemen Organisasi yang dapat mengonfigurasi akun anggota sebagai administrator yang didelegasikan untuk Amazon Security Lake di organisasi

Anda dapat menentukan akun administrator yang didelegasikan menggunakan konsol Amazon Security Lake, tindakan Amazon Security Lake `CreateDatalakeDelegatedAdmin` API, atau perintah `create-datalake-delegated-admin` CLI. Atau, Anda dapat menggunakan operasi Organizations `RegisterDelegatedAdministrator` CLI atau SDK. Untuk petunjuk tentang mengaktifkan akun administrator yang didelegasikan untuk Amazon Security Lake, lihat Menunjuk administrator Security Lake yang didelegasikan dan menambahkan akun anggota di panduan pengguna Amazon Security Lake.

AWS CLI, AWS API

Jika Anda ingin mengonfigurasi akun administrator yang didelegasikan menggunakan AWS CLI atau salah AWS satu SDK, Anda dapat menggunakan perintah berikut:

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \ --service-principal securitylake.amazonaws.com
```

- AWS SDK: Hubungi `RegisterDelegatedAdministrator` operasi Organizations dan nomor ID akun anggota dan identifikasi prinsipal layanan akun `account.amazonaws.com` sebagai parameter.

Menonaktifkan administrator yang didelegasikan untuk Amazon Security Lake

Hanya administrator di akun manajemen Organizations atau akun administrator yang didelegasikan Amazon Security Lake yang dapat menghapus akun administrator yang didelegasikan dari organisasi.

Anda dapat menghapus akun administrator yang didelegasikan dengan menggunakan tindakan Amazon Security Lake `DeleteDatalakeDelegatedAdmin` API, perintah `delete-datalake-delegated-admin` CLI, atau dengan menggunakan operasi Organizations `DeregisterDelegatedAdministrator` CLI atau SDK. Untuk menghapus administrator yang didelegasikan menggunakan Amazon Security Lake, lihat Menghapus administrator yang didelegasikan Amazon Security Lake di panduan pengguna Amazon Security Lake.

AWS Service Catalog dan AWS Organizations

Katalog Layanan memungkinkan Anda untuk membuat dan mengelola katalog layanan TI yang disetujui untuk digunakan pada. AWS

Integrasi Katalog Layanan dengan AWS Organizations menyederhanakan berbagi portofolio dan penyalinan produk di seluruh organisasi. Administrator Katalog Layanan dapat mereferensikan organisasi yang ada AWS Organizations saat berbagi portofolio, dan mereka dapat berbagi portofolio dengan unit organisasi tepercaya (OU) dalam struktur pohon organisasi. Ini menghilangkan kebutuhan untuk berbagi ID portofolio, dan untuk akun penerima untuk secara manual mereferensikan ID portofolio ketika mengimpor portofolio. Portofolio yang dibagikan melalui mekanisme ini tercantum dalam akun bersama di tampilan Portofolio Impor administrator di Katalog Layanan.

Untuk informasi selengkapnya tentang Katalog Layanan, lihat Panduan Administrator Katalog Layanan.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan AWS Service Catalog dengan AWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

AWS Service Catalog tidak membuat peran tertaut layanan sebagai bagian dari mengaktifkan akses terpercaya.

Prinsipal layanan yang digunakan untuk memberikan izin

Untuk mengaktifkan akses terpercaya, Anda harus menentukan prinsipal layanan berikut:

- `servicecatalog.amazonaws.com`

Mengaktifkan akses tepercaya dengan Katalog Layanan

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Anda dapat mengaktifkan akses terpercaya menggunakan konsol AWS Service Catalog atau konsol AWS Organizations.

> **Important**
>
> Kami sangat merekomendasikan bahwa bila memungkinkan, Anda menggunakan konsol AWS Service Catalog atau alat untuk memungkinkan integrasi dengan Organizations. Hal ini memungkinkan AWS Service Catalog melakukan konfigurasi yang diperlukan, seperti membuat sumber daya yang dibutuhkan oleh layanan. Lanjutkan dengan langkah-langkah ini hanya jika Anda tidak dapat mengaktifkan integrasi menggunakan alat yang disediakan olehAWS Service Catalog. Untuk informasi lebih lanjut, lihat catatan ini.
> Jika Anda mengaktifkan akses terpercaya dengan menggunakan konsol AWS Service Catalog atau alat, Anda tidak perlu menyelesaikan langkah-langkah ini.

Untuk mengaktifkan akses tepercaya menggunakan Service Catalog CLI atau AWS SDK

Panggil salah satu perintah atau operasi berikut ini:

- AWS CLI: aws enable-aws-organizations-access
- AWSSDK: AWSServiceCatalog: :Aktifkan AWSOrganizationsAccess

Anda dapat mengaktifkan akses terpercaya dengan menggunakan konsol AWS Organizations, dengan menjalankan perintah AWS CLI, atau dengan memanggil operasi API di salah satu SDK AWS.

AWS Management Console

Untuk mengaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk AWS Service Catalog, pilih nama layanan, dan kemudian Mengaktifkan akses terpercaya.
3. Di kotak dialog konfirmasi, aktifkan Menampilkan opsi untuk mengaktifkan akses terpercaya, masukkan **`enable`** dalam kotak, dan kemudian pilih Mengaktifkan akses terpercaya.
4. Jika Anda adalah administrator hanya AWS Organizations, beritahu administrator AWS Service Catalog bahwa mereka sekarang dapat mengaktifkan layanan tersebut menggunakan konsolnya untuk bekerja dengan AWS Organizations.

AWS CLI, AWS API

Untuk mengaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk mengaktifkan atau mengaktifkan akses layanan terpercaya:

- AWS CLI: enable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk mengaktifkan AWS Service Catalog sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal servicecatalog.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.

- AWSAPI: Aktifkan AWSServiceAccess

Menonaktifkan akses tepercaya dengan Katalog Layanan

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Jika Anda menonaktifkan akses tepercaya menggunakan AWS Organizations saat Anda menggunakan Katalog Layanan, itu tidak menghapus saham Anda saat ini, tetapi mencegah Anda membuat saham baru di seluruh organisasi Anda. Berbagi saat ini tidak akan sinkron dengan struktur organisasi Anda jika berubah setelah Anda memanggil tindakan ini.

Anda dapat menonaktifkan akses terpercaya menggunakan AWS Service Catalog atau alat AWS Organizations.

> **Important**
>
> Kami sangat merekomendasikan bahwa bila memungkinkan, Anda menggunakan konsol AWS Service Catalog atau alat untuk menonaktifkan integrasi dengan Organizations. Hal ini memungkinkan AWS Service Catalog melakukan pembersihan apa pun yang diperlukan, seperti menghapus sumber daya atau peran akses yang tidak lagi diperlukan oleh layanan. Lanjutkan dengan langkah-langkah ini hanya jika Anda tidak dapat menonaktifkan integrasi menggunakan alat yang disediakan oleh AWS Service Catalog.
> Jika Anda menonaktifkan akses tepercaya dengan menggunakan konsol AWS Service Catalog atau alat, Anda tidak perlu menyelesaikan langkah-langkah ini.

Untuk menonaktifkan akses tepercaya menggunakan Service Catalog CLI atau AWS SDK

Panggil salah satu perintah atau operasi berikut ini:

- AWS CLI: aws disable-aws-organizations-access
- AWSSDK: Nonaktifkan AWSOrganizationsAccess

Anda dapat menonaktifkan akses terpercaya dengan menggunakan konsol AWS Organizations, dengan menjalankan perintah AWS CLI, atau dengan memanggil operasi API Organizations di salah satu SDK AWS.

AWS Management Console

Untuk menonaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk AWS Service Catalog dan kemudian pilih nama layanan.
3. Pilih Menonaktifkan akses terpercaya.
4. Di kotak dialog konfirmasi, masukkan **`disable`** dalam kotak, dan kemudian pilih Menonaktifkan akses terpercaya.
5. Jika Anda adalah administrator hanya AWS Organizations, beritahu administrator AWS Service Catalog bahwa mereka sekarang dapat menonaktifkan layanan tersebut menggunakan konsolnya untuk bekerja dengan AWS Organizations.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk menonaktifkan akses layanan terpercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan AWS Service Catalog sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal servicecatalog.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.

- AWSAPI: Nonaktifkan AWSServiceAccess

Service Quotas dan AWS Organizations

Service Quotas adalah sebuah layanan AWS yang memungkinkan Anda melihat dan mengelola kuota dari lokasi pusat. Kuota, juga disebut sebagai batasan, adalah nilai maksimum untuk sumber daya, tindakan, dan item Anda di Akun AWS.

Ketika Service Quotas dikaitkan dengan AWS Organizations, Anda dapat membuat templat permintaan kuota untuk secara otomatis meminta kenaikan kuota saat akun dibuat.

Untuk informasi selengkapnya tentang Service Quotas, lihat Panduan Pengguna Service Quotas.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan Service Quotas dengan AWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat di akun pengelolaan organisasi Anda bila Anda mengaktifkan akses terpercaya. Peran ini memungkinkan Service Quotas untuk melakukan operasi yang didukung dalam akun organisasi Anda di organisasi Anda.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses terpercaya antara Service Quotas dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

- `AWSServiceRoleForServiceQuotas`

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran tertaut layanan yang digunakan oleh Service Quotas memberikan akses ke prinsipal layanan berikut:

- `servicequotas.amazonaws.com`

Mengaktifkan akses terpercaya dengan Service Quotas

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Anda dapat mengaktifkan akses terpercaya hanya menggunakan Service Quotas.

Anda dapat mengaktifkan akses terpercaya menggunakan konsol Service QuotasAWS CLI atau SDK:

- Untuk mengaktifkan akses terpercaya menggunakan konsol Service Quotas

  Masuk dengan akun pengelolaan AWS Organizations dan kemudian konfigurasi templat pada konsol Service Quotas. Untuk informasi selengkapnya, lihat Menggunakan TemplatService Quotas di Panduan Pengguna Service Quotas.
- Untuk mengaktifkan akses terpercaya menggunakan AWS CLI Service Quotas atau SDK

  Panggil perintah atau operasi berikut ini:
  - AWS CLI: kuota layanan aws associate-service-quota-template
  - AWSSDK: AssociateServiceQuotaTemplate

AWS IAM Identity Center dan AWS Organizations

AWS IAM Identity Centermenyediakan akses masuk tunggal untuk semua aplikasi Anda Akun AWS dan cloud. Ini terhubung dengan Microsoft Active Directory AWS Directory Service untuk memungkinkan pengguna di direktori itu masuk ke portal AWS akses yang dipersonalisasi menggunakan nama pengguna dan kata sandi Active Directory yang ada. Dari portal AWS akses, pengguna memiliki akses ke semua Akun AWS dan aplikasi cloud yang mereka miliki izinnya.

Untuk informasi selengkapnya tentang Pusat Identitas IAM, lihat Panduan AWS IAM Identity Center Pengguna.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan AWS IAM Identity Center dengan AWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat di akun pengelolaan organisasi Anda bila Anda mengaktifkan akses terpercaya. Peran ini memungkinkan Pusat Identitas IAM untuk melakukan operasi yang didukung dalam akun organisasi Anda di organisasi Anda.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses tepercaya antara IAM Identity Center dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

- `AWSServiceRoleForSSO`

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran terkait layanan yang digunakan oleh IAM Identity Center memberikan akses ke prinsip layanan berikut:

- `sso.amazonaws.com`

Mengaktifkan akses tepercaya dengan IAM Identity Center

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Anda dapat mengaktifkan akses terpercaya menggunakan konsol AWS IAM Identity Center atau konsol AWS Organizations.

> **Important**
>
> Kami sangat merekomendasikan bahwa bila memungkinkan, Anda menggunakan konsol AWS IAM Identity Center atau alat untuk memungkinkan integrasi dengan Organizations. Hal ini memungkinkan AWS IAM Identity Center melakukan konfigurasi yang diperlukan, seperti membuat sumber daya yang dibutuhkan oleh layanan. Lanjutkan dengan langkah-langkah ini hanya jika Anda tidak dapat mengaktifkan integrasi menggunakan alat yang disediakan olehAWS IAM Identity Center. Untuk informasi lebih lanjut, lihat catatan ini.
> Jika Anda mengaktifkan akses terpercaya dengan menggunakan konsol AWS IAM Identity Center atau alat, Anda tidak perlu menyelesaikan langkah-langkah ini.

Pusat Identitas IAM membutuhkan akses tepercaya AWS Organizations untuk berfungsi. Akses tepercaya diaktifkan saat Anda menyiapkan Pusat Identitas IAM. Untuk informasi selengkapnya, lihat Memulai - Langkah 1: Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center.

Anda dapat mengaktifkan akses terpercaya dengan menggunakan konsol AWS Organizations, dengan menjalankan perintah AWS CLI, atau dengan memanggil operasi API di salah satu SDK AWS.

AWS Management Console

Untuk mengaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk AWS IAM Identity Center, pilih nama layanan, dan kemudian Mengaktifkan akses terpercaya.
3. Di kotak dialog konfirmasi, aktifkan Menampilkan opsi untuk mengaktifkan akses terpercaya, masukkan **`enable`** dalam kotak, dan kemudian pilih Mengaktifkan akses terpercaya.
4. Jika Anda adalah administrator hanya AWS Organizations, beritahu administrator AWS IAM Identity Center bahwa mereka sekarang dapat mengaktifkan layanan tersebut menggunakan konsolnya untuk bekerja dengan AWS Organizations.

AWS CLI, AWS API

Untuk mengaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk mengaktifkan atau mengaktifkan akses layanan terpercaya:

- AWS CLI: enable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk mengaktifkan AWS IAM Identity Center sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal sso.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWSAPI: Aktifkan AWSServiceAccess

Menonaktifkan akses tepercaya dengan IAM Identity Center

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

IAM Identity Center membutuhkan akses tepercaya AWS Organizations untuk beroperasi. Jika Anda menonaktifkan akses tepercaya menggunakan AWS Organizations saat Anda menggunakan IAM Identity Center, itu berhenti berfungsi karena tidak dapat mengakses organisasi. Pengguna tidak dapat menggunakan Pusat Identitas IAM untuk mengakses akun. Peran apa pun yang dibuat oleh IAM Identity Center tetap ada, tetapi layanan IAM Identity Center tidak dapat mengaksesnya. Peran terkait layanan IAM Identity Center tetap ada. Jika Anda mengaktifkan kembali akses tepercaya, IAM Identity Center terus beroperasi seperti sebelumnya, tanpa perlu Anda mengkonfigurasi ulang layanan.

Jika Anda menghapus akun dari organisasi, Pusat Identitas IAM secara otomatis membersihkan metadata dan sumber daya apa pun, seperti peran terkait layanannya. Akun mandiri yang dihapus dari organisasi tidak lagi berfungsi dengan IAM Identity Center.

Anda dapat menonaktifkan akses terpercaya hanya menggunakan alat Organizations.

Anda dapat menonaktifkan akses terpercaya dengan menggunakan konsol AWS Organizations, dengan menjalankan perintah AWS CLI, atau dengan memanggil operasi API Organizations di salah satu SDK AWS.

AWS Management Console

Untuk menonaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk AWS IAM Identity Center dan kemudian pilih nama layanan.
3. Pilih Menonaktifkan akses terpercaya.
4. Di kotak dialog konfirmasi, masukkan **`disable`** dalam kotak, dan kemudian pilih Menonaktifkan akses terpercaya.
5. Jika Anda adalah administrator hanya AWS Organizations, beritahu administrator AWS IAM Identity Center bahwa mereka sekarang dapat menonaktifkan layanan tersebut menggunakan konsolnya untuk bekerja dengan AWS Organizations.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk menonaktifkan akses layanan terpercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan AWS IAM Identity Center sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal sso.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWSAPI: Nonaktifkan AWSServiceAccess

Mengaktifkan akun administrator yang didelegasikan untuk IAM Identity Center

Saat Anda menetapkan akun anggota sebagai administrator yang didelegasikan untuk organisasi, pengguna dan peran dari akun tersebut dapat melakukan tindakan administratif untuk Pusat Identitas IAM yang hanya dapat dilakukan oleh pengguna atau peran dalam akun manajemen organisasi. Ini membantu Anda memisahkan manajemen organisasi dari manajemen Pusat Identitas IAM.

> **Izin minimum**
>
> Hanya pengguna atau peran dalam akun manajemen Organizations yang dapat mengonfigurasi akun anggota sebagai administrator yang didelegasikan untuk Pusat Identitas IAM di organisasi.

Untuk petunjuk tentang cara mengaktifkan akun administrator yang didelegasikan untuk Pusat Identitas IAM, lihat Administrasi yang didelegasikan di Panduan Pengguna. AWS IAM Identity Center

AWS Systems Manager dan AWS Organizations

AWS Systems Manager adalah kumpulan kemampuan yang memungkinkan visibilitas dan kendali sumber daya AWS. Kemampuan Systems Manager berikut bekerja dengan Organizations Akun AWS di semua organisasi Anda:

- Penjelajah Systems Manager, adalah dasbor operasi yang bisa dikustomisasi yang melaporkan informasi tentang sumber daya AWS. Anda dapat menyinkronkan data operasi di semua Akun

AWS di organisasi Anda dengan menggunakan Organizations dan Penjelajah Systems Manager. Untuk informasi selengkapnya, lihat Penjelajah Systems Manager di Panduan Pengguna AWS Systems Manager.

- Pengelola Perubahan Systems Manager adalah kerangka manajemen perubahan perusahaan untuk meminta, menyetujui, menerapkan, dan melaporkan perubahan operasional untuk konfigurasi aplikasi dan infrastruktur Anda. Untuk informasi selengkapnya, lihat Pengelola Perubahan AWS Systems Manager dalam Panduan Pengguna AWS Systems Manager.
- Systems Manager OpsCenter menyediakan lokasi pusat di mana insinyur operasi dan profesional TI dapat melihat, menyelidiki, dan menyelesaikan item kerja operasional (OpsItems) yang terkait dengan AWS sumber daya. Bila Anda menggunakan OpsCenter dengan Organizations, ini mendukung bekerja dengan OpsItems dari akun manajemen (baik akun manajemen Organizations atau akun administrator yang didelegasikan Systems Manager) dan satu akun lainnya selama satu sesi. Setelah dikonfigurasi, pengguna dapat melakukan jenis tindakan berikut:
  - Buat, lihat, dan perbarui OpsItems di akun lain.
  - Lihat informasi terperinci tentang AWS sumber daya yang ditentukan OpsItems di akun lain.
  - Mulai runbook Systems Manager Automation untuk memulihkan masalah dengan AWS sumber daya di akun lain.

  Untuk informasi lebih lanjut, lihat AWS Systems Manager OpsCenter di Panduan Pengguna AWS Systems Manager.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan AWS Systems Manager dengan AWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat di akun pengelolaan organisasi Anda bila Anda mengaktifkan akses terpercaya. Peran ini memungkinkan Systems Manager untuk melakukan operasi yang didukung dalam akun organisasi Anda di organisasi Anda.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses terpercaya antara Systems Manager dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

- `AWSServiceRoleForAmazonSSM_AccountDiscovery`

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran tertaut layanan yang digunakan oleh Systems Manager memberikan akses ke prinsipal layanan berikut:

- `ssm.amazonaws.com`

Mengaktifkan akses terpercaya dengan Systems Manager

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Anda dapat mengaktifkan akses terpercaya hanya menggunakan alat Organizations.

Anda dapat mengaktifkan akses terpercaya dengan menggunakan konsol AWS Organizations, dengan menjalankan perintah AWS CLI, atau dengan memanggil operasi API di salah satu SDK AWS.

AWS Management Console

Untuk mengaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk AWS Systems Manager, pilih nama layanan, dan kemudian Mengaktifkan akses terpercaya.
3. Di kotak dialog konfirmasi, aktifkan Menampilkan opsi untuk mengaktifkan akses terpercaya, masukkan **`enable`** dalam kotak, dan kemudian pilih Mengaktifkan akses terpercaya.
4. Jika Anda adalah administrator hanya AWS Organizations, beritahu administrator AWS Systems Manager bahwa mereka sekarang dapat mengaktifkan layanan tersebut menggunakan konsolnya untuk bekerja dengan AWS Organizations.

AWS CLI, AWS API

Untuk mengaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk mengaktifkan atau mengaktifkan akses layanan terpercaya:

- AWS CLI: enable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk mengaktifkan AWS Systems Manager sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal ssm.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWSAPI: Aktifkan AWSServiceAccess

Menonaktifkan akses terpercaya dengan Systems Manager

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Systems Manager memerlukan akses terpercaya dengan AWS Organizations untuk menyinkronkan data operasi di seluruh Akun AWS di organisasi Anda. Jika Anda menonaktifkan akses terpercaya, kemudian Systems Manager gagal untuk menyinkronkan operasi data dan laporan kesalahan.

Anda dapat menonaktifkan akses terpercaya hanya menggunakan alat Organizations.

Anda dapat menonaktifkan akses terpercaya dengan menggunakan konsol AWS Organizations, dengan menjalankan perintah AWS CLI, atau dengan memanggil operasi API Organizations di salah satu SDK AWS.

AWS Management Console

Untuk menonaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk AWS Systems Manager dan kemudian pilih nama layanan.
3. Pilih Menonaktifkan akses terpercaya.

4. Di kotak dialog konfirmasi, masukkan **`disable`** dalam kotak, dan kemudian pilih Menonaktifkan akses terpercaya.
5. Jika Anda adalah administrator hanya AWS Organizations, beritahu administrator AWS Systems Manager bahwa mereka sekarang dapat menonaktifkan layanan tersebut menggunakan konsolnya untuk bekerja dengan AWS Organizations.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk menonaktifkan akses layanan terpercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan AWS Systems Manager sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ssm.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWSAPI: Nonaktifkan AWSServiceAccess

Mengaktifkan akun administrator yang didelegasikan untuk Systems Manager

Ketika Anda menetapkan akun anggota sebagai administrator yang didelegasikan untuk organisasi, pengguna dan peran dari akun tersebut dapat melakukan tindakan administratif untuk Systems Manager yang jika tidak dapat dilakukan hanya oleh pengguna atau peran dalam akun pengelolaan organisasi. Ini membantu Anda untuk memisahkan manajemen organisasi dari manajemen Systems Manager.

Jika Anda menggunakan Pengelola Perubahan di seluruh organisasi, Anda menggunakan akun administrator yang didelegasikan. Ini adalah Akun AWS yang telah ditetapkan sebagai akun untuk mengelola perubahan templat, mengubah permintaan, mengubah runbook dan alur kerja persetujuan di Pengelola Perubahan. Akun yang didelegasikan mengelola aktivitas perubahan di seluruh organisasi Anda. Saat menyiapkan organisasi untuk digunakan dengan Pengelola Perubahan, Anda menentukan akun mana yang berfungsi dalam peran ini. Itu tidak harus merupakan akun pengelolaan

organisasi. Akun administrator yang didelegasikan tidak diperlukan jika Anda menggunakan Change Manager hanya dengan satu akun.

Untuk menunjuk akun anggota sebagai administrator yang didelegasikan, lihat topik berikut di AWS Systems ManagerPanduan Pengguna:

- Untuk Explorer dan OpsCenter, lihat Mengkonfigurasi Administrator Delegasi.
- Untuk Mengubah Manajer, lihat Menyiapkan organisasi dan akun yang didelegasikan untuk Change Manager.

Kebijakan tag dan AWS Organizations

Kebijakan tag adalah jenis kebijakan di AWS Organizations yang dapat membantu Anda menstandardisasi tag di seluruh sumber daya di akun organisasi Anda. Untuk informasi lebih lanjut tentang kebijakan tag, lihat Kebijakan tag.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan kebijakan tag dengan AWS Organizations.

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Organizations berinteraksi dengan tag yang dilampirkan pada sumber daya Anda menggunakan prinsipal layanan berikut.

- `tagpolicies.tag.amazonaws.com`

Mengaktifkan akses terpercaya untuk kebijakan tag

Anda dapat mengaktifkan akses terpercaya baik dengan mengaktifkan kebijakan tag dalam organisasi, atau dengan menggunakan konsol AWS Organizations.

> **Important**
>
> Kami sangat merekomendasikan agar Anda mengaktifkan akses terpercaya dengan mengaktifkan kebijakan tag. Ini memungkinkan Organizations untuk melakukan tugas pengaturan yang diperlukan.

Anda dapat mengaktifkan akses terpercaya untuk kebijakan tag dengan mengaktifkan jenis kebijakan tag di konsol AWS Organizations. Untuk informasi lebih lanjut, lihat Mengaktifkan jenis kebijakan.

Anda dapat mengaktifkan akses terpercaya dengan menggunakan konsol AWS Organizations, dengan menjalankan perintah AWS CLI, atau dengan memanggil operasi API di salah satu SDK AWS.

AWS Management Console

Untuk mengaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk kebijakan tag, pilih nama layanan,dan kemudian Mengaktifkan akses terpercaya.
3. Di kotak dialog konfirmasi, aktifkan Menampilkan opsi untuk mengaktifkan akses terpercaya, masukkan **`enable`** dalam kotak, dan kemudian pilih Mengaktifkan akses terpercaya.
4. Jika Anda adalah administrator hanya AWS Organizations, beri tahu administrator kebijakan tag bahwa mereka sekarang dapat mengaktifkan layanan tersebut menggunakan konsolnya untuk bekerja dengan AWS Organizations.

AWS CLI, AWS API

Untuk mengaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk mengaktifkan atau mengaktifkan akses layanan terpercaya:

- AWS CLI: enable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk mengaktifkan kebijakan tag sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal tagpolicies.tag.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- API AWS: AktifkanAWSServiceAccess

Menonaktifkan akses terpercaya dengan kebijakan tag

Anda dapat menonaktifkan akses terpercaya untuk kebijakan tag dengan menonaktifkan jenis kebijakan tag di konsol AWS Organizations. Untuk informasi selengkapnya, lihat Menonaktifkan sebuah jenis kebijakan.

AWS Trusted Advisor dan AWS Organizations

AWS Trusted Advisor memeriksa lingkungan AWS Anda dan membuat rekomendasi ketika ada peluang untuk menghemat uang, meningkatkan ketersediaan dan kinerja sistem, atau membantu menutup kesenjangan keamanan. Saat diintegrasikan dengan Organizations, Anda dapat menerima hasil pemeriksaan Trusted Advisor untuk semua akun di organisasi Anda dan mengunduh laporan untuk melihat ringkasan pemeriksaan Anda dan sumber daya yang terpengaruh.

Untuk informasi selengkapnya, lihat Tampilan organisasi untuk AWS Trusted Advisor di Panduan Pengguna AWS Support.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan AWS Trusted Advisor dengan AWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat di akun pengelolaan organisasi Anda bila Anda mengaktifkan akses terpercaya. Peran ini memungkinkan Trusted Advisor untuk menjalankan operasi yang didukung di akun organisasi Anda di organisasi Anda.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses terpercaya antara Trusted Advisor dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

- `AWSServiceRoleForTrustedAdvisorReporting`

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran tertaut layanan yang digunakan oleh Trusted Advisor memberikan akses ke prinsipal layanan berikut:

- `reporting.trustedadvisor.amazonaws.com`

Mengaktifkan akses terpercaya dengan Trusted Advisor

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Anda dapat mengaktifkan akses terpercaya hanya menggunakan AWS Trusted Advisor.

Untuk mengaktifkan akses menggunakan konsol Trusted Advisor

Lihat Mengaktifkan tampilan organisasi di Panduan Pengguna AWS Support.

Menonaktifkan akses terpercaya dengan Trusted Advisor

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Setelah Anda menonaktifkan fitur ini, Trusted Advisor berhenti merekam informasi pemeriksaan untuk semua akun lain di organisasi Anda. Anda tidak dapat melihat atau mengunduh laporan yang ada atau membuat laporan baru.

Anda dapat menonaktifkan akses terpercaya menggunakan AWS Trusted Advisor atau alat AWS Organizations.

> **Important**
>
> Kami sangat merekomendasikan bahwa bila memungkinkan, Anda menggunakan konsol AWS Trusted Advisor atau alat untuk menonaktifkan integrasi dengan Organizations. Hal ini memungkinkan AWS Trusted Advisor melakukan pembersihan apa pun yang diperlukan, seperti menghapus sumber daya atau peran akses yang tidak lagi diperlukan oleh layanan. Lanjutkan dengan langkah-langkah ini hanya jika Anda tidak dapat menonaktifkan integrasi menggunakan alat yang disediakan oleh AWS Trusted Advisor.
> Jika Anda menonaktifkan akses tepercaya dengan menggunakan konsol AWS Trusted Advisor atau alat, Anda tidak perlu menyelesaikan langkah-langkah ini.

Untuk menonaktifkan akses terpercaya menggunakan konsol Trusted Advisor

Lihat Menonaktifkan tampilan organisasi di Panduan Pengguna AWS Support.

Anda dapat menonaktifkan akses terpercaya dengan menjalankan perintah AWS CLI Organizations, atau dengan memanggil operasi API Organizations di salah satu SDK AWS.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk menonaktifkan akses layanan terpercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan AWS Trusted Advisor sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal reporting.trustedadvisor.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWSAPI:NonaktifkanAWSServiceAccess

Mengaktifkan akun administrator yang didelegasikan untukTrusted Advisor

Ketika Anda menetapkan akun anggota untuk menjadi administrator yang didelegasikan untuk organisasi, pengguna dan peran dari akun yang ditunjuk dapat mengelolaAkun AWSmetadata untuk akun anggota lain di organisasi. Jika Anda tidak mengaktifkan akun admin yang didelegasikan, maka tugas ini hanya dapat dilakukan oleh akun manajemen organisasi. Ini membantu Anda memisahkan manajemen organisasi dari pengelolaan detail akun Anda.

> **Izin minimum**
>
> Hanya pengguna atau peran dalam akun manajemen Organisasi yang dapat mengonfigurasi akun anggota sebagai administrator yang didelegasikanTrusted Advisordalam organisasi

Untuk instruksi tentang mengaktifkan akun administrator yang didelegasikanTrusted Advisor, lihatDaftarkan administrator yang didelegasikandi dalamAWS SupportPanduan Pengguna.

AWS CLI, AWS API

Jika Anda ingin mengonfigurasi akun administrator yang didelegasikan menggunakan CLI AWS atau salah satu dari SDK AWS, Anda dapat menggunakan perintah berikut:

- AWS CLI:

