Panduan Pengguna

AWS IAM Identity Center

AWS IAM Identity Center: Panduan Pengguna

Table of Contents

Apa itu Pusat Identitas IAM?

AWS IAM Identity Center adalah direkomendasikan Layanan AWS untuk mengelola akses pengguna manusia ke AWS sumber daya. Ini adalah satu tempat di mana Anda dapat menetapkan pengguna tenaga kerja Anda, juga dikenal sebagaiworkforce identities, akses konsisten ke beberapa Akun AWS dan aplikasi. Pusat Identitas IAM ditawarkan tanpa biaya tambahan.

Dengan IAM Identity Center, Anda dapat membuat atau menghubungkan pengguna tenaga kerja dan mengelola akses mereka secara terpusat di semua aplikasi dan aplikasi mereka Akun AWS . Anda dapat menggunakan izin multi-akun untuk menetapkan akses pengguna tenaga kerja Anda. Akun AWS Anda dapat menggunakan penetapan aplikasi untuk menetapkan akses pengguna ke aplikasi yang AWS dikelola dan dikelola pelanggan.

> **Note**
>
> Meskipun nama layanan AWS Single Sign-On telah dihentikan, istilah single sign-on masih digunakan di seluruh panduan ini untuk menggambarkan skema otentikasi yang memungkinkan pengguna untuk masuk satu kali untuk mengakses beberapa aplikasi dan situs web.

Kemampuan IAM Identity Center

IAM Identity Center mencakup kemampuan dan fitur inti berikut:

Kelola identitas tenaga kerja

Pengguna manusia yang membangun atau mengoperasikan beban kerja juga AWS dikenal sebagai pengguna tenaga kerja, atau identitas tenaga kerja. Pengguna tenaga kerja adalah karyawan atau kontraktor yang Anda izinkan untuk mengakses Akun AWS di organisasi dan aplikasi bisnis internal Anda. Orang-orang ini mungkin pengembang yang membangun sistem internal dan pelanggan Anda, atau pengguna sistem database internal dan aplikasi. Anda dapat membuat pengguna dan grup tenaga kerja di Pusat Identitas IAM, atau menghubungkan dan menyinkronkan ke kumpulan pengguna dan grup yang ada di sumber identitas Anda sendiri untuk digunakan di semua aplikasi dan aplikasi Anda Akun AWS . Untuk informasi selengkapnya, lihat Kelola sumber identitas Anda.

Mengelola contoh Pusat Identitas IAM

IAM Identity Center mendukung dua jenis instance: instans organisasi dan instans akun. Contoh organisasi adalah praktik terbaik. Ini adalah satu-satunya contoh yang memungkinkan Anda mengelola akses Akun AWS dan direkomendasikan untuk semua penggunaan aplikasi produksi. Instance organisasi diterapkan di akun AWS Organizations manajemen dan memberi Anda satu titik untuk mengelola akses pengguna di seluruh AWS lingkungan.

Instans akun terikat pada Akun AWS di mana mereka diaktifkan. Gunakan instans akun IAM Identity Center hanya untuk mendukung penerapan terisolasi dari aplikasi terkelola tertentu. AWS Untuk informasi selengkapnya, lihat Mengelola instans organisasi dan akun IAM Identity Center.

Kelola akses ke beberapa Akun AWS

Dengan izin multi-akun, Anda dapat merencanakan dan menerapkan izin secara terpusat di beberapa Akun AWS sekaligus tanpa perlu mengonfigurasi setiap akun secara manual. Anda dapat membuat izin berdasarkan fungsi pekerjaan umum atau menentukan izin khusus yang memenuhi kebutuhan keamanan Anda. Anda kemudian dapat menetapkan izin tersebut kepada pengguna tenaga kerja untuk mengontrol akses mereka atas akun tertentu.

Fitur opsional ini hanya tersedia untuk instance organisasi. Jika Anda menggunakan manajemen peran IAM per akun di lingkungan Anda, kedua sistem dapat hidup berdampingan. Jika Anda ingin mencoba izin multi-akun, Anda dapat mulai dengan menerapkan sistem ini secara terbatas dan memigrasikan lebih banyak lingkungan Anda untuk menggunakan sistem ini dari waktu ke waktu.

Kelola akses ke aplikasi

IAM Identity Center memungkinkan Anda untuk menyederhanakan manajemen akses aplikasi. Dengan IAM Identity Center, Anda dapat memberi pengguna tenaga kerja Anda di IAM Identity Center akses masuk tunggal ke aplikasi.

AWS aplikasi terkelola

AWS menyediakan aplikasi seperti Amazon Redshift, Amazon Managed Grafana, dan Amazon Monitron, yang terintegrasi dengan IAM Identity Center. Aplikasi ini dapat menggunakan IAM Identity Center untuk otentikasi, layanan direktori, dan propagasi identitas tepercaya. Pengguna Anda mendapat manfaat dari pengalaman masuk tunggal yang konsisten, dan karena aplikasi berbagi pandangan umum tentang pengguna, grup, dan keanggotaan grup, pengguna juga memiliki pengalaman yang konsisten saat berbagi sumber daya aplikasi dengan orang lain. Anda dapat mengonfigurasi aplikasi AWS terkelola untuk bekerja dengan IAM Identity Center langsung dari dalam konsol aplikasi yang relevan atau melalui API.

Aplikasi yang dikelola pelanggan

Anda dapat memberi pengguna tenaga kerja Anda di Pusat Identitas IAM akses masuk tunggal ke aplikasi yang mendukung federasi identitas dengan SAFL 2.0. Banyak aplikasi SAFL 2.0 yang umum digunakan, seperti Salesforce dan Microsoft 365, bekerja dengan IAM Identity Center dan tersedia dalam katalog aplikasi di konsol IAM Identity Center. Ini adalah fitur opsional yang dapat membantu jika Anda menggunakan aplikasi tersebut dan Anda membuat pengguna dan grup Anda di IAM Identity Center, atau Anda menggunakan Microsoft Active Directory Domain Service sebagai sumber identitas Anda.

Propagasi identitas tepercaya di seluruh aplikasi

Propagasi identitas tepercaya memberikan pengalaman masuk tunggal yang efisien bagi pengguna alat kueri dan aplikasi intelijen bisnis (BI) yang memerlukan akses ke data dalam layanan. AWS Manajemen akses data didasarkan pada identitas pengguna, sehingga administrator dapat memberikan akses berdasarkan keanggotaan pengguna dan grup yang ada. Akses pengguna ke AWS layanan dan peristiwa lainnya dicatat dalam log khusus layanan dan dalam CloudTrail peristiwa, sehingga auditor mengetahui tindakan apa yang diambil pengguna dan sumber daya mana yang diakses pengguna.

AWS akses akses portal untuk pengguna Anda

Portal AWS akses adalah portal web sederhana yang memberi pengguna Anda akses tanpa batas ke semua yang ditugaskan Akun AWS dan aplikasi mereka.

Nama Pusat Identitas IAM

Pada 26 Juli 2022, AWS Single Sign-On diubah namanya menjadi. AWS IAM Identity Center Untuk pelanggan yang sudah ada, tabel berikut dimaksudkan untuk menggambarkan beberapa perubahan istilah yang lebih umum yang telah diperbarui di seluruh panduan ini sebagai hasil dari penggantian nama.

Istilah warisan	Istilah saat ini
AWS Pengguna SSO atau pengguna SSO	pengguna atau pengguna tenaga kerja
AWS Portal pengguna SSO atau portal pengguna	AWS portal akses
AWS Aplikasi terintegrasi SSO	AWS aplikasi terkelola

Istilah warisan	Istilah saat ini
AWS Direktori SSO	Direktori Pusat Identitas
AWS Toko SSO atau toko identitas AWS SSO	toko identitas yang digunakan oleh IAM Identity Center

Tabel berikut menjelaskan perubahan nama panduan referensi pengguna, pengembang, dan API yang berlaku yang juga terjadi sebagai akibat dari penggantian nama ini.

Panduan warisan	Panduan saat ini
AWS Panduan Pengguna Single Sign-On	Panduan Pengguna Pusat Identitas IAM
AWS Panduan Pengembang Implementasi SCIM Masuk Tunggal	Panduan Pengembang Implementasi SCIM Pusat Identitas IAM
AWS Panduan Referensi API Masuk Tunggal	Referensi API Pusat Identitas IAM
AWS Panduan Referensi API Toko Identitas Masuk Tunggal	Referensi API Toko Identitas
AWS Panduan Referensi API OIDC Masuk Tunggal	Pusat Identitas IAM OIDC API Referensi
AWS Panduan Referensi API Portal Masuk Tunggal	Referensi API Portal Pusat Identitas IAM

Ruang nama lama tetap sama

Ruang nama `identitystore` API `sso` dan bersama dengan ruang nama terkait berikut tetap tidak berubah untuk tujuan kompatibilitas mundur.

- Perintah CLI
  - `aws configure sso`
  - `identitystore`

  - `sso`
  - `sso-admin`
  - `sso-oidc`
- Kebijakan terkelola yang berisi `AWSSSO` dan `AWSIdentitySync` awalan
- Titik akhir layanan yang berisi `sso` dan `identitystore`
- AWS CloudFormationsumber daya yang mengandung `AWS::SSO` awalan
- Peran terkait layanan yang mengandung `AWSServiceRoleForSSO`
- URL konsol yang berisi `sso` dan `singlesignon`
- URL dokumentasi yang berisi `singlesignon`

Mengaktifkan AWS IAM Identity Center

Selesaikan langkah-langkah berikut untuk masuk ke AWS Management Console dan mengaktifkan instance organisasi IAM Identity Center.

1. Lakukan salah satu dari berikut ini untuk masuk ke AWS Management Console.
   - Baru di AWS (pengguna root) - Masuk sebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di halaman berikutnya, masukkan kata sandi Anda.
   - Sudah menggunakan AWS (kredensil IAM) - Masuk menggunakan kredensil IAM Anda dengan izin administratif.
2. Buka konsol Pusat Identitas IAM.
3. Di bawah Aktifkan Pusat Identitas IAM, pilih Aktifkan dengan AWS Organizations.
4. Opsional Tambahkan tag yang ingin Anda kaitkan dengan instance organisasi ini.
5. Opsional Konfigurasikan administrasi yang didelegasikan.

> **Note**
>
> Jika Anda menggunakan lingkungan multi-akun, kami sarankan Anda mengonfigurasi administrasi yang didelegasikan. Dengan administrasi yang didelegasikan, Anda dapat membatasi jumlah orang yang memerlukan akses ke akun manajemen di AWS Organizations. Untuk informasi selengkapnya, lihat Administrator yang didelegasikan.

> **Important**
>
> Kemampuan untuk membuat instance akun IAM Identity Center diaktifkan secara default. Instance akun IAM Identity Center mencakup subset fitur yang tersedia untuk instance organisasi. Anda dapat mengontrol apakah pengguna dapat mengakses fitur ini dengan menggunakan Kebijakan Kontrol Layanan.

Apakah Anda perlu memperbarui firewall dan gateway?

Jika Anda memfilter akses ke AWS domain atau titik akhir URL tertentu dengan menggunakan solusi pemfilteran konten web seperti firewall generasi berikutnya (NGFW) atau Secure Web Gateways (SWG), Anda harus menambahkan domain atau titik akhir URL berikut ke daftar izin solusi pemfilteran konten web Anda. Melakukannya memungkinkan Anda mengakses portal AWS akses Anda.

- *[Directory ID or alias]*.awsapps.com
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.amazonaws.com
- *.sso.amazonaws.com
- *.sso.*[Region]*.amazonaws.com
- *.sso-portal.*[Region]*.amazonaws.com
- *[Region]*.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com

Pertimbangan untuk mengizinkan daftar domain dan titik akhir URL

Memahami dampak dari mengizinkan daftar domain di luar portal AWS akses.

- Untuk mengakses Akun AWS, konsol AWS Management Console, dan IAM Identity Center dari portal AWS akses Anda, Anda harus mengizinkan daftar domain tambahan. Lihat Pemecahan Masalah di PanduanAWS Management Console Memulai untuk daftar domain. AWS Management Console
- Untuk mengakses aplikasi AWS terkelola dari portal AWS akses Anda, Anda harus mengizinkan daftar domain masing-masing. Lihat dokumentasi layanan masing-masing untuk panduan.
- Daftar yang diizinkan ini mencakup AWS layanan. Jika Anda menggunakan perangkat lunak eksternal, seperti eksternal IdPs (misalnya, Okta danMicrosoft Entra ID), Anda harus menyertakan domain mereka dalam daftar yang diizinkan.

Anda sekarang siap untuk mengkonfigurasi IAM Identity Center. Ketika Anda mengaktifkan IAM Identity Center, secara otomatis dikonfigurasi dengan direktori Pusat Identitas sebagai sumber identitas default Anda, yang merupakan cara tercepat untuk memulai menggunakan IAM Identity Center. Untuk petunjuk, lihat Konfigurasikan akses pengguna dengan direktori IAM Identity Center default.

Jika Anda ingin mempelajari lebih lanjut tentang cara IAM Identity Center bekerja dengan Organizations, sumber identitas, dan peran IAM, lihat topik berikut.

Topik

Prasyarat dan pertimbangan

Topik berikut memberikan informasi tentang prasyarat dan pertimbangan lain untuk mendirikan IAM Identity Center.

Pertimbangan untuk memilih Wilayah AWS

Anda dapat mengaktifkan instans Pusat Identitas IAM dalam satu, didukung Wilayah AWS pilihan Anda. Memilih Wilayah memerlukan penilaian prioritas Anda berdasarkan kasus penggunaan dan kebijakan perusahaan Anda. Akses ke Akun AWS dan aplikasi cloud dari IAM Identity Center Anda tidak bergantung pada pilihan ini; Namun, akses ke aplikasi yang AWS dikelola dan kemampuan untuk digunakan AWS Managed Microsoft AD sebagai sumber identitas dapat bergantung pada pilihan ini. Lihat titik akhir dan kuota PusatAWS Identitas IAM dalam daftar Wilayah yang didukung Referensi Umum AWS Pusat Identitas IAM.

Pertimbangan utama untuk memilih. Wilayah AWS

- Lokasi geografis — Saat Anda memilih Wilayah yang secara geografis paling dekat dengan mayoritas pengguna akhir Anda, mereka akan memiliki latensi akses yang lebih rendah ke portal AWS akses dan aplikasi AWS terkelola, seperti Amazon. SageMaker Studio
- Ketersediaan aplikasi AWS AWS terkelola - aplikasi yang dikelola, seperti Amazon SageMaker, hanya dapat beroperasi di yang Wilayah AWS mereka dukung. Aktifkan Pusat Identitas IAM di Wilayah yang didukung oleh aplikasi AWS terkelola yang ingin Anda gunakan dengannya. Banyak aplikasi AWS terkelola juga dapat beroperasi hanya di Wilayah yang sama tempat Anda mengaktifkan Pusat Identitas IAM.

- Kedaulatan digital — Peraturan kedaulatan digital atau kebijakan perusahaan dapat mengamanatkan penggunaan tertentu. Wilayah AWSKonsultasikan dengan departemen hukum perusahaan Anda.
- Sumber identitas - Jika Anda menggunakan AWS Managed Microsoft AD atau AD Connector sebagai sumber identitas, Wilayah beranda harus cocok dengan tempat Anda mengaktifkan Pusat Identitas IAM. Wilayah AWS
- Wilayah dinonaktifkan secara default — AWS awalnya mengaktifkan semua yang baru Wilayah AWS untuk digunakan secara Akun AWS default, yang secara otomatis memungkinkan pengguna Anda untuk membuat sumber daya di Wilayah mana pun. Sekarang ketika AWS menambahkan Wilayah baru, penggunaannya dinonaktifkan secara default di semua akun. Jika Anda menyebarkan Pusat Identitas IAM di Wilayah yang dinonaktifkan secara default, maka Anda harus mengaktifkan Wilayah ini di semua akun yang ingin Anda kelola aksesnya ke Pusat Identitas IAM. Ini diperlukan bahkan jika Anda tidak berencana untuk membuat sumber daya apa pun di Wilayah tersebut di akun tersebut.

  Anda dapat mengaktifkan Wilayah untuk akun saat ini di organisasi Anda dan Anda harus mengulangi tindakan ini untuk akun baru yang mungkin Anda tambahkan nanti. Untuk petunjuk, lihat Mengaktifkan atau menonaktifkan Wilayah di organisasi Anda dalam panduan AWS Organizations pengguna. Untuk menghindari pengulangan langkah-langkah tambahan ini, Anda dapat memilih untuk menerapkan Pusat Identitas IAM Anda di Wilayah yang diaktifkan secara default. Sebagai referensi, Wilayah berikut diaktifkan secara default:

  - AS Timur (Ohio)
  - AS Timur (Virginia Utara)
  - AS Barat (Oregon)
  - AS Barat (California Utara)
  - Eropa (Paris)
  - Amerika Selatan (São Paulo)
  - Asia Pasifik (Mumbai)
  - Eropa (Stockholm)
  - Asia Pasifik (Seoul)
  - Asia Pasifik (Tokyo)
  - Eropa (Irlandia)
  - Eropa (Frankfurt)
  - Eropa (London)

- Asia Pasifik (Singapura)
- Asia Pacific (Sydney)
- Kanada (Pusat)
- Asia Pasifik (Osaka)

- Panggilan Lintas Wilayah - Di beberapa Wilayah, Pusat Identitas IAM dapat menghubungi Amazon Simple Email Service di Wilayah lain untuk mengirim email. Dalam panggilan Lintas wilayah ini, Pusat Identitas IAM mengirimkan atribut pengguna tertentu ke Wilayah lain. Untuk informasi selengkapnya tentang Wilayah, lihat AWS IAM Identity Center Ketersediaan wilayah.

Beralih Wilayah AWS

Anda dapat mengganti Wilayah Pusat Identitas IAM Anda hanya dengan menghapus instance saat ini dan membuat instance baru di Wilayah lain. Jika Anda sudah mengaktifkan aplikasi AWS terkelola dengan instans yang ada, Anda harus menghapusnya terlebih dahulu sebelum menghapus Pusat Identitas IAM Anda. Anda harus membuat ulang pengguna, grup, set izin, aplikasi, dan tugas dalam contoh baru. Anda dapat menggunakan akun IAM Identity Center dan API penetapan aplikasi untuk mendapatkan snapshot konfigurasi Anda dan kemudian menggunakan snapshot itu untuk membangun kembali konfigurasi Anda di Wilayah baru. Anda mungkin juga perlu membuat ulang beberapa konfigurasi Pusat Identitas IAM melalui Konsol Manajemen instans baru Anda. Untuk petunjuk tentang menghapus Pusat Identitas IAM, lihat. Hapus konfigurasi Pusat Identitas IAM

Kuota untuk peran IAM yang dibuat oleh IAM Identity Center

IAM Identity Center membuat peran IAM untuk memberi pengguna izin ke sumber daya. Saat Anda menetapkan set izin, Pusat Identitas IAM akan membuat peran IAM yang dikontrol Pusat Identitas IAM yang sesuai di setiap akun, dan melampirkan kebijakan yang ditentukan dalam izin yang disetel ke peran tersebut. IAM Identity Center mengelola peran, dan memungkinkan pengguna resmi yang telah Anda tentukan untuk mengambil peran, dengan menggunakan portal AWS akses atau. AWS CLISaat Anda mengubah set izin, IAM Identity Center memastikan bahwa kebijakan dan peran IAM yang sesuai diperbarui sesuai dengan itu.

Jika Anda sudah mengonfigurasi peran IAM Akun AWS, kami sarankan Anda memeriksa apakah akun Anda mendekati kuota untuk peran IAM. Kuota default untuk peran IAM per akun adalah 1000 peran. Untuk informasi selengkapnya, lihat kuota objek IAM.

Jika Anda mendekati kuota, pertimbangkan untuk meminta kenaikan kuota. Jika tidak, Anda mungkin mengalami masalah dengan Pusat Identitas IAM saat Anda memberikan set izin ke akun yang telah

melebihi kuota peran IAM. Untuk informasi tentang cara meminta kenaikan kuota, lihat Meminta kenaikan kuota pada Panduan Pengguna Service Quotas.

> **Note**
>
> Jika Anda meninjau peran IAM di akun yang sudah menggunakan IAM Identity Center, Anda mungkin melihat nama peran yang diawali. “AWSReservedSSO_” Ini adalah peran yang dibuat oleh layanan Pusat Identitas IAM di akun, dan mereka berasal dari menetapkan izin yang ditetapkan ke akun.

Pusat Identitas IAM dan AWS Organizations

AWS Organizations direkomendasikan, tetapi tidak diperlukan, untuk digunakan dengan IAM Identity Center. Jika Anda belum mendirikan organisasi, Anda tidak perlu melakukannya. Ketika Anda mengaktifkan IAM Identity Center, Anda akan memilih apakah akan mengaktifkan layanan dengan AWS Organizations. Ketika Anda mendirikan sebuah organisasi, Akun AWS yang mengatur organisasi menjadi akun manajemen organisasi. Pengguna root sekarang Akun AWS adalah pemilik akun manajemen organisasi. Setiap tambahan yang Akun AWS Anda undang ke organisasi Anda adalah akun anggota. Akun manajemen membuat sumber daya organisasi, unit organisasi, dan kebijakan yang mengelola akun anggota. Izin didelegasikan ke akun anggota oleh akun manajemen.

> **Note**
>
> Kami menyarankan Anda mengaktifkan Pusat Identitas IAM dengan AWS Organizations, yang membuat instance organisasi dari IAM Identity Center. Contoh organisasi adalah praktik terbaik yang kami rekomendasikan karena mendukung semua fitur Pusat Identitas IAM dan menyediakan kemampuan manajemen pusat. Untuk informasi selengkapnya, lihat Mengelola instans organisasi dan akun IAM Identity Center.

Jika Anda sudah menyiapkan AWS Organizations dan akan menambahkan Pusat Identitas IAM ke organisasi Anda, pastikan semua AWS Organizations fitur diaktifkan. Saat Anda membuat organisasi, mengaktifkan semua fitur adalah default. Untuk informasi selengkapnya, lihat Mengaktifkan semua fitur di organisasi Anda dalam Panduan PenggunaAWS Organizations .

Untuk mengaktifkan Pusat Identitas IAM, Anda harus masuk ke AWS Management Console dengan masuk ke akun AWS Organizations manajemen Anda sebagai pengguna yang memiliki kredensi

administratif atau sebagai pengguna root (tidak disarankan kecuali tidak ada pengguna administratif lain). Anda tidak dapat mengaktifkan Pusat Identitas IAM saat masuk dengan kredensi administratif dari akun AWS Organizations anggota. Untuk informasi selengkapnya, lihat Membuat dan mengelola AWS Organisasi di PanduanAWS Organizations Pengguna.

Konfirmasikan sumber identitas Anda di Pusat Identitas IAM

Sumber identitas Anda di IAM Identity Center menentukan di mana pengguna dan grup Anda dikelola. Setelah mengaktifkan Pusat Identitas IAM, konfirmasikan bahwa Anda menggunakan sumber identitas pilihan Anda.

Konfirmasikan sumber identitas Anda

1. Pergi ke Dashboard
2. Di bagian Optimalkan Pusat Identitas IAM, pilih tombol Konfirmasi sumber identitas. Anda juga dapat mengakses halaman ini dengan memilih Pengaturan dan memilih tab Sumber identitas.
3. Tidak ada tindakan jika Anda ingin menyimpan sumber identitas yang ditetapkan. Jika Anda lebih suka mengubahnya, pilih Tindakan, lalu pilih Ubah sumber identitas.

   Anda dapat memilih salah satu dari berikut ini sebagai sumber identitas Anda:

   Direktori Pusat Identitas

   Ketika Anda mengaktifkan IAM Identity Center untuk pertama kalinya, itu secara otomatis dikonfigurasi dengan direktori Pusat Identitas sebagai sumber identitas default Anda. Jika Anda belum menggunakan penyedia identitas eksternal lain, Anda dapat mulai membuat pengguna dan grup, dan menetapkan tingkat akses mereka ke aplikasi Akun AWS dan Anda. Untuk tutorial tentang menggunakan sumber identitas ini, lihatKonfigurasikan akses pengguna dengan direktori IAM Identity Center default.

   Direktori Aktif

   Jika Anda sudah mengelola pengguna dan grup di AWS Managed Microsoft AD direktori menggunakan AWS Directory Service atau direktori yang dikelola sendiriActive Directory (AD), sebaiknya sambungkan direktori tersebut saat mengaktifkan IAM Identity Center. Jangan membuat pengguna dan grup apa pun di direktori Pusat Identitas default. IAM Identity Center menggunakan koneksi yang disediakan oleh AWS Directory Service untuk menyinkronkan informasi pengguna, grup, dan keanggotaan dari direktori sumber Anda di

Active Directory ke toko identitas IAM Identity Center. Untuk informasi selengkapnya, lihat Connect ke Microsoft AD direktori.

> **Note**
>
> IAM Identity Center tidak mendukung Simple AD berbasis Samba4 sebagai sumber identitas.

Penyedia identitas eksternal

Untuk penyedia identitas eksternal (IdPs) seperti Okta atauMicrosoft Entra ID, Anda dapat menggunakan IAM Identity Center untuk mengautentikasi identitas dari IdPs melalui standar Security Assertion Markup Language (SAMP) 2.0. Protokol SAMP tidak menyediakan cara untuk menanyakan IDP untuk mempelajari tentang pengguna dan grup. Anda membuat Pusat Identitas IAM mengetahui pengguna dan grup tersebut dengan menyediakannya ke Pusat Identitas IAM. Anda dapat melakukan penyediaan otomatis (sinkronisasi) informasi pengguna dan grup dari IDP Anda ke Pusat Identitas IAM menggunakan protokol System for Cross-domain Identity Management (SCIM) v2.0 jika IDP Anda mendukung SCIM. Jika tidak, Anda dapat menyediakan pengguna dan grup secara manual dengan memasukkan nama pengguna, alamat email, dan grup secara manual ke Pusat Identitas IAM.

Untuk petunjuk terperinci tentang pengaturan sumber identitas Anda, lihatMemulai tutorial.

> **Note**
>
> Jika Anda berencana untuk menggunakan penyedia identitas eksternal, perhatikan bahwa IDP eksternal, bukan Pusat Identitas IAM, mengelola pengaturan otentikasi multi-faktor (MFA). MFA di IAM Identity Center tidak didukung untuk digunakan oleh eksternal. IdPs Untuk informasi selengkapnya, lihat Meminta pengguna untuk MFA.

Sumber identitas yang Anda pilih menentukan lokasi IAM Identity Center mencari pengguna dan grup yang memerlukan akses masuk tunggal. Setelah mengonfirmasi atau mengubah sumber identitas Anda, Anda akan membuat atau menentukan pengguna dan menetapkan mereka izin administratif untuk Anda. Akun AWS

> **Important**
>
> Jika Anda sudah mengelola pengguna dan grup di Active Directory atau penyedia identitas eksternal (iDP), sebaiknya Anda mempertimbangkan untuk menghubungkan sumber identitas ini saat mengaktifkan Pusat Identitas IAM dan memilih sumber identitas Anda. Ini harus dilakukan sebelum Anda membuat pengguna dan grup apa pun di direktori Pusat Identitas default dan membuat tugas apa pun.
>
> Jika Anda sudah mengelola pengguna dan grup dalam satu sumber identitas di Pusat Identitas IAM, mengubah ke sumber identitas yang berbeda dapat menghapus semua penetapan pengguna dan grup yang Anda konfigurasikan di Pusat Identitas IAM. Jika ini terjadi, semua pengguna, termasuk pengguna administratif di IAM Identity Center, akan kehilangan akses masuk tunggal ke aplikasi dan aplikasi mereka Akun AWS . Untuk informasi selengkapnya, lihat Pertimbangan untuk mengubah sumber identitas Anda.

Setelah mengonfigurasi sumber identitas, Anda dapat mencari pengguna atau grup untuk memberi mereka akses masuk tunggal, aplikasi cloud Akun AWS, atau keduanya.

Memulai tutorial

Anda dapat memiliki satu sumber identitas per organisasi sehingga penting untuk meluangkan waktu untuk menguji kemampuan yang dimiliki masing-masing organisasi.

Di bagian ini, Anda dapat memilih salah satu tutorial berikut untuk menyiapkan Pusat Identitas IAM dengan sumber identitas pilihan Anda, membuat pengguna administratif, dan mengonfigurasi set izin untuk memberi pengguna Anda akses ke sumber daya.

Sebelum memulai salah satu tutorial ini, aktifkan IAM Identity Center. Lihat informasi yang lebih lengkap di Mengaktifkan AWS IAM Identity Center.

Topik

- Konfigurasikan akses pengguna dengan direktori IAM Identity Center default
- Menggunakan Active Directory sebagai sumber identitas
- Setting up SCIM provisioning between CyberArk and IAM Identity Center
- Konfigurasikan SAMP dan SCIM dengan Google Workspace dan IAM Identity Center
- Menggunakan IAM Identity Center untuk terhubung dengan Platform JumpCloud Direktori
- Konfigurasikan SAMP dan SCIM dengan Microsoft Entra ID dan IAM Identity Center
- Konfigurasikan SAFL dan SCIM dengan Okta dan IAM Identity Center
- Menyiapkan penyediaan SCIM antara OneLogin dan IAM Identity Center
- Menggunakan Ping Identity produk dengan IAM Identity Center

Konfigurasikan akses pengguna dengan direktori IAM Identity Center default

Ketika Anda mengaktifkan IAM Identity Center untuk pertama kalinya, itu secara otomatis dikonfigurasi dengan direktori Pusat Identitas sebagai sumber identitas default Anda, sehingga Anda tidak perlu memilih sumber identitas. Jika organisasi Anda menggunakan penyedia identitas lain seperti AWS Directory Service for Microsoft Active Directory,Microsoft Entra ID, atau Okta pertimbangkan untuk mengintegrasikan sumber identitas tersebut dengan IAM Identity Center alih-alih menggunakan konfigurasi default.

Tujuan

Dalam tutorial ini, Anda akan menggunakan direktori default sebagai sumber identitas Anda dan mengatur dan menguji akses pengguna. Dalam skenario ini, Anda mengelola semua pengguna dan grup di Pusat Identitas IAM. Pengguna masuk melalui portal AWS akses. Tutorial ini ditujukan untuk pengguna yang baru AWS atau yang telah menggunakan IAM untuk mengelola pengguna dan grup. Pada langkah selanjutnya, Anda akan membuat yang berikut:

- Pengguna administratif bernama *Nikki Wolf*
- Grup bernama *Admin Team*
- Sebuah set izin bernama *AdminAccess*

Untuk memverifikasi semuanya dibuat dengan benar, Anda akan masuk dan mengatur kata sandi pengguna administratif. Setelah menyelesaikan tutorial ini, Anda dapat menggunakan pengguna administratif untuk menambahkan lebih banyak pengguna di IAM Identity Center, membuat set izin tambahan, dan mengatur akses organisasi ke aplikasi.

Jika Anda belum mengaktifkan IAM Identity Center, lihatMengaktifkan AWS IAM Identity Center.

Sebelum Anda memulai:

Lakukan salah satu dari berikut ini untuk masuk ke AWS Management Console.

- Baru di AWS (pengguna root) - Masuk sebagai pemilik akun dengan memilih pengguna Akun AWS root dan memasukkan alamat Akun AWS email Anda. Di halaman berikutnya, masukkan kata sandi Anda.
- Sudah menggunakan AWS (kredensi IAM) - Masuk menggunakan kredenal IAM Anda dengan izin administratif.

Buka konsol Pusat Identitas IAM.

Langkah 1: Tambahkan pengguna

1. Di panel navigasi Pusat Identitas IAM, pilih Pengguna, lalu pilih Tambah pengguna.
2. Pada halaman Tentukan detail pengguna, lengkapi informasi berikut:
   - Nama pengguna - Untuk tutorial ini, masukkan *nikkiw*.

Saat membuat pengguna, pilih nama pengguna yang mudah diingat. Pengguna Anda harus mengingat nama pengguna untuk masuk ke portal AWS akses dan Anda tidak dapat mengubahnya nanti.

- Kata Sandi - Pilih Kirim email ke pengguna ini dengan instruksi pengaturan kata sandi (Disarankan).

  Opsi ini mengirimkan email kepada pengguna yang dialamatkan dari Amazon Web Services, dengan baris subjek Undangan untuk bergabung dengan IAM Identity Center (penerus AWS Single Sign-On). Email berasal dari salah satu `no-reply@signin.aws` atau `no-reply@login.awsapps.com`. Tambahkan alamat email ini ke daftar pengirim yang disetujui.
- Alamat email - Masukkan alamat email untuk pengguna tempat Anda dapat menerima email. Kemudian, masukkan lagi untuk mengonfirmasinya. Setiap pengguna harus memiliki alamat email yang unik.
- Nama depan - Masukkan nama depan untuk pengguna. Untuk tutorial ini, masukkan *`Nikki`*.
- Nama belakang - Masukkan nama belakang untuk pengguna. Untuk tutorial ini, masukkan *`Wolf`*.
- Nama tampilan - Nilai default adalah nama depan dan belakang pengguna. Jika Anda ingin mengubah nama tampilan, Anda dapat memasukkan sesuatu yang berbeda. Nama tampilan terlihat di portal masuk dan daftar pengguna.
- Lengkapi informasi opsional jika diinginkan. Ini tidak digunakan selama tutorial ini dan Anda dapat mengubahnya nanti.

3. Pilih Berikutnya. Halaman Tambahkan pengguna ke grup muncul. *`Kami akan membuat grup untuk menetapkan izin administratif alih-alih memberikannya langsung ke Nikki.`*

   Pilih Buat grup

   Tab browser baru terbuka untuk menampilkan halaman Buat grup.

   a. Di bawah Detail grup, di Nama grup masukkan nama untuk grup. Kami merekomendasikan nama grup yang mengidentifikasi peran grup. Untuk tutorial ini, masukkan *`tim Admin`*.

   b. Pilih Buat grup

   c. Tutup tab Browser Grup untuk kembali ke tab Tambah browser pengguna

4. Di area Grup, pilih tombol Refresh. Grup *`tim Admin`* muncul dalam daftar.

Pilih kotak centang di samping *tim Admin*, lalu pilih Berikutnya.

5. Pada halaman Tinjau dan tambahkan pengguna, konfirmasikan hal berikut:

   - Informasi utama muncul seperti yang Anda inginkan
   - Grup menunjukkan pengguna yang ditambahkan ke grup yang Anda buat

   Jika Anda ingin membuat perubahan, pilih Edit. Ketika semua detail sudah benar pilih Tambahkan pengguna.

   Pesan pemberitahuan memberi tahu Anda bahwa pengguna telah ditambahkan.

Selanjutnya, Anda akan menambahkan izin administratif untuk grup *tim Admin* sehingga *Nikki* memiliki akses ke sumber daya.

Langkah 2: Tambahkan izin administratif

1. Di panel navigasi Pusat Identitas IAM, di bawah izin Multi-akun, pilih. Akun AWS
2. Pada Akun AWShalaman, struktur Organisasi menampilkan organisasi Anda dengan akun Anda di bawahnya dalam hierarki. Pilih kotak centang untuk akun manajemen Anda, lalu pilih Tetapkan pengguna atau grup.
3. Tampilan alur kerja Tetapkan pengguna dan grup. Ini terdiri dari tiga langkah:

   a. Untuk Langkah 1: Pilih pengguna dan grup pilih grup *tim Admin* yang Anda buat. Lalu pilih Selanjutnya.

   b. Untuk Langkah 2: Pilih set izin pilih Buat set izin untuk membuka tab baru yang memandu Anda melalui tiga sub-langkah yang terlibat dalam membuat set izin.

      i. Untuk Langkah 1: Pilih jenis set izin lengkapi yang berikut ini:

         - Dalam Jenis set izin, pilih Set izin yang telah ditentukan sebelumnya.
         - Dalam Kebijakan untuk set izin yang telah ditentukan sebelumnya, pilih AdministratorAccess.

         Pilih Berikutnya.

      ii. Untuk Langkah 2: Tentukan detail set izin, pertahankan pengaturan default, dan pilih Berikutnya.

Pengaturan default membuat set izin bernama *AdministratorAccess*dengan durasi sesi diatur ke satu jam.

iii. Untuk Langkah 3: Tinjau dan buat, verifikasi bahwa jenis set Izin menggunakan kebijakan AWS terkelola AdministratorAccess. Pilih Buat. Pada halaman Set izin, pemberitahuan muncul memberi tahu Anda bahwa set izin telah dibuat. Anda dapat menutup tab ini di browser web Anda sekarang.

Pada tab Tetapkan pengguna dan grup browser, Anda masih pada Langkah 2: Pilih set izin dari mana Anda memulai alur kerja set izin buat.

Di area set Izin, pilih tombol Refresh. Set *AdministratorAccess*izin yang Anda buat muncul dalam daftar. Pilih kotak centang untuk set izin tersebut dan kemudian pilih Berikutnya.

c. Pada Langkah 3: Tinjau dan kirimkan halaman tugas, konfirmasikan bahwa grup *tim Admin* dipilih dan set *AdministratorAccess*izin dipilih, lalu pilih Kirim.

Halaman diperbarui dengan pesan bahwa Anda Akun AWS sedang dikonfigurasi. Tunggu sampai proses selesai.

Anda dikembalikan ke Akun AWS halaman. Pesan notifikasi memberi tahu Anda bahwa pesan Anda Akun AWS telah direvisi dan set izin yang diperbarui diterapkan.

> **Selamat!**
>
> Anda telah berhasil mengatur set pengguna, grup, dan izin pertama Anda.

Pada bagian berikutnya dari tutorial ini Anda akan menguji akses *Nikki* dengan masuk ke portal AWS akses dengan kredensi administratif mereka dan mengatur kata sandi mereka. Keluar dari konsol sekarang.

Langkah 3: Uji akses pengguna

Sekarang *Nikki Wolf* adalah pengguna di organisasi Anda, mereka dapat masuk dan mengakses sumber daya yang mereka berikan izin sesuai dengan set izin mereka. Untuk memverifikasi bahwa pengguna dikonfigurasi dengan benar, pada langkah selanjutnya ini Anda akan menggunakan *kredensi Nikki* untuk masuk dan mengatur kata sandi mereka. Ketika Anda menambahkan

pengguna *Nikki Wolf* di langkah 1 Anda memilih untuk meminta *Nikki* menerima email dengan instruksi pengaturan kata sandi. Saatnya membuka email itu dan melakukan hal berikut:

1. Di email, pilih tautan Terima undangan untuk menerima undangan.

   > **Note**
   >
   > Email tersebut juga menyertakan nama *pengguna Nikki* dan URL portal AWS akses yang akan mereka gunakan untuk masuk ke organisasi. Catat informasi ini untuk digunakan di masa mendatang.

   Anda dibawa ke halaman pendaftaran pengguna baru di mana Anda dapat mengatur kata sandi *Nikki*.

2. Setelah menyetel kata sandi *Nikki*, Anda dinavigasi ke halaman Masuk. Masukkan ***nikkiw*** dan pilih Berikutnya, lalu masukkan kata sandi ***Nikki*** dan pilih Masuk.
3. Portal AWS akses terbuka menampilkan organisasi dan aplikasi yang dapat Anda akses.

   Pilih organisasi untuk memperluasnya ke dalam daftar Akun AWS lalu pilih akun untuk menampilkan peran yang dapat Anda gunakan untuk mengakses sumber daya di akun.

   Setiap set izin memiliki dua metode manajemen yang dapat Anda gunakan, kunci Peran atau Akses.

   - Peran, misalnya *AdministratorAccess*- Membuka AWS Console Home.
   - Kunci akses - Menyediakan kredenal yang dapat Anda gunakan dengan AWS CLI atau dan AWS SDK. Termasuk informasi untuk menggunakan kredensi jangka pendek yang secara otomatis menyegarkan atau kunci akses jangka pendek. Untuk informasi selengkapnya, lihat Mendapatkan kredensi pengguna IAM Identity Center untuk atau SDK AWS CLIAWS.
4. Pilih tautan Peran untuk masuk ke AWS Console Home.

Anda masuk dan dinavigasi ke AWS Console Home halaman. Jelajahi konsol dan konfirmasikan bahwa Anda memiliki akses yang Anda harapkan.

Langkah selanjutnya

Sekarang setelah Anda membuat pengguna administratif di IAM Identity Center, Anda dapat:

- Tetapkan aplikasi
- Tambahkan pengguna lain
- Tetapkan pengguna ke akun
- Konfigurasikan set izin tambahan

> **Note**
>
> Anda dapat menetapkan beberapa set izin ke pengguna yang sama. Untuk mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit, setelah Anda membuat pengguna administratif, buat set izin yang lebih ketat dan tetapkan ke pengguna yang sama. Dengan begitu, Anda dapat mengakses Anda hanya Akun AWS dengan izin yang Anda butuhkan, bukan izin administratif.

Setelah pengguna Anda menerima undangan mereka untuk mengaktifkan akun mereka dan mereka masuk ke portal AWS akses, satu-satunya item yang muncul di portal adalah untuk Akun AWS, peran, dan aplikasi yang mereka tetapkan.

> **Important**
>
> Kami sangat menyarankan agar Anda mengaktifkan otentikasi multi-faktor (MFA) untuk pengguna Anda. Untuk informasi selengkapnya, lihat Otentikasi multi-faktor untuk pengguna Pusat Identitas.

Menggunakan Active Directory sebagai sumber identitas

Jika Anda mengelola pengguna di AWS Managed Microsoft AD direktori menggunakan AWS Directory Service atau direktori yang dikelola sendiri di Active Directory (AD), Anda dapat mengubah sumber identitas Pusat Identitas IAM agar berfungsi dengan pengguna tersebut. Kami menyarankan Anda mempertimbangkan untuk menghubungkan sumber identitas ini ketika Anda mengaktifkan IAM Identity Center dan memilih sumber identitas Anda. Melakukan hal ini sebelum Anda membuat pengguna dan grup di direktori Pusat Identitas default akan membantu Anda menghindari konfigurasi tambahan yang diperlukan jika Anda mengubah sumber identitas Anda nanti.

Untuk menggunakan Active Directory sebagai sumber identitas Anda, konfigurasi Anda harus memenuhi prasyarat berikut:

- Jika Anda menggunakanAWS Managed Microsoft AD, Anda harus mengaktifkan IAM Identity Center di tempat yang sama Wilayah AWS di mana AWS Managed Microsoft AD direktori Anda diatur. IAM Identity Center menyimpan data penugasan di Wilayah yang sama dengan direktori. Untuk mengelola Pusat Identitas IAM, Anda mungkin perlu beralih ke Wilayah tempat Pusat Identitas IAM dikonfigurasi. Juga, perhatikan bahwa portal AWS akses menggunakan URL akses yang sama dengan direktori Anda.
- Gunakan Active Directory yang berada di akun manajemen:

  Anda harus memiliki AD Connector atau AWS Managed Microsoft AD direktori yang sudah adaAWS Directory Service, dan direktori tersebut harus berada di dalam akun AWS Organizations manajemen Anda. Anda hanya dapat menghubungkan satu direktori AD Connector atau satu direktori sekaligus. AWS Managed Microsoft AD Jika Anda perlu mendukung beberapa domain atau hutan, gunakanAWS Managed Microsoft AD. Untuk informasi selengkapnya, lihat:

  - Connect direktori AWS Managed Microsoft AD ke IAM Identity Center
  - Connect direktori yang dikelola sendiri di Active Directory ke IAM Identity Center
- Gunakan Active Directory yang berada di akun administrator yang didelegasikan:

  Jika Anda berencana untuk mengaktifkan administrator yang didelegasikan IAM Identity Center dan menggunakan Active Directory sebagai sumber identitas Pusat Identitas IAM, Anda dapat menggunakan AD Connector atau AWS Managed Microsoft AD direktori yang sudah ada yang disiapkan di Direktori yang berada di AWS akun admin yang didelegasikan.

  Jika Anda memutuskan untuk mengubah sumber identitas IAM Identity Center dari sumber lain ke Active Directory, atau mengubahnya dari Active Directory ke sumber lain, direktori harus berada di (dimiliki oleh) akun anggota administrator yang didelegasikan IAM Identity Center jika ada; jika tidak, itu harus berada di akun manajemen.

Tutorial ini memandu Anda melalui pengaturan dasar untuk menggunakan Active Directory sebagai sumber identitas IAM Identity Center.

Langkah 1: Connect Active Directory dan tentukan pengguna

Jika Anda sudah menggunakan Active Directory, topik berikut akan membantu Anda mempersiapkan diri untuk menghubungkan direktori Anda ke IAM Identity Center.

> **Note**
>
> Sebagai praktik keamanan terbaik, kami sangat menyarankan Anda mengaktifkan otentikasi multi-faktor. Jika Anda berencana untuk menghubungkan AWS Managed Microsoft AD direktori atau direktori yang dikelola sendiri di Active Directory dan Anda tidak menggunakan RADIUS MFA, aktifkan MFA di AWS Directory Service IAM Identity Center.

AWS Managed Microsoft AD

1. Tinjau panduan diConnect ke Microsoft AD direktori.
2. Ikuti langkah-langkahnya di Connect direktori AWS Managed Microsoft AD ke IAM Identity Center.
3. Konfigurasikan Active Directory untuk menyinkronkan pengguna yang ingin Anda berikan izin administratif ke IAM Identity Center. Untuk informasi selengkapnya, lihat Sinkronisasi pengguna administratif ke IAM Identity Center.

Direktori yang dikelola sendiri di Direktori Aktif

1. Tinjau panduan diConnect ke Microsoft AD direktori.
2. Ikuti langkah-langkahnya di Connect direktori yang dikelola sendiri di Active Directory ke IAM Identity Center.
3. Konfigurasikan Active Directory untuk menyinkronkan pengguna yang ingin Anda berikan izin administratif ke IAM Identity Center. Untuk informasi selengkapnya, lihat Sinkronisasi pengguna administratif ke IAM Identity Center.

Langkah 2: Sinkronisasi pengguna administratif ke IAM Identity Center

Setelah Anda menghubungkan direktori Anda ke IAM Identity Center, Anda dapat menentukan pengguna yang ingin Anda berikan izin administratif, dan kemudian menyinkronkan pengguna tersebut dari direktori Anda ke Pusat Identitas IAM.

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Sumber identitas, pilih Tindakan, lalu pilih Kelola Sinkronisasi.
4. Pada halaman Kelola Sinkronisasi, pilih tab Pengguna, lalu pilih Tambahkan pengguna dan grup.

5. Pada tab Pengguna, di bawah Pengguna, masukkan nama pengguna yang tepat dan pilih Tambah.
6. Di bawah Pengguna dan Grup yang Ditambahkan, lakukan hal berikut:
    a. Konfirmasikan bahwa pengguna yang ingin Anda berikan izin administratif ditentukan.
    b. Pilih kotak centang di sebelah kiri nama pengguna.
    c. Pilih Kirim.
7. Di halaman Kelola sinkronisasi, pengguna yang Anda tentukan muncul di daftar cakupan pengguna dalam sinkronisasi.
8. Di panel navigasi, pilih Users (Pengguna).
9. Pada halaman Pengguna, mungkin diperlukan beberapa waktu bagi pengguna yang Anda tentukan untuk muncul dalam daftar. Pilih ikon penyegaran untuk memperbarui daftar pengguna.

Pada titik ini, pengguna Anda tidak memiliki akses ke akun manajemen. Anda akan mengatur akses administratif ke akun ini dengan membuat set izin administratif dan menetapkan pengguna ke set izin tersebut. Untuk informasi selengkapnya, lihat Buat set izin.

Setting up SCIM provisioning between CyberArk and IAM Identity Center

IAM Identity Center mendukung penyediaan otomatis (sinkronisasi) informasi pengguna dari CyberArk Directory Platform ke IAM Identity Center. Penyediaan ini menggunakan protokol System for Cross-domain Identity Management (SCIM) v2.0. Anda mengonfigurasi koneksi ini CyberArk menggunakan titik akhir dan token akses IAM Identity Center SCIM Anda. Saat mengonfigurasi sinkronisasi SCIM, Anda membuat pemetaan atribut pengguna CyberArk ke atribut bernama di Pusat Identitas IAM. Hal ini menyebabkan atribut yang diharapkan cocok antara IAM Identity Center danCyberArk.

Panduan ini didasarkan pada CyberArk per Agustus 2021. Langkah-langkah untuk versi yang lebih baru dapat bervariasi. Panduan ini berisi beberapa catatan mengenai konfigurasi otentikasi pengguna melalui SAMP.

> **Note**
>
> Sebelum Anda mulai menerapkan SCIM, kami sarankan Anda terlebih dahulu meninjau. Pertimbangan untuk menggunakan penyediaan otomatis Kemudian lanjutkan meninjau pertimbangan tambahan di bagian selanjutnya.

Topik

Prasyarat

Anda akan memerlukan yang berikut ini sebelum Anda dapat memulai:

- CyberArkberlangganan atau uji coba gratis. Untuk mendaftar untuk kunjungan uji coba gratis CyberArk.
- Akun yang diaktifkan Pusat Identitas IAM (gratis). Untuk informasi selengkapnya, lihat Mengaktifkan Pusat Identitas IAM.
- Sambungan SAFL dari CyberArk akun Anda ke Pusat Identitas IAM, seperti yang dijelaskan dalam CyberArkdokumentasi untuk Pusat Identitas IAM.
- Kaitkan konektor Pusat Identitas IAM dengan peran, pengguna, dan organisasi yang ingin Anda izinkan aksesnya. Akun AWS

Pertimbangan SCIM

Berikut ini adalah pertimbangan saat menggunakan CyberArk federasi untuk IAM Identity Center:

- Hanya peran yang dipetakan di bagian Penyediaan aplikasi yang akan disinkronkan ke Pusat Identitas IAM.

- Skrip penyediaan hanya didukung dalam status defaultnya, setelah diubah, penyediaan SCIM mungkin gagal.
  - Hanya satu atribut nomor telepon yang dapat disinkronkan dan defaultnya adalah “telepon kerja”.
- Jika pemetaan peran dalam aplikasi CyberArk IAM Identity Center diubah, perilaku di bawah ini diharapkan:
  - Jika nama peran diubah - tidak ada perubahan pada nama grup di Pusat Identitas IAM.
  - Jika nama grup diubah - grup baru akan dibuat di IAM Identity Center, grup lama akan tetap ada tetapi tidak akan memiliki anggota.
- Sinkronisasi pengguna dan perilaku de-provisioning dapat diatur dari aplikasi CyberArk IAM Identity Center, pastikan Anda mengatur perilaku yang tepat untuk organisasi Anda. Ini adalah opsi yang Anda miliki:
  - Menimpa (atau tidak) pengguna di direktori Pusat Identitas dengan nama utama yang sama.
  - De-penyediaan pengguna dari Pusat Identitas IAM saat pengguna dihapus dari peran. CyberArk
  - Perilaku pengguna de-penyediaan - nonaktifkan atau hapus.

Langkah 1: Aktifkan penyediaan di IAM Identity Center

Pada langkah pertama ini, Anda menggunakan konsol IAM Identity Center untuk mengaktifkan penyediaan otomatis.

Untuk mengaktifkan penyediaan otomatis di Pusat Identitas IAM

1. Setelah Anda menyelesaikan prasyarat, buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan di panel navigasi kiri.
3. Pada halaman Pengaturan, cari kotak Informasi penyediaan otomatis, lalu pilih Aktifkan. Ini segera memungkinkan penyediaan otomatis di IAM Identity Center dan menampilkan titik akhir SCIM dan informasi token akses yang diperlukan.
4. Dalam kotak dialog Penyediaan otomatis masuk, salin setiap nilai untuk opsi berikut. Anda harus menempelkannya nanti saat mengonfigurasi penyediaan di iDP Anda.
   a. Titik akhir SCIM
   b. Token akses
5. Pilih Tutup.

Sekarang setelah Anda menyiapkan penyediaan di konsol Pusat Identitas IAM, Anda harus menyelesaikan tugas yang tersisa menggunakan aplikasi Pusat Identitas CyberArk IAM. Langkah-langkah ini dijelaskan dalam prosedur berikut.

Langkah 2: Konfigurasikan penyediaan di CyberArk

Gunakan prosedur berikut dalam aplikasi CyberArk IAM Identity Center untuk mengaktifkan penyediaan dengan IAM Identity Center. Prosedur ini mengasumsikan bahwa Anda telah menambahkan aplikasi CyberArk IAM Identity Center ke konsol CyberArk admin Anda di bawah Aplikasi Web. Jika Anda belum melakukannya, lihatPrasyarat, dan kemudian selesaikan prosedur ini untuk mengkonfigurasi penyediaan SCIM.

Untuk mengonfigurasi penyediaan di CyberArk

1. Buka aplikasi CyberArk IAM Identity Center yang Anda tambahkan sebagai bagian dari konfigurasi SAFL untuk CyberArk (Apps > Web App). Lihat Prasyarat.
2. Pilih aplikasi IAM Identity Center dan pergi ke bagian Provisioning.
3. Centang kotak untuk Aktifkan penyediaan untuk aplikasi ini dan pilih Mode Langsung.
4. Pada prosedur sebelumnya, Anda menyalin nilai endpoint SCIM dari IAM Identity Center. Tempelkan nilai itu ke bidang URL Layanan SCIM, dalam aplikasi Pusat Identitas CyberArk IAM atur Jenis Otorisasi menjadi Header Otorisasi. Pastikan Anda menghapus garis miring ke depan di akhir URL.
5. Atur Jenis Header ke Token Pembawa.
6. Dari prosedur sebelumnya Anda menyalin nilai token Access di IAM Identity Center. Tempelkan nilai itu ke bidang Bearer Token di aplikasi CyberArk IAM Identity Center.
7. Klik Verifikasi untuk menguji dan menerapkan konfigurasi.
8. Di bawah Opsi Sinkronisasi, pilih perilaku yang tepat yang Anda inginkan agar CyberArk penyediaan keluar berfungsi. Anda dapat memilih untuk menimpa (atau tidak) pengguna IAM Identity Center yang ada dengan nama utama yang sama, dan perilaku de-provisioning.
9. Di bawah Pemetaan Peran, atur pemetaan dari CyberArk peran, di bawah bidang Nama ke grup Pusat Identitas IAM, di bawah Grup Tujuan.
10. Klik Simpan di bagian bawah setelah Anda selesai.
11. Untuk memverifikasi bahwa pengguna telah berhasil disinkronkan ke Pusat Identitas IAM, kembali ke konsol Pusat Identitas IAM dan pilih Pengguna. Pengguna yang disinkronkan dari CyberArk akan muncul di halaman Pengguna. Pengguna ini sekarang dapat ditugaskan ke akun dan dapat terhubung dalam Pusat Identitas IAM.

(Opsional) Langkah 3: Konfigurasikan atribut pengguna CyberArk untuk kontrol akses (ABAC) di Pusat Identitas IAM

Ini adalah prosedur opsional jika CyberArk Anda memilih untuk mengkonfigurasi atribut untuk IAM Identity Center untuk mengelola akses ke AWS sumber daya Anda. Atribut yang Anda tentukan CyberArk diteruskan dalam pernyataan SAMP ke IAM Identity Center. Anda kemudian membuat set izin di Pusat Identitas IAM untuk mengelola akses berdasarkan atribut yang Anda lewati. CyberArk

Sebelum Anda memulai prosedur ini, Anda harus terlebih dahulu mengaktifkan Atribut untuk kontrol akses fitur tersebut. Untuk informasi selengkapnya tentang cara melakukan ini, lihat Aktifkan dan konfigurasikan atribut untuk kontrol akses.

Untuk mengonfigurasi atribut pengguna CyberArk untuk kontrol akses di Pusat Identitas IAM

1. Buka aplikasi CyberArk IAM Identity Center yang Anda instal sebagai bagian dari konfigurasi SAFL untuk CyberArk (Apps > Web Apps).
2. Buka opsi Saml Response.
3. Di bawah Atribut, tambahkan atribut yang relevan ke tabel berikut logika di bawah ini:
    a. Nama Atribut adalah nama atribut asli dariCyberArk.
    b. Nilai Atribut adalah nama atribut yang dikirim dalam pernyataan SAMP ke IAM Identity Center.
4. Pilih Simpan.

(Opsional) Melewati atribut untuk kontrol akses

Anda dapat secara opsional menggunakan Atribut untuk kontrol akses fitur di IAM Identity Center untuk meneruskan `Attribute` elemen dengan `Name` atribut yang disetel ke. `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` Elemen ini memungkinkan Anda untuk meneruskan atribut sebagai tanda sesi dalam pernyataan SAML. Untuk informasi selengkapnya tentang tag sesi, lihat Melewati tag sesi AWS STSdi Panduan Pengguna IAM.

Untuk menyampaikan atribut sebagai tag sesi, sertakan elemen `AttributeValue` yang menentukan nilai tag. Misalnya, untuk meneruskan pasangan nilai kunci tag`CostCenter = blue`, gunakan atribut berikut.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
```

```
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Jika Anda perlu menambahkan beberapa atribut, sertakan `Attribute` elemen terpisah untuk setiap tag.

Konfigurasikan SAMP dan SCIM dengan Google Workspace dan IAM Identity Center

Jika organisasi Anda menggunakan, Google Workspace Anda dapat mengintegrasikan pengguna dan grup Anda dari Google Workspace Pusat Identitas IAM untuk memberi mereka akses ke AWS sumber daya dengan mengubah sumber identitas Pusat Identitas IAM Anda dari sumber identitas Pusat Identitas IAM default menjadi. Google Workspace

Informasi pengguna dari Google Workspace disinkronkan ke IAM Identity Center menggunakan protokol System for Cross-domain Identity Management (SCIM) v2.0. Anda mengonfigurasi koneksi ini Google Workspace dengan menggunakan endpoint SCIM Anda untuk IAM Identity Center dan token pembawa IAM Identity Center. Saat mengonfigurasi sinkronisasi SCIM, Anda membuat pemetaan atribut pengguna Google Workspace ke atribut bernama di Pusat Identitas IAM. Pemetaan ini cocok dengan atribut pengguna yang diharapkan antara IAM Identity Center dan. Google Workspace Untuk melakukan ini, Anda perlu mengatur Google Workspace sebagai penyedia identitas IAM dan penyedia identitas Pusat Identitas IAM.

Tujuan

Langkah-langkah dalam tutorial ini membantu memandu Anda melalui membangun koneksi SAMP antara Google Workspace dan AWS. Nanti, Anda akan menyinkronkan pengguna dari Google Workspace menggunakan SCIM. Untuk memverifikasi semuanya dikonfigurasi dengan benar, setelah menyelesaikan langkah-langkah konfigurasi Anda akan masuk sebagai Google Workspace pengguna dan memverifikasi akses ke AWS sumber daya. Perhatikan bahwa tutorial ini didasarkan pada lingkungan pengujian Google Workspace direktori kecil. Struktur direktori seperti grup dan unit organisasi tidak disertakan.

> **Note**
>
> Untuk mendaftar untuk uji coba Google Workspace kunjungan gratis Google Workspacedi situs Google's web.

Jika Anda belum mengaktifkan IAM Identity Center, lihatMengaktifkan AWS IAM Identity Center.