```
$  aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal reporting.trustedadvisor.amazonaws.com
```

- AWSSDK: Hubungi Organisasi`RegisterDelegatedAdministrator`operasi dan nomor ID akun anggota dan mengidentifikasi prinsipal layanan akun`account.amazonaws.com`sebagai parameter.

Menonaktifkan administrator yang didelegasikan untukTrusted Advisor

Anda dapat menghapus administrator yang didelegasikan menggunakanTrusted Advisorkonsol, atau dengan menggunakan Organisasi`DeregisterDelegatedAdministrator`Operasi CLI atau SDK. Untuk informasi tentang cara menonaktifkan admin yang didelegasikanTrusted Advisorakun menggunakanTrusted Advisorkonsol, lihatAdministrator yang didelegasikan Deregisterdi dalamAWS Supportpanduan pengguna.

AWS Well-Architected Tool dan AWS Organizations

AWS Well-Architected ToolIni membantu Anda mendokumentasikan keadaan beban kerja Anda dan membandingkannya dengan praktik terbaikAWS arsitektur terbaru.

MenggunakanAWS Well-Architected Tool dengan Organizations memungkinkan keduaAWS Well-Architected Tool dan Organizations pelanggan untuk menyederhanakan proses berbagiAWS Well-Architected Tool sumber daya dengan anggota lain dari organisasi mereka.

Untuk informasi selengkapnya, lihat MembagikanAWS Well-Architected Tool sumber daya Anda di PanduanAWS Well-Architected Tool Pengguna.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan AWS Well-Architected Tool dengan AWS Organizations.

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat di akun pengelolaan organisasi Anda bila Anda mengaktifkan akses terpercaya. Peran ini memungkinkan AWS WA Tool untuk menjalankan operasi yang didukung di akun organisasi Anda di organisasi Anda.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses terpercaya antara AWS WA Tool dan Organizations, atau jika Anda menghapus akun anggota dari organisasi.

- `AWSServiceRoleForWellArchitected`

Kebijakan peran layanan adalah`AWSWellArchitectedOrganizationsServiceRolePolicy`

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran tertaut layanan yang digunakan oleh AWS WA Tool memberikan akses ke prinsipal layanan berikut:

- `wellarchitected.amazonaws.com`

Mengaktifkan akses terpercaya dengan AWS WA Tool

Memungkinkan pemutakhiranAWS WA Tool untuk mencerminkan perubahan hirarkis dalam suatu organisasi.

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Anda dapat mengaktifkan akses terpercaya menggunakan konsol AWS Well-Architected Tool atau konsol AWS Organizations.

> **Important**
>
> Kami sangat merekomendasikan bahwa bila memungkinkan, Anda menggunakan konsol AWS Well-Architected Tool atau alat untuk memungkinkan integrasi dengan Organizations. Hal ini memungkinkan AWS Well-Architected Tool melakukan konfigurasi yang diperlukan, seperti membuat sumber daya yang dibutuhkan oleh layanan. Lanjutkan dengan langkah-langkah ini hanya jika Anda tidak dapat mengaktifkan integrasi menggunakan alat yang disediakan olehAWS Well-Architected Tool. Untuk informasi selengkapnya, lihat catatan ini. Jika Anda mengaktifkan akses terpercaya dengan menggunakan konsol AWS Well-Architected Tool atau alat, Anda tidak perlu menyelesaikan langkah-langkah ini.

Untuk mengaktifkan akses menggunakan konsol AWS WA Tool

Lihat MembagikanAWS Well-Architected Tool sumber daya Anda di PanduanAWS Well-Architected Tool Pengguna.

Anda dapat mengaktifkan akses terpercaya dengan menggunakan konsol AWS Organizations, dengan menjalankan perintah AWS CLI, atau dengan memanggil operasi API di salah satu SDK AWS.

AWS Management Console

Untuk mengaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk AWS Well-Architected Tool, pilih nama layanan, dan kemudian Mengaktifkan akses terpercaya.
3. Di kotak dialog konfirmasi, aktifkan Menampilkan opsi untuk mengaktifkan akses terpercaya, masukkan **`enable`** dalam kotak, dan kemudian pilih Mengaktifkan akses terpercaya.
4. Jika Anda adalah administrator hanya AWS Organizations, beritahu administrator AWS Well-Architected Tool bahwa mereka sekarang dapat mengaktifkan layanan tersebut menggunakan konsolnya untuk bekerja dengan AWS Organizations.

AWS CLI, AWS API

Untuk mengaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk mengaktifkan atau mengaktifkan akses layanan terpercaya:

- AWS CLI: enable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk mengaktifkan AWS Well-Architected Tool sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal wellarchitected.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- API AWS: AktifkanAWSServiceAccess

Menonaktifkan akses terpercaya dengan AWS WA Tool

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Anda dapat menonaktifkan akses terpercaya menggunakan AWS Well-Architected Tool atau alat AWS Organizations.

> **Important**
>
> Kami sangat merekomendasikan bahwa bila memungkinkan, Anda menggunakan konsol AWS Well-Architected Tool atau alat untuk menonaktifkan integrasi dengan Organizations. Hal ini memungkinkan AWS Well-Architected Tool melakukan pembersihan apa pun yang diperlukan, seperti menghapus sumber daya atau peran akses yang tidak lagi diperlukan oleh layanan. Lanjutkan dengan langkah-langkah ini hanya jika Anda tidak dapat menonaktifkan integrasi menggunakan alat yang disediakan oleh AWS Well-Architected Tool.
> Jika Anda menonaktifkan akses tepercaya dengan menggunakan konsol AWS Well-Architected Tool atau alat, Anda tidak perlu menyelesaikan langkah-langkah ini.

Untuk menonaktifkan akses terpercaya menggunakan konsol AWS WA Tool

Lihat MembagikanAWS Well-Architected Tool sumber daya Anda di PanduanAWS Well-Architected Tool Pengguna.

Anda dapat menonaktifkan akses terpercaya dengan menjalankan perintah AWS CLI Organizations, atau dengan memanggil operasi API Organizations di salah satu SDK AWS.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk menonaktifkan akses layanan terpercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan AWS Well-Architected Tool sebagai layanan terpercaya dengan Organizations.