Sebelum Anda memulai

Sebelum Anda mengonfigurasi penyediaan SCIM antara Google Workspace dan IAM Identity Center, kami sarankan Anda meninjau terlebih dahulu Pertimbangan untuk menggunakan penyediaan otomatis

Konfirmasikan item berikut sebelum Anda memulai:

- Setiap Google Workspace pengguna harus memiliki nilai Nama depan, nama belakang, nama pengguna dan nama tampilan yang ditentukan.
- Setiap Google Workspace pengguna hanya memiliki satu nilai per atribut data, seperti alamat email atau nomor telepon. Setiap pengguna yang memiliki banyak nilai akan gagal untuk disinkronkan. Jika ada pengguna yang memiliki beberapa nilai dalam atributnya, hapus atribut duplikat sebelum mencoba menyediakan pengguna di Pusat Identitas IAM. Misalnya, hanya satu atribut nomor telepon yang dapat disinkronkan, karena atribut nomor telepon default adalah “telepon kerja”, gunakan atribut “telepon kerja” untuk menyimpan nomor telepon pengguna, bahkan jika nomor telepon untuk pengguna adalah telepon rumah atau ponsel.

Note

- Atribut masih disinkronkan jika pengguna dinonaktifkan di Pusat Identitas IAM, tetapi masih aktif di. Google Workspace
- Jika ada pengguna yang ada di direktori Identity Center dengan nama pengguna dan email yang sama, pengguna akan ditimpa dan disinkronkan menggunakan SCIM dari. Google Workspace

Langkah 1: Buat atribut pengguna khusus untuk AWS

1. Masuk ke konsol Google Admin Anda menggunakan akun dengan hak administrator super.
2. Di panel navigasi kiri, perluas Direktori dan kemudian pilih Pengguna.
3. Di bagian atas daftar Pengguna, pilih Opsi lainnya, lalu pilih Kelola atribut khusus.

4. Di kanan atas halaman, pilih ADD CUSTOM ATTRIBUTE.
5. Di jendela Tambahkan bidang khusus, lengkapi bidang berikut:

    a. Dalam Kategori masukkan Amazon.
    b. Dalam Deskripsi, masukkan Atribut Kustom Amazon.
    c. Dalam Nama masukkan Peran.
    d. Di Jenis Info pilih Teks.
    e. Di Visibilitas pilih Terlihat oleh pengguna dan admin.
    f. Dalam Jumlah nilai pilih Multi-nilai.

    Pilih Tambahkan. Atribut baru muncul di halaman Kelola atribut pengguna di bawah atribut Kustom.

Tetap masuk ke konsol Google Admin Anda, Anda akan terus menggunakan konsol itu di langkah berikutnya.

Langkah 2: Unduh metadata penyedia identitas

1. Di panel navigasi kiri konsol Google Admin Anda, perluas Keamanan, pilih Otentikasi, SSO dengan aplikasi SAMP. Bergantung pada tata letak konsol Anda, Anda mungkin harus memilih Tampilkan lebih banyak untuk menampilkan bagian Keamanan pada panel navigasi.
2. Di bawah metadata iDP pilih UNDUH METADATA. File GoogleIDPMetadata.xml disimpan ke folder unduhan default Anda.

Biarkan konsol Google Admin terbuka, saat Anda terus bekerja di konsol itu di berbagai waktu dalam tutorial ini.

Langkah 3: Siapkan aplikasi Amazon Web Services di Google Workspace

Aplikasi Amazon Web Services mendukung penyediaan SCIM otomatis Google Workspace pengguna Anda ke Pusat Identitas IAM.

1. Di panel navigasi kiri konsol Google Admin Anda, perluas Aplikasi, pilih Web dan aplikasi seluler.
2. Pilih Tambahkan aplikasi, lalu pilih Cari aplikasi.
3. Di kotak pencarian, masukkan Amazon Web Services, lalu pilih aplikasi Amazon Web Services (SAMP) dari daftar.

4. Pada halaman detail Penyedia Google Identitas, adalah opsi untuk mengunduh metadata atau menyalin URL SSO, ID entitas, dan sertifikat. Anda tidak perlu melakukan salah satu dari item ini karena Anda mengunduh metadata iDP di langkah 2. Anda dapat memilih Lanjutkan.
5. Pada halaman detail penyedia layanan, URL ACS dan nilai ID Entitas untuk AWS dikonfigurasi secara default, pilih Lanjutkan.
6. Pada halaman Pemetaan Atribut, di bawah Atribut tambahkan bidang ini di bawah atribut Direktori Google:

   - Pilih bidang Informasi Dasar, Email Utama dan kemudian untuk atribut Aplikasi masukkan `https://aws.amazon.com/SAML/Attributes/RoleSessionName`
   - Pilih bidang Amazon, Peran dan kemudian untuk atribut Aplikasi masukkan `https://aws.amazon.com/SAML/Attributes/Role`

   > **Note**
   >
   > Amazon, Peran adalah atribut khusus yang Anda buat di langkah 1 tutorial ini.

7. Pilih Selesai

Langkah 4: Ubah sumber identitas IAM Identity Center dan atur Google Workspace sebagai penyedia identitas SAMP

1. Masuk ke konsol Pusat Identitas IAM menggunakan peran dengan izin administratif.
2. Pilih Pengaturan di panel navigasi kiri.
3. Pada halaman Pengaturan, pilih Tindakan, lalu pilih Ubah sumber identitas.
4. Di bawah Pilih sumber identitas, pilih Penyedia identitas eksternal, lalu pilih Berikutnya.
5. Halaman Konfigurasi penyedia identitas eksternal terbuka. Untuk melengkapi halaman ini, Anda perlu mengatur IAM Identity Center sebagai aplikasi SAMP Google Workspace dan mendapatkan informasi dariGoogle Admin console, lakukan hal berikut:

   a. Di panel navigasi kiri konsol Google Admin Anda, perluas Aplikasi, pilih Web dan aplikasi seluler.

   b. Pilih Tambah aplikasi dan kemudian pilih Tambahkan aplikasi SAMP kustom.

c. Di Masukkan nama aplikasi, masukkan portalAWS akses lalu di Deskripsi masukkan teks deskriptif, untuk tutorial ini masukkan portalAWS akses untuk Google Workspace tutorial, lalu pilih Lanjutkan.

d. Pada halaman detail Penyedia Google Identitas, pilih Lanjutkan.

e. Pada halaman detail penyedia layanan, masukkan nilai ACS URL dan Entity ID. Kembali ke konsol Pusat Identitas IAM Anda untuk menemukan nilai-nilai ini:

   - Di konsol Pusat Identitas IAM di bawah metadata penyedia layanan, salin URL IAM Identity Center Assertion Consumer Service (ACS).

     Kembali ke konsol Google Admin - Halaman detail penyedia layanan dan tempel URL ke bidang URL ACS.

   - Di konsol Pusat Identitas IAM di bawah metadata penyedia layanan, salin URL penerbit Pusat Identitas IAM.

     Kembali ke konsol Google Admin - Halaman detail penyedia layanan dan tempel URL ke bidang ID Entitas.

f. Pada konsol Google Admin - Halaman detail penyedia layanan, lengkapi bidang di bawah ID Nama sebagai berikut:

   - Untuk format ID Nama, pilih EMAIL
   - Untuk ID Nama, pilih Informasi Dasar > Email utama

   Pilih Lanjutkan.

g. Pada halaman Pemetaan Atribut, di bawah Atribut pilih ADD MAPPING lalu konfigurasikan bidang ini di bawah atribut Direktori Google:

   - Pilih bidang Informasi Dasar, Email Utama lalu, untuk atribut Aplikasi, masukkan `https://aws.amazon.com/SAML/Attributes/RoleSessionName`
   - Pilih bidang Amazon, Peran lalu, untuk atribut App, masukkan `https://aws.amazon.com/SAML/Attributes/Role`

   > **Note**
   >
   > Amazon, Peran adalah atribut khusus yang Anda buat di langkah 1. Jika tidak ada, lihatLangkah 1: Buat atribut pengguna khusus untuk AWS.

h. Pilih Selesai

6. Kembali ke konsol Pusat Identitas IAM, tempat Anda berada di halaman Konfigurasi penyedia identitas eksternal. Di bawah metadata penyedia identitas, di bawah metadata IDP SAMP, pilih Pilih file dan kemudian unggah file GoogleIDPMetadata.xml yang Anda unduh di Langkah 2.

   Pilih Berikutnya.

7. Pada halaman Konfirmasi perubahan, tinjau informasi dan kemudian masukkan TERIMA ke dalam ruang yang disediakan.

   Pilih Ubah sumber identitas.

Anda sekarang siap untuk mengaktifkan aplikasi Amazon Web Services Google Workspace sehingga pengguna Anda dapat menjadi ketentuan ke IAM Identity Center.

Langkah 5: Aktifkan aplikasi di Google Workspace

1. Di panel navigasi kiri konsol Google Admin Anda, perluas Aplikasi, pilih Web dan aplikasi seluler.
2. Dalam daftar Apps, pilih ikon Amazon Web Services untuk membuka halaman detail aplikasi.
3. Di panel akses Pengguna, di sebelah Akses pengguna pilih panah bawah Perluas akses Pengguna untuk menampilkan panel Status layanan.
4. Dalam Status layanan pilih ON untuk semua orang, lalu pilih SIMPAN.
5. Pilih ikon portalAWS akses untuk membuka halaman detail aplikasi.
6. Di panel akses Pengguna, di sebelah Akses pengguna pilih panah bawah Perluas akses Pengguna untuk menampilkan panel Status layanan.
7. Dalam Status layanan pilih ON untuk semua orang, lalu pilih SIMPAN.

> **Note**
>
> Untuk membantu mempertahankan prinsip hak istimewa yang paling rendah, kami sarankan setelah Anda menyelesaikan tutorial ini, Anda mengubah status Layanan menjadi OFF untuk semua orang untuk kedua aplikasi ini. Hanya pengguna yang membutuhkan akses yang AWS harus mengaktifkan layanan. Anda dapat menggunakan Google Workspace grup atau unit organisasi untuk memberikan akses pengguna ke subset tertentu dari pengguna Anda.

Langkah 6: Siapkan penyediaan otomatis IAM Identity Center

1. Masuk ke konsol Pusat Identitas IAM menggunakan peran dengan izin administratif.
2. Pada halaman Pengaturan, cari kotak Informasi penyediaan otomatis, lalu pilih Aktifkan. Ini segera memungkinkan penyediaan otomatis di IAM Identity Center dan menampilkan titik akhir SCIM dan informasi token akses yang diperlukan.
3. Di kotak dialog Penyediaan otomatis masuk, salin setiap nilai untuk opsi berikut:

   - Titik akhir SCIM
   - Token akses

   Kemudian dalam tutorial ini Anda memasukkan nilai-nilai ini untuk mengonfigurasi penyediaan. Google Workspace
4. Pilih Tutup.

   Sekarang setelah Anda menyiapkan penyediaan di konsol Pusat Identitas IAM, pada langkah berikutnya Anda menggunakan konektor Pusat Identitas IAM penyediaan Google Workspace otomatis untuk menyelesaikan tugas yang tersisa.

Langkah 7: Konfigurasikan penyediaan otomatis di Google Workspace

1. Masuk ke konsol Admin Google Anda menggunakan akun administrator, lalu navigasikan ke Apps > Web dan aplikasi seluler.
2. Pilih aplikasi Amazon Web Services.
3. Di bagian Auto provisioning, pilih Configure auto provisioning.
4. Pada prosedur sebelumnya, Anda menyalin nilai token Access di IAM Identity Center. Tempelkan nilai itu ke bidang Access token di Google Workspace dan pilih Lanjutkan. Juga, dalam prosedur sebelumnya, Anda menyalin nilai endpoint SCIM di IAM Identity Center. Tempelkan nilai itu ke bidang URL Endpoint. Pastikan Anda menghapus garis miring di akhir URL dan pilih Lanjutkan.
5. Verifikasi bahwa semua atribut Pusat Identitas IAM wajib (yang ditandai dengan*) dipetakan ke Google Cloud Directory atribut. Jika tidak, pilih panah bawah dan petakan ke atribut yang sesuai. Pilih Lanjutkan.

6. Dalam cakupan Penyediaan, Anda dapat memilih grup dengan Google Workspace direktori Anda untuk menyediakan akses ke aplikasi Amazon Web Services. Lewati langkah ini dan pilih Lanjutkan.
7. Di Deprovisioning, Anda dapat memilih cara merespons berbagai peristiwa yang menghapus akses dari pengguna. Untuk setiap situasi Anda dapat menentukan jumlah waktu sebelum deprovisioning mulai:

   - dalam waktu 24 jam
   - setelah satu hari
   - setelah tujuh hari
   - setelah 21 hari

   Setiap situasi memiliki pengaturan waktu kapan harus menangguhkan akses akun dan kapan harus menghapus akun.

   > **Tip**
   >
   > Selalu atur lebih banyak waktu sebelum menghapus akun pengguna daripada menangguhkan akun pengguna.

8. Pilih Selesai. Anda dikembalikan ke halaman aplikasi Amazon Web Services.
9. Di bagian Penyediaan otomatis, aktifkan sakelar sakelar untuk mengubahnya dari Tidak Aktif menjadi Aktif.

   > **Note**
   >
   > Penggeser aktivasi dinonaktifkan jika IAM Identity Center tidak diaktifkan untuk pengguna. Pilih Akses pengguna dan nyalakan aplikasi untuk mengaktifkan slider.

10. Di kotak dialog konfirmasi, pilih Aktifkan.
11. Untuk memverifikasi bahwa pengguna berhasil disinkronkan ke Pusat Identitas IAM, kembali ke konsol Pusat Identitas IAM dan pilih Pengguna. Halaman Pengguna mencantumkan pengguna dari Google Workspace direktori Anda yang dibuat oleh SCIM. Jika pengguna belum terdaftar, mungkin penyediaan masih dalam proses. Penyediaan dapat memakan waktu hingga 24 jam, meskipun dalam banyak kasus selesai dalam beberapa menit. Pastikan untuk menyegarkan jendela browser setiap beberapa menit.

Pilih pengguna dan lihat detailnya. Informasi tersebut cocok dengan informasi dalam Google Workspace direktori.

> **Selamat!**
>
> Anda telah berhasil mengatur koneksi SAMP antara Google Workspace dan AWS dan telah memverifikasi bahwa penyediaan otomatis berfungsi. Anda sekarang dapat menetapkan pengguna ini ke akun dan aplikasi di IAM Identity Center. Untuk tutorial ini, pada langkah berikutnya mari kita menunjuk salah satu pengguna sebagai administrator IAM Identity Center dengan memberikan mereka izin administratif ke akun manajemen.

Langkah 8: Berikan Google Workspace pengguna akses ke akun

1. Di panel navigasi Pusat Identitas IAM, di bawah izin Multi-akun, pilih. Akun AWS
2. Pada Akun AWShalaman, struktur Organisasi menampilkan akar organisasi Anda dengan akun Anda di bawahnya dalam hierarki. Pilih kotak centang untuk akun manajemen Anda, lalu pilih Tetapkan pengguna atau grup.
3. Tampilan alur kerja Tetapkan pengguna dan grup. Ini terdiri dari tiga langkah:

    a. Untuk Langkah 1: Pilih pengguna dan grup pilih pengguna yang akan melakukan fungsi pekerjaan administrator. Lalu pilih Selanjutnya.

    b. Untuk Langkah 2: Pilih set izin pilih Buat set izin untuk membuka tab baru yang memandu Anda melalui tiga sub-langkah yang terlibat dalam membuat set izin.

        i. Untuk Langkah 1: Pilih jenis set izin lengkapi yang berikut ini:

            - Dalam Jenis set izin, pilih Set izin yang telah ditentukan sebelumnya.
            - Dalam Kebijakan untuk set izin yang telah ditentukan, pilih AdministratorAccess.

            Pilih Berikutnya.

        ii. Untuk Langkah 2: Tentukan detail set izin, pertahankan pengaturan default, dan pilih Berikutnya.

            Pengaturan default membuat set izin bernama *`AdministratorAccess`*dengan durasi sesi diatur ke satu jam.

iii. Untuk Langkah 3: Tinjau dan buat, verifikasi bahwa jenis set Izin menggunakan kebijakan AWS terkelola AdministratorAccess. Pilih Buat. Pada halaman Set izin, pemberitahuan muncul memberi tahu Anda bahwa set izin telah dibuat. Anda dapat menutup tab ini di browser web Anda sekarang.

Pada tab Tetapkan pengguna dan grup browser, Anda masih pada Langkah 2: Pilih set izin dari mana Anda memulai alur kerja set izin buat.

Di area set Izin, pilih tombol Refresh. Set *AdministratorAccess*izin yang Anda buat muncul dalam daftar. Pilih kotak centang untuk set izin tersebut dan kemudian pilih Berikutnya.

c. Untuk Langkah 3: Tinjau dan kirimkan ulasan pengguna dan set izin yang dipilih, lalu pilih Kirim.

Halaman diperbarui dengan pesan bahwa Anda Akun AWS sedang dikonfigurasi. Tunggu sampai proses selesai.

Anda dikembalikan ke Akun AWS halaman. Pesan notifikasi memberi tahu Anda bahwa pesan Anda Akun AWS telah direvisi dan set izin yang diperbarui diterapkan. Saat pengguna masuk, mereka akan memiliki opsi untuk memilih peran. *AdministratorAccess*

> **Note**
>
> Sinkronisasi otomatis SCIM Google Workspace hanya mendukung pengguna penyediaan; grup tidak disediakan secara otomatis. Anda tidak dapat membuat grup untuk Google Workspace pengguna menggunakan AWS Management Console. Setelah menyediakan pengguna, Anda dapat membuat grup menggunakan operasi CLI atau API

Langkah 9: Konfirmasikan akses Google Workspace pengguna ke AWS sumber daya

1. Masuk Google menggunakan akun pengguna uji.
2. Pilih ikon Google apps peluncur (wafel).
3. Gulir ke bagian bawah daftar aplikasi tempat Google Workspace aplikasi kustom Anda berada. Dua aplikasi ditampilkan Amazon Web Services dan portalAWS akses.

4. Pilih aplikasi portalAWS akses. Anda masuk ke portal dan dapat melihat Akun AWS ikonnya. Perluas ikon itu untuk melihat daftar Akun AWS yang dapat diakses pengguna. Dalam tutorial ini Anda hanya bekerja dengan satu akun, jadi memperluas ikon hanya menampilkan satu akun.

   > **Note**
   >
   > Jika Anda memilih aplikasi Amazon Web Services, Anda akan menerima kesalahan SAMP. Aplikasi itu digunakan untuk Google Workspace pengguna yang telah disediakan sebagai pengguna IAM dan tutorial ini menyediakan pengguna Anda sebagai pengguna di IAM Google Workspace Identity Center.

5. Pilih akun untuk menampilkan set izin yang tersedia bagi pengguna. Dalam tutorial ini Anda membuat set AdministratorAccessizin.
6. Di samping set izin adalah tautan untuk jenis akses yang tersedia untuk set izin tersebut. Saat Anda membuat set izin, Anda menetapkan konsol manajemen dan akses terprogram diaktifkan, sehingga dua opsi tersebut ada. Pilih Konsol manajemen untuk membuka AWS Management Console.
7. Pengguna masuk ke konsol.

(Opsional) Melewati atribut untuk kontrol akses

Anda dapat menggunakan Atribut untuk kontrol akses fitur ini secara opsional di Pusat Identitas IAM untuk meneruskan `Attribute` elemen dengan `Name` atribut yang disetel ke. `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` Elemen ini memungkinkan Anda untuk meneruskan atribut sebagai tanda sesi dalam pernyataan SAML. Untuk informasi selengkapnya tentang tag sesi, lihat Melewati tag sesi AWS STSdi Panduan Pengguna IAM.

Untuk menyampaikan atribut sebagai tag sesi, sertakan elemen `AttributeValue` yang menentukan nilai tag. Misalnya, untuk meneruskan pasangan nilai kunci tag`CostCenter = blue`, gunakan atribut berikut.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Jika Anda perlu menambahkan beberapa atribut, sertakan `Attribute` elemen terpisah untuk setiap tag.

Langkah selanjutnya

Sekarang setelah Anda mengonfigurasi Google Workspace sebagai penyedia identitas dan pengguna yang disediakan di Pusat Identitas IAM, Anda dapat:

- Gunakan AWS CLI operasi atau CreateGroupAPI Identity Store create-group untuk membuat grup bagi pengguna Anda.

  Grup berguna saat menetapkan akses ke Akun AWS dan aplikasi. Daripada menetapkan setiap pengguna satu per satu, Anda memberikan izin ke grup. Kemudian, saat Anda menambah atau menghapus pengguna dari grup, pengguna secara dinamis mendapatkan atau kehilangan akses ke akun dan aplikasi yang Anda tetapkan ke grup.
- Mengkonfigurasi izin berdasarkan fungsi pekerjaan, lihat Membuat set izin.

  Set izin menentukan tingkat akses yang dimiliki pengguna dan grup ke file Akun AWS. Set izin disimpan di Pusat Identitas IAM dan dapat disediakan untuk satu atau lebih. Akun AWSAnda dapat menetapkan lebih dari satu izin yang disetel ke pengguna.

> **Note**
>
> Sebagai administrator Pusat Identitas IAM, Anda kadang-kadang perlu mengganti sertifikat iDP yang lebih lama dengan yang lebih baru. Misalnya, Anda mungkin perlu mengganti sertifikat iDP saat tanggal kedaluwarsa sertifikat mendekati. Proses penggantian sertifikat yang lebih lama dengan yang lebih baru disebut sebagai rotasi sertifikat. Pastikan untuk meninjau cara mengelola sertifikat SAMP untukGoogle Workspace.

Menggunakan IAM Identity Center untuk terhubung dengan Platform JumpCloud Direktori

IAM Identity Center mendukung penyediaan otomatis (sinkronisasi) informasi pengguna dari JumpCloud Directory Platform ke IAM Identity Center. Penyediaan ini menggunakan protokol System for Cross-domain Identity Management (SCIM) v2.0. Anda mengonfigurasi koneksi ini JumpCloud menggunakan titik akhir dan token akses IAM Identity Center SCIM Anda. Saat mengonfigurasi

sinkronisasi SCIM, Anda membuat pemetaan atribut pengguna JumpCloud ke atribut bernama di Pusat Identitas IAM. Hal ini menyebabkan atribut yang diharapkan cocok antara IAM Identity Center danJumpCloud.

Panduan ini didasarkan pada pada JumpCloud Juni 2021. Langkah-langkah untuk versi yang lebih baru dapat bervariasi. Panduan ini berisi beberapa catatan mengenai konfigurasi otentikasi pengguna melalui SAMP.

Langkah-langkah berikut memandu Anda melalui cara mengaktifkan penyediaan otomatis pengguna dan grup dari JumpCloud Pusat Identitas IAM menggunakan protokol SCIM.

> **Note**
>
> Sebelum Anda mulai menerapkan SCIM, kami sarankan Anda terlebih dahulu meninjau. Pertimbangan untuk menggunakan penyediaan otomatis Kemudian lanjutkan meninjau pertimbangan tambahan di bagian selanjutnya.

Topik

Prasyarat

Anda akan memerlukan yang berikut ini sebelum Anda dapat memulai:

- JumpCloudberlangganan atau uji coba gratis. Untuk mendaftar untuk kunjungan uji coba gratis JumpCloud.
- Akun yang diaktifkan Pusat Identitas IAM (gratis). Untuk informasi selengkapnya, lihat Mengaktifkan Pusat Identitas IAM.
- Sambungan SAMP dari JumpCloud akun Anda ke Pusat Identitas IAM, seperti yang dijelaskan dalam JumpClouddokumentasi untuk Pusat Identitas IAM.

- Kaitkan konektor Pusat Identitas IAM dengan grup yang ingin Anda izinkan akses ke AWS akun.

Pertimbangan SCIM

Berikut ini adalah pertimbangan saat menggunakan JumpCloud federasi untuk IAM Identity Center.

- Hanya grup yang terkait dengan konektor AWS Single Sign-On yang JumpCloud akan disinkronkan dengan SCIM.
- Hanya satu atribut nomor telepon yang dapat disinkronkan dan defaultnya adalah “telepon kerja.”
- Pengguna dalam JumpCloud direktori harus memiliki nama depan dan belakang yang dikonfigurasi untuk disinkronkan ke IAM Identity Center dengan SCIM.
- Atribut masih disinkronkan jika pengguna dinonaktifkan di IAM Identity Center tetapi masih aktif di. JumpCloud
- Anda dapat memilih untuk mengaktifkan sinkronisasi SCIM hanya untuk informasi pengguna dengan menghapus centang pada “Aktifkan pengelolaan Grup Pengguna dan keanggotaan Grup” di konektor.
- Jika ada pengguna yang ada di direktori Identity Center dengan nama pengguna dan email yang sama, pengguna akan ditimpa dan disinkronkan dengan SCIM dari. JumpCloud

Langkah 1: Aktifkan penyediaan di IAM Identity Center

Pada langkah pertama ini, Anda menggunakan konsol IAM Identity Center untuk mengaktifkan penyediaan otomatis.

Untuk mengaktifkan penyediaan otomatis di Pusat Identitas IAM

1. Setelah Anda menyelesaikan prasyarat, buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan di panel navigasi kiri.
3. Pada halaman Pengaturan, cari kotak Informasi penyediaan otomatis, lalu pilih Aktifkan. Ini segera memungkinkan penyediaan otomatis di IAM Identity Center dan menampilkan titik akhir SCIM dan informasi token akses yang diperlukan.
4. Dalam kotak dialog Penyediaan otomatis masuk, salin setiap nilai untuk opsi berikut. Anda harus menempelkannya nanti saat mengonfigurasi penyediaan di iDP Anda.

    a. Titik akhir SCIM

   b. Token akses
5. Pilih Tutup.

Sekarang setelah Anda menyiapkan penyediaan di konsol Pusat Identitas IAM, Anda harus menyelesaikan tugas yang tersisa menggunakan konektor JumpCloud IAM Identity Center. Langkah-langkah ini dijelaskan dalam prosedur berikut.

Langkah 2: Konfigurasikan penyediaan di JumpCloud

Gunakan prosedur berikut di konektor JumpCloud IAM Identity Center untuk mengaktifkan penyediaan dengan IAM Identity Center. Prosedur ini mengasumsikan bahwa Anda telah menambahkan konektor JumpCloud IAM Identity Center ke portal dan grup JumpCloud admin Anda. Jika Anda belum melakukannya, lihatPrasyarat, dan kemudian selesaikan prosedur ini untuk mengonfigurasi penyediaan SCIM.

Untuk mengonfigurasi penyediaan di JumpCloud

1. Buka konektor JumpCloud IAM Identity Center yang Anda instal sebagai bagian dari konfigurasi SAMP untuk JumpCloud (User Authentication > IAM Identity Center). Lihat Prasyarat.
2. Pilih konektor IAM Identity Center, lalu pilih tab ketiga Manajemen Identitas.
3. Centang kotak untuk Aktifkan pengelolaan Grup Pengguna dan keanggotaan Grup dalam aplikasi ini jika Anda ingin grup disinkronkan SCIM.
4. Klik Konfigurasi.
5. Pada prosedur sebelumnya, Anda menyalin nilai endpoint SCIM di IAM Identity Center. Tempelkan nilai itu ke bidang URL Dasar di konektor JumpCloud IAM Identity Center. Pastikan Anda menghapus garis miring ke depan di akhir URL.
6. Dari prosedur sebelumnya Anda menyalin nilai token Access di IAM Identity Center. Tempelkan nilai itu ke bidang Token Key di konektor JumpCloud IAM Identity Center.
7. Klik Aktifkan untuk menerapkan konfigurasi.
8. Pastikan Anda memiliki indikator hijau di sebelah Single Sign-On yang diaktifkan.
9. Pindah ke tab keempat Grup Pengguna dan periksa grup yang ingin Anda sediakan dengan SCIM.
10. Klik Simpan di bagian bawah setelah Anda selesai.
11. Untuk memverifikasi bahwa pengguna telah berhasil disinkronkan ke Pusat Identitas IAM, kembali ke konsol Pusat Identitas IAM dan pilih Pengguna. Pengguna yang disinkronkan

JumpCloud muncul di halaman Pengguna. Pengguna ini sekarang dapat ditugaskan ke akun dalam IAM Identity Center.

(Opsional) Langkah 3: Konfigurasikan atribut pengguna JumpCloud untuk kontrol akses di Pusat Identitas IAM

Ini adalah prosedur opsional jika JumpCloud Anda memilih untuk mengkonfigurasi atribut untuk IAM Identity Center untuk mengelola akses ke AWS sumber daya Anda. Atribut yang Anda tentukan JumpCloud diteruskan dalam pernyataan SAMP ke IAM Identity Center. Anda kemudian membuat set izin di Pusat Identitas IAM untuk mengelola akses berdasarkan atribut yang Anda lewati. JumpCloud

Sebelum Anda memulai prosedur ini, Anda harus terlebih dahulu mengaktifkan fitur Attributes for access control. Untuk informasi selengkapnya tentang cara melakukannya, lihat Mengaktifkan dan mengonfigurasi atribut untuk kontrol akses.

Untuk mengonfigurasi atribut pengguna JumpCloud untuk kontrol akses di Pusat Identitas IAM

1. Buka konektor JumpCloud IAM Identity Center yang Anda instal sebagai bagian dari konfigurasi SAMP untuk JumpCloud (User Authentication > IAM Identity Center).
2. Pilih konektor IAM Identity Center. Kemudian, pilih tab kedua IAM Identity Center.
3. Di bagian bawah tab ini Anda memiliki Pemetaan Atribut Pengguna, pilih Tambahkan atribut baru, dan kemudian lakukan hal berikut: Anda harus melakukan langkah-langkah ini untuk setiap atribut yang akan Anda tambahkan untuk digunakan di Pusat Identitas IAM untuk kontrol akses.

    a. Di bidang Service Provide Attribute Name, masukkan `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`**`.` Ganti **`AttributeName`** dengan nama atribut yang Anda harapkan di Pusat Identitas IAM. Misalnya, `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Email`**.

    b. Di bidang Nama JumpCloud Atribut, pilih atribut pengguna dari JumpCloud direktori Anda. Misalnya, Email (Kerja).
4. Pilih Simpan.

(Opsional) Melewati atribut untuk kontrol akses

Anda dapat menggunakan Atribut untuk kontrol akses fitur ini secara opsional di Pusat Identitas IAM untuk meneruskan `Attribute` elemen dengan `Name` atribut yang disetel ke. `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` Elemen ini memungkinkan Anda untuk meneruskan atribut sebagai tanda sesi dalam pernyataan SAML. Untuk informasi selengkapnya tentang tag sesi, lihat Melewati tag sesi AWS STS di Panduan Pengguna IAM.

Untuk menyampaikan atribut sebagai tag sesi, sertakan elemen `AttributeValue` yang menentukan nilai tag. Misalnya, untuk meneruskan pasangan nilai kunci tag`CostCenter = blue`, gunakan atribut berikut.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Jika Anda perlu menambahkan beberapa atribut, sertakan `Attribute` elemen terpisah untuk setiap tag.

Konfigurasikan SAMP dan SCIM dengan Microsoft Entra ID dan IAM Identity Center

AWS IAM Identity Centermendukung integrasi dengan Security Assertion Markup Language (SAMP) 2.0 serta penyediaan otomatis (sinkronisasi) informasi pengguna dan grup dari Microsoft Entra ID (sebelumnya dikenal sebagai Azure Active Directory atau) ke IAM Identity Center menggunakan protokol System for Cross-domain Identity Management (SCIMAzure AD) 2.0.

Objektif

Dalam tutorial ini, Anda akan menyiapkan lab uji dan mengkonfigurasi koneksi SAMP dan penyediaan SCIM antara Microsoft Entra ID dan IAM Identity Center. Selama langkah persiapan awal, Anda akan membuat pengguna uji (Nikki Wolf) di keduanya Microsoft Entra ID dan IAM Identity Center yang akan Anda gunakan untuk menguji koneksi SAMP di kedua arah. Kemudian, sebagai bagian dari langkah-langkah SCIM, Anda akan membuat pengguna uji yang berbeda (Richard Roe) untuk memverifikasi bahwa atribut baru disinkronkan ke IAM Identity Center seperti yang diharapkan. Microsoft Entra ID

Prasyarat

Sebelum Anda dapat memulai dengan tutorial ini, Anda harus terlebih dahulu mengatur yang berikut:

- Microsoft Entra IDPenyewa. Untuk informasi selengkapnya, lihat Mulai cepat: Mengatur penyewa di situs web Microsoft.
- Akun AWS IAM Identity Center yang diaktifkan. Untuk informasi selengkapnya, lihat Mengaktifkan Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Langkah 1: Siapkan penyewa Microsoft Anda

Pada langkah ini, Anda akan menelusuri cara menginstal dan mengkonfigurasi aplikasi AWS IAM Identity Center perusahaan Anda dan menetapkan akses ke pengguna Microsoft Entra ID uji yang baru dibuat.

Step 1.1 >

Langkah 1.1: Siapkan aplikasi AWS IAM Identity Center perusahaan di Microsoft Entra ID

Dalam prosedur ini, Anda menginstal aplikasi AWS IAM Identity Center perusahaan diMicrosoft Entra ID. Anda akan memerlukan aplikasi ini nanti untuk mengkonfigurasi koneksi SAFL Anda denganAWS.

1. Masuk ke pusat admin Microsoft Entra setidaknya sebagai Administrator Aplikasi Cloud.
2. Arahkan ke Identity > Applications > Enterprise Applications, lalu pilih New Application.
3. Pada halaman Browse Microsoft Entra Gallery, masukkan **`AWS IAM Identity Center`**di kotak pencarian.
4. Pilih AWS IAM Identity Centerdari area hasil.
5. Pilih Buat.

Step 1.2 >

Langkah 1.2: Buat pengguna uji di Microsoft Entra ID

Nikki Wolf adalah nama pengguna Microsoft Entra ID uji Anda yang akan Anda buat dalam prosedur ini.

1. Di konsol pusat admin Microsoft Entra, navigasikan ke Identity > Users > All users.

2. Pilih Pengguna baru, lalu pilih Buat pengguna baru di bagian atas layar.
3. Di Nama utama pengguna, masukkan **`NikkiWolf`**, lalu pilih domain dan ekstensi pilihan Anda. Misalnya, NikkiWolf@ *`example.org`*.
4. Di Nama tampilan, masukkan **`NikkiWolf`**.
5. Di Kata Sandi, masukkan kata sandi yang kuat atau pilih ikon mata untuk menampilkan kata sandi yang dibuat secara otomatis, dan salin atau tuliskan nilai yang ditampilkan.
6. Pilih Properti, di Nama depan, masukkan **`Nikki`**. Di Nama belakang, masukkan **`Wolf`**.
7. Pilih Review + create, lalu pilih Create.

Step 1.3

Langkah 1.3: Uji pengalaman Nikki sebelum menetapkan izinnya AWS IAM Identity Center

Dalam prosedur ini, Anda akan memverifikasi apa yang Nikki berhasil masuk ke portal Microsoft My Account-nya.

1. Di browser yang sama, buka tab baru, buka halaman masuk portal Akun Saya, dan masukkan alamat email lengkap Nikki. Misalnya, NikkiWolf@ *`example.org`*.
2. Saat diminta, masukkan kata sandi Nikki, lalu pilih Masuk. Jika ini adalah kata sandi yang dibuat secara otomatis, Anda akan diminta untuk mengubah kata sandi.
3. Pada halaman Action Required, pilih Tanya nanti untuk melewati prompt untuk metode keamanan tambahan.
4. Di halaman Akun saya, di navigasi kiri, pilih Aplikasi Saya. Perhatikan bahwa selain Add-in, tidak ada aplikasi yang ditampilkan saat ini. Anda akan menambahkan AWS IAM Identity Centeraplikasi yang akan muncul di sini di langkah selanjutnya.

Step 1.4

Langkah 1.4: Tetapkan izin ke Nikki di Microsoft Entra ID

Sekarang setelah Anda memverifikasi bahwa Nikki berhasil mengakses portal Akun saya, gunakan prosedur ini untuk menetapkan penggunanya ke aplikasi. AWS IAM Identity Center

1. Di konsol pusat admin Microsoft Entra, navigasikan ke Identity > Applications > Enterprise Applications dan kemudian pilih AWS IAM Identity Centerdari daftar.
2. Di sebelah kiri, pilih Pengguna dan grup.

3. Pilih Tambahkan pengguna/grup. Anda dapat mengabaikan pesan yang menyatakan bahwa grup tidak tersedia untuk penetapan. Tutorial ini tidak menggunakan grup untuk tugas.
4. Pada halaman Tambahkan Penugasan, di bawah Pengguna, pilih Tidak Ada yang Dipilih.
5. Pilih NikkiWolf, lalu pilih Pilih.
6. Pada halaman Add Assignment, pilih Assign. NikkiWolf sekarang muncul di daftar pengguna yang ditugaskan ke AWS IAM Identity Centeraplikasi.

Langkah 2: Siapkan AWS akun Anda

Pada langkah ini, Anda akan menelusuri cara menggunakan IAM Identity Centeruntuk mengonfigurasi izin akses (melalui set izin), membuat pengguna Nikki Wolf yang sesuai secara manual, dan memberinya izin yang diperlukan untuk mengelola sumber daya. AWS

Step 2.1 >

Langkah 2.1: Buat RegionalAdmin izin yang ditetapkan IAM Identity Center

Set izin ini akan digunakan untuk memberikan Nikki izin AWS akun yang diperlukan yang diperlukan untuk mengelola Wilayah dari halaman Akun di dalam. AWS Management Console Semua izin lain untuk melihat atau mengelola informasi lain untuk akun Nikki ditolak secara default.

1. Buka konsol Pusat Identitas IAM.
2. Di bawah Izin multi-akun, pilih Set izin.
3. Pilih Buat set izin.
4. Pada halaman Pilih jenis set izin, pilih Set izin khusus, lalu pilih Berikutnya.
5. Pilih Kebijakan sebaris untuk memperluasnya, lalu buat kebijakan untuk set izin menggunakan langkah-langkah berikut:

   a. Pilih Tambahkan pernyataan baru untuk membuat pernyataan kebijakan.

   b. Di bawah Edit pernyataan, pilih Akun dari daftar, lalu pilih kotak centang berikut.

      - **`ListRegions`**
      - **`GetRegionOptStatus`**
      - **`DisableRegion`**
      - **`EnableRegion`**

c. Di samping Tambahkan sumber daya, pilih Tambah.

d. Pada halaman Tambahkan sumber daya, di bawah Jenis sumber daya, pilih Semua Sumber Daya, lalu pilih Tambah sumber daya. Verifikasi bahwa kebijakan Anda terlihat seperti berikut:

```
{
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": [
                "account:ListRegions",
                "account:DisableRegion",
                "account:EnableRegion",
                "account:GetRegionOptStatus"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

6. Pilih Berikutnya.
7. Pada halaman Tentukan detail set izin, di bawah Nama set izin **`RegionalAdmin`**, masukkan, lalu pilih Berikutnya.
8. Pada halaman Tinjau dan buat, pilih Buat. Anda akan melihat RegionalAdminditampilkan dalam daftar set izin.

Step 2.2 >

Langkah 2.2: Buat NikkiWolf pengguna yang sesuai di IAM Identity Center

Karena protokol SAMP tidak menyediakan mekanisme untuk menanyakan IDP Microsoft Entra ID () dan secara otomatis membuat pengguna di sini di IAM Identity Center, gunakan prosedur berikut untuk membuat pengguna secara manual di IAM Identity Center yang mencerminkan atribut inti dari pengguna Nikki Wolfs di. Microsoft Entra ID

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengguna, pilih Tambahkan pengguna, lalu berikan informasi berikut:

a. Untuk Nama Pengguna dan Alamat Email — Masukkan **NikkiWolf@*yourcompanydomain.extension*** yang sama dengan yang Anda gunakan saat membuat pengguna Anda. Microsoft Entra ID Misalnya, NikkiWolf@ *example.org*.

b. Konfirmasikan alamat email — Masukkan kembali alamat email dari langkah sebelumnya

c. Nama depan — Enter **Nikki**

d. Nama belakang — Enter **Wolf**

e. Nama tampilan - Enter **Nikki Wolf**

3. Pilih Berikutnya dua kali, lalu pilih Tambah pengguna.
4. Pilih Tutup.

Step 2.3

Langkah 2.3: Tetapkan Nikki ke RegionalAdmin izin yang ditetapkan IAM Identity Center

Di sini Anda menemukan tempat Nikki akan mengelola Wilayah, dan kemudian menetapkan izin yang diperlukan agar dia berhasil mengakses portal akses. Akun AWS AWS

1. Buka konsol Pusat Identitas IAM.
2. Di bawah Izin multi-akun, pilih. Akun AWS
3. Pilih kotak centang di samping nama akun (misalnya, *Kotak Pasir*) tempat Anda ingin memberi Nikki akses untuk mengelola Wilayah, lalu pilih Tetapkan pengguna dan grup.
4. Pada halaman Tetapkan pengguna dan grup, pilih tab Pengguna, temukan dan centang kotak di sebelah Nikki, lalu pilih Berikutnya.

Langkah 3: Konfigurasikan dan uji koneksi SAFL Anda

Pada langkah ini, Anda mengonfigurasi koneksi SAMP Anda menggunakan aplikasi AWS IAM Identity Center perusahaan Microsoft Entra ID bersama dengan pengaturan iDP eksternal di IAM Identity Center.

Step 3.1 >

Langkah 3.1: Kumpulkan metadata penyedia layanan yang diperlukan dari IAM Identity Center

Pada langkah ini, Anda akan meluncurkan panduan Ubah sumber identitas dari dalam konsol Pusat Identitas IAM dan mengambil file metadata dan URL masuk AWS tertentu yang harus Anda masukkan saat mengonfigurasi koneksi di langkah berikutnya. Microsoft Entra ID

1. Di konsol Pusat Identitas IAM, pilih Pengaturan.
2. Pada halaman Pengaturan, pilih tab Sumber identitas, lalu pilih Tindakan > Ubah sumber identitas.
3. Pada halaman Pilih sumber identitas, pilih Penyedia identitas eksternal, lalu pilih Berikutnya.
4. Pada halaman Konfigurasi penyedia identitas eksternal, di bawah metadata penyedia layanan, pilih Unduh file metadata untuk mengunduhnya di sistem Anda.
5. Di bagian yang sama, cari nilai URL masuk portal AWS akses dan salin. Anda harus memasukkan nilai ini saat diminta pada langkah berikutnya.
6. Biarkan halaman ini terbuka, dan lanjutkan ke langkah berikutnya (**`Step 3.2`**) untuk mengonfigurasi aplikasi AWS IAM Identity Center perusahaanMicrosoft Entra ID. Kemudian, Anda akan kembali ke halaman ini untuk menyelesaikan prosesnya.

Step 3.2 >

Langkah 3.2: Konfigurasikan aplikasi AWS IAM Identity Center perusahaan di Microsoft Entra ID

Prosedur ini menetapkan setengah dari koneksi SAMP di sisi Microsoft menggunakan nilai dari file metadata dan URL Sign-On yang Anda peroleh pada langkah terakhir.

1. Di konsol pusat admin Microsoft Entra, navigasikan ke Identity > Applications > Enterprise Applications dan kemudian pilih AWS IAM Identity Center.
2. Di sebelah kiri, pilih Single sign-on.
3. Pada halaman Set up Single Sign-On with SAMP, pilih Upload file metadata, pilih ikon folder, pilih file metadata penyedia layanan yang Anda unduh pada langkah sebelumnya, lalu pilih Tambah.
4. Pada halaman Konfigurasi SAMP Dasar, verifikasi bahwa nilai URL Pengenal dan Balas sekarang menunjuk ke titik akhir di awal AWS itu. `https://<REGION>.signin.aws.amazon.com/platform/saml/`
5. Di bawah URL Masuk (Opsional), tempel nilai URL masuk portal AWS akses yang Anda salin di langkah sebelumnya (**`Step 3.1`**), pilih Simpan, lalu pilih X untuk menutup jendela.

6. Jika diminta untuk menguji sistem masuk tunggalAWS IAM Identity Center, pilih Tidak, saya akan menguji nanti. Anda akan melakukan verifikasi ini di langkah selanjutnya.
7. Pada halaman Set up Single Sign-On with SAMP, di bagian SAMP Certificates, di sebelah Federation Metadata XHTML, pilih Download untuk menyimpan file metadata ke sistem Anda. Anda harus mengunggah file ini saat diminta pada langkah berikutnya.

Step 3.3 **>**

Langkah 3.3: Konfigurasikan iDP Microsoft Entra ID eksternal di AWS IAM Identity Center

Di sini Anda akan kembali ke wizard Ubah sumber identitas di konsol Pusat Identitas IAM untuk menyelesaikan paruh kedua koneksi SAMP di. AWS

1. Kembali ke sesi browser yang Anda biarkan terbuka **`Step 3.1`**di konsol Pusat Identitas IAM.
2. Pada halaman Konfigurasi penyedia identitas eksternal, di bagian metadata penyedia identitas, di bawah metadata IDP SAMP, pilih tombol Pilih file, dan pilih file metadata penyedia identitas yang Anda unduh dari Microsoft Entra ID langkah sebelumnya, lalu pilih Buka.
3. Pilih Berikutnya.
4. Setelah Anda membaca disclaimer dan siap untuk melanjutkan, masukkan. **`ACCEPT`**
5. Pilih Ubah sumber identitas untuk menerapkan perubahan Anda.

Step 3.4 **>**

Langkah 3.4: Uji bahwa Nikki diarahkan ke portal akses AWS

Dalam prosedur ini, Anda akan menguji koneksi SAMP dengan masuk ke portal Akun Saya Microsoft dengan kredensi Nikki. Setelah diautentikasi, Anda akan memilih AWS IAM Identity Center aplikasi yang akan mengarahkan Nikki ke portal akses. AWS

1. Buka halaman masuk portal Akun Saya, dan masukkan alamat email lengkap Nikki. Misalnya, ***`NikkiWolf`***@ *`example.org`*.
2. Saat diminta, masukkan kata sandi Nikki, lalu pilih Masuk.
3. Di halaman Akun saya, di navigasi kiri, pilih Aplikasi Saya.
4. Pada halaman Aplikasi Saya, pilih aplikasi bernama AWS IAM Identity Center. Ini akan meminta Anda untuk otentikasi tambahan.

5. Pada halaman masuk Microsoft, pilih NikkiWolf kredensil Anda. Jika diminta untuk kedua kalinya untuk otentikasi, pilih NikkiWolf kredensyal Anda lagi. Ini akan secara otomatis mengarahkan Anda ke portal AWS akses.

   > **Tip**
   >
   > Jika Anda tidak berhasil dialihkan, periksa untuk memastikan nilai URL masuk portal AWS akses yang Anda masukkan **`Step 3.2`**cocok dengan nilai yang Anda salin. **`Step 3.1`**

6. Verifikasi bahwa Anda melihat ikon AWSAkun

   ditampilkan.

   > **Tip**
   >
   > Jika halaman kosong dan tidak ada ikon AWSAkun yang ditampilkan, konfirmasikan bahwa Nikki berhasil ditetapkan ke set RegionalAdminizin (lihat **`Step 2.3`**).

Step 3.5

Langkah 3.5: Uji tingkat akses Nikki untuk mengelolanya Akun AWS

Pada langkah ini, Anda akan memeriksa untuk menentukan tingkat akses Nikki untuk mengelola pengaturan Wilayah untuknyaAkun AWS. Nikki seharusnya hanya memiliki hak administrator yang cukup untuk mengelola Wilayah dari halaman Akun.

1. Di portal AWS akses, pilih ikon AWSAkun

   untuk memperluas daftar akun. Setelah memilih ikon, nama akun, ID akun, dan alamat email yang terkait dengan akun mana pun yang menetapkan set izin akan muncul.
2. Pilih nama akun (misalnya, *`Sandbox`*) tempat Anda menerapkan set izin (lihat **`Step 2.3`**). Ini akan memperluas daftar set izin yang dapat dipilih Nikki untuk mengelola akunnya.
3. Di samping RegionalAdminmemilih Konsol manajemen untuk mengambil peran yang Anda tetapkan dalam set RegionalAdminizin. Ini akan mengarahkan Anda ke halaman AWS Management Console beranda.

4. Di sudut kanan atas konsol, pilih nama akun Anda, lalu pilih Akun. Ini akan membawa Anda ke halaman Akun. Perhatikan bahwa semua bagian lain di halaman ini menampilkan pesan bahwa Anda tidak memiliki izin yang diperlukan untuk melihat atau mengubah pengaturan tersebut.
5. Pada halaman Akun, gulir ke bawah ke bagian AWSWilayah. Pilih kotak centang untuk Wilayah yang tersedia di tabel. Perhatikan bahwa Nikki memang memiliki izin yang diperlukan untuk Mengaktifkan atau Menonaktifkan daftar Wilayah untuk akunnya seperti yang dimaksudkan.

> Dilakukan dengan baik!
>
> Langkah 1 hingga 3 membantu Anda untuk berhasil menerapkan dan menguji koneksi SAMB Anda. Sekarang, untuk menyelesaikan tutorial, kami mendorong Anda untuk beralih ke Langkah 4 untuk menerapkan penyediaan otomatis.

Langkah 4: Konfigurasikan dan uji sinkronisasi SCIM Anda

Pada langkah ini, Anda akan mengatur penyediaan otomatis (sinkronisasi) informasi pengguna dari Microsoft Entra ID ke Pusat Identitas IAM menggunakan protokol SCIM v2.0. Anda mengonfigurasi koneksi ini Microsoft Entra ID menggunakan endpoint SCIM Anda untuk IAM Identity Center dan token pembawa yang dibuat secara otomatis oleh IAM Identity Center.

Saat mengonfigurasi sinkronisasi SCIM, Anda membuat pemetaan atribut pengguna Microsoft Entra ID ke atribut bernama di Pusat Identitas IAM. Hal ini menyebabkan atribut yang diharapkan cocok antara IAM Identity Center danMicrosoft Entra ID.

Langkah-langkah berikut memandu Anda melalui cara mengaktifkan penyediaan otomatis pengguna yang terutama berada di Microsoft Entra ID Pusat Identitas IAM menggunakan aplikasi Pusat Identitas IAM di. Microsoft Entra ID

Step 4.1 >

Langkah 4.1: Buat pengguna uji kedua di Microsoft Entra ID

Untuk tujuan pengujian, Anda akan membuat pengguna baru (Richard Roe) diMicrosoft Entra ID. Kemudian, setelah Anda mengatur sinkronisasi SCIM, Anda akan menguji bahwa pengguna ini dan semua atribut yang relevan berhasil disinkronkan ke IAM Identity Center.

1. Di konsol pusat admin Microsoft Entra, navigasikan ke Identity > Users > All users.
2. Pilih Pengguna baru, lalu pilih Buat pengguna baru di bagian atas layar.
3. Di Nama utama pengguna, masukkan **RichRoe**, lalu pilih domain dan ekstensi pilihan Anda. Misalnya, RichRoe@ *example.org*.
4. Di Nama tampilan, masukkan **RichRoe**.
5. Di Kata Sandi, masukkan kata sandi yang kuat atau pilih ikon mata untuk menampilkan kata sandi yang dibuat secara otomatis, dan salin atau tuliskan nilai yang ditampilkan.
6. Pilih Properties, dan kemudian berikan nilai-nilai berikut:
   - Nama depan - Enter **Richard**
   - Nama belakang - Enter **Roe**
   - Judul Pekerjaan - Enter **Marketing Lead**
   - Departemen - Masuk **Sales**
   - ID Karyawan - Masukkan **12345**
7. Pilih Review + create, lalu pilih Create.

Step 4.2 >

Langkah 4.2: Aktifkan penyediaan otomatis di IAM Identity Center

Dalam prosedur ini, Anda akan menggunakan konsol Pusat Identitas IAM untuk mengaktifkan penyediaan otomatis pengguna dan grup yang berasal dari Microsoft Entra ID Pusat Identitas IAM.

1. Buka konsol Pusat Identitas IAM, dan pilih Pengaturan di panel navigasi kiri.
2. Pada halaman Pengaturan, di bawah tab Sumber identitas, perhatikan bahwa metode Penyediaan diatur ke Manual.
3. Temukan kotak Informasi penyediaan otomatis, lalu pilih Aktifkan. Ini segera memungkinkan penyediaan otomatis di IAM Identity Center dan menampilkan titik akhir SCIM dan informasi token akses yang diperlukan.
4. Dalam kotak dialog Penyediaan otomatis masuk, salin setiap nilai untuk opsi berikut. Anda harus menempelkan ini di langkah berikutnya saat Anda mengonfigurasi penyediaan. Microsoft Entra ID

a. Titik akhir SCIM - Misalnya, https://scim. *us-east-2 .amazonaws.com/ 111111111-2222-3333-4444-555555555555 /scim/v2/*

b. Token akses - Pilih Tampilkan token untuk menyalin nilainya.

5. Pilih Tutup
6. Di bawah tab Identity source, perhatikan bahwa metode Provisioning sekarang diatur ke SCIM.

Step 4.3 >

Langkah 4.3: Konfigurasikan penyediaan otomatis di Microsoft Entra ID

Sekarang setelah Anda memiliki pengguna RichRoe pengujian dan telah mengaktifkan SCIM di IAM Identity Center, Anda dapat melanjutkan dengan mengonfigurasi pengaturan sinkronisasi SCIM di. Microsoft Entra ID

1. Di konsol pusat admin Microsoft Entra, navigasikan ke Identity > Applications > Enterprise Applications dan kemudian pilih AWS IAM Identity Center.
2. Pilih Penyediaan, di bawah Kelola, pilih Penyediaan lagi.
3. Dalam Mode Penyediaan pilih Otomatis.
4. Di bawah Kredensial Admin, di URL Penyewa tempel di nilai URL titik akhir SCIM yang Anda salin sebelumnya. **`Step 4.1`** Di Token Rahasia, tempel nilai token Access.
5. Pilih Uji Koneksi . Anda akan melihat pesan yang menunjukkan bahwa kredenal yang diuji berhasil diotorisasi untuk mengaktifkan penyediaan.
6. Pilih Simpan.
7. Di bawah Kelola, pilih Pengguna dan grup, lalu pilih Tambahkan pengguna/grup.
8. Pada halaman Tambahkan Penugasan, di bawah Pengguna, pilih Tidak Ada yang Dipilih.
9. Pilih RichRoe, lalu pilih Pilih.
10. Pada halaman Add Assignment, pilih Assign.
11. Pilih Ikhtisar, lalu pilih Mulai penyediaan.

Step 4.4

Langkah 4.4: Verifikasi bahwa sinkronisasi terjadi

Di bagian ini, Anda akan memverifikasi bahwa pengguna Richard berhasil disediakan dan bahwa semua atribut ditampilkan di Pusat Identitas IAM.

1. Di konsol Pusat Identitas IAM, pilih Pengguna.
2. Pada halaman Pengguna, Anda akan melihat RichRoepengguna Anda ditampilkan. Perhatikan bahwa di kolom Dibuat oleh nilai diatur ke SCIM.
3. Pilih RichRoe, di bawah Profil, verifikasi bahwa atribut berikut telah disalinMicrosoft Entra ID.

   - Nama depan - **`Richard`**
   - Nama belakang - **`Roe`**
   - Departemen - **`Sales`**
   - Judul - **`Marketing Lead`**
   - Nomor karyawan - **`12345`**

   Sekarang pengguna Richard telah dibuat di IAM Identity Center, Anda dapat menetapkannya ke set izin apa pun sehingga Anda dapat mengontrol tingkat akses yang dia miliki ke sumber daya AndaAWS. Misalnya, Anda dapat menetapkan RichRoeke set **`RegionalAdmin`** izin yang Anda gunakan sebelumnya untuk memberikan Nikki izin untuk mengelola Wilayah (lihat **`Step 2.3`**) dan kemudian menguji tingkat aksesnya menggunakan. **`Step 3.5`**

> Selamat!
>
> Anda telah berhasil mengatur koneksi SAMP antara Microsoft dan AWS dan telah memverifikasi bahwa penyediaan otomatis berfungsi untuk menjaga semuanya tetap sinkron. Sekarang Anda dapat menerapkan apa yang telah Anda pelajari untuk mengatur lingkungan produksi Anda dengan lebih lancar.

Pertimbangan untuk menggunakan SCIM dengan Microsoft Entra ID dalam lingkungan produksi

Berikut ini adalah pertimbangan penting tentang hal Microsoft Entra ID itu dapat memengaruhi cara Anda berencana untuk menerapkan penyediaan otomatis dengan IAM Identity Center di lingkungan produksi Anda menggunakan protokol SCIM v2.

> **Note**
>
> Sebelum Anda mulai menerapkan SCIM, kami sarankan Anda meninjau terlebih dahulu. Pertimbangan untuk menggunakan penyediaan otomatis

Atribut untuk kontrol akses

Atribut untuk kontrol akses digunakan dalam kebijakan izin yang menentukan siapa di sumber identitas Anda yang dapat mengakses AWS sumber daya Anda. Jika atribut dihapus dari pengguna diMicrosoft Entra ID, atribut itu tidak akan dihapus dari pengguna terkait di Pusat Identitas IAM. Ini adalah batasan yang diketahui dalamMicrosoft Entra ID. Jika atribut diubah ke nilai yang berbeda (tidak kosong) pada pengguna, perubahan itu akan disinkronkan ke Pusat Identitas IAM.

Grup Bersarang

Layanan penyediaan Microsoft Entra ID pengguna tidak dapat membaca atau menyediakan pengguna dalam grup bersarang. Hanya pengguna yang merupakan anggota langsung dari grup yang ditetapkan secara eksplisit yang dapat dibaca dan disediakan. Microsoft Entra IDtidak secara rekursif membongkar keanggotaan grup dari pengguna atau grup yang ditetapkan secara tidak langsung (pengguna atau grup yang merupakan anggota grup yang ditugaskan secara langsung). Untuk informasi selengkapnya, lihat Pelingkupan berbasis tugas dalam dokumentasi. Microsoft Entra ID

Grup Dinamis

Layanan penyediaan Microsoft Entra ID pengguna dapat membaca dan menyediakan pengguna dalam grup dinamis. Lihat di bawah untuk contoh yang menunjukkan struktur pengguna dan grup saat menggunakan grup dinamis dan bagaimana mereka ditampilkan di Pusat Identitas IAM. Pengguna dan grup ini disediakan dari Microsoft Entra ID Pusat Identitas IAM melalui SCIM

Misalnya, jika Microsoft Entra ID struktur untuk grup dinamis adalah sebagai berikut:

1. Grup A dengan anggota ua1, ua2
2. Grup B dengan anggota ub1
3. Grup C dengan anggota uc1
4. Grup K dengan aturan untuk memasukkan anggota Grup A, B, C
5. Grup L dengan aturan untuk memasukkan anggota Grup B dan C

Setelah informasi pengguna dan grup disediakan dari Microsoft Entra ID Pusat Identitas IAM melalui SCIM, strukturnya adalah sebagai berikut:

1. Grup A dengan anggota ua1, ua2
2. Grup B dengan anggota ub1
3. Grup C dengan anggota uc1
4. Grup K dengan anggota ua1, ua2, ub1, uc1
5. Grup L dengan anggota ub1, uc1

Saat Anda mengonfigurasi penyediaan otomatis menggunakan grup dinamis, ingatlah pertimbangan berikut.

- Grup dinamis dapat mencakup grup bersarang. Namun, layanan Microsoft Entra ID penyediaan tidak meratakan grup bersarang. Misalnya, jika Anda memiliki Microsoft Entra ID struktur berikut untuk grup dinamis:
  - Grup A adalah induk dari kelompok B.
  - Grup A memiliki ua1 sebagai anggota.
  - Grup B memiliki ub1 sebagai anggota.

Grup dinamis yang mencakup Grup A hanya akan mencakup anggota langsung grup A (yaitu, ua1). Ini tidak akan secara rekursif mencakup anggota grup B.

- Grup dinamis tidak dapat berisi grup dinamis lainnya. Untuk informasi selengkapnya, lihat Pratinjau batasan dalam Microsoft Entra ID dokumentasi.

Memecahkan masalah SCIM dengan Microsoft Entra ID

Jika Anda mengalami masalah dengan Microsoft Entra ID pengguna yang tidak melakukan sinkronisasi ke Pusat Identitas IAM, mungkin karena masalah sintaks yang ditandai oleh IAM Identity Center saat pengguna baru ditambahkan ke IAM Identity Center. Anda dapat mengonfirmasi hal ini dengan memeriksa log Microsoft Entra ID audit untuk peristiwa yang gagal, seperti `'Export'`. Alasan Status untuk acara ini akan menyatakan:

```
{"schema":["urn:ietf:params:scim:api:messages:2.0:Error"],"detail":"Request is
 unparsable, syntactically incorrect, or violates schema.","status":"400"}
```

Anda juga dapat memeriksa AWS CloudTrail acara yang gagal. Ini dapat dilakukan dengan mencari di konsol Riwayat Acara CloudTrail menggunakan filter berikut:

```
"eventName":"CreateUser"
```

Kesalahan dalam CloudTrail acara tersebut akan menyatakan sebagai berikut:

```
"errorCode": "ValidationException",
        "errorMessage": "Currently list attributes only allow single item“
```

Pada akhirnya, pengecualian ini berarti bahwa salah satu nilai yang dilewatkan Microsoft Entra ID mengandung lebih banyak nilai daripada yang diantisipasi. Solusinya di sini adalah meninjau atribut penggunaMicrosoft Entra ID, memastikan bahwa tidak ada yang mengandung nilai duplikat. Salah satu contoh umum dari nilai duplikat adalah memiliki beberapa nilai yang ada untuk nomor kontak seperti ponsel, pekerjaan, dan faks. Meskipun nilai terpisah, mereka semua diteruskan ke IAM Identity Center di bawah atribut induk tunggal PhoneNumbers.

Untuk tips pemecahan masalah SCIM umum, lihat. Memecahkan masalah Pusat Identitas IAM

Langkah 5: (Opsional) Konfigurasikan ABAC

Sekarang setelah Anda berhasil mengkonfigurasi SAMP dan SCIM, Anda dapat memilih untuk mengonfigurasi kontrol akses berbasis atribut (ABAC). ABAC adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut.

DenganMicrosoft Entra ID, Anda dapat menggunakan salah satu dari dua metode berikut untuk mengkonfigurasi ABAC untuk digunakan dengan IAM Identity Center.

Method 1

> Metode 1: Konfigurasikan atribut pengguna Microsoft Entra ID untuk kontrol akses di Pusat Identitas IAM
>
> Dalam prosedur berikut, Anda akan menentukan atribut mana yang Microsoft Entra ID harus digunakan oleh IAM Identity Center untuk mengelola akses ke AWS sumber daya Anda. Setelah ditentukan, Microsoft Entra ID kirimkan atribut ini ke IAM Identity Center melalui pernyataan SAMB. Anda kemudian perlu Buat set izin di IAM Identity Center untuk mengelola akses berdasarkan atribut yang Anda lewati. Microsoft Entra ID

Sebelum Anda memulai prosedur ini, Anda harus mengaktifkan Atribut untuk kontrol akses fitur terlebih dahulu. Untuk informasi selengkapnya tentang cara melakukan ini, lihat Aktifkan dan konfigurasikan atribut untuk kontrol akses.

1. Di konsol pusat admin Microsoft Entra, navigasikan ke Identity > Applications > Enterprise Applications dan kemudian pilih AWS IAM Identity Center.
2. Pilih Single sign-on.
3. Di bagian Atribut & Klaim, pilih Edit.
4. Pada halaman Atribut & Klaim, lakukan hal berikut:
    a. Pilih Tambahkan klaim baru
    b. Untuk Nama, masukkan `AccessControl:`*`AttributeName`*. Ganti *`AttributeName`*dengan nama atribut yang Anda harapkan di IAM Identity Center. Sebagai contoh, `AccessControl:`**`Department`**.
    c. Untuk Namespace, masukkan **`https://aws.amazon.com/SAML/Attributes`**.
    d. Untuk Sumber, pilih Atribut.
    e. Untuk atribut Source, gunakan daftar drop-down untuk memilih atribut Microsoft Entra ID pengguna. Sebagai contoh, `user.`**`department`**.
5. Ulangi langkah sebelumnya untuk setiap atribut yang perlu Anda kirim ke IAM Identity Center dalam pernyataan SAMB.
6. Pilih Simpan.

Method 2

Metode 2: Konfigurasikan ABAC menggunakan IAM Identity Center

Dengan metode ini, Anda menggunakan Atribut untuk kontrol akses fitur di IAM Identity Center untuk meneruskan `Attribute` elemen dengan `Name` atribut yang disetel kehttps:// `aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`**. Anda dapat menggunakan elemen ini untuk meneruskan atribut sebagai tag sesi dalam pernyataan SAFL. Untuk informasi selengkapnya tentang tag sesi, lihat Melewati tag sesi AWS STS di Panduan Pengguna IAM.

Untuk menyampaikan atribut sebagai tag sesi, sertakan elemen `AttributeValue` yang menentukan nilai tag. Misalnya, untuk meneruskan pasangan nilai kunci tag`CostCenter = blue`, gunakan atribut berikut:

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/
AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Jika Anda perlu menambahkan beberapa atribut, sertakan `Attribute` elemen terpisah untuk setiap tag.

Konfigurasikan SAFL dan SCIM dengan Okta dan IAM Identity Center

Anda dapat secara otomatis menyediakan (menyinkronkan) informasi pengguna dan grup dari Okta Pusat Identitas IAM menggunakan protokol System for Cross-domain Identity Management (SCIM) v2.0. Untuk mengonfigurasi koneksi iniOkta, Anda menggunakan titik akhir SCIM untuk Pusat Identitas IAM dan token pembawa yang dibuat secara otomatis oleh IAM Identity Center. Saat mengonfigurasi sinkronisasi SCIM, Anda membuat pemetaan atribut pengguna Okta ke atribut bernama di Pusat Identitas IAM. Pemetaan ini cocok dengan atribut pengguna yang diharapkan antara IAM Identity Center dan Anda. Okta

Oktamendukung fitur penyediaan berikut saat terhubung ke IAM Identity Center melalui SCIM:

- Buat pengguna - Pengguna yang ditugaskan ke aplikasi Pusat Identitas IAM di Okta disediakan di Pusat Identitas IAM.
- Perbarui atribut pengguna - Perubahan atribut untuk pengguna yang ditugaskan ke aplikasi Pusat Identitas IAM di diperbarui di Okta Pusat Identitas IAM.
- Nonaktifkan pengguna - Pengguna yang tidak ditugaskan dari aplikasi Pusat Identitas IAM dinonaktifkan di Okta Pusat Identitas IAM.
- Group push — Grup (dan anggotanya) Okta disinkronkan ke IAM Identity Center.

> **Note**
>
> Untuk meminimalkan overhead administratif di keduanya Okta dan Pusat Identitas IAM, sebaiknya Anda menetapkan dan mendorong grup alih-alih pengguna individu.

Jika Anda belum mengaktifkan IAM Identity Center, lihatMengaktifkan AWS IAM Identity Center.

Objektif

Dalam tutorial ini, Anda akan berjalan melalui pengaturan koneksi SAFL dengan Okta IAM Identity Center. Nanti, Anda akan menyinkronkan pengguna dariOkta, menggunakan SCIM. Dalam skenario ini, Anda mengelola semua pengguna dan grupOkta. Pengguna masuk melalui Okta portal. Untuk memverifikasi semuanya dikonfigurasi dengan benar, setelah menyelesaikan langkah-langkah konfigurasi Anda akan masuk sebagai Okta pengguna dan memverifikasi akses ke AWS sumber daya.

> **Note**
>
> Anda dapat mendaftar untuk Okta akun (uji coba gratis) yang telah menginstal aplikasi Okta's IAM Identity Center. Untuk Okta produk berbayar, Anda mungkin perlu mengonfirmasi bahwa Okta lisensi mendukung manajemen siklus hidup atau kemampuan serupa yang memungkinkan penyediaan keluar. Fitur-fitur ini mungkin diperlukan untuk mengkonfigurasi SCIM dari Okta ke IAM Identity Center.

Sebelum Anda memulai

Sebelum Anda mengonfigurasi penyediaan SCIM antara Okta dan IAM Identity Center, kami sarankan Anda meninjau terlebih dahulu. Pertimbangan untuk menggunakan penyediaan otomatis

Konfirmasikan item berikut sebelum Anda memulai:

- Setiap Okta pengguna harus memiliki nilai Nama depan, nama belakang, nama pengguna dan nama tampilan yang ditentukan.
- Setiap Okta pengguna hanya memiliki satu nilai per atribut data, seperti alamat email atau nomor telepon. Setiap pengguna yang memiliki banyak nilai akan gagal untuk menyinkronkan. Jika ada pengguna yang memiliki beberapa nilai dalam atributnya, hapus atribut duplikat sebelum mencoba menyediakan pengguna di Pusat Identitas IAM. Misalnya, hanya satu atribut nomor telepon yang dapat disinkronkan, karena atribut nomor telepon default adalah “telepon kerja”, gunakan atribut “telepon kerja” untuk menyimpan nomor telepon pengguna, bahkan jika nomor telepon untuk pengguna adalah telepon rumah atau ponsel.
- Jika Anda memperbarui alamat pengguna, Anda harus memiliki StreetAddress, kota, negara bagian, ZipCode, dan nilai CountryCode yang ditentukan. Jika salah satu nilai ini tidak ditentukan

untuk Okta pengguna pada saat sinkronisasi, pengguna (atau perubahan pada pengguna) tidak akan disediakan.

> **Note**
>
> Hak dan atribut peran tidak didukung dan tidak dapat disinkronkan dengan Pusat Identitas IAM.
> Menggunakan Okta grup yang sama untuk tugas dan push grup saat ini tidak didukung. Untuk mempertahankan keanggotaan grup yang konsisten antara Okta dan Pusat Identitas IAM, buat grup terpisah dan konfigurasikan untuk mendorong grup ke Pusat Identitas IAM.

Langkah 1: Dapatkan metadata SAFL dari akun Anda Okta

1. Masuk keOkta admin dashboard, perluas Aplikasi, lalu pilih Aplikasi.
2. Pada halaman Aplikasi, pilih Jelajahi Katalog Aplikasi.
3. Di kotak pencarian, ketik AWS IAM Identity Center, pilih aplikasi untuk menambahkan aplikasi Pusat Identitas IAM.
4. Pilih tab Masuk.
5. Di bawah Sertifikat Penandatanganan SAMP, pilih Tindakan, lalu pilih Lihat Metadata IDP. Tab browser baru terbuka menunjukkan pohon dokumen dari file XML. Pilih semua XMLnya dari `<md:EntityDescriptor>` to `</md:EntityDescriptor>` dan salin ke file teks.
6. Simpan file teks sebagai`metadata.xml`.

Biarkan Okta admin dashboard terbuka, Anda akan terus menggunakan konsol itu di langkah selanjutnya.

Langkah 2: Konfigurasikan Okta sebagai sumber identitas untuk IAM Identity Center

1. Buka konsol Pusat Identitas IAM sebagai pengguna dengan hak administratif.
2. Pilih Pengaturan di panel navigasi kiri.
3. Pada halaman Pengaturan, pilih Tindakan, lalu pilih Ubah sumber identitas.
4. Di bawah Pilih sumber identitas, pilih Penyedia identitas eksternal, lalu pilih Berikutnya.
5. Di bawah Konfigurasi penyedia identitas eksternal, lakukan hal berikut:

a. Di bawah metadata penyedia layanan, pilih Unduh file metadata untuk mengunduh file metadata Pusat Identitas IAM dan menyimpannya di sistem Anda. Anda akan memberikan file metadata IAM Identity Center SAM untuk Okta nanti dalam tutorial ini.

   Salin item berikut ke file teks untuk memudahkan akses:

   - URL Layanan Konsumen (ACS) Pernyataan Pusat Identitas IAM
   - URL penerbit IAM Identity Center

   Anda akan membutuhkan nilai-nilai ini nanti dalam tutorial ini.

b. Di bawah metadata penyedia identitas, di bawah IDP SAMP meta pilih Pilih file dan kemudian pilih file yang Anda buat pada langkah `metadata.xml` sebelumnya.

c. Pilih Berikutnya.

6. Setelah Anda membaca disclaimer dan siap untuk melanjutkan, masukkan ACCEPT.
7. Pilih Ubah sumber identitas.

   Biarkan AWS konsol terbuka, Anda akan terus menggunakan konsol itu di langkah berikutnya.

8. Kembali ke Okta admin dashboard dan pilih tab Masuk AWS IAM Identity Center aplikasi, lalu klik Edit.
9. Di bawah Pengaturan Masuk Lanjutan, masukkan yang berikut ini:

   - Untuk URL ACS, masukkan nilai yang Anda salin untuk URL IAM Identity Center Assertion Consumer Service (ACS)
   - Untuk URL Penerbit masukkan nilai yang Anda salin untuk URL penerbit IAM Identity Center
   - Untuk format nama pengguna Aplikasi pilih salah satu opsi dari menu tarik-turun.

     Buat sehingga nilai yang Anda pilih unik untuk setiap pengguna. Untuk tutorial ini, pilih nama pengguna Okta

10. Pilih Simpan.

Anda sekarang siap untuk menyediakan pengguna dari Pusat Okta Identitas IAM. Biarkan Okta admin dashboard terbuka, dan kembali ke konsol IAM Identity Center untuk langkah selanjutnya.

Langkah 3: Untuk menyediakan pengguna dari Okta

1. Di konsol Pusat Identitas IAM di halaman Pengaturan, cari kotak Informasi penyediaan otomatis, lalu pilih Aktifkan. Ini memungkinkan penyediaan otomatis di IAM Identity Center dan menampilkan titik akhir SCIM dan informasi token akses yang diperlukan.
2. Di kotak dialog Penyediaan otomatis masuk, salin setiap nilai untuk opsi berikut:

   - Titik akhir SCIM
   - Token akses

   Nanti dalam tutorial ini Anda akan memasukkan nilai-nilai ini untuk mengonfigurasi penyediaan. Okta
3. Pilih Tutup.
4. Kembali ke Okta admin dashboard dan navigasikan ke aplikasi Pusat Identitas IAM.
5. Pada halaman aplikasi Pusat Identitas IAM, pilih tab Penyediaan, lalu di navigasi kiri di bawah Pengaturan, pilih Integrasi.
6. Pilih Edit, lalu pilih kotak centang di samping Aktifkan integrasi API untuk mengaktifkan penyediaan.
7. Konfigurasikan Okta dengan nilai penyediaan SCIM dari IAM Identity Center yang Anda salin sebelumnya dalam tutorial ini:

   a. Di bidang URL Dasar, masukkan nilai titik akhir SCIM. Pastikan Anda menghapus garis miring ke depan di akhir URL.

   b. Di bidang Token API, masukkan nilai token Access.
8. Pilih Test API Credentials untuk memverifikasi kredensi yang dimasukkan valid.

   Pesan berhasilAWS IAM Identity Center diverifikasi! menampilkan.
9. Pilih Simpan. Anda dinavigasi ke area Pengaturan, dengan Integrasi dipilih.
10. Di bawah Pengaturan, pilih Ke Aplikasi, lalu pilih kotak centang Aktifkan untuk setiap fitur Penyediaan ke Aplikasi yang ingin Anda aktifkan. Untuk tutorial ini, pilih semua opsi.
11. Pilih Simpan.

Anda sekarang siap untuk menyinkronkan pengguna Anda Okta dengan IAM Identity Center.

Langkah 4: Sinkronisasi pengguna Okta dengan IAM Identity Center

Secara default, tidak ada grup atau pengguna yang ditetapkan ke aplikasi Pusat Okta Identitas IAM Anda. Grup penyediaan menyediakan pengguna yang menjadi anggota grup. Selesaikan langkah-langkah berikut untuk menyinkronkan grup dan pengguna dengan IAM Identity Center.

1. Di halaman aplikasi Pusat Okta Identitas IAM, pilih tab Penugasan. Anda dapat menetapkan orang dan grup ke aplikasi Pusat Identitas IAM.

   a. Untuk menugaskan orang:

      - Di halaman Penugasan, pilih Tetapkan, lalu pilih Tetapkan ke orang.
      - Pilih Okta pengguna yang ingin Anda akses ke aplikasi Pusat Identitas IAM. Pilih Tetapkan, pilih Simpan dan Kembali, lalu pilih Selesai.

      Ini memulai proses penyediaan pengguna ke IAM Identity Center.

   b. Untuk menetapkan grup:

      - Di halaman Penugasan, pilih Tetapkan, lalu pilih Tetapkan ke grup.
      - Pilih Okta grup yang ingin Anda akses ke aplikasi Pusat Identitas IAM. Pilih Tetapkan, pilih Simpan dan Kembali, lalu pilih Selesai.

      Ini memulai proses penyediaan pengguna dalam grup ke IAM Identity Center.

      > **Note**
      >
      > Anda mungkin diminta untuk menentukan atribut tambahan untuk grup jika atribut tersebut tidak ada di semua catatan pengguna. Atribut yang ditentukan untuk grup akan mengganti nilai atribut individual apa pun.

2. Pilih tab Push Groups. Pilih Okta grup yang berisi semua grup yang Anda tetapkan ke aplikasi Pusat Identitas IAM. Pilih Simpan.

   Status grup berubah menjadi Aktif setelah grup dan anggotanya didorong ke Pusat Identitas IAM.

3. Kembali ke tab Tugas.
4. Jika Anda memiliki pengguna yang bukan anggota grup yang Anda dorong ke IAM Identity Center, tambahkan mereka satu per satu menggunakan langkah-langkah berikut:

Di halaman Penugasan, pilih Tetapkan, lalu pilih Tetapkan ke Orang.

5. Pilih Okta pengguna yang ingin Anda akses ke aplikasi Pusat Identitas IAM. Pilih Tetapkan, pilih Simpan dan Kembali, lalu pilih Selesai.

   Ini memulai proses penyediaan pengguna individu ke IAM Identity Center.

   > **Note**
   >
   > Anda juga dapat menetapkan pengguna dan grup ke AWS IAM Identity Center aplikasi, dari halaman Aplikasi. Okta admin dashboard Untuk melakukan ini pilih ikon Pengaturan dan kemudian pilih Tetapkan ke Pengguna atau Tetapkan ke Grup dan kemudian tentukan pengguna atau grup.

6. Kembali ke konsol Pusat Identitas IAM. Di navigasi kiri, pilih Pengguna, Anda akan melihat daftar pengguna yang diisi oleh Okta pengguna Anda.

> **Selamat!**
>
> Anda telah berhasil mengatur koneksi SAMP antara Okta dan AWS dan telah memverifikasi bahwa penyediaan otomatis berfungsi. Anda sekarang dapat menetapkan pengguna ini ke akun dan aplikasi di IAM Identity Center. Untuk tutorial ini, pada langkah berikutnya mari kita menunjuk salah satu pengguna sebagai administrator IAM Identity Center dengan memberikan mereka izin administratif ke akun manajemen.

Langkah 5: Berikan Okta pengguna akses ke akun

1. Di panel navigasi Pusat Identitas IAM, di bawah izin Multi-akun, pilih. Akun AWS
2. Pada Akun AWShalaman, struktur Organisasi menampilkan akar organisasi Anda dengan akun Anda di bawahnya dalam hierarki. Pilih kotak centang untuk akun manajemen Anda, lalu pilih Tetapkan pengguna atau grup.
3. Tampilan alur kerja Tetapkan pengguna dan grup. Ini terdiri dari tiga langkah:

   a. Untuk Langkah 1: Pilih pengguna dan grup pilih pengguna yang akan melakukan fungsi pekerjaan administrator. Lalu pilih Selanjutnya.

b. Untuk Langkah 2: Pilih set izin pilih Buat set izin untuk membuka tab baru yang memandu Anda melalui tiga sub-langkah yang terlibat dalam membuat set izin.

   i. Untuk Langkah 1: Pilih jenis set izin lengkapi yang berikut ini:

      - Dalam Jenis set izin, pilih Set izin yang telah ditentukan sebelumnya.
      - Dalam Kebijakan untuk set izin yang telah ditentukan sebelumnya, pilih AdministratorAccess.

      Pilih Berikutnya.

   ii. Untuk Langkah 2: Tentukan detail set izin, pertahankan pengaturan default, dan pilih Berikutnya.

      Pengaturan default membuat set izin bernama *AdministratorAccess*dengan durasi sesi diatur ke satu jam.

   iii. Untuk Langkah 3: Tinjau dan buat, verifikasi bahwa jenis set Izin menggunakan kebijakan AWS terkelola AdministratorAccess. Pilih Buat. Pada halaman Set izin, pemberitahuan muncul memberi tahu Anda bahwa set izin telah dibuat. Anda dapat menutup tab ini di browser web Anda sekarang.

   Pada tab Tetapkan pengguna dan grup browser, Anda masih pada Langkah 2: Pilih set izin dari mana Anda memulai alur kerja set izin buat.

   Di area set Izin, pilih tombol Refresh. Set *AdministratorAccess*izin yang Anda buat muncul dalam daftar. Pilih kotak centang untuk set izin tersebut dan kemudian pilih Berikutnya.

c. Untuk Langkah 3: Tinjau dan kirimkan ulasan pengguna dan set izin yang dipilih, lalu pilih Kirim.

   Halaman diperbarui dengan pesan bahwa Anda Akun AWS sedang dikonfigurasi. Tunggu sampai proses selesai.

   Anda dikembalikan ke Akun AWS halaman. Pesan notifikasi memberi tahu Anda bahwa pesan Anda Akun AWS telah direvisi dan set izin yang diperbarui diterapkan. Saat pengguna masuk, mereka akan memiliki opsi untuk memilih peran. *AdministratorAccess*

> **Note**
>
> Sinkronisasi otomatis SCIM Okta hanya mendukung pengguna penyediaan; grup tidak disediakan secara otomatis. Anda tidak dapat membuat grup untuk Okta pengguna menggunakan AWS Management Console. Setelah menyediakan pengguna, Anda dapat membuat grup menggunakan operasi CLI atau API

Langkah 6: Konfirmasikan akses Okta pengguna ke AWS sumber daya

1. Masuk ke Okta dashboard menggunakan akun pengguna uji.
2. Di bawah Aplikasi Saya pilih AWS IAM Identity Center ikon.
3. Anda masuk ke portal dan dapat melihat Akun AWS ikonnya. Perluas ikon itu untuk melihat daftar Akun AWS yang dapat diakses pengguna. Dalam tutorial ini Anda hanya bekerja dengan satu akun, jadi memperluas ikon hanya menampilkan satu akun.
4. Pilih akun untuk menampilkan set izin yang tersedia bagi pengguna. Dalam tutorial ini Anda membuat set AdministratorAccessizin.
5. Di samping set izin adalah tautan untuk jenis akses yang tersedia untuk set izin tersebut. Saat Anda membuat set izin, Anda menetapkan konsol manajemen dan akses terprogram diaktifkan, sehingga dua opsi tersebut ada. Pilih Konsol manajemen untuk membuka AWS Management Console.
6. Pengguna masuk ke konsol.

(Opsional) Melewati atribut untuk kontrol akses

Anda dapat menggunakan Atribut untuk kontrol akses fitur ini secara opsional di Pusat Identitas IAM untuk meneruskan `Attribute` elemen dengan `Name` atribut yang disetel ke. `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` Elemen ini memungkinkan Anda untuk meneruskan atribut sebagai tanda sesi dalam pernyataan SAML. Untuk informasi selengkapnya tentang tag sesi, lihat Melewati tag sesi AWS STSdi Panduan Pengguna IAM.

Untuk menyampaikan atribut sebagai tag sesi, sertakan elemen `AttributeValue` yang menentukan nilai tag. Misalnya, untuk meneruskan pasangan nilai kunci tag`CostCenter = blue`, gunakan atribut berikut.

```
<saml:AttributeStatement>
```

```
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Jika Anda perlu menambahkan beberapa atribut, sertakan `Attribute` elemen terpisah untuk setiap tag.

Langkah selanjutnya

Sekarang setelah Anda mengonfigurasi Okta sebagai penyedia identitas dan pengguna yang disediakan di Pusat Identitas IAM, Anda dapat:

- Berikan akses ke Akun AWS, lihatTetapkan akses pengguna ke Akun AWS.
- Berikan akses ke aplikasi cloud, lihatTetapkan akses pengguna ke aplikasi di konsol Pusat Identitas IAM.
- Mengonfigurasi izin berdasarkan fungsi pekerjaan, lihat Membuat set izin

Menyiapkan penyediaan SCIM antara OneLogin dan IAM Identity Center

IAM Identity Center mendukung penyediaan otomatis (sinkronisasi) informasi pengguna dan grup dari OneLogin ke Pusat Identitas IAM menggunakan protokol System for Cross-domain Identity Management (SCIM) v2.0. Anda mengonfigurasi koneksi iniOneLogin, menggunakan titik akhir SCIM Anda untuk IAM Identity Center dan token pembawa yang dibuat secara otomatis oleh IAM Identity Center. Saat mengonfigurasi sinkronisasi SCIM, Anda membuat pemetaan atribut pengguna OneLogin ke atribut bernama di Pusat Identitas IAM. Hal ini menyebabkan atribut yang diharapkan cocok antara IAM Identity Center danOneLogin.

Langkah-langkah berikut memandu Anda melalui cara mengaktifkan penyediaan otomatis pengguna dan grup dari OneLogin Pusat Identitas IAM menggunakan protokol SCIM.

> **Note**
>
> Sebelum Anda mulai menerapkan SCIM, kami sarankan Anda terlebih dahulu meninjau. Pertimbangan untuk menggunakan penyediaan otomatis

Topik

Prasyarat

Anda akan memerlukan yang berikut ini sebelum Anda dapat memulai:

- Sebuah OneLogin akun. Jika Anda tidak memiliki akun yang ada, Anda mungkin dapat memperoleh uji coba gratis atau akun pengembang dari OneLoginsitus web.
- Akun berkemampuan Pusat Identitas IAM (gratis). Untuk informasi selengkapnya, lihat Mengaktifkan Pusat Identitas IAM.
- Koneksi SAMP dari OneLogin akun Anda ke IAM Identity Center. Untuk informasi selengkapnya, lihat Mengaktifkan Single Sign-On Antara OneLogin dan AWS di Blog Jaringan AWS Mitra.

Langkah 1: Aktifkan penyediaan di IAM Identity Center

Pada langkah pertama ini, Anda menggunakan konsol IAM Identity Center untuk mengaktifkan penyediaan otomatis.

Untuk mengaktifkan penyediaan otomatis di Pusat Identitas IAM

1. Setelah Anda menyelesaikan prasyarat, buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan di panel navigasi kiri.
3. Pada halaman Pengaturan, cari kotak Informasi penyediaan otomatis, lalu pilih Aktifkan. Ini segera memungkinkan penyediaan otomatis di IAM Identity Center dan menampilkan titik akhir SCIM dan informasi token akses yang diperlukan.
4. Dalam kotak dialog Penyediaan otomatis masuk, salin setiap nilai untuk opsi berikut. Anda harus menempelkannya nanti saat mengonfigurasi penyediaan di iDP Anda.

a. Titik akhir SCIM

b. Token akses

5. Pilih Tutup.

Anda sekarang telah menyiapkan penyediaan di konsol Pusat Identitas IAM. Sekarang Anda perlu melakukan tugas yang tersisa menggunakan konsol OneLogin admin seperti yang dijelaskan dalam prosedur berikut.

Langkah 2: Konfigurasikan penyediaan di OneLogin

Gunakan prosedur berikut di konsol OneLogin admin untuk mengaktifkan integrasi antara IAM Identity Center dan aplikasi IAM Identity Center. Prosedur ini mengasumsikan Anda telah mengkonfigurasi aplikasi AWS Single Sign-On OneLogin untuk otentikasi SAMP. Jika Anda belum membuat koneksi SAMP ini, lakukan sebelum melanjutkan dan kemudian kembali ke sini untuk menyelesaikan proses penyediaan SCIM. Untuk informasi selengkapnya tentang mengonfigurasi SAMP denganOneLogin, lihat Mengaktifkan Single Sign-On Between OneLogin dan AWS di Blog Jaringan Mitra. AWS

Untuk mengonfigurasi penyediaan di OneLogin

1. Masuk keOneLogin, lalu arahkan ke Applications > Applications.
2. Pada halaman Aplikasi, cari aplikasi yang Anda buat sebelumnya untuk membentuk koneksi SAMP Anda dengan IAM Identity Center. Pilih dan kemudian pilih Konfigurasi dari bilah navigasi kiri.
3. Pada prosedur sebelumnya, Anda menyalin nilai endpoint SCIM di IAM Identity Center. Tempelkan nilai itu ke bidang URL Dasar SCIM diOneLogin. Pastikan Anda menghapus garis miring di akhir URL. Juga, dalam prosedur sebelumnya Anda menyalin nilai token Access di IAM Identity Center. Tempelkan nilai itu ke bidang Token Pembawa SCIM di. OneLogin
4. Di samping Koneksi API, klik Aktifkan, lalu klik Simpan untuk menyelesaikan konfigurasi.
5. Di bilah navigasi kiri, pilih Penyediaan.
6. Pilih kotak centang untuk Aktifkan penyediaan, Buat pengguna, Hapus pengguna, dan Perbarui pengguna, lalu pilih Simpan.
7. Di bilah navigasi kiri, pilih Pengguna.
8. Klik Tindakan Lainnya dan pilih Sinkronkan login. Anda harus menerima pesan Sinkronisasi pengguna dengan AWS Single Sign-On.

9. Klik Tindakan Lainnya lagi, lalu pilih Terapkan kembali pemetaan hak. Anda akan menerima pesan Pemetaan sedang diterapkan kembali.
10. Pada titik ini, proses penyediaan harus dimulai. Untuk mengonfirmasi hal ini, navigasikan ke Aktivitas > Acara, dan pantau progres. Acara penyediaan yang berhasil, serta kesalahan, akan muncul di aliran acara.
11. Untuk memverifikasi bahwa semua pengguna dan grup Anda telah berhasil disinkronkan ke Pusat Identitas IAM, kembali ke konsol Pusat Identitas IAM dan pilih Pengguna. Pengguna Anda yang disinkronkan OneLogin muncul di halaman Pengguna. Anda juga dapat melihat grup yang disinkronkan di halaman Grup.
12. Untuk menyinkronkan perubahan pengguna secara otomatis ke Pusat Identitas IAM, arahkan ke halaman Penyediaan, cari bagian Memerlukan persetujuan admin sebelum tindakan ini dilakukan, hapus pilihan Buat Pengguna, Hapus Pengguna, dan/atau Perbarui Pengguna, dan klik Simpan.

(Opsional) Langkah 3: Konfigurasikan atribut pengguna OneLogin untuk kontrol akses di Pusat Identitas IAM

Ini adalah prosedur opsional OneLogin jika Anda memilih untuk mengkonfigurasi atribut yang akan Anda gunakan di IAM Identity Center untuk mengelola akses ke AWS sumber daya Anda. Atribut yang Anda tentukan OneLogin diteruskan dalam pernyataan SAMP ke IAM Identity Center. Anda kemudian akan membuat set izin di IAM Identity Center untuk mengelola akses berdasarkan atribut yang Anda lewati. OneLogin

Sebelum Anda memulai prosedur ini, Anda harus terlebih dahulu mengaktifkan Atribut untuk kontrol akses fitur tersebut. Untuk informasi selengkapnya tentang cara melakukan ini, lihat Aktifkan dan konfigurasikan atribut untuk kontrol akses.

Untuk mengonfigurasi atribut pengguna OneLogin untuk kontrol akses di Pusat Identitas IAM

1. Masuk keOneLogin, lalu arahkan ke Applications > Applications.
2. Pada halaman Aplikasi, cari aplikasi yang Anda buat sebelumnya untuk membentuk koneksi SAMP Anda dengan IAM Identity Center. Pilih dan kemudian pilih Parameter dari bilah navigasi kiri.
3. Di bagian Parameter yang Diperlukan, lakukan hal berikut untuk setiap atribut yang ingin Anda gunakan di Pusat Identitas IAM:

a. Pilih +.

b. Di Nama bidang, masukkan`https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`**, dan ganti **`AttributeName`** dengan nama atribut yang Anda harapkan di Pusat Identitas IAM. Misalnya, `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Department`**.

c. Di bawah Bendera, centang kotak di samping Sertakan dalam pernyataan SAMP, dan pilih Simpan.

d. Di bidang Nilai, gunakan daftar drop-down untuk memilih atribut OneLogin pengguna. Misalnya, Departemen.

4. Pilih Simpan.

(Opsional) Melewati atribut untuk kontrol akses

Anda dapat menggunakan Atribut untuk kontrol akses fitur ini secara opsional di Pusat Identitas IAM untuk meneruskan `Attribute` elemen dengan `Name` atribut yang disetel ke. `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`** Elemen ini memungkinkan Anda untuk meneruskan atribut sebagai tanda sesi dalam pernyataan SAML. Untuk informasi selengkapnya tentang tag sesi, lihat Melewati tag sesi AWS STS di Panduan Pengguna IAM.

Untuk menyampaikan atribut sebagai tag sesi, sertakan elemen `AttributeValue` yang menentukan nilai tag. Misalnya, untuk meneruskan pasangan nilai kunci tag`CostCenter = blue`, gunakan atribut berikut.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Jika Anda perlu menambahkan beberapa atribut, sertakan `Attribute` elemen terpisah untuk setiap tag.

Memecahkan masalah

Berikut ini dapat membantu Anda memecahkan masalah umum yang mungkin Anda temui saat menyiapkan penyediaan otomatis. OneLogin

Grup tidak disediakan untuk IAM Identity Center

Secara default, grup mungkin tidak disediakan dari OneLogin Pusat Identitas IAM. Pastikan Anda telah mengaktifkan penyediaan grup untuk aplikasi Pusat Identitas IAM Anda di. OneLogin Untuk melakukannya, masuk ke konsol OneLogin admin, dan periksa untuk memastikan bahwa opsi Sertakan dalam Penyediaan Pengguna dipilih di bawah properti aplikasi Pusat Identitas IAM (aplikasi Pusat Identitas IAM > Parameter> Grup). Untuk detail selengkapnya tentang cara membuat grupOneLogin, termasuk cara menyinkronkan OneLogin peran sebagai grup di SCIM, silakan lihat situs web. OneLogin

Tidak ada yang OneLogin disinkronkan dari Pusat Identitas IAM, meskipun semua pengaturan sudah benar

Selain catatan di atas mengenai persetujuan admin, Anda perlu Menerapkan kembali pemetaan hak agar banyak perubahan konfigurasi diterapkan. Ini dapat ditemukan di Applications > Applications > Aplikasi IAM Identity Center > More Actions. Anda dapat melihat detail dan log untuk sebagian besar tindakanOneLogin, termasuk peristiwa sinkronisasi, di bawah Aktivitas > Acara.

Saya telah menghapus atau menonaktifkan grup diOneLogin, tetapi masih muncul di Pusat Identitas IAM

OneLoginsaat ini tidak mendukung operasi SCIM DELETE untuk grup, yang berarti bahwa grup terus ada di IAM Identity Center. Oleh karena itu, Anda harus menghapus grup dari Pusat Identitas IAM secara langsung untuk memastikan bahwa izin yang sesuai di Pusat Identitas IAM untuk grup tersebut dihapus.

Saya menghapus grup di IAM Identity Center tanpa terlebih dahulu menghapusnya OneLogin dan sekarang saya mengalami masalah sinkronisasi pengguna/grup

Untuk memperbaiki situasi ini, pertama-tama pastikan bahwa Anda tidak memiliki aturan atau konfigurasi penyediaan grup yang berlebihan. OneLogin Misalnya, grup yang langsung ditugaskan ke aplikasi bersama dengan aturan yang menerbitkan ke grup yang sama. Selanjutnya, hapus grup yang tidak diinginkan di Pusat Identitas IAM. Terakhir, diOneLogin, Segarkan kembali hak (Aplikasi Pusat Identitas IAM > Penyediaan> Hak), lalu Terapkan kembali pemetaan hak (Aplikasi Pusat Identitas IAM > Tindakan Lainnya). Untuk menghindari masalah ini di masa mendatang, pertama-tama lakukan perubahan untuk menghentikan penyediaan grupOneLogin, lalu hapus grup dari IAM Identity Center.

Menggunakan Ping Identity produk dengan IAM Identity Center

Ping IdentityProduk-produk berikut telah diuji dengan IAM Identity Center.

Topik

PingFederate

IAM Identity Center mendukung penyediaan otomatis (sinkronisasi) informasi pengguna dan grup dari PingFederate produk dengan Ping Identity (selanjutnya “Ping”) ke Pusat Identitas IAM. Penyediaan ini menggunakan protokol System for Cross-domain Identity Management (SCIM) v2.0. Anda mengonfigurasi koneksi ini PingFederate menggunakan titik akhir dan token akses IAM Identity Center SCIM Anda. Saat mengonfigurasi sinkronisasi SCIM, Anda membuat pemetaan atribut pengguna PingFederate ke atribut bernama di Pusat Identitas IAM. Hal ini menyebabkan atribut yang diharapkan cocok antara IAM Identity Center danPingFederate.

Panduan ini didasarkan pada PingFederate versi 10.2. Langkah-langkah untuk versi lain dapat bervariasi. Hubungi Ping untuk informasi selengkapnya tentang cara mengonfigurasi penyediaan ke IAM Identity Center untuk versi lain. PingFederate

Langkah-langkah berikut memandu Anda melalui cara mengaktifkan penyediaan otomatis pengguna dan grup dari PingFederate Pusat Identitas IAM menggunakan protokol SCIM.

> **Note**
>
> Sebelum Anda mulai menerapkan SCIM, kami sarankan Anda terlebih dahulu meninjau. Pertimbangan untuk menggunakan penyediaan otomatis Kemudian lanjutkan meninjau pertimbangan tambahan di bagian selanjutnya.

Topik

- Langkah 2: Konfigurasikan penyediaan di PingFederate
- (Opsional) Langkah 3: Konfigurasikan atribut pengguna di PingFed erate untuk kontrol akses di IAM Identity Center
- (Opsional) Melewati atribut untuk kontrol akses

Prasyarat

Anda akan memerlukan yang berikut ini sebelum Anda dapat memulai:

- PingFederateServer yang berfungsi. Jika Anda tidak memiliki PingFederate server yang ada, Anda mungkin dapat memperoleh uji coba gratis atau akun pengembang dari situs web Ping Identity. Uji coba mencakup lisensi dan unduhan perangkat lunak dan dokumentasi terkait.
- Salinan perangkat lunak PingFederate IAM Identity Center Connector yang diinstal pada PingFederate server Anda. Untuk informasi lebih lanjut tentang cara mendapatkan perangkat lunak ini, lihat Konektor Pusat Identitas IAM di ing Identity situs web P.
- Akun berkemampuan Pusat Identitas IAM (gratis). Untuk informasi selengkapnya, lihat Mengaktifkan Pusat Identitas IAM.
- Koneksi SAFL dari PingFederate instans Anda ke IAM Identity Center. Untuk petunjuk tentang cara mengkonfigurasi koneksi ini, lihat PingFederate dokumentasi. Singkatnya, jalur yang disarankan adalah menggunakan Konektor Pusat Identitas IAM untuk mengonfigurasi “Browser SSO”PingFederate, menggunakan fitur metadata “unduh” dan “impor” di kedua ujungnya untuk bertukar metadata SAFL antara dan IAM Identity Center. PingFederate

Pertimbangan tambahan

Berikut ini adalah pertimbangan penting tentang hal PingFederate itu dapat memengaruhi cara Anda menerapkan penyediaan dengan IAM Identity Center.

- Jika atribut (seperti nomor telepon) dihapus dari pengguna di penyimpanan data yang dikonfigurasiPingFederate, atribut tersebut tidak akan dihapus dari pengguna terkait di Pusat Identitas IAM. Ini adalah batasan yang diketahui dalam PingFederate’s implementasi penyedia. Jika atribut diubah ke nilai yang berbeda (tidak kosong) pada pengguna, perubahan itu akan disinkronkan ke Pusat Identitas IAM.

Langkah 1: Aktifkan penyediaan di IAM Identity Center

Pada langkah pertama ini, Anda menggunakan konsol IAM Identity Center untuk mengaktifkan penyediaan otomatis.

Untuk mengaktifkan penyediaan otomatis di Pusat Identitas IAM

1. Setelah Anda menyelesaikan prasyarat, buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan di panel navigasi kiri.
3. Pada halaman Pengaturan, cari kotak Informasi penyediaan otomatis, lalu pilih Aktifkan. Ini segera memungkinkan penyediaan otomatis di IAM Identity Center dan menampilkan titik akhir SCIM dan informasi token akses yang diperlukan.
4. Dalam kotak dialog Penyediaan otomatis masuk, salin setiap nilai untuk opsi berikut. Anda harus menempelkannya nanti saat mengonfigurasi penyediaan di iDP Anda.
    a. Titik akhir SCIM
    b. Token akses
5. Pilih Tutup.

Sekarang setelah Anda mengatur penyediaan di konsol Pusat Identitas IAM, Anda harus menyelesaikan tugas yang tersisa menggunakan konsol PingFederate administratif., Langkah-langkahnya dijelaskan dalam prosedur berikut.

Langkah 2: Konfigurasikan penyediaan di PingFederate

Gunakan prosedur berikut di konsol PingFederate administratif untuk mengaktifkan integrasi antara IAM Identity Center dan IAM Identity Center Connector. Prosedur ini mengasumsikan bahwa Anda telah menginstal perangkat lunak IAM Identity Center Connector. Jika Anda belum melakukannya, lihatPrasyarat, dan kemudian selesaikan prosedur ini untuk mengonfigurasi penyediaan SCIM.

> **Important**
>
> Jika PingFederate server Anda belum dikonfigurasi sebelumnya untuk penyediaan SCIM keluar, Anda mungkin perlu membuat perubahan file konfigurasi untuk mengaktifkan penyediaan. Untuk informasi lebih lanjut, lihat Ping dokumentasi. Singkatnya, Anda harus mengubah `pf.provisioner.mode` pengaturan dalam pingfederate-<version>/pingfederate/bin/run.propertiesfile ke nilai selain `OFF` (yang merupakan default), dan restart server jika

sedang berjalan. Misalnya, Anda dapat memilih untuk menggunakan `STANDALONE` jika saat ini Anda tidak memiliki konfigurasi ketersediaan tinggi denganPingFederate.

Untuk mengonfigurasi penyediaan di PingFederate

1. Masuk ke konsol PingFederate administratif.
2. Pilih Aplikasi dari bagian atas halaman, lalu klik SP Connections.
3. Temukan aplikasi yang Anda buat sebelumnya untuk membentuk koneksi SAMP Anda dengan IAM Identity Center, dan klik pada nama koneksi.
4. Pilih Jenis Koneksi dari judul navigasi gelap di dekat bagian atas halaman. Anda akan melihat Browser SSO sudah dipilih dari konfigurasi SAMP Anda sebelumnya. Jika tidak, Anda harus menyelesaikan langkah-langkah itu terlebih dahulu sebelum Anda dapat melanjutkan.
5. Pilih kotak centang Outbound Provisioning, pilih IAM Identity Center Cloud Connector sebagai jenisnya, dan klik Simpan. Jika IAM Identity Center Cloud Connector tidak muncul sebagai opsi, pastikan Anda telah menginstal Konektor Pusat Identitas IAM dan telah memulai ulang server Anda. PingFederate
6. Klik Berikutnya berulang kali sampai Anda tiba di halaman Outbound Provisioning, dan kemudian klik tombol Configure Provisioning.
7. Pada prosedur sebelumnya, Anda menyalin nilai endpoint SCIM di IAM Identity Center. Tempelkan nilai itu ke bidang URL SCIM di PingFederate konsol. Pastikan Anda menghapus garis miring ke depan di akhir URL. Juga, dalam prosedur sebelumnya Anda menyalin nilai token Access di IAM Identity Center. Tempelkan nilai itu ke bidang Token Akses di PingFederate konsol. Klik Simpan.
8. Pada halaman Konfigurasi Saluran (Konfigurasi Saluran), klik Buat.
9. Masukkan Nama Saluran untuk saluran penyediaan baru ini (seperti**`AWSIAMIdentityCenterchannel`**), dan klik Berikutnya.
10. Pada halaman Sumber, pilih Active Data Store yang ingin Anda gunakan untuk koneksi ke IAM Identity Center, dan klik Berikutnya.

> **Note**
>
> Jika Anda belum mengonfigurasi sumber data, Anda harus melakukannya sekarang. Lihat dokumentasi Ping produk untuk informasi tentang cara memilih dan mengonfigurasi sumber dataPingFederate.

11. Pada halaman Pengaturan Sumber, konfirmasikan semua nilai sudah benar untuk instalasi Anda, lalu klik Berikutnya.
12. Pada halaman Lokasi Sumber, masukkan pengaturan yang sesuai dengan sumber data Anda, lalu klik Berikutnya. Misalnya, jika menggunakan Active Directory sebagai direktori LDAP:
    a. Masukkan Base DN hutan AD Anda (seperti**`DC=myforest,DC=mydomain,DC=com`**).
    b. Di Users > Group DN, tentukan satu grup yang berisi semua pengguna yang ingin Anda berikan ke IAM Identity Center. Jika tidak ada grup tunggal seperti itu, buat grup itu di AD, kembali ke pengaturan ini, lalu masukkan DN yang sesuai.
    c. Tentukan apakah akan mencari subgrup (Pencarian Bersarang), dan Filter LDAP yang diperlukan.
    d. Di Grup > Grup DN, tentukan satu grup yang berisi semua grup yang ingin Anda berikan ke Pusat Identitas IAM. Dalam banyak kasus, ini mungkin DN yang sama seperti yang Anda tentukan di bagian Pengguna. Masukkan nilai Pencarian Bersarang dan Filter sesuai kebutuhan.
13. Pada halaman Pemetaan Atribut, pastikan hal berikut, lalu klik Berikutnya:
    a. Bidang UserName harus dipetakan ke Atribut yang diformat sebagai email (user@domain.com). Itu juga harus sesuai dengan nilai yang akan digunakan pengguna untuk masuk ke Ping. Nilai ini pada gilirannya diisi dalam `nameId` klaim SAMP selama otentikasi federasi dan digunakan untuk pencocokan dengan pengguna di Pusat Identitas IAM. Misalnya, saat menggunakan Active Directory, Anda dapat memilih untuk menentukan `UserPrincipalName` sebagai UserName.
    b. Bidang lain yang diakhiran dengan* harus dipetakan ke atribut yang bukan null untuk pengguna Anda.
14. Pada halaman Aktivasi & Ringkasan, atur Status Saluran ke Aktif untuk menyebabkan sinkronisasi dimulai segera setelah konfigurasi disimpan.
15. Konfirmasikan bahwa semua nilai konfigurasi pada halaman sudah benar, dan klik Selesai.
16. Pada halaman Kelola Saluran, klik Simpan.
17. Pada titik ini, penyediaan dimulai. Untuk mengonfirmasi aktivitas, Anda dapat melihat file provisioner.log, yang terletak secara default di pingfederate-<version>/pingfederate/logdirektori di PingFederate server Anda.
18. Untuk memverifikasi bahwa pengguna dan grup telah berhasil disinkronkan ke Pusat Identitas IAM, kembali ke Konsol Pusat Identitas IAM dan pilih Pengguna. Pengguna yang disinkronkan

PingFederate muncul di halaman Pengguna. Anda juga dapat melihat grup yang disinkronkan di halaman Grup.

(Opsional) Langkah 3: Konfigurasikan atribut pengguna di PingFed erate untuk kontrol akses di IAM Identity Center

Ini adalah prosedur opsional PingFederate jika Anda memilih untuk mengkonfigurasi atribut yang akan Anda gunakan di IAM Identity Center untuk mengelola akses ke AWS sumber daya Anda. Atribut yang Anda tentukan PingFederate diteruskan dalam pernyataan SAMP ke IAM Identity Center. Anda kemudian akan membuat set izin di IAM Identity Center untuk mengelola akses berdasarkan atribut yang Anda lewati. PingFederate

Sebelum Anda memulai prosedur ini, Anda harus terlebih dahulu mengaktifkan Atribut untuk kontrol akses fitur tersebut. Untuk informasi selengkapnya tentang cara melakukan ini, lihat Aktifkan dan konfigurasikan atribut untuk kontrol akses.

Untuk mengonfigurasi atribut pengguna PingFederate untuk kontrol akses di Pusat Identitas IAM

1. Masuk ke konsol PingFederate administratif.
2. Pilih Aplikasi dari bagian atas halaman, lalu klik SP Connections.
3. Temukan aplikasi yang Anda buat sebelumnya untuk membentuk koneksi SAMP Anda dengan IAM Identity Center, dan klik pada nama koneksi.
4. Pilih Browser SSO dari judul navigasi gelap di dekat bagian atas halaman. Kemudian klik Konfigurasi Browser SSO.
5. Pada halaman Configure Browser SSO, pilih Assertion Creation, dan kemudian klik Configure Assertion Creation.
6. Pada halaman Configure Assertion Creation, pilih Attribute Contract.
7. Pada halaman Kontrak Atribut, di bawah bagian Perpanjang Kontrak, tambahkan atribut baru dengan melakukan langkah-langkah berikut:

    a. Di kotak teks, masukkan`https://aws.amazon.com/SAML/Attributes/AccessControl:`**`AttributeName`**, ganti **`AttributeName`** dengan nama atribut yang Anda harapkan di Pusat Identitas IAM. Misalnya, `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Department`**.

    b. Untuk Format Nama Atribut, pilih urn:oasis:names:tc:SAML:2.0:attrname-format:uri.

    c. Pilih Tambah, lalu pilih Berikutnya.

8. Pada halaman Pemetaan Sumber Otentikasi, pilih Instans Adaptor yang dikonfigurasi dengan aplikasi Anda.
9. Pada halaman Pemenuhan Kontrak Atribut, pilih Sumber (penyimpanan data) dan Nilai (atribut penyimpanan data) untuk Kontrak **`https://aws.amazon.com/SAML/Attributes/AccessControl:Department`** Atribut.

   > **Note**
   >
   > Jika Anda belum mengonfigurasi sumber data, Anda harus melakukannya sekarang. Lihat dokumentasi Ping produk untuk informasi tentang cara memilih dan mengonfigurasi sumber dataPingFederate.

10. Klik Berikutnya berulang kali sampai Anda tiba di halaman Aktivasi & Ringkasan, lalu klik Simpan.

(Opsional) Melewati atribut untuk kontrol akses

Anda dapat secara opsional menggunakan Atribut untuk kontrol akses fitur di IAM Identity Center untuk meneruskan `Attribute` elemen dengan `Name` atribut yang disetel ke. `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}` Elemen ini memungkinkan Anda untuk meneruskan atribut sebagai tanda sesi dalam pernyataan SAML. Untuk informasi selengkapnya tentang tag sesi, lihat Melewati tag sesi AWS STS di Panduan Pengguna IAM.

Untuk menyampaikan atribut sebagai tag sesi, sertakan elemen `AttributeValue` yang menentukan nilai tag. Misalnya, untuk meneruskan pasangan nilai kunci tag`CostCenter = blue`, gunakan atribut berikut.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Jika Anda perlu menambahkan beberapa atribut, sertakan `Attribute` elemen terpisah untuk setiap tag.

PingOne

IAM Identity Center mendukung penyediaan otomatis (sinkronisasi) informasi pengguna dari PingOne produk dengan Ping Identity (selanjutnya “Ping”) ke Pusat Identitas IAM. Penyediaan ini menggunakan protokol System for Cross-domain Identity Management (SCIM) v2.0. Anda mengonfigurasi koneksi ini PingOne menggunakan titik akhir dan token akses IAM Identity Center SCIM Anda. Saat mengonfigurasi sinkronisasi SCIM, Anda membuat pemetaan atribut pengguna PingOne ke atribut bernama di Pusat Identitas IAM. Hal ini menyebabkan atribut yang diharapkan cocok antara IAM Identity Center danPingOne.

Panduan ini didasarkan pada PingOne per Oktober 2020. Langkah-langkah untuk versi yang lebih baru dapat bervariasi. Hubungi Ping untuk informasi selengkapnya tentang cara mengonfigurasi penyediaan ke IAM Identity Center untuk versi lain. PingOne Panduan ini juga berisi beberapa catatan mengenai konfigurasi otentikasi pengguna melalui SAMP.

Langkah-langkah berikut memandu Anda melalui cara mengaktifkan penyediaan otomatis pengguna dari PingOne Pusat Identitas IAM menggunakan protokol SCIM.

> **Note**
>
> Sebelum Anda mulai menerapkan SCIM, kami sarankan Anda terlebih dahulu meninjau. Pertimbangan untuk menggunakan penyediaan otomatis Kemudian lanjutkan meninjau pertimbangan tambahan di bagian selanjutnya.

Topik

Prasyarat

Anda akan memerlukan yang berikut ini sebelum Anda dapat memulai:

- PingOneLangganan atau uji coba gratis, dengan otentikasi federasi dan kemampuan penyediaan. Untuk informasi lebih lanjut tentang cara mendapatkan uji coba gratis, lihat situs Ping Identityweb.
- Akun berkemampuan Pusat Identitas IAM (gratis). Untuk informasi selengkapnya, lihat Mengaktifkan Pusat Identitas IAM.
- Aplikasi PingOne IAM Identity Center ditambahkan ke portal PingOne admin Anda. Anda dapat memperoleh aplikasi PingOne IAM Identity Center dari Katalog PingOne Aplikasi. Untuk informasi umum, lihat Menambahkan aplikasi dari Katalog Aplikasi di Ping Identity situs web.
- Koneksi SAFL dari PingOne instans Anda ke IAM Identity Center. Setelah aplikasi PingOne IAM Identity Center ditambahkan ke portal PingOne admin Anda, Anda harus menggunakannya untuk mengonfigurasi koneksi SAFL dari PingOne instans Anda ke IAM Identity Center. Gunakan fitur metadata “unduh” dan “impor” di kedua ujungnya untuk bertukar metadata SAMP antara PingOne dan IAM Identity Center. Untuk petunjuk tentang cara mengkonfigurasi koneksi ini, lihat PingOne dokumentasi.

Pertimbangan tambahan

Berikut ini adalah pertimbangan penting tentang hal PingOne itu dapat memengaruhi cara Anda menerapkan penyediaan dengan IAM Identity Center.

- Per Oktober 2020, PingOne tidak mendukung penyediaan grup melalui SCIM. Hubungi Ping untuk informasi terbaru tentang dukungan grup di SCIM untukPingOne.
- Pengguna dapat terus disediakan PingOne setelah menonaktifkan penyediaan di portal admin. PingOne Jika Anda perlu segera menghentikan penyediaan, hapus token pembawa SCIM yang relevan, dan/atau nonaktifkan Penyediaan otomatis di Pusat Identitas IAM.
- Jika atribut untuk pengguna dihapus dari penyimpanan data yang dikonfigurasiPingOne, atribut tersebut tidak akan dihapus dari pengguna terkait di Pusat Identitas IAM. Ini adalah batasan yang diketahui dalam PingOne’s implementasi penyedia. Jika atribut diubah, perubahan akan disinkronkan ke IAM Identity Center.
- Berikut ini adalah catatan penting mengenai konfigurasi SAMP Anda diPingOne:
  - IAM Identity Center hanya mendukung `emailaddress` sebagai `NameId` format. Ini berarti Anda harus memilih atribut pengguna yang unik dalam direktori Anda diPingOne, non-null, dan diformat sebagai email/UPN (misalnya, user@domain.com) untuk pemetaan SAML_SUBJECT Anda di. PingOne Email (Work) adalah nilai yang wajar untuk digunakan untuk konfigurasi pengujian dengan direktori PingOne bawaan.

- Pengguna PingOne dengan alamat email yang berisi karakter + mungkin tidak dapat masuk ke Pusat Identitas IAM, dengan kesalahan seperti `'SAML_215'` atau`'Invalid input'`. Untuk memperbaikinya, diPingOne, pilih opsi Lanjutan untuk pemetaan SAML_SUBJECT di Pemetaan Atribut. Kemudian atur Format ID Nama untuk dikirim ke SP: ke urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddressdalam menu drop-down.

Langkah 1: Aktifkan penyediaan di IAM Identity Center

Pada langkah pertama ini, Anda menggunakan konsol IAM Identity Center untuk mengaktifkan penyediaan otomatis.

Untuk mengaktifkan penyediaan otomatis di Pusat Identitas IAM

1. Setelah Anda menyelesaikan prasyarat, buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan di panel navigasi kiri.
3. Pada halaman Pengaturan, cari kotak Informasi penyediaan otomatis, lalu pilih Aktifkan. Ini segera memungkinkan penyediaan otomatis di IAM Identity Center dan menampilkan titik akhir SCIM dan informasi token akses yang diperlukan.
4. Dalam kotak dialog Penyediaan otomatis masuk, salin setiap nilai untuk opsi berikut. Anda harus menempelkannya nanti saat mengonfigurasi penyediaan di iDP Anda.
   a. Titik akhir SCIM
   b. Token akses
5. Pilih Tutup.

Sekarang setelah Anda menyiapkan penyediaan di konsol Pusat Identitas IAM, Anda harus menyelesaikan tugas yang tersisa menggunakan aplikasi Pusat Identitas PingOne IAM. Langkah-langkah ini dijelaskan dalam prosedur berikut.

Langkah 2: Konfigurasikan penyediaan di PingOne

Gunakan prosedur berikut dalam aplikasi PingOne IAM Identity Center untuk mengaktifkan penyediaan dengan IAM Identity Center. Prosedur ini mengasumsikan bahwa Anda telah menambahkan aplikasi PingOne IAM Identity Center ke portal PingOne admin Anda. Jika Anda belum melakukannya, lihatPrasyarat, dan kemudian selesaikan prosedur ini untuk mengonfigurasi penyediaan SCIM.