```
$ aws organizations disable-aws-service-access \
```

```
    --service-principal wellarchitected.amazonaws.com
```

Perintah ini tidak menghasilkan output saat berhasil.

- API AWS: NonaktifkanAWSServiceAccess

Pengelola Alamat IP Amazon VPC (IPAM) dan AWS Organizations

Amazon VPC IP Address Manager (IPAM) adalah fitur VPC yang memudahkan Anda merencanakan, melacak, dan memantau alamat IP untuk beban kerja Anda. AWS

Penggunaan AWS Organizations memungkinkan Anda memantau penggunaan alamat IP di seluruh organisasi Anda dan berbagi kumpulan alamat IP di seluruh akun anggota.

Untuk informasi selengkapnya, lihat Mengintegrasikan IPAM dengan AWS Organizations di Panduan Pengguna Amazon VPC IPAM.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan Amazon VPC IP Address Manager (IPAM) dengan. AWS Organizations

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat di akun manajemen organisasi Anda dan setiap akun anggota saat Anda mengintegrasikan IPAM dengan AWS Organizations menggunakan konsol IPAM atau menggunakan API IPAM. `EnableIpamOrganizationAdminAccount`

- `AWSServiceRoleForIPAM`

Untuk informasi selengkapnya, lihat Peran tertaut layanan untuk IPAM di Panduan Pengguna Amazon VPC IPAM.

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran tertaut layanan yang digunakan oleh IPAM M M M M M M M M M M.

- `ipam.amazonaws.com`

Untuk mengaktifkan akses terpercaya dengan IPAM M M M M M M M M M

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

> **Note**
>
> Bila Anda menetapkan administrator yang didelegasikan untuk organisasi Anda. IPAM memerlukan akses terpercaya ke AWS Organizations sebelum Anda dapat menetapkan akun anggota menjadi administrator yang didelegasikan untuk layanan ini untuk organisasi Anda.

Anda dapat mengaktifkan akses terpercaya hanya menggunakan alat Amazon VPC Address Manager (IPAM).

Jika Anda mengintegrasikan IPAM dengan AWS Organizations menggunakan konsol IPAM atau menggunakan IPAM `EnableIpamOrganizationAdminAccount` API, Anda secara otomatis memberikan akses tepercaya ke IPAM. Pemberian akses tepercaya menciptakan peran terkait layanan `AWSServiceRoleForIPAM` di akun manajemen dan di semua akun anggota di organisasi. IPAM menggunakan peran terkait layanan untuk memantau CIDR yang terkait dengan sumber daya jaringan EC2 di organisasi Anda dan untuk menyimpan metrik yang terkait dengan IPAM di Amazon. CloudWatch Untuk informasi selengkapnya, lihat Peran tertaut layanan untuk IPAM di Panduan Pengguna Amazon VPC IPAM.

Untuk petunjuk tentang mengaktifkan akses tepercaya, lihat Mengintegrasikan IPAM dengan AWS Organizations Panduan Pengguna Amazon VPC IPAM.

> **Note**
>
> Anda tidak dapat mengaktifkan akses tepercaya dengan IPAM menggunakan AWS Organizations konsol atau dengan `EnableAWSServiceAccess`API.

Untuk menonaktifkan akses terpercaya dengan IPAM M M M M M M M M

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Hanya administrator di AWS Organizations pengelolaan yang dapat menonaktifkan akses terpercaya dengan IPAM menggunakan AWS Organizations `disable-aws-service-access` API.

Untuk informasi tentang menonaktifkan izin akun IPAM dan menghapus peran tertaut layanan, lihat Peran tertaut layanan untuk IPAM di Panduan Pengguna Amazon VPC IPAM.

Anda dapat menonaktifkan akses terpercaya dengan menjalankan perintah AWS CLI Organizations, atau dengan memanggil operasi API Organizations di salah satu SDK AWS.

AWS CLI, AWS API

Cara menonaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk menonaktifkan akses layanan terpercaya:

- AWS CLI: disable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk menonaktifkan Amazon VPC IP Address Manager (IPAM) sebagai layanan terpercaya dengan Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ipam.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.

- AWSAPI: Nonaktifkan AWSServiceAccess

Mengaktifkan akun administrator yang didelegasikan untuk IPAM M M M M M M M M M M

Akun administrator yang didelegasikan untuk IPAM bertanggung jawab untuk membuat kumpulan IPAM dan alamat IP, mengelola dan memantau penggunaan alamat IP di organisasi, dan berbagi kumpulan alamat IP di seluruh akun anggota. Untuk informasi selengkapnya, lihat Mengintegrasikan IPAM dengan AWS Organizations di Panduan Pengguna Amazon VPC IPAM.

Hanya administrator di akun manajemen organisasi yang dapat mengonfigurasi administrator yang didelegasikan untuk IPAM.

Anda dapat menentukan akun administrator yang didelegasikan dari konsol IPAM, atau dengan menggunakan API. `enable-ipam-organization-admin-account` Untuk informasi selengkapnya, lihat enable-ipam-organization-admin-account di Referensi AWS AWS CLI Perintah.

> **Izin minimum**
>
> Hanya pengguna yang peran dalam organisasi Organizations yang dapat mengonfigurasi akun anggota sebagai administrator yang didelegasikan untuk IPAM dalam organisasi

Untuk mengonfigurasi administrator yang didelegasikan menggunakan konsol IPAM, lihat Mengintegrasikan IPAM dengan AWS Organizations Panduan Pengguna Amazon VPC IPAM.

Menonaktifkan administrator yang didelegasikan untuk IPAM M M M M M M M M M M M M.

Hanya administrator di akun manajemen organisasi yang dapat mengonfigurasi administrator yang didelegasikan untuk IPAM.

Untuk menghapus administrator didelegasikan menggunakan AWSAWS CLI, lihat disable-ipam-organization-admin-account di Referensi Perintah. AWS AWS CLI

Untuk menonaktifkan akun IPAM admin yang didelegasikan menggunakan konsol IPAM, lihat Mengintegrasikan IPAM dengan AWS Organizations Panduan Pengguna Amazon VPC IPAM.

Amazon VPC Reachability Analyzer dan AWS Organizations

Reachability Analyzer adalah alat analisis konfigurasi yang memungkinkan Anda melakukan pengujian konektivitas antara sumber daya sumber daya dan sumber daya tujuan di cloud pribadi virtual (VPC) Anda.

Menggunakan AWS Organizations dengan Reachability Analyzer memungkinkan Anda melacak jalur di seluruh akun di organisasi Anda.

Untuk informasi selengkapnya, lihat Analisis lintas akun untuk Reachability Analyzer di panduan pengguna Reachability Analyzer.

Gunakan informasi berikut untuk membantu Anda mengintegrasikan Reachability Analyzer dengan. AWS Organizations

Peran tertaut layanan yang dibuat saat Anda mengaktifkan integrasi

Peran tertaut layanan berikut secara otomatis dibuat di akun pengelolaan organisasi Anda bila Anda mengaktifkan akses terpercaya. Peran ini memungkinkan Reachability Analyzer untuk melakukan operasi yang didukung dalam akun organisasi Anda di organisasi Anda.

Anda dapat menghapus atau mengubah peran ini hanya jika Anda menonaktifkan akses tepercaya antara Reachability Analyzer dan Organisasi, atau jika Anda menghapus akun anggota dari organisasi.

- `AWSServiceRoleForReachabilityAnalyzer`

Untuk informasi selengkapnya, lihat Analisis lintas akun untuk Reachability Analyzer di panduan pengguna Reachability Analyzer.

Prinsipal layanan yang digunakan oleh peran tertaut layanan

Peran tertaut layanan di bagian sebelumnya dapat diambil hanya oleh prinsipal layanan yang diotorisasi oleh hubungan kepercayaan yang ditetapkan untuk peran tersebut. Peran terkait layanan yang digunakan oleh Reachability Analyzer memberikan akses ke prinsip-prinsip layanan berikut:

- `reachabilityanalyzer.networkinsights.amazonaws.com`

Untuk mengaktifkan akses tepercaya dengan Reachability Analyzer

Untuk informasi tentang izin yang diperlukan untuk mengaktifkan akses terpercaya, lihat Izin yang diperlukan untuk mengaktifkan akses terpercaya.

Ketika Anda menunjuk administrator yang didelegasikan untuk Reachability Analyzer, secara otomatis mengaktifkan akses tepercaya untuk Reachability Analyzer untuk organisasi Anda.

Reachability Analyzer memerlukan akses tepercaya AWS Organizations sebelum Anda dapat menunjuk akun anggota untuk menjadi administrator yang didelegasikan untuk layanan ini untuk organisasi Anda.

> **Important**
>
> - Anda dapat mengaktifkan akses tepercaya menggunakan konsol Reachability Analyzer atau konsol Organisasi. Namun, kami sangat

menyarankan agar Anda menggunakan konsol Reachability Analyzer atau `EnableMultiAccountAnalysisForAwsOrganization` API untuk mengaktifkan integrasi dengan Organisasi. Hal ini memungkinkan Reachability Analyzer melakukan konfigurasi apa pun yang dibutuhkannya, seperti membuat sumber daya yang dibutuhkan oleh layanan.

- Pemberian akses tepercaya menciptakan peran terkait layanan `AWSServiceRoleForReachabilityAnalyzer` di akun manajemen dan di semua akun anggota di organisasi. Reachability Analyzer menggunakan peran terkait layanan untuk memungkinkan manajemen, dan administrator yang didelegasikan untuk menjalankan analisis konektivitas antara sumber daya apa pun di organisasi. Reachability Analyzer mampu mengambil snapshot dari elemen jaringan akun dalam sebuah organisasi untuk menjawab kueri konektivitas.
- Untuk informasi selengkapnya, dan untuk petunjuk tentang mengaktifkan akses tepercaya melalui Reachability Analyzer, lihat Analisis lintas akun untuk Penganalisis Reachability di panduan pengguna Reachability Analyzer.

Anda dapat mengaktifkan akses terpercaya dengan menggunakan konsol AWS Organizations, dengan menjalankan perintah AWS CLI, atau dengan memanggil operasi API di salah satu SDK AWS.

AWS Management Console

Untuk mengaktifkan akses layanan terpercaya menggunakan konsol Organizations

1. Masuklah ke konsol AWS Organizations. Anda harus masuk sebagai pengguna IAM, mengambil IAM role, atau masuk sebagai pengguna akar (tidak Disarankan) di akun pengelolaan organisasi.
2. Pada halaman Layanan, temukan baris untuk VPC Reachability Analyzer, pilih nama layanan, lalu pilih Aktifkan akses tepercaya.
3. Di kotak dialog konfirmasi, aktifkan Menampilkan opsi untuk mengaktifkan akses terpercaya, masukkan **`enable`** dalam kotak, dan kemudian pilih Mengaktifkan akses terpercaya.
4. Jika Anda hanya administratorAWS Organizations, beri tahu administrator Reachability Analyzer bahwa mereka sekarang dapat mengaktifkan layanan tersebut menggunakan konsolnya untuk digunakan. AWS Organizations

AWS CLI, AWS API

Untuk mengaktifkan akses layanan terpercaya menggunakan CLI/SDK Organizations

Anda dapat menggunakan perintah AWS CLI atau operasi API untuk mengaktifkan atau mengaktifkan akses layanan terpercaya:

- AWS CLI: enable-aws-service-access

  Anda dapat menjalankan perintah berikut untuk mengaktifkan Reachability Analyzer sebagai layanan tepercaya dengan Organisasi.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal reachabilityanalyzer.networkinsights.amazonaws.com
  ```

  Perintah ini tidak menghasilkan output saat berhasil.
- AWSAPI: Aktifkan AWSServiceAccess

Untuk menonaktifkan akses tepercaya dengan Reachability Analyzer

Untuk informasi tentang izin yang diperlukan untuk menonaktifkan akses terpercaya, lihat Izin yang diperlukan untuk menonaktifkan akses terpercaya.

Anda dapat menonaktifkan akses tepercaya menggunakan konsol Reachability Analyzer (disarankan), atau konsol Organisasi. Untuk menonaktifkan akses tepercaya menggunakan konsol Reachability Analyzer, lihat Analisis lintas akun untuk Reachability Analyzer di panduan pengguna Reachability Analyzer.

Mengaktifkan akun administrator yang didelegasikan untuk Reachability Analyzer

Akun administrator yang didelegasikan dapat menjalankan analisis konektivitas di semua sumber daya dalam organisasi. Untuk informasi selengkapnya, lihat Mengintegrasikan Penganalisis Reachability dengan AWS Organizations di panduan pengguna Reachability Analyzer.

Hanya administrator di akun manajemen organisasi yang dapat mengonfigurasi administrator yang didelegasikan untuk Reachability Analyzer.

Anda dapat menentukan akun administrator yang didelegasikan dari konsol Reachability Analyzer, atau dengan menggunakan API. `RegisterDelegatedAdministrator` Untuk informasi selengkapnya, lihat RegisterDelegatedAdministratordi Referensi Perintah Organisasi.

Izin minimum

Hanya pengguna atau peran dalam akun manajemen Organisasi yang dapat mengonfigurasi akun anggota sebagai administrator yang didelegasikan untuk Reachability Analyzer di organisasi

Untuk mengonfigurasi administrator yang didelegasikan menggunakan konsol Reachability Analyzer, lihat Mengintegrasikan Penganalisis Reachability dengan di panduan pengguna Reachability Analyzer. AWS Organizations

Menonaktifkan administrator yang didelegasikan untuk Reachability Analyzer

Hanya administrator di akun manajemen organisasi yang dapat mengonfigurasi administrator yang didelegasikan untuk Reachability Analyzer.

Anda dapat menghapus administrator yang didelegasikan menggunakan konsol atau API Reachability Analyzer, atau dengan menggunakan operasi CLI atau SDK Organisasi`DeregisterDelegatedAdministrator`.

Untuk menonaktifkan akun Admin Reachability Analyzer yang didelegasikan menggunakan konsol Reachability Analyzer, lihat Analisis lintas akun untuk Reachability Analyzer di panduan pengguna Reachability Analyzer.

Administrator yang didelegasikan untuk AWS layanan yang bekerja dengan Organisasi

Kami menyarankan Anda menggunakan akun AWS Organizations manajemen dan pengguna serta perannya hanya untuk tugas yang harus dilakukan oleh akun tersebut. Kami juga menyarankan Anda menyimpan AWS sumber daya Anda di akun anggota lain di organisasi dan menjauhkannya dari akun manajemen. Ini karena fitur keamanan seperti Kebijakan kontrol layanan Organisasi (SCP) tidak membatasi pengguna atau peran dalam akun manajemen. Memisahkan sumber daya Anda dari akun manajemen Anda juga dapat membantu Anda memahami biaya pada faktur Anda.

Banyak AWS layanan yang terintegrasi dengan Organisasi memungkinkan Anda mengurangi penggunaan akun manajemen. Layanan ini memungkinkan Anda untuk mendaftarkan satu atau beberapa akun anggota sebagai administrator yang dapat mengelola semua akun organisasi yang digunakan dalam layanan. Akun ini disebut administrator yang didelegasikan untuk layanan tertentu

tersebut. Dengan mendaftarkan akun anggota sebagai administrator yang didelegasikan untuk AWS layanan, Anda mengaktifkan akun tersebut untuk memiliki beberapa izin administratif untuk layanan tersebut, serta izin untuk tindakan hanya-baca Organisasi.

Sebelum Anda mendaftarkan akun sebagai administrator yang didelegasikan untuk layanan:

- Konfirmasikan bahwa layanan mendukung administrator yang didelegasikan. Lihat tabel di AWS Layanan yang dapat Anda gunakan dengan AWS Organizations untuk mempelajari layanan mana yang mendukung administrator yang didelegasikan.
- Aktifkan akses tepercaya untuk layanan tersebut.

> **Note**
>
> Untuk mempelajari cara mengaktifkan layanan administrator yang didelegasikan, rujuk tabel AWS Layanan yang dapat Anda gunakan dengan AWS Organizations dan pilih tautan Pelajari lebih lanjut di kolom Administrator Delegasi Dukungan untuk layanan tersebut.

Izin yang diberikan ke akun administrator yang didelegasikan

Setiap akun administrator yang didelegasikan khusus layanan memiliki izin yang diberikan oleh layanan tersebut. Untuk mempelajari lebih lanjut, rujuk tabel AWS Layanan yang dapat Anda gunakan dengan AWS Organizations dan pilih tautan Pelajari lebih lanjut di kolom Administrator Delegasi Dukungan untuk layanan tersebut.

Akun administrator yang didelegasikan juga memiliki izin hanya-baca ini:

- `DescribeAccount`
- `DescribeCreateAccountStatus`
- `DescribeEffectivePolicy`
- `DescribeHandshake`
- `DescribeOrganization`
- `DescribeOrganizationalUnit`
- `DescribePolicy`
- `DescribeResourcePolicy`
- `ListAccounts`

- `ListAccountsForParent`
- `ListAWSServiceAccessForOrganization`
- `ListChildren`
- `ListCreateAccountStatus`
- `ListDelegatedAdministrators`
- `ListDelegatedServicesForAccount`
- `ListHandshakesForAccount`
- `ListHandshakesForOrganization`
- `ListOrganizationalUnitsForParent`
- `ListParents`
- `ListPolicies`
- `ListPoliciesForTarget`
- `ListRoots`
- `ListTagsForResource`
- `ListTargetsForPolicy`

Izin ini memungkinkan Anda untuk melihat, tetapi tidak mengubah item konsol ini:

- Struktur organisasi, semua akun dan OU, dan kebijakan organisasi
- Keanggotaan
- Semua akun dan OU.
- Kebijakan organisasi

Keamanan di AWS Organizations

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 menjelaskan hal ini sebagai keamanan dari 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. Auditor pihak ketiga secara berkala menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari AWS program kepatuhan. Untuk mempelajari tentang program kepatuhan yang berlaku AWS Organizations, lihat AWS Layanan dalam Lingkup berdasarkan Program Kepatuhan.
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Organizations. Topik berikut menunjukkan kepada Anda cara mengonfigurasi Organizations untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Organizations Anda.

Topik

AWS PrivateLink untuk AWS Organizations

Dengan AWS PrivateLink for AWS Organizations, Anda dapat mengakses AWS Organizations layanan dari dalam Virtual Private Cloud (VPC) tanpa harus melintasi internet publik.

Amazon VPC memungkinkan Anda meluncurkan AWS sumber daya di jaringan virtual khusus. Anda dapat menggunakan VPC untuk mengendalikan pengaturan jaringan, seperti rentang alamat IP, subnet, tabel rute, dan gateway jaringan. Untuk informasi lebih lanjut tentang Amazon VPC, lihat Panduan Pengguna Amazon VPC.

Untuk menghubungkan VPC Amazon Anda AWS Organizations, Anda harus terlebih dahulu menentukan titik akhir VPC antarmuka (titik akhir antarmuka). Titik akhir antarmuka diwakili oleh satu atau lebih antarmuka jaringan elastis (ENI) yang ditugaskan alamat IP privat dari subnet di VPC Anda. Permintaan dari VPC Anda ke titik akhir antarmuka AWS Organizations berlebih tetap berada di jaringan Amazon.

Untuk informasi umum tentang titik akhir antarmuka, lihat Mengakses AWS layanan menggunakan titik akhir VPC antarmuka di Panduan Pengguna Amazon VPC.

Topik

- Keterbatasan dan pembatasan AWS PrivateLink untuk AWS Organizations
- Membuat titik akhir VPC
- Membuat kebijakan VPC endpoint untuk AWS Organizations

Keterbatasan dan pembatasan AWS PrivateLink untuk AWS Organizations

Batasan VPC berlaku untuk AWS PrivateLink . AWS Organizations Untuk informasi selengkapnya, lihat Mengakses AWS layanan menggunakan titik akhir VPC antarmuka dan AWS PrivateLink kuota di Panduan Pengguna Amazon VPC. Selain itu, pembatasan berikut berlaku:

- Hanya tersedia di `us-east-1` wilayah
- Tidak mendukung Transport Layer Security (TLS) 1.1

Membuat titik akhir VPC

Anda dapat membuat AWS Organizations titik akhir di VPC menggunakan Konsol VPC Amazon, AWS Command Line Interface () atau.AWS CLI AWS CloudFormation

Untuk informasi tentang membuat dan mengonfigurasi titik akhir menggunakan konsol VPC Amazon atau konsol AWS CLI, lihat Membuat titik akhir VPC di Panduan Pengguna Amazon VPC. Untuk informasi tentang membuat dan mengonfigurasi titik akhir menggunakan AWS CloudFormation, lihat sumber daya AWS: :EC2: :vpcendPoint di Panduan Pengguna.AWS CloudFormation

Saat Anda membuat AWS Organizations titik akhir, gunakan yang berikut ini sebagai nama layanan:

```
com.amazonaws.us-east-1.organizations
```

Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 saat mengakses AWS, gunakan nama layanan FIPS berikut: AWS Organizations

```
com.amazonaws.us-east-1.organizations-fips
```

Membuat kebijakan VPC endpoint untuk AWS Organizations

Anda dapat melampirkan kebijakan titik akhir ke titik akhir VPC yang mengontrol akses ke Organizations. Kebijakan titik akhir menentukan informasi berikut:

- Prinsipal yang dapat melakukan tindakan.
- Tindakan yang dapat dilakukan.
- Sumber daya yang menjadi target tindakan.

Untuk informasi selengkapnya, lihat Mengontrol akses ke titik akhir VPC menggunakan kebijakan titik akhir di Panduan Pengguna Amazon VPC.

Contoh: Kebijakan VPC endpoint untuk tindakan AWS Organizations

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "Organizations:DescribeAccount"
         ],
         "Resource":"*"
      }
```

```
    ]
}
```

AWS Identity and Access Management dan AWS Organizations

Akses ke AWS Organizations memerlukan kredensial. Kredensial tersebut harus memiliki izin untuk mengakses sumber daya AWS, seperti bucket Amazon Simple Storage Service (Amazon S3), instans Amazon Elastic Compute Cloud (Amazon EC2), atau sebuah unit organisasi (OU) AWS Organizations. Bagian berikut memberikan detail tentang cara Anda menggunakan AWS Identity and Access Management (IAM) untuk membantu mengamankan akses ke organisasi Anda dengan mengendalikan siapa yang dapat mengelolanya.

Untuk menentukan siapa yang dapat mengelola bagian mana dari organisasi Anda, AWS Organizations menggunakan model izin berbasis IAM yang sama seperti layanan AWS. Sebagai administrator di akun pengelolaan organisasi, Anda dapat memberikan izin berbasis IAM untuk melakukan tugas AWS Organizations dengan melampirkan kebijakan ke pengguna, grup, dan peran dalam akun pengelolaan tersebut. Kebijakan tersebut menentukan tindakan yang dapat dilakukan oleh prinsipal utama tersebut. Anda melampirkan kebijakan izin IAM ke grup yang penggunanya merupakan anggota grup atau langsung ke pengguna atau peran. Sebagai praktik terbaik, kami menyarankan agar Anda melampirkan kebijakan pada grup, bukan ke pengguna. Anda juga memiliki opsi untuk memberikan izin administrator penuh kepada yang lain.

Untuk sebagian besar operasi administrator untuk AWS Organizations, Anda harus melampirkan izin ke pengguna atau grup di akun pengelolaan. Jika pengguna di akun anggota perlu melakukan operasi administrator untuk organisasi Anda, maka Anda harus memberikan izin AWS Organizations ke IAM role di akun pengelolaan dan memungkinkan pengguna dalam akun anggota untuk mengambil peran tersebut. Untuk informasi selengkapnya tentang kebijakan izin IAM, lihat Gambaran Umum Kebijakan IAM dalam Panduan Pengguna IAM.

Topik

- Autentikasi
- Pengendalian akses
- Mengelola izin akses untuk organisasi AWS Anda
- Menggunakan Kebijakan Berbasis Identitas (IAM Policy) untuk AWS Organizations
- Kontrol akses berbasis atribut dengan tag dan AWS Organizations

Autentikasi

Anda dapat mengakses AWS sebagai salah satu jenis identitas berikut:

- Pengguna root Akun AWS – Saat mendaftar ke AWS, Anda memberikan alamat dan kata sandi yang dikaitkan dengan akun Akun AWS Anda. Ini adalah kredensial root Anda, dan memberikan akses penuh ke semua sumber daya AWS Anda.

  > **Important**
  >
  > Saat Anda mendaftar Akun AWS, Pengguna root akun AWS akan dibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya dalam akun. Sebagai praktik terbaik keamanan, tetapkan akses administratif ke pengguna administratif, dan hanya gunakan pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

- Pengguna IAM – Pengguna IAM adalah identitas dalam akun Akun AWS Anda yang memiliki izin kustom spesifik (misalnya, izin untuk membuat sistem file di Amazon Elastic File System). Anda dapat menggunakan nama pengguna dan kata sandi IAM untuk masuk guna mengamankan halaman web AWS seperti AWS Management Console, AWS Forum Diskusi, atau Pusat Support AWS.

  Selain nama pengguna dan kata sandi, Anda juga dapat membuat access key untuk setiap pengguna. Anda dapat menggunakan kunci ini ketika mengakses layanan AWS secara terprogram, baik melalui salah satu dari beberapa SDK atau dengan menggunakan AWS Command Line Interface (AWS CLI). Alat SDK dan AWS CLI menggunakan kunci akses untuk menandatangani permintaan Anda secara kriptografis. Jika Anda tidak menggunakan alat AWS, maka Anda harus menandatangani permintaan tersebut sendiri. AWS Organizations men-support Tanda Tangan Versi 4, sebuah protokol untuk autentikasi permintaan API inbound. Untuk informasi selengkapnya tentang mengautentikasi permintaan, lihat Menandatangani permintaan AWS API di Panduan Pengguna IAM.

- IAM role – IAM role adalah identitas IAM lain yang dapat Anda buat di akun Anda dengan izin tertentu. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. IAM role memungkinkan Anda memperoleh access key sementara yang dapat mengakses layanan dan sumber daya AWS. Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

  - Akses pengguna gabungan – Alih-alih membuat pengguna IAM, Anda dapat menggunakan identitas pengguna yang ada dari AWS Directory Service, direktori pengguna korporasi Anda, atau penyedia identitas web. Ini dikenal sebagai pengguna gabungan. AWS menetapkan peran

ke pengguna gabungan ketika akses diminta melalui penyedia identitas. Untuk informasi lebih lanjut tentang pengguna gabungan, lihat Pengguna gabungan dan peran dalam Panduan Pengguna IAM.

- Akses lintas akun – Anda dapat menggunakan IAM role di akun Anda untuk memberikan izin kepada Akun AWS lain untuk mengakses sumber daya akun Anda. Sebagai contoh, lihat Tutorial: Mendelegasikan akses Akun AWS menggunakan peran IAM dalam Panduan Pengguna IAM.
- Akses layanan AWS – Anda dapat menggunakan IAM role di akun Anda untuk memberikan izin kepada akun AWS lain untuk mengakses sumber daya akun Anda. 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 layanan AWS dalam Panduan Pengguna IAM.
- Aplikasi yang berjalan di Amazon EC2 – Alih-alih menyimpan access key dalam Instans EC2 untuk digunakan oleh aplikasi yang berfungsi pada instans dan membuat permintaan API AWS, Anda dapat menggunakan IAM role untuk mengelola kredensial sementara untuk aplikasi ini. Untuk menetapkan peran AWS ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda dapat membuat profil instans yang terlampir ke instans. Profil instans memuat peran dan memungkinkan program yang berjalan di instans EC2 untuk mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat Menggunakan IAM role untuk memberikan izin pada aplikasi yang berjalan di instans Amazon EC2 dalam Panduan Pengguna IAM.

Pengendalian akses

Anda dapat memiliki kredensial yang benar untuk mengautentikasi permintaan Anda, tetapi kecuali jika Anda memiliki izin, Anda tidak dapat mengelola atau mengakses sumber daya AWS Organizations. Misalnya, Anda harus memiliki izin untuk membuat OU atau melampirkan kebijakan kontrol layanan (SCP) ke akun.

Bagian berikut menjelaskan cara mengelola izin untuk AWS Organizations.

- Mengelola izin akses untuk organisasi AWS Anda
- Menggunakan Kebijakan Berbasis Identitas (IAM Policy) untuk AWS Organizations
- Kontrol akses berbasis atribut dengan tag dan AWS Organizations

Mengelola izin akses untuk organisasi AWS Anda

Semua sumber daya AWS, termasuk root, OU, akun, dan kebijakan dalam suatu organisasi, dimiliki olehAkun AWS, dan izin untuk membuat atau mengakses sumber daya diatur oleh kebijakan izin. Untuk sebuah organisasi, akun pengelolaannya memiliki semua sumber daya. Administrator akun dapat mengontrol akses ke sumber daya AWS dengan melampirkan kebijakan izin ke identitas IAM (pengguna, grup, dan peran).

> **Note**
>
> Administrator akun (atau pengguna administrator) adalah pengguna dengan izin administrator. Untuk informasi selengkapnya tentang administrator, lihat Praktik terbaik keamanan di IAM di dalam Panduan Pengguna IAM.

Ketika memberikan izin, Anda memutuskan siapa yang mendapatkan izin, sumber daya yang mereka dapatkan izinnya, dan tindakan khusus yang ingin Anda izinkan di sumber daya tersebut.

Secara default, pengguna, grup, dan peran IAM tidak memiliki izin. Sebagai administrator di akun pengelolaan sebuah organisasi, Anda dapat melakukan tugas-tugas administratif atau mendelegasikan izin administrator kepada pengguna atau peran IAM lain dalam akun pengelolaan. Untuk melakukannya, Anda harus melampirkan kebijakan izin IAM ke pengguna, grup, atau peran IAM. Secara default, pengguna tidak memiliki izin sama sekali; hal ini kadang-kadang disebut penolakan implisit. Kebijakan tersebut menimpa penolakan implisit dengan izin eksplisit yang menentukan tindakan yang dapat dilakukan pengguna, dan sumber daya di mana mereka dapat melakukan tindakan. Jika izin diberikan ke sebuah peran, maka pengguna di akun lain dalam organisasi dapat mengambil peran itu.

Sumber daya dan operasi AWS Organizations

Bagian ini membahas bagaimana konsep AWS Organizations memetakan ke konsep setara-IAM mereka.

Sumber daya

Di AWS Organizations, Anda dapat mengontrol akses ke sumber daya berikut:

- Root dan OU yang membentuk struktur hirarkis dari suatu organisasi
- Akun yang merupakan anggota organisasi

- Kebijakan yang Anda lampirkan ke entitas dalam organisasi
- Jabat tangan yang Anda gunakan untuk mengubah status organisasi

Setiap sumber daya ini memiliki Amazon Resource Name (ARN) yang unik yang terkait dengannya. Anda mengontrol akses ke sumber daya dengan menentukan ARN di elemen `Resource` dari sebuah kebijakan izin IAM. Untuk daftar lengkap format ARN untuk sumber daya yang digunakanAWS Organizations, lihat Jenis sumber daya yang ditentukan oleh AWS Organizations dalam Referensi Otorisasi Layanan.

Operasi

AWS menyediakan serangkaian operasi untuk bekerja dengan sumber daya dalam suatu organisasi. Mereka memungkinkan Anda untuk melakukan hal-hal seperti membuat, membuat daftar, memodifikasi, mengakses isi, dan menghapus sumber daya. Sebagian besar operasi dapat direferensikan dalam elemen `Action` dari sebuah kebijakan IAM untuk mengontrol siapa yang dapat menggunakan operasi itu. Untuk daftar AWS Organizations operasi yang dapat digunakan sebagai izin dalam kebijakan IAM, lihat Tindakan yang ditentukan oleh AWS Organizations dalam Referensi Otorisasi Layanan.

Saat Anda menggabungkan `Action` dan sebuah `Resource` dalam satu kebijakan izin `Statement`, Anda mengontrol dengan tepat sumber daya mana yang set tertentu tindakan dapat digunakan padanya.

Kunci syarat

AWS menyediakan kunci syarat yang dapat Anda buat kueri-nya untuk memberikan kontrol yang lebih terperinci atas tindakan tertentu. Anda dapat melakukan referensi atas kunci syarat ini di elemen `Condition` dari sebuah kebijakan IAM untuk menentukan keadaan tambahan yang harus dipenuhi untuk pernyataan yang akan dianggap cocok.

Kunci syarat berikut ini sangat berguna khususnya dengan AWS Organizations:

- `aws:PrincipalOrgID` — Menyederhanakan penentuan elemen `Principal` dalam kebijakan berbasis sumber daya. Kunci global ini menyediakan alternatif untuk mendaftar semua ID akun untuk semua Akun AWS di suatu organisasi. Alih-alih membuat daftar dari semua akun yang merupakan anggota organisasi, Anda dapat menentukan ID Organisasi dalam elemen `Condition`.

> **Note**
>
> Syarat global ini juga berlaku pada akun pengelolaan dari suatu organisasi.

Untuk informasi selengkapnya, lihat deskripsi kunci konteks kondisi AWS global `PrincipalOrgID` di Panduan Pengguna IAM.

- `aws:PrincipalOrgPaths` — Gunakan kunci syarat ini untuk mencocokkan anggota root organisasi tertentu, OU, atau anak-anaknya. Kunci syarat `aws:PrincipalOrgPaths` mengembalikan BETUL ketika prinsipal utama (root user, IAM user, atau peran) membuat permintaan di path organisasi yang ditentukan. Path adalah representasi teks dari struktur dari sebuah entitas AWS Organizations. Untuk informasi selengkapnya tentang jalur, lihat Memahami jalur AWS Organizations entitas di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang penggunaan kunci kondisi ini, lihat aws: PrincipalOrgPaths di Panduan Pengguna IAM.

  Misalnya, elemen syarat berikut cocok untuk anggota dari salah satu dari dua OU yang ada dalam organisasi yang sama.

  ```
  "Condition": {
      "ForAnyValue:StringLike": {
          "aws:PrincipalOrgPaths": [
              "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
              "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-jkl0-awsddddd/"
          ]
      }
  }
  ```

- `organizations:PolicyType` — Anda dapat menggunakan kunci syarat ini untuk membatasi operasi API terkait kebijakan Organizations untuk bekerja hanya pada kebijakan Organizations dari jenis tertentu. Anda dapat menerapkan kunci syarat ini untuk setiap pernyataan kebijakan yang mencakup tindakan yang berinteraksi dengan kebijakan Organizations.

  Anda dapat menggunakan nilai berikut dengan kunci syarat ini:

  - `AISERVICES_OPT_OUT_POLICY`
  - `BACKUP_POLICY`
  - `SERVICE_CONTROL_POLICY`
  - `TAG_POLICY`

Misalnya, kebijakan contoh berikut memungkinkan pengguna untuk melakukan operasi Organizations. Namun, jika pengguna melakukan operasi yang mengambil argumen kebijakan, maka operasi diperbolehkan hanya jika kebijakan tertentu adalah kebijakan penandaan. Operasi gagal jika pengguna menentukan jenis kebijakan lainnya.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IfTaggingAPIThenAllowOnOnlyTaggingPolicies",
            "Effect": "Allow",
            "Action": "organizations:*",
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [ "TAG_POLICY" ]
                }
            }
        }
    ]
}
```

- `organizations:ServicePrincipal`— Tersedia sebagai kondisi jika Anda menggunakan AWSServiceAccess operasi Aktifkan AWSServiceAccess atau Nonaktifkan untuk mengaktifkan atau menonaktifkan akses tepercaya dengan AWS layanan lain. Anda dapat menggunakan `organizations:ServicePrincipal` untuk membatasi permintaan yang dibuat operasi tersebut ke daftar nama prinsipal utama layanan yang disetujui.

  Misalnya, kebijakan berikut memungkinkan pengguna untuk menentukan hanya AWS Firewall Manager saat mengaktifkan dan menonaktifkan akses tepercaya dengan AWS Organizations.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowOnlyAWSFirewallIntegration",
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:ServicePrincipal": [ "fms.amazonaws.com" ]
                }
            }
        }
    ]
}
```

Untuk daftar semua kunci kondisi AWS Organizations khusus yang dapat digunakan sebagai izin dalam kebijakan IAM, lihat Kunci kondisi untuk Referensi AWS Organizations Otorisasi Layanan.

Memahami kepemilikan sumber daya

Akun AWS memiliki sumber daya yang dibuat dalam akun, terlepas dari siapa yang membuat sumber daya tersebut. Secara khusus, pemilik sumber daya adalah entitas utama (yaitu, pengguna root, pengguna IAM, atau peran IAM) yang mengautentikasi permintaan pembuatan sumber daya. Akun AWS Untuk organisasi AWS, yaitu selalu akun pengelolaan. Anda tidak dapat memanggil sebagian besar operasi yang membuat atau mengakses sumber daya organisasi dari akun anggota. Contoh berikut menggambarkan cara kerjanya:

- Jika Anda menggunakan kredensial akun root dari akun pengelolaan Anda untuk membuat OU, maka akun pengelolaan Anda adalah pemilik sumber daya . (Dalam AWS Organizations, sumber daya adalah OU.)
- Jika Anda membuat pengguna IAM dalam akun pengelolaan Anda dan memberikan izin untuk membuat tabel sebuah OU ke pengguna tersebut, maka pengguna dapat membuat OU. Namun, akun pengelolaan Anda yang memiliki pengguna, memiliki sumber daya OU.
- Jika Anda membuat IAM role di akun pengelolaan Anda dengan izin untuk membuat OU, siapa pun yang dapat menggunakan peran tersebut dapat membuat OU. Akun pengelolaan, yang memiliki peran (bukan pengguna yang mengambil), memiliki sumber daya OU.

Mengelola akses ke sumber daya

Kebijakan izin menjelaskan siapa yang memiliki akses ke suatu objek. Bagian berikut menjelaskan pilihan yang tersedia untuk membuat kebijakan izin.

> **Note**
>
> Bagian ini membahas penggunaan IAM dalam konteks AWS Organizations. Bagian ini tidak memberikan informasi terperinci tentang layanan IAM. Untuk dokumentasi lengkap IAM, lihat Panduan Pengguna IAM. Untuk informasi tentang sintaks dan deskripsi kebijakan IAM, lihat referensi kebijakan IAM JSON di Panduan Pengguna IAM.

Kebijakan yang terlampir pada identitas IAM disebut sebagai kebijakan berbasis identitas (kebijakan IAM). Kebijakan yang terlampir pada sumber daya disebut sebagai kebijakan berbasis sumber daya. AWS Organizations hanya mendukung kebijakan berbasis identitas (kebijakan IAM).

Topik

- Kebijakan izin berbasis identitas (kebijakan IAM)
- Kebijakan berbasis sumber daya

Kebijakan izin berbasis identitas (kebijakan IAM)

Anda dapat melampirkan kebijakan ke identitas IAM untuk mengizinkan identitas tersebut melakukan operasi di sumber daya AWS. Misalnya, Anda dapat melakukan hal berikut:

- Melampirkan kebijakan izin ke pengguna atau grup di akun Anda — Untuk memberikan izin pengguna untuk membuat AWS Organizations sumber daya, seperti kebijakan kontrol layanan (SCP) atau OU, Anda dapat melampirkan kebijakan izin ke pengguna atau grup tempat pengguna tersebut berada. Pengguna atau grup harus ada dalam akun pengelolaan organisasi.
- Melampirkan kebijakan izin untuk peran (memberikan izin lintas akun) – Anda dapat melampirkan kebijakan izin berbasis identitas ke IAM role untuk memberikan izin lintas akun ke sebuah organisasi. Misalnya, administrator dalam akun pengelolaan dapat membuat peran untuk memberikan izin lintas akun ke pengguna yang ada dalam akun anggota sebagai berikut:
  1. Administrator akun pengelolaan membuat IAM role dan melampirkan kebijakan izin untuk peran yang memberikan izin pada sumber daya organisasi.
  2. Administrator akun pengelolaan melampirkan kebijakan kepercayaan ke peran yang mengidentifikasi ID akun anggota sebagai `Principal` yang dapat mengambil peran tersebut.
  3. Administrator akun anggota kemudian dapat mendelegasikan izin untuk mengambil peran untuk setiap pengguna yang ada di akun anggota. Dengan melakukan hal ini akan memungkinkan pengguna di akun anggota untuk membuat atau mengakses sumber daya di akun pengelolaan

dan organisasi. Prinsipal dalam kebijakan kepercayaan juga dapat berupa AWS jika Anda ingin memberikan izin ke layanan AWS untuk mengambil peran.

Untuk informasi selengkapnya tentang menggunakan IAM untuk mendelegasikan izin, lihat Manajemen Akses dalam Panduan Pengguna IAM.

Berikut ini adalah contoh kebijakan yang memungkinkan pengguna untuk melakukan `CreateAccount` tindakan di organisasi Anda.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"Stmt1OrgPermissions",
         "Effect":"Allow",
         "Action":[
            "organizations:CreateAccount"
         ],
         "Resource":"*"
      }
   ]
}
```

Anda juga dapat memberikan ARN sebagian dalam `Resource` elemen kebijakan untuk menunjukkan jenis sumber daya.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowCreatingAccountsOnResource",
         "Effect":"Allow",
         "Action":"organizations:CreateAccount",
         "Resource":"arn:aws:organizations::*:account/*"
      }
   ]
}
```

Anda juga dapat menolak pembuatan akun yang tidak menyertakan tag khusus ke akun yang sedang dibuat.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyCreatingAccountsOnResourceBasedOnTag",
         "Effect":"Deny",
         "Action":"organizations:CreateAccount",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/key":"value"
            }
         }
      }
   ]
}
```

Untuk informasi selengkapnya tentang pengguna, grup, peran, dan izin, lihat identitas IAM (pengguna, grup pengguna, dan peran) di Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Layanan lain, seperti Amazon S3, men-support kebijakan izin berbasis sumber daya. Misalnya, Anda dapat melampirkan kebijakan ke bucket Amazon S3 untuk mengelola izin akses ke bucket tersebut. AWS Organizations saat ini tidak men-support kebijakan berbasis sumber daya.

Menentukan elemen kebijakan: Tindakan, syarat, efek, dan sumber daya

Untuk setiap sumber daya AWS Organizations, layanan menentukan serangkaian operasi API, atau tindakan, yang dapat berinteraksi dengan atau memanipulasi sumber daya tersebut dalam beberapa cara. Untuk memberikan izin bagi operasi ini, AWS Organizations menentukan serangkaian tindakan yang dapat Anda tentukan dalam kebijakan. Misalnya, untuk sumber daya OU, AWS Organizations menetapkan tindakan seperti berikut:

- `AttachPolicy` dan `DetachPolicy`
- `CreateOrganizationalUnit` dan `DeleteOrganizationalUnit`
- `ListOrganizationalUnits` dan `DescribeOrganizationalUnit`

Dalam beberapa kasus, melakukan operasi API mungkin memerlukan izin untuk lebih dari satu tindakan dan mungkin memerlukan izin untuk lebih dari satu sumber daya.