Untuk mengonfigurasi penyediaan di PingOne

1. Buka aplikasi PingOne IAM Identity Center yang Anda instal sebagai bagian dari konfigurasi SAFL untuk PingOne (Applications > My Applications). Lihat Prasyarat.
2. Gulir ke bagian bawah halaman. Di bawah Penyediaan Pengguna, pilih tautan lengkap untuk menavigasi ke konfigurasi penyediaan pengguna koneksi Anda.
3. Pada halaman Petunjuk Penyediaan, pilih Lanjutkan ke Langkah Berikutnya.
4. Pada prosedur sebelumnya, Anda menyalin nilai endpoint SCIM di IAM Identity Center. Tempelkan nilai itu ke bidang URL SCIM di aplikasi PingOne IAM Identity Center. Pastikan Anda menghapus garis miring ke depan di akhir URL. Juga, dalam prosedur sebelumnya Anda menyalin nilai token Access di IAM Identity Center. Tempelkan nilai itu ke bidang ACCESS_TOKEN di aplikasi PingOne IAM Identity Center.
5. Untuk REMOVE_ACTION, pilih salah satu Dinonaktifkan atau Dihapus (lihat teks deskripsi di halaman untuk detail selengkapnya).
6. Pada halaman Pemetaan Atribut, pilih nilai yang akan digunakan untuk pernyataan SAML_SUBJECT (`NameId`), mengikuti panduan dari sebelumnya di halaman ini. Pertimbangan tambahan Kemudian pilih Lanjutkan ke Langkah Berikutnya.
7. Pada halaman Kustomisasi PingOne Aplikasi - Pusat Identitas IAM, buat perubahan penyesuaian yang diinginkan (opsional), dan klik Lanjutkan ke Langkah Berikutnya.
8. Pada halaman Akses Grup, pilih grup yang berisi pengguna yang ingin Anda aktifkan untuk penyediaan dan masuk tunggal ke Pusat Identitas IAM. Pilih Lanjutkan ke Langkah Berikutnya.
9. Gulir ke bagian bawah halaman, dan pilih Selesai untuk memulai penyediaan.
10. Untuk memverifikasi bahwa pengguna telah berhasil disinkronkan ke Pusat Identitas IAM, kembali ke konsol Pusat Identitas IAM dan pilih Pengguna. Pengguna yang disinkronkan dari PingOne akan muncul di halaman Pengguna. Pengguna ini sekarang dapat ditugaskan ke akun dan aplikasi dalam IAM Identity Center.

    Ingat bahwa PingOne tidak mendukung penyediaan kelompok atau keanggotaan kelompok melalui SCIM. Hubungi Ping untuk informasi lebih lanjut.

(Opsional) Langkah 3: Konfigurasikan atribut pengguna PingOne untuk kontrol akses di Pusat Identitas IAM

Ini adalah prosedur opsional PingOne jika Anda memilih untuk mengkonfigurasi atribut untuk IAM Identity Center untuk mengelola akses ke AWS sumber daya Anda. Atribut yang Anda tentukan

PingOne diteruskan dalam pernyataan SAMP ke IAM Identity Center. Anda kemudian membuat set izin di Pusat Identitas IAM untuk mengelola akses berdasarkan atribut yang Anda lewati. PingOne

Sebelum Anda memulai prosedur ini, Anda harus terlebih dahulu mengaktifkan Atribut untuk kontrol akses fitur tersebut. Untuk informasi selengkapnya tentang cara melakukan ini, lihat Aktifkan dan konfigurasikan atribut untuk kontrol akses.

Untuk mengonfigurasi atribut pengguna PingOne untuk kontrol akses di Pusat Identitas IAM

1. Buka aplikasi PingOne IAM Identity Center yang Anda instal sebagai bagian dari konfigurasi SAFL untuk PingOne (Applications > My Applications).
2. Pilih Edit, lalu pilih Lanjutkan ke Langkah Berikutnya hingga Anda masuk ke halaman Pemetaan Atribut.
3. Pada halaman Pemetaan Atribut, pilih Tambahkan atribut baru, lalu lakukan hal berikut. Anda harus melakukan langkah-langkah ini untuk setiap atribut yang akan Anda tambahkan untuk digunakan di Pusat Identitas IAM untuk kontrol akses.

    a. Di bidang Atribut Aplikasi, masukkan`https://aws.amazon.com/SAML/Attributes/AccessControl:`*`AttributeName`*. Ganti *`AttributeName`*dengan nama atribut yang Anda harapkan di IAM Identity Center. Misalnya, `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`Email`**.

    b. Di bidang Atribut Jembatan Identitas atau Nilai Literal, pilih atribut pengguna dari PingOne direktori Anda. Misalnya, Email (Kerja).
4. Pilih Berikutnya beberapa kali, lalu pilih Selesai.

(Opsional) Melewati atribut untuk kontrol akses

Anda dapat secara opsional menggunakan Atribut untuk kontrol akses fitur di IAM Identity Center untuk meneruskan `Attribute` elemen dengan `Name` atribut yang disetel ke. `https://aws.amazon.com/SAML/Attributes/AccessControl:`**`{TagKey}`** Elemen ini memungkinkan Anda untuk meneruskan atribut sebagai tanda sesi dalam pernyataan SAML. Untuk informasi selengkapnya tentang tag sesi, lihat Melewati tag sesi AWS STS di Panduan Pengguna IAM.

Untuk menyampaikan atribut sebagai tag sesi, sertakan elemen `AttributeValue` yang menentukan nilai tag. Misalnya, untuk meneruskan pasangan nilai kunci tag`CostCenter = blue`, gunakan atribut berikut.

```
<saml:AttributeStatement>
```

```
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Jika Anda perlu menambahkan beberapa atribut, sertakan `Attribute` elemen terpisah untuk setiap tag.

Memulai tugas-tugas umum di IAM Identity Center

Jika Anda adalah pengguna baru IAM Identity Center, alur kerja dasar untuk mulai menggunakan layanan ini adalah:

1. Masuk ke konsol akun manajemen Anda jika Anda menggunakan instans organisasi Pusat Identitas IAM atau Akun AWS jika Anda menggunakan instance akun Pusat Identitas IAM dan arahkan ke konsol Pusat Identitas IAM.
2. Pilih direktori yang Anda gunakan untuk menyimpan identitas pengguna dan grup Anda dari konsol Pusat Identitas IAM. IAM Identity Center memberi Anda direktori secara default yang dapat Anda gunakan untuk mengonfigurasi akses pengguna. Jika Anda lebih suka menggunakan sumber identitas lain, Anda dapat menghubungkan direktori aktif atau penyedia identitas eksternal.
3. Untuk instance organisasi, tetapkan akses pengguna Akun AWS dengan memilih akun di organisasi Anda, lalu pilih pengguna atau grup dari direktori Anda dan izin yang ingin Anda berikan kepada mereka.
4. Berikan pengguna akses ke aplikasi dengan:
   a. Siapkan aplikasi SAMP 2.0 yang dikelola pelanggan dengan memilih salah satu aplikasi pra-terintegrasi dari katalog aplikasi atau menambahkan aplikasi SAMP 2.0 Anda sendiri.
   b. Konfigurasikan properti aplikasi.
   c. Tetapkan akses pengguna ke aplikasi. Kami menyarankan Anda menetapkan akses pengguna melalui keanggotaan grup daripada dengan menambahkan izin pengguna individu. Dengan grup, Anda dapat memberikan atau menolak izin ke grup pengguna, alih-alih menerapkan izin tersebut ke setiap individu. Jika pengguna pindah ke organisasi yang berbeda, Anda cukup memindahkan pengguna tersebut ke grup yang berbeda. Pengguna kemudian secara otomatis menerima izin yang diperlukan untuk organisasi baru.
5. Jika Anda menggunakan direktori IAM Identity Center default, beri tahu pengguna Anda cara masuk ke portal AWS akses. Pengguna baru di IAM Identity Center harus mengaktifkan kredensialnya sebelum dapat digunakan untuk masuk ke portal akses. AWS Untuk informasi selengkapnya, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna

Topik di bagian ini membantu membiasakan Anda dengan tugas-tugas umum yang dilakukan setelah Anda menyelesaikan konfigurasi awal Pusat Identitas IAM.

Jika Anda belum mengaktifkan IAM Identity Center, lihatMengaktifkan AWS IAM Identity Center.

Topik

Buat set izin

Set izin disimpan di Pusat Identitas IAM dan menentukan tingkat akses yang dimiliki pengguna dan grup ke. Akun AWS Set izin pertama yang Anda buat adalah set izin administratif. Jika Anda menyelesaikan salah satu dari Memulai tutorial Anda sudah membuat set izin administratif Anda. Gunakan prosedur ini untuk membuat kumpulan izin seperti yang dijelaskan dalam topik kebijakan AWS terkelola untuk fungsi pekerjaan di Panduan Pengguna IAM.

1. Lakukan salah satu dari berikut ini untuk masuk ke AWS Management Console.
   - Baru di AWS (pengguna root) - Masuk sebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di halaman berikutnya, masukkan kata sandi Anda.
   - Sudah menggunakan AWS (kredensil IAM) - Masuk menggunakan kredensil IAM Anda dengan izin administratif.
2. Buka konsol Pusat Identitas IAM.
3. Di panel navigasi Pusat Identitas IAM, di bawah izin Multi-akun, pilih Set izin.
4. Pilih Buat set izin.
   a. Pada halaman Pilih jenis set izin, di bagian Jenis set izin, pilih Set izin yang telah ditentukan sebelumnya.
   b. Di bagian Kebijakan untuk set izin yang telah ditentukan sebelumnya, pilih salah satu dari berikut ini:
      - AdministratorAccess
      - Penagihan
      - DatabaseAdministrator

- DataScientist
- NetworkAdministrator
- PowerUserAccess
- ReadOnlyAccess
- SecurityAudit
- SupportUser
- SystemAdministrator
- ViewOnlyAccess

5. Pada halaman Tentukan detail set izin, pertahankan pengaturan default dan pilih Berikutnya. Pengaturan default membatasi sesi Anda menjadi satu jam.
6. Pada halaman Tinjau dan buat, konfirmasikan hal berikut:

    1. Untuk Langkah 1: Pilih jenis set izin, menampilkan jenis set izin yang Anda pilih.
    2. Untuk Langkah 2: Tentukan rincian set izin, menampilkan nama set izin yang Anda pilih.
    3. Pilih Buat.

Buat set izin yang menerapkan izin hak istimewa paling sedikit

Untuk mengikuti praktik terbaik menerapkan izin hak istimewa terkecil, setelah Anda membuat set izin administratif, Anda membuat set izin yang lebih ketat dan menetapkannya ke satu atau beberapa pengguna. Set izin yang dibuat dalam prosedur sebelumnya memberikan titik awal bagi Anda untuk menilai jumlah akses ke sumber daya yang dibutuhkan pengguna Anda. Untuk beralih ke izin hak istimewa terkecil, Anda dapat menjalankan IAM Access Analyzer untuk memantau prinsipal dengan kebijakan terkelola. AWS Setelah mengetahui izin yang mereka gunakan, Anda dapat menulis kebijakan khusus atau membuat kebijakan hanya dengan izin yang diperlukan untuk tim Anda.

Dengan IAM Identity Center, Anda dapat menetapkan beberapa set izin ke pengguna yang sama. Pengguna administratif Anda juga harus diberi set izin tambahan yang lebih ketat. Dengan begitu, mereka dapat mengakses Anda hanya Akun AWS dengan izin yang diperlukan, daripada selalu menggunakan izin administratif mereka.

Misalnya, jika Anda seorang pengembang, setelah membuat pengguna administratif di Pusat Identitas IAM, Anda dapat membuat set izin baru yang memberikan izin, lalu menetapkan `PowerUserAccess` izin yang disetel ke diri Anda sendiri. Tidak seperti set izin administratif, yang menggunakan `AdministratorAccess` izin, set `PowerUserAccess` izin tidak mengizinkan

pengelolaan pengguna dan grup IAM. Ketika Anda masuk ke portal AWS akses untuk mengakses AWS akun Anda, Anda dapat memilih `PowerUserAccess` daripada `AdministratorAccess` untuk melakukan tugas pengembangan di akun.

Perhatikan sejumlah pertimbangan berikut:

- Untuk memulai dengan cepat dengan membuat set izin yang lebih ketat, gunakan set izin yang telah ditentukan sebelumnya daripada set izin khusus.

  Dengan set izin yang telah ditentukan, yang menggunakan izin yang telah ditentukan sebelumnya, Anda memilih satu kebijakan AWS terkelola dari daftar kebijakan yang tersedia. Setiap kebijakan memberikan tingkat akses tertentu ke AWS layanan dan sumber daya atau izin untuk fungsi pekerjaan umum. Untuk informasi tentang masing-masing kebijakan ini, lihat kebijakan AWS terkelola untuk fungsi pekerjaan.
- Anda dapat mengonfigurasi durasi sesi untuk izin yang disetel untuk mengontrol lamanya waktu pengguna masuk Akun AWS.

  Saat pengguna bergabung Akun AWS dan menggunakan AWS Management Console atau AWS Command Line Interface (AWS CLI), IAM Identity Center menggunakan pengaturan durasi sesi pada izin yang ditetapkan untuk mengontrol durasi sesi. Secara default, nilai untuk durasi Sesi, yang menentukan lamanya waktu pengguna dapat masuk Akun AWS sebelum AWS menandatangani pengguna keluar dari sesi, diatur ke satu jam. Anda dapat menentukan nilai maksimum 12 jam. Untuk informasi selengkapnya, lihat Tetapkan durasi sesi.
- Anda juga dapat mengonfigurasi durasi sesi portal AWS akses untuk mengontrol lamanya waktu pengguna tenaga kerja masuk ke portal.

  Secara default, nilai durasi sesi maksimum, yang menentukan lamanya waktu pengguna tenaga kerja dapat masuk ke portal AWS akses sebelum mereka harus mengautentikasi ulang, adalah delapan jam. Anda dapat menentukan nilai maksimum 90 hari. Untuk informasi selengkapnya, lihat Konfigurasikan durasi sesi portal AWS akses dan aplikasi terintegrasi IAM Identity Center.
- Saat Anda masuk ke portal AWS akses, pilih peran yang memberikan izin hak istimewa paling sedikit.

  Setiap set izin yang Anda buat dan tetapkan ke pengguna Anda muncul sebagai peran yang tersedia di portal AWS akses. Saat Anda masuk ke portal sebagai pengguna tersebut, pilih peran yang sesuai dengan set izin paling ketat yang dapat Anda gunakan untuk melakukan tugas di akun, bukan`AdministratorAccess`.

- Anda dapat menambahkan pengguna lain ke Pusat Identitas IAM dan menetapkan set izin yang ada atau baru untuk pengguna tersebut.

  Untuk informasi, lihat,Tetapkan Akun AWS akses untuk grup.

Tetapkan Akun AWS akses untuk pengguna Pusat Identitas IAM

Untuk mengatur Akun AWS akses bagi pengguna Pusat Identitas IAM, Anda harus menetapkan pengguna ke set izin Akun AWS dan.

1. Lakukan salah satu dari berikut ini untuk masuk ke AWS Management Console.

   - Baru di AWS (pengguna root) - Masuk sebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di halaman berikutnya, masukkan kata sandi Anda.
   - Sudah menggunakan AWS (kredensil IAM) - Masuk menggunakan kredensil IAM Anda dengan izin administratif.
2. Buka konsol Pusat Identitas IAM.
3. Di panel navigasi, di bawah Izin multi-akun, pilih. Akun AWS
4. Pada Akun AWShalaman, daftar tampilan pohon organisasi Anda ditampilkan. Pilih kotak centang di sebelah yang Akun AWS ingin Anda tetapkan aksesnya. Jika Anda menyiapkan akses administratif untuk Pusat Identitas IAM, pilih kotak centang di sebelah akun manajemen.
5. Pilih Tetapkan pengguna atau grup.
6. Untuk Langkah 1: Pilih pengguna dan grup, pada halaman Tetapkan pengguna dan grup ke "***Akun AWS nama***", lakukan hal berikut:

   1. Pada tab Pengguna, pilih pengguna yang ingin Anda berikan izin administratif.

      Untuk memfilter hasil, mulailah mengetik nama pengguna yang Anda inginkan di kotak pencarian.

   2. Setelah Anda mengonfirmasi bahwa pengguna yang benar dipilih, pilih Berikutnya.
7. Untuk Langkah 2: Pilih set izin, pada halaman Tetapkan set izin ke "***Akun AWS nama*** ", di bawah Set izin, pilih set izin untuk menentukan tingkat akses yang dimiliki pengguna dan grup untuk ini Akun AWS.
8. Pilih Berikutnya.

9. Untuk Langkah 3: Tinjau dan Kirim, pada Tinjau dan kirimkan tugas ke halaman "***Akun AWS nama***", lakukan hal berikut:

    1. Tinjau pengguna yang dipilih dan set izin.
    2. Setelah Anda mengonfirmasi bahwa pengguna yang benar ditetapkan ke set izin, pilih Kirim.

    > **Important**
    >
    > Proses penugasan pengguna mungkin membutuhkan waktu beberapa menit untuk diselesaikan. Biarkan halaman ini terbuka sampai proses berhasil diselesaikan.

10. Jika salah satu dari berikut ini berlaku, ikuti langkah-langkah Meminta pengguna untuk MFA untuk mengaktifkan MFA untuk Pusat Identitas IAM:

    - Anda menggunakan direktori Pusat Identitas default sebagai sumber identitas Anda.
    - Anda menggunakan AWS Managed Microsoft AD direktori atau direktori yang dikelola sendiri di Active Directory sebagai sumber identitas Anda dan Anda tidak menggunakan RADIUS AWS Directory Service MFA.

    > **Note**
    >
    > Jika Anda menggunakan penyedia identitas eksternal, perhatikan bahwa iDP eksternal, bukan Pusat Identitas IAM, mengelola pengaturan MFA. MFA di Pusat Identitas IAM tidak didukung untuk digunakan oleh eksternal. IdPs

Saat Anda mengatur akses akun untuk pengguna administratif, Pusat Identitas IAM akan membuat peran IAM yang sesuai. Peran ini, yang dikendalikan oleh Pusat Identitas IAM, dibuat dalam peran yang relevan Akun AWS, dan kebijakan yang ditentukan dalam kumpulan izin dilampirkan ke peran.

Masuk ke portal AWS akses dengan kredensil Pusat Identitas IAM Anda

Portal AWS akses menyediakan pengguna IAM Identity Center dengan akses masuk tunggal ke semua yang ditugaskan Akun AWS dan aplikasi mereka melalui portal web.

Selesaikan langkah-langkah berikut untuk mengonfirmasi bahwa pengguna IAM Identity Center dapat masuk ke portal AWS akses dan mengakses. Akun AWS

1. Lakukan salah satu dari berikut ini untuk masuk ke AWS Management Console.
   - Baru di AWS (pengguna root) - Masuk sebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di halaman berikutnya, masukkan kata sandi Anda.
   - Sudah menggunakan AWS (kredensil IAM) - Masuk dengan kredensil IAM Anda dan pilih peran admin.
2. Buka konsol Pusat Identitas IAM.
3. Di panel navigasi, pilih Dasbor.
4. Pada halaman Dasbor, di bawah Ringkasan pengaturan, pilih URL portal AWS akses.
5. Masuk dengan menggunakan salah satu dari berikut ini:
   - Jika Anda menggunakan Active Directory atau penyedia identitas eksternal (iDP) sebagai sumber identitas Anda, masuk dengan menggunakan kredensional Active Directory atau pengguna iDP.
   - Jika Anda menggunakan direktori Pusat Identitas default sebagai sumber identitas Anda, masuk dengan menggunakan nama pengguna yang Anda tentukan saat Anda membuat pengguna dan kata sandi baru yang Anda tentukan untuk pengguna.

Ada pengalaman portal yang berbeda tergantung pada lokasi Wilayah AWS Anda Akun AWS , Portal AWS akses standar, dan portal AWS akses Legacy.

Setelah Anda masuk ke portal AWS akses, jika Anda disajikan dengan Akun AWS ikon,

ikuti prosedur di tab Portal AWS akses Legacy, jika tidak, ikuti prosedur di tab Portal AWS akses standar.

Standard AWS access portal

1. Di tab Akun, cari Akun AWS dan perluas.
2. Peran yang tersedia untuk Anda ditampilkan. Misalnya, jika Anda diberi set AdministratorAccessizin dan set izin Penagihan, peran tersebut akan ditampilkan di portal AWS akses. Pilih nama peran IAM yang ingin Anda gunakan untuk sesi tersebut.

3. Jika Anda dialihkan ke AWS Management Console, Anda berhasil menyelesaikan pengaturan akses ke. Akun AWS

> **Note**
>
> Jika Anda tidak melihat Akun AWSdaftar apa pun, kemungkinan pengguna belum ditetapkan ke izin yang ditetapkan untuk akun tersebut. Untuk petunjuk tentang menetapkan pengguna ke set izin, lihatTetapkan akses pengguna ke Akun AWS.

Sekarang setelah Anda mengonfirmasi bahwa Anda dapat masuk menggunakan kredensil Pusat Identitas IAM, beralihlah ke browser yang Anda gunakan untuk masuk AWS Management Console dan keluar dari pengguna root atau kredensi pengguna IAM Anda.

> **Important**
>
> Kami sangat menyarankan agar Anda menggunakan kredensil pengguna administratif Pusat Identitas IAM ketika Anda masuk ke portal AWS akses untuk melakukan tugas administratif alih-alih menggunakan pengguna IAM atau kredenal pengguna root. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk memungkinkan pengguna lain mengakses akun dan aplikasi Anda, dan untuk mengelola Pusat Identitas IAM, buat dan tetapkan set izin hanya melalui IAM Identity Center.

Legacy AWS access portal

1. Pilih nama akun untuk menampilkan set izin yang tersedia.

   Saat Anda masuk, nama set izin yang ditetapkan pengguna akan muncul sebagai peran yang tersedia di portal AWS akses. Jika Anda menetapkan pengguna ini ke AdministratorAccessdan set izin Penagihan, peran tersebut akan muncul di portal AWS akses.
2. Pilih tautan Management Console di sebelah kanan nama set izin yang ingin Anda gunakan untuk sesi tersebut.
3. Jika Anda dialihkan ke AWS Management Console, Anda berhasil menyelesaikan pengaturan akses ke. Akun AWS

Sekarang setelah Anda mengonfirmasi bahwa Anda dapat masuk menggunakan kredensil Pusat Identitas IAM, beralihlah ke browser yang Anda gunakan untuk masuk AWS Management Console dan keluar dari pengguna root atau kredensi pengguna IAM Anda.

> **Important**
>
> Kami sangat menyarankan agar Anda menggunakan kredensil pengguna administratif Pusat Identitas IAM ketika Anda masuk ke portal AWS akses untuk melakukan tugas administratif alih-alih menggunakan pengguna IAM atau kredenal pengguna root. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk memungkinkan pengguna lain mengakses akun dan aplikasi Anda, dan untuk mengelola Pusat Identitas IAM, buat dan tetapkan set izin hanya melalui IAM Identity Center.

Tetapkan Akun AWS akses untuk grup

Setelah Anda membuat pengguna administratif di Pusat Identitas IAM dan membuat set izin tambahan yang dapat Anda gunakan untuk melakukan tugas dengan izin yang paling tidak memiliki hak istimewa, Anda dapat memberikan akses ke grup pengguna Anda. Akun AWS

Kami menyarankan Anda menetapkan akses langsung ke grup daripada ke pengguna individu. Misalnya, jika Anda membuat grup dan set izin berdasarkan unit organisasi, jika pengguna pindah ke unit organisasi yang berbeda, Anda cukup memindahkan pengguna tersebut ke grup yang berbeda dan mereka secara otomatis menerima izin yang diperlukan untuk unit organisasi baru dan kehilangan izin dari unit organisasi sebelumnya.

Untuk menetapkan akses grup pengguna ke Akun AWS

1. Buka konsol Pusat Identitas IAM.

   > **Note**
   >
   > Jika sumber identitas Anda adalah AWS Managed Microsoft AD pastikan bahwa konsol IAM Identity Center menggunakan Wilayah tempat AWS Managed Microsoft AD direktori Anda berada sebelum Anda pindah ke langkah berikutnya.

2. Di panel navigasi, di bawah Izin multi-akun, pilih. Akun AWS

3. Pada Akun AWShalaman, daftar tampilan pohon organisasi Anda akan muncul. Pilih kotak centang di sebelah satu atau lebih yang Akun AWS ingin Anda tetapkan akses masuk tunggal.

   > **Note**
   >
   > Anda dapat memilih hingga 10 Akun AWS per set izin.

4. Pilih Tetapkan pengguna atau grup.
5. Untuk Langkah 1: Pilih pengguna dan grup, pada halaman Tetapkan pengguna dan grup ke "***AWS-account-name*** ", pilih tab Grup, lalu pilih satu atau beberapa grup.

   Untuk memfilter hasil, mulailah mengetik nama grup yang Anda inginkan di kotak pencarian.

   Untuk menampilkan grup yang Anda pilih, pilih segitiga menyamping di samping Pengguna dan grup yang dipilih.

   Setelah Anda mengonfirmasi bahwa grup yang benar dipilih, pilih Berikutnya.
6. Untuk Langkah 2: Pilih set izin, pada halaman Tetapkan izin ke halaman "***AWS-account-name***", pilih satu atau beberapa set izin

   > **Note**
   >
   > Jika Anda tidak membuat set izin yang Anda inginkan sebelum memulai prosedur ini, pilih Buat set izin, dan ikuti langkah-langkahnyaBuat set izin. Setelah Anda membuat set izin yang ingin Anda terapkan, di konsol Pusat Identitas IAM, kembali ke Akun AWSdan ikuti instruksi hingga Anda mencapai Langkah 2: Pilih set izin. Ketika Anda mencapai langkah ini, pilih set izin baru yang Anda buat, dan lanjutkan ke langkah berikutnya dalam prosedur ini.

   Setelah Anda mengonfirmasi bahwa set izin yang benar dipilih, pilih Berikutnya.
7. Untuk Langkah 3: Tinjau dan Kirim, pada Tinjau dan kirimkan tugas ke halaman "***AWS-account-name***", lakukan hal berikut:

   1. Tinjau grup yang dipilih, dan set izin.
   2. Setelah Anda mengonfirmasi bahwa grup yang benar, dan set izin dipilih, pilih Kirim.

> **Important**
>
> Proses penugasan kelompok mungkin memakan waktu beberapa menit untuk diselesaikan. Biarkan halaman ini terbuka sampai proses berhasil diselesaikan.

> **Note**
>
> Anda mungkin perlu memberikan izin kepada pengguna atau grup untuk beroperasi di akun AWS Organizations manajemen. Karena ini adalah akun yang sangat istimewa, pembatasan keamanan tambahan mengharuskan Anda untuk memiliki FullAccess kebijakan IAM atau izin yang setara sebelum Anda dapat mengaturnya. Pembatasan keamanan tambahan ini tidak diperlukan untuk akun anggota mana pun di AWS organisasi Anda.

Atau, Anda dapat menggunakan AWS CloudFormationuntuk membuat dan menetapkan set izin dan menetapkan pengguna ke set izin tersebut. Pengguna kemudian dapat masuk ke portal AWS akses atau menggunakan perintah AWS Command Line Interface (AWS CLI).

Siapkan akses masuk tunggal ke aplikasi Anda

IAM Identity Center mendukung dua jenis aplikasi: aplikasi AWS terkelola dan aplikasi yang dikelola pelanggan.

AWS aplikasi terkelola dikonfigurasi langsung dari dalam konsol aplikasi yang relevan atau melalui API aplikasi.

Aplikasi yang dikelola pelanggan harus ditambahkan ke konsol Pusat Identitas IAM dan dikonfigurasi dengan metadata yang sesuai untuk Pusat Identitas IAM dan penyedia layanan. Anda dapat memilih dari katalog aplikasi yang umum digunakan yang mendukung SAMP 2.0, atau Anda dapat mengatur aplikasi SAMP 2.0 Anda sendiri atau aplikasi OAuth 2.0.

Langkah-langkah konfigurasi untuk mengatur akses masuk tunggal ke aplikasi bervariasi berdasarkan jenis aplikasi.

Siapkan aplikasi AWS terkelola

AWS aplikasi terkelola seperti Amazon Managed Grafana dan Amazon Monitron terintegrasi dengan IAM Identity Center dan dapat menggunakannya untuk otentikasi dan layanan direktori. Untuk menyiapkan aplikasi AWS terkelola agar berfungsi dengan IAM Identity Center, Anda harus mengonfigurasi aplikasi langsung dari konsol untuk layanan yang berlaku, atau Anda harus menggunakan API aplikasi.

Siapkan aplikasi dari katalog aplikasi

Anda dapat memilih aplikasi SAMP 2.0 dari katalog aplikasi yang umum digunakan di konsol IAM Identity Center. Gunakan prosedur ini untuk mengatur hubungan kepercayaan SAMP 2.0 antara IAM Identity Center dan penyedia layanan aplikasi Anda.

Untuk mengatur aplikasi dari katalog aplikasi

1. Buka konsol Pusat Identitas IAM.
2. Pilih Aplikasi.
3. Pilih tab yang dikelola Pelanggan.
4. Pilih Tambahkan aplikasi.
5. Pada halaman Pilih jenis aplikasi, di bawah Preferensi pengaturan, pilih Saya ingin memilih aplikasi dari katalog.
6. Di bawah Katalog aplikasi, mulailah mengetik nama aplikasi yang ingin Anda tambahkan di kotak pencarian.
7. Pilih nama aplikasi dari daftar saat muncul di hasil pencarian, lalu pilih Berikutnya.
8. Pada halaman Konfigurasi aplikasi, kolom Nama Tampilan dan Deskripsi diisi sebelumnya dengan detail yang relevan untuk aplikasi. Anda dapat mengedit informasi ini.
9. Di bawah metadata IAM Identity Center, lakukan hal berikut:
    a. Di bawah file metadata SAMP Pusat Identitas IAM, pilih Unduh untuk mengunduh metadata penyedia identitas.
    b. Di bawah sertifikat Pusat Identitas IAM, pilih Unduh sertifikat untuk mengunduh sertifikat penyedia identitas.

> **Note**
>
> Anda akan memerlukan file-file ini nanti ketika Anda mengatur aplikasi dari situs web penyedia layanan. Ikuti instruksi dari penyedia itu.

10. (Opsional) Di bawah Properti aplikasi, Anda dapat menentukan URL mulai aplikasi, status Relay, dan Durasi sesi. Untuk informasi selengkapnya, lihat Konfigurasikan properti aplikasi di konsol Pusat Identitas IAM.
11. Di bawah metadata Aplikasi, lakukan salah satu hal berikut:
    a. Jika Anda memiliki file metadata, pilih Unggah file metadata SAM aplikasi. Kemudian, pilih Pilih file untuk menemukan dan pilih file metadata.
    b. Jika Anda tidak memiliki file metadata, pilih Ketik nilai metadata Anda secara manual, lalu berikan URL ACS Aplikasi dan nilai audiens SAMP Aplikasi.
12. Pilih Kirim. Anda dibawa ke halaman detail aplikasi yang baru saja Anda tambahkan.

Siapkan aplikasi SAFL 2.0 Anda sendiri

Gunakan prosedur ini untuk mengatur hubungan kepercayaan SAMP 2.0 Anda sendiri antara IAM Identity Center dan penyedia layanan aplikasi SAMP 2.0 Anda sendiri. Sebelum Anda memulai prosedur ini, pastikan Anda memiliki sertifikat penyedia layanan dan file pertukaran metadata sehingga Anda dapat menyelesaikan pengaturan kepercayaan.

Untuk mengatur aplikasi SAFL 2.0 Anda sendiri

1. Buka konsol Pusat Identitas IAM.
2. Pilih Aplikasi.
3. Pilih tab yang dikelola Pelanggan.
4. Pilih Tambahkan aplikasi.
5. Pada halaman Pilih jenis aplikasi, di bawah preferensi Pengaturan, pilih Saya memiliki aplikasi yang ingin saya atur.
6. Di bawah Jenis aplikasi, pilih SAFL 2.0.
7. Pilih Berikutnya.

8. Pada halaman Konfigurasi aplikasi, di bawah Konfigurasi aplikasi, masukkan nama Tampilan untuk aplikasi, seperti**`MyApp`**. Kemudian, masukkan Deskripsi.
9. Di bawah metadata IAM Identity Center, lakukan hal berikut:

    a. Di bawah file metadata SAMP Pusat Identitas IAM, pilih Unduh untuk mengunduh metadata penyedia identitas.

    b. Di bawah sertifikat Pusat Identitas IAM, pilih Unduh untuk mengunduh sertifikat penyedia identitas.

    > **Note**
    >
    > Anda akan memerlukan file-file ini nanti ketika Anda mengatur aplikasi khusus dari situs web penyedia layanan.

10. (Opsional) Di bawah Properti aplikasi, Anda juga dapat menentukan URL mulai aplikasi, status Relay, dan Durasi sesi. Untuk informasi selengkapnya, lihat Konfigurasikan properti aplikasi di konsol Pusat Identitas IAM.
11. Di bawah Metadata aplikasi, pilih Ketik nilai metadata Anda secara manual. Kemudian, berikan URL ACS Aplikasi dan nilai audiens SALL Aplikasi.
12. Pilih Kirim. Anda dibawa ke halaman detail aplikasi yang baru saja Anda tambahkan.

Setelah Anda menyiapkan aplikasi, pengguna dapat mengakses aplikasi Anda dari dalam portal AWS akses mereka berdasarkan izin yang Anda tetapkan.

Jika Anda memiliki aplikasi yang dikelola pelanggan yang mendukung OAuth 2.0 dan pengguna Anda memerlukan akses dari aplikasi ini ke AWS layanan, Anda dapat menggunakan propagasi identitas tepercaya. Dengan propagasi identitas tepercaya, pengguna dapat masuk ke aplikasi, dan aplikasi itu dapat meneruskan identitas pengguna dalam permintaan untuk mengakses data dalam AWS layanan. Untuk informasi selengkapnya, lihat Menggunakan propagasi identitas tepercaya dengan aplikasi yang dikelola pelanggan.

Untuk informasi selengkapnya tentang jenis aplikasi yang didukung, lihatKelola akses ke aplikasi.

Lihat tugas pengguna dan grup

Anda dapat melihat siapa yang memiliki akses ke apa di Pusat Identitas IAM dari halaman Pengguna dan Grup. Gunakan prosedur ini untuk melihat tingkat akses yang dimiliki pengguna ke AWS akun, set izin, aplikasi, dan grup.

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengguna atau Grup berdasarkan apakah Anda ingin mengedit grup pengguna atau satu pengguna yang ditetapkan secara individual.
3. Pilih pengguna atau grup dari daftar.
4. Pilih apakah Anda ingin melihat penetapan akun, penetapan aplikasi, atau tugas grup:

   - AWS akun dan izin menetapkan tugas
     1. Pilih tab Akun.
     2. Pilih akun dari daftar untuk melihat penetapan set izin pengguna dan grup.
     3. Pilih set izin yang akan ditampilkan untuk melihat detail kebijakan dan penetapan.
   - Penugasan aplikasi
     1. Pilih tab Aplikasi untuk melihat aplikasi mana yang ditetapkan ke pengguna atau grup.
     2. Pilih aplikasi dari daftar untuk melihat detail tugas.
   - Penugasan kelompok
     1. Dari halaman Pengguna, pilih tab Grup.
     2. Pilih grup untuk melihat tugas grup bagi pengguna.

Mengelola instans organisasi dan akun IAM Identity Center

Instance adalah penyebaran tunggal IAM Identity Center. Ada dua jenis instance yang tersedia untuk IAM Identity Center: instance organisasi dan instans akun.

Akun AWS jenis yang dapat mengaktifkan Pusat Identitas IAM

Untuk mengaktifkan Pusat Identitas IAM, masuk ke AWS Management Console dengan menggunakan salah satu kredensi berikut, tergantung pada jenis instans yang ingin Anda buat:

- Akun AWS Organizations manajemen Anda (disarankan) - Diperlukan untuk membuat instance organisasi dari IAM Identity Center. Gunakan instance organisasi untuk izin multi-akun dan penetapan aplikasi di seluruh organisasi.
- Akun AWS Organizations anggota Anda — Gunakan untuk membuat instance akun IAM Identity Center untuk mengaktifkan penugasan aplikasi dalam akun anggota tersebut. Satu atau lebih akun dengan instance tingkat anggota dapat ada dalam suatu organisasi.
- Mandiri Akun AWS — Gunakan untuk membuat instance organisasi atau instance akun dari IAM Identity Center. Standalone Akun AWS tidak dikelola oleh AWS OrganizationsHanya satu instance IAM Identity Center yang dapat dikaitkan dengan standalone Akun AWS dan Anda dapat menggunakan instance untuk penugasan aplikasi dalam standalone itu. Akun AWS

Kemampuan	Instance di akun AWS Organizations manajemen (disarankan)	Instance di akun anggota	Instance dalam standalone Akun AWS
Mengelola pengguna	 Y	 Y	 Ya
AWS akses portal untuk akses masuk tunggal ke aplikasi AWS terkelola Anda	 Y	 Y	 Ya

Kemampuan	Instance di akun AWS Organizations manajemen (disarankan)	Instance di akun anggota	Instance dalam standalone Akun AWS
Izin multi-akun	 Y	 T	 Tidak
AWS akses portal untuk akses masuk tunggal ke Anda Akun AWS	 Y	 T	 Tidak
Aplikasi yang dikelola pelanggan	 Y	 T	 Tidak
Administrator yang didelegasikan dapat mengelola instance	 Y	 T	 Tidak

Topik

- Contoh organisasi Pusat Identitas IAM
- Instans akun Pusat Identitas IAM
- Aktifkan instance akun di AWS Management Console
- Kontrol pembuatan instans akun dengan Kebijakan Kontrol Layanan
- Buat instance akun dari IAM Identity Center

Contoh organisasi Pusat Identitas IAM

Saat Anda mengaktifkan Pusat Identitas IAM bersama dengan AWS Organizations, Anda membuat instance organisasi dari IAM Identity Center. Instans organisasi Anda harus diaktifkan di akun manajemen Anda dan Anda dapat mengelola akses pengguna dan grup secara terpusat dengan satu

instans organisasi. Anda hanya dapat memiliki satu instans organisasi untuk setiap akun manajemen AWS Organizations.

Jika Anda mengaktifkan Pusat Identitas IAM sebelum 15 November 2023, Anda memiliki instans organisasi Pusat Identitas IAM.

Kapan menggunakan instance organisasi

Sebuah instance organisasi adalah metode utama untuk mengaktifkan IAM Identity Center dan dalam banyak kasus, sebuah instance organisasi direkomendasikan. Contoh organisasi menawarkan manfaat berikut:

- Support untuk semua fitur IAM Identity Center — Termasuk mengelola izin untuk beberapa Akun AWS di organisasi Anda dan menetapkan akses ke aplikasi yang dikelola pelanggan.
- Kurangi jumlah poin manajemen — Sebuah contoh organisasi memiliki satu titik manajemen, akun manajemen. Sebaiknya aktifkan instans organisasi, bukan instans akun, untuk mengurangi jumlah poin manajemen.
- Kontrol pembuatan instans akun — Anda dapat mengontrol apakah instans akun dapat dibuat oleh akun anggota di organisasi Anda selama Anda belum menerapkan instance Pusat Identitas IAM ke organisasi Anda di Wilayah keikutsertaan (Wilayah AWS yang dinonaktifkan secara default).

Instans akun Pusat Identitas IAM

Dengan instance akun IAM Identity Center, Anda dapat menerapkan aplikasi terkelola yang didukung dan aplikasi yang AWS dikelola pelanggan berbasis OIDC. Instans akun mendukung penerapan aplikasi yang terisolasi dalam satu Akun AWS, memanfaatkan identitas tenaga kerja IAM Identity Center dan mengakses fitur portal.

Instans akun terikat pada satu Akun AWS dan hanya digunakan untuk mengelola akses pengguna dan grup untuk aplikasi yang didukung di akun yang sama dan Wilayah AWS. Anda dibatasi untuk satu contoh akun per Akun AWS. Anda dapat membuat instance akun dari salah satu dari berikut ini:

- Akun anggota di AWS Organizations.
- Sebuah standalone Akun AWS yang tidak dikelola oleh AWS Organizations.

Kendala ketersediaan untuk akun anggota

Anda dapat menerapkan instance akun di akun anggota organisasi jika berikut ini benar:

- Anda tidak memiliki instance Pusat Identitas IAM yang diterapkan ke organisasi Anda sebelum 15 November 2023.
- Anda memiliki instance IAM Identity Center yang diterapkan ke organisasi Anda sebelum 15 November 2023 secara default Wilayah AWS diaktifkan dan administrator Anda telah memilih fitur instans akun.
- Administrator Anda belum membuat Kebijakan Kontrol Layanan yang mencegah pembuatan instance akun.
- Anda sudah memiliki instance IAM Identity Center di akun yang sama ini terlepas dari. Wilayah AWS
- Anda belum menerapkan instance Pusat Identitas IAM ke organisasi Anda di Wilayah keikutsertaan (Wilayah AWS yang dinonaktifkan secara default) terlepas dari tanggal penerapan. Artinya, setiap instance organisasi dari IAM Identity Center yang digunakan dalam opt-in Wilayah AWS akan mencegah pembuatan instance akun.
- Anda bekerja di Wilayah AWS tempat Pusat Identitas IAM tidak tersedia. Untuk informasi tentang Wilayah, lihatAWS IAM Identity Center Ketersediaan wilayah.

Topik

Kapan menggunakan instance akun

Dalam kebanyakan kasus, contoh organisasi direkomendasikan. Instans akun harus digunakan hanya jika salah satu skenario berikut berlaku:

- Anda ingin menjalankan uji coba sementara aplikasi AWS terkelola yang didukung untuk menentukan apakah aplikasi tersebut sesuai dengan kebutuhan bisnis Anda.
- Anda tidak memiliki rencana untuk mengadopsi IAM Identity Center di seluruh organisasi Anda, tetapi Anda ingin mendukung satu atau lebih aplikasi AWS terkelola.
- Anda memiliki instans organisasi IAM Identity Center, tetapi Anda ingin menerapkan aplikasi AWS terkelola yang didukung ke kumpulan pengguna terisolasi yang berbeda dari pengguna di instans organisasi Anda.

> **Important**
>
> Jika Anda berencana menggunakan IAM Identity Center untuk mendukung aplikasi di beberapa akun, buat instance organisasi dan jangan gunakan instance akun.

Pertimbangan contoh akun

Instans akun dirancang untuk kasus penggunaan khusus, menawarkan subset fitur yang tersedia untuk instance organisasi. Pertimbangkan hal berikut sebelum membuat instance akun:

- Instans akun tidak mendukung set izin dan oleh karena itu tidak mendukung akses ke Akun AWS.
- Anda tidak dapat mengonversi instance akun menjadi instans organisasi.
- Anda tidak dapat menggabungkan instance akun ke instans organisasi.
- Hanya pilih aplikasiAWS terkelola yang mendukung instans akun.
- Gunakan instance akun untuk pengguna terisolasi yang akan menggunakan aplikasi dalam satu akun saja dan seumur hidup aplikasi yang digunakan.
- Aplikasi yang dilampirkan ke instance akun harus tetap dilampirkan ke instance akun sampai Anda menghapus aplikasi dan sumber dayanya.
- Contoh akun harus tetap berada di Akun AWS tempat pembuatannya.
- Pembuatan instans akun akan diblokir setelah Anda membuat instance organisasi jika Anda menerapkan instance Pusat Identitas IAM ke organisasi Anda di Wilayah keikutsertaan (Wilayah AWS yang dinonaktifkan secara default). Instans akun yang ada akan terus berfungsi.

Aplikasi AWS terkelola yang didukung

Berikut adalah beberapa AWS aplikasi yang mendukung instance akun. Verifikasi ketersediaan pembuatan instans akun dengan aplikasi AWS terkelola Anda.

- Amazon Athena
- Amazon CodeCatalyst
- Amazon EMR
- AWS Lake Formation
- Amazon Redshift

Aktifkan instance akun di AWS Management Console

Jika Anda mengaktifkan Pusat Identitas IAM sebelum 15 November 2023, Anda memiliki instans organisasi Pusat Identitas IAM dan kemampuan akun anggota untuk membuat instance akun dinonaktifkan secara default. Anda dapat memilih apakah akun anggota Anda dapat membuat instance akun dengan mengaktifkan fitur instans akun di. AWS Management Console

> **Note**
>
> Akun anggota dapat membuat instance akun selama Anda belum menerapkan instance Pusat Identitas IAM ke organisasi Anda di Wilayah keikutsertaan (Wilayah AWS yang dinonaktifkan secara default) terlepas dari tanggal penerapan. Setiap instans organisasi dari IAM Identity Center yang digunakan dalam opt-in Wilayah AWS akan mencegah pembuatan instance akun. Untuk informasi tentang Wilayah, lihatAWS IAM Identity Center Ketersediaan wilayah.

Untuk mengaktifkan pembuatan instans akun oleh akun anggota di organisasi Anda

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan, lalu pilih tab Manajemen.
3. Di bagian Instance Akun Pusat Identitas IAM, pilih Aktifkan instans akun dari Pusat Identitas IAM.
4. Di kotak dialog Aktifkan instance akun Pusat Identitas IAM, konfirmasikan bahwa Anda ingin mengizinkan akun anggota di organisasi Anda untuk membuat instance akun dengan memilih Aktifkan.

> **Important**
>
> Mengaktifkan instance akun Pusat Identitas IAM untuk akun anggota adalah tindakan satu kali. Ini berarti bahwa tindakan ini tidak dapat dibalik. Setelah diaktifkan, Anda dapat membatasi pembuatan instance akun dengan membuat kebijakan kontrol layanan (SCP). Untuk petunjuknya, lihat Mengontrol pembuatan instans akun dengan Kebijakan Kontrol Layanan.

Kontrol pembuatan instans akun dengan Kebijakan Kontrol Layanan

Pengguna dapat membuat instance IAM Identity Center yang terikat pada satu Akun AWS, yang disebut instance akun IAM Identity Center. Anda dapat mengontrol pembuatan instans akun dengan Kebijakan Kontrol Layanan (SCP).

1. Buka konsol Pusat Identitas IAM.
2. Di Dasbor, di bagian Manajemen pusat, pilih tombol Cegah instans akun.
3. Di kotak dialog Lampirkan SCP untuk mencegah pembuatan instance akun baru, SCP disediakan untuk Anda. Salin SCP dan pilih tombol Go to SCP dashboard. Anda akan diarahkan ke AWS Organizations konsol untuk membuat SCP atau melampirkannya sebagai pernyataan ke SCP yang ada.

   Kebijakan kontrol layanan adalah fitur dari AWS Organizations. Untuk petunjuk tentang melampirkan SCP, lihat Melampirkan dan melepaskan kebijakan kontrol layanan di Panduan Pengguna.AWS Organizations

Daripada mencegah pembuatan instans akun, Anda dapat membatasi pembuatan instans akun ke spesifik Akun AWS dalam organisasi Anda:

Example : SCP untuk mengontrol pembuatan instance