Berikut ini adalah elemen paling basic yang dapat Anda gunakan dalam kebijakan izin IAM:

- Tindakan – Gunakan kata kunci untuk mengidentifikasi operasi (tindakan) yang ingin Anda izinkan atau tolak. Misalnya, tergantung pada `Effect`, `organizations:CreateAccount` mengizinkan atau menolak izin pengguna untuk melakukan operasi AWS Organizations `CreateAccount`. Untuk informasi selengkapnya, lihat elemen kebijakan IAM JSON: Tindakan dalam Panduan Pengguna IAM.
- Sumber Daya – Gunakan kata kunci ini untuk menentukan ARN dari sumber daya yang kepadanya pernyataan kebijakan berlaku. Untuk informasi selengkapnya, lihat elemen kebijakan IAM JSON: Sumber daya dalam Panduan Pengguna IAM.
- Syarat – Gunakan kata kunci ini untuk menentukan syarat yang harus dipenuhi agar pernyataan kebijakan dapat diterapkan. `Condition` biasanya menentukan keadaan tambahan yang harus BETUL agar kebijakan dapat dicocokkan. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Syarat di Panduan Pengguna IAM.
- Efek – Gunakan kata kunci ini untuk menentukan apakah pernyataan kebijakan mengizinkan atau menolak tindakan pada sumber daya. Jika Anda tidak secara eksplisit memberikan akses ke (mengizinkan) sumber daya, maka 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 melakukan tindakan tertentu pada sumber daya tertentu, meskipun kebijakan yang berbeda memberikan akses. Untuk informasi selengkapnya, lihat elemen kebijakan IAM JSON: Efek dalam Panduan Pengguna IAM.
- Prinsipal – Dalam kebijakan berbasis identitas (kebijakan IAM), pengguna yang kepadanya kebijakan tersebut terlampir secara otomatis adalah prinsipal. Untuk kebijakan berbasis sumber daya, Anda menentukan pengguna, akun, layanan, atau entitas lain yang ingin Anda terima izinnya (berlaku hanya untuk kebijakan berbasis-sumber daya). AWS Organizations men-support kebijakan berbasis-identitas saat ini, tidak men-support kebijakan berbasis sumber daya.

Untuk mempelajari lebih lanjut tentang sintaks dan deskripsi kebijakan IAM, lihat referensi kebijakan IAM JSON di Panduan Pengguna IAM.

Menggunakan Kebijakan Berbasis Identitas (IAM Policy) untuk AWS Organizations

Sebagai administrator akun pengelolaan sebuah organisasi, Anda dapat mengontrol akses ke sumber daya AWS dengan melampirkan kebijakan izin untuk identitas (IAM) AWS Identity and Access Management (pengguna, grup, dan peran) dalam organisasi. Ketika memberikan izin, Anda

memutuskan orang yang mendapatkan izin, sumber daya yang mereka dapatkan izinnya, dan tindakan khusus yang ingin Anda izinkan di sumber daya tersebut. Jika izin diberikan ke sebuah peran, maka peran tersebut dapat diambil oleh pengguna di akun lain dalam organisasi.

Secara default, pengguna tidak memiliki izin apa pun. Semua izin harus secara eksplisit diberikan oleh kebijakan. Jika izin tidak secara eksplisit diberikan, maka izin itu secara implisit ditolak. Jika izin secara eksplisit ditolak, maka itu mengesampingkan kebijakan lain yang mungkin telah mengizinkannya. Dengan kata lain, pengguna hanya memiliki izin yang secara eksplisit diberikan dan yang tidak secara eksplisit ditolak.

Selain teknik basic yang dijelaskan dalam topik ini, Anda dapat mengontrol akses ke organisasi Anda dengan menggunakan tag yang diterapkan ke sumber daya di organisasi Anda: root organisasi, unit organisasi (OU), akun, dan kebijakan. Untuk informasi lebih lanjut, lihat Kontrol akses berbasis atribut dengan tag dan AWS Organizations.

Memberikan izin admin penuh ke pengguna

Anda dapat membuat kebijakan IAM yang memberikan izin administrator AWS Organizations penuh kepada pengguna IAM di organisasi Anda. Anda dapat melakukan ini menggunakan editor kebijakan JSON di konsol IAM.

Untuk 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 dokumen kebijakan JSON berikut:

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

```
    }
}
```

6. 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. 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.
8. Pilih Buat kebijakan untuk menyimpan kebijakan baru Anda.

Untuk mempelajari selengkapnya tentang membuat kebijakan IAM, lihat Membuat kebijakan IAM di Panduan Pengguna IAM.

Memberikan akses terbatas berdasarkan tindakan

Jika Anda ingin memberikan izin terbatas bukan izin penuh, Anda dapat membuat kebijakan yang mencantumkan izin tersendiri yang ingin Anda izinkan di elemen `Action` dari kebijakan izin IAM. Seperti yang ditunjukkan dalam contoh berikut, Anda dapat menggunakan karakter wildcard (*) untuk memberikan izin `Describe*` dan izin `List*` saja, pada dasarnya menyediakan akses hanya-baca ke organisasi.

> **Note**
>
> Dalam kebijakan kontrol layanan (SCP), karakter wildcard (*) dalam elemen `Action` hanya dapat digunakan oleh dirinya sendirinya atau di akhir string. Ia tidak dapat muncul di awal atau tengah string. Karena itu, `"servicename:action*"` valid, tapi `"servicename:*action"` dan `"servicename:some*action"` keduanya tidak valid di SCP.

```
{
```

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

Untuk daftar semua izin yang tersedia untuk ditetapkan dalam kebijakan IAM, lihat Tindakan yang ditentukan oleh AWS Organizations dalam Referensi Otorisasi Layanan.

Memberikan akses ke sumber daya tertentu

Selain membatasi akses ke tindakan tertentu, Anda dapat membatasi akses ke entitas tertentu dalam organisasi Anda. Elemen `Resource` dalam contoh di bagian sebelumnya, keduanya menentukan karakter wildcard ("*"), yang berarti "sumber daya apa pun yang dapat diakses oleh tindakan." Sebaliknya, Anda dapat mengganti "*" dengan Amazon Resource Name (ARN) entitas tertentu yang ingin Anda izinkan akses-nya.

Contoh: Memberikan izin untuk satu OU

Pernyataan pertama dari kebijakan berikut memungkinkan pengguna IAM akses baca ke seluruh organisasi, tetapi pernyataan kedua memungkinkan pengguna untuk melakukan tindakan administratif AWS Organizations hanya dalam satu unit organisasi (OU) tertentu. Hal ini tidak meluas ke setiap OU anak. Tidak ada akses penagihan yang diberikan. Perhatikan bahwa ia tidak memberikan akses administratif ke Akun AWS di OU. Ia hanya memberikan izin untuk melakukan operasi AWS Organizations pada akun yang ada dalam OU tertentu:

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

```
    {
      "Effect": "Allow",
      "Action": "organizations:*",
      "Resource": "arn:aws:organizations::<masterAccountId>:ou/o-<organizationId>/ou-
<organizationalUnitId>"
    }
  ]
}
```

Anda mendapatkan ID untuk OU dan organisasi dari konsol AWS Organizations atau dengan memanggil API `List*`. Pengguna atau grup yang kepadanya Anda menerapkan kebijakan ini, dapat melakukan tindakan apapun (`"organizations:*"`) pada setiap entitas yang secara langsung terkandung dalam OU tertentu. OU diidentifikasi oleh Amazon Resource Name (ARN).

Untuk informasi selengkapnya tentang ARN untuk berbagai sumber daya, lihat Jenis sumber daya yang ditentukan oleh AWS Organizations dalam Referensi Otorisasi Layanan.

Memberikan kemampuan untuk mengaktifkan akses terpercaya ke prinsipal layanan terbatas

Anda dapat menggunakan elemen `Condition` dari sebuah pernyataan kebijakan untuk lebih membatasi keadaan di mana pernyataan kebijakan dianggap cocok.

Contoh: Memberikan izin untuk mengaktifkan akses terpercaya ke satu layanan tertentu

Pernyataan berikut menunjukkan bagaimana Anda dapat membatasi kemampuan untuk mengaktifkan akses terpercaya hanya untuk layanan yang Anda tentukan. Jika pengguna mencoba untuk memanggil API dengan prinsipal utama layanan yang berbeda dari yang untuk AWS IAM Identity Center, maka kebijakan ini tidak cocok dan permintaan ditolak:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "organizations:EnableAWSServiceAccess",
            "Resource": "*",
            "Condition": {
                "StringEquals" : {
                    "organizations:ServicePrincipal" : "sso.amazonaws.com"
                }
            }
```

```
        }
    ]
}
```

Untuk informasi selengkapnya tentang ARN untuk berbagai sumber daya, lihat Jenis sumber daya yang ditentukan oleh AWS Organizations dalam Referensi Otorisasi Layanan.

Kontrol akses berbasis atribut dengan tag dan AWS Organizations

Kontrol akses berbasis atribut memungkinkan Anda menggunakan atribut yang dikelola administrator seperti tag yang dilampirkan pada sumber daya AWS dan identitas AWS untuk mengontrol akses ke sumber daya tersebut. Sebagi contoh, Anda dapat menentukan bahwa pengguna dapat mengakses sumber daya ketika pengguna dan sumber daya memiliki nilai yang sama untuk tag tertentu.

Sumber daya yang diberi tag AWS Organizations termasuk Akun AWS, root organisasi, unit organisasi (UO), atau kebijakan. Bila Anda melampirkan tag ke sumber daya Organizations, Anda kemudian dapat menggunakan tag tersebut untuk mengontrol siapa yang dapat mengakses sumber daya tersebut. Anda melakukan ini dengan menambahkan elemen `Condition` untuk pernyataan izin kebijakan AWS Identity and Access Management (IAM) yang memeriksa apakah kunci dan nilai tag tertentu sudah hadir sebelum memungkinkan tindakan. Hal ini memungkinkan Anda untuk membuat kebijakan IAM yang secara efektif mengatakan "Izinkan pengguna untuk mengelola OU yang memiliki tag dengan kunci X dan nilai Y saja" atau "Izinkan pengguna mengelola OU yang ditandai dengan kunci Z yang memiliki nilai yang sama dengan kunci tag Z terlampir pengguna."

Anda dapat mendasarkan pengujian `Condition` Anda pada berbagai jenis referensi tag dalam kebijakan IAM.

- Memeriksa tag yang dilampirkan ke sumber daya yang ditentukan dalam permintaan
- Memeriksa tag yang dilampirkan ke pengguna atau peran IAM yang membuat permintaan
- Periksa tag yang disertakan sebagai parameter dalam permintaan

Untuk informasi selengkapnya tentang menggunakan tag untuk kontrol akses dalam kebijakan, lihat Mengontrol akses ke dan untuk pengguna dan peran IAM menggunakan dengan tag sumber daya. Untuk sintaksis lengkap kebijakan izin IAM, lihat Referensi kebijakan IAM JSON

Memeriksa tag yang dilampirkan ke sumber daya yang ditentukan dalam permintaan

Ketika Anda membuat permintaan dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau salah satu AWS SDK, Anda menentukan sumber daya

apa yang ingin Anda akses dengan permintaan tersebut. Apakah Anda mencoba untuk membuat daftar sumber daya yang tersedia dari jenis tertentu, membaca sumber daya, atau menulis ke, memodifikasi, atau memperbarui sumber daya, Anda menentukan sumber daya yang akan diakses sebagai parameter dalam permintaan. Permintaan tersebut dikontrol oleh kebijakan izin IAM yang Anda lampirkan ke pengguna dan peran Anda. Dalam kebijakan ini, Anda dapat membandingkan tag yang terlampir pada sumber daya yang diminta dan memilih untuk mengizinkan atau menolak akses berdasarkan kunci dan nilai tag tersebut.

Untuk memeriksa tag yang terlampir pada sumber daya, Anda referensi tag dalam elemen `Condition` dengan melakukan prefacing pada name kunci tag dengan string berikut: `aws:ResourceTag/`

Sebagai contoh, kebijakan contoh berikut memungkinkan pengguna atau peran untuk melakukan operasi AWS Organizations kecuali sumber daya yang memiliki tag dengan kunci `department` dan nilai `security`. Jika kunci dan nilai tersebut hadir, maka kebijakan secara eksplisit menyangkal operasi `UntagResource`.

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

        },
        {
            "Effect" : "Deny",
            "Action" : "organizations:UntagResource",
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "aws:ResourceTag/department" : "security"
                }
            }
        }
    ]
}
```

Untuk informasi selengkapnya tentang cara menggunakan elemen ini, lihat Mengontrol akses ke sumber daya dan aws:ResourceTAG dalam Panduan Pengguna IAM.

Memeriksa tag yang dilampirkan ke pengguna atau peran IAM yang membuat permintaan

Anda dapat mengontrol apa yang boleh dilakukan oleh orang yang membuat permintaan (prinsipal) berdasarkan tag yang dilampirkan ke pengguna atau peran IAM orang tersebut. Untuk melakukannya, gunakan kunci syarat `aws:PrincipalTag/key-name` untuk menentukan tag dan nilai yang harus dilampirkan ke pengguna atau peran yang memanggil.

Contoh berikut menunjukkan cara mengizinkan tindakan hanya ketika tag tertentu (`cost-center`) memiliki nilai yang sama pada prinsipal utama yang memanggil operasi, dan sumber daya yang sedang diakses oleh operasi. Dalam contoh ini, pengguna yang memanggil dapat memulai dan menghentikan instans Amazon EC2 hanya jika instans tersebut ditandai dengan nilai `cost-center` yang sama sebagai pengguna.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "ec2:startInstances",
            "ec2:stopInstances"
        ],
        "Resource": "*",
        "Condition": {"StringEquals":
            {"ec2:ResourceTag/cost-center": "${aws:PrincipalTag/cost-center}"}}
    }
}
```

Untuk informasi selengkapnya tentang cara menggunakan elemen ini, lihat Mengontrol akses ke prinsipal IAM dan `aws:PrincipalTag` di Panduan Pengguna IAM.

Periksa tag yang disertakan sebagai parameter dalam permintaan

Beberapa operasi memungkinkan Anda untuk menentukan tag sebagai bagian dari permintaan. Sebagai contoh, ketika Anda membuat sumber daya, Anda dapat menentukan tag yang terlampir pada sumber daya baru. Anda dapat menentukan elemen `Condition` yang menggunakan `aws:TagKeys` untuk mengizinkan atau menolak operasi berdasarkan apakah kunci tag tertentu, atau sekumpulan kunci, disertakan dalam permintaan. Operator perbandingan ini tidak peduli nilai yang terkandung dalam tag. Ia hanya memeriksa apakah tag dengan kunci tertentu hadir.

Untuk memeriksa kunci tag, atau membuat daftar kunci, tentukan elemen `Condition` dengan sintaksis berikut:

```
"aws:TagKeys": [ "tag-key-1", "tag-key-2", ... , "tag-key-n" ]
```

Anda dapat menggunakan `ForAllValues:` melakukan preface atas operator perbandingan untuk memastikan bahwa semua kunci dalam permintaan harus sesuai dengan salah satu kunci yang ditentukan dalam kebijakan. Sebagai contoh, kebijakan contoh berikut memungkinkan setiap operasi Organizations hanya jika tiga semuanya dari kunci tag yang ditentukan hadir dalam permintaan.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "organizations:*",
        "Resource": "*",
        "Condition": {
            "ForAllValues:StringEquals": {
                "aws:TagKeys": [
                    "department",
                    "costcenter",
                    "manager"
                ]
            }
        }
    }
}
```

Atau, snda dapat menggunakan `ForAnyValue:` melakukan preface atas operator perbandingan untuk memastikan bahwa paling tidak satu dari semua kunci dalam permintaan sesuai dengan salah satu kunci yang ditentukan dalam kebijakan. Sebagai contoh, kebijakan berikut memungkinkan operasi Organizations hanya jika paling tidak satu dari kunci tag yang ditentukan hadir dalam permintaan.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "organizations:*",
        "Resource": "*",
        "Condition": {
```

```
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": [
                    "stage",
                    "region",
                    "domain"
                ]
            }
        }
    }
}
```

Beberapa operasi memungkinkan Anda untuk menentukan tag sebagai bagian dari permintaan. Sebagai contoh, ketika Anda membuat sumber daya, Anda dapat menentukan tag yang terlampir pada sumber daya baru. Anda dapat membandingkan pasangan nilai kunci tag dalam kebijakan dengan pasangan nilai kunci yang disertakan dengan permintaan tersebut. Untuk melakukannya, referensi tag dalam elemen `Condition` dengan melakukan preface atas tag nama kunci dengan string berikut: `aws:RequestTag/`*`key-name`* dan kemudian tentukan nilai tag yang harus ada.

Sebagai contoh, kebijakan contoh berikut menolak permintaan oleh pengguna atau peran untuk membuat Akun AWS di mana permintaan kehilangan tag `costcenter`, atau menyediakan tag dengan nilai selain 1, 2, atau 3.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "organizations:CreateAccount",
            "Resource": "*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/costcenter": "true"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": "organizations:CreateAccount",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringNotEquals": {
                    "aws:RequestTag/costcenter": [
```

```
                        "1",
                        "2",
                        "3"
                    ]
                }
            }
        }
    ]
}
```

Untuk informasi selengkapnya tentang cara menggunakan elemen ini, lihat aws:TagKeys dan aws:RequestTag dalam Panduan Pengguna IAM.

Pencatatan dan pemantauan di AWS Organizations

Sebagai praktik terbaik, Anda harus memantau organisasi Anda untuk memastikan bahwa perubahan dicatat. Hal ini membantu Anda untuk memastikan bahwa setiap perubahan yang tidak terduga dapat diselidiki dan perubahan yang tidak diinginkan dapat dibatalkan. AWS Organizations saat ini men-support dua layanan AWS yang memungkinkan Anda untuk memantau organisasi Anda dan aktivitas yang terjadi di dalamnya.

Topik

- Mencatat log AWS Organizations panggilan API dengan AWS CloudTrail
- Amazon EventBridge

Mencatat log AWS Organizations panggilan API dengan AWS CloudTrail

AWS Organizationsterintegrasi denganAWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan diAWS Organizations. CloudTrail menangkap semua panggilan API untuk AWS Organizations sebagai peristiwa, termasuk panggilan dari AWS Organizations konsol dan dari panggilan kode ke AWS Organizations API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara berkelanjutan ke bucket Amazon S3, termasuk acara untuk. AWS Organizations 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 dibuatAWS Organizations, alamat IP tempat itu dibuat, siapa yang membuatnya, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

> **Important**
>
> Anda dapat melihat semua CloudTrail informasi AWS Organizations hanya di Wilayah AS Timur (Virginia N.). Jika Anda tidak melihat AWS Organizations aktivitas di CloudTrail konsol, atur konsol Anda ke US East (Virginia N.) menggunakan menu di sudut kanan atas. Jika Anda melakukan kueri CloudTrail dengan alat SDK AWS CLI atau SDK, arahkan kueri Anda ke titik akhir AS Timur (Virginia N.).

Informasi AWS Organizations di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi diAWS Organizations, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di Akun AWS Anda. Untuk informasi selengkapnya, lihat Melihat Acara dengan Riwayat CloudTrail Acara.