```
{
    "Version": "2012-10-17",
    "Statement" : [
        {
            "Sid": "DenyMemberAccountInstances",
            "Effect": "Deny",
            "Action": "sso:CreateInstance",
            "Resource": "*",
            "Condition": {
                 "StringNotEquals": {
                    "aws:PrincipalAccount": ["<ALLOWED-ACCOUNT-ID>"]
                }
            }
        }
    ]
}
```

Buat instance akun dari IAM Identity Center

Sebuah instance organisasi adalah metode utama dan direkomendasikan untuk mengaktifkan IAM Identity Center. Pastikan kasus penggunaan Anda mendukung pembuatan instance akun dan Anda mengetahui pertimbangannya.

Buat instance akun dari akun anggota organisasi atau mandiri Akun AWS

1. Lakukan salah satu dari berikut ini untuk masuk ke AWS Management Console.
   - Baru di AWS (pengguna root) - Masuk sebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di halaman berikutnya, masukkan kata sandi Anda.
   - Sudah menggunakan AWS (kredensi IAM) - Masuk menggunakan kredenal IAM Anda dengan izin administratif.
2. Buka konsol Pusat Identitas IAM.
3. Di bawah Aktifkan Pusat Identitas IAM, pilih Aktifkan.
4. Pilih Lanjutkan membuat instance akun dan pilih Lanjutkan.

> **Note**
>
> Jika instans organisasi dari IAM Identity Center ada, pastikan bahwa kasus penggunaan Anda memerlukan instance akun sendiri dari IAM Identity Center. Jika tidak, pilih Batal dan gunakan instance organisasi.

5. Opsional. Tambahkan tag yang ingin Anda kaitkan dengan instance akun ini.

Pemberitahuan di konsol menunjukkan instance akun yang berhasil dibuat dan menyertakan ID instans. Anda dapat memberi nama instance Anda di ringkasan Pengaturan.

> **Note**
>
> Otentikasi multi-faktor (MFA) diaktifkan secara default untuk instance akun. Pengguna diminta untuk masuk dengan MFA saat perangkat, browser, atau lokasi mereka berubah. Sebagai praktik keamanan terbaik, kami sangat merekomendasikan MFA untuk identitas tenaga kerja Anda. Pelajari tentang Kelola perangkat MFA di Pusat Identitas IAM.

Fitur manajemen seperti mengonfirmasi sumber identitas Anda, menyesuaikan pengaturan otentikasi multi-faktor, dan menambahkan aplikasi AWS terkelola harus diselesaikan di konsol Pusat Identitas IAM.

Autentikasi

Pengguna masuk ke portal AWS akses menggunakan nama pengguna mereka. Ketika mereka melakukannya, IAM Identity Center mengalihkan permintaan ke layanan otentikasi IAM Identity Center berdasarkan direktori yang terkait dengan alamat email pengguna. Setelah diautentikasi, pengguna memiliki akses masuk tunggal ke salah satu AWS akun dan aplikasi pihak ketiga (software-as-a-service SaaS) yang muncul di portal tanpa petunjuk masuk tambahan. Ini berarti bahwa pengguna tidak perlu lagi melacak beberapa kredensi akun untuk berbagai AWS aplikasi yang ditugaskan yang mereka gunakan setiap hari.

Sesi otentikasi

Ada dua jenis sesi otentikasi yang dikelola oleh IAM Identity Center: satu untuk mewakili pengguna masuk ke IAM Identity Center, dan satu lagi untuk mewakili akses pengguna ke aplikasi yang AWS dikelola, seperti Amazon Studio SageMaker atau Amazon Managed Grafana. Setiap kali pengguna masuk ke Pusat Identitas IAM, sesi masuk dibuat untuk durasi yang dikonfigurasi di Pusat Identitas IAM, yang dapat mencapai 90 hari. Untuk informasi selengkapnya, lihat Mengelola durasi sesi portal AWS akses dan aplikasi terintegrasi IAM Identity Center. Setiap kali pengguna mengakses aplikasi, sesi masuk Pusat Identitas IAM digunakan untuk mendapatkan sesi aplikasi Pusat Identitas IAM untuk aplikasi itu. Sesi aplikasi IAM Identity Center memiliki masa pakai 1 jam yang dapat disegarkan - yaitu, sesi aplikasi IAM Identity Center secara otomatis diperbarui setiap jam selama sesi masuk Pusat Identitas IAM dari mana mereka diperoleh masih berlaku. Ketika pengguna menggunakan Pusat Identitas IAM untuk mengakses AWS Management Console atau CLI, sesi masuk Pusat Identitas IAM digunakan untuk mendapatkan sesi IAM, sebagaimana ditentukan dalam set izin Pusat Identitas IAM yang sesuai (lebih khusus lagi, Pusat Identitas IAM mengasumsikan peran IAM, yang dikelola Pusat Identitas IAM, di akun target).

Saat Anda menonaktifkan atau menghapus pengguna di Pusat Identitas IAM, pengguna tersebut akan segera dicegah masuk untuk membuat sesi masuk Pusat Identitas IAM baru. Sesi masuk Pusat Identitas IAM di-cache selama satu jam, yang berarti bahwa ketika Anda menonaktifkan atau menghapus pengguna saat mereka memiliki sesi masuk Pusat Identitas IAM yang aktif, sesi masuk Pusat Identitas IAM yang ada akan berlanjut hingga satu jam, tergantung kapan sesi masuk terakhir disegarkan. Selama waktu ini, pengguna dapat memulai aplikasi IAM Identity Center baru dan sesi peran IAM.

Setelah sesi masuk Pusat Identitas IAM berakhir, pengguna tidak dapat lagi memulai aplikasi Pusat Identitas IAM baru atau sesi peran IAM. Namun, sesi aplikasi IAM Identity Center juga dapat di-cache

hingga satu jam, sehingga pengguna dapat mempertahankan akses ke aplikasi hingga satu jam setelah sesi masuk Pusat Identitas IAM kedaluwarsa. Setiap sesi peran IAM yang ada akan berlanjut berdasarkan durasi yang dikonfigurasi dalam set izin Pusat Identitas IAM (dapat dikonfigurasi admin, hingga 12 jam).

Tabel di bawah ini merangkum perilaku ini:

Pengalaman pengguna/perilaku sistem	Waktu setelah pengguna dinonaktifkan/dihapus
Pengguna tidak dapat lagi masuk ke Pusat Identitas IAM; pengguna tidak dapat memperoleh sesi masuk Pusat Identitas IAM baru	Tidak ada (efektif segera)
Pengguna tidak dapat lagi memulai aplikasi baru atau sesi peran IAM melalui IAM Identity Center	Hingga 1 jam
Pengguna tidak dapat lagi mengakses aplikasi apa pun (semua sesi aplikasi dihentikan)	Hingga 2 jam (hingga 1 jam untuk kedaluwarsa sesi masuk IAM Identity Center, ditambah hingga 1 jam untuk kedaluwarsa sesi aplikasi IAM Identity Center)
Pengguna tidak dapat lagi mengaksesnya Akun AWS melalui IAM Identity Center	Hingga 13 jam (hingga 1 jam untuk kedaluwarsa sesi masuk IAM Identity Center, ditambah hingga 12 jam untuk kedaluwarsa sesi peran IAM yang dikonfigurasi administrator per pengaturan durasi sesi IAM Identity Center untuk set izin)

Untuk informasi lebih lanjut tentang sesi, lihatTetapkan durasi sesi.

Mengelola identitas tenaga kerja

AWS Identity and Access Management(IAM) membantu Anda mengelola identitas dan akses ke AWS layanan dan sumber daya dengan aman. Sebagai layanan IAM, AWS IAM Identity Center adalah tempat Anda membuat, atau menghubungkan, identitas tenaga kerja Anda AWS sekaligus dan mengelola akses secara terpusat ke beberapa dan aplikasi Anda. Akun AWS

Untuk pelanggan IAM Identity Center, tidak ada perubahan pada cara Anda mengelola akses ke beberapa Akun AWS atau aplikasi secara terpusat. Untuk pelanggan baru ke IAM Identity Center, Anda dapat secara fleksibel mengkonfigurasi IAM Identity Center untuk berjalan bersama atau mengganti manajemen Akun AWS akses tunggal menggunakan IAM.

Topik

Kasus penggunaan

Berikut ini adalah kasus penggunaan yang menunjukkan bagaimana Anda dapat menggunakan IAM Identity Center untuk memenuhi kebutuhan bisnis yang berbeda.

Topik

Aktifkan akses masuk tunggal ke AWS aplikasi Anda (Peran admin aplikasi)

Kasus penggunaan ini memberikan panduan jika Anda adalah administrator aplikasi yang mengelola AWS aplikasi terkelola seperti Amazon SageMaker atauAWS IoT SiteWise, dan Anda harus memberikan akses masuk tunggal ke pengguna Anda.

Sebelum Anda memulai, pertimbangkan hal berikut:

- Apakah Anda ingin membuat lingkungan pengujian atau produksi di organisasi terpisah diAWS Organizations?
- Apakah Pusat Identitas IAM sudah diaktifkan di organisasi Anda? Apakah Anda memiliki izin untuk mengaktifkan Pusat Identitas IAM di akun manajemen? AWS Organizations

Tinjau panduan berikut untuk menentukan langkah selanjutnya berdasarkan kebutuhan bisnis Anda.

Konfigurasikan AWS aplikasi saya secara mandiri Akun AWS

Jika Anda harus menyediakan akses masuk tunggal ke AWS aplikasi dan mengetahui bahwa departemen TI Anda belum menggunakan IAM Identity Center, Anda mungkin perlu membuat standalone Akun AWS untuk memulai. Secara default, ketika Anda membuat sendiriAkun AWS, Anda akan memiliki izin yang Anda perlukan untuk membuat dan mengelola AWS organisasi Anda sendiri. Untuk mengaktifkan Pusat Identitas IAM, Anda harus memiliki Pengguna root akun AWS izin.

IAM Identity Center dan AWS Organizations dapat diaktifkan secara otomatis selama penyiapan untuk beberapa AWS aplikasi (misalnya, Amazon Managed Grafana). Jika AWS aplikasi Anda tidak menyediakan opsi untuk mengaktifkan layanan ini, Anda harus menyiapkan AWS Organizations dan Pusat Identitas IAM sebelum Anda dapat memberikan akses masuk tunggal ke aplikasi Anda.

Pusat Identitas IAM tidak dikonfigurasi di organisasi saya

Dalam peran Anda sebagai administrator aplikasi, Anda mungkin tidak dapat mengaktifkan Pusat Identitas IAM, tergantung pada izin Anda. Pusat Identitas IAM memerlukan izin khusus di akun AWS Organizations manajemen. Dalam hal ini, hubungi administrator yang sesuai untuk mengaktifkan Pusat Identitas IAM di akun manajemen Organisasi.

Jika Anda memiliki izin yang cukup untuk mengaktifkan IAM Identity Center, lakukan ini terlebih dahulu, lalu lanjutkan dengan pengaturan aplikasi. Untuk informasi selengkapnya, lihat Memulai tugas-tugas umum di IAM Identity Center.

Pusat Identitas IAM saat ini dikonfigurasi di organisasi saya

Dalam skenario ini, Anda dapat terus menerapkan AWS aplikasi Anda tanpa mengambil tindakan lebih lanjut.

> **Note**
>
> Jika organisasi Anda mengaktifkan Pusat Identitas IAM di akun manajemen sebelum 25 November 2019, Anda juga harus mengaktifkan aplikasi AWS terkelola di akun manajemen

dan secara opsional di akun anggota. Jika Anda mengaktifkannya hanya di akun manajemen, Anda dapat mengaktifkannya di akun anggota nanti. Untuk mengaktifkan aplikasi ini, pilih Aktifkan akses di halaman Pengaturan konsol IAM Identity Center di bagian aplikasi AWS terkelola. Untuk informasi selengkapnya, lihat Mengkonfigurasi IAM Identity Center untuk berbagi informasi identitas .

Aktifkan akses masuk tunggal ke instans Windows Amazon EC2

Anda dapat mengaktifkan akses masuk tunggal ke instans Windows Amazon EC2 jika Anda adalah administrator aplikasi yang mengelola pengguna di direktori Pusat Identitas (sumber identitas default untuk Pusat Identitas IAM) atau penyedia identitas eksternal (iDP) yang didukung, dan Anda harus memberikan akses Pusat Identitas IAM ke desktop Windows Amazon EC2 dari konsol Fleet Manager. AWS

Dengan konfigurasi ini, Anda dapat mengakses instans Windows Amazon EC2 dengan aman dengan kredensi perusahaan yang ada. Anda tidak perlu berbagi kredensi administrator, mengakses kredensi beberapa kali, atau mengonfigurasi perangkat lunak klien akses jarak jauh. Anda dapat secara terpusat memberikan dan mencabut akses ke instans Windows Amazon EC2 Anda dalam skala besar di beberapa. Akun AWS Misalnya, jika Anda menghapus karyawan dari sumber identitas terintegrasi IAM Identity Center, mereka secara otomatis kehilangan akses ke semua AWS sumber daya, termasuk instans Windows Amazon EC2.

Untuk informasi selengkapnya, lihat Cara mengaktifkan sistem masuk tunggal yang aman ke instans Windows Amazon EC2 dengan IAM Identity Center.

Untuk demonstrasi cara mengonfigurasi Pusat Identitas IAM untuk mengaktifkan kemampuan ini, lihat Mengaktifkan Single Sign-on ke Amazon EC2 Windows dengan IAM Identity Center.

Pengguna, grup, dan penyediaan

Ingatlah pertimbangan berikut saat Anda bekerja dengan pengguna dan grup di Pusat Identitas IAM.

Keunikan nama pengguna dan alamat email

Pengguna di IAM Identity Center harus dapat diidentifikasi secara unik. IAM Identity Center mengimplementasikan nama pengguna yang merupakan pengenal utama bagi pengguna Anda. Meskipun kebanyakan orang menetapkan nama pengguna sama dengan alamat email pengguna, IAM Identity Center dan standar SALL 2.0 tidak memerlukan ini. Namun, banyak aplikasi

berbasis SAFL 2.0 menggunakan alamat email sebagai pengenal unik bagi pengguna. Aplikasi ini memperoleh informasi ini dari pernyataan yang dikirim oleh penyedia identitas SAFL 2.0 selama otentikasi. Aplikasi semacam itu tergantung pada keunikan alamat email untuk setiap pengguna. Untuk alasan ini, IAM Identity Center memungkinkan Anda untuk menentukan sesuatu selain alamat email untuk login pengguna. IAM Identity Center mensyaratkan bahwa semua nama pengguna dan alamat email untuk pengguna Anda adalah non-Null dan unik.

Grup

Grup adalah kombinasi logis dari pengguna yang Anda tentukan. Anda dapat membuat grup dan menambahkan pengguna ke grup. Pusat Identitas IAM tidak mendukung penambahan grup ke grup (grup bersarang). Grup berguna saat menetapkan akses ke Akun AWS dan aplikasi. Daripada menetapkan setiap pengguna satu per satu, Anda memberikan izin ke grup. Kemudian, saat Anda menambah atau menghapus pengguna dari grup, pengguna secara dinamis mendapatkan atau kehilangan akses ke akun dan aplikasi yang Anda tetapkan ke grup.

Penyediaan pengguna dan grup

Provisioning adalah proses membuat informasi pengguna dan grup tersedia untuk digunakan oleh IAM Identity Center dan aplikasi terkelola atau aplikasi yang AWS dikelola pelanggan. Anda dapat membuat pengguna dan grup secara langsung di Pusat Identitas IAM, atau bekerja dengan pengguna dan grup yang Anda miliki di Active Directory atau penyedia identitas eksternal. Sebelum Anda dapat menggunakan Pusat Identitas IAM untuk menetapkan izin akses pengguna dan grup dalam sebuahAkun AWS, Pusat Identitas IAM harus mengetahui pengguna dan grup. Demikian pula, aplikasi AWS terkelola dan aplikasi yang dikelola pelanggan dapat bekerja dengan pengguna dan grup yang disadari oleh IAM Identity Center.

Penyediaan di IAM Identity Center bervariasi berdasarkan sumber identitas yang Anda gunakan. Untuk informasi selengkapnya, lihat Kelola sumber identitas Anda.

Kelola sumber identitas Anda

Sumber identitas Anda di IAM Identity Center menentukan di mana pengguna dan grup Anda dikelola. Setelah mengonfigurasi sumber identitas, Anda dapat mencari pengguna atau grup untuk memberi mereka akses masuk tunggal ke Akun AWS aplikasi, atau keduanya.

Anda hanya dapat memiliki satu sumber identitas per organisasi diAWS Organizations. Anda dapat memilih salah satu dari berikut ini sebagai sumber identitas Anda:

- Direktori Pusat Identitas - Ketika Anda mengaktifkan IAM Identity Center untuk pertama kalinya, secara otomatis dikonfigurasi dengan direktori Pusat Identitas sebagai sumber identitas default Anda. Di sinilah Anda membuat pengguna dan grup, dan menetapkan tingkat akses mereka ke aplikasi Akun AWS dan Anda.
- Active Directory - Pilih opsi ini jika Anda ingin terus mengelola pengguna di AWS Managed Microsoft AD direktori Anda menggunakan AWS Directory Service atau direktori yang dikelola sendiri diActive Directory (AD).
- Penyedia identitas eksternal — Pilih opsi ini jika Anda ingin mengelola pengguna di penyedia identitas eksternal (iDP) seperti Okta atau. Microsoft Entra ID

> **Note**
>
> IAM Identity Center tidak mendukung Simple AD berbasis Samba4 sebagai sumber identitas.

Topik

Pertimbangan untuk mengubah sumber identitas Anda

Meskipun Anda dapat mengubah sumber identitas kapan saja, kami sarankan Anda mempertimbangkan bagaimana perubahan ini dapat memengaruhi penerapan Anda saat ini.

Jika Anda sudah mengelola pengguna dan grup dalam satu sumber identitas, mengubah ke sumber identitas yang berbeda dapat menghapus semua penetapan pengguna dan grup yang Anda konfigurasikan di Pusat Identitas IAM. Jika ini terjadi, semua pengguna, termasuk pengguna administratif di IAM Identity Center, akan kehilangan akses masuk tunggal ke aplikasi dan aplikasi mereka Akun AWS .

Sebelum Anda mengubah sumber identitas untuk IAM Identity Center, tinjau pertimbangan berikut sebelum Anda melanjutkan. Jika Anda ingin melanjutkan dengan mengubah sumber identitas Anda, lihat Ubah sumber identitas Anda untuk informasi lebih lanjut.

Perubahan antara IAM Identity Center dan Active Directory

Jika Anda sudah mengelola pengguna dan grup di Active Directory, sebaiknya pertimbangkan untuk menghubungkan direktori saat mengaktifkan IAM Identity Center dan memilih sumber identitas Anda. Lakukan ini sebelum Anda membuat pengguna dan grup apa pun di direktori Pusat Identitas default dan buat tugas apa pun.

Jika Anda sudah mengelola pengguna dan grup di direktori Pusat Identitas default, pertimbangkan hal berikut:

- Penugasan dihapus dan pengguna dan grup dihapus — Mengubah sumber identitas Anda ke Active Directory menghapus pengguna dan grup Anda dari direktori Pusat Identitas. Perubahan ini juga menghapus tugas Anda. Dalam hal ini, setelah Anda mengubah ke Active Directory, Anda harus menyinkronkan pengguna dan grup dari Active Directory ke direktori Pusat Identitas, dan kemudian menerapkan kembali tugas mereka.

  Jika Anda memilih untuk tidak menggunakan Active Directory, Anda harus membuat pengguna dan grup di direktori Pusat Identitas, dan kemudian membuat tugas.
- Penugasan tidak dihapus saat identitas dihapus — Saat identitas dihapus di direktori Pusat Identitas, tugas yang sesuai juga akan dihapus di Pusat Identitas IAM. Namun di Active Directory, ketika identitas dihapus (baik di Active Directory atau identitas yang disinkronkan), tugas yang sesuai tidak dihapus.
- Tidak ada sinkronisasi keluar untuk API — Jika Anda menggunakan Active Directory sebagai sumber identitas, sebaiknya gunakan API Buat, Perbarui, dan Hapus dengan hati-hati. Pusat Identitas IAM tidak mendukung sinkronisasi keluar, sehingga sumber identitas Anda tidak diperbarui secara otomatis dengan perubahan yang Anda buat pada pengguna atau grup yang menggunakan API ini.
- URL portal akses akan berubah — Mengubah sumber identitas Anda antara IAM Identity Center dan Active Directory juga mengubah URL untuk portal AWS akses.

Untuk informasi tentang cara IAM Identity Center menyediakan pengguna dan grup, lihatConnect ke Microsoft AD direktori.

Mengubah dari IAM Identity Center ke iDP eksternal

Jika Anda mengubah sumber identitas dari IAM Identity Center ke penyedia identitas eksternal (iDP), pertimbangkan hal berikut:

- Penugasan dan keanggotaan berfungsi dengan pernyataan yang benar — tugas pengguna, penugasan grup, dan keanggotaan grup Anda akan terus berfungsi selama iDP baru mengirimkan pernyataan yang benar (misalnya, NAMEID SAM). Pernyataan ini harus cocok dengan nama pengguna dan grup di Pusat Identitas IAM.
- Tidak ada sinkronisasi keluar - Pusat Identitas IAM tidak mendukung sinkronisasi keluar, sehingga IDP eksternal Anda tidak akan diperbarui secara otomatis dengan perubahan pada pengguna dan grup yang Anda buat di Pusat Identitas IAM.
- Penyediaan SCIM - jika Anda menggunakan penyediaan SCIM, perubahan pada pengguna dan grup di penyedia identitas Anda hanya tercermin di Pusat Identitas IAM setelah penyedia identitas Anda mengirimkan perubahan tersebut ke Pusat Identitas IAM. Lihat Pertimbangan untuk menggunakan penyediaan otomatis.
- Rollback — Anda dapat mengembalikan sumber identitas Anda kembali menggunakan IAM Identity Center kapan saja. Lihat Mengubah dari iDP eksternal ke IAM Identity Center.

Untuk informasi tentang cara IAM Identity Center menyediakan pengguna dan grup, lihatConnect ke penyedia identitas eksternal.

Mengubah dari iDP eksternal ke IAM Identity Center

Jika Anda mengubah sumber identitas dari penyedia identitas eksternal (iDP) menjadi IAM Identity Center, pertimbangkan hal berikut:

- IAM Identity Center mempertahankan semua tugas Anda.
- Reset paksa kata sandi — Pengguna yang memiliki kata sandi di Pusat Identitas IAM dapat melanjutkan masuk dengan kata sandi lama mereka. Untuk pengguna yang berada di IDP eksternal dan tidak berada di Pusat Identitas IAM, administrator harus memaksa pengaturan ulang kata sandi.

Untuk informasi tentang cara IAM Identity Center menyediakan pengguna dan grup, lihatKelola identitas di Pusat Identitas IAM.

Mengubah dari satu iDP eksternal ke iDP eksternal lainnya

Jika Anda sudah menggunakan iDP eksternal sebagai sumber identitas untuk IAM Identity Center dan Anda mengubah ke iDP eksternal yang berbeda, pertimbangkan hal berikut:

- Tugas dan keanggotaan bekerja dengan pernyataan yang benar - IAM Identity Center mempertahankan semua tugas Anda. Penugasan pengguna, penugasan grup, dan keanggotaan grup akan terus berfungsi selama iDP baru mengirimkan pernyataan yang benar (misalnya, NAMEID SAM).

  Pernyataan ini harus cocok dengan nama pengguna di Pusat Identitas IAM saat pengguna Anda mengautentikasi melalui iDP eksternal yang baru.
- Penyediaan SCIM - Jika Anda menggunakan SCIM untuk penyediaan ke IAM Identity Center, kami sarankan Anda meninjau informasi khusus IDP dalam panduan ini dan dokumentasi yang disediakan oleh IDP untuk memastikan bahwa penyedia baru akan cocok dengan pengguna dan grup dengan benar saat SCIM diaktifkan.

Untuk informasi tentang cara IAM Identity Center menyediakan pengguna dan grup, lihatConnect ke penyedia identitas eksternal.

Mengubah antara Active Directory dan iDP eksternal

Jika Anda mengubah sumber identitas dari iDP eksternal ke Active Directory, atau dari Active Directory ke iDP eksternal, pertimbangkan hal berikut:

- Pengguna, grup, dan tugas dihapus - Semua pengguna, grup, dan tugas dihapus dari Pusat Identitas IAM. Tidak ada informasi pengguna atau grup yang terpengaruh baik di IDP eksternal atau Direktori Aktif.
- Menyediakan pengguna — Jika Anda mengubah ke iDP eksternal, Anda harus mengonfigurasi Pusat Identitas IAM untuk menyediakan pengguna Anda. Atau, Anda harus secara manual menyediakan pengguna dan grup untuk iDP eksternal sebelum Anda dapat mengonfigurasi tugas.
- Buat tugas dan grup — Jika Anda mengubah ke Active Directory, Anda harus membuat tugas dengan pengguna dan grup yang ada di direktori Anda di Active Directory.

Untuk informasi tentang cara IAM Identity Center menyediakan pengguna dan grup, lihatConnect ke Microsoft AD direktori.

Ubah sumber identitas Anda

Prosedur berikut menjelaskan cara mengubah dari direktori yang disediakan IAM Identity Center (direktori Pusat Identitas default) ke Active Directory atau penyedia identitas eksternal, atau sebaliknya. Sebelum Anda melanjutkan, tinjau informasi diPertimbangan untuk mengubah sumber identitas Anda. Bergantung pada penerapan Anda saat ini, perubahan ini dapat menghapus tugas pengguna dan grup apa pun yang Anda konfigurasikan di IAM Identity Center. Jika ini terjadi, semua pengguna, termasuk pengguna administratif di IAM Identity Center, akan kehilangan akses masuk tunggal ke merekaAkun AWSdan aplikasi.

Untuk mengubah sumber identitas Anda

1. BukaKonsol IAM Identity Center.
2. Pilih Pengaturan.
3. PadaPengaturanhalaman, pilihSumber identitastab. PilihTindakan, lalu pilihUbah sumber identitas.
4. Di bawahPilih sumber identitas, sumber yang ingin Anda ubah, dan kemudian memilihSelanjutnya.

   Jika Anda mengubah ke Active Directory, pilih direktori yang tersedia dari menu di halaman berikutnya.

   > **Important**
   >
   > Mengubah sumber identitas Anda ke atau dari Active Directory menghapus pengguna dan grup dari direktori Pusat Identitas. Perubahan ini juga menghapus tugas apa pun yang Anda konfigurasikan di IAM Identity Center.

   Jika Anda beralih ke penyedia identitas eksternal, kami sarankan agar Anda mengikuti langkah diCara terhubung ke penyedia identitas eksternal.
5. Setelah Anda membaca sangkalan dan siap untuk melanjutkan, ketikMENERIMA.
6. PilihUbah sumber identitas. Jika Anda mengubah sumber identitas Anda ke Active Directory, lanjutkan ke langkah berikutnya.
7. Mengubah sumber identitas Anda ke Active Directory membawa Anda kePengaturanhalaman. PadaPengaturanHalaman, lakukan salah satu dari berikut:

- PilihPengaturan terpandu. Untuk informasi selengkapnya tentang cara menyelesaikan proses pengaturan terpandu, lihatPengaturan terpandu.
- DiSumber identitasbagian, pilihTindakan, lalu pilihSinkronisasiuntuk mengkonfigurasi AndaLingkup sinkron, daftar pengguna dan grup untuk disinkronkan.

Mengelola login dan penggunaan atribut untuk semua jenis sumber identitas

IAM Identity Center menyediakan serangkaian fitur berikut yang memungkinkan admin mengontrol penggunaan portal AWS akses, mengatur durasi sesi bagi pengguna di portal AWS akses dan aplikasi Anda, dan menggunakan atribut untuk kontrol akses. Fitur-fitur ini bekerja dengan direktori Pusat Identitas atau penyedia identitas eksternal sebagai sumber identitas Anda.

> **Note**
>
> Jika Anda menggunakan Active Directory sebagai sumber identitas untuk IAM Identity Center, manajemen sesi tidak didukung.

Topik

- Mengelola durasi sesi portal AWS akses dan aplikasi terintegrasi IAM Identity Center
- Konfigurasikan durasi sesi portal AWS akses dan aplikasi terintegrasi IAM Identity Center
- Hapus sesi untuk portal AWS akses dan aplikasi AWS terintegrasi
- Atribut pengguna dan grup yang didukung

Mengelola durasi sesi portal AWS akses dan aplikasi terintegrasi IAM Identity Center

Administrator Pusat Identitas IAM dapat mengonfigurasi durasi sesi untuk kedua aplikasi yang terintegrasi dengan Pusat Identitas IAM dan. Portal akses AWSKonfigurasi durasi sesi menentukan seberapa sering pengguna diminta untuk mengautentikasi ulang. Administrator Pusat Identitas IAM dapat mengakhiri sesi portal AWS akses aktif dan dengan melakukan itu juga mengakhiri sesi aplikasi terintegrasi.

Untuk informasi selengkapnya, lihat Konfigurasikan durasi sesi portal AWS akses dan aplikasi terintegrasi IAM Identity Center. Untuk informasi selengkapnya tentang cara mengelola dan mengakhiri sesi pengguna, lihatHapus sesi untuk portal AWS akses dan aplikasi AWS terintegrasi.

> **Note**
>
> Memodifikasi durasi sesi portal AWS akses dan mengakhiri sesi portal AWS akses tidak berpengaruh pada durasi sesi Konsol AWS Manajemen yang Anda tentukan dalam set izin.

Konfigurasikan durasi sesi portal AWS akses dan aplikasi terintegrasi IAM Identity Center

Durasi sesi otentikasi ke dalam aplikasi terintegrasi Portal akses AWS dan IAM Identity Center adalah durasi maksimum waktu pengguna dapat masuk tanpa autentikasi ulang. Durasi sesi default adalah 8 jam. Administrator Pusat Identitas IAM dapat menentukan durasi yang berbeda, dari minimal 15 menit hingga maksimum 90 hari. Untuk informasi selengkapnya tentang durasi sesi otentikasi dan perilaku pengguna, lihatAutentikasi.

Topik berikut memberikan informasi tentang mengkonfigurasi durasi sesi portal AWS akses dan aplikasi terintegrasi IAM Identity Center.

Topik

- Prasyarat dan pertimbangan
- Cara mengkonfigurasi durasi sesi

Prasyarat dan pertimbangan

Berikut ini adalah prasyarat dan pertimbangan untuk mengonfigurasi durasi sesi untuk portal AWS akses dan aplikasi terintegrasi IAM Identity Center.

Penyedia identitas eksternal

IAM Identity Center menggunakan `SessionNotOnOrAfter` atribut dari pernyataan SAMP untuk membantu menentukan berapa lama sesi dapat valid.

- Jika `SessionNotOnOrAfter` tidak diteruskan dalam pernyataan SAMP, durasi sesi portal AWS akses tidak terpengaruh oleh durasi sesi IDP eksternal Anda. Misalnya, jika durasi sesi IDP adalah

24 jam dan Anda menetapkan durasi sesi 18 jam di Pusat Identitas IAM, pengguna Anda harus melakukan autentikasi ulang di portal akses setelah 18 jam. AWS

- Jika `SessionNotOnOrAfter` diteruskan dalam pernyataan SAMP, nilai durasi sesi diatur ke durasi sesi portal AWS akses yang lebih pendek dan durasi sesi IDP SAMP Anda. Jika Anda menetapkan durasi sesi 72 jam di IAM Identity Center dan idP Anda memiliki durasi sesi 18 jam, pengguna Anda akan memiliki akses ke AWS sumber daya selama 18 jam yang ditentukan dalam IDP Anda.
- Jika durasi sesi IDP Anda lebih lama dari yang ditetapkan di IAM Identity Center, pengguna Anda akan dapat memulai sesi Pusat Identitas IAM baru tanpa memasukkan kembali kredensialnya, berdasarkan sesi login mereka yang masih valid dengan IDP Anda.

> **Note**
>
> Jika Anda menggunakan Active Directory sebagai sumber identitas untuk IAM Identity Center, manajemen sesi tidak didukung.

AWS CLI dan sesi SDK

Jika Anda menggunakan AWS Command Line Interface, Perangkat Pengembangan AWS Perangkat Lunak (SDK), atau alat AWS pengembangan lainnya untuk mengakses AWS layanan secara terprogram, prasyarat berikut harus dipenuhi untuk menetapkan durasi sesi untuk portal AWS akses dan aplikasi terintegrasi Pusat Identitas IAM.

- Anda harus mengonfigurasi durasi sesi portal AWS akses di konsol Pusat Identitas IAM.
- Anda harus menentukan profil untuk pengaturan masuk tunggal di file AWS konfigurasi bersama Anda. Profil ini digunakan untuk terhubung ke portal AWS akses. Kami menyarankan Anda menggunakan konfigurasi penyedia token SSO. Dengan konfigurasi ini, AWS SDK atau alat Anda dapat secara otomatis mengambil token otentikasi yang diperbarui. Untuk informasi selengkapnya, lihat konfigurasi penyedia token SSO di AWS SDK dan Panduan Referensi Alat.
- Pengguna harus menjalankan versi AWS CLI atau SDK yang mendukung manajemen sesi.

Versi minimum dari AWS CLI yang mendukung manajemen sesi

Berikut ini adalah versi minimum dari AWS CLI yang mendukung manajemen sesi.

- AWS CLI V2 2.9 atau yang lebih baru

- AWS CLI V1 1.27.10 atau yang lebih baru

Untuk informasi tentang cara menginstal atau memperbarui AWS CLI versi terbaru, lihat Menginstal atau memperbarui versi terbaru AWS CLI.

Jika pengguna menjalankan AWS CLI, jika Anda menyegarkan izin yang disetel tepat sebelum sesi Pusat Identitas IAM diatur untuk kedaluwarsa dan durasi sesi disetel ke 20 jam sementara durasi yang ditetapkan izin disetel ke 12 jam, AWS CLI sesi berjalan maksimal 20 jam ditambah 12 jam dengan total 32 jam. Untuk informasi selengkapnya tentang CLI Pusat Identitas IAM, AWS CLI lihat Referensi Perintah.

Versi minimum SDK yang mendukung manajemen sesi IAM Identity Center

Berikut ini adalah versi minimum SDK yang mendukung manajemen sesi IAM Identity Center.

SDK	Versi minimum
Python	1.26.10
PHP	3.245.0
Ruby	aws-sdk-core 3.167.0
Java V2	AWS SDK for Java v2 (2.18.13)
Pergi V2	Seluruh SDK: rilis-2022-11-11 dan modul Go tertentu: kredensial/v1.13.0, config/v1.18.0
JS V2	2.1253.0
JS V3	v3.210.0
C++	1.9.372
.NET	v3.7.400.0

Cara mengkonfigurasi durasi sesi

Gunakan prosedur berikut untuk mengonfigurasi durasi sesi portal AWS akses dan aplikasi terintegrasi IAM Identity Center.

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Otentikasi.
4. Di bawah Otentikasi, di samping Pengaturan sesi, pilih Konfigurasi. Sebuah kotak dialog Konfigurasi pengaturan sesi muncul.
5. Dalam kotak dialog Konfigurasi pengaturan sesi, pilih durasi sesi maksimum dalam menit, jam, dan hari untuk pengguna Anda dengan memilih panah tarik-turun. Pilih panjang sesi, lalu pilih Simpan. Anda kembali ke halaman Pengaturan.

Hapus sesi untuk portal AWS akses dan aplikasi AWS terintegrasi

Gunakan prosedur berikut untuk melihat dan menghapus sesi aktif untuk pengguna Pusat Identitas IAM.

Untuk menghapus sesi aktif portal AWS akses dan aplikasi terintegrasi IAM Identity Center

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengguna.
3. Pada halaman Pengguna, pilih nama pengguna pengguna yang sesinya ingin Anda kelola. Ini membawa Anda ke halaman dengan informasi pengguna.
4. Pada halaman pengguna, pilih tab Sesi aktif. Angka dalam tanda kurung di samping sesi Aktif menunjukkan jumlah sesi aktif saat ini untuk pengguna ini.
5. Pilih kotak centang di samping sesi yang ingin Anda hapus, lalu pilih Hapus sesi. Kotak dialog muncul yang mengonfirmasi bahwa Anda menghapus sesi aktif untuk pengguna ini. Baca informasi di kotak dialog, dan jika Anda ingin melanjutkan, pilih Hapus sesi.
6. Anda dikembalikan ke halaman pengguna. Bilah lampu kilat hijau muncul untuk menunjukkan bahwa sesi yang dipilih berhasil dihapus.

Untuk informasi selengkapnya tentang perilaku sesi autentikasi yang dicabut, lihat. Sesi otentikasi

Atribut pengguna dan grup yang didukung

Atribut adalah potongan informasi yang membantu Anda menentukan dan mengidentifikasi pengguna individu atau objek grup, sepertiname,email, ataumembers. IAM Identity Center mendukung atribut yang paling umum digunakan terlepas dari apakah mereka dimasukkan secara manual selama pembuatan pengguna atau ketika secara otomatis disediakan menggunakan mesin sinkronisasi

seperti yang didefinisikan dalam spesifikasi Sistem untuk Manajemen Identitas Lintas Domain (SCIM). Untuk informasi lebih lanjut tentang spesifikasi ini, lihat https://tools.ietf.org/html/rfc7642. Untuk informasi selengkapnya tentang penyediaan manual dan otomatis, lihat. Penyediaan saat pengguna berasal dari iDP eksternal

Karena IAM Identity Center mendukung SCIM untuk kasus penggunaan penyediaan otomatis, direktori Identity Center mendukung semua atribut pengguna dan grup yang sama yang tercantum dalam spesifikasi SCIM, dengan beberapa pengecualian. Bagian berikut menjelaskan atribut mana yang tidak didukung oleh IAM Identity Center.

Objek pengguna

Semua atribut dari skema pengguna SCIM (https://tools.ietf.org/html/rfc7643#section-8.3) didukung di toko identitas Pusat Identitas IAM, kecuali untuk yang berikut ini:

- `password`
- `ims`
- `photos`
- `entitlements`
- `x509Certificates`

Semua sub-atribut untuk pengguna didukung, kecuali yang berikut ini:

- `'display'`sub-atribut dari setiap atribut multi-nilai (Misalnya, `emails` atau) `phoneNumbers`
- `'version'`sub-atribut atribut `'meta'`

Objek grup

Semua atribut dari skema grup SCIM (https://tools.ietf.org/html/rfc7643#section-8.4) didukung.

Semua sub-atribut untuk grup didukung, kecuali yang berikut ini:

- `'display'`sub-atribut dari setiap atribut multi-nilai (Misalnya, anggota).

Kelola identitas di Pusat Identitas IAM

IAM Identity Center menyediakan kemampuan berikut untuk pengguna dan grup Anda:

- Buat pengguna dan grup Anda.
- Tambahkan pengguna Anda sebagai anggota ke grup.
- Tetapkan grup dengan tingkat akses yang diinginkan ke Anda Akun AWS dan aplikasi.

Untuk mengelola pengguna dan grup di toko Pusat Identitas IAM, AWS mendukung operasi API yang tercantum dalam Tindakan Pusat Identitas.

Penyediaan saat pengguna berada di Pusat Identitas IAM

Saat Anda membuat pengguna dan grup secara langsung di Pusat Identitas IAM, penyediaan dilakukan secara otomatis. Identitas ini segera tersedia untuk digunakan dalam membuat tugas dan untuk digunakan oleh aplikasi. Untuk informasi selengkapnya, lihat Penyediaan pengguna dan grup.

Mengubah Sumber Identitas Anda

Jika Anda lebih suka mengelola pengguna AWS Managed Microsoft AD, Anda dapat berhenti menggunakan direktori Pusat Identitas kapan saja dan sebagai gantinya menghubungkan Pusat Identitas IAM ke direktori Anda di Microsoft AD dengan menggunakan AWS Directory Service. Untuk informasi lebih lanjut, lihat pertimbangan untukPerubahan antara IAM Identity Center dan Active Directory.

Jika Anda lebih suka mengelola pengguna di penyedia identitas eksternal (iDP), Anda dapat menghubungkan Pusat Identitas IAM ke IDP Anda dan mengaktifkan penyediaan otomatis. Untuk informasi lebih lanjut, lihat pertimbangan untukMengubah dari IAM Identity Center ke iDP eksternal.

Topik

- Tambahkan pengguna
- Tambahkan grup
- Tambahkan pengguna ke grup
- Hapus grup di Pusat Identitas IAM
- Hapus pengguna di Pusat Identitas IAM
- Nonaktifkan akses pengguna di Pusat Identitas IAM
- Edit properti pengguna
- Setel ulang kata sandi pengguna IAM Identity Center untuk pengguna akhir
- Kirim email OTP untuk pengguna yang dibuat dari API
- Persyaratan kata sandi saat mengelola identitas di IAM Identity Center

Tambahkan pengguna

Pengguna dan grup yang Anda buat di direktori Pusat Identitas hanya tersedia di Pusat Identitas IAM. Gunakan prosedur berikut untuk menambahkan pengguna ke direktori Pusat Identitas Anda menggunakan konsol IAM Identity Center. Atau, Anda dapat memanggil operasi AWS API CreateUseruntuk menambahkan pengguna.

Untuk menambahkan pengguna

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengguna.
3. Pilih Tambah pengguna dan berikan informasi yang diperlukan berikut:

    a. Nama pengguna — Nama pengguna ini diperlukan untuk masuk ke portal AWS akses dan tidak dapat diubah nanti. Itu harus antara 1 dan 100 karakter.

    b. Kata sandi - Anda dapat mengirim email dengan instruksi pengaturan kata sandi (ini adalah opsi default) atau membuat kata sandi satu kali. Jika Anda membuat pengguna administratif dan Anda memilih untuk mengirim email, pastikan Anda menentukan alamat email yang dapat Anda akses.

        i. Kirim email ke pengguna ini dengan instruksi pengaturan kata sandi. — Opsi ini secara otomatis mengirimkan email kepada pengguna yang dialamatkan dari Amazon Web Services, dengan baris subjek Undangan untuk bergabung AWS IAM Identity Center (penerus AWS Single Sign-On). Email mengundang pengguna atas nama perusahaan Anda untuk mengakses portal AWS akses Pusat Identitas IAM.

> **Note**
>
> Di Wilayah tertentu, IAM Identity Center mengirimkan email ke pengguna yang menggunakan Amazon Simple Email Service dari yang lain Wilayah AWS. Untuk informasi tentang cara email dikirim, lihatPanggilan Lintas Wilayah. Semua email yang dikirim oleh layanan IAM Identity Center akan berasal dari alamat `no-reply@signin.aws.com` atau`no-reply@login.awsapps.com`. Kami menyarankan Anda mengonfigurasi sistem email Anda sehingga menerima email dari alamat email pengirim ini dan tidak menanganinya sebagai sampah atau spam.

ii. Buat kata sandi satu kali yang dapat Anda bagikan dengan pengguna ini. — Opsi ini memberi Anda URL portal AWS akses dan detail kata sandi yang dapat Anda kirim secara manual ke pengguna dari alamat email Anda.

c. Alamat email — Alamat email harus unik.

d. Konfirmasikan alamat email

e. Nama depan — Anda harus memasukkan nama di sini agar penyediaan otomatis berfungsi. Untuk informasi selengkapnya, lihat Penyediaan otomatis.

f. Nama belakang — Anda harus memasukkan nama di sini agar penyediaan otomatis berfungsi.

g. Nama tampilan

> **Note**
>
> (Opsional) Jika berlaku, Anda dapat menentukan nilai untuk atribut tambahan seperti ID kekal Microsoft 365 pengguna untuk membantu memberikan pengguna akses masuk tunggal ke aplikasi bisnis tertentu.

4. Pilih Berikutnya.
5. Jika berlaku, pilih satu atau beberapa grup yang ingin Anda tambahkan pengguna, dan pilih Berikutnya.
6. Tinjau informasi yang Anda tentukan untuk Langkah 1: Tentukan detail pengguna dan Langkah 2: Tambahkan pengguna ke grup - opsional. Pilih Edit dengan salah satu langkah untuk membuat perubahan apa pun. Setelah Anda mengonfirmasi bahwa informasi yang benar ditentukan untuk kedua langkah, pilih Tambah pengguna.

Tambahkan grup

Gunakan prosedur berikut untuk menambahkan grup ke direktori Pusat Identitas Anda menggunakan konsol Pusat Identitas IAM. Atau, Anda dapat memanggil operasi AWS API CreateGroupuntuk menambahkan grup.

Untuk menambahkan grup

1. Buka konsol Pusat Identitas IAM.
2. Pilih Grup.
3. Pilih Buat grup.

4. Masukkan nama Grup dan Deskripsi - opsional. Deskripsi harus memberikan rincian tentang izin apa yang telah atau akan ditetapkan ke grup. Di bawah Tambahkan pengguna ke grup - opsional, temukan pengguna yang ingin Anda tambahkan sebagai anggota. Kemudian pilih kotak centang di sebelah masing-masing.
5. Pilih Buat grup.

Setelah menambahkan grup ini ke direktori Pusat Identitas, Anda dapat menetapkan akses masuk tunggal ke grup ini. Untuk informasi selengkapnya, lihat Tetapkan akses pengguna ke Akun AWS.

Tambahkan pengguna ke grup

Gunakan prosedur berikut untuk menambahkan pengguna sebagai anggota grup yang sebelumnya Anda buat di direktori Pusat Identitas menggunakan konsol Pusat Identitas IAM. Atau, Anda dapat memanggil operasi AWS API CreateGroupMembershipuntuk menambahkan pengguna sebagai anggota grup.

Untuk menambahkan pengguna sebagai anggota grup

1. Buka konsol Pusat Identitas IAM.
2. Pilih Grup.
3. Pilih nama grup yang ingin Anda perbarui.
4. Pada halaman detail grup, di bawah Pengguna dalam grup ini, pilih Tambahkan pengguna ke grup.
5. Pada halaman Tambahkan pengguna ke grup, di bawah Pengguna lain, temukan pengguna yang ingin Anda tambahkan sebagai anggota. Kemudian, pilih kotak centang di sebelah masing-masing.
6. Pilih Add Users (Tambahkan pengguna).

Hapus grup di Pusat Identitas IAM

Ketika Anda menghapus grup di direktori Pusat Identitas IAM Anda, itu menghapus akses ke Akun AWS dan aplikasi untuk semua pengguna yang menjadi anggota grup ini. Setelah grup dihapus, grup tidak dapat dibatalkan. Gunakan prosedur berikut untuk menghapus grup di direktori Pusat Identitas Anda menggunakan konsol Pusat Identitas IAM.

Untuk menghapus grup di Pusat Identitas IAM

> **Important**
>
> Instruksi pada halaman ini berlaku untuk AWS IAM Identity Center. Mereka tidak berlaku untuk AWS Identity and Access Management(IAM). Pengguna, grup, dan kredenal pengguna IAM Identity Center berbeda dari pengguna IAM, grup, dan kredenal pengguna IAM. Jika Anda mencari petunjuk tentang menghapus grup di IAM, lihat Menghapus grup pengguna IAM di Panduan Pengguna.AWS Identity and Access Management

1. Buka konsol Pusat Identitas IAM.
2. Pilih Grup.
3. Ada dua cara Anda dapat menghapus grup:
   - Pada halaman Grup, Anda dapat memilih beberapa grup untuk dihapus. Pilih nama grup yang ingin Anda hapus dan pilih Hapus grup.
   - Pilih nama grup yang ingin Anda hapus. Pada halaman detail grup, pilih Hapus grup.
4. Anda mungkin diminta untuk mengonfirmasi maksud Anda untuk menghapus grup.
   - Jika Anda menghapus beberapa grup sekaligus, konfirmasikan maksud Anda dengan mengetikkan **`Delete`** kotak dialog Hapus grup.
   - Jika Anda menghapus satu grup yang berisi pengguna, konfirmasikan maksud Anda dengan mengetikkan nama grup yang ingin Anda hapus di kotak dialog Hapus grup.
5. Pilih Hapus grup. Jika Anda memilih beberapa grup untuk dihapus, pilih Hapus # grup.

Hapus pengguna di Pusat Identitas IAM

Ketika Anda menghapus pengguna di direktori Pusat Identitas IAM Anda, itu menghapus akses Akun AWS dan aplikasi mereka. Setelah pengguna dihapus, itu tidak dapat dibatalkan. Gunakan prosedur berikut untuk menghapus pengguna di direktori Pusat Identitas Anda menggunakan konsol Pusat Identitas IAM.

> **Note**
>
> Saat Anda menonaktifkan akses pengguna atau menghapus pengguna di Pusat Identitas IAM, pengguna tersebut akan segera dicegah masuk ke portal AWS akses dan tidak akan dapat membuat sesi masuk baru. Untuk informasi selengkapnya, lihat Sesi otentikasi.

Untuk menghapus pengguna di Pusat Identitas IAM

> **Important**
>
> Instruksi pada halaman ini berlaku untuk AWS IAM Identity Center. Mereka tidak berlaku untuk AWS Identity and Access Management(IAM). Pengguna, grup, dan kredenal pengguna IAM Identity Center berbeda dari pengguna IAM, grup, dan kredenal pengguna IAM. Jika Anda mencari petunjuk tentang menghapus pengguna di IAM, lihat Menghapus pengguna IAM di Panduan Pengguna.AWS Identity and Access Management

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengguna.
3. Ada dua cara Anda dapat menghapus pengguna:
   - Pada halaman Pengguna, Anda dapat memilih beberapa pengguna untuk dihapus. Pilih nama pengguna yang ingin Anda hapus dan pilih Hapus pengguna.
   - Pilih nama pengguna yang ingin Anda hapus. Pada halaman detail pengguna, pilih Hapus pengguna.
4. Jika Anda menghapus beberapa pengguna sekaligus, konfirmasikan maksud Anda dengan mengetikkan **`Delete`** kotak dialog Hapus pengguna.
5. Pilih Hapus pengguna. Jika Anda memilih beberapa pengguna untuk dihapus, pilih Hapus # pengguna.

Nonaktifkan akses pengguna di Pusat Identitas IAM

Ketika Anda menonaktifkan akses pengguna di direktori Pusat Identitas IAM Anda, Anda tidak dapat mengedit detail pengguna mereka, mengatur ulang kata sandi mereka, menambahkan pengguna ke

grup, atau melihat keanggotaan grup mereka. Gunakan prosedur berikut untuk menonaktifkan akses pengguna di direktori Pusat Identitas Anda menggunakan konsol Pusat Identitas IAM.

> **Note**
>
> Saat Anda menonaktifkan akses pengguna atau menghapus pengguna di Pusat Identitas IAM, pengguna tersebut akan segera dicegah masuk ke portal AWS akses dan tidak akan dapat membuat sesi masuk baru. Untuk informasi selengkapnya, lihat Sesi otentikasi.

Untuk menonaktifkan akses pengguna di Pusat Identitas IAM

1. Buka konsol Pusat Identitas IAM.

   > **Important**
   >
   > Instruksi pada halaman ini berlaku untuk AWS IAM Identity Center. Mereka tidak berlaku untuk AWS Identity and Access Management(IAM). Pengguna, grup, dan kredenal pengguna IAM Identity Center berbeda dari pengguna IAM, grup, dan kredenal pengguna IAM. Jika Anda mencari petunjuk tentang menonaktifkan pengguna di IAM, lihat Mengelola pengguna IAM di Panduan Pengguna.AWS Identity and Access Management

2. Pilih Pengguna.
3. Pilih nama pengguna pengguna yang aksesnya ingin Anda nonaktifkan.
4. Di bagian Informasi umum, pilih Nonaktifkan akses pengguna.
5. Dalam kotak dialog Nonaktifkan akses pengguna, pilih Nonaktifkan akses pengguna.

Edit properti pengguna

Gunakan prosedur berikut untuk mengedit properti pengguna di direktori Pusat Identitas Anda menggunakan konsol IAM Identity Center. Atau, Anda dapat memanggil operasi AWS API UpdateUseruntuk memperbarui properti pengguna.

Untuk mengedit properti pengguna di Pusat Identitas IAM

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengguna.

3. Pilih pengguna yang ingin Anda edit.
4. Pada halaman Profil pengguna, di samping Detail profil, pilih Edit.
5. Pada halaman Edit detail profil, perbarui properti sesuai kebutuhan. Kemudian, pilih Simpan perubahan.

> **Note**
>
> (Opsional) Anda dapat mengubah atribut tambahan seperti Nomor Karyawan dan ID Immutable Office 365 untuk membantu memetakan identitas pengguna di Pusat Identitas IAM dengan aplikasi bisnis tertentu yang perlu digunakan pengguna.

> **Note**
>
> Atribut Alamat email adalah bidang yang dapat diedit dan nilai yang Anda berikan harus unik.

Setel ulang kata sandi pengguna IAM Identity Center untuk pengguna akhir

Prosedur ini untuk administrator yang perlu mengatur ulang kata sandi untuk pengguna di direktori Pusat Identitas IAM Anda. Anda akan menggunakan konsol IAM Identity Center untuk mengatur ulang kata sandi.

Pertimbangan untuk penyedia identitas dan tipe pengguna

- MicrosoftActive Directory atau penyedia eksternal — Jika Anda menghubungkan IAM Identity Center ke Microsoft Active Directory atau penyedia eksternal, pengaturan ulang kata sandi pengguna harus dilakukan dari dalam Active Directory atau penyedia eksternal. Ini berarti bahwa kata sandi untuk pengguna tersebut tidak dapat diatur ulang dari konsol Pusat Identitas IAM.
- Pengguna di direktori Pusat Identitas IAM — Jika Anda pengguna Pusat Identitas IAM, Anda dapat mengatur ulang kata sandi Pusat Identitas IAM Anda sendiri, lihat. Menyetel ulang kata sandi pengguna IAM Identity Center

Untuk mengatur ulang kata sandi untuk pengguna akhir IAM Identity Center

> **Important**
>
> Instruksi pada halaman ini berlaku untuk AWS IAM Identity Center. Mereka tidak berlaku untuk AWS Identity and Access Management(IAM). Pengguna, grup, dan kredenal pengguna IAM Identity Center berbeda dari pengguna IAM, grup, dan kredenal pengguna IAM. Jika Anda mencari petunjuk tentang mengubah kata sandi untuk pengguna IAM, lihat Mengelola kata sandi untuk pengguna IAM di AWS Identity and Access Management Panduan Pengguna.

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengguna.
3. Pilih nama pengguna pengguna yang kata sandinya ingin Anda atur ulang.
4. Pada halaman detail pengguna, pilih Setel ulang kata sandi.
5. Dalam kotak dialog Reset password, pilih salah satu pilihan berikut, lalu pilih Reset password:

   a. Kirim email ke pengguna dengan instruksi untuk mengatur ulang kata sandi — Opsi ini secara otomatis mengirimkan email kepada pengguna yang dialamatkan dari Amazon Web Services yang memandu mereka melalui cara mengatur ulang kata sandi mereka.

   > **Warning**
   >
   > Sebagai praktik keamanan terbaik, verifikasi bahwa alamat email untuk pengguna ini benar sebelum memilih opsi ini. Jika email pengaturan ulang kata sandi ini dikirim ke alamat email yang salah atau salah konfigurasi, penerima jahat dapat menggunakannya untuk mendapatkan akses tidak sah ke lingkungan Anda AWS .

   b. Buat kata sandi satu kali dan bagikan kata sandi dengan pengguna — Opsi ini memberi Anda detail kata sandi yang dapat Anda kirim secara manual ke pengguna dari alamat email Anda.

Kirim email OTP untuk pengguna yang dibuat dari API

Saat Anda membuat pengguna dengan operasi CreateUserAPI, mereka tidak memiliki kata sandi. Anda dapat mengubahnya dengan memilih untuk mengirim kata sandi satu kali (OTP) email

kepada pengguna saat mereka dibuat dengan API. Pengguna menerima email OTP ketika mereka pertama kali mencoba masuk. Setelah menerima email OTP, ketika pengguna masuk, mereka harus menetapkan kata sandi baru. Jika Anda tidak mengaktifkan pengaturan ini, maka Anda harus membuat dan berbagi OTP dengan pengguna yang Anda buat menggunakan CreateUserAPI.

Untuk mengirim email OTP ke pengguna yang dibuat dengan API CreateUser

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Otentikasi.
4. Di bagian Otentikasi standar, pilih Konfigurasi.
5. Sebuah kotak dialog muncul. Centang kotak di sebelah Kirim email OTP. Lalu, pilih Simpan. Status diperbarui dari Dinonaktifkan ke Diaktifkan.

Persyaratan kata sandi saat mengelola identitas di IAM Identity Center

> **Note**
>
> Persyaratan ini hanya berlaku untuk pengguna yang dibuat di direktori Pusat Identitas. Jika Anda telah mengonfigurasi sumber identitas selain Pusat Identitas IAM untuk otentikasi, seperti Active Directoryatau penyedia identitas eksternal, kebijakan kata sandi untuk pengguna Anda ditentukan dan diberlakukan dalam sistem tersebut, bukan di Pusat Identitas IAM. Jika sumber identitas Anda AWS Managed Microsoft AD, lihat Mengelola kebijakan kata sandi AWS Managed Microsoft AD untuk informasi selengkapnya.

Saat Anda menggunakan IAM Identity Center sebagai sumber identitas Anda, pengguna harus mematuhi persyaratan kata sandi berikut untuk mengatur atau mengubah kata sandi mereka:

- Kata sandi peka huruf besar/kecil.
- Kata sandi harus memiliki panjang antara 8 dan 64 karakter.
- Kata sandi harus mengandung setidaknya satu karakter dari masing-masing dari empat kategori berikut:
  - Huruf kecil (a-z)
  - Huruf besar (A-Z)
  - Angka (0-9)

  - Karakter non-alfanumerik (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
- Tiga kata sandi terakhir tidak dapat digunakan kembali.
- Kata sandi yang diketahui publik melalui kumpulan data yang bocor dari pihak ketiga tidak dapat digunakan.

Connect ke Microsoft AD direktori

Dengan AWS IAM Identity Center, Anda dapat menghubungkan direktori yang dikelola sendiri di Active Directory (AD) atau direktori AWS Managed Microsoft AD dengan menggunakan AWS Directory Service. Direktori Microsoft AD ini mendefinisikan kumpulan identitas yang dapat diambil administrator saat menggunakan konsol Pusat Identitas IAM untuk menetapkan akses masuk tunggal. Setelah menghubungkan direktori perusahaan Anda ke IAM Identity Center, Anda kemudian dapat memberikan pengguna AD atau grup akses ke Akun AWS, aplikasi, atau keduanya.

AWS Directory Service membantu Anda mengatur dan menjalankan AWS Managed Microsoft AD direktori mandiri yang dihosting di AWS Cloud. Anda juga dapat menggunakan AWS Directory Service untuk menghubungkan AWS sumber daya Anda dengan iklan yang dikelola sendiri yang ada. Untuk mengonfigurasi AWS Directory Service agar berfungsi dengan AD yang dikelola sendiri, Anda harus terlebih dahulu menyiapkan hubungan kepercayaan untuk memperluas autentikasi ke cloud.

IAM Identity Center menggunakan koneksi yang disediakan oleh AWS Directory Service untuk melakukan otentikasi pass-through ke instance AD sumber. Saat Anda menggunakan AWS Managed Microsoft AD sebagai sumber identitas, IAM Identity Center dapat bekerja dengan pengguna dari AWS Managed Microsoft AD atau dari domain apa pun yang terhubung melalui kepercayaan AD. Jika Anda ingin menemukan pengguna Anda di empat domain atau lebih, pengguna harus menggunakan `DOMAIN\user` sintaks sebagai nama pengguna mereka saat melakukan login ke IAM Identity Center.

> **Catatan**
>
> - Sebagai langkah prasyarat, pastikan AD Connector atau direktori in AWS Directory Service berada di AWS Managed Microsoft AD dalam akun manajemen Anda. AWS Organizations Untuk informasi selengkapnya, lihat Konfirmasikan sumber identitas Anda di Pusat Identitas IAM.
> - IAM Identity Center tidak mendukung Simple AD berbasis SAMBA 4 sebagai direktori yang terhubung.

Pertimbangan untuk menggunakan Active Directory

Jika Anda ingin menggunakan Active Directory sebagai sumber identitas Anda, konfigurasi Anda harus memenuhi prasyarat berikut:

- Jika Anda menggunakan AWS Managed Microsoft AD, Anda harus mengaktifkan IAM Identity Center di tempat yang sama Wilayah AWS di mana AWS Managed Microsoft AD direktori Anda diatur. IAM Identity Center menyimpan data penugasan di Wilayah yang sama dengan direktori. Untuk mengelola Pusat Identitas IAM, Anda mungkin perlu beralih ke Wilayah tempat Pusat Identitas IAM dikonfigurasi. Juga, perhatikan bahwa portal AWS akses menggunakan URL akses yang sama dengan direktori Anda.
- Gunakan Active Directory yang berada di akun manajemen:

  Anda harus memiliki AD Connector atau AWS Managed Microsoft AD direktori yang sudah ada AWS Directory Service, dan direktori tersebut harus berada di dalam akun AWS Organizations manajemen Anda. Anda hanya dapat menghubungkan satu direktori AD Connector atau satu direktori sekaligus. AWS Managed Microsoft AD Jika Anda perlu mendukung beberapa domain atau hutan, gunakan AWS Managed Microsoft AD. Lihat informasi yang lebih lengkap di:

  - Connect direktori AWS Managed Microsoft AD ke IAM Identity Center
  - Connect direktori yang dikelola sendiri di Active Directory ke IAM Identity Center
- Gunakan Active Directory yang berada di akun admin yang didelegasikan:

  Jika Anda berencana untuk mengaktifkan admin yang didelegasikan IAM Identity Center dan menggunakan Active Directory sebagai sumber identitas Pusat Identitas IAM, Anda dapat menggunakan AD Connector atau AWS Managed Microsoft AD direktori yang sudah ada di Direktori yang berada di AWS akun admin yang didelegasikan.

  Jika Anda memutuskan untuk mengubah sumber identitas IAM Identity Center dari sumber lain ke Active Directory, atau mengubahnya dari Active Directory ke sumber lain, direktori harus berada di (dimiliki oleh) akun anggota administrator yang didelegasikan IAM Identity Center jika ada; jika tidak, itu harus berada di akun manajemen.

Connect Active Directory dan tentukan pengguna

Jika Anda sudah menggunakan Active Directory, topik berikut akan membantu Anda mempersiapkan diri untuk menghubungkan direktori Anda ke IAM Identity Center.

Anda dapat menghubungkan AWS Managed Microsoft AD direktori atau direktori yang dikelola sendiri di Active Directory dengan IAM Identity Center. Jika Anda berencana untuk menghubungkan AWS Managed Microsoft AD direktori atau direktori yang dikelola sendiri di Active Directory, pastikan konfigurasi Active Directory Anda memenuhi prasyarat di. Konfirmasikan sumber identitas Anda di Pusat Identitas IAM

> **Note**
>
> Sebagai praktik keamanan terbaik, kami sangat menyarankan Anda mengaktifkan otentikasi multi-faktor. Jika Anda berencana untuk menghubungkan AWS Managed Microsoft AD direktori atau direktori yang dikelola sendiri di Active Directory dan Anda tidak menggunakan RADIUS MFA, aktifkan MFA di AWS Directory ServiceIAM Identity Center.

AWS Managed Microsoft AD

1. Tinjau panduan diConnect ke Microsoft AD direktori.
2. Ikuti langkah-langkahnya di Connect direktori AWS Managed Microsoft AD ke IAM Identity Center.
3. Konfigurasikan Active Directory untuk menyinkronkan pengguna yang ingin Anda berikan izin administratif ke IAM Identity Center. Untuk informasi selengkapnya, lihat Sinkronisasi pengguna administratif ke IAM Identity Center.

Direktori yang dikelola sendiri di Direktori Aktif

1. Tinjau panduan diConnect ke Microsoft AD direktori.
2. Ikuti langkah-langkahnya di Connect direktori yang dikelola sendiri di Active Directory ke IAM Identity Center.
3. Konfigurasikan Active Directory untuk menyinkronkan pengguna yang ingin Anda berikan izin administratif ke IAM Identity Center. Untuk informasi selengkapnya, lihat Sinkronisasi pengguna administratif ke IAM Identity Center.

IDP Eksternal

1. Tinjau panduan diConnect ke penyedia identitas eksternal.
2. Ikuti langkah-langkahnya di Cara terhubung ke penyedia identitas eksternal.
3. Konfigurasikan IDP Anda untuk menyediakan pengguna ke Pusat Identitas IAM.

> **Note**
>
> Sebelum Anda mengatur penyediaan otomatis berbasis grup untuk semua identitas tenaga kerja Anda dari IDP Anda ke IAM Identity Center, kami sarankan Anda menyinkronkan satu pengguna yang ingin Anda berikan izin administratif ke IAM Identity Center.

Sinkronisasi pengguna administratif ke IAM Identity Center

Setelah Anda menghubungkan direktori Anda ke IAM Identity Center, Anda dapat menentukan pengguna yang ingin Anda berikan izin administratif, dan kemudian menyinkronkan pengguna tersebut dari direktori Anda ke Pusat Identitas IAM.

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Sumber identitas, pilih Tindakan, lalu pilih Kelola Sinkronisasi.
4. Pada halaman Kelola Sinkronisasi, pilih tab Pengguna, lalu pilih Tambahkan pengguna dan grup.
5. Pada tab Pengguna, di bawah Pengguna, masukkan nama pengguna yang tepat dan pilih Tambah.
6. Di bawah Pengguna dan Grup yang Ditambahkan, lakukan hal berikut:
    a. Konfirmasikan bahwa pengguna yang ingin Anda berikan izin administratif ditentukan.
    b. Pilih kotak centang di sebelah kiri nama pengguna.
    c. Pilih Kirim.
7. Di halaman Kelola sinkronisasi, pengguna yang Anda tentukan muncul di daftar cakupan pengguna dalam sinkronisasi.
8. Di panel navigasi, pilih Pengguna.
9. Pada halaman Pengguna, mungkin diperlukan beberapa waktu bagi pengguna yang Anda tentukan untuk muncul dalam daftar. Pilih ikon penyegaran untuk memperbarui daftar pengguna.

Pada titik ini, pengguna Anda tidak memiliki akses ke akun manajemen. Anda akan mengatur akses administratif ke akun ini dengan membuat set izin administratif dan menetapkan pengguna ke set izin tersebut. Untuk informasi selengkapnya, lihat Buat set izin.

Penyediaan saat pengguna berasal dari Active Directory

IAM Identity Center menggunakan koneksi yang disediakan oleh AWS Directory Service untuk menyinkronkan informasi pengguna, grup, dan keanggotaan dari direktori sumber Anda di Active Directory ke toko identitas IAM Identity Center. Tidak ada informasi kata sandi yang disinkronkan ke IAM Identity Center, karena otentikasi pengguna berlangsung langsung dari direktori sumber di Active Directory. Data identitas ini digunakan oleh aplikasi untuk memfasilitasi pencarian dalam aplikasi, otorisasi, dan skenario kolaborasi tanpa meneruskan aktivitas LDAP kembali ke direktori sumber di Active Directory.

Untuk informasi lebih lanjut di atas penyediaan, lihat. Penyediaan pengguna dan grup

Topik

- Connect direktori AWS Managed Microsoft AD ke IAM Identity Center
- Connect direktori yang dikelola sendiri di Active Directory ke IAM Identity Center
- Pemetaan atribut untuk direktori AWS Managed Microsoft AD
- Menyediakan pengguna dan grup dari Active Directory

Connect direktori AWS Managed Microsoft AD ke IAM Identity Center

Gunakan prosedur berikut untuk menghubungkan direktori yang dikelola oleh AWS Directory Service IAM Identity Center. AWS Managed Microsoft AD

Untuk terhubung AWS Managed Microsoft AD ke Pusat Identitas IAM

1. Buka konsol Pusat Identitas IAM.

   > **Note**
   >
   > Pastikan konsol IAM Identity Center menggunakan salah satu Wilayah tempat AWS Managed Microsoft AD direktori Anda berada sebelum Anda pindah ke langkah berikutnya.

2. Pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Sumber identitas, lalu pilih Tindakan > Ubah sumber identitas.
4. Di bawah Pilih sumber identitas, pilih Active Directory, lalu pilih Berikutnya.

5. Di bawah Connect active directory, pilih direktori AWS Managed Microsoft AD dari daftar, lalu pilih Berikutnya.
6. Di bawah Konfirmasi perubahan, tinjau informasi dan saat siap ketik TERIMA, lalu pilih Ubah sumber identitas.

> **Important**
>
> Untuk menentukan pengguna di Active Directory sebagai pengguna administratif di IAM Identity Center, Anda harus terlebih dahulu menyinkronkan pengguna yang ingin Anda berikan izin administratif dari Active Directory ke IAM Identity Center. Untuk melakukannya, ikuti langkah yang ada di Sinkronisasi pengguna administratif ke IAM Identity Center.

Connect direktori yang dikelola sendiri di Active Directory ke IAM Identity Center

Pengguna di direktori yang dikelola sendiri di Active Directory (AD) juga dapat memiliki akses masuk tunggal Akun AWS dan aplikasi di portal akses. AWS Untuk mengonfigurasi akses masuk tunggal bagi pengguna ini, Anda dapat melakukan salah satu hal berikut:

- Buat hubungan kepercayaan dua arah — Ketika hubungan kepercayaan dua arah dibuat antara AWS Managed Microsoft AD dan direktori yang dikelola sendiri di AD, pengguna di direktori yang dikelola sendiri di AD dapat masuk dengan kredenal perusahaan mereka ke berbagai layanan dan aplikasi bisnis. AWS Perwalian satu arah tidak bekerja dengan IAM Identity Center.

  AWS IAM Identity Center memerlukan kepercayaan dua arah sehingga memiliki izin untuk membaca informasi pengguna dan grup dari domain Anda untuk menyinkronkan metadata pengguna dan grup. IAM Identity Center menggunakan metadata ini saat menetapkan akses ke set izin atau aplikasi. Metadata pengguna dan grup juga digunakan oleh aplikasi untuk kolaborasi, seperti ketika Anda berbagi dasbor dengan pengguna atau grup lain. Kepercayaan dari AWS Directory Service Microsoft Active Directory ke domain Anda memungkinkan IAM Identity Center untuk mempercayai domain Anda untuk otentikasi. Kepercayaan pada arah yang berlawanan memberikan AWS izin untuk membaca metadata pengguna dan grup.

  Untuk informasi selengkapnya tentang menyiapkan kepercayaan dua arah, lihat Kapan Membuat Hubungan Kepercayaan dalam PanduanAWS Directory Service Administrasi.

- Buat Konektor AD — AD Connector adalah gateway direktori yang dapat mengarahkan permintaan direktori ke AD yang dikelola sendiri tanpa menyimpan informasi apa pun di cloud. Untuk informasi selengkapnya, lihat Connect to a Directory di PanduanAWS Directory Service Administrasi.

> **Note**
>
> Jika Anda menghubungkan IAM Identity Center ke direktori AD Connector, pengaturan ulang kata sandi pengguna di masa mendatang harus dilakukan dari dalam AD. Ini berarti bahwa pengguna tidak akan dapat mengatur ulang kata sandi mereka dari portal AWS akses.
> Jika Anda menggunakan AD Connector untuk menghubungkan Layanan Domain Direktori Aktif ke Pusat Identitas IAM, Pusat Identitas IAM hanya memiliki akses ke pengguna dan grup domain tunggal yang dilampirkan oleh AD Connector. Jika Anda perlu mendukung beberapa domain atau hutan, gunakan AWS Directory Service untuk Microsoft Active Directory.

> **Note**
>
> IAM Identity Center tidak bekerja dengan direktori Simple AD berbasis Samba4.

Pemetaan atribut untuk direktori AWS Managed Microsoft AD

Pemetaan atribut digunakan untuk memetakan tipe atribut yang ada di Pusat Identitas IAM dengan atribut serupa dalam direktori. AWS Managed Microsoft AD IAM Identity Center mengambil atribut pengguna dari direktori Microsoft AD Anda dan memetakannya ke atribut pengguna IAM Identity Center. Pemetaan atribut pengguna IAM Identity Center ini juga digunakan untuk menghasilkan pernyataan SAFL 2.0 untuk aplikasi Anda. Setiap aplikasi menentukan daftar atribut SAMP 2.0 yang dibutuhkan untuk proses masuk tunggal yang berhasil.

IAM Identity Center mengisi ulang sekumpulan atribut untuk Anda di bawah tab pemetaan Atribut yang ditemukan di halaman konfigurasi aplikasi Anda. IAM Identity Center menggunakan atribut pengguna ini untuk mengisi pernyataan SAMB (sebagai atribut SALL) yang dikirim ke aplikasi. Atribut pengguna ini pada gilirannya diambil dari direktori Microsoft AD Anda. Untuk informasi selengkapnya, lihat Petakan atribut dalam aplikasi Anda ke atribut IAM Identity Center.

IAM Identity Center juga mengelola serangkaian atribut untuk Anda di bawah bagian pemetaan Atribut dari halaman konfigurasi direktori Anda. Untuk informasi selengkapnya, lihat Petakan atribut di Pusat Identitas IAM ke atribut di direktori Anda AWS Managed Microsoft AD.

Atribut direktori yang didukung

Tabel berikut mencantumkan semua atribut AWS Managed Microsoft AD direktori yang didukung dan yang dapat dipetakan ke atribut pengguna di IAM Identity Center.

Atribut yang didukung di direktori Microsoft AD
`${dir:email}`
`${dir:displayname}`
`${dir:distinguishedName}`
`${dir:firstname}`
`${dir:guid}`
`${dir:initials}`
`${dir:lastname}`
`${dir:proxyAddresses}`
`${dir:proxyAddresses:smtp}`
`${dir:proxyAddresses:SMTP}`
`${dir:windowsUpn}`

Anda dapat menentukan kombinasi atribut direktori Microsoft AD yang didukung untuk dipetakan ke atribut tunggal yang dapat berubah di Pusat Identitas IAM. Misalnya, Anda dapat memilih `subject` atribut di bawah atribut Pengguna di kolom Pusat Identitas IAM. Kemudian petakan ke salah satu `${dir:displayname}` atau `${dir:lastname}${dir:firstname }` atau atribut tunggal yang didukung atau kombinasi arbitrer dari atribut yang didukung. Untuk daftar pemetaan default untuk atribut pengguna di Pusat Identitas IAM, lihat. Pemetaan default

> **Warning**
>
> Atribut Pusat Identitas IAM tertentu tidak dapat dimodifikasi karena tidak dapat diubah dan dipetakan secara default ke atribut direktori Microsoft AD tertentu.
> Misalnya, “nama pengguna” adalah atribut wajib di IAM Identity Center. Jika Anda memetakan “nama pengguna” ke atribut direktori AD dengan nilai kosong, Pusat Identitas IAM akan mempertimbangkan `windowsUpn` nilai sebagai nilai default untuk “nama pengguna”. Jika Anda ingin mengubah pemetaan atribut untuk “nama pengguna” dari pemetaan Anda saat ini, konfirmasikan alur Pusat Identitas IAM dengan ketergantungan pada “nama pengguna” akan terus berfungsi seperti yang diharapkan, sebelum melakukan perubahan.

Jika Anda menggunakan tindakan ListUsersatau ListGroupsAPI atau perintah list-usersdan list-groups AWS CLI untuk menetapkan pengguna dan grup akses ke Akun AWS dan ke aplikasi, Anda harus menentukan nilai untuk `AttributeValue` sebagai FQDN. Nilai ini harus dalam format berikut: user@example.com. Dalam contoh berikut, `AttributeValue` diatur `kejanedoe@example.com`.