Untuk catatan berkelanjutan tentang peristiwa di Akun AWS, termasuk peristiwa untuk AWS Organizations, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Saat CloudTrail logging diaktifkan di AndaAkun AWS, panggilan API yang dilakukan untuk AWS Organizations tindakan dilacak dalam file CloudTrail log, di mana mereka ditulis dengan catatan AWS layanan lainnya. Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan bertindak atas data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat yang berikut:

- Ikhtisar untuk Membuat Jejak
- CloudTrail Layanan dan Integrasi yang Didukung
- Mengkonfigurasi Notifikasi Amazon SNS untuk CloudTrail

Semua AWS Organizations tindakan dicatat oleh CloudTrail dan didokumentasikan dalam Referensi AWS Organizations API. Misalnya, panggilan ke `CreateAccount` (termasuk `CreateAccountResult` acara),, `ListHandshakesForAccountCreatePolicy`, dan `InviteAccountToOrganization` menghasilkan entri dalam file CloudTrail log.

Setiap entri log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas pengguna dalam entri log membantu Anda menentukan hal berikut:

- Apakah permintaan dibuat dengan pengguna root atau kredenal pengguna IAM
- Jika permintaan tersebut dibuat dengan kredensial keamanan sementara untuk IAM role atau pengguna gabungan
- Jika permintaan tersebut dibuat oleh layanan AWS lainnya

Untuk informasi lain, lihat Elemen userIdentity CloudTrail.

Memahami entri file log AWS Organizations

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. Peristuwa mewakili satu permintaan dari sumber apa pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh entri log: CloseAccount

Contoh berikut menunjukkan entri CloudTrail log untuk `CloseAccount` panggilan sampel yang dihasilkan saat API dipanggil dan alur kerja untuk menutup akun mulai diproses di latar belakang.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE:my-admin-role",
        "arn": "arn:aws:sts::111122223333:assumed-role/my-admin-role/my-session-id",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAMVNPBQA3EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/my-admin-role",
                "accountId": "111122223333",
                "userName": "my-session-id"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2022-03-18T18:17:06Z"
```

```
            }
        }
    },
    "eventTime": "2022-03-18T18:17:06Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CloseAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.1",
    "userAgent":  "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)...",
    "requestParameters": {
        "accountId": "555555555555"
    },
    "responseElements": null,
    "requestID": "e28932f8-d5da-4d7a-8238-ef74f3d5c09a",
    "eventID": "19fe4c10-f57e-4cb7-a2bc-6b5c30233592",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Contoh berikut menunjukkan entri CloudTrail log untuk `CloseAccountResult` panggilan setelah alur kerja latar belakang untuk menutup akun berhasil diselesaikan.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "organizations.amazonaws.com"
  },
  "eventTime": "2022-03-18T18:17:06Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CloseAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "organizations.amazonaws.com",
  "userAgent": "organizations.amazonaws.com",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "readOnly": false,
```

```
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "closeAccountStatus": {
      "accountId": "555555555555",
      "state": "SUCCEEDED",
      "requestedTimestamp": "Mar 18, 2022 6:16:58 PM",
      "completedTimestamp": "Mar 18, 2022 6:16:58 PM"
    }
   },
   "eventCategory": "Management"
}
```

Contoh entri log: CreateAccount

Contoh berikut menunjukkan entri CloudTrail log untuk `CreateAccount` panggilan sampel yang dihasilkan saat API dipanggil dan alur kerja untuk membuat akun mulai diproses di latar belakang.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE:my-admin-role",
        "arn": "arn:aws:sts::111122223333:assumed-role/my-admin-role/my-session-id",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAMVNPBQA3EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/my-admin-role",
                "accountId": "111122223333",
                "userName": "my-session-id"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-09-16T21:16:45Z"
            }
        }
    },
    "eventTime": "2018-06-21T22:06:27Z",
```

```
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CreateAccount",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.1",
    "userAgent":  "Mozilla/5.0 (Windows NT 10.0; Win64; x64)...",
    "requestParameters": {
        "tags": [],
        "email": "****",
        "accountName": "****"
    },
    "responseElements": {
        "createAccountStatus": {
            "accountName": "****",
            "state": "IN_PROGRESS",
            "id": "car-examplecreateaccountrequestid111",
            "requestedTimestamp": "Sep 16, 2020 9:20:50 PM"
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

Contoh berikut menunjukkan entri CloudTrail log untuk `CreateAccount` panggilan setelah alur kerja latar belakang untuk membuat akun berhasil diselesaikan.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "..."
  },
  "eventTime": "2020-09-16T21:20:53Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "....",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
```

```
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "SUCCEEDED",
      "accountName": "****",
      "accountId": "444455556666",
      "requestedTimestamp": "Sep 16, 2020 9:20:50 PM",
      "completedTimestamp": "Sep 16, 2020 9:20:53 PM"
    }
  }
}
```

Contoh berikut menunjukkan entri CloudTrail log yang dihasilkan setelah alur kerja `CreateAccount` latar belakang gagal membuat akun.

```
  {
  "eventVersion": "1.06",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "AWS Internal"
  },
  "eventTime": "2018-06-21T22:06:27Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CreateAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "AWS Internal",
  "userAgent": "AWS Internal",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "createAccountStatus": {
      "id": "car-examplecreateaccountrequestid111",
      "state": "FAILED",
      "accountName": "****",
      "failureReason": "EMAIL_ALREADY_EXISTS",
      "requestedTimestamp": Jun 21, 2018 10:06:27 PM,
```

```
      "completedTimestamp": Jun 21, 2018 10:07:15 PM
    }
  }
}
```

Contoh entri log: CreateOrganizationalUnit

Contoh berikut menunjukkan entri CloudTrail log untuk `CreateOrganizationalUnit` panggilan sampel.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:40:11Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CreateOrganizationalUnit",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "requestParameters": {
        "name": "OU-Developers-1",
        "parentId": "r-a1b2"
    },
    "responseElements": {
        "organizationalUnit": {
            "arn": "arn:aws:organizations::111111111111:ou/o-aa111bb222/ou-
examplerootid111-exampleouid111",
            "id": "ou-examplerootid111-exampleouid111",
            "name": "test-cloud-trail"
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
```

```
}
```

Contoh entri log: InviteAccountToOrganization

Contoh berikut menunjukkan entri CloudTrail log untuk `InviteAccountToOrganization` panggilan sampel.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:41:17Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "InviteAccountToOrganization",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "requestParameters": {
        "notes": "This is a request for Mary's account to join Diego's organization.",
        "target": {
            "type": "ACCOUNT",
            "id": "111111111111"
        }
    },
    "responseElements": {
        "handshake": {
            "requestedTimestamp": "Jan 18, 2017 9:41:16 PM",
            "state": "OPEN",
            "arn": "arn:aws:organizations::111111111111:handshake/o-aa111bb222/invite/
h-examplehandshakeid111",
            "id": "h-examplehandshakeid111",
            "parties": [
                {
                    "type": "ORGANIZATION",
                    "id": "o-aa111bb222"
                },
```

```
                {
                    "type": "ACCOUNT",
                    "id": "222222222222"
                }
            ],
            "action": "invite",
            "expirationTimestamp": "Feb 2, 2017 9:41:16 PM",
            "resources": [
                {
                    "resources": [
                        {
                            "type": "MASTER_EMAIL",
                            "value": "diego@example.com"
                        },
                        {
                            "type": "MASTER_NAME",
                            "value": "Management account for organization"
                        },
                        {
                            "type": "ORGANIZATION_FEATURE_SET",
                            "value": "ALL"
                        }
                    ],
                    "type": "ORGANIZATION",
                    "value": "o-aa111bb222"
                },
                {
                    "type": "ACCOUNT",
                    "value": "222222222222"
                },
                {
                    "type": "NOTES",
                    "value": "This is a request for Mary's account to join Diego's
 organization."
                }
            ]
        }
    },
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

Contoh entri log: AttachPolicy

Contoh berikut menunjukkan entri CloudTrail log untuk `AttachPolicy` panggilan sampel. Respons menunjukkan bahwa panggilan gagal karena jenis kebijakan yang diminta tidak diaktifkan di root di mana permintaan yang akan dilampirkan telah dicoba.

```
{
    "eventVersion": "1.06",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::111111111111:user/diego",
        "accountId": "111111111111",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "diego"
    },
    "eventTime": "2017-01-18T21:42:44Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "AttachPolicy",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36",
    "errorCode": "PolicyTypeNotEnabledException",
    "errorMessage": "The given policy type ServiceControlPolicy is not enabled on the
 current view",
    "requestParameters": {
        "policyId": "p-examplepolicyid111",
        "targetId": "ou-examplerootid111-exampleouid111"
    },
    "responseElements": null,
    "requestID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111111111111"
}
```

Amazon EventBridge

AWS Organizationsdapat bekerja dengan Amazon EventBridge, sebelumnya Amazon CloudWatch Events, untuk memunculkan peristiwa ketika tindakan yang ditentukan administrator terjadi dalam suatu organisasi. Sebagai contoh, karena sensitivitas tindakan tersebut, sebagian besar administrator

ingin diperingatkan setiap kali seseorang membuat akun baru dalam organisasi atau ketika administrator akun anggota mencoba untuk meninggalkan organisasi. Anda dapat mengonfigurasi EventBridge aturan yang mencari tindakan ini dan kemudian mengirim peristiwa yang dihasilkan ke target yang ditentukan administrator. Target dapat sebuah topik Amazon SNS yang email atau pesan teks merupakan pelanggannya. Anda juga dapat membuat fungsi AWS Lambda yang mencatat detail tindakan untuk Anda tinjau nanti.

Untuk tutorial yang menunjukkan cara mengaktifkan EventBridge untuk memantau aktivitas utama di organisasi Anda, lihatTutorial: Pantau perubahan penting pada organisasi Anda dengan Amazon EventBridge.

Untuk mempelajari selengkapnya EventBridge, termasuk cara mengonfigurasi dan mengaktifkannya, lihat Panduan EventBridge Pengguna Amazon.

Validasi kepatuhan untuk AWS Organizations

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan 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 AWS yang berfokus pada keamanan dan kepatuhan.
- Arsitektur untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi yang memenuhi syarat HIPAA.

> **Note**
>
> Tidak semua memenuhi Layanan AWS syarat HIPAA. Untuk informasi selengkapnya, lihat Referensi Layanan yang Memenuhi Syarat HIPAA.

- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan di AWS Organizations

Infrastruktur global AWS dibangun di sekitar Wilayah AWS dan Availability Zone. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi yang terhubung dengan jaringan latensi rendah, throughput tinggi, dan jaringan yang sangat berlebihan. Dengan Availability Zone, Anda dapat merancang dan mengoperasikan aplikasi dan basis data yang secara otomatis melakukan failover di antara Availability Zone tanpa gangguan. Availability Zone memiliki ketersediaan yang tinggi, toleran terhadap kesalahan, dan dapat diskalakan jika dibandingkan dengan infrastruktur pusat data tunggal atau ganda tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur Global AWS.

Keamanan infrastruktur dalam AWS Organizations

Sebagai layanan terkelola, AWS Organizations dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan AWS Cloud. Untuk merancang AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja Pilar Keamanan yang AWS Diarsiteksikan dengan Baik.

Anda menggunakan panggilan API AWS yang dipublikasikan untuk mengakses Organizations melalui jaringan. Klien harus mendukung hal berikut:

- Transport Layer Security (TLS). Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Suite cipher dengan kerahasiaan maju sempurna (PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan sistem yang lebih baru mendukung mode ini.

Selain itu, permintaan harus ditandatangani menggunakan access key ID dan secret access key yang terkait dengan principal IAM. Atau Anda bisa menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 ketika mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Untuk informasi lebih lanjut tentang titik akhir FIPS yang tersedia, lihat Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Referensi AWS Organizations

Gunakan topik pada bagian ini untuk menemukan materi referensi detail untuk berbagai aspek AWS Organizations.

Topik

Kuota untuk AWS Organizations

Bagian ini menentukan kuota yang mempengaruhi AWS Organizations.

Pedoman penamaan

Berikut ini adalah panduan untuk nama yang Anda buat AWS Organizations, termasuk nama akun, unit organisasi (OU), akar, dan kebijakan:

- Mereka harus terdiri dari karakter Unicode
- Panjang string maksimum untuk nama bervariasi berdasarkan objek. Untuk melihat batas aktual untuk masing-masing, lihat Referensi API AWS Organizations dan cari operasi API yang menciptakan objek. Lihat detail untuk parameter `Name`. Misalnya: Nama akun, atau Nama OU.

Nilai maksimum dan minimum

Berikut ini adalah maksimum default untuk entitas di AWS Organizations.

> **Note**
>
> Anda dapat meminta peningkatan untuk beberapa nilai ini dengan menggunakan konsol Service Quotas.
> Organizations adalah layanan global yang secara fisik di-host di Wilayah US East (N. Virginia) (`us-east-1`). Oleh karena itu, Anda harus menggunakan `us-east-1` untuk mengakses kuota Organizations saat menggunakan konsol Service Quotas, AWS CLI the, atau AWS SDK.

Jumlah Akun AWS dalam suatu organisasi	10 — Jumlah maksimum akun default yang diizinkan dalam suatu organisasi. Jika Anda membutuhkan lebih banyak, Anda dapat meminta peningkatan dengan menggunakan konsol Service Quotas. Undangan yang dikirim ke akun dihitung terhadap kuota ini. Hitungan tersebut dikembalikan jika akun yang diundang menolak, akun pengelolaan membatalkan undangan, atau undangan kedaluwarsa. Akun dan organisasi yang baru dibuat mungkin mengalami kuota di bawah default 10 akun.
Jumlah root dalam suatu organisasi	1
Jumlah OU dalam suatu organisasi	1000
Jumlah kebijakan dari setiap jenis dalam suatu organisasi	Kebijakan opt-out layanan AI: 1000 Kebijakan Backup: 1000 Kebijakan kontrol layanan: 2000 Kebijakan tag: 1000
Ukuran maksimum dokumen kebijakan	Kebijakan penolakan layanan AI: 2500 karakter Kebijakan Backup: 10.000 karakter Kebijakan kontrol layanan: 5120 karakter Kebijakan Tag: 10.000 karakter Catatan: Jika Anda menyimpan kebijakan menggunakan AWS Management Console, spasi putih ekstra (seperti spasi dan jeda baris) antara elemen JSON dan di luar tanda kutip, akan dihapus dan tidak dihitung. Jika Anda menyimpan kebijakan menggunakan operasi SDK atau operasi AWS CLI, kebijakan akan disimpan persis seperti yang Anda berikan dan tidak terjadi penghapusan karakter secara otomatis.

OU maksimum membuat nest dalam sebuah root	Lima tingkat OU jauh di bawah root.
Jumlah maksimum percobaan undangan yang dapat Anda lakukan dalam periode 24 jam	Baik 20 atau jumlah maksimum akun yang diizinkan yang ada di organisasi Anda, mana saja yang lebih besar. Undangan yang diterima tidak dihitung masuk dalam kuota ini. Segera setelah satu undangan diterima, Anda dapat mengirim undangan lain pada hari yang sama. Jika jumlah maksimum akun yang diizinkan yang ada di organisasi Anda kurang dari 20, maka Anda mendapatkan pengecualian "batas akun terlampaui" jika Anda mencoba mengundang lebih banyak akun daripada jumlah akun yang dapat ada dalam organisasi Anda. Namun, Anda dapat membatalkan undangan dan mengirim undangan baru hingga maksimal 20 kali dalam satu hari.
Jumlah akun anggota yang dapat Anda buat secara bersamaan	5 — Segera setelah satu selesai, Anda dapat memulai yang lain, tetapi hanya lima yang dapat berlangsung pada suatu waktu.
Jumlah akun anggota yang dapat Anda tutup dalam periode 30 hari	10% dari akun anggota dalam suatu organisasi, dengan maksimum 1000. • < 100 akun - Anda dapat menutup hingga 10 akun anggota • 100 - 10.000 akun - Anda dapat menutup hingga 10% dari akun anggota Anda • > 10.000 akun - Anda dapat menutup hingga 1000 akun anggota Misalnya, jika Anda memiliki 10.500 akun anggota, Anda dapat menutup hingga 1000 (bukan 1050) akun dalam periode 30 hari. Setelah Anda mencapai kuota ini, Anda dapat menutup akun tambahan di AWS Billing konsol atau menunggu hingga kuota Anda diatur ulang. Untuk informasi selengkapnya, lihat Apa yang perlu Anda ketahui sebelum menutup akun Anda di Panduan Manajemen AWS Akun.

Jumlah akun anggota yang dapat Anda tutup secara bersamaan	3 — Hanya tiga penutupan akun yang dapat berlangsung pada saat yang bersamaan. Segera setelah satu selesai, Anda dapat menutup akun lain.
Jumlah entitas yang dapat Anda lampiri dengan kebijakan	Tidak terbatas
Jumlah tag yang dapat Anda lampirkan ke root, OU, atau akun	50
Ukuran maksimum kebijakan delegasi berbasis sumber daya	40.000 karakter

Waktu kedaluwarsa untuk jabat tangan

Berikut ini adalah batas waktu untuk berjabat tangan. AWS Organizations

Undangan untuk bergabung dengan organisasi	15 hari
Meminta untuk mengaktifkan semua fitur dalam organisasi	90 hari
Jabat tangan dihapus dan tidak lagi muncul dalam daftar	30 hari setelah jabat tangan selesai

Jumlah kebijakan yang dapat dilampirkan ke sebuah entitas

Jumlah minimum dan maksimum-nya tergantung pada jenis kebijakan dan entitas hendak Anda lampiri kebijakan. Tabel berikut menunjukkan setiap jenis kebijakan dan jumlah entitas yang dapat Anda lampirkan untuk setiap jenisnya.

> **Note**
>
> Angka-angka ini berlaku untuk kebijakan yang secara langsung dilampirkan ke OU atau akun saja. Kebijakan yang mempengaruhi OU atau akun karena warisan tidak dihitung masuk dalam batas ini.

Tipe kebijakan	Jumlah minimum yang dilampirkan pada entitas	Jumlah maksimum yang dilampirkan ke root	Jumlah maksimum yang dilampirkan per OU	Jumlah maksimum yang dilampirkan per akun
Kebijakan kontrol layanan	1 — Setiap entitas harus memiliki paling tidak satu SCP terlampir setiap saat. Anda tidak dapat menghapus SCP terakhir dari sebuah entitas.	5	5	5
Kebijakan menolak layanan AI	0	5	5	5
Kebijakan Backup	0	10	10	10
kebijakan tag	0	10	10	10

> **Note**
>
> Saat ini, Anda hanya dapat memiliki satu root dalam sebuah organisasi.

Batas pelambatan

Tabel berikut mencantumkan AWS Organizations API menurut kategori manajemen, dan menunjukkan kecepatan throttle masing-masing di tingkat akun dan organisasi.

AWS Organizations API	Batas per akun (tingkat, burst)	Batas per organisasi (tingkat, burst)
Pengelolaan akun		
CloseAccount	.05, 1	
CreateAccount, CreateGovCloudAccount	0,1, 3	
DescribeAccount	20, 30	24, 36
DescribeCreateAccountStatus	2, 2	2, 3
LeaveOrganization	1, 1	
ListCreateAccountStatus	5, 8	6, 10
Manajemen jabat tangan		
AcceptHandshake, DescribeHandshake	1, 1	
CancelHandshake	2, 3	
DeclineHandshake	1, 3	
InviteAccountToOrganization	3, 5	
ListHandshakesForAccount, ListHandshakesForOrganization	5, 8	6, 10
Manajemen organisasi		

AWS Organizations API	Batas per akun (tingkat, burst)	Batas per organisasi (tingkat, burst)
CreateOrganization, DeleteOrganization, EnableFullControl	1, 1	
CreateOrganizationalUnit, DescribeOrganization	1, 2	
MoveAccount, UpdateOrganizationalUnit, DeleteOrganizationalUnit	2, 3	
DescribeOrganizationalUnit	2, 2	2, 3
ListAccounts	8, 12	9, 15
ListChildren	6, 10	7, 12
ListParents, ListAccountsForParent, ListOrganizationalUnitsForParent	5, 8	6, 10
ListRoots	1, 2	1, 3
ListTagsForResource	10, 15	12, 18
RemoveAccountFromOrganization	2, 2	
TagResource, UntagResource	4, 6	
Manajemen kebijakan		
CreatePolicy, DeletePolicy, AttachPolicy, DetachPolicy	2, 3	
DescribePolicy	2, 2	2, 3

AWS Organizations API	Batas per akun (tingkat, burst)	Batas per organisasi (tingkat, burst)
DisablePolicyType, EnablePolicyType	1, 1	
ListPolicies, ListPoliciesForTarget, ListTargetsForPolicy	5, 8	6, 10
UpdatePolicy	2, 3	
Manajemen layanan		
AktifkanAWSServiceAccess, Nonaktifkan AWSServiceAccess	1, 2	
DaftarAWSServiceAccessForOrganization, ListDelegatedServicesForAccount	1, 3	1, 4
ListDelegatedAdministrators	5, 8	6, 10
RegisterDelegatedAdministrator, DeregisterDelegatedAdministrator	1, 2	

Kebijakan terkelola AWS tersedia untuk digunakan dengan AWS Organizations

Bagian ini mengidentifikasi kebijakan terkelola AWS yang disediakan untuk Anda gunakan untuk mengelola organisasi Anda. Anda tidak dapat memodifikasi atau menghapus kebijakan terkelola AWS, namun Anda dapat melampirkan atau melepaskannya ke entitas yang ada di organisasi Anda jika diperlukan.

Kebijakan terkelola AWS Organizations untuk digunakan dengan AWS Identity and Access Management (IAM)

Kebijakan terkelola IAM disediakan dan dikelola oleh AWS. Kebijakan terkelola menyediakan izin untuk tugas umum yang dapat Anda tetapkan kepada pengguna dengan melampirkan kebijakan terkelola tersebut ke objek pengguna IAM atau peran yang sesuai. Anda tidak perlu menulis kebijakan sendiri, dan saat AWS memperbarui kebijakan yang sesuai untuk men-support layanan baru, Anda secara otomatis dan langsung mendapatkan manfaat dari pembaruan tersebut. Anda dapat melihat daftar kebijakan terkelola AWS di halaman Kebijakan pada konsol IAM. Gunakan drop-down Filter kebijakan untuk memilih terkelola AWS.

Anda dapat menggunakan kebijakan terkelola berikut ini untuk memberikan izin kepada pengguna yang ada di organisasi Anda.

Nama kebijakan	Deskripsi	ARN

AWSOrganizationsFullAccess	Menyediakan semua izin yang diperlukan untuk membuat dan sepenuhnya mengelola sebuah organisasi. Isi pernyataan kebijakan ini ditampilkan dalam cuplikan berikut: <pre>{
	    "Version": "2012-10-17",
	    "Statement": [
	        {
	            "Sid": "AWSOrganizationsFullAccess",
	            "Effect": "Allow",
	            "Action": "organizations:*",
	            "Resource": "*"
	        },
	        {
	            "Sid": "AWSOrganizationsFullAccessAccount",
	            "Effect": "Allow",
	            "Action": [</pre>
		arn:aws:iam: :aws:policy/AWSOrganizationsFullAccess

Nama kebijakan	Deskripsi	ARN

```
                "account:
PutAlternateContact",
                "account:
DeleteAlternateContact",
                "account:
GetAlternateContact",
                "account:
GetContactInformation",
                "account:
PutContactInformation",
                "account:
ListRegions",
                "account:
EnableRegion",
                "account:
DisableRegion"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AWSOrgan
izationsFullAccessCreateSLR
",
            "Effect": "Allow",
            "Action":
 "iam:CreateServiceLinkedRol
e",
            "Resource": "*",
            "Condition": {
                "StringEq
uals": {
                    "iam:AWSS
erviceName": "organiza
tions.amazonaws.com"
                }
            }
        }
    ]
}
```

Nama kebijakan	Deskripsi	ARN
AWSOrganizationsReadOnlyAccess	Menyediakan akses baca saja ke informasi tentang organisasi. Izin ini tidak mengizinkan pengguna untuk melakukan perubahan. Isi pernyataan kebijakan ini ditampilkan dalam cuplikan berikut: `{ "Version":"2012-10-17", "Statement":[{ "Sid": "AWSOrganizationsReadOnly", "Effect":"Allow", "Action":["organizations:Describe*", "organizations:List*"], "Resource": "*" }, { "Sid": "AWSOrganizationsReadOnlyAccount", "Effect":"Allow", "Action":["account:GetAlternateContact", "account:GetContactInformation", "account:ListRegions"], "Resource": "*" }] }`	arn:aws:iam: :aws:policy/AWSOrganizationsReadOnlyAccess

Pembaruan untuk Kebijakan terkelola AWS Organizations

Tabel berikut memberikan detail tentang pembaruan untuk kebijakan terkelola AWS sejak layanan ini mulai melacak perubahan-perubahan tersebut. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman Riwayat Dokumen AWS Organizations.

Perubahan	Deskripsi	Tanggal
AWSOrganizationsFullAccess— diperbarui untuk memasukkan `Sid` elemen yang menggambarkan pernyataan kebijakan.	Organizations menambahkan `Sid` elemen untuk kebijakan yang `AWSOrganizationsFullAccess` dikelola.	Februari 6, 2024
AWSOrganizationsReadOnlyAccess— diperbarui untuk memasukkan `Sid` elemen yang menggambarkan pernyataan kebijakan.	Organizations menambahkan `Sid` elemen untuk kebijakan yang `AWSOrganizationsReadOnlyAccess` dikelola.	Februari 6, 2024
AWSOrganizationsFullAccess— diperbarui untuk memungkinkan izin API akun yang diperlukan untuk mengaktifkan atau menonaktifkan Wilayah AWS melalui konsol Organizations.	Organizations menambahkan `account:ListRegions`, `account:EnableRegion` dan `account:DisableRegion` tindakan ke kebijakan untuk mengaktifkan akses tulis guna mengaktifkan atau menonaktifkan Wilayah untuk akun.	22 Desember 2022
AWSOrganizationsReadOnlyAccess— diperbarui untuk memungkinkan izin API akun yang diperlukan untuk mendaftar Wilayah AWS melalui konsol Organizations.	Organizations menambahkan `account:ListRegions` tindakan ke kebijakan untuk mengaktifkan akses untuk melihat Wilayah untuk akun.	22 Desember 2022
AWSOrganizationsFullAccess— diperbarui untuk memungkinkan izin API akun yang diperlukan untuk menambah atau mengedit kontak akun melalui konsol Organizations.	Organizations menambahkan `account:PutContactInformation` tindakan `account:GetContactInformation` dan ke kebijakan	22 Oktober 2022

Perubahan	Deskripsi	Tanggal
	untuk mengaktifkan akses tulis untuk mengubah kontak untuk akun.	
AWSOrganizationsReadOnlyAccess— diperbarui untuk memungkinkan izin API akun yang diperlukan untuk melihat kontak akun melalui konsol Organizations.	Organizations menambahkan `account:GetContactInformation` tindakan ke kebijakan untuk mengaktifkan akses untuk melihat kontak untuk akun.	22 Oktober 2022
AWSOrganizationsFullAccess— diperbarui untuk memungkinkan pembuatan organisasi.	Organizations menambahkan izin `CreateServiceLinkedRole` ke kebijakan untuk mengaktifkan pembuatan peran terkait layanan yang diperlukan untuk membuat organisasi. Izin ini dibatasi untuk menciptakan peran yang dapat digunakan oleh layanan `organizations.amazonaws.com` saja.	Agustus 24, 2022
AWSOrganizationsFullAccess— diperbarui untuk memungkinkan izin API akun yang diperlukan untuk menambah, mengedit, atau menghapus kontak alternatif akun melalui konsol Organizations.	Organizations menambahkan `account:GetAlternateContact` `account:DeleteAlternateContact` ,, `account:PutAlternateContact` tindakan ke kebijakan untuk mengaktifkan akses tulis untuk mengubah kontak alternatif untuk akun.	Februari 7, 2022
AWSOrganizationsReadOnlyAccess— diperbarui untuk memungkinkan izin API akun yang diperlukan untuk melihat kontak alternatif akun melalui konsol Organizations.	Organizations menambahkan `account:GetAlternateContact` tindakan ke kebijakan untuk mengaktifkan akses untuk melihat kontak alternatif untuk akun.	Februari 7, 2022

Kebijakan kontrol layanan terkelola AWS Organizations

Kebijakan Kontrol Layanan (SCP) mirip dengan kebijakan izin IAM, tetapi merupakan fitur dari AWS Organizations, bukan fitur dari IAM. Anda menggunakan SCP untuk menentukan izin maksimum untuk entitas yang terpengaruh. Anda dapat melampirkan SCP ke root, unit organisasi (UO), atau akun-akun yang ada di organisasi Anda. Anda dapat membuat kebijakan Anda sendiri, atau Anda dapat menggunakan kebijakan yang ditetapkan IAM. Anda dapat melihat daftar kebijakan di organisasi Anda di halaman Kebijakan di konsol Organizations.

> **Important**
>
> Setiap root, OU, dan akun harus memiliki setidaknya satu SCP terlampir setiap saat.

Nama kebijakan	Deskripsi	ARN
Penuh AWSAccess	Menyediakan akses akun pengelolaan AWS Organizations ke akun anggota.	arn:aws:organisasi: :aws:policy/service_control_policy/p-full AWSAccess

Pemecahan masalah AWS Organizations

Jika Anda mengalami masalah saat bekerja dengan AWS Organizations, konsultasikan topik tersebut di bagian ini.

Topik

Memecahkan masalah umum

Gunakan informasi di sini untuk membantu Anda mendiagnosis dan memperbaiki masalah akses ditolak dan masalah umum lainnya yang mungkin Anda temui saat bekerja dengan AWS Organizations.

Topik

Saya mendapatkan pesan "akses ditolak" ketika saya mengajukan permintaan ke AWS Organizations

- Pastikan bahwa Anda memiliki izin untuk memanggil tindakan dan sumber daya yang Anda minta. Administrator harus memberikan izin dengan melampirkan kebijakan IAM ke pengguna, grup, grup, atau peran IAM Anda. Jika pernyataan kebijakan yang memberikan izin tersebut menyertakan syarat apapun, seperti time-of-day atau batasan alamat IP, maka Anda juga harus memenuhi persyaratan tersebut ketika Anda mengirim permintaan. Untuk informasi tentang melihat atau mengubah kebijakan untuk pengguna, grup, atau peran IAM, lihat Bekerja dengan Kebijakan dalam Panduan Pengguna IAM.
- Jika Anda menandatangani permintaan API secara manual (tanpa menggunakan AWS SDK), verifikasi bahwa Anda telah menandatangani permintaan dengan benar.

Saya mendapatkan pesan "akses ditolak" ketika saya membuat permintaan dengan kredensial keamanan sementara

- Verifikasi bahwa pengguna atau peran yang Anda gunakan untuk membuat permintaan memiliki izin yang benar. Izin untuk kredensia keamanan sementara berasal dari pengguna atau peran keamanan sementara berasal dari pengguna atau peran sementara. Untuk informasi lebih lanjut tentang bagaiman izin kredensial keamanan sementara ditentukan, lihat Mengontrol Izin untuk Kredensial Keamanan Sementara dalam Panduan Pengguna IAM.
- Verifikasi bahwa permintaan Anda ditandatangani dengan benar dan bahwa permintaan tersebut memiliki bentuk yang baik. Untuk detailnya, lihat dokumentasi toolkit untuk SDK pilihan Anda atau Menggunakan Kredensial Keamanan Sementara untuk Meminta Akses ke Sumber Daya AWS dalam Panduan Pengguna IAM.
- Verifikasikan bahwa kredensial keamanan sementara Anda belum kedaluwarsa. Untuk informasi lebih lanjut, lihat Meminta Kredensial Keamanan Sementara dalam Panduan Pengguna IAM.

Saya mendapatkan pesan "akses ditolak" saat mencoba meninggalkan organisasi sebagai akun anggota atau menghapus akun anggota sebagai akun pengelolaan

- Anda dapat menghapus akun anggota hanya setelah Anda mengaktifkan akses pengguna IAM untuk penagihan di akun anggota. Untuk informasi lebih lanjut, lihat Mengaktifkan Akses ke Konsol Manajemen Penagihan dan Biaya dalam Panduan Pengguna AWS Billing.
- Anda dapat menghapus akun dari organisasi Anda hanya jika akun tersebut memiliki informasi yang diperlukan untuk beroperasi sebagai akun mandiri. Saat Anda membuat akun di sebuah organisasi menggunakan konsol AWS Organizations, API, atau perintah AWS CLI, informasi tersebut tidak dikumpulkan secara otomatis. Untuk akun yang ingin Anda mandiri, Anda harus menerima Perjanjian Pelanggan AWS, pilih paket support, berikan dan verifikasi informasi kontak yang diperlukan, dan berikan metode pembayaran saat ini. AWS menggunakan metode pembayaran untuk mengenakan biaya untuk setiap aktivitas AWS yang bisa ditagih (bukan Tingkat Gratis AWS) yang terjadi saat akun tidak dilampirkan ke organisasi. Untuk informasi lebih lanjut, lihat Tinggalkan organisasi dari akun anggota Anda.

Saya menerima pesan "kuota terlampaui" saat mencoba menambahkan akun ke organisasi saya

Ada jumlah akun maksimum yang dapat Anda miliki dalam sebuah organisasi. Akun yang dihapus atau ditutup akan tetap dihitung terhadap kuota ini.

Undangan untuk bergabung dihitung terhadap jumlah maksimum akun yang ada di organisasi Anda. Hitungan tersebut dikembalikan jika akun yang diundang menolak, akun pengelolaan membatalkan undangan, atau undangan kedaluwarsa.

- Sebelum Anda menutup atau menghapus Akun AWS, hapus ia dari organisasi Anda sehingga tidak terus dihitung terhadap kuota Anda.
- Lihat Nilai maksimum dan minimum untuk informasi lebih lanjut tentang cara meminta kenaikan kuota.

Saya mendapatkan pesan "operasi ini memerlukan waktu tunggu" saat menambahkan atau menghapus akun

Beberapa tindakan membutuhkan waktu tunggu. Misalnya, Anda tidak dapat langsung menghapus akun yang baru dibuat. Coba tindakan itu lagi dalam beberapa hari. Jika Anda mengalami masalah dengan kuota akun saat menambahkan dan menghapus akun, lihat Nilai maksimum dan minimum untuk informasi tentang cara meminta kenaikan kuota.

Saya mendapatkan pesan "organisasi masih menginisialisasi" saat mencoba menambahkan akun ke organisasi saya

Jika Anda menerima kesalahan ini dan sudah lebih dari satu jam sejak Anda membuat organisasi, kontak AWS Support.

Saya menerima pesan "Undangan dinonaktifkan" saat mencoba mengundang akun ke organisasi saya.

Hal ini terjadi ketika Anda mengaktifkan semua fitur di organisasi Anda. Operasi ini dapat memakan waktu lama dan mengharuskan semua akun anggota merespons. Hingga operasi tersebut selesai, Anda tidak dapat mengundang akun baru untuk bergabung dengan organisasi.

Perubahan yang saya buat tidak selalu langsung bisa terlihat

Sebagai layanan yang diakses melalui komputer di pusat data di seluruh dunia, AWS Organizations menggunakan model komputasi terdistribusi yang disebut eventual consistency. Setiap perubahan yang Anda lakukan di AWS Organizations membutuhkan waktu agar bisa terlihat dari semua titik akhir yang memungkinkan. Beberapa penundaan diakibatkan karena waktu yang diperlukan untuk mengirim data dari server ke server atau dari zona replikasi ke zona replikasi. AWS Organizations juga menggunakan caching untuk meningkatkan performa, tetapi dalam beberapa kasus, hal ini dapat memerlukan tambahan waktu. Perubahan mungkin tidak terlihat sampai waktu data yang disimpan di-cache sebelumnya habis.

Rancang aplikasi global Anda untuk memperhitungkan potensi penundaan ini dan pastikan aplikasi bekerja sesuai harapan Anda, bahkan ketika perubahan yang dilakukan di satu lokasi tidak secara langsung bisa terlihat di lokasi lain.

Untuk informasi lebih lanjut tentang bagaimana beberapa layanan AWS lainnya dipengaruhi oleh hal ini, pelajari sumber daya berikut:

- Mengelola Konsistensi Data di Panduan Developer Basis Data Amazon Redshift
- Model Konsistensi Data Amazon S3 di Panduan Pengguna Amazon Simple Storage Service
- Memastikan Konsistensi Saat Menggunakan Amazon S3 dan Amazon Elastic MapReduce untuk Alur Kerja ETL di BlogAWS Big Data
- EC2 Eventual Consistency di Referensi API Amazon EC2.

Memecahkan masalah kebijakan AWS Organizations

Gunakan informasi di sini untuk membantu Anda mendiagnosis dan memperbaiki kesalahan umum yang ditemukan di kebijakan AWS Organizations.

Kebijakan kontrol layanan

Kebijakan Kontrol Layanan (SCP) di AWS Organizations mirip dengan kebijakan IAM dan berbagi sintaksis umum. Sintaks ini dimulai dengan aturan JavaScript Object Notation (JSON). JSON menggambarkan objek dengan nama dan nilai pasangan yang membentuk objek tersebut. Tata bahasa kebijakan IAM dibangun di atas landasan bahwa dengan menentukan nama dan nilai-nilai yang memiliki arti untuk, dan dipahami oleh, layanan AWS yang menggunakan kebijakan untuk memberikan izin.

AWS Organizations menggunakan subset dari sintaksis dan tata bahasa IAM. Untuk detailnya, lihat Sintaksis SCP.

Kesalahan kebijakan umum

- Lebih dari satu objek kebijakan
- Lebih dari satu elemen pernyataan
- Dokumen kebijakan melebihi ukuran maksimum

Lebih dari satu objek kebijakan

SCP harus terdiri dari satu dan hanya satu objek JSON. Anda menunjukkan sebuah objek dengan menempatkan rungkup { } di sekitarnya. Meskipun Anda dapat membuatkan nest untuk objek lain di dalam objek JSON dengan menyematkan rungkup { } tambahan di dalam pasangan bagian luar, kebijakan hanya dapat berisi satu pasang rungkup { } terluar. Contoh berikut ini salah karena berisi dua objek di tingkat atas (dipanggill dalam warna *merah*):

```
{
```

```
  "Version": "2012-10-17",
  "Statement":
  {
     "Effect":"Allow",
     "Action":"ec2:Describe*",
     "Resource":"*"
  }
}
{
  "Statement": {
     "Effect": "Deny",
     "Action": "s3:*",
     "Resource": "*"
  }
}
```

Namun demikian, Anda dapat memenuhi maksud dari contoh sebelumnya dengan menggunakan tata bahasa kebijakan yang benar. Alih-alih memasukkan dua objek kebijakan lengkap, masing-masing dengan elemen `Statement` sendiri, Anda dapat menggabungkan kedua blok menjadi satu elemen `Statement`. Elemen `Statement` memiliki susunan dua objek sebagai nilainya, seperti yang ditunjukkan dalam contoh berikut:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource":" *"
    },
    {
      "Effect": "Deny",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

Contoh ini tidak dapat dikompresi lebih lanjut menjadi sebuah `Statement` dengan satu elemen karena kedua elemen memiliki efek yang berbeda. Umumnya, Anda dapat menggabungkan pernyataan hanya ketika elemen `Effect` dan `Resource` dalam setiap pernyataan identik.

Lebih dari satu elemen pernyataan

Kesalahan ini pada awalnya mungkin tampak seperti variasi pada kesalahan di bagian sebelumnya. Namun demikian, secara sintaksis ini adalah jenis kesalahan yang berbeda. Dalam contoh berikut, hanya ada satu objek kebijakan yang ditandai dengan sepasang rungkup { } di tingkat atas. Namun, objek tersebut berisi dua elemen `Statement` di dalamnya.

SCP harus berisi hanya satu elemen `Statement`, yang terdiri atas nama (`Statement`) yang muncul di sebelah kiri titik dua, diikuti dengan nilainya di sebelah kanan. Nilai dari elemen `Statement` harus berupa objek, yang ditandai dengan rungkup { }, yang berisi satu elemen `Effect`, satu elemen `Action`, dan satu elemen `Resource`. Contoh berikut ini salah karena berisi dua elemen `Statement` dalam objek kebijakan:

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "ec2:Describe*",
    "Resource": "*"
  },
  "Statement": {
    "Effect": "Deny",
    "Action": "s3:*",
    "Resource": "*"
  }
}
```