```
aws identitystore list-users --identity-store-id d-12345a678b --filters
 AttributePath=UserName,AttributeValue=janedoe@example.com
```

Atribut Pusat Identitas IAM yang didukung

Tabel berikut mencantumkan semua atribut IAM Identity Center yang didukung dan yang dapat dipetakan ke atribut pengguna di direktori Anda AWS Managed Microsoft AD . Setelah Anda mengatur pemetaan atribut aplikasi Anda, Anda dapat menggunakan atribut Pusat Identitas IAM yang sama ini untuk memetakan ke atribut aktual yang digunakan oleh aplikasi tersebut.

Atribut yang didukung di Pusat Identitas IAM
`${user:AD_GUID}`
`${user:email}`
`${user:familyName}`
`${user:givenName}`

Atribut yang didukung di Pusat Identitas IAM
`${user:middleName}`
`${user:name}`
`${user:preferredUsername}`
`${user:subject}`

Atribut penyedia identitas eksternal yang didukung

Tabel berikut mencantumkan semua atribut penyedia identitas eksternal (iDP) yang didukung dan yang dapat dipetakan ke atribut yang dapat Anda gunakan saat mengonfigurasi Atribut untuk kontrol akses di Pusat Identitas IAM. Saat menggunakan pernyataan SAMP, Anda dapat menggunakan atribut apa pun yang didukung idP Anda.

Atribut yang didukung di IDP
`${path:userName}`
`${path:name.familyName}`
`${path:name.givenName}`
`${path:displayName}`
`${path:nickName}`
`${path:emails[primary eq true].value}`
`${path:addresses[type eq "work"].streetAddress}`
`${path:addresses[type eq "work"].locality}`
`${path:addresses[type eq "work"].region}`
`${path:addresses[type eq "work"].postalCode}`
`${path:addresses[type eq "work"].country}`

Atribut yang didukung di IDP
`${path:addresses[type eq "work"].formatted}`
`${path:phoneNumbers[type eq "work"].value}`
`${path:userType}`
`${path:title}`
`${path:locale}`
`${path:timezone}`
`${path:enterprise.employeeNumber}`
`${path:enterprise.costCenter}`
`${path:enterprise.organization}`
`${path:enterprise.division}`
`${path:enterprise.department}`
`${path:enterprise.manager.value}`

Pemetaan default

Tabel berikut mencantumkan pemetaan default untuk atribut pengguna di Pusat Identitas IAM ke atribut pengguna di direktori Anda. AWS Managed Microsoft AD IAM Identity Center hanya mendukung daftar atribut dalam atribut User di kolom IAM Identity Center.

> **Note**
>
> Jika Anda tidak memiliki tugas untuk pengguna dan grup di Pusat Identitas IAM saat Anda mengaktifkan sinkronisasi AD yang dapat dikonfigurasi, pemetaan default dalam tabel berikut akan digunakan. Untuk informasi tentang cara menyesuaikan pemetaan ini, lihat. Konfigurasikan pemetaan atribut untuk sinkronisasi Anda

Atribut pengguna di Pusat Identitas IAM	Memetakan ke atribut ini di direktori Microsoft AD
AD_GUID	${dir:guid}
email *	${dir:windowsUpn}
familyName	${dir:lastname}
givenName	${dir:firstname}
middleName	${dir:initials}
name	${dir:displayname}
preferredUsername	${dir:displayname}
subject	${dir:windowsUpn}

* Atribut email di IAM Identity Center harus unik dalam direktori. Jika tidak, proses login JIT bisa gagal.

Anda dapat mengubah pemetaan default atau menambahkan lebih banyak atribut ke pernyataan SAMP 2.0 berdasarkan kebutuhan Anda. Misalnya, asumsikan bahwa aplikasi Anda memerlukan email pengguna dalam atribut `User.Email` SAMP 2.0. Selain itu, asumsikan bahwa alamat email disimpan dalam `windowsUpn` atribut di direktori Microsoft AD Anda. Untuk mencapai pemetaan ini, Anda harus membuat perubahan di dua tempat berikut di konsol Pusat Identitas IAM:

1. Pada halaman Direktori, di bawah bagian pemetaan Atribut, Anda perlu memetakan atribut pengguna **`email`**ke **`${dir:windowsUpn}`**atribut (di Maps to this atribut di kolom direktori Anda)
2. Pada halaman Aplikasi, pilih aplikasi dari tabel. Pilih tab Pemetaan Atribut. Kemudian petakan `User.Email` atribut ke **`${user:email}`**atribut (di Maps ke nilai string ini atau atribut pengguna di kolom IAM Identity Center).

Perhatikan bahwa Anda harus menyediakan setiap atribut direktori dalam bentuk ${dir:**`AttributeName`**}. Misalnya, `firstname` atribut di direktori Microsoft AD Anda menjadi`${dir:firstname}`. Adalah penting bahwa setiap atribut direktori memiliki nilai aktual yang ditetapkan. Atribut kehilangan nilai setelahnya `${dir:` akan menyebabkan masalah login pengguna.

Petakan atribut di Pusat Identitas IAM ke atribut di direktori Anda AWS Managed Microsoft AD

Anda dapat menggunakan prosedur berikut untuk menentukan bagaimana atribut pengguna Anda di Pusat Identitas IAM harus dipetakan ke atribut yang sesuai di direktori Microsoft AD Anda.

Untuk memetakan atribut di Pusat Identitas IAM ke atribut di direktori Anda

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Atribut untuk kontrol akses, lalu pilih Kelola Atribut.
4. Pada halaman Kelola atribut untuk kontrol akses, temukan atribut di Pusat Identitas IAM yang ingin Anda petakan, lalu ketik nilai di kotak teks. Misalnya, Anda mungkin ingin memetakan atribut pengguna IAM Identity Center **`email`**ke atribut **`${dir:windowsUpn}`**direktori Microsoft AD.
5. Pilih Simpan perubahan.

Menyediakan pengguna dan grup dari Active Directory

IAM Identity Center menyediakan dua cara berikut untuk menyediakan pengguna dan grup dari Active Directory.

- IAM Identity Center dapat dikonfigurasi Active Directory (AD) sync (disarankan) - Dengan metode sinkronisasi ini, Anda dapat melakukan hal berikut:
  - Kontrol batas data dengan secara eksplisit mendefinisikan pengguna dan grup di Microsoft Active Directory yang secara otomatis disinkronkan ke IAM Identity Center. Anda dapat menambahkan pengguna dan grup atau menghapus pengguna dan grup untuk mengubah cakupan sinkronisasi kapan saja.
  - Tetapkan pengguna yang disinkronkan dan kelompokkan akses masuk tunggal ke Akun AWSatau akses ke aplikasi. Aplikasi dapat berupa aplikasi yang AWS dikelola atau aplikasi yang dikelola pelanggan.
  - Kontrol proses sinkronisasi dengan menjeda dan melanjutkan sinkronisasi sesuai kebutuhan. Ini membantu Anda mengatur beban pada sistem produksi.
- IAM Identity Center AD sync — Dengan metode sinkronisasi ini, Anda menggunakan IAM Identity Center untuk menetapkan pengguna dan grup dalam akses Active Directory ke AWS akun dan aplikasi. Semua identitas dengan tugas secara otomatis disinkronkan ke Pusat Identitas IAM.

Pusat Identitas IAM sinkronisasi AD yang dapat dikonfigurasi

Sinkronisasi Active Directory (AD) IAM Identity Center yang dapat dikonfigurasi memungkinkan Anda untuk secara eksplisit mengonfigurasi identitas di Microsoft Active Directory yang secara otomatis disinkronkan ke Pusat Identitas IAM dan mengontrol proses sinkronisasi.

Topik berikut menyediakan informasi untuk memungkinkan Anda mengonfigurasi dan mengelola sinkronisasi AD yang dapat dikonfigurasi.

Topik

Prasyarat dan pertimbangan

Sebelum Anda menggunakan sinkronisasi AD yang dapat dikonfigurasi, perhatikan prasyarat dan pertimbangan berikut:

- Menentukan pengguna dan grup di Active Directory untuk disinkronkan

  Sebelum Anda dapat menggunakan Pusat Identitas IAM untuk menetapkan akses pengguna dan grup baru ke Akun AWS dan ke aplikasi terkelola atau aplikasi yang AWS dikelola pelanggan, Anda harus menentukan pengguna dan grup di Active Directory untuk disinkronkan, dan kemudian menyinkronkannya ke Pusat Identitas IAM.

  - Sinkronisasi AD — Saat Anda membuat penugasan untuk pengguna dan grup baru menggunakan konsol Pusat Identitas IAM atau tindakan API penetapan terkait, Pusat Identitas IAM mencari pengontrol domain secara langsung untuk pengguna atau grup yang ditentukan, menyelesaikan penetapan, dan kemudian secara berkala menyinkronkan metadata pengguna atau grup ke Pusat Identitas IAM.
  - Sinkronisasi AD yang dapat dikonfigurasi — Pusat Identitas IAM tidak mencari pengontrol domain Anda secara langsung untuk pengguna dan grup. Sebagai gantinya, Anda harus terlebih dahulu menentukan daftar pengguna dan grup untuk disinkronkan. Anda dapat mengonfigurasi daftar ini, juga dikenal sebagai cakupan sinkronisasi, dengan salah satu cara berikut, tergantung pada apakah Anda memiliki pengguna dan grup yang sudah disinkronkan ke Pusat Identitas IAM, atau Anda memiliki pengguna dan grup baru yang Anda sinkronkan untuk pertama kalinya dengan menggunakan sinkronisasi AD yang dapat dikonfigurasi.

  - Pengguna dan grup yang ada: Jika Anda memiliki pengguna dan grup yang sudah disinkronkan ke Pusat Identitas IAM, cakupan sinkronisasi dalam sinkronisasi AD yang dapat dikonfigurasi akan diisi sebelumnya dengan daftar pengguna dan grup tersebut. Untuk menetapkan pengguna atau grup baru, Anda harus secara khusus menambahkannya ke lingkup sinkronisasi. Untuk informasi selengkapnya, lihat Menambahkan pengguna dan grup ke cakupan sinkronisasi.
  - Pengguna dan grup baru: Jika Anda ingin menetapkan akses pengguna dan grup baru ke dan ke aplikasi, Anda harus menentukan pengguna Akun AWS dan grup mana yang akan ditambahkan ke cakupan sinkronisasi dalam sinkronisasi AD yang dapat dikonfigurasi sebelum Anda dapat menggunakan Pusat Identitas IAM untuk membuat penetapan. Untuk informasi selengkapnya, lihat Menambahkan pengguna dan grup ke cakupan sinkronisasi.

- Membuat tugas ke grup bersarang di Active Directory

  Grup yang merupakan anggota kelompok lain disebut kelompok bersarang (atau kelompok anak). Saat Anda membuat penetapan ke grup di Active Directory yang berisi grup bersarang, cara penerapan penetapan bergantung pada apakah Anda menggunakan sinkronisasi AD atau sinkronisasi AD yang dapat dikonfigurasi.

  - Sinkronisasi AD — Saat Anda membuat penugasan ke grup di Direktori Aktif yang berisi grup bersarang, hanya anggota langsung grup yang dapat mengakses akun tersebut. Misalnya, jika Anda menetapkan akses ke Grup A, dan Grup B adalah anggota Grup A, hanya anggota langsung Grup A yang dapat mengakses akun tersebut. Tidak ada anggota Grup B yang mewarisi akses tersebut.
  - Sinkronisasi AD yang dapat dikonfigurasi — Menggunakan sinkronisasi AD yang dapat dikonfigurasi untuk membuat penetapan ke grup di Direktori Aktif yang berisi grup bersarang dapat meningkatkan cakupan pengguna yang memiliki akses ke atau ke Akun AWS aplikasi. Dalam hal ini, penugasan berlaku untuk semua pengguna, termasuk yang berada di grup bersarang. Misalnya, jika Anda menetapkan akses ke Grup A, dan Grup B adalah anggota Grup A, anggota Grup B juga mewarisi akses ini.
- Memperbarui alur kerja otomatis

  Jika Anda memiliki alur kerja otomatis yang menggunakan tindakan API penyimpanan identitas Pusat Identitas IAM dan tindakan API penetapan Pusat Identitas IAM untuk menetapkan akses pengguna dan grup baru ke akun dan aplikasi, dan untuk menyinkronkannya ke Pusat Identitas IAM, Anda harus menyesuaikan alur kerja tersebut sebelum 15 April 2022 agar berfungsi seperti

yang diharapkan dengan sinkronisasi AD yang dapat dikonfigurasi. Sinkronisasi AD yang dapat dikonfigurasi mengubah urutan penetapan dan penyediaan pengguna dan grup, serta cara kueri dilakukan.

- Sinkronisasi AD — Proses penugasan terjadi terlebih dahulu. Anda menetapkan akses pengguna dan grup ke Akun AWS dan ke aplikasi. Setelah pengguna dan grup diberi akses, mereka secara otomatis disediakan (disinkronkan ke Pusat Identitas IAM). Jika Anda memiliki alur kerja otomatis, ini berarti bahwa ketika Anda menambahkan pengguna baru ke Active Directory, alur kerja otomatis Anda dapat menanyakan Active Directory untuk pengguna dengan menggunakan tindakan `ListUser` API penyimpanan identitas, lalu menetapkan akses pengguna dengan menggunakan tindakan API penetapan IAM Identity Center. Karena pengguna memiliki tugas, pengguna tersebut secara otomatis disediakan ke Pusat Identitas IAM.
- Sinkronisasi AD yang dapat dikonfigurasi — Penyediaan terjadi terlebih dahulu, dan tidak dilakukan secara otomatis. Sebagai gantinya, Anda harus terlebih dahulu menambahkan pengguna dan grup secara eksplisit ke toko identitas dengan menambahkannya ke lingkup sinkronisasi Anda. Untuk informasi tentang langkah-langkah yang disarankan untuk mengotomatiskan konfigurasi sinkronisasi untuk sinkronisasi AD yang dapat dikonfigurasi, lihat. Otomatiskan konfigurasi sinkronisasi Anda untuk sinkronisasi AD yang dapat dikonfigurasi

Cara kerja sinkronisasi AD yang dapat dikonfigurasi

IAM Identity Center menyegarkan data identitas berbasis iklan di toko identitas dengan menggunakan proses berikut.

Pembuatan

Setelah menghubungkan direktori yang dikelola sendiri di Active Directory atau AWS Managed Microsoft AD direktori yang dikelola oleh AWS Directory Service IAM Identity Center, Anda dapat secara eksplisit mengonfigurasi pengguna dan grup Active Directory yang ingin Anda sinkronkan ke dalam penyimpanan identitas IAM Identity Center. Identitas yang Anda pilih akan disinkronkan setiap tiga jam atau lebih ke toko identitas IAM Identity Center. Bergantung pada ukuran direktori Anda, proses sinkronisasi mungkin memakan waktu lebih lama.

Grup yang merupakan anggota kelompok lain (disebut grup bersarang atau kelompok anak) juga ditulis ke toko identitas. Saat Anda membuat penetapan ke grup di Active Directory yang berisi grup bersarang, cara penerapan penetapan bergantung pada apakah Anda menggunakan sinkronisasi AD atau sinkronisasi AD yang dapat dikonfigurasi. Untuk informasi selengkapnya, lihat Making assignments to nested groups in Active Directory.

Anda hanya dapat menetapkan akses ke pengguna atau grup baru setelah mereka disinkronkan ke toko identitas Pusat Identitas IAM.

Perbarui

Data identitas di toko identitas IAM Identity Center tetap segar dengan membaca data secara berkala dari direktori sumber di Active Directory. IAM Identity Center menyinkronkan data dari Active Directory Anda setiap jam dalam siklus sinkronisasi secara default. Mungkin diperlukan waktu 30 menit hingga 2 jam agar data disinkronkan ke Pusat Identitas IAM, berdasarkan ukuran Direktori Aktif Anda.

Objek pengguna dan grup yang berada dalam lingkup sinkronisasi dan keanggotaannya dibuat atau diperbarui di Pusat Identitas IAM untuk dipetakan ke objek yang sesuai di direktori sumber di Active Directory. Untuk atribut pengguna, hanya subset atribut yang tercantum di bagian Atribut untuk kontrol akses konsol Pusat Identitas IAM yang diperbarui di Pusat Identitas IAM. Mungkin diperlukan satu siklus sinkronisasi untuk pembaruan atribut apa pun yang Anda buat di Active Directory untuk tercermin di Pusat Identitas IAM.

Anda juga dapat memperbarui subset pengguna dan grup yang Anda sinkronkan ke toko identitas IAM Identity Center. Anda dapat memilih untuk menambahkan pengguna atau grup baru ke subset ini, atau menghapusnya. Setiap identitas yang Anda tambahkan disinkronkan pada sinkronisasi terjadwal berikutnya. Identitas yang Anda hapus dari subset akan berhenti diperbarui di toko identitas Pusat Identitas IAM. Setiap pengguna yang tidak disinkronkan selama lebih dari 28 hari akan dinonaktifkan di toko identitas IAM Identity Center. Objek pengguna yang sesuai akan dinonaktifkan secara otomatis di penyimpanan identitas Pusat Identitas IAM selama siklus sinkronisasi berikutnya, kecuali mereka adalah bagian dari grup lain yang masih merupakan bagian dari lingkup sinkronisasi.

Penghapusan

Pengguna dan grup dihapus dari penyimpanan identitas IAM Identity Center ketika objek pengguna atau grup yang sesuai dihapus dari direktori sumber di Active Directory. Atau, Anda dapat secara eksplisit menghapus objek pengguna dari penyimpanan identitas Pusat Identitas IAM dengan menggunakan konsol Pusat Identitas IAM. Jika Anda menggunakan konsol Pusat Identitas IAM, Anda juga harus menghapus pengguna dari lingkup sinkronisasi untuk memastikan bahwa mereka tidak disinkronkan kembali ke Pusat Identitas IAM selama siklus sinkronisasi berikutnya.

Anda juga dapat menjeda dan memulai ulang sinkronisasi kapan saja. Jika Anda menjeda sinkronisasi selama lebih dari 28 hari, semua pengguna Anda akan dinonaktifkan.

Konfigurasikan dan kelola cakupan sinkronisasi

Anda dapat mengonfigurasi cakupan sinkronisasi dengan salah satu cara berikut:

- Pengaturan terpandu: Jika Anda menyinkronkan pengguna dan grup dari Active Directory ke IAM Identity Center untuk pertama kalinya, ikuti langkah-langkah Pengaturan terpandu untuk mengonfigurasi cakupan sinkronisasi Anda. Setelah menyelesaikan penyiapan terpandu, Anda dapat mengubah cakupan sinkronisasi kapan saja dengan mengikuti prosedur lain di bagian ini.
- Jika Anda sudah memiliki pengguna dan grup yang disinkronkan ke Pusat Identitas IAM atau Anda tidak ingin mengikuti pengaturan yang dipandu, pilih Kelola sinkronisasi. Lewati prosedur penyiapan terpandu dan ikuti prosedur lain di bagian ini sebagaimana diperlukan untuk mengonfigurasi dan mengelola cakupan sinkronisasi Anda.

Prosedur

- Pengaturan terpandu
- Menambahkan pengguna dan grup ke cakupan sinkronisasi
- Hapus pengguna dan grup dari cakupan sinkronisasi Anda
- Jeda dan lanjutkan sinkronisasi
- Konfigurasikan pemetaan atribut untuk sinkronisasi Anda
- Otomatiskan konfigurasi sinkronisasi Anda untuk sinkronisasi AD yang dapat dikonfigurasi

Pengaturan terpandu

1. Buka konsol Pusat Identitas IAM.

   > **Note**
   >
   > Pastikan bahwa konsol IAM Identity Center menggunakan salah satu Wilayah AWS tempat AWS Managed Microsoft AD direktori Anda berada sebelum Anda pindah ke langkah berikutnya.

2. Pilih Pengaturan.
3. Di bagian atas halaman, dalam pesan notifikasi, pilih Mulai penyiapan yang dipandu.
4. Pada Langkah 1 - opsional: Konfigurasikan pemetaan atribut, tinjau pemetaan atribut pengguna dan grup default. Jika tidak ada perubahan yang diperlukan, pilih Berikutnya. Jika perubahan diperlukan, buat perubahan, lalu pilih Simpan perubahan.

5. Pada Langkah 2 — opsional: Konfigurasikan lingkup sinkronisasi, pilih tab Pengguna. Kemudian, masukkan nama pengguna yang tepat dari pengguna yang ingin Anda tambahkan ke lingkup sinkronisasi Anda dan pilih Tambah. Selanjutnya, pilih tab Grup. Masukkan nama grup yang tepat dari grup yang ingin Anda tambahkan ke cakupan sinkronisasi Anda dan pilih Tambah. Lalu, pilih Selanjutnya. Jika Anda ingin menambahkan pengguna dan grup ke cakupan sinkronisasi nanti, jangan buat perubahan dan pilih Berikutnya.
6. Pada Langkah 3: Tinjau dan simpan konfigurasi, konfirmasikan pemetaan Atribut Anda di Langkah 1: Pemetaan atribut dan Pengguna serta grup Anda di Langkah 2: Lingkup sinkronisasi. Pilih Simpan konfigurasi. Ini akan membawa Anda ke halaman Kelola Sinkronisasi.

Menambahkan pengguna dan grup ke cakupan sinkronisasi

Untuk menambahkan pengguna

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Sumber identitas, pilih Tindakan, lalu pilih Kelola Sinkronisasi.
4. Pada halaman Kelola Sinkronisasi, pilih tab Pengguna, lalu pilih Tambahkan pengguna dan grup.
5. Pada tab Pengguna, di bawah Pengguna, masukkan nama pengguna yang tepat dan pilih Tambah.
6. Di bawah Pengguna dan Grup yang Ditambahkan, tinjau pengguna yang ingin Anda tambahkan.
7. Pilih Kirim.
8. Di panel navigasi, pilih Pengguna.
9. Pada halaman Pengguna, mungkin diperlukan beberapa waktu bagi pengguna yang Anda tentukan untuk muncul dalam daftar. Pilih ikon penyegaran untuk memperbarui daftar pengguna.

Untuk menambahkan grup

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Sumber identitas, pilih Tindakan, lalu pilih Kelola Sinkronisasi.
4. Pada halaman Kelola Sinkronisasi, pilih tab Grup, lalu pilih Tambahkan pengguna dan grup.

5. Pilih tab Grup. Di bawah Grup, masukkan nama grup yang tepat dan pilih Tambah.
6. Di bawah Pengguna dan Grup yang Ditambahkan, tinjau grup yang ingin Anda tambahkan.
7. Pilih Kirim.
8. Di panel navigasi, pilih Grup.
9. Pada halaman Grup, mungkin perlu beberapa waktu untuk grup yang Anda tentukan muncul dalam daftar. Pilih ikon penyegaran untuk memperbarui daftar grup.

Hapus pengguna dan grup dari cakupan sinkronisasi Anda

Untuk informasi selengkapnya tentang apa yang terjadi saat Anda menghapus pengguna dan grup dari cakupan sinkronisasi, lihatCara kerja sinkronisasi AD yang dapat dikonfigurasi.

Untuk menghapus pengguna

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Sumber identitas, pilih Tindakan, lalu pilih Kelola Sinkronisasi.
4. Pilih tab Pengguna.
5. Di bawah Pengguna dalam lingkup sinkronisasi, pilih kotak centang di samping pengguna yang ingin Anda hapus. Untuk menghapus semua pengguna, pilih kotak centang di samping Nama Pengguna.
6. Pilih Hapus.

Untuk menghapus grup

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Sumber identitas, pilih Tindakan, lalu pilih Kelola Sinkronisasi.
4. Pilih tab Grup.
5. Di bawah Grup dalam lingkup sinkronisasi, pilih kotak centang di samping pengguna yang ingin Anda hapus. Untuk menghapus semua grup, pilih kotak centang di samping Nama grup.
6. Pilih Hapus.

Jeda dan lanjutkan sinkronisasi

Menjeda sinkronisasi akan menjeda semua siklus sinkronisasi di masa mendatang dan mencegah perubahan apa pun yang Anda buat pada pengguna dan grup di Active Directory agar tidak tercermin di IAM Identity Center. Setelah Anda melanjutkan sinkronisasi, siklus sinkronisasi mengambil perubahan ini dari sinkronisasi terjadwal berikutnya.

Untuk menjeda sinkronisasi

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Sumber identitas, pilih Tindakan, lalu pilih Kelola Sinkronisasi.
4. Di bawah Kelola Sinkronisasi, pilih Jeda sinkronisasi.

Untuk melanjutkan sinkronisasi

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Sumber identitas, pilih Tindakan, lalu pilih Kelola Sinkronisasi.
4. Di bawah Kelola Sinkronisasi, pilih Lanjutkan sinkronisasi.

> **Note**
>
> Jika Anda melihat Jeda sinkronisasi bukan Lanjutkan sinkronisasi, sinkronisasi dari Active Directory ke IAM Identity Center telah dilanjutkan.

Konfigurasikan pemetaan atribut untuk sinkronisasi Anda

Untuk informasi selengkapnya tentang atribut yang tersedia, lihatPemetaan atribut untuk direktori AWS Managed Microsoft AD.

Untuk mengonfigurasi pemetaan atribut di Pusat Identitas IAM ke direktori Anda

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan.

3. Pada halaman Pengaturan, pilih tab Sumber identitas, pilih Tindakan, lalu pilih Kelola Sinkronisasi.
4. Di bawah Kelola Sinkronisasi, pilih Lihat pemetaan atribut.
5. Di bawah atribut pengguna Active Directory, konfigurasikan atribut penyimpanan identitas IAM Identity Center dan atribut pengguna Active Directory. Misalnya, Anda mungkin ingin memetakan atribut penyimpanan identitas Pusat Identitas IAM `email` ke atribut `${objectguid}` direktori pengguna Active Directory.

   > **Note**
   >
   > Di bawah atribut Grup, atribut penyimpanan identitas Pusat Identitas IAM dan atribut grup Direktori Aktif tidak dapat diubah.

6. Pilih Simpan perubahan. Ini mengembalikan Anda ke halaman Kelola Sinkronisasi.

Otomatiskan konfigurasi sinkronisasi Anda untuk sinkronisasi AD yang dapat dikonfigurasi

Untuk memastikan alur kerja otomatis Anda berfungsi seperti yang diharapkan dengan sinkronisasi AD yang dapat dikonfigurasi, sebaiknya Anda melakukan langkah-langkah berikut untuk mengotomatiskan konfigurasi sinkronisasi Anda.

Untuk mengotomatiskan konfigurasi sinkronisasi Anda untuk sinkronisasi AD yang dapat dikonfigurasi

1. Di Active Directory, buat grup sinkronisasi induk untuk memuat semua pengguna dan grup yang ingin Anda sinkronkan ke Pusat Identitas IAM. Misalnya, Anda dapat memberi nama grup IAM IdentityCenterAllUsersAndGroups.
2. Di Pusat Identitas IAM, tambahkan grup sinkronisasi induk ke daftar sinkronisasi yang dapat dikonfigurasi. IAM Identity Center akan menyinkronkan semua pengguna, grup, sub-grup, dan anggota dari semua grup yang terdapat dalam grup sinkronisasi induk.
3. Gunakan tindakan API manajemen pengguna dan grup Active Directory yang disediakan oleh Microsoft untuk menambah atau menghapus pengguna dan grup dari grup sinkronisasi induk.

Sinkronisasi AD Pusat Identitas IAM

Dengan sinkronisasi AD Pusat Identitas IAM, Anda menggunakan Pusat Identitas IAM untuk menetapkan pengguna dan grup dalam akses Direktori Aktif ke Akun AWS dan ke aplikasi terkelola

atau aplikasi yang AWS dikelola pelanggan. Semua identitas dengan tugas secara otomatis disinkronkan ke Pusat Identitas IAM.

Cara kerja sinkronisasi AD Pusat Identitas IAM

IAM Identity Center menyegarkan data identitas berbasis iklan di toko identitas menggunakan proses berikut.

Pembuatan

Saat Anda menetapkan pengguna atau grup ke atau aplikasi menggunakan AWS konsol Akun AWS atau panggilan API penetapan, informasi tentang pengguna, grup, dan keanggotaan disinkronkan secara berkala ke dalam penyimpanan identitas Pusat Identitas IAM. Pengguna atau grup yang ditambahkan ke tugas IAM Identity Center biasanya muncul di toko AWS identitas dalam waktu dua jam. Bergantung pada jumlah data yang disinkronkan, proses ini mungkin memakan waktu lebih lama. Hanya pengguna dan grup yang langsung diberi akses, atau anggota grup yang diberi akses, yang disinkronkan.

Grup yang merupakan anggota kelompok lain (disebut grup bersarang) juga ditulis ke toko identitas. Saat Anda membuat penetapan ke grup di Active Directory yang berisi grup bersarang, cara penerapan penetapan bergantung pada apakah Anda menggunakan sinkronisasi AD atau sinkronisasi AD yang dapat dikonfigurasi.

- Sinkronisasi AD — Saat Anda membuat penugasan ke grup di Direktori Aktif yang berisi grup bersarang, hanya anggota langsung grup yang dapat mengakses akun tersebut. Misalnya, jika Anda menetapkan akses ke Grup A, dan Grup B adalah anggota Grup A, hanya anggota langsung Grup A yang dapat mengakses akun tersebut. Tidak ada anggota Grup B yang mewarisi akses tersebut.
- Sinkronisasi AD yang dapat dikonfigurasi — Menggunakan sinkronisasi AD yang dapat dikonfigurasi untuk membuat penetapan ke grup di Direktori Aktif yang berisi grup bersarang dapat meningkatkan cakupan pengguna yang memiliki akses ke atau ke Akun AWS aplikasi. Dalam hal ini, penugasan berlaku untuk semua pengguna, termasuk yang berada di grup bersarang. Misalnya, jika Anda menetapkan akses ke Grup A, dan Grup B adalah anggota Grup A, anggota Grup B juga mewarisi akses ini.

Jika pengguna mengakses Pusat Identitas IAM sebelum objek penggunanya disinkronkan untuk pertama kalinya, objek penyimpanan identitas pengguna tersebut dibuat sesuai permintaan menggunakan penyediaan just-in-time (JIT). Pengguna yang dibuat oleh penyediaan JIT tidak

disinkronkan kecuali mereka telah secara langsung menetapkan atau hak Pusat Identitas IAM berbasis grup. Keanggotaan grup untuk pengguna yang disediakan JIT tidak tersedia hingga setelah sinkronisasi.

Untuk petunjuk tentang cara menetapkan akses pengguna Akun AWS, lihatAkses masuk tunggal ke Akun AWS.

Perbarui

Data identitas di toko identitas IAM Identity Center tetap segar dengan membaca data secara berkala dari direktori sumber di Active Directory. Data identitas yang diubah di Active Directory biasanya akan muncul di toko AWS identitas dalam waktu empat jam. Bergantung pada jumlah data yang disinkronkan, proses ini mungkin memakan waktu lebih lama.

Objek pengguna dan grup dan keanggotaannya dibuat atau diperbarui di Pusat Identitas IAM untuk dipetakan ke objek yang sesuai di direktori sumber di Active Directory. Untuk atribut pengguna, hanya subset atribut yang tercantum di bagian Kelola atribut untuk kontrol akses konsol Pusat Identitas IAM yang diperbarui di Pusat Identitas IAM. Selain itu, atribut pengguna diperbarui dengan setiap peristiwa otentikasi pengguna.

Penghapusan

Pengguna dan grup dihapus dari penyimpanan identitas IAM Identity Center ketika objek pengguna atau grup yang sesuai dihapus dari direktori sumber di Active Directory.

Connect ke penyedia identitas eksternal

Jika Anda menggunakan direktori yang dikelola sendiri di Active Directory atau direktori AWS Managed Microsoft AD, lihatConnect ke Microsoft AD direktori. Untuk penyedia identitas eksternal lainnya (IdPs), Anda dapat menggunakan AWS IAM Identity Center untuk mengautentikasi identitas dari IdPs melalui standar Security Assertion Markup Language (SAMP) 2.0. Hal ini memungkinkan pengguna Anda untuk masuk ke portal AWS akses dengan kredensi perusahaan mereka. Mereka kemudian dapat menavigasi ke akun, peran, dan aplikasi yang ditetapkan yang dihosting di eksternal IdPs.

Misalnya, Anda dapat menghubungkan IDP eksternal seperti Okta atauMicrosoft Entra ID, ke IAM Identity Center. Pengguna Anda kemudian dapat masuk ke portal AWS akses dengan kredensialnya yang ada Okta atau Microsoft Entra ID kredensialnya. Untuk mengontrol apa yang dapat dilakukan pengguna setelah mereka masuk, Anda dapat menetapkan izin akses secara terpusat di semua akun dan aplikasi di organisasi Anda. AWS Selain itu, pengembang cukup masuk ke AWS Command Line

Interface (AWS CLI) menggunakan kredensialnya yang ada, dan mendapat manfaat dari pembuatan dan rotasi kredenal jangka pendek otomatis.

Protokol SAMP tidak menyediakan cara untuk menanyakan IDP untuk mempelajari tentang pengguna dan grup. Oleh karena itu, Anda harus membuat Pusat Identitas IAM mengetahui pengguna dan grup tersebut dengan menyediakannya ke Pusat Identitas IAM.

Penyediaan saat pengguna berasal dari iDP eksternal

Saat menggunakan iDP eksternal, Anda harus menyediakan semua pengguna dan grup yang berlaku ke Pusat Identitas IAM sebelum Anda dapat membuat tugas atau aplikasi apa pun. Akun AWS Untuk melakukan ini, Anda dapat mengonfigurasi Penyediaan otomatis untuk pengguna dan grup Anda, atau gunakanPenyediaan manual. Terlepas dari bagaimana Anda menyediakan pengguna, IAM Identity Center mengalihkan, antarmuka baris perintah AWS Management Console, dan otentikasi aplikasi ke iDP eksternal Anda. IAM Identity Center kemudian memberikan akses ke sumber daya tersebut berdasarkan kebijakan yang Anda buat di IAM Identity Center. Untuk informasi selengkapnya tentang penyediaan, lihat. Penyediaan pengguna dan grup

Cara terhubung ke penyedia identitas eksternal

Ada step-by-step tutorial yang tersedia untuk yang didukung IdPs:

- CyberArk
- Google Workspace
- JumpCloud
- Microsoft Entra ID
- Okta
- OneLogin
- Identitas Ping

Ada berbagai prasyarat, pertimbangan, dan prosedur penyediaan untuk eksternal yang didukung berbeda. IdPs Prosedur berikut memberikan gambaran umum tentang prosedur yang digunakan dengan semua penyedia identitas eksternal.

Untuk terhubung ke penyedia identitas eksternal

1. Buka konsol Pusat Identitas IAM.

2. Pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Sumber identitas, lalu pilih Tindakan > Ubah sumber identitas.
4. Di bawah Pilih sumber identitas, pilih Penyedia identitas eksternal, lalu pilih Berikutnya.
5. Di bawah Konfigurasi penyedia identitas eksternal, lakukan hal berikut:

    a. Di bawah metadata penyedia layanan, pilih Unduh file metadata untuk mengunduh file metadata dan menyimpannya di sistem Anda. File metadata SAMP Pusat Identitas IAM diperlukan oleh penyedia identitas eksternal Anda.

    b. Di bawah Metadata penyedia identitas, pilih Pilih file, dan temukan file metadata yang Anda unduh dari penyedia identitas eksternal Anda. Kemudian unggah file tersebut. File metadata ini berisi sertifikat x509 publik yang diperlukan yang digunakan untuk mempercayai pesan yang dikirim dari iDP.

    c. Pilih Berikutnya.

    > **Important**
    >
    > Mengubah sumber Anda ke atau dari Active Directory menghapus semua penetapan pengguna dan grup yang ada. Anda harus mengajukan kembali tugas secara manual setelah Anda berhasil mengubah sumber Anda.

6. Setelah Anda membaca disclaimer dan siap untuk melanjutkan, masukkan ACCEPT.
7. Pilih Ubah sumber identitas. Pesan status memberi tahu Anda bahwa Anda berhasil mengubah sumber identitas.

Topik

- Menggunakan federasi identitas SAMP dan SCIM dengan penyedia identitas eksternal
- Profil SCIM dan implementasi SAMP 2.0

Menggunakan federasi identitas SAMP dan SCIM dengan penyedia identitas eksternal

IAM Identity Center mengimplementasikan protokol berbasis standar berikut untuk federasi identitas:

- SAMP 2.0 untuk otentikasi pengguna
- SCIM untuk penyediaan

Setiap penyedia identitas (IDP) yang mengimplementasikan protokol standar ini diharapkan dapat berhasil beroperasi dengan IAM Identity Center, dengan pertimbangan khusus berikut:

- SAM
  - IAM Identity Center memerlukan format alamat email SAMP NameID (yaitu,). `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
  - Nilai bidang NameId dalam pernyataan harus berupa string RFC 2822 (https://tools.ietf.org/html/rfc2822) yang sesuai dengan spesifikasi addr-(“”) (https://tools.ietf.org/html/rfc2822#section-3.4.1). `name@domain.com`
  - File metadata tidak boleh lebih dari 75000 karakter.
  - Metadata harus berisi EntityID, sertifikat X509, dan SingleSignOnService sebagai bagian dari URL masuk.
  - Kunci enkripsi tidak didukung.

- SCIM
  - Implementasi IAM Identity Center SCIM didasarkan pada SCIM RFC 7642 (https://tools.ietf.org/html/rfc7642), 7643 (https://tools.ietf.org/html/rfc7643), dan 7644 (https://tools.ietf.org/html/rfc7644), dan persyaratan interoperabilitas yang tercantum dalam draf Maret 2020 dari Profil SCIM Dasar 1.0 (https://openid.net/specs/fastfed-scim-1_0-02.html#rfc.section.4). FastFed Perbedaan apa pun antara dokumen ini dan implementasi saat ini di Pusat Identitas IAM dijelaskan di bagian Operasi API yang Didukung dari Panduan Pengembang Implementasi SCIM Pusat Identitas IAM.

IdPs yang tidak sesuai dengan standar dan pertimbangan yang disebutkan di atas tidak didukung. Silakan hubungi IDP Anda untuk pertanyaan atau klarifikasi mengenai kesesuaian produk mereka dengan standar dan pertimbangan ini.

Jika Anda memiliki masalah dalam menghubungkan IDP Anda ke IAM Identity Center, kami sarankan Anda memeriksa:

- AWS CloudTrail log dengan memfilter pada nama ExternalId acara P DirectoryLogin
- Log khusus IDP dan/atau log debug
- Memecahkan masalah Pusat Identitas IAM

> **Note**
>
> Beberapa IdPs, seperti yang ada diMemulai tutorial, menawarkan pengalaman konfigurasi yang disederhanakan untuk IAM Identity Center dalam bentuk “aplikasi” atau “konektor” yang dibangun khusus untuk IAM Identity Center. Jika IDP Anda menyediakan opsi ini, kami sarankan Anda menggunakannya, berhati-hati untuk memilih item yang dibuat khusus untuk IAM Identity Center. Item lain yang disebut “AWS”, “AWS federasi”, atau nama “AWS" generik serupa dapat menggunakan pendekatan federasi dan/atau titik akhir lainnya, dan mungkin tidak berfungsi seperti yang diharapkan dengan IAM Identity Center.

Profil SCIM dan implementasi SAMP 2.0

Baik SCIM dan SAMP merupakan pertimbangan penting untuk mengkonfigurasi IAM Identity Center.

Implementasi SAMP 2.0

IAM Identity Center mendukung federasi identitas dengan SAMP (Security Assertion Markup Language) 2.0. Hal ini memungkinkan IAM Identity Center untuk mengautentikasi identitas dari penyedia identitas eksternal (). IdPs SAMP 2.0 adalah standar terbuka yang digunakan untuk bertukar pernyataan SAMP dengan aman. SAMP 2.0 meneruskan informasi tentang pengguna antara otoritas SAMP (disebut penyedia identitas atau IDP), dan konsumen SAMP (disebut penyedia layanan atau SP). Layanan IAM Identity Center menggunakan informasi ini untuk menyediakan sistem masuk tunggal federasi. Single sign-on memungkinkan pengguna untuk mengakses Akun AWS dan mengkonfigurasi aplikasi berdasarkan kredensi penyedia identitas yang ada.

IAM Identity Center menambahkan kemampuan SAMP iDP ke toko IAM Identity Center Anda, AWS Managed Microsoft AD, atau ke penyedia identitas eksternal. Pengguna kemudian dapat masuk tunggal ke layanan yang mendukung SAMP, termasuk aplikasi AWS Management Console dan pihak ketiga sepertiMicrosoft 365,, Concur dan. Salesforce

Namun protokol SAMP tidak menyediakan cara untuk menanyakan IDP untuk mempelajari tentang pengguna dan grup. Oleh karena itu, Anda harus membuat Pusat Identitas IAM mengetahui pengguna dan grup tersebut dengan menyediakannya ke Pusat Identitas IAM.

Profil SCIM

IAM Identity Center menyediakan dukungan untuk standar System for Cross-domain Identity Management (SCIM) v2.0. SCIM menjaga identitas IAM Identity Center Anda tetap sinkron dengan

identitas dari IDP Anda. Ini termasuk penyediaan, pembaruan, dan penonaktifan pengguna antara IDP dan Pusat Identitas IAM Anda.

Untuk informasi selengkapnya tentang cara menerapkan SCIM, lihatPenyediaan otomatis. Untuk detail tambahan tentang implementasi SCIM IAM Identity Center, lihat Panduan Pengembang Implementasi SCIM Pusat Identitas IAM.

Topik

- Penyediaan otomatis
- Penyediaan manual
- Kelola sertifikat SAMP 2.0

Penyediaan otomatis

IAM Identity Center mendukung penyediaan otomatis (sinkronisasi) informasi pengguna dan grup dari penyedia identitas Anda (IDP) ke Pusat Identitas IAM menggunakan protokol System for Cross-domain Identity Management (SCIM) v2.0. Saat mengonfigurasi sinkronisasi SCIM, Anda membuat pemetaan atribut pengguna penyedia identitas (iDP) Anda ke atribut bernama di Pusat Identitas IAM. Hal ini menyebabkan atribut yang diharapkan cocok antara IAM Identity Center dan IDP Anda. Anda mengonfigurasi koneksi ini di IDP Anda menggunakan endpoint SCIM Anda untuk IAM Identity Center dan token pembawa yang Anda buat di IAM Identity Center.

Topik

- Pertimbangan untuk menggunakan penyediaan otomatis
- Cara memantau kedaluwarsa token akses
- Cara mengaktifkan penyediaan otomatis
- Cara menonaktifkan penyediaan otomatis
- Cara menghasilkan token akses baru
- Cara menghapus token akses
- Cara memutar token akses

Pertimbangan untuk menggunakan penyediaan otomatis

Sebelum Anda mulai menerapkan SCIM, kami sarankan Anda terlebih dahulu meninjau pertimbangan penting berikut tentang cara kerjanya dengan IAM Identity Center. Untuk pertimbangan penyediaan tambahan, lihat yang Memulai tutorial berlaku untuk IDP Anda.

- Jika Anda menyediakan alamat email utama, nilai atribut ini harus unik untuk setiap pengguna. Dalam beberapa IdPs, alamat email utama mungkin bukan alamat email asli. Misalnya, itu mungkin Universal Principal Name (UPN) yang hanya terlihat seperti email. Ini IdPs mungkin memiliki alamat email sekunder atau “lain” yang berisi alamat email asli pengguna. Anda harus mengonfigurasi SCIM di IDP Anda untuk memetakan alamat email unik non-Null ke atribut alamat email utama IAM Identity Center. Dan Anda harus memetakan pengenal masuk unik non-Null pengguna ke atribut nama pengguna IAM Identity Center. Periksa untuk melihat apakah IDP Anda memiliki nilai tunggal yang merupakan pengenal masuk dan nama email pengguna. Jika demikian, Anda dapat memetakan bidang IDP tersebut ke email utama IAM Identity Center dan nama pengguna IAM Identity Center.
- Agar sinkronisasi SCIM berfungsi, setiap pengguna harus memiliki nilai Nama Depan, Nama belakang, Nama Pengguna, dan Nama tampilan yang ditentukan. Jika salah satu dari nilai-nilai ini hilang dari pengguna, pengguna tersebut tidak akan disediakan.
- Jika Anda perlu menggunakan aplikasi pihak ketiga, Anda harus terlebih dahulu memetakan atribut subjek SAMP keluar ke atribut nama pengguna. Jika aplikasi pihak ketiga memerlukan alamat email yang dapat dirutekan, Anda harus memberikan atribut email ke IDP Anda.
- Penyediaan SCIM dan interval pembaruan dikendalikan oleh penyedia identitas Anda. Perubahan pada pengguna dan grup di penyedia identitas Anda hanya tercermin di Pusat Identitas IAM setelah penyedia identitas Anda mengirimkan perubahan tersebut ke Pusat Identitas IAM. Periksa dengan penyedia identitas Anda untuk detail tentang frekuensi pembaruan pengguna dan grup.
- Saat ini, atribut multivalue (seperti beberapa email atau nomor telepon untuk pengguna tertentu) tidak disediakan dengan SCIM. Upaya untuk menyinkronkan atribut multivalue ke IAM Identity Center dengan SCIM akan gagal. Untuk menghindari kegagalan, pastikan bahwa hanya satu nilai yang dilewatkan untuk setiap atribut. Jika Anda memiliki pengguna dengan atribut multivalue, hapus atau modifikasi pemetaan atribut duplikat di SCIM di idP Anda untuk koneksi ke IAM Identity Center.
- Verifikasi bahwa pemetaan `externalId` SCIM di IDP Anda sesuai dengan nilai yang unik, selalu ada, dan paling tidak mungkin berubah untuk pengguna Anda. Misalnya, IDP Anda mungkin memberikan jaminan `objectId` atau pengenal lain yang tidak terpengaruh oleh perubahan atribut pengguna seperti nama dan email. Jika demikian, Anda dapat memetakan nilai itu ke `externalId` bidang SCIM. Ini memastikan bahwa pengguna Anda tidak akan kehilangan AWS hak, penetapan, atau izin jika Anda perlu mengubah nama atau email mereka.
- Pengguna yang belum ditugaskan ke aplikasi atau Akun AWS tidak dapat disediakan ke Pusat Identitas IAM. Untuk menyinkronkan pengguna dan grup, pastikan bahwa mereka ditetapkan ke aplikasi atau pengaturan lain yang mewakili koneksi IDP Anda ke IAM Identity Center.

- Perilaku deprovisioning pengguna dikelola oleh penyedia identitas dan dapat bervariasi menurut implementasinya. Periksa dengan penyedia identitas Anda untuk detail tentang deprovisioning pengguna.

Untuk informasi selengkapnya tentang implementasi SCIM IAM Identity Center, lihat Panduan Pengembang Implementasi IAM Identity Center SCIM.

Cara memantau kedaluwarsa token akses

Token akses SCIM dihasilkan dengan validitas satu tahun. Ketika token akses SCIM Anda diatur untuk kedaluwarsa dalam 90 hari atau kurang, AWS mengirimkan pengingat di konsol Pusat Identitas IAM dan melalui AWS Health Dasbor untuk membantu Anda memutar token. Dengan memutar token akses SCIM sebelum kedaluwarsa, Anda terus mengamankan penyediaan otomatis informasi pengguna dan grup. Jika token akses SCIM kedaluwarsa, sinkronisasi informasi pengguna dan grup dari penyedia identitas Anda ke Pusat Identitas IAM berhenti, sehingga penyediaan otomatis tidak dapat lagi melakukan pembaruan atau membuat dan menghapus informasi. Gangguan terhadap penyediaan otomatis dapat menimbulkan peningkatan risiko keamanan dan berdampak pada akses ke layanan Anda.

Pengingat konsol Pusat Identitas tetap ada hingga Anda memutar token akses SCIM dan menghapus token akses yang tidak digunakan atau kedaluwarsa. Acara AWS Health Dasbor diperbarui setiap minggu antara 90 hingga 60 hari, dua kali per minggu dari 60 hingga 30 hari, tiga kali per minggu dari 30 hingga 15 hari, dan setiap hari dari 15 hari hingga token akses SCIM kedaluwarsa.

Cara mengaktifkan penyediaan otomatis

Gunakan prosedur berikut untuk mengaktifkan penyediaan otomatis pengguna dan grup dari IDP Anda ke Pusat Identitas IAM menggunakan protokol SCIM.

> **Note**
>
> Sebelum Anda memulai prosedur ini, kami sarankan Anda terlebih dahulu meninjau pertimbangan penyediaan yang berlaku untuk IDP Anda. Untuk informasi selengkapnya, lihat Memulai tutorial untuk IDP Anda.

Untuk mengaktifkan penyediaan otomatis di Pusat Identitas IAM

1. Setelah Anda menyelesaikan prasyarat, buka konsol Pusat Identitas IAM.

2. Pilih Pengaturan di panel navigasi kiri.
3. Pada halaman Pengaturan, cari kotak Informasi penyediaan otomatis, lalu pilih Aktifkan. Ini segera memungkinkan penyediaan otomatis di IAM Identity Center dan menampilkan titik akhir SCIM dan informasi token akses yang diperlukan.
4. Dalam kotak dialog Penyediaan otomatis masuk, salin setiap nilai untuk opsi berikut. Anda harus menempelkannya nanti saat mengonfigurasi penyediaan di iDP Anda.
   a. Titik akhir SCIM
   b. Token akses
5. Pilih Tutup.

Setelah Anda menyelesaikan prosedur ini, Anda harus mengonfigurasi penyediaan otomatis di IDP Anda. Untuk informasi selengkapnya, lihat Memulai tutorial untuk IDP Anda.

Cara menonaktifkan penyediaan otomatis

Gunakan prosedur berikut untuk menonaktifkan penyediaan otomatis di konsol Pusat Identitas IAM.

> **Important**
>
> Anda harus menghapus token akses sebelum memulai prosedur ini. Untuk informasi selengkapnya, lihat Cara menghapus token akses.

Untuk menonaktifkan penyediaan otomatis di konsol Pusat Identitas IAM

1. Di konsol Pusat Identitas IAM, pilih Pengaturan di panel navigasi kiri.
2. Pada halaman Pengaturan, pilih tab Sumber identitas, lalu pilih Tindakan > Kelola penyediaan.
3. Pada halaman Penyediaan otomatis, pilih Nonaktifkan.
4. Di kotak dialog Nonaktifkan penyediaan otomatis, tinjau informasi, ketik DISABLE, lalu pilih Nonaktifkan penyediaan otomatis.

Cara menghasilkan token akses baru

Gunakan prosedur berikut untuk menghasilkan token akses baru di konsol Pusat Identitas IAM.

> **Note**
>
> Prosedur ini mengharuskan Anda sebelumnya mengaktifkan penyediaan otomatis. Untuk informasi selengkapnya, lihat Cara mengaktifkan penyediaan otomatis.

Untuk menghasilkan token akses baru

1. Di konsol Pusat Identitas IAM, pilih Pengaturan di panel navigasi kiri.
2. Pada halaman Pengaturan, pilih tab Sumber identitas, lalu pilih Tindakan > Kelola penyediaan.
3. Pada halaman Penyediaan otomatis, di bawah Token akses, pilih Hasilkan token.
4. Di kotak dialog Generate new access token, salin token akses baru dan simpan di tempat yang aman.
5. Pilih Tutup.

Cara menghapus token akses

Gunakan prosedur berikut untuk menghapus token akses yang ada di konsol Pusat Identitas IAM.

Untuk menghapus token akses yang ada

1. Di konsol Pusat Identitas IAM, pilih Pengaturan di panel navigasi kiri.
2. Pada halaman Pengaturan, pilih tab Sumber identitas, lalu pilih Tindakan > Kelola penyediaan.
3. Pada halaman Penyediaan otomatis, di bawah Token akses, pilih token akses yang ingin Anda hapus, lalu pilih Hapus.
4. Di kotak dialog Hapus akses token, tinjau informasi, ketik DELETE, lalu pilih Hapus token akses.

Cara memutar token akses

Direktori IAM Identity Center mendukung hingga dua token akses sekaligus. Untuk menghasilkan token akses tambahan sebelum rotasi apa pun, hapus token akses yang kedaluwarsa atau tidak terpakai.

Jika token akses SCIM Anda hampir kedaluwarsa, Anda dapat menggunakan prosedur berikut untuk memutar token akses yang ada di konsol Pusat Identitas IAM.

Untuk memutar token akses

1. Di konsol Pusat Identitas IAM, pilih Pengaturan di panel navigasi kiri.
2. Pada halaman Pengaturan, pilih tab Sumber identitas, lalu pilih Tindakan > Kelola penyediaan.
3. Pada halaman Penyediaan otomatis, di bawah Token akses, catat ID token token yang ingin Anda putar.
4. Ikuti langkah-langkah Cara menghasilkan token akses baru untuk membuat token baru. Jika Anda telah membuat jumlah maksimum token akses SCIM, Anda harus terlebih dahulu menghapus salah satu token yang ada.
5. Buka situs web penyedia identitas Anda dan konfigurasikan token akses baru untuk penyediaan SCIM, lalu uji konektivitas ke Pusat Identitas IAM menggunakan token akses SCIM baru. Setelah Anda mengonfirmasi bahwa penyediaan berhasil menggunakan token baru, lanjutkan ke langkah berikutnya dalam prosedur ini.
6. Ikuti langkah-langkah Cara menghapus token akses untuk menghapus token akses lama yang Anda catat sebelumnya. Anda juga dapat menggunakan tanggal pembuatan token sebagai petunjuk untuk token mana yang akan dihapus.

Penyediaan manual

Beberapa IdPs tidak memiliki dukungan System for Cross-domain Identity Management (SCIM) atau memiliki implementasi SCIM yang tidak kompatibel. Dalam kasus tersebut, Anda dapat menyediakan pengguna secara manual melalui konsol Pusat Identitas IAM. Saat Anda menambahkan pengguna ke IAM Identity Center, pastikan bahwa Anda menetapkan nama pengguna agar identik dengan nama pengguna yang Anda miliki di iDP Anda. Minimal, Anda harus memiliki alamat email dan nama pengguna yang unik. Untuk informasi selengkapnya, lihat Keunikan nama pengguna dan alamat email.

Anda juga harus mengelola semua grup secara manual di Pusat Identitas IAM. Untuk melakukan ini, Anda membuat grup dan menambahkannya menggunakan konsol Pusat Identitas IAM. Kelompok-kelompok ini tidak perlu mencocokkan apa yang ada di IDP Anda. Untuk informasi selengkapnya, lihat Grup.

Kelola sertifikat SAMP 2.0

IAM Identity Center menggunakan sertifikat untuk mengatur hubungan kepercayaan SAMP antara IAM Identity Center dan penyedia identitas eksternal (iDP) Anda. Ketika Anda menambahkan IDP eksternal di IAM Identity Center, Anda juga harus mendapatkan setidaknya satu sertifikat SAMP 2.0

X.509 publik dari iDP eksternal. Sertifikat itu biasanya diinstal secara otomatis selama pertukaran metadata IDP SAMP selama pembuatan kepercayaan.

Sebagai administrator Pusat Identitas IAM, Anda kadang-kadang perlu mengganti sertifikat iDP yang lebih lama dengan yang lebih baru. Misalnya, Anda mungkin perlu mengganti sertifikat IDP saat tanggal kedaluwarsa sertifikat mendekati. Proses penggantian sertifikat yang lebih lama dengan yang lebih baru disebut sebagai rotasi sertifikat.

Topik

Putar sertifikat SAMP 2.0

Anda mungkin perlu mengimpor sertifikat secara berkala untuk memutar sertifikat yang tidak valid atau kedaluwarsa yang dikeluarkan oleh penyedia identitas Anda. Ini membantu mencegah gangguan otentikasi atau downtime. Semua sertifikat yang diimpor aktif secara otomatis. Sertifikat hanya boleh dihapus setelah memastikan bahwa mereka tidak lagi digunakan dengan penyedia identitas terkait.

Anda juga harus mempertimbangkan bahwa beberapa IdPs mungkin tidak mendukung beberapa sertifikat. Dalam hal ini, tindakan memutar sertifikat dengan ini IdPs mungkin berarti gangguan layanan sementara bagi pengguna Anda. Layanan dipulihkan ketika kepercayaan dengan IDP tersebut telah berhasil dibangun kembali. Rencanakan operasi ini dengan hati-hati selama jam sibuk di luar jika memungkinkan.

> **Note**
>
> Sebagai praktik terbaik keamanan, jika ada tanda-tanda kompromi atau kesalahan penanganan sertifikat SAMP yang ada, Anda harus segera menghapus dan memutar sertifikat.

Memutar sertifikat IAM Identity Center adalah proses multistep yang melibatkan hal-hal berikut:

- Memperoleh sertifikat baru dari IDP
- Mengimpor sertifikat baru ke IAM Identity Center
- Mengaktifkan sertifikat baru di IDP

- Menghapus sertifikat yang lebih lama

Gunakan semua prosedur berikut untuk menyelesaikan proses rotasi sertifikat sambil menghindari downtime otentikasi.

Langkah 1: Dapatkan sertifikat baru dari IDP

Kunjungi situs web iDP dan unduh sertifikat SAMP 2.0 mereka. Pastikan file sertifikat diunduh dalam format yang dikodekan PEM. Sebagian besar penyedia memungkinkan Anda membuat beberapa sertifikat SAMP 2.0 di IDP. Kemungkinan ini akan ditandai sebagai dinonaktifkan atau tidak aktif.

Langkah 2: Impor sertifikat baru ke IAM Identity Center

Gunakan prosedur berikut untuk mengimpor sertifikat baru menggunakan konsol IAM Identity Center.

1. Di konsol Pusat Identitas IAM, pilih Pengaturan.
2. Pada halaman Pengaturan, pilih tab Sumber identitas, lalu pilih Tindakan > Kelola otentikasi.
3. Pada halaman Kelola sertifikat SAMP 2.0, pilih Impor sertifikat.
4. Pada dialog Impor sertifikat SAMP 2.0, pilih Pilih file, navigasikan ke file sertifikat Anda dan pilih, lalu pilih Impor sertifikat.

Pada titik ini, IAM Identity Center akan mempercayai semua pesan SAMP masuk yang ditandatangani dari kedua sertifikat yang telah Anda impor.

Langkah 3: Aktifkan sertifikat baru di IDP

Kembali ke situs web iDP dan tandai sertifikat baru yang Anda buat sebelumnya sebagai primer atau aktif. Pada titik ini semua pesan SAMP yang ditandatangani oleh iDP harus menggunakan sertifikat baru.

Langkah 4: Hapus sertifikat lama

Gunakan prosedur berikut untuk menyelesaikan proses rotasi sertifikat untuk IDP Anda. Harus selalu ada setidaknya satu sertifikat yang valid yang terdaftar, dan tidak dapat dihapus.

> **Note**
>
> Pastikan penyedia identitas Anda tidak lagi menandatangani tanggapan SAMP dengan sertifikat ini sebelum menghapusnya.

1. Pada halaman Kelola sertifikat SAMP 2.0, pilih sertifikat yang ingin Anda hapus. Pilih Hapus.
2. Dalam kotak dialog Hapus sertifikat SAMP 2.0, ketik **DELETE** untuk mengonfirmasi, lalu pilih Hapus.
3. Kembali ke situs web IDP dan lakukan langkah-langkah yang diperlukan untuk menghapus sertifikat tidak aktif yang lebih lama.

Indikator status kedaluwarsa sertifikat

Saat berada di halaman Kelola sertifikat SAMP 2.0, Anda mungkin melihat ikon indikator status berwarna. Ikon ini muncul di kolom Kedaluwarsa di samping setiap sertifikat dalam daftar. Berikut ini menjelaskan kriteria yang digunakan IAM Identity Center untuk menentukan ikon mana yang ditampilkan untuk setiap sertifikat.

- Merah - Menunjukkan bahwa sertifikat saat ini kedaluwarsa.
- Kuning - Menunjukkan bahwa sertifikat akan kedaluwarsa dalam 90 hari atau kurang.
- Hijau - Menunjukkan bahwa sertifikat saat ini valid dan akan tetap berlaku setidaknya selama 90 hari lagi.

Untuk memeriksa status sertifikat saat ini

1. Di konsol Pusat Identitas IAM, pilih Pengaturan.
2. Pada halaman Pengaturan, pilih tab Sumber identitas, lalu pilih Tindakan > Kelola otentikasi.
3. Pada halaman Kelola otentikasi SAMP 2.0, di bawah Kelola sertifikat SAMP 2.0, tinjau status sertifikat dalam daftar seperti yang ditunjukkan dalam kolom Kedaluwarsa pada.

Menggunakan portal AWS akses

Portal AWS akses memberi Anda (pengguna akhir) akses masuk tunggal ke semua aplikasi cloud Anda Akun AWS dan yang paling umum digunakan seperti Office 365, Concur, Salesforce, dan banyak lagi. Anda dapat dengan cepat meluncurkan beberapa aplikasi hanya dengan memilih ikon Akun AWS atau aplikasi di portal. Kehadiran ikon aplikasi di portal AWS akses Anda berarti bahwa administrator dari perusahaan Anda telah memberi Anda akses ke aplikasi Akun AWS atau aplikasi tersebut. Ini juga berarti bahwa Anda dapat mengakses semua akun atau aplikasi ini dari portal AWS akses tanpa petunjuk masuk tambahan.

Hubungi administrator Anda untuk meminta akses tambahan dalam situasi berikut:

- Anda tidak melihat aplikasi Akun AWS atau aplikasi yang perlu Anda akses.
- Akses yang Anda miliki ke akun atau aplikasi tertentu tidak seperti yang Anda harapkan.

Topik

Menerima undangan untuk bergabung dengan IAM Identity Center

Jika ini adalah pertama kalinya Anda masuk ke portal AWS akses, periksa email Anda untuk petunjuk tentang cara mengaktifkan kredensi pengguna Anda.

Untuk mengaktifkan kredensi pengguna Anda

1. Bergantung pada email yang Anda terima dari perusahaan Anda, pilih salah satu metode berikut untuk mengaktifkan kredensi pengguna Anda sehingga Anda dapat mulai menggunakan portal AWS akses.

   a. Jika Anda menerima email dengan subjek Undangan untuk bergabung dengan AWS IAM Identity Center (penerus AWS Single Sign-On), buka dan pilih Terima undangan. Pada halaman pendaftaran pengguna baru, masukkan dan konfirmasikan kata sandi, lalu pilih Tetapkan kata sandi baru. Anda akan menggunakan kata sandi itu setiap kali Anda masuk ke portal.

   b. Jika Anda dikirimi email dari dukungan TI atau administrator TI perusahaan Anda, ikuti instruksi yang mereka berikan untuk mengaktifkan kredensi pengguna Anda.

2. Setelah Anda mengaktifkan kredensi pengguna Anda dengan memberikan kata sandi baru, portal AWS akses akan menandatangani Anda secara otomatis. Jika ini tidak terjadi, Anda dapat masuk secara manual ke portal AWS akses dengan menggunakan instruksi yang disediakan di bagian berikutnya.

Masuk ke portal AWS akses

Pada saat ini, Anda seharusnya telah diberikan URL masuk khusus ke portal AWS akses oleh administrator. Setelah Anda memiliki URL ini, Anda dapat melanjutkan dengan masuk ke portal. Untuk informasi selengkapnya, lihat Masuk ke portal AWS akses.

> **Note**
>
> Setelah Anda masuk, durasi default untuk sesi portal AWS akses Anda adalah 8 jam. Ketahuilah bahwa administrator dapat mengubah durasi sesi ini.

Perangkat tepercaya

Bila Anda memilih opsi Ini adalah perangkat tepercaya dari halaman login, IAM Identity Center menganggap semua login di masa mendatang dari perangkat tersebut sebagai otorisasi. Ini berarti Pusat Identitas IAM tidak akan menyajikan opsi untuk memasukkan kode MFA selama Anda menggunakan perangkat tepercaya itu. Namun, ada beberapa pengecualian, termasuk masuk dari browser baru atau ketika perangkat Anda telah mengeluarkan alamat IP yang tidak dikenal.

Kiat masuk untuk portal AWS akses

Berikut adalah beberapa tips untuk membantu Anda mengelola pengalaman portal AWS akses Anda.

- Terkadang, Anda mungkin perlu keluar dan masuk kembali ke portal AWS akses. Ini mungkin diperlukan untuk mengakses aplikasi baru yang baru-baru ini ditetapkan administrator Anda kepada Anda. Ini tidak diperlukan, bagaimanapun, karena semua aplikasi baru disegarkan setiap jam.
- Saat Anda masuk ke portal AWS akses, Anda dapat membuka salah satu aplikasi yang tercantum di portal dengan memilih ikon aplikasi. Setelah Anda selesai menggunakan aplikasi, Anda dapat menutup aplikasi atau keluar dari portal AWS akses. Menutup aplikasi akan membuat Anda keluar dari aplikasi itu saja. Aplikasi lain yang telah Anda buka dari portal AWS akses tetap terbuka dan berjalan.
- Sebelum Anda dapat masuk sebagai pengguna lain, Anda harus terlebih dahulu keluar dari portal AWS akses. Keluar dari portal sepenuhnya menghapus kredensional Anda dari sesi browser.
- Setelah masuk ke portal AWS akses, Anda dapat beralih ke peran. Beralih peran untuk sementara mengesampingkan izin pengguna asli Anda dan sebagai gantinya memberi Anda izin yang ditetapkan untuk peran tersebut. Untuk informasi selengkapnya, lihat Beralih ke peran (konsol).

Keluar dari portal AWS akses

Ketika Anda keluar dari portal, kredensional Anda sepenuhnya dihapus dari sesi browser. Untuk informasi selengkapnya, lihat Keluar dari portal AWS akses di AWS Sign-Inpanduan.

Untuk keluar dari portal AWS akses

- Di portal AWS akses, pilih Keluar dari bilah navigasi.

> **Note**
>
> Jika Anda ingin masuk sebagai pengguna lain, Anda harus terlebih dahulu keluar dari portal AWS akses.

Menyetel ulang kata sandi pengguna IAM Identity Center

Portal AWS akses memberi pengguna IAM Identity Center akses masuk tunggal ke semua AWS akun dan aplikasi cloud yang ditugaskan melalui portal web. Portal AWS akses berbeda dari AWS Management Console, yang merupakan kumpulan konsol layanan untuk mengelola AWS sumber daya.

Gunakan prosedur ini untuk mengatur ulang kata sandi pengguna IAM Identity Center Anda untuk portal AWS akses. Pelajari lebih lanjut tentang jenis Pengguna di Panduan AWS Sign-In Pengguna.

Pertimbangan

Fungsi reset kata sandi Anda untuk portal AWS akses Anda hanya tersedia untuk pengguna instans Pusat Identitas yang menggunakan direktori Pusat Identitas atau AWS Managed Microsoft ADsebagai sumber identitas mereka. Jika pengguna Anda terhubung ke penyedia identitas eksternal, pengaturan ulang kata sandi pengguna harus dilakukan dari penyedia identitas eksternal.

- Jika sumber identitas Anda adalah direktori Pusat Identitas IAM, lihatPersyaratan kata sandi saat mengelola identitas di IAM Identity Center.
- Jika sumber identitas Anda adalah AWS Managed Microsoft AD, lihat Persyaratan kata sandi saat mengatur ulang kata sandi. AWS Managed Microsoft AD

Untuk mengatur ulang kata sandi Anda ke portal AWS akses

1. Buka browser web dan buka halaman masuk untuk portal AWS akses Anda.

   Jika Anda tidak memiliki URL portal AWS akses Anda, periksa email Anda. Anda seharusnya telah dikirimi email undangan untuk bergabung dengan AWS IAM Identity Center yang menyertakan URL masuk tertentu ke portal akses. AWS Atau, administrator Anda mungkin secara langsung memberi Anda kata sandi satu kali dan URL portal AWS akses. Jika Anda tidak dapat menemukan informasi ini, minta administrator Anda untuk mengirimkannya kepada Anda.

   Untuk informasi selengkapnya tentang masuk ke portal AWS akses, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.
2. Masukkan Nama Pengguna Anda, lalu pilih Berikutnya.
3. Di bawah Kata Sandi, pilih Lupa kata sandi.

   Verifikasi Nama Pengguna Anda dan masukkan karakter untuk gambar yang disediakan untuk mengonfirmasi bahwa Anda bukan robot. Lalu pilih Selanjutnya. Anda mungkin perlu menonaktifkan perangkat lunak pemblokir iklan jika Anda tidak dapat memasukkan karakter.
4. Sebuah pesan muncul untuk mengonfirmasi bahwa email setel ulang kata sandi telah dikirim. Pilih Lanjutkan.
5. Anda akan menerima email dari `no-reply@signin.aws` subjek Reset kata sandi yang diminta. Di email Anda, pilih Setel ulang kata sandi.
6. Pada halaman Reset kata sandi, verifikasi Nama Pengguna Anda, tentukan kata sandi baru untuk portal AWS akses, lalu pilih Tetapkan kata sandi baru.
7. Anda akan menerima email dari `no-reply@signin.aws` baris subjek Kata sandi diperbarui.

> **Note**
>
> Administrator dapat mengatur ulang kata sandi Anda dengan mengirim email kepada Anda dengan instruksi untuk mengatur ulang kata sandi Anda atau membuat kata sandi satu kali dan membagikannya kepada Anda. Jika Anda seorang administrator, lihatSetel ulang kata sandi pengguna IAM Identity Center untuk pengguna akhir.

Mendapatkan kredensi pengguna IAM Identity Center untuk atau SDK AWS CLIAWS

Anda dapat mengakses AWS layanan secara terprogram dengan menggunakan AWS Command Line Interface atau AWS Software Development Kit (SDK) dengan kredensi pengguna dari IAM Identity Center. Topik ini menjelaskan cara mendapatkan kredensi sementara untuk pengguna di Pusat Identitas IAM.

Portal AWS akses menyediakan pengguna IAM Identity Center dengan akses masuk tunggal ke aplikasi mereka Akun AWS dan cloud. Setelah Anda masuk ke portal AWS akses sebagai pengguna Pusat Identitas IAM, Anda bisa mendapatkan kredensi sementara. Anda kemudian dapat menggunakan kredensialnya, juga disebut sebagai kredensial pengguna IAM Identity Center, di AWS CLI atau AWS SDK untuk mengakses sumber daya dalam file. Akun AWS

Jika Anda menggunakan AWS CLI untuk mengakses AWS layanan secara terprogram, Anda dapat menggunakan prosedur dalam topik ini untuk memulai akses ke. AWS CLI Untuk informasi tentang AWS CLI, lihat Panduan AWS Command Line Interface Pengguna.

Jika Anda menggunakan AWS SDK untuk mengakses AWS layanan secara terprogram, mengikuti prosedur dalam topik ini juga secara langsung menetapkan otentikasi untuk SDK. AWS Untuk informasi tentang AWS SDK, lihat Panduan Referensi AWS SDK dan Alat.

> **Note**
>
> Pengguna di IAM Identity Center berbeda dari pengguna IAM. Pengguna IAM diberikan kredensi jangka panjang untuk sumber daya. AWS Pengguna di Pusat Identitas IAM diberikan kredensitas sementara. Kami menyarankan Anda menggunakan kredensi sementara sebagai praktik terbaik keamanan untuk mengakses Anda Akun AWS karena kredensi ini dihasilkan setiap kali Anda masuk.

Prasyarat

Untuk mendapatkan kredensi sementara bagi pengguna Pusat Identitas IAM Anda, Anda memerlukan yang berikut ini:

- Pengguna Pusat Identitas IAM — Anda akan masuk ke portal AWS akses sebagai pengguna ini. Anda atau administrator Anda dapat membuat pengguna ini. Untuk informasi tentang cara

mengaktifkan Pusat Identitas IAM dan membuat pengguna Pusat Identitas IAM, lihat. Memulai tugas-tugas umum di IAM Identity Center

- Akses pengguna ke Akun AWS - Untuk memberikan izin pengguna IAM Identity Center untuk mengambil kredensialnya sementara, Anda atau administrator harus menetapkan pengguna Pusat Identitas IAM ke set izin. Set izin disimpan di Pusat Identitas IAM dan menentukan tingkat akses yang dimiliki pengguna Pusat Identitas IAM ke. Akun AWS Jika administrator Anda membuat pengguna IAM Identity Center untuk Anda, minta mereka untuk menambahkan akses ini untuk Anda. Untuk informasi selengkapnya, lihat Tetapkan akses pengguna ke Akun AWS.
- AWS CLI diinstal — Untuk menggunakan kredensi sementara, Anda harus menginstal file. AWS CLI Untuk petunjuk, lihat Menginstal atau memperbarui versi terbaru AWS CLI dari Panduan AWS CLI Pengguna.

Pertimbangan

Sebelum Anda menyelesaikan langkah-langkah untuk mendapatkan kredensi sementara untuk pengguna Pusat Identitas IAM Anda, ingatlah pertimbangan berikut:

- Pusat Identitas IAM membuat peran IAM — Saat Anda menetapkan pengguna di Pusat Identitas IAM ke set izin, Pusat Identitas IAM membuat peran IAM yang sesuai dari kumpulan izin. Peran IAM yang dibuat oleh set izin berbeda dari peran IAM yang dibuat dengan AWS Identity and Access Management cara berikut:
  - IAM Identity Center memiliki dan mengamankan peran yang dibuat oleh set izin. Hanya Pusat Identitas IAM yang dapat memodifikasi peran ini.
  - Hanya pengguna di Pusat Identitas IAM yang dapat mengambil peran yang sesuai dengan set izin yang ditetapkan. Anda tidak dapat menetapkan akses setel izin ke pengguna IAM, pengguna federasi IAM, atau akun layanan.
  - Anda tidak dapat mengubah kebijakan kepercayaan peran pada peran ini untuk mengizinkan akses ke kepala sekolah di luar Pusat Identitas IAM.

  Untuk informasi tentang cara mendapatkan kredensi sementara untuk peran yang Anda buat di IAM, lihat Menggunakan kredenal keamanan sementara dengan di AWS CLI Panduan Pengguna.AWS Identity and Access Management
- Anda dapat mengatur durasi sesi untuk set izin — Setelah Anda masuk ke portal AWS akses, izin yang disetel ke mana pengguna Pusat Identitas IAM Anda ditetapkan akan muncul sebagai peran yang tersedia. IAM Identity Center membuat sesi terpisah untuk peran ini. Sesi ini bisa dari satu

hingga 12 jam, tergantung durasi sesi yang dikonfigurasi untuk set izin. Durasi sesi default adalah satu jam. Untuk informasi selengkapnya, lihat Tetapkan durasi sesi.

Mendapatkan dan menyegarkan kredensi sementara

Anda bisa mendapatkan dan menyegarkan kredensi sementara untuk pengguna Pusat Identitas IAM Anda secara otomatis atau manual.

Topik

- Penyegaran kredenal otomatis (disarankan)
- Penyegaran kredenal manual

Penyegaran kredenal otomatis (disarankan)

Penyegaran kredenal otomatis menggunakan standar Otorisasi Kode Perangkat Open ID Connect (OIDC). Dengan metode ini, Anda memulai akses langsung dengan menggunakan `aws configure sso` perintah di. AWS CLI Anda dapat menggunakan perintah ini untuk secara otomatis mengakses peran apa pun yang terkait dengan kumpulan izin apa pun yang Anda tetapkan untuk peran apa pun Akun AWS.

Untuk mengakses peran yang dibuat untuk pengguna IAM Identity Center Anda, jalankan `aws configure sso` perintah, lalu otorisasi AWS CLI dari jendela browser. Selama Anda memiliki sesi portal AWS akses aktif, AWS CLI secara otomatis mengambil kredensi sementara dan menyegarkan kredensialnya secara otomatis.

Untuk informasi selengkapnya, lihat Mengkonfigurasi profil Anda dengan `aws configure sso wizard` di Panduan AWS Command Line Interface Pengguna.

Untuk mendapatkan kredensi sementara yang secara otomatis menyegarkan

1. Masuk ke portal AWS akses menggunakan URL masuk khusus yang disediakan oleh administrator Anda. Jika Anda membuat pengguna Pusat Identitas IAM, AWS kirimkan undangan email yang menyertakan URL masuk Anda. Untuk informasi selengkapnya, lihat Masuk ke portal AWS akses di Panduan Pengguna AWS Masuk.
2. Di tab Akun atau dengan memilih Akun AWS ikon, cari Akun AWS dari mana Anda ingin mengambil kredensialnya. Saat Anda memilih akun, nama akun, ID akun, dan alamat email yang terkait dengan akun akan muncul.

> **Note**
>
> Jika Anda tidak melihat Akun AWSdaftar apa pun, kemungkinan Anda belum ditetapkan ke izin yang ditetapkan untuk akun tersebut. Dalam hal ini, hubungi administrator Anda dan minta mereka menambahkan akses ini untuk Anda. Untuk informasi selengkapnya, lihat Tetapkan akses pengguna ke Akun AWS.

3. Di bawah nama akun, izin yang disetel ke mana pengguna Pusat Identitas IAM Anda ditetapkan muncul sebagai peran yang tersedia. Misalnya, jika pengguna Pusat Identitas IAM Anda ditetapkan ke set PowerUserAccessizin untuk akun, peran akan muncul di portal AWS akses sebagai PowerUserAccess.
4. Bergantung pada opsi Anda di sebelah nama peran, pilih tombol Akses atau pilih Baris perintah atau akses terprogram.
5. Di kotak dialog Dapatkan kredensi, pilih macOS dan Linux, Windows, atau PowerShell, tergantung pada sistem operasi tempat Anda menginstal file. AWS CLI
6. Di bawah kredensi AWS IAM Identity Center (Direkomendasikan), Anda `SSO Start URL` dan `SSO Region` ditampilkan. Nilai-nilai ini diperlukan untuk mengonfigurasi profil yang diaktifkan Pusat Identitas IAM dan `sso-session` profil Anda AWS CLI. Untuk menyelesaikan konfigurasi ini, ikuti petunjuk di Konfigurasikan profil Anda dengan `aws configure sso wizard` di Panduan AWS Command Line Interface Pengguna.

Lanjutkan menggunakan AWS CLI yang diperlukan untuk Anda Akun AWS sampai kredensialnya kedaluwarsa.

Penyegaran kredenal manual

Anda dapat menggunakan metode penyegaran kredenal manual untuk mendapatkan kredenal sementara untuk peran yang dikaitkan dengan izin tertentu yang ditetapkan dalam peran tertentu. Akun AWS Untuk melakukannya, Anda menyalin dan menempelkan perintah yang diperlukan untuk kredensi sementara. Dengan metode ini, Anda harus menyegarkan kredensi sementara secara manual.

Anda dapat menjalankan AWS CLI perintah hingga kredensi sementara Anda kedaluwarsa.

Untuk mendapatkan kredensional yang Anda refresh secara manual

1. Masuk ke portal AWS akses menggunakan URL masuk khusus yang disediakan oleh administrator Anda. Jika Anda membuat pengguna Pusat Identitas IAM, AWS kirimkan undangan email yang menyertakan URL masuk Anda. Untuk informasi selengkapnya, lihat Masuk ke portal AWS akses di Panduan Pengguna AWS Masuk.
2. Di tab Accounts atau dengan memilih Akun AWS ikon, cari Akun AWS dari mana Anda ingin mengambil kredensi akses dan memperluas untuk menampilkan nama peran IAM (misalnya Administrator). Bergantung pada opsi Anda di sebelah nama peran IAM, pilih tombol Akses atau pilih Baris perintah atau akses terprogram.

   > **Note**
   >
   > Jika Anda tidak melihat Akun AWSdaftar apa pun, kemungkinan Anda belum ditetapkan ke izin yang ditetapkan untuk akun tersebut. Dalam hal ini, hubungi administrator Anda dan minta mereka menambahkan akses ini untuk Anda. Untuk informasi selengkapnya, lihat Tetapkan akses pengguna ke Akun AWS.

3. Di kotak dialog Dapatkan kredensi, pilih macOS dan Linux, Windows, atau PowerShell, tergantung pada sistem operasi tempat Anda menginstal file. AWS CLI
4. Pilih salah satu opsi berikut:

   - Opsi 1: Mengatur variabel AWS lingkungan

     Pilih opsi ini untuk mengganti semua pengaturan kredensi, termasuk pengaturan apa pun dalam `credentials` file dan `config` file. Untuk informasi selengkapnya, lihat Variabel lingkungan untuk mengonfigurasi AWS CLI dalam Panduan AWS CLI Pengguna.

     Untuk menggunakan opsi ini, salin perintah ke clipboard Anda, tempel perintah ke jendela AWS CLI terminal Anda, lalu tekan Enter untuk mengatur variabel lingkungan yang diperlukan.

   - Opsi 2: Tambahkan profil ke file AWS kredensional Anda

     Pilih opsi ini untuk menjalankan perintah dengan kumpulan kredensional yang berbeda.

     Untuk menggunakan opsi ini, salin perintah ke clipboard Anda, lalu tempelkan perintah ke AWS `credentials` file bersama Anda untuk menyiapkan profil bernama baru. Untuk informasi selengkapnya, lihat File konfigurasi dan kredensial bersama di Panduan Referensi AWS SDK dan Alat. Untuk menggunakan kredensi ini, tentukan `--profile` opsi dalam AWS

CLI perintah Anda. Ini memengaruhi semua lingkungan yang menggunakan file kredensi yang sama.

- Opsi 3: Gunakan nilai individual di klien AWS layanan Anda

  Pilih opsi ini untuk mengakses AWS sumber daya dari klien AWS layanan. Untuk informasi selengkapnya, lihat Alat untuk Dibangun AWS.

  Untuk menggunakan opsi ini, salin nilai ke clipboard Anda, tempel nilai ke dalam kode Anda, dan tetapkan ke variabel yang sesuai untuk SDK Anda. Untuk informasi selengkapnya, lihat dokumentasi untuk SDK API spesifik Anda.

Mem-bookmark peran IAM

Untuk akses yang lebih cepat ke peran IAM yang sering digunakan dari portal AWS akses, Anda dapat membuat bookmark untuk peran tertentu yang terkait dengan peran tertentu. Akun AWS

Untuk menandai peran IAM untuk yang spesifik Akun AWS

1. Saat masuk ke portal AWS akses, di tab Akun atau dengan memilih Akun AWS ikon, cari bookmark yang ingin Akun AWS Anda tandai dan perluas untuk memilih nama peran IAM (misalnya Akses Administrator).
2. Bergantung pada opsi Anda, klik kanan nama peran IAM (misalnya Administrator) atau konsol Manajemen, salin alamat tautan, lalu gunakan URL tersebut untuk membuat bookmark Anda.

Mendaftarkan perangkat untuk MFA

Gunakan prosedur berikut dalam portal AWS akses untuk mendaftarkan perangkat baru Anda untuk otentikasi multi-faktor (MFA).

> **Note**
>
> Kami menyarankan Anda terlebih dahulu mengunduh aplikasi Authenticator yang sesuai ke perangkat Anda sebelum memulai langkah-langkah dalam prosedur ini. Untuk daftar aplikasi yang dapat Anda gunakan untuk perangkat MFA, lihat. Aplikasi otentikator virtual

Untuk mendaftarkan perangkat Anda untuk digunakan dengan MFA

1. Masuk ke portal AWS akses Anda. Untuk informasi selengkapnya, lihat Masuk ke portal AWS akses.
2. Di dekat kanan atas halaman, pilih perangkat MFA.
3. Pada halaman perangkat otentikasi multi-faktor (MFA), pilih Daftarkan perangkat.

> **Note**
>
> Jika opsi Daftarkan perangkat MFA berwarna abu-abu, hubungi administrator Anda untuk bantuan mendaftarkan perangkat Anda.

4. Pada halaman Daftarkan perangkat MFA, pilih salah satu jenis perangkat MFA berikut, dan ikuti petunjuknya:

   - Aplikasi Authenticator
     1. Pada halaman Mengatur aplikasi autentikator, Anda mungkin melihat informasi konfigurasi untuk perangkat MFA baru, termasuk grafik kode QR. Grafik adalah representasi dari kunci rahasia yang tersedia untuk entri manual pada perangkat yang tidak mendukung kode QR.
     2. Menggunakan perangkat MFA fisik, lakukan hal berikut:
        a. Buka aplikasi autentikator MFA yang kompatibel. Untuk daftar aplikasi teruji yang dapat Anda gunakan dengan perangkat MFA, lihat. Aplikasi otentikator virtual Jika aplikasi MFA mendukung beberapa akun (beberapa perangkat MFA), pilih opsi untuk membuat akun baru (perangkat MFA baru).
        b. Tentukan apakah aplikasi MFA mendukung kode QR, lalu lakukan salah satu hal berikut di halaman Siapkan aplikasi autentikator:
           i. Pilih Tampilkan kode QR, lalu gunakan aplikasi untuk memindai kode QR. Misalnya, Anda dapat memilih ikon kamera atau memilih opsi yang mirip dengan kode Pindai. Kemudian gunakan kamera perangkat untuk memindai kode.
           ii. Pilih tampilkan kunci rahasia, lalu masukkan kunci rahasia itu ke aplikasi MFA Anda.

> **Important**
>
> Saat Anda mengonfigurasi perangkat MFA untuk IAM Identity Center, kami sarankan Anda menyimpan salinan kode QR atau kunci rahasia di tempat yang aman. Ini dapat membantu jika Anda kehilangan ponsel atau harus

menginstal ulang aplikasi otentikator MFA. Jika salah satu dari hal-hal itu terjadi, Anda dapat dengan cepat mengkonfigurasi ulang aplikasi untuk menggunakan konfigurasi MFA yang sama.

3. Pada halaman Siapkan aplikasi autentikator, di bawah kode Authenticator, masukkan kata sandi satu kali yang saat ini muncul di perangkat MFA fisik.

> **Important**
>
> Kirim permintaan Anda segera setelah membuat kode. Jika Anda membuat kode dan kemudian menunggu terlalu lama untuk mengirimkan permintaan, perangkat MFA berhasil dikaitkan dengan pengguna Anda, tetapi perangkat MFA tidak sinkron. Hal ini terjadi karena kata sandi sekali pakai berbasis waktu (TOTP) kedaluwarsa setelah periode waktu yang singkat. Jika ini terjadi, Anda dapat menyinkronkan perangkat lagi.

4. Pilih Tugaskan MFA. Perangkat MFA sekarang dapat mulai menghasilkan kata sandi satu kali dan sekarang siap digunakan. AWS

- Kunci keamanan atau Autentikator bawaan

1. Pada halaman Daftarkan kunci keamanan pengguna Anda, ikuti petunjuk yang diberikan oleh browser atau platform Anda.

> **Note**
>
> Pengalaman akan bervariasi berdasarkan browser atau platform. Setelah perangkat berhasil didaftarkan, Anda dapat mengaitkan nama tampilan yang ramah dengan perangkat yang baru terdaftar. Untuk mengubah nama, pilih Ganti nama, masukkan nama baru, lalu pilih Simpan.

Menyesuaikan URL portal AWS akses

Secara default, Anda dapat mengakses portal AWS akses dengan menggunakan URL yang mengikuti format ini:`d-xxxxxxxxxx.awsapps.com/start`. Anda dapat menyesuaikan URL sebagai berikut:`your_subdomain.awsapps.com/start`.

> **Important**
>
> Jika Anda mengubah URL portal AWS akses, Anda tidak dapat mengeditnya nanti.

Untuk menyesuaikan URL Anda

1. Buka AWS IAM Identity Center konsol di https://console.aws.amazon.com/singlesignon/.
2. Di konsol Pusat Identitas IAM, pilih Dasbor di panel navigasi dan temukan bagian Ringkasan pengaturan.
3. Pilih tombol Sesuaikan di bawah tautan ke URL portal AWS akses Anda.

   > **Note**
   >
   > Jika tombol Kustomisasi tidak ditampilkan, ini berarti portal AWS akses telah dimodifikasi di masa lalu. URL ini hanya dapat diubah satu kali.

4. Masukkan nama subdomain yang Anda inginkan dan pilih Simpan.

Sekarang Anda dapat masuk ke AWS Konsol melalui portal AWS akses dengan `awsapps.com/start` URL yang disesuaikan.

Otentikasi multi-faktor untuk pengguna Pusat Identitas

Otentikasi multi-faktor (MFA) menyediakan cara sederhana dan aman untuk menambahkan lapisan perlindungan tambahan di atas mekanisme otentikasi default nama pengguna dan kata sandi.

Ketika administrator mengaktifkan MFA, pengguna harus masuk ke AWS portal akses dengan dua faktor:

- Nama pengguna dan kata sandi mereka. Ini adalah faktor pertama dan merupakan sesuatu yang diketahui pengguna.
- Baik kode, kunci keamanan, atau biometrik. Ini adalah faktor kedua dan merupakan sesuatu yang dimiliki pengguna (kepemilikan) atau (biometrik). Faktor kedua mungkin berupa kode otentikasi yang dihasilkan dari perangkat seluler mereka, kunci keamanan yang terhubung ke komputer mereka, atau pemindaian biometrik pengguna.

Bersama-sama, beberapa faktor ini memberikan peningkatan keamanan dengan mencegah akses tidak sah ke AWS sumber daya Anda kecuali tantangan MFA yang valid telah berhasil diselesaikan.

Setiap pengguna dapat mendaftarkan hingga dua aplikasi otentikator virtual, yang merupakan aplikasi autentikator kata sandi satu kali yang diinstal pada perangkat seluler atau tablet Anda, dan enam otentikator FIDO, yang mencakup autentikator bawaan dan kunci keamanan, dengan total delapan perangkat MFA. Pelajari lebih lanjut tentang Tersedia tipe MFA untuk IAM Identity Center.

> **Important**
>
> Sebagai praktik terbaik keamanan, kami sangat menyarankan Anda mengaktifkan MFA.

Topik

- Tersedia tipe MFA untuk IAM Identity Center
- Konfigurasikan MFA
- Kelola perangkat MFA di Pusat Identitas IAM

Tersedia tipe MFA untuk IAM Identity Center

Otentikasi multi-faktor (MFA) adalah mekanisme sederhana dan efektif untuk meningkatkan keamanan pengguna Anda. Faktor pertama pengguna — kata sandi mereka — adalah rahasia yang mereka hafal, juga dikenal sebagai faktor pengetahuan. Faktor lain dapat berupa faktor kepemilikan (sesuatu yang Anda miliki, seperti kunci keamanan) atau faktor warisan (sesuatu yang Anda miliki, seperti pemindaian biometrik). Kami sangat menyarankan Anda mengonfigurasi MFA untuk menambahkan lapisan keamanan tambahan ke akun Anda.

IAM Identity Center MFA mendukung jenis perangkat berikut. Semua jenis MFA didukung untuk akses konsol berbasis browser serta menggunakan AWS CLI v2 dengan IAM Identity Center.

- Otentikator FIDO2, termasuk autentikator bawaan dan kunci keamanan
- Aplikasi otentikator virtual
- RADIUS MFAImplementasi Anda sendiri terhubung melalui AWS Managed Microsoft AD

Seorang pengguna dapat memiliki hingga delapan perangkat MFA, yang mencakup hingga dua aplikasi otentikator virtual dan enam otentikator FIDO, terdaftar ke satu akun. Anda juga dapat mengonfigurasi pengaturan pemberdayaan MFA untuk meminta MFA setiap kali pengguna Anda

masuk atau mengaktifkan perangkat tepercaya yang tidak memerlukan MFA pada setiap proses masuk. Untuk informasi selengkapnya tentang cara mengonfigurasi jenis MFA untuk pengguna Anda, lihat Pilih jenis MFA dan. Konfigurasikan penegakan perangkat MFA

Otentikator FIDO2

FIDO2 adalah standar yang mencakup CTAP2 dan WebAuthndan didasarkan pada kriptografi kunci publik. Kredensi FIDO tahan terhadap phishing karena unik untuk situs web tempat kredensialnya dibuat. AWS

AWSmendukung dua faktor bentuk yang paling umum untuk otentikator FIDO: autentikator bawaan dan kunci keamanan. Lihat di bawah untuk informasi selengkapnya tentang jenis autentikator FIDO yang paling umum.

Topik

- Autentikator bawaan
- Kunci keamanan
- Pengelola kata sandi, penyedia kunci sandi, dan autentikator FIDO lainnya

Autentikator bawaan

Banyak komputer dan ponsel modern memiliki autentikator bawaan, seperti TouchID di Macbook atau kamera yang kompatibel dengan Windows Hello. Jika perangkat Anda memiliki autentikator bawaan yang kompatibel dengan FIDO, Anda dapat menggunakan sidik jari, wajah, atau pin perangkat sebagai faktor kedua.

Kunci keamanan

Kunci keamanan adalah otentikator perangkat keras eksternal yang kompatibel dengan FIDO yang dapat Anda beli dan sambungkan ke perangkat Anda melalui USB, BLE, atau NFC. Ketika Anda diminta untuk MFA, Anda cukup menyelesaikan gerakan dengan sensor tombol. Beberapa contoh kunci keamanan termasuk YubiKeys dan kunci Feitian, dan kunci keamanan yang paling umum membuat kredenal FIDO terikat perangkat. Untuk daftar semua kunci keamanan bersertifikat FIDO, lihat Produk Bersertifikat FIDO.

Pengelola kata sandi, penyedia kunci sandi, dan autentikator FIDO lainnya

Beberapa penyedia pihak ketiga mendukung otentikasi FIDO dalam aplikasi seluler, sebagai fitur dalam pengelola kata sandi, kartu pintar dengan mode FIDO, dan faktor bentuk lainnya.

Perangkat yang kompatibel dengan FIDO ini dapat bekerja dengan IAM Identity Center, tetapi kami menyarankan Anda menguji autentikator FIDO sendiri sebelum mengaktifkan opsi ini untuk MFA.

> **Note**
>
> Beberapa autentikator FIDO dapat membuat kredensil FIDO yang dapat ditemukan yang dikenal sebagai kunci sandi. Passkey mungkin terikat ke perangkat yang membuatnya, atau mereka dapat disinkronkan dan dicadangkan ke cloud. Misalnya, Anda dapat mendaftarkan kunci sandi menggunakan Apple Touch ID di Macbook yang didukung, lalu masuk ke situs dari laptop Windows menggunakan Google Chrome dengan kunci sandi Anda di iCloud dengan mengikuti petunjuk di layar saat masuk. Untuk informasi selengkapnya tentang perangkat mana yang mendukung kunci sandi yang dapat disinkronkan dan interoperabilitas kunci sandi saat ini antara sistem operasi dan browser, lihat Dukungan Perangkat di passkeys.dev, sumber daya yang dikelola oleh FIDO Alliance And World Wide Web Consortium (W3C).

Aplikasi otentikator virtual

Aplikasi Authenticator pada dasarnya adalah one-time password (OTP) — based third party authenticator. Anda dapat menggunakan aplikasi autentikator yang diinstal pada perangkat seluler atau tablet Anda sebagai perangkat MFA resmi. Aplikasi autentikator pihak ketiga harus sesuai dengan RFC 6238, yang merupakan algoritma kata sandi satu kali berbasis waktu (TOTP) berbasis waktu berbasis standar yang mampu menghasilkan kode otentikasi enam digit.

Saat diminta untuk MFA, pengguna harus memasukkan kode yang valid dari aplikasi autentikator mereka di dalam kotak input yang disajikan. Setiap perangkat MFA yang ditetapkan ke pengguna harus unik. Dua aplikasi autentikator dapat didaftarkan untuk setiap pengguna tertentu.

Aplikasi autentikator yang diuji

Setiap aplikasi yang sesuai dengan TOTP akan bekerja dengan IAM Identity Center MFA. Tabel berikut mencantumkan aplikasi autentikator pihak ketiga yang terkenal untuk dipilih.

Sistem operasi	Aplikasi autentikator yang diuji
Android	Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator

Sistem operasi	Aplikasi autentikator yang diuji
iOS	Authy, Duo Mobile, Microsoft Authenticator, Google Authenticator

RADIUS MFA

Remote Authentication Dial-In User Service (RADIUS) adalah protokol client-server standar industri yang menyediakan otentikasi, otorisasi, dan manajemen akuntansi sehingga pengguna dapat terhubung ke layanan jaringan. AWS Directory Servicetermasuk klien RADIUS yang terhubung ke server RADIUS tempat Anda menerapkan solusi MFA Anda. Untuk informasi selengkapnya, lihat Mengaktifkan Otentikasi Multi-Faktor untuk. AWS Managed Microsoft AD

Anda dapat menggunakan RADIUS MFA atau MFA di IAM Identity Center untuk login pengguna ke portal pengguna, tetapi tidak keduanya. MFA di IAM Identity Center adalah alternatif untuk RADIUS MFA dalam kasus di mana Anda ingin otentikasi dua faktor AWS asli untuk akses ke portal.

Saat Anda mengaktifkan MFA di Pusat Identitas IAM, pengguna Anda memerlukan perangkat MFA untuk masuk ke portal akses. AWS Jika sebelumnya Anda pernah menggunakan RADIUS MFA, mengaktifkan MFA di IAM Identity Center secara efektif mengesampingkan RADIUS MFA bagi pengguna yang masuk ke portal akses. AWS Namun, RADIUS MFA terus menantang pengguna ketika mereka masuk ke semua aplikasi lain yang berfungsiAWS Directory Service, seperti Amazon. WorkDocs

Jika MFA Anda Dinonaktifkan pada konsol Pusat Identitas IAM dan Anda telah mengonfigurasi RADIUS MFA dengan, AWS Directory Service RADIUS MFA mengatur akses masuk portal. AWS Ini berarti bahwa IAM Identity Center kembali ke konfigurasi RADIUS MFA jika MFA dinonaktifkan.

Konfigurasikan MFA

Topik berikut memberikan petunjuk untuk mengkonfigurasi perangkat MFA di IAM Identity Center.

Topik

- Pertimbangan sebelum mengaktifkan MFA di IAM Identity Center
- Aktifkan MFA di Pusat Identitas IAM
- Pilih jenis MFA
- Konfigurasikan penegakan perangkat MFA

- Memungkinkan pengguna untuk mendaftarkan perangkat MFA mereka sendiri

Pertimbangan sebelum mengaktifkan MFA di IAM Identity Center

Sebelum Anda mengaktifkan MFA, pertimbangkan hal berikut:

- Pengguna didorong untuk mendaftarkan beberapa otentikator cadangan untuk semua jenis MFA yang diaktifkan. Praktik ini dapat mencegah hilangnya akses jika perangkat MFA rusak atau salah tempat.
- Jangan memilih opsi Memerlukan Mereka untuk Memberikan Kata Sandi Satu Kali yang Dikirim oleh Email jika pengguna Anda harus masuk ke portal AWS akses untuk mengakses email mereka. Misalnya, pengguna Anda mungkin menggunakan Microsoft 365 portal AWS akses untuk membaca email mereka. Dalam hal ini, pengguna tidak akan dapat mengambil kode verifikasi dan tidak dapat masuk ke portal AWS akses. Untuk informasi selengkapnya, lihat Konfigurasikan penegakan perangkat MFA.
- Jika Anda sudah menggunakan RADIUS MFA yang Anda konfigurasi denganAWS Directory Service, Anda tidak perlu mengaktifkan MFA dalam IAM Identity Center. MFA di IAM Identity Center adalah alternatif untuk RADIUS MFA untuk Microsoft Active Directory pengguna IAM Identity Center. Untuk informasi selengkapnya, lihat RADIUS MFA.
- Anda dapat menggunakan kemampuan MFA di Pusat Identitas IAM ketika sumber identitas Anda dikonfigurasi dengan penyimpanan identitas IAM Identity Center, atau AWS Managed Microsoft AD AD Connector. MFA di Pusat Identitas IAM saat ini tidak didukung untuk penyedia identitas eksternal.

Aktifkan MFA di Pusat Identitas IAM

Anda dapat mengaktifkan akses aman ke portal AWS akses, aplikasi terintegrasi IAM Identity Center, dan AWS CLI dengan mengaktifkan otentikasi multi-faktor (MFA).

Topik

- Meminta pengguna untuk MFA
- Nonaktifkan MFA untuk direktori Pusat Identitas IAM Anda

Meminta pengguna untuk MFA

Gunakan langkah-langkah berikut untuk mengaktifkan MFA di konsol Pusat Identitas IAM. Sebelum Anda mulai, kami sarankan Anda memahamiTersedia tipe MFA untuk IAM Identity Center.

> **Note**
>
> Jika Anda menggunakan IDP eksternal, bagian otentikasi Multi-faktor tidak akan tersedia. IDP eksternal Anda mengelola pengaturan MFA, bukan Pusat Identitas IAM yang mengelolanya.

Untuk mengaktifkan MFA

1. Buka konsol Pusat Identitas IAM.
2. Pada panel navigasi kiri, pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Otentikasi.
4. Di bagian Otentikasi multi-faktor, pilih Konfigurasi.
5. Pada halaman Konfigurasi otentikasi multi-faktor, di bawah Pengguna Prompt untuk MFA, pilih salah satu mode otentikasi berikut berdasarkan tingkat keamanan yang dibutuhkan bisnis Anda:

   - Hanya ketika konteks masuk mereka berubah (sadar konteks)

     Dalam mode ini (default), IAM Identity Center memberi pengguna opsi untuk mempercayai perangkat mereka saat masuk. Setelah pengguna menunjukkan bahwa mereka ingin mempercayai perangkat, IAM Identity Center meminta pengguna untuk MFA sekali dan menganalisis konteks login (seperti perangkat, browser, dan lokasi) untuk login pengguna berikutnya. Untuk login berikutnya, IAM Identity Center menentukan apakah pengguna masuk dengan konteks tepercaya sebelumnya. Jika konteks login pengguna berubah, IAM Identity Center meminta pengguna untuk MFA selain alamat email dan kredensialnya.

     Mode ini memberikan kemudahan penggunaan bagi pengguna yang sering masuk dari tempat kerja mereka, sehingga mereka tidak perlu menyelesaikan MFA pada setiap login. Mereka hanya diminta untuk MFA jika konteks masuk mereka berubah.

   - Setiap kali mereka masuk (selalu aktif)

     Dalam mode ini, IAM Identity Center mengharuskan pengguna dengan perangkat MFA terdaftar akan diminta setiap kali mereka masuk. Anda harus menggunakan mode ini jika Anda memiliki kebijakan organisasi atau kepatuhan yang mengharuskan pengguna

Anda menyelesaikan MFA setiap kali mereka masuk ke portal AWS akses. Misalnya, PCI DSS sangat merekomendasikan MFA selama setiap login untuk mengakses aplikasi yang mendukung transaksi pembayaran berisiko tinggi.

- Tidak pernah (dinonaktifkan)

  Saat dalam mode ini, semua pengguna hanya akan masuk dengan nama pengguna dan kata sandi standar mereka. Memilih opsi ini menonaktifkan MFA Pusat Identitas IAM.

  > **Note**
  >
  > Jika Anda sudah menggunakan RADIUS MFA denganAWS Directory Service, dan ingin terus menggunakannya sebagai tipe MFA default Anda, maka Anda dapat membiarkan mode otentikasi dinonaktifkan untuk melewati kemampuan MFA di IAM Identity Center. Mengubah dari mode Dinonaktifkan ke mode Context-aware atau Always-on akan mengganti pengaturan MFA RADIUS yang ada. Untuk informasi selengkapnya, lihat RADIUS MFA.

6. Pilih Save changes (Simpan perubahan).

   Topik Terkait

   - Pilih jenis MFA
   - Konfigurasikan penegakan perangkat MFA
   - Memungkinkan pengguna untuk mendaftarkan perangkat MFA mereka sendiri

Nonaktifkan MFA untuk direktori Pusat Identitas IAM Anda

Saat Anda menonaktifkan otentikasi multi-faktor (MFA) untuk direktori Pusat Identitas IAM Anda, ini memungkinkan pengguna untuk masuk dengan nama pengguna dan kata sandi standar mereka saja. Meskipun MFA dinonaktifkan untuk direktori Pusat Identitas bagi pengguna, Anda tidak dapat mengelola perangkat MFA di detail pengguna mereka, dan pengguna direktori Pusat Identitas tidak dapat mengelola perangkat MFA dari portal akses. AWS

Untuk menonaktifkan MFA untuk direktori Pusat Identitas IAM Anda

> **Important**
>
> Instruksi di bagian ini berlaku untuk AWS IAM Identity Center. Mereka tidak berlaku untuk AWS Identity and Access Management(IAM). Pengguna, grup, dan kredenal pengguna IAM Identity Center berbeda dari pengguna IAM, grup, dan kredenal pengguna IAM. Jika Anda mencari petunjuk tentang menonaktifkan MFA untuk pengguna IAM, lihat Menonaktifkan perangkat MFA di Panduan Pengguna. AWS Identity and Access Management

1. Buka konsol Pusat Identitas IAM.
2. Pada panel navigasi kiri, pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Otentikasi.
4. Di bagian Otentikasi multi-faktor, pilih Konfigurasi.
5. Pada halaman Konfigurasi otentikasi multi-faktor, di bagian Prompt users for MFA, pilih tombol radio Never (disabled).
6. Pilih Simpan perubahan.

Pilih jenis MFA

Gunakan prosedur berikut untuk memilih jenis perangkat yang dapat diautentikasi oleh pengguna Anda saat diminta untuk MFA di portal akses. AWS

Untuk mengonfigurasi jenis MFA untuk pengguna Anda

1. Buka konsol Pusat Identitas IAM.
2. Pada panel navigasi kiri, pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Otentikasi.
4. Di bagian Otentikasi multi-faktor, pilih Konfigurasi.
5. Pada halaman Konfigurasi otentikasi multi-faktor, di bawah Pengguna dapat mengautentikasi dengan jenis MFA ini, pilih salah satu jenis MFA berikut berdasarkan kebutuhan bisnis Anda. Untuk informasi selengkapnya, lihat Tersedia tipe MFA untuk IAM Identity Center.
   - Otentikator FIDO2, termasuk autentikator bawaan dan kunci keamanan
   - Aplikasi otentikator virtual

6. Pilih Simpan perubahan.

Konfigurasikan penegakan perangkat MFA

Gunakan prosedur berikut untuk menentukan apakah pengguna Anda harus memiliki perangkat MFA terdaftar saat masuk ke portal AWS akses.

Untuk mengonfigurasi penegakan perangkat MFA untuk pengguna Anda

1. Buka konsol Pusat Identitas IAM.
2. Pada panel navigasi kiri, pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Otentikasi.
4. Di bagian Otentikasi multi-faktor, pilih Konfigurasi.
5. Pada halaman Konfigurasi autentikasi multi-faktor, di bawah Jika pengguna belum memiliki perangkat MFA terdaftar, pilih salah satu pilihan berikut berdasarkan kebutuhan bisnis Anda:

   - Minta mereka mendaftarkan perangkat MFA saat masuk

     Ini adalah pengaturan default ketika Anda pertama kali mengkonfigurasi MFA untuk IAM Identity Center. Gunakan opsi ini ketika Anda ingin meminta pengguna yang belum memiliki perangkat MFA terdaftar, untuk mendaftarkan sendiri perangkat saat masuk setelah otentikasi kata sandi berhasil. Ini memungkinkan Anda untuk mengamankan AWS lingkungan organisasi Anda dengan MFA tanpa harus mendaftarkan dan mendistribusikan perangkat otentikasi secara individual kepada pengguna Anda. Selama pendaftaran mandiri, pengguna dapat mendaftarkan perangkat apa pun dari perangkat yang tersedia yang telah Tersedia tipe MFA untuk IAM Identity Center Anda aktifkan sebelumnya. Setelah menyelesaikan pendaftaran, pengguna memiliki opsi untuk memberikan nama ramah pada perangkat MFA mereka yang baru terdaftar, setelah itu IAM Identity Center mengarahkan pengguna ke tujuan aslinya. Jika perangkat pengguna hilang atau dicuri, Anda cukup menghapus perangkat itu dari akun mereka, dan IAM Identity Center akan meminta mereka untuk mendaftarkan sendiri perangkat baru selama login berikutnya.

   - Minta mereka untuk memberikan kata sandi satu kali yang dikirim melalui email untuk masuk

     Gunakan opsi ini ketika Anda ingin memiliki kode verifikasi yang dikirim ke pengguna melalui email. Karena email tidak terikat ke perangkat tertentu, opsi ini tidak memenuhi standar untuk otentikasi multi-faktor standar industri. Tapi itu meningkatkan keamanan karena memiliki kata sandi saja. Verifikasi email hanya akan diminta jika pengguna belum mendaftarkan

perangkat MFA. Jika metode otentikasi Context-aware telah diaktifkan, pengguna akan memiliki kesempatan untuk menandai perangkat tempat mereka menerima email sebagai tepercaya. Setelah itu mereka tidak akan diminta untuk memverifikasi kode email pada login future dari perangkat, browser, dan kombinasi alamat IP tersebut.

> **Note**
>
> Jika Anda menggunakan Active Directory sebagai sumber identitas yang diaktifkan IAM Identity Center, alamat email akan selalu didasarkan pada `email` atribut Active Directory. Pemetaan atribut Custom Active Directory tidak akan mengesampingkan perilaku ini.

- Blokir login mereka

  Gunakan opsi Blokir Masuk Mereka saat Anda ingin menerapkan penggunaan MFA oleh setiap pengguna sebelum mereka dapat masuk. AWS

  > **Important**
  >
  > Jika metode autentikasi Anda disetel ke Context-aware, pengguna dapat memilih kotak centang Ini adalah perangkat tepercaya di halaman login. Dalam hal ini, pengguna tersebut tidak akan diminta untuk MFA bahkan jika Anda mengaktifkan pengaturan Blokir masuk mereka. Jika Anda ingin pengguna ini diminta, ubah metode otentikasi Anda menjadi Selalu Aktif.

- Izinkan mereka untuk masuk

  Gunakan opsi ini untuk menunjukkan bahwa perangkat MFA tidak diperlukan agar pengguna Anda masuk ke portal AWS akses. Pengguna yang memilih untuk mendaftarkan perangkat MFA masih akan diminta untuk MFA.

6. Pilih Simpan perubahan.

Memungkinkan pengguna untuk mendaftarkan perangkat MFA mereka sendiri

Gunakan prosedur berikut untuk memungkinkan pengguna Anda mendaftarkan sendiri perangkat MFA mereka sendiri.

Untuk memungkinkan pengguna mendaftarkan perangkat MFA mereka sendiri

1. Buka konsol Pusat Identitas IAM.
2. Pada panel navigasi kiri, pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Otentikasi.
4. Di bagian Otentikasi multi-faktor, pilih Konfigurasi.
5. Pada halaman Konfigurasi otentikasi multi-faktor, di bawah Siapa yang dapat mengelola perangkat MFA, pilih Pengguna dapat menambahkan dan mengelola perangkat MFA mereka sendiri.
6. Pilih Simpan perubahan.

> **Note**
>
> Setelah mengatur pendaftaran mandiri untuk pengguna, Anda mungkin ingin mengirimi mereka tautan ke prosedurMendaftarkan perangkat untuk MFA. Topik ini memberikan instruksi tentang cara mengatur perangkat MFA mereka sendiri.

Kelola perangkat MFA di Pusat Identitas IAM

Topik berikut memberikan instruksi untuk mengelola perangkat MFA di IAM Identity Center.

Topik

- Daftarkan perangkat MFA
- Mengelola perangkat MFA pengguna

Daftarkan perangkat MFA

Gunakan prosedur berikut untuk menyiapkan perangkat MFA baru untuk diakses oleh pengguna tertentu di konsol Pusat Identitas IAM. Anda harus memiliki akses fisik ke perangkat MFA pengguna untuk mendaftarkannya. Misalnya, jika Anda mengonfigurasi MFA untuk pengguna yang akan menggunakan perangkat MFA yang berjalan di ponsel cerdas, Anda memerlukan akses fisik ke ponsel cerdas untuk menyelesaikan proses pendaftaran. Atau, Anda dapat mengizinkan pengguna untuk mengonfigurasi dan mengelola perangkat MFA mereka sendiri. Untuk informasi selengkapnya, lihat Memungkinkan pengguna untuk mendaftarkan perangkat MFA mereka sendiri.

Untuk mendaftarkan perangkat MFA

1. Buka konsol Pusat Identitas IAM.
2. Pada panel navigasi kiri, pilih Pengguna. Pilih pengguna dalam daftar. Jangan pilih kotak centang di sebelah pengguna untuk langkah ini.
3. Pada halaman detail pengguna, pilih tab Perangkat MFA, lalu pilih Daftarkan perangkat MFA.
4. Pada halaman Daftarkan perangkat MFA, pilih salah satu jenis perangkat MFA berikut, dan ikuti petunjuknya:

   - Aplikasi Authenticator

     1. Pada halaman Siapkan aplikasi autentikator, Pusat Identitas IAM menampilkan informasi konfigurasi untuk perangkat MFA baru, termasuk grafik kode QR. Grafik adalah representasi dari kunci rahasia yang tersedia untuk entri manual pada perangkat yang tidak mendukung kode QR.
     2. Menggunakan perangkat MFA fisik, lakukan hal berikut:

        a. Buka aplikasi autentikator MFA yang kompatibel. Untuk daftar aplikasi teruji yang dapat Anda gunakan dengan perangkat MFA, lihat. Aplikasi otentikator virtual Jika aplikasi MFA mendukung beberapa akun (beberapa perangkat MFA), pilih opsi untuk membuat akun baru (perangkat MFA baru).

        b. Tentukan apakah aplikasi MFA mendukung kode QR, lalu lakukan salah satu hal berikut di halaman Siapkan aplikasi autentikator:

           i. Pilih Tampilkan kode QR, lalu gunakan aplikasi untuk memindai kode QR. Misalnya, Anda dapat memilih ikon kamera atau memilih opsi yang mirip dengan kode Pindai. Kemudian gunakan kamera perangkat untuk memindai kode.

           ii. Pilih tampilkan kunci rahasia, lalu ketik kunci rahasia itu ke dalam aplikasi MFA Anda.

> **Important**
>
> Saat Anda mengonfigurasi perangkat MFA untuk IAM Identity Center, kami sarankan Anda menyimpan salinan kode QR atau kunci rahasia di tempat yang aman. Ini dapat membantu jika pengguna yang ditugaskan kehilangan telepon atau harus menginstal ulang aplikasi autentikator MFA. Jika salah satu dari hal-hal itu terjadi, Anda dapat dengan cepat mengkonfigurasi ulang aplikasi untuk menggunakan konfigurasi MFA yang sama. Ini menghindari

kebutuhan untuk membuat perangkat MFA baru di IAM Identity Center untuk pengguna.

3. Pada halaman Siapkan aplikasi autentikator, di bawah kode Authenticator, ketikkan kata sandi satu kali yang saat ini muncul di perangkat MFA fisik.

> **Important**
>
> Kirim permintaan Anda segera setelah membuat kode. Jika Anda membuat kode dan kemudian menunggu terlalu lama untuk mengirimkan permintaan, perangkat MFA berhasil dikaitkan dengan pengguna. Tetapi perangkat MFA tidak sinkron. Hal ini terjadi karena kata sandi sekali pakai berbasis waktu (TOTP) kedaluwarsa setelah periode waktu yang singkat. Jika ini terjadi, Anda dapat menyinkronisasi ulang perangkat.

4. Pilih Tugaskan MFA. Perangkat MFA sekarang dapat mulai menghasilkan kata sandi satu kali dan sekarang siap digunakan. AWS

- Kunci keamanan

1. Pada halaman Daftarkan kunci keamanan pengguna Anda, ikuti instruksi yang diberikan kepada Anda oleh browser atau platform Anda.

> **Note**
>
> Pengalaman di sini bervariasi berdasarkan sistem operasi dan browser yang berbeda, jadi silakan ikuti instruksi yang ditampilkan oleh browser atau platform Anda. Setelah perangkat pengguna berhasil didaftarkan, Anda akan diberikan opsi untuk mengaitkan nama tampilan yang ramah ke perangkat pengguna yang baru terdaftar. Jika Anda ingin mengubah ini, pilih Ganti nama, masukkan nama baru, lalu pilih Simpan. Jika Anda telah mengaktifkan opsi untuk memungkinkan pengguna mengelola perangkat mereka sendiri, pengguna akan melihat nama ramah ini di portal AWS akses.

Mengelola perangkat MFA pengguna

Gunakan prosedur berikut saat Anda perlu mengganti nama atau menghapus perangkat MFA pengguna.

Untuk mengganti nama perangkat MFA

1. Buka konsol Pusat Identitas IAM.
2. Pada panel navigasi kiri, pilih Pengguna. Pilih pengguna dalam daftar. Jangan pilih kotak centang di sebelah pengguna untuk langkah ini.
3. Pada halaman detail pengguna, pilih tab Perangkat MFA, pilih perangkat, lalu pilih Ganti nama.
4. Saat diminta, masukkan nama baru lalu pilih Ganti nama.

Untuk menghapus perangkat MFA

1. Buka konsol Pusat Identitas IAM.
2. Pada panel navigasi kiri, pilih Pengguna. Pilih pengguna dalam daftar.
3. Pada halaman detail pengguna, pilih tab Perangkat MFA, pilih perangkat, lalu pilih Hapus.
4. Untuk mengonfirmasi, ketik DELETE, lalu pilih Hapus.

Kelola akses ke Akun AWS

AWS IAM Identity Center terintegrasi dengan AWS Organizations, yang memungkinkan Anda mengelola izin secara terpusat di beberapa Akun AWS tanpa mengonfigurasi setiap akun Anda secara manual. Anda dapat menentukan izin dan menetapkan izin ini kepada pengguna tenaga kerja untuk mengontrol akses mereka ke spesifik. Akun AWS

Akun AWS jenis

Ada dua jenis Akun AWS di AWS Organizations:

- Akun manajemen - Akun AWS Yang digunakan untuk membuat organisasi.
- Akun anggota - Akun AWS Sisanya milik organisasi.

Untuk informasi selengkapnya tentang Akun AWS jenis, lihat AWS Organizations Terminologi dan Konsep di Panduan AWS Organizations Pengguna.

Anda juga dapat memilih untuk mendaftarkan akun anggota sebagai administrator yang didelegasikan untuk IAM Identity Center. Pengguna di akun ini dapat melakukan sebagian besar tugas administrasi Pusat Identitas IAM. Untuk informasi selengkapnya, lihat Administrator yang didelegasikan.

Untuk setiap tugas dan jenis akun, tabel berikut menunjukkan apakah tugas administratif Pusat Identitas IAM dapat dilakukan oleh pengguna di akun.

Tugas administrasi Pusat Identitas IAM	Akun anggota	Akun administrator yang didelegasikan	Akun manajemen
Membaca pengguna atau grup (membaca grup itu sendiri dan keanggotaan grup)	Y	Y	Ya
Menambahkan, mengedit, atau menghapus pengguna atau grup	T	Y	Ya

Tugas administrasi Pusat Identitas IAM	Akun anggota	Akun administrator yang didelegasikan	Akun manajemen
Mengaktifkan atau menonaktifkan akses pengguna	T	Y	Ya
Mengaktifkan, menonaktifkan, atau mengelola atribut masuk	T	Y	Ya
Mengubah atau mengelola sumber identitas	T	Y	Ya
Membuat, mengedit, atau menghapus aplikasi	T	Y	Ya
Konfigurasikan MFA	T	Y	Ya
Mengelola set izin yang tidak disediakan di akun manajemen	T	Y	Ya
Mengelola set izin yang disediakan di akun manajemen	T	T	Ya
Aktifkan Pusat Identitas IAM	T	T	Ya

Tugas administrasi Pusat Identitas IAM	Akun anggota	Akun administrator yang didelegasikan	Akun manajemen
Hapus konfigurasi Pusat Identitas IAM	T	T	Ya
Mengaktifkan atau menonaktifkan akses pengguna di akun manajemen	T	T	Ya
Mendaftarkan atau membatalkan pendaftaran akun anggota sebagai administrator yang didelegasikan	T	T	Ya

Menetapkan akses Akun AWS

Anda dapat menggunakan set izin untuk menyederhanakan cara Anda menetapkan pengguna dan grup dalam akses organisasi Anda. Akun AWS Set izin disimpan di Pusat Identitas IAM dan menentukan tingkat akses yang dimiliki pengguna dan grup ke. Akun AWS Anda dapat membuat satu set izin dan menetapkannya ke beberapa Akun AWS dalam organisasi Anda. Anda juga dapat menetapkan beberapa set izin ke pengguna yang sama.

Untuk informasi selengkapnya tentang set izin, lihatMembuat, mengelola, dan menghapus set izin.

> **Note**
>
> Anda juga dapat menetapkan pengguna Anda akses masuk tunggal ke aplikasi. Untuk informasi, lihat Kelola akses ke aplikasi.

Pengalaman pengguna akhir

Portal AWS akses menyediakan pengguna IAM Identity Center dengan akses masuk tunggal ke semua yang ditugaskan Akun AWS dan aplikasi mereka melalui portal web. Portal AWS akses berbeda dari AWS Management Console, yang merupakan kumpulan konsol layanan untuk mengelola AWS sumber daya.

Saat Anda membuat set izin, nama yang Anda tentukan untuk set izin akan muncul di portal AWS akses sebagai peran yang tersedia. Pengguna masuk ke portal AWS akses, pilih Akun AWS, lalu pilih peran. Setelah mereka memilih peran, mereka dapat mengakses AWS layanan dengan menggunakan AWS Management Console atau mengambil kredensi sementara untuk mengakses AWS layanan secara terprogram.

Untuk membuka AWS Management Console atau mengambil kredensi sementara untuk mengakses AWS secara terprogram, pengguna menyelesaikan langkah-langkah berikut:

1. Pengguna membuka jendela browser dan menggunakan URL masuk yang Anda berikan untuk menavigasi ke portal AWS akses.
2. Dengan menggunakan kredensi direktori mereka, mereka masuk ke portal AWS akses.
3. Setelah otentikasi, pada halaman portal AWS akses, mereka memilih tab Akun untuk menampilkan daftar yang Akun AWS dapat mereka akses.
4. Pengguna kemudian memilih Akun AWS yang ingin mereka gunakan.
5. Di bawah nama Akun AWS, setiap set izin yang ditetapkan pengguna muncul sebagai peran yang tersedia. Misalnya, jika Anda menetapkan pengguna `john_stiles` ke set `PowerUser` izin, peran akan ditampilkan di portal AWS akses sebagai`PowerUser/john_stiles`. Pengguna yang diberi beberapa set izin memilih peran mana yang akan digunakan. Pengguna dapat memilih peran mereka untuk mengakses AWS Management Console.
6. Selain peran, pengguna portal AWS akses dapat mengambil kredensi sementara untuk baris perintah atau akses terprogram dengan memilih kunci Access.

Untuk step-by-step panduan yang dapat Anda berikan kepada pengguna tenaga kerja Anda, lihat Menggunakan portal AWS akses danMendapatkan kredensi pengguna IAM Identity Center untuk atau SDK AWS CLIAWS.

Menegakkan dan membatasi akses

Saat Anda mengaktifkan Pusat Identitas IAM, Pusat Identitas IAM membuat peran terkait layanan. Anda juga dapat menggunakan kebijakan kontrol layanan (SCP).

Mendelegasikan dan menegakkan akses

Peran terkait layanan adalah jenis peran IAM yang ditautkan langsung ke layanan. AWS Setelah Anda mengaktifkan Pusat Identitas IAM, Pusat Identitas IAM dapat membuat peran terkait layanan di masing-masing Akun AWS di organisasi Anda. Peran ini memberikan izin yang telah ditentukan sebelumnya yang memungkinkan Pusat Identitas IAM untuk mendelegasikan dan menegakkan pengguna mana yang memiliki akses masuk tunggal ke spesifik di organisasi Anda. Akun AWS AWS Organizations Anda perlu menetapkan satu atau beberapa pengguna dengan akses ke akun, untuk menggunakan peran ini. Lihat informasi yang lebih lengkap di Peran terkait layanan dan Menggunakan peran terkait layanan untuk IAM Identity Center.

Membatasi akses ke toko identitas dari akun anggota

Untuk layanan penyimpanan identitas yang digunakan oleh IAM Identity Center, pengguna yang memiliki akses ke akun anggota dapat menggunakan tindakan API yang memerlukan izin Baca. Akun anggota memiliki akses ke tindakan Baca di ruang nama direktori sso-dan identitystore. Untuk informasi selengkapnya, lihat Kunci tindakan, sumber daya, dan kondisi untuk AWS IAM Identity Center direktori dan Tindakan, sumber daya, dan kunci kondisi untuk AWS Identity Store di Referensi Otorisasi Layanan.

Untuk mencegah pengguna di akun anggota menggunakan operasi API di toko identitas, Anda dapat melampirkan kebijakan kontrol layanan (SCP). SCP adalah jenis kebijakan organisasi yang dapat Anda gunakan untuk mengelola izin di organisasi Anda. Contoh SCP berikut mencegah pengguna di akun anggota mengakses operasi API apa pun di toko identitas.

```
{
    "Sid": "ExplicitlyBlockIdentityStoreAccess",
    "Effect": "Deny",
    "Action": "identitystore:*", "sso-directory:*"],
    "Resource": "*"
}
```

> **Note**
>
> Membatasi akses akun anggota dapat mengganggu fungsionalitas dalam aplikasi yang diaktifkan IAM Identity Center.

Untuk informasi selengkapnya , lihat Kebijakan Kontrol Layanan (SCP) di Panduan Pengguna AWS Organizations .

Administrator yang didelegasikan

Administrasi yang didelegasikan menyediakan cara yang nyaman bagi pengguna yang ditugaskan di akun anggota terdaftar untuk melakukan sebagian besar tugas administratif Pusat Identitas IAM. Saat Anda mengaktifkan Pusat Identitas IAM, instans Pusat Identitas IAM Anda dibuat di akun manajemen secara AWS Organizations default. Ini awalnya dirancang dengan cara ini sehingga Pusat Identitas IAM dapat menyediakan, menghilangkan penyediaan, dan memperbarui peran di semua akun anggota organisasi Anda. Meskipun instans Pusat Identitas IAM Anda harus selalu berada di akun manajemen, Anda dapat memilih untuk mendelegasikan administrasi Pusat Identitas IAM ke akun anggota AWS Organizations, sehingga memperluas kemampuan untuk mengelola Pusat Identitas IAM dari luar akun manajemen.

Mengaktifkan administrasi yang didelegasikan memberikan manfaat berikut:

- Meminimalkan jumlah orang yang memerlukan akses ke akun manajemen untuk membantu mengurangi masalah keamanan
- Memungkinkan administrator tertentu untuk menetapkan pengguna dan grup ke aplikasi dan ke akun anggota organisasi Anda

Untuk informasi selengkapnya tentang cara kerja IAM Identity Center AWS Organizations, lihatKelola akses ke Akun AWS. Untuk informasi tambahan dan untuk meninjau contoh skenario perusahaan yang menunjukkan cara mengonfigurasi administrasi yang didelegasikan, lihat Memulai administrasi delegasi Pusat Identitas IAM di Blog Keamanan.AWS

Topik

- Praktik terbaik
- Prasyarat
- Daftarkan akun anggota

- Membatalkan pendaftaran akun anggota
- Lihat akun anggota mana yang telah terdaftar sebagai administrator yang didelegasikan

Praktik terbaik

Berikut adalah beberapa praktik terbaik yang perlu dipertimbangkan sebelum Anda mengonfigurasi administrasi yang didelegasikan.

- Berikan hak istimewa paling sedikit ke akun manajemen - Mengetahui bahwa akun manajemen adalah akun yang sangat istimewa dan untuk mematuhi prinsip hak istimewa paling sedikit, kami sangat menyarankan Anda membatasi akses ke akun manajemen kepada sesedikit mungkin orang. Fitur administrator yang didelegasikan dimaksudkan untuk meminimalkan jumlah orang yang memerlukan akses ke akun manajemen.
- Buat set izin untuk digunakan hanya di akun manajemen — Ini memudahkan pengelolaan set izin yang disesuaikan hanya untuk pengguna yang mengakses akun manajemen Anda dan membantu membedakannya dari kumpulan izin yang dikelola oleh akun administrator yang didelegasikan.
- Pertimbangkan lokasi Direktori Aktif Anda — Jika Anda berencana menggunakan Active Directory sebagai sumber identitas Pusat Identitas IAM Anda, cari direktori di akun anggota tempat Anda mengaktifkan fitur administrator yang didelegasikan IAM Identity Center. Jika Anda memutuskan untuk mengubah sumber identitas IAM Identity Center dari sumber lain ke Active Directory, atau mengubahnya dari Active Directory ke sumber lain, direktori harus berada di (dimiliki oleh) akun anggota administrator yang didelegasikan IAM Identity Center jika ada; jika tidak, itu harus berada di akun manajemen.
- Buat penugasan pengguna hanya di akun manajemen — Administrator yang didelegasikan tidak dapat mengubah set izin yang disediakan di akun manajemen. Namun, administrator yang didelegasikan dapat menambah, mengedit, dan menghapus grup dan tugas grup.

Prasyarat

Sebelum Anda dapat mendaftarkan akun sebagai administrator yang didelegasikan, Anda harus terlebih dahulu menerapkan lingkungan berikut:

- AWS Organizations harus diaktifkan dan dikonfigurasi dengan setidaknya satu akun anggota selain akun manajemen default Anda.
- Jika sumber identitas Anda disetel ke Active Directory, Pusat Identitas IAM sinkronisasi AD yang dapat dikonfigurasi fitur tersebut harus diaktifkan.

Daftarkan akun anggota

Untuk mengonfigurasi administrasi yang didelegasikan, Anda harus terlebih dahulu mendaftarkan akun anggota di organisasi Anda sebagai administrator yang didelegasikan. Pengguna di akun anggota yang memiliki izin yang memadai akan memiliki akses administratif ke Pusat Identitas IAM. Setelah akun anggota berhasil didaftarkan untuk administrasi yang didelegasikan, itu disebut sebagai akun administrator yang didelegasikan. Untuk mempelajari lebih lanjut tentang tugas yang dapat dilakukan oleh akun administrator yang didelegasikan, lihatAkun AWS jenis.

IAM Identity Center mendukung pendaftaran hanya satu akun anggota sebagai administrator yang didelegasikan pada satu waktu. Anda hanya dapat mendaftarkan akun anggota saat masuk dengan kredensi dari akun manajemen.

Gunakan prosedur berikut untuk memberikan akses administratif ke Pusat Identitas IAM dengan mendaftarkan akun anggota tertentu di AWS organisasi Anda sebagai administrator yang didelegasikan.

Important

Operasi ini mendelegasikan akses administratif Pusat Identitas IAM ke pengguna admin di akun anggota ini. Semua pengguna yang memiliki izin yang cukup untuk akun administrator yang didelegasikan ini dapat melakukan semua tugas administratif Pusat Identitas IAM dari akun, kecuali untuk:

- Mengaktifkan Pusat Identitas IAM
- Menghapus konfigurasi Pusat Identitas IAM
- Mengelola set izin yang disediakan di akun manajemen
- Mendaftarkan atau membatalkan pendaftaran akun anggota lain sebagai administrator yang didelegasikan
- Mengaktifkan atau menonaktifkan akses pengguna di akun manajemen

Administrator yang didelegasikan dapat mengedit keanggotaan grup.

Untuk mendaftarkan akun anggota

1. Masuk ke AWS Management Console menggunakan kredensi akun manajemen Anda. AWS Organizations Kredensi akun manajemen diperlukan untuk menjalankan API. RegisterDelegatedAdministrator
2. Pilih Wilayah tempat Pusat Identitas IAM diaktifkan, lalu buka konsol Pusat Identitas IAM.
3. Pilih Pengaturan, lalu pilih tab Manajemen.
4. Di bagian Administrator yang didelegasikan, pilih Daftar akun.
5. Pada halaman Daftarkan administrator yang didelegasikan, pilih yang ingin Akun AWS Anda daftarkan, lalu pilih Daftar akun.

Membatalkan pendaftaran akun anggota

Anda hanya dapat membatalkan pendaftaran akun anggota saat masuk dengan kredensi dari akun manajemen.

Gunakan prosedur berikut untuk menghapus akses administratif dari Pusat Identitas IAM dengan membatalkan pendaftaran akun anggota di AWS organisasi Anda yang sebelumnya telah ditetapkan sebagai administrator yang didelegasikan.

> **Important**
>
> Saat Anda membatalkan pendaftaran akun, Anda secara efektif menghapus kemampuan semua pengguna admin untuk mengelola Pusat Identitas IAM dari akun itu. Akibatnya, mereka tidak dapat lagi mengelola identitas Pusat Identitas IAM, manajemen akses, otentikasi, atau akses aplikasi dari akun ini. Operasi ini tidak akan memengaruhi izin atau tugas apa pun yang dikonfigurasi di Pusat Identitas IAM dan oleh karena itu tidak akan berdampak pada pengguna akhir Anda karena mereka akan terus memiliki akses ke aplikasi mereka dan Akun AWS dari dalam portal akses. AWS

Untuk membatalkan pendaftaran akun anggota

1. Masuk ke AWS Management Console menggunakan kredensi akun manajemen Anda. AWS Organizations Kredensi akun manajemen diperlukan untuk menjalankan API. DeregisterDelegatedAdministrator
2. Pilih Wilayah tempat Pusat Identitas IAM diaktifkan, lalu buka konsol Pusat Identitas IAM.

3. Pilih Pengaturan, lalu pilih tab Manajemen.
4. Di bagian Administrator yang didelegasikan, pilih Akun deregister.
5. Di kotak dialog Deregister account, tinjau implikasi keamanan, lalu masukkan nama akun anggota untuk mengonfirmasi bahwa Anda mengerti.
6. Pilih Akun Deregister.

Lihat akun anggota mana yang telah terdaftar sebagai administrator yang didelegasikan

Gunakan prosedur berikut untuk menemukan akun anggota mana yang AWS Organizations telah dikonfigurasi sebagai administrator yang didelegasikan untuk IAM Identity Center.

Untuk melihat akun anggota terdaftar Anda

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan.
3. Di bagian Detail, cari nama akun terdaftar di bawah Administrator yang didelegasikan. Anda juga dapat menemukan informasi ini dengan memilih tab Manajemen, dan melihatnya di bawah bagian Administrator yang didelegasikan.

Akses tinggi sementara

Semua akses ke Anda Akun AWS melibatkan beberapa tingkat hak istimewa. Operasi sensitif, seperti mengubah konfigurasi untuk sumber daya bernilai tinggi, misalnya, lingkungan produksi, memerlukan perlakuan khusus karena ruang lingkup dan dampak potensial. Akses tinggi sementara (juga dikenal sebagai just-in-time akses) adalah cara untuk meminta, menyetujui, dan melacak penggunaan izin untuk melakukan tugas tertentu selama waktu yang ditentukan. Akses tinggi sementara melengkapi bentuk kontrol akses lainnya, seperti set izin dan otentikasi multi-faktor.

AWS IAM Identity Center menyediakan opsi berikut untuk manajemen akses tinggi sementara di lingkungan bisnis dan teknis yang berbeda:

- Solusi yang dikelola vendor dan didukung - AWS telah memvalidasi integrasi IAM Identity Center dari penawaran mitra terpilih dan menilai kemampuan mereka terhadap serangkaian persyaratan pelanggan yang umum. Pilih solusi yang paling sesuai dengan skenario Anda dan ikuti panduan penyedia untuk mengaktifkan kemampuan dengan IAM Identity Center.

- Dikelola sendiri dan didukung sendiri — Opsi ini memberikan titik awal jika Anda tertarik pada akses sementara yang ditinggikan AWS saja dan Anda dapat menerapkan, menyesuaikan, dan mempertahankan kemampuan sendiri. Untuk informasi selengkapnya, lihat Manajemen akses tinggi sementara (TEAM).

Mitra AWS Keamanan yang Divalidasi untuk akses sementara yang ditingkatkan

AWS Mitra Keamanan menggunakan pendekatan yang berbeda untuk mengatasi serangkaian persyaratan akses sementara yang ditinggikan secara umum. Kami menyarankan Anda meninjau setiap solusi mitra dengan cermat, sehingga Anda dapat memilih salah satu yang paling sesuai dengan kebutuhan dan preferensi Anda, termasuk bisnis Anda, arsitektur lingkungan cloud Anda, dan anggaran Anda.

> **Note**
>
> Untuk pemulihan bencana, kami sarankan Anda mengatur akses darurat ke AWS Management Console sebelum gangguan terjadi.

AWS Identity telah memvalidasi kemampuan dan integrasi dengan IAM Identity Center untuk just-in-time penawaran berikut oleh Mitra Keamanan: AWS

- CyberArk Secure Cloud Access— Bagian dariCyberArk Identity Security Platform, penawaran ini menyediakan akses yang lebih tinggi sesuai permintaan ke AWS dan lingkungan multi-cloud. Persetujuan ditangani melalui integrasi dengan ITSM atau ChatOps perkakas. Semua sesi dapat direkam untuk audit dan kepatuhan.
- Tenable (previously Ermetic)TenablePlatform ini mencakup penyediaan akses just-in-time istimewa untuk operasi administratif di AWS dan lingkungan multi-cloud. Log sesi dari semua lingkungan cloud, termasuk log AWS CloudTrail akses, tersedia dalam satu antarmuka untuk analisis dan audit. Kemampuan ini terintegrasi dengan alat perusahaan dan pengembang seperti Slack dan Microsoft Teams.
- OktaPermintaan Akses — Bagian dari Tata Kelola Okta Identitas, memungkinkan Anda mengonfigurasi alur kerja permintaan just-in-time akses menggunakan Okta sebagai penyedia identitas eksternal (iDP) Pusat Identitas IAM dan set izin Pusat Identitas IAM Anda.

Daftar ini akan diperbarui sebagai AWS memvalidasi kemampuan solusi mitra tambahan dan integrasi solusi ini dengan IAM Identity Center.

> **Note**
>
> Jika Anda menggunakan kebijakan berbasis sumber daya, Amazon Elastic Kubernetes Service (Amazon EKS),AWS KMS atau () AWS Key Management Service , lihat sebelum Anda memilih solusi Anda. Mereferensikan set izin dalam kebijakan sumber daya, Amazon EKS, dan AWS KMS just-in-time

Kemampuan akses sementara yang ditingkatkan dinilai untuk validasi AWS mitra

AWS Identitas telah memvalidasi bahwa kemampuan akses sementara yang ditawarkan oleh CyberArk Secure Cloud Access, Tenable, dan Permintaan Okta Akses memenuhi persyaratan umum pelanggan berikut:

- Pengguna dapat meminta akses ke set izin untuk periode waktu yang ditentukan pengguna, menentukan AWS akun, set izin, periode waktu, dan alasan.
- Pengguna dapat menerima status persetujuan untuk permintaan mereka.
- Pengguna tidak dapat memanggil sesi dengan cakupan tertentu, kecuali ada permintaan yang disetujui dengan cakupan yang sama dan mereka memanggil sesi selama periode waktu yang disetujui.
- Ada cara untuk menentukan siapa yang dapat menyetujui permintaan.
- Penyetuju tidak dapat menyetujui permintaan mereka sendiri.
- Pemberi persetujuan memiliki daftar permintaan yang tertunda, disetujui, dan ditolak dan dapat mengekspornya untuk auditor.
- Pemberi persetujuan dapat menyetujui dan menolak permintaan yang tertunda.
- Pemberi persetujuan dapat menambahkan catatan yang menjelaskan keputusan mereka.
- Pemberi persetujuan dapat mencabut permintaan yang disetujui, mencegah penggunaan akses yang ditinggikan di masa mendatang.

> **Note**
>
> Jika pengguna masuk dengan akses tinggi saat permintaan yang disetujui dicabut, sesi mereka tetap aktif hingga satu jam setelah persetujuan dicabut. Untuk informasi tentang sesi otentikasi, lihatAutentikasi.

- Tindakan dan persetujuan pengguna tersedia untuk audit.

Akses masuk tunggal ke Akun AWS

Anda dapat menetapkan pengguna di izin direktori tersambung ke akun manajemen atau akun anggota di organisasi Anda AWS Organizations berdasarkan fungsi pekerjaan umum. Atau Anda dapat menggunakan izin khusus untuk memenuhi persyaratan keamanan spesifik Anda. Misalnya, Anda dapat memberikan izin luas kepada administrator database ke Amazon RDS di akun pengembangan tetapi membatasi izinnya di akun produksi. IAM Identity Center mengonfigurasi semua izin pengguna yang diperlukan di Anda secara otomatis. Akun AWS

> **Note**
>
> Anda mungkin perlu memberikan izin kepada pengguna atau grup untuk beroperasi di akun AWS Organizations manajemen. Karena ini adalah akun yang sangat istimewa, pembatasan keamanan tambahan mengharuskan Anda untuk memiliki FullAccess kebijakan IAM atau izin yang setara sebelum Anda dapat mengaturnya. Pembatasan keamanan tambahan ini tidak diperlukan untuk akun anggota mana pun di AWS organisasi Anda.

Tetapkan akses pengguna ke Akun AWS

Gunakan prosedur berikut untuk menetapkan akses masuk tunggal ke pengguna dan grup di direktori tersambung Anda dan gunakan set izin untuk menentukan tingkat akses mereka.

Untuk memeriksa akses pengguna dan grup yang ada, lihatLihat tugas pengguna dan grup.

> **Note**
>
> Untuk menyederhanakan administrasi izin akses, kami menyarankan Anda menetapkan akses langsung ke grup daripada ke pengguna individu. Dengan grup, Anda dapat

memberikan atau menolak izin ke grup pengguna daripada harus menerapkan izin tersebut ke setiap individu. Jika pengguna pindah ke organisasi lain, Anda cukup memindahkan pengguna tersebut ke grup yang berbeda dan mereka secara otomatis menerima izin yang diperlukan untuk organisasi baru.

Untuk menetapkan akses pengguna atau grup ke Akun AWS

1. Buka konsol Pusat Identitas IAM.

   > **Note**
   >
   > Pastikan bahwa konsol IAM Identity Center menggunakan Wilayah tempat AWS Managed Microsoft AD direktori Anda berada sebelum Anda pindah ke langkah berikutnya.

2. Di panel navigasi, di bawah Izin multi-akun, pilih. Akun AWS
3. Pada Akun AWShalaman, daftar tampilan pohon organisasi Anda akan muncul. Pilih kotak centang di samping satu atau lebih yang Akun AWS ingin Anda tetapkan akses masuk tunggal.

   > **Note**
   >
   > Anda dapat memilih hingga 10 Akun AWS sekaligus per izin yang ditetapkan saat Anda menetapkan akses masuk tunggal ke pengguna dan grup. Untuk menetapkan lebih dari 10 Akun AWS ke kumpulan pengguna dan grup yang sama, ulangi prosedur ini seperti yang diperlukan untuk akun tambahan. Saat diminta, pilih set pengguna, grup, dan izin yang sama.

4. Pilih Tetapkan pengguna atau grup.
5. Untuk Langkah 1: Pilih pengguna dan grup, pada halaman Tetapkan pengguna dan grup ke "***AWS-account-name***", lakukan hal berikut:

   1. Pada tab Pengguna, pilih satu atau beberapa pengguna yang akan diberikan akses masuk tunggal.

      Untuk memfilter hasil, mulailah mengetik nama pengguna yang Anda inginkan di kotak pencarian.

   2. Pada tab Grup, pilih satu atau beberapa grup yang akan memberikan akses masuk tunggal.

Untuk memfilter hasil, mulailah mengetik nama grup yang Anda inginkan di kotak pencarian.

3. Untuk menampilkan pengguna dan grup yang Anda pilih, pilih segitiga menyamping di samping Pengguna dan grup yang dipilih.
4. Setelah Anda mengonfirmasi bahwa pengguna dan grup yang benar dipilih, pilih Berikutnya.

6. Untuk Langkah 2: Pilih set izin, pada halaman Tetapkan izin ke halaman "***AWS-account-name***", lakukan hal berikut:

   1. Pilih satu atau beberapa set izin. Jika diperlukan, Anda dapat membuat dan memilih set izin baru.
      - Untuk memilih satu atau beberapa set izin yang ada, di bawah Set izin, pilih set izin yang ingin Anda terapkan ke pengguna dan grup yang Anda pilih di langkah sebelumnya.
      - Untuk membuat satu atau beberapa set izin baru, pilih Buat set izin, dan ikuti langkah-langkahnyaBuat set izin. Setelah Anda membuat set izin yang ingin Anda terapkan, di konsol Pusat Identitas IAM, kembali ke Akun AWSdan ikuti instruksi hingga Anda mencapai Langkah 2: Pilih set izin. Ketika Anda mencapai langkah ini, pilih set izin baru yang Anda buat, dan lanjutkan ke langkah berikutnya dalam prosedur ini.
   2. Setelah Anda mengonfirmasi bahwa set izin yang benar dipilih, pilih Berikutnya.

7. Untuk Langkah 3: Tinjau dan Kirim, pada Tinjau dan kirimkan tugas ke halaman "***AWS-account-name***", lakukan hal berikut:

   1. Tinjau set pengguna, grup, dan izin yang dipilih.
   2. Setelah Anda mengonfirmasi bahwa pengguna, grup, dan kumpulan izin yang benar dipilih, pilih Kirim.

> **Important**
>
> Proses penugasan pengguna dan grup mungkin membutuhkan waktu beberapa menit untuk diselesaikan. Biarkan halaman ini terbuka sampai proses berhasil diselesaikan.

> **Note**
>
> Anda mungkin perlu memberikan izin kepada pengguna atau grup untuk beroperasi di akun AWS Organizations manajemen. Karena ini adalah akun yang sangat istimewa, pembatasan keamanan tambahan mengharuskan Anda untuk memiliki FullAccess

kebijakan IAM atau izin yang setara sebelum Anda dapat mengaturnya. Pembatasan keamanan tambahan ini tidak diperlukan untuk akun anggota mana pun di AWS organisasi Anda.

Hapus akses pengguna dan grup

Gunakan prosedur ini untuk menghapus akses masuk tunggal ke satu atau Akun AWS beberapa pengguna dan grup di direktori Anda yang terhubung.

Untuk menghapus akses pengguna dan grup ke Akun AWS

1. Buka konsol Pusat Identitas IAM.
2. Di panel navigasi, di bawah Izin multi-akun, pilih. Akun AWS
3. Pada Akun AWShalaman, daftar tampilan pohon organisasi Anda akan muncul. Pilih nama Akun AWS yang berisi pengguna dan grup yang ingin Anda hapus akses masuk tunggal.
4. Pada halaman Ringkasan untuk Akun AWS, di bawah Pengguna dan grup yang ditugaskan, pilih nama satu atau beberapa pengguna atau grup, lalu pilih Hapus akses.
5. Dalam kotak dialog Hapus akses, konfirmasikan bahwa nama pengguna atau grup sudah benar, dan pilih Hapus akses.

Delegasikan siapa yang dapat menetapkan akses masuk tunggal ke pengguna dan grup di akun manajemen

Menetapkan akses masuk tunggal ke akun manajemen menggunakan konsol Pusat Identitas IAM adalah tindakan istimewa. Secara default, hanya pengguna yang memiliki AWSSSOMasterAccountAdministratordan IAMFullAccess AWS mengelola kebijakan yang dilampirkan, yang dapat menetapkan akses masuk tunggal ke akun manajemen. Pengguna root akun AWS IAMFullAccessKebijakan AWSSSOMasterAccountAdministratordan mengelola akses masuk tunggal ke akun manajemen dalam suatu AWS Organizations organisasi.

Gunakan langkah-langkah berikut untuk mendelegasikan izin untuk mengelola akses masuk tunggal ke pengguna dan grup di direktori Anda.

Untuk memberikan izin untuk mengelola akses masuk tunggal ke pengguna dan grup di direktori Anda

1. Masuk ke konsol Pusat Identitas IAM sebagai pengguna root akun manajemen atau dengan pengguna lain yang memiliki izin administrator ke akun manajemen.
2. Ikuti langkah-langkah Buat set izin untuk membuat set izin, lalu lakukan hal berikut:
    1. Pada halaman Buat set izin baru, pilih kotak centang Buat set izin khusus, lalu pilih Berikutnya: Detail.
    2. Pada halaman Buat set izin baru, tentukan nama untuk set izin khusus dan opsional, deskripsi. Jika diperlukan, ubah durasi sesi dan tentukan URL status relai.

        > **Note**
        >
        > Untuk URL status relai, Anda harus menentukan URL yang ada di AWS Management Console. Sebagai contoh:
        > **`https://console.aws.amazon.com/ec2/`**
        > Untuk informasi selengkapnya, lihat Atur status relai.

    3. Di bawah Kebijakan apa yang ingin Anda sertakan dalam set izin Anda? , pilih kotak centang Lampirkan kebijakan AWS terkelola.
    4. Dalam daftar kebijakan IAM, pilih kebijakan AWSSSOMasterAccountAdministratordan kebijakan yang IAMFullAccess AWS dikelola. Kebijakan ini memberikan izin kepada pengguna dan grup mana pun yang diberi akses ke izin ini yang ditetapkan di masa mendatang.
    5. Pilih Berikutnya: Tanda.
    6. Di bawah Tambahkan tag (opsional), tentukan nilai untuk Kunci dan Nilai (opsional), lalu pilih Berikutnya: Ulasan. Untuk informasi selengkapnya tentang tag, lihat Penandaan pada sumber daya AWS IAM Identity Center.
    7. Tinjau pilihan yang Anda buat, lalu pilih Buat.
3. Ikuti langkah-langkah Tetapkan akses pengguna ke Akun AWS untuk menetapkan pengguna dan grup yang sesuai ke set izin yang baru saja Anda buat.
4. Komunikasikan hal berikut kepada pengguna yang ditetapkan: Saat mereka masuk ke portal AWS akses dan memilih tab Akun, mereka harus memilih nama peran yang sesuai untuk diautentikasi dengan izin yang baru saja Anda delegasikan.

Set izin

Kumpulan izin adalah templat yang Anda buat dan pertahankan yang menentukan kumpulan satu atau beberapa kebijakan IAM. Set izin menyederhanakan penetapan Akun AWS akses untuk pengguna dan grup di organisasi Anda. Misalnya, Anda dapat membuat kumpulan izin Admin Database yang menyertakan kebijakan untuk mengelola layanan AWS RDS, DynamoDB, dan Aurora, dan menggunakan satu set izin tersebut untuk memberikan akses ke daftar Akun AWS target dalam Organisasi Anda untuk administrator database Anda.AWS

Pusat Identitas IAM memberikan akses ke pengguna atau grup dalam satu atau lebih Akun AWS dengan set izin. Saat Anda menetapkan set izin, Pusat Identitas IAM akan membuat peran IAM yang dikendalikan Pusat Identitas IAM terkait di setiap akun, dan melampirkan kebijakan yang ditentukan dalam izin yang disetel ke peran tersebut. IAM Identity Center mengelola peran, dan memungkinkan pengguna resmi yang telah Anda tentukan untuk mengambil peran, dengan menggunakan Portal Pengguna Pusat Identitas IAM atau CLI AWS . Saat Anda mengubah set izin, IAM Identity Center memastikan bahwa kebijakan dan peran IAM yang sesuai diperbarui sesuai dengan itu.

Anda dapat menambahkan kebijakan AWS terkelola, kebijakan terkelola pelanggan, kebijakan sebaris, dan kebijakan AWS terkelola untuk fungsi pekerjaan ke set izin Anda. Anda juga dapat menetapkan kebijakan AWS terkelola atau kebijakan yang dikelola pelanggan sebagai batas izin.

Untuk membuat set izin, lihatMembuat, mengelola, dan menghapus set izin.

Topik

- Izin yang telah ditentukan
- Izin kustom
- Membuat, mengelola, dan menghapus set izin
- Konfigurasikan properti set izin
- Mereferensikan set izin dalam kebijakan sumber daya, Amazon EKS, dan AWS KMS
- Hapus set izin

Izin yang telah ditentukan

Anda dapat membuat set izin yang telah ditentukan sebelumnya dengan kebijakan AWS terkelola.

Saat membuat set izin dengan izin yang telah ditentukan sebelumnya, Anda memilih satu kebijakan dari daftar kebijakan AWS terkelola. Dalam kebijakan yang tersedia, Anda dapat memilih dari Kebijakan izin umum dan kebijakan fungsi Job.

Kebijakan izin umum

Pilih dari daftar kebijakan AWS terkelola yang memungkinkan untuk mengakses sumber daya secara keseluruhan Akun AWS. Anda dapat menambahkan salah satu kebijakan berikut:

- AdministratorAccess
- PowerUserAccess
- ReadOnlyAccess
- ViewOnlyAccess

Kebijakan fungsi Job

Pilih dari daftar kebijakan AWS terkelola yang memungkinkan untuk mengakses sumber daya di Anda Akun AWS yang mungkin relevan dengan pekerjaan dalam organisasi Anda. Anda dapat menambahkan salah satu kebijakan berikut:

- Billing
- DataScientist
- DatabaseAdministrator
- NetworkAdministrator
- SecurityAudit
- SupportUser
- SystemAdministrator

Untuk deskripsi terperinci tentang kebijakan izin umum dan kebijakan fungsi pekerjaan yang tersedia, lihat kebijakan AWS terkelola untuk fungsi pekerjaan di panduan AWS Identity and Access Management pengguna.

Untuk petunjuk tentang cara membuat set izin, lihatMembuat, mengelola, dan menghapus set izin.

Izin kustom

Saat membuat set izin dengan Izin khusus, Anda dapat menggabungkan kebijakan AWS terkelola dan yang dikelola pelanggan AWS Identity and Access Management (IAM) dengan kebijakan sebaris,

dan batas izin yang menetapkan izin maksimum yang dapat diberikan oleh kebijakan lain kepada pengguna yang ditetapkan izin Anda.

Untuk petunjuk tentang cara membuat set izin, lihatMembuat, mengelola, dan menghapus set izin.

Jenis kebijakan yang dapat dilampirkan ke set izin

Topik

- Kebijakan inline
- AWS kebijakan terkelola
- Kebijakan yang dikelola pelanggan
- Batas izin

Kebijakan inline

Anda dapat melampirkan kebijakan inline ke set izin. Kebijakan inline adalah blok teks yang diformat sebagai kebijakan IAM yang Anda tambahkan langsung ke set izin. Anda dapat menempelkan kebijakan, atau membuat kebijakan baru dengan alat pembuatan kebijakan di konsol Pusat Identitas IAM saat Anda membuat set izin baru. Anda juga dapat membuat kebijakan IAM dengan AWS Policy Generator.

Saat Anda menerapkan set izin dengan kebijakan sebaris, Pusat Identitas IAM akan membuat kebijakan IAM di Akun AWS tempat Anda menetapkan set izin. Pusat Identitas IAM membuat kebijakan saat Anda menetapkan izin yang disetel ke akun. Kebijakan ini kemudian dilampirkan ke peran IAM dalam Anda Akun AWS yang diasumsikan pengguna Anda.

Saat Anda membuat kebijakan sebaris dan menetapkan set izin, Pusat Identitas IAM akan mengonfigurasi kebijakan untuk Anda. Akun AWS Saat membuat set izinKebijakan yang dikelola pelanggan, Anda harus membuat kebijakan Akun AWS sendiri sebelum menetapkan set izin.

AWS kebijakan terkelola

Anda dapat melampirkan kebijakan AWS terkelola ke set izin Anda. AWS kebijakan terkelola adalah kebijakan IAM yang AWS memelihara. Sebaliknya, Kebijakan yang dikelola pelanggan adalah kebijakan IAM di akun Anda yang Anda buat dan pertahankan. AWS kebijakan terkelola menangani kasus penggunaan hak istimewa paling umum di Anda Akun AWS. Anda dapat menetapkan kebijakan AWS terkelola sebagai izin untuk peran yang dibuat Pusat Identitas IAM, atau sebagai batas izin.

AWS memelihara kebijakan AWS terkelola untuk fungsi pekerjaan yang menetapkan izin akses khusus pekerjaan ke sumber daya Anda. AWS Anda dapat menambahkan satu kebijakan fungsi pekerjaan ketika Anda memilih untuk menggunakan izin yang telah ditentukan sebelumnya dengan set izin Anda. Saat memilih Izin khusus, Anda dapat menambahkan lebih dari satu kebijakan fungsi pekerjaan.

Anda Akun AWS juga berisi sejumlah besar kebijakan IAM AWS terkelola untuk spesifik Layanan AWS dan kombinasi. Layanan AWS Saat membuat set izin dengan izin khusus, Anda dapat memilih dari banyak kebijakan AWS terkelola tambahan yang akan ditetapkan ke set izin Anda.

AWS mengisi setiap Akun AWS dengan kebijakan AWS terkelola. Untuk menerapkan izin yang disetel dengan kebijakan AWS terkelola, Anda tidak perlu membuat kebijakan terlebih dahulu. Akun AWS Saat membuat set izinKebijakan yang dikelola pelanggan, Anda harus membuat kebijakan Akun AWS sendiri sebelum menetapkan set izin.

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

Kebijakan yang dikelola pelanggan

Anda dapat melampirkan kebijakan yang dikelola pelanggan ke set izin Anda. Kebijakan yang dikelola pelanggan adalah kebijakan IAM di akun Anda yang Anda buat dan pertahankan. Sebaliknya, AWS kebijakan terkelola adalah kebijakan IAM di akun Anda yang AWS memelihara. Anda dapat menetapkan kebijakan terkelola pelanggan sebagai izin untuk peran yang dibuat Pusat Identitas IAM, atau sebagai batas izin.

Saat membuat set izin dengan kebijakan terkelola pelanggan, Anda harus membuat kebijakan IAM dengan nama dan jalur yang sama di masing-masing Akun AWS tempat Pusat Identitas IAM menetapkan set izin Anda. Jika Anda menentukan jalur khusus, pastikan untuk menentukan jalur yang sama di masing-masing Akun AWS jalur. Untuk informasi selengkapnya, lihat Nama dan jalur yang mudah diingat dalam Panduan Pengguna IAM. IAM Identity Center melampirkan kebijakan IAM ke peran IAM yang dibuatnya di Anda. Akun AWS Sebagai praktik terbaik, terapkan izin yang sama ke kebijakan di setiap akun tempat Anda menetapkan izin yang ditetapkan. Untuk informasi selengkapnya, lihat Gunakan kebijakan IAM dalam set izin.

Untuk informasi selengkapnya, lihat Kebijakan yang dikelola pelanggan di Panduan Pengguna IAM.

Batas izin

Anda dapat melampirkan batas izin ke set izin Anda. Batas izin adalah kebijakan IAM AWS terkelola atau terkelola pelanggan yang menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada prinsipal IAM. Saat Anda menerapkan batas izin, Anda Kebijakan inlineKebijakan yang dikelola pelanggan, dan tidak AWS kebijakan terkelola dapat memberikan izin apa pun yang melebihi izin yang diberikan oleh batas izin Anda. Batas izin tidak memberikan izin apa pun, melainkan membuatnya sehingga IAM mengabaikan semua izin di luar batas.

Bila Anda membuat set izin dengan kebijakan terkelola pelanggan sebagai batas izin, Anda harus membuat kebijakan IAM dengan nama yang sama di setiap Akun AWS tempat Pusat Identitas IAM menetapkan set izin Anda. IAM Identity Center melampirkan kebijakan IAM sebagai batas izin ke peran IAM yang dibuatnya di Anda. Akun AWS

Untuk informasi lebih lanjut, lihat Batas izin untuk entitas IAM dalam Panduan Pengguna IAM.

Membuat, mengelola, dan menghapus set izin

Set izin menentukan tingkat akses yang dimiliki pengguna dan grup ke file Akun AWS. Set izin disimpan di Pusat Identitas IAM dan dapat disediakan untuk satu atau lebih. Akun AWS Anda dapat menetapkan lebih dari satu izin yang disetel ke pengguna. Untuk informasi selengkapnya tentang set izin dan cara penggunaannya di Pusat Identitas IAM, lihatSet izin.

Ingatlah pertimbangan berikut saat membuat set izin:

- Mulai dengan set izin yang telah ditentukan

  Dengan set izin yang telah ditentukan, yang menggunakan izin yang telah ditentukan sebelumnya, Anda memilih satu kebijakan AWS terkelola dari daftar kebijakan yang tersedia. Setiap kebijakan memberikan tingkat akses tertentu ke AWS layanan dan sumber daya atau izin untuk fungsi pekerjaan umum. Untuk informasi tentang masing-masing kebijakan ini, lihat kebijakan AWS terkelola untuk fungsi pekerjaan. Setelah mengumpulkan data penggunaan, Anda dapat menyempurnakan set izin agar lebih ketat.
- Batasi durasi sesi manajemen hingga periode kerja yang wajar

  Saat pengguna bergabung Akun AWS dan menggunakan AWS Management Console atau AWS Command Line Interface (AWS CLI), IAM Identity Center menggunakan pengaturan durasi sesi pada izin yang ditetapkan untuk mengontrol durasi sesi. Ketika sesi pengguna mencapai durasi sesi, mereka keluar dari konsol dan diminta untuk masuk lagi. Sebagai praktik keamanan terbaik, kami menyarankan agar Anda tidak mengatur durasi sesi lebih lama dari yang diperlukan

untuk menjalankan peran. Secara default, nilai untuk durasi Sesi adalah satu jam. Anda dapat menentukan nilai maksimum 12 jam. Untuk informasi selengkapnya, lihat Tetapkan durasi sesi.

- Batasi durasi sesi portal pengguna tenaga kerja

  Pengguna tenaga kerja menggunakan sesi portal untuk memilih peran dan mengakses aplikasi. Secara default, nilai durasi sesi maksimum, yang menentukan lamanya waktu pengguna tenaga kerja dapat masuk ke portal AWS akses sebelum mereka harus mengautentikasi ulang, adalah delapan jam. Anda dapat menentukan nilai maksimum 90 hari. Untuk informasi selengkapnya, lihat Konfigurasikan durasi sesi portal AWS akses dan aplikasi terintegrasi IAM Identity Center.

- Gunakan peran yang memberikan izin hak istimewa paling sedikit

  Setiap set izin yang Anda buat dan tetapkan ke pengguna Anda muncul sebagai peran yang tersedia di portal AWS akses. Saat Anda masuk ke portal sebagai pengguna tersebut, pilih peran yang sesuai dengan set izin paling ketat yang dapat Anda gunakan untuk melakukan tugas di akun, bukan`AdministratorAccess`. Uji set izin Anda untuk memverifikasi bahwa mereka menyediakan akses yang diperlukan sebelum mengirim undangan pengguna.

> **Note**
>
> Anda juga dapat menggunakan AWS CloudFormationuntuk membuat dan menetapkan set izin dan menetapkan pengguna ke set izin tersebut.

Topik

- Buat set izin
- Mendelegasikan administrasi set izin
- Gunakan kebijakan IAM dalam set izin

Buat set izin

Gunakan prosedur ini untuk membuat set izin yang telah ditentukan sebelumnya yang menggunakan kebijakan AWS terkelola tunggal, atau set izin khusus yang menggunakan hingga 10 kebijakan AWS terkelola atau terkelola pelanggan serta kebijakan sebaris. Anda dapat meminta penyesuaian jumlah maksimum 10 kebijakan di konsol Service Quotas untuk IAM.

Anda dapat membuat set izin di konsol Pusat Identitas IAM.

Untuk membuat set izin

1. Buka konsol Pusat Identitas IAM.
2. Di bawah Izin multi-akun, pilih Set izin.
3. Pilih Buat set izin.
4. Pada halaman Pilih jenis set izin, di bawah Jenis set izin, pilih jenis set izin.
5. Pilih satu atau beberapa kebijakan yang ingin Anda gunakan untuk set izin, berdasarkan jenis set izin:

   - Set izin yang telah ditentukan sebelumnya
     1. Pilih Berikutnya.
     2. Di bawah Kebijakan yang telah ditentukan sebelumnya, pilih salah satu kebijakan fungsi IAM Job atau Kebijakan izin umum dalam daftar, lalu pilih Berikutnya. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola untuk fungsi pekerjaan dan kebijakan AWS terkelola di Panduan AWS Identity and Access Management Pengguna.
     3. Pada layar Tinjau dan buat, tinjau pilihan yang Anda buat, lalu pilih Buat.
   - Set izin khusus
     1. Pilih Berikutnya.
     2. Pada halaman Tentukan kebijakan, pilih jenis kebijakan IAM yang ingin Anda terapkan ke set izin baru Anda. Secara default, Anda dapat menambahkan kombinasi hingga 10 kebijakan AWS terkelola dan kebijakan yang dikelola Pelanggan ke set izin Anda. Kuota ini ditetapkan oleh IAM. Untuk menaikkannya, minta peningkatan kuota IAM Kebijakan terkelola yang dilampirkan ke peran IAM di konsol Service Quotas di setiap Akun AWS tempat Anda ingin menetapkan set izin.
        - Perluas kebijakan AWS terkelola untuk menambahkan kebijakan dari IAM yang AWS membangun dan memelihara. Untuk informasi selengkapnya, lihat AWS kebijakan terkelola.
          a. Cari dan pilih kebijakan AWS terkelola yang ingin Anda terapkan pada pengguna di set izin.
          b. Jika Anda ingin menambahkan jenis kebijakan lain, pilih wadahnya dan tentukan pilihan Anda. Pilih Berikutnya ketika Anda telah memilih semua kebijakan yang ingin Anda terapkan.

- Perluas kebijakan yang dikelola Pelanggan untuk menambahkan kebijakan dari IAM yang Anda buat dan pertahankan. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola pelanggan.

  a. Pilih Lampirkan kebijakan dan masukkan nama kebijakan yang ingin ditambahkan ke set izin. Di setiap akun tempat Anda ingin menetapkan set izin, buat kebijakan dengan nama yang Anda masukkan. Sebagai praktik terbaik, tetapkan izin yang sama ke kebijakan di setiap akun.

  b. Pilih Lampirkan lebih banyak untuk menambahkan kebijakan lain.

  c. Jika Anda ingin menambahkan jenis kebijakan lain, pilih wadahnya dan tentukan pilihan Anda. Pilih Berikutnya ketika Anda telah memilih semua kebijakan yang ingin Anda terapkan.

- Perluas kebijakan sebaris kustom untuk menambahkan teks kebijakan berformat JSON kustom. Kebijakan sebaris tidak sesuai dengan sumber daya IAM yang ada. Untuk membuat kebijakan inline, masukkan bahasa kebijakan kustom dalam formulir yang disediakan. Pusat Identitas IAM menambahkan kebijakan ke sumber daya IAM yang dibuatnya di akun anggota Anda. Untuk informasi selengkapnya, lihat Kebijakan inline.

  a. Pilih Desain untuk menggunakan editor interaktif untuk memilih izin yang ingin Anda sertakan dalam kebijakan inline Anda. Pilih Kode untuk ditempelkan di JSON kebijakan yang telah diformat sebelumnya.

  b. Jika Anda ingin menambahkan jenis kebijakan lain, pilih wadahnya dan tentukan pilihan Anda. Pilih Berikutnya ketika Anda telah memilih semua kebijakan yang ingin Anda terapkan.

- Perluas batas Izin untuk menambahkan kebijakan IAM AWS terkelola atau terkelola pelanggan karena izin maksimum yang dapat ditetapkan oleh kebijakan Anda yang lain dalam kumpulan izin. Untuk informasi selengkapnya, lihat Batas izin.

  a. Pilih Gunakan batas izin untuk mengontrol izin maksimum.

  b. Pilih kebijakan AWS terkelola untuk menetapkan kebijakan dari IAM yang AWSdibangun dan dipertahankan sebagai batas izin Anda. Memilih kebijakan yang dikelola Pelanggan untuk menetapkan kebijakan dari IAM yang Anda buat dan pertahankan sebagai batas izin Anda.

  c. Jika Anda ingin menambahkan jenis kebijakan lain, pilih wadahnya dan tentukan pilihan Anda. Pilih Berikutnya ketika Anda telah memilih semua kebijakan yang ingin Anda terapkan.

6. Pada halaman Tentukan detail set izin, lakukan hal berikut:

1. Di bawah nama set Izin, ketik nama untuk mengidentifikasi izin ini yang ditetapkan di Pusat Identitas IAM. Nama yang Anda tentukan untuk set izin ini muncul di portal AWS akses sebagai peran yang tersedia. Pengguna masuk ke portal AWS akses, pilih Akun AWS, lalu pilih peran.
2. (Opsional) Anda juga dapat mengetik deskripsi. Deskripsi hanya muncul di konsol Pusat Identitas IAM, bukan portal AWS akses.
3. (Opsional) Tentukan nilai untuk Durasi sesi. Nilai ini menentukan lamanya waktu pengguna dapat login sebelum konsol mencatatnya keluar dari sesi mereka. Untuk informasi selengkapnya, lihat Tetapkan durasi sesi.
4. (Opsional) Tentukan nilai untuk status Relay. Nilai ini digunakan dalam proses federasi untuk mengarahkan pengguna ke dalam akun. Untuk informasi selengkapnya, lihat Atur status relai.

   > **Note**
   >
   > URL status relai harus berada di dalam file AWS Management Console. Sebagai contoh:
   > **`https://console.aws.amazon.com/ec2/`**

5. Perluas Tag (opsional), pilih Tambahkan tag, lalu tentukan nilai untuk Kunci dan Nilai (opsional).

   Untuk informasi tentang tanda, lihat Penandaan pada sumber daya AWS IAM Identity Center.
6. Pilih Berikutnya.
7. Pada halaman Tinjau dan buat, tinjau pilihan yang Anda buat, lalu pilih Buat.
8. Secara default, saat Anda membuat set izin, set izin tidak disediakan (digunakan di salah Akun AWS satu). Untuk memberikan izin yang ditetapkan Akun AWS, Anda harus menetapkan akses Pusat Identitas IAM ke pengguna dan grup di akun, lalu menerapkan izin yang disetel ke pengguna dan grup tersebut. Untuk informasi selengkapnya, lihat Akses masuk tunggal ke Akun AWS.

Mendelegasikan administrasi set izin

Pusat Identitas IAM memungkinkan Anda untuk mendelegasikan pengelolaan set izin dan penetapan di akun dengan membuat kebijakan IAM yang mereferensikan Nama Sumber Daya Amazon (ARN)

sumber daya Pusat Identitas IAM. Misalnya, Anda dapat membuat kebijakan yang memungkinkan administrator berbeda mengelola penetapan di akun tertentu untuk set izin dengan tag tertentu.

Anda dapat menggunakan salah satu metode berikut untuk membuat jenis kebijakan ini.

- (Disarankan) Buat set izin di Pusat Identitas IAM, masing-masing dengan kebijakan berbeda, dan tetapkan set izin ke pengguna atau grup yang berbeda. Ini memungkinkan Anda mengelola izin administratif bagi pengguna yang masuk menggunakan sumber identitas Pusat Identitas IAM yang Anda pilih.
- Buat kebijakan kustom di IAM, lalu lampirkan ke peran IAM yang diasumsikan administrator Anda. Untuk informasi tentang peran, lihat peran IAM untuk mendapatkan izin administratif Pusat Identitas IAM yang ditetapkan.

> **Important**
>
> ARN sumber daya Pusat Identitas IAM peka huruf besar/kecil.

Berikut ini menunjukkan kasus yang tepat untuk mereferensikan set izin IAM Identity Center dan tipe sumber daya akun.

Jenis Sumber Daya	ARN	Kunci Konteks
PermissionSet	`arn:${Partition}:sso:::permissionSet/${InstanceId}/${PermissionSetId}`	`aws:ResourceTag/${TagKey}`
Akun	`arn:${Partition}:sso:::account/${AccountId}`	Tidak Berlaku

Gunakan kebijakan IAM dalam set izin

DiBuat set izin, Anda mempelajari cara menambahkan kebijakan, termasuk kebijakan yang dikelola pelanggan dan batasan izin, ke set izin. Saat Anda menambahkan kebijakan dan izin terkelola pelanggan ke set izin, Pusat Identitas IAM tidak membuat kebijakan di mana pun. Akun AWS

Sebagai gantinya, Anda harus membuat kebijakan tersebut terlebih dahulu di setiap akun tempat Anda ingin menetapkan set izin, dan mencocokkannya dengan spesifikasi nama dan jalur dari set izin Anda. Saat Anda menetapkan izin yang disetel ke Akun AWS dalam organisasi Anda, Pusat Identitas IAM akan membuat peran AWS Identity and Access Management (IAM) dan melampirkan kebijakan IAM Anda ke peran tersebut.

> **Note**
>
> Sebelum Anda menetapkan izin yang ditetapkan dengan kebijakan IAM, Anda harus menyiapkan akun anggota Anda. Nama kebijakan IAM di akun anggota Anda harus berupa kecocokan peka huruf besar/kecil dengan nama kebijakan di akun manajemen Anda. Pusat Identitas IAM gagal menetapkan izin yang ditetapkan jika kebijakan tidak ada di akun anggota Anda.
> Izin yang diberikan kebijakan tidak harus sama persis antar akun.

Untuk menetapkan kebijakan IAM ke set izin

1. Buat kebijakan IAM di setiap Akun AWS tempat Anda ingin menetapkan set izin.
2. Tetapkan izin ke kebijakan IAM. Anda dapat menetapkan izin yang berbeda di akun yang berbeda. Untuk pengalaman yang konsisten, konfigurasikan dan pertahankan izin identik di setiap kebijakan. Anda dapat menggunakan sumber daya otomatisasi seperti AWS CloudFormation StackSets membuat salinan kebijakan IAM dengan nama dan izin yang sama di setiap akun anggota. Untuk informasi selengkapnya CloudFormation StackSets, lihat Bekerja dengan AWS CloudFormation StackSets di Panduan AWS CloudFormation pengguna.
3. Buat izin yang ditetapkan di akun manajemen Anda dan tambahkan kebijakan IAM Anda di bawah Kebijakan terkelola Pelanggan atau batas Izin. Untuk detail selengkapnya tentang cara membuat set izin, LihatBuat set izin.
4. Tambahkan kebijakan sebaris, kebijakan AWS terkelola, atau kebijakan IAM tambahan yang telah Anda siapkan.
5. Buat dan tetapkan set izin Anda.

Konfigurasikan properti set izin

Di Pusat Identitas IAM Anda dapat menyesuaikan pengalaman pengguna dengan mengonfigurasi properti set izin berikut.

Topik

Tetapkan durasi sesi

Untuk setiap set izin, Anda dapat menentukan durasi sesi untuk mengontrol lamanya waktu pengguna dapat masuk Akun AWS. Ketika durasi yang ditentukan berlalu, AWS tandatangani pengguna keluar dari sesi.

Saat Anda membuat set izin baru, durasi sesi diatur ke 1 jam (dalam detik) secara default. Durasi sesi minimum adalah 1 jam, dan dapat diatur hingga maksimal 12 jam. Pusat Identitas IAM secara otomatis membuat peran IAM di setiap akun yang ditetapkan untuk setiap set izin, dan mengonfigurasi peran ini dengan durasi sesi maksimum 12 jam.

Saat pengguna melakukan federasi ke Akun AWS konsol mereka atau saat AWS Command Line Interface (AWS CLI) digunakan, Pusat Identitas IAM menggunakan