Karena objek nilai dapat berupa array berbagai objek nilai, maka Anda dapat memecahkan masalah ini dengan menggabungkan kedua elemen `Statement` ke dalam satu elemen dengan objek array, seperti ditunjukkan dalam contoh berikut:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource":"*"
    },
    {
      "Effect": "Deny",
```

```
      "Action": "s3:*",
      "Resource": "*"
    }
 ]
}
```

Nilai dari elemen `Statement` merupakan himpunan objek. Array dalam contoh ini terdiri dari dua objek, yang masing-masing merupakan nilai yang benar untuk elemen `Statement`. Setiap objek di himpunan dipisahkan dengan koma.

Dokumen kebijakan melebihi ukuran maksimum

Ukuran maksimum dokumen SCP adalah 5.120 karakter. Ukuran maksimum ini mencakup semua karakter, termasuk spasi kosong. Untuk mengurangi ukuran SCP Anda, Anda dapat menghapus semua karakter spasi kosong (seperti spasi dan baris putus) yang berada di luar tanda kutip.

Memanggil API dengan membuat permintaan Kueri HTTP

Bagian ini berisi informasi umum tentang menggunakan Kueri API untuk AWS Organizations. Untuk detail tentang operasi API dan kesalahan, lihat Referensi API AWS Organizations.

> **Note**
>
> Alih-alih membuat panggilan langsung ke API Kueri AWS Organizations, Anda dapat menggunakan salah satu SDK AWS. SDK AWS terdiri atas perpustakaan dan kode sampel untuk berbagai bahasa dan platform pemrograman (Java, Ruby, .NET, iOS, Android, dan banyak lagi). SDK menyediakan sebuah cara yang nyaman untuk membuat akses terprogram ke AWS Organizations dan AWS. Misalnya, SDK menangani tugas seperti menandatangani permintaan secara kriptografis, mengelola kesalahan, dan mencoba kembali permintaan secara otomatis. Untuk informasi tentang AWS SDK, termasuk cara mengunduh dan menginstalnya, lihat Alat untuk Amazon Web Services.

API Kueri untuk AWS Organizations memungkinkan Anda melakukan tindakan-tindakan layanan. Permintaan API Kueri adalah permintaan HTTPS yang harus berisi parameter `Action` untuk menunjukkan operasi yang akan dilakukan. AWS Organizations men-support permintaan GET dan POST untuk semua operasi. Artinya, API tidak mewajibkan Anda menggunakan GET untuk beberapa tindakan dan POST untuk yang lainnya. Namun, permintaan GET harus memenuhi ukuran batas dari sebuah URL. Meskipun batas ini bergantung pada peramban, batas umumnya adalah 2048 byte. Oleh karena itu, untuk permintaan API Kueri yang memerlukan ukuran lebih besar, Anda harus menggunakan permintaan POST.

Responsnya adalah dokumen XML. Untuk detail tentang respons, lihat halaman masing-masing tindakan di Referensi API AWS Organizations.

Topik

Titik akhir

AWS Organizations memiliki titik akhir API global tunggal yang di-host di Wilayah US East (N. Virginia).

Untuk informasi selengkapnya tentang AWS titik akhir dan wilayah untuk semua layanan, lihat Titik akhir Regional di. Referensi Umum AWS

HTTPS diperlukan

Karena API Kueri mengembalikan informasi sensitif seperti kredensial keamanan, Anda harus menggunakan HTTPS untuk mengenkripsi semua permintaan API.

Menandatangani permintaan API AWS Organizations

Permintaan harus ditandatangani menggunakan access key ID dan secret access key. Kami sangat menyarankan agar Anda tidak menggunakan Pengguna root akun AWS kredensi Anda untuk pekerjaan sehari-hari. AWS Organizations Anda dapat menggunakan kredensialnya untuk pengguna atau peran.

Untuk menandatangani permintaan API Anda, Anda harus menggunakan Tanda Tangan Versi 4 AWS. Untuk selengkapnya tentang penggunaan Tanda Tangan Versi 4, lihat Menandatangani permintaan AWS API di Panduan Pengguna IAM.

AWS Organizations tidak men-support versi sebelumnya, seperti Tanda Tangan Versi 2.

Untuk informasi selengkapnya, lihat hal berikut:

- AWSSecurity Credentials — Memberikan informasi umum tentang jenis kredensial yang dapat Anda gunakan untuk mengakses. AWS
- Praktik terbaik keamanan di IAM — Menawarkan saran untuk menggunakan layanan IAM untuk membantu mengamankan AWS sumber daya Anda, termasuk yang ada di. AWS Organizations
- Kredensial keamanan sementara di IAM — Menjelaskan cara membuat dan menggunakan kredenal keamanan sementara.

Riwayat dokumen untuk AWS Organizations

Tabel berikut menjelaskan pembaruan dokumentasi utama untuk AWS Organizations.

- Versi API: 2016-11-28

Perubahan	Deskripsi	Tanggal
Pernyataan kebijakan yang diperbarui	Menambahkan `Sid` elemen baru ke pernyataan kebijakan AWS Organizations terkelola.	Februari 6, 2024
Topik akun manajemen tutup baru	Menambahkan tautan ke pertimbangan dan langkah-langkah terperinci yang berjalan melalui cara menutup akun manajemen.	Februari 1, 2024
Praktik terbaik yang diperbarui	Menambahkan informasi baru ke bagian praktik terbaik untuk membantu menyelaraskan dengan praktik terbaik IAM.	12 Juni 2023
Memperbarui AWSOrganizationsFullAccess dan AWSOrganizationsReadOnlyAccess mengelola kebijakan	Kedua kebijakan terkelola diperbarui untuk mengaktifkan akses tulis atau baca ke kontak untuk akun.	22 Oktober 2022
Memperbarui kebijakan AWSOrganizationsFullAccess terkelola	Kebijakan terkelola diperbarui untuk memungkinkan pembuatan organisasi dengan menambahkan izin yang diperlukan untuk membuat peran tertaut layanan yang dibutuhkan oleh organisasi baru.	Agustus 24, 2022

Organizations menutup kemampuan akun dari AWS Organizations konsol	Prinsipal di akun manajemen dapat menutup akun anggota dari AWS Organizations konsol, dan melindungi akun anggota dari penutupan yang tidak disengaja dengan menggunakan kebijakan IAM.	29 Maret 2022
Pengumuman yang diperbarui untuk memperbarui kontak alternatif dengan AWS Organizations konsol	Organizations sekarang menyediakan kemampuan untuk memperbarui kontak alternatif untuk akun dalam organisasi Anda menggunakan AWS Organizations konsol. Umumkan kemampuan baru dan arahkan ke Referensi Manajemen Akun untuk instruksi.	8 Februari 2022
Organizations managed policy updates - Update ke kebijakan yang sudah ada	Memperbarui AWSOrganizationsFullAccess dan AWSOrganizationsReadOnlyAccess mengelola kebijakan untuk mengizinkan izin API akun yang diperlukan untuk memperbarui atau melihat kontak alternatif akun melalui AWS Organizations konsol.	Februari 7, 2022
Integrasi Organisasi dengan Amazon DevOps Guru	Anda dapat menginteg rasikan Amazon DevOps Guru AWS Organizations untuk memantau kesehatan aplikasi secara holistik di semua akun organisasi Anda dan mendapatkan wawasan.	Januari 3, 2022

Integrasi Organisasi dengan Amazon Detective	Anda dapat menginteg rasikan Amazon Detective AWS Organizations untuk memastikan bahwa grafik perilaku Detektif Anda memberikan visibilitas ke dalam aktivitas untuk semua akun organisasi Anda.	Desember 16, 2021
Integrasi Organizations dengan AWS Config sekarang mendukung agregasi data multi-wilayah multi-akun.	Anda dapat menggunak an akun administrator yang didelegasikan untuk mengumpulkan data konfigura si dan kepatuhan sumber daya dari semua akun anggota dalam organisasi Anda. Untuk informasi selengkapnya, lihat Agregasi data multi-wil ayah multi-akundi Panduan Developer AWS Config.	16 Juni 2021
Integrasi Organizations dengan AWS Firewall Manager now mencakup dukungan untuk administrator yang didelegasikan	Sekarang Anda dapat menetapkan akun anggota di organisasi Anda untuk menjadi administrator Firewall Manager untuk seluruh organisasi. Hal ini memungkinkan pemisahan izin yang lebih baik dari akun pengelolaan organisasi.	30 April 2021
Kebijakan cadangan Organizat ions sekarang mendukung pencadangan berkelanjutan	Anda dapat menggunakan fitur backup berkelanjutan AWS Backup dengan kebijakan backup organisasi Anda.	10 Maret 2021

Integrasi Organizations dengan AWS CloudFormation StackSets now mencakup dukungan untuk administrator yang didelegasikan	Anda sekarang dapat menunjuk akun anggota di organisasi Anda untuk menjadi AWS CloudFormation StackSets administrator untuk seluruh organisasi. Hal ini memungkinkan pemisahan izin yang lebih baik dari akun pengelolaan organisasi.	18 Februari 2021
Lanjutkan mengundang akun saat Anda mengaktifkan semua fitur	AWS telah memperbarui proses untuk mengaktifkan semua fitur dalam organisasi. Sekarang Anda dapat terus mengundang akun baru untuk bergabung dengan organisasi Anda saat menunggu akun yang ada merespons undangan mereka.	3 Februari 2021
Memperkenalkan konsol versi 2.0 AWS Organizations	AWS memperkenalkan konsol AWS versi baru. Semua dokumentasi telah diperbarui untuk mencerminkan cara baru melakukan tugas.	21 Januari 2021
Organizations sekarang mendukung integrasi dengan AWS Marketplace	Sekarang Anda dapat mengaktifkan AWS Marketplace untuk lebih mudah berbagi lisensi perangkat lunak Anda di semua akun di organisasi Anda.	3 Desember 2020

Organizations sekarang mendukung integrasi dengan Amazon S3 Lens	Amazon S3 Lens men-support akses terpercaya dan administrator didelegasikan dengan Organizations. Untuk detailnya, lihat Lensa Penyimpanan Amazon S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.	18 November 2020
Salinan cadangan lintas akun	Bila menggunakan kebijakan backup untuk mencadangkan sumber daya di organisasi Anda, sekarang Anda dapat menyimpan salinan backup di Akun AWS dalam organisasi tersebut.	18 November 2020
Wilayah AWSdi China sekarang mendukung AWS Resource Access Manager sebagai layanan terpercaya Organizations	Sekarang Anda dapat menggunakan AWS RAM yang terintegrasi dengan Organizations sebagai layanan tepercaya saat Anda menggunakan Organizations dan AWS RAM di Cina.	18 November 2020
Organizations sekarang mendukung integrasi dengan AWS Security Hub	Anda dapat mengaktifkan Security Hub di semua akun yang ada di organisasi Anda, dan menetapkan salah satu akun anggota organisasi Anda sebagai akun administrator yang didelegasikan untuk Security Hub.	12 November 2020

Mengganti nama akun master	AWS Organizations telah mengubah nama dari “akun utama” menjadi “akun pengelolaan”. Ini hanya pembaruan nama, tidak ada perubahan dalam fungsiona litas.	20 Oktober 2020
Bagian dan topik Praktik Terbaik Baru	Menambahkan bagian baru untuk praktik terbaik untuk AWS Organizations. Bagian baru mencakup topik yang membahas praktik terbaik untuk akun pengelolaan dan pengguna akar akun anggota dan pengelolaan kata sandi.	6 Oktober 2020
Ditambahkan bagian praktik terbaik baru dan dua halaman pertama	Ada bagian baru untuk topik yang menjelaskan praktik terbaik untuk AWS Organizat ions. Pembaruan ini mencakup topik untuk praktik terbaik untuk akun pengelolaan organisasi dan topik untuk praktik terbaik untuk akun anggota.	2 Oktober 2020

Kebijakan pencadangan Organizations sekarang mendukung pencadangan yang konsisten aplikasi pada instans Windows EC2 dengan menggunakan VSS (Volume Shadow Copy Service)	Kebijakan Backup men-support bagian `advanced_backup_settings` " baru. Entri pertama di bagian baru ini adalah pengaturan `ec2` yang disebut `WindowsVSS` yang dapat Anda aktifkan atau nonaktifkan. Untuk detailnya , lihat Membuat Backup Windows Diaktifkan-VSS di Panduan Developer AWS Backup.	24 September 2020
Organizations mendukung tag-on-create dan kontrol akses berbasis tag	Anda dapat menambahkan tag ke sumber daya Organizations saat Anda membuatnya. Anda dapat menggunakan kebijakan tag untuk menstandardisasi penggunaan tag pada sumber daya Organizations. Anda dapat menggunakan Kebijakan IAM untuk membatasi akses hanya ke sumber daya yang telah menetapkan kunci dan nilai tag saja.	15 September 2020
Ditambahkan AWS Health sebagai layanan terpercaya	Anda dapat mengumpulkan peristiwa AWS Health di seluruh akun di organisasi Anda.	4 Agustus 2020

Kebijakan opt-out layanan Artificial Intelligence (AI)	Anda dapat menggunakan kebijakan berhenti berlangga nan layanan AI untuk mengontrol apakah layanan AI AWS dapat menyimpan dan menggunakan konten pelanggan yang diproses oleh layanan tersebut (konten AI) untuk pengembangan dan perbaikan berkelanjutan layanan dan teknologi AI AWS.	8 Juli 2020
Menambahkan kebijakan cadangan dan integrasi dengan AWS Backup	Anda dapat menggunak an kebijakan backup untuk membuat dan menerapkan kebijakan backup di semua akun di organisasi Anda.	24 Juni 2020
Support administrasi yang didelegasikan untuk IAM Access Analyzer	Memungkinkan Anda untuk mendelegasikan akses administratif untuk Access Analyzer di organisasi Anda untuk akun anggota yang ditunjuk.	30 Maret 2020
Integrasi dengan AWS CloudFormation StackSets	Anda dapat membuat tumpukan terkelola layanan untuk men-deploy instans tumpukan ke akun yang dikelola oleh AWS Organizat ions.	11 Februari 2020
Integrasi dengan Compute Optimizer	Compute Optimizer ditambahk an sebagai layanan yang dapat bekerja dengan akun di organisasi Anda.	4 Februari 2020

Kebijakan tag	Anda dapat menggunakan kebijakan tag untuk membantu menstandardisasi tag di seluruh sumber daya di akun organisasi Anda.	26 November 2019
Integrasi dengan Systems Manager	Anda dapat menyinkronkan data operasi di semua Akun AWS di organisasi Anda di Penjelajah Systems Manager .	26 November 2019
aws: PrincipalOrgPaths	Kunci syarat global baru memeriksa path AWS Organizations untuk pengguna IAM, IAM role, atau pengguna akar Akun AWS yang membuat permintaan.	20 November 2019
Integrasi dengan AWS Config aturan	Anda dapat menggunakan operasi API AWS Config untuk mengelola aturan AWS Config di semua Akun AWS di organisasi Anda.	8 Juli 2019
Layanan baru untuk akses tepercaya	Service Quotas ditambahkan sebagai layanan yang dapat bekerja dengan akun di organisasi Anda.	24 Juni 2019
Integrasi dengan AWS Control Tower	AWS Control Tower ditambahkan sebagai layanan yang dapat bekerja dengan akun di organisasi Anda.	24 Juni 2019

Integrasi dengan AWS Identity and Access Management	IAM menyediakan data layanan terakhir diakses untuk entitas organisasi Anda (akar organisasi, OU, dan akun). Anda dapat menggunakan data ini untuk membatasi akses hanya ke layanan AWS yang Anda butuhkan.	20 Juni 2019
Menandai akun	Anda dapat memberi tag dan melepaskan tag akun di organisasi Anda dan melihat tag pada akun di organisasi Anda.	6 Juni 2019
Sumber daya, kondisi, dan `NotAction` elemen dalam kebijakan kontrol layanan (SCP)	Anda sekarang dapat menentukan sumber daya, kondisi, dan elemen `NotAction` di SCP untuk menolak akses di seluruh akun di organisasi atau unit organisasi (OU) Anda.	25 Maret 2019
Layanan baru untuk akses tepercaya	AWS License Managerdan Service Catalog ditambahkan sebagai layanan yang dapat bekerja dengan akun di organisasi Anda.	21 Desember 2018
Layanan baru untuk akses tepercaya	AWS CloudTrail dan AWS RAM ditambahkan sebagai layanan yang dapat bekerja dengan akun di organisasi Anda.	4 Desember 2018

Layanan baru untuk akses tepercaya	AWS Directory Service ditambahkan sebagai layanan yang dapat berfungsi dengan akun di organisasi Anda.	25 September 2018
Verifikasi alamat email	Anda harus memverifikasi bahwa Anda memiliki alamat email yang dikaitkan dengan akun pengelolaan sebelum Anda dapat mengundang akun yang ada ke organisasi Anda.	20 September 2018
CreateAccount pemberitahuan	`CreateAccount` pemberitahuan dipublikasikan ke CloudTrail log akun manajemen.	28 Juni 2018
Layanan baru untuk akses tepercaya	AWS Artifact ditambahkan sebagai layanan yang dapat berfungsi dengan akun di organisasi Anda.	20 Juni 2018
Layanan baru untuk akses tepercaya	AWS Config dan AWS Firewall Manager ditambahkan sebagai layanan yang dapat bekerja dengan akun di organisasi Anda.	18 April 2018
Akses layanan tepercaya	Anda sekarang dapat mengaktifkan atau menonaktifkan akses untuk AWS layanan tertentu agar berfungsi di akun di organisasi Anda. IAM Identity Center adalah layanan terpercaya awal yang didukung.	29 Maret 2018

Penghapusan akun sekarang layanan mandiri	Sekarang Anda dapat menghapus akun yang dibuat dari dalam AWS Organizations tanpa menghubungi AWS Support.	19 Desember 2017
Menambahkan dukungan untuk layanan baru AWS IAM Identity Center	AWS Organizationssekarang mendukung integrasi dengan AWS IAM Identity Center (IAM Identity Center).	7 Desember 2017
AWSmenambahkan peran terkait layanan ke semua akun organisasi	Peran yang terhubung dengan layanan bernama `AWSServiceRoleForOrganizations` ditambahkan ke semua akun di sebuah organisasi untuk memungkinkan integrasi antara AWS Organizations dan layanan AWS lainnya.	11 Oktober 2017
Anda sekarang dapat menghapus akun yang dibuat	Pelanggan sekarang dapat menghapus akun yang dibuat dari organisasi mereka, dengan bantuan dari AWS Support.	15 Juni 2017
Peluncuran layanan	Versi awal dari dokumentasi AWS Organizations yang menyertai peluncuran layanan baru.	17 Februari 2017

AWSGlosarium

Untuk AWS terminologi terbaru, lihat AWSglosarium di Referensi. Glosarium AWS

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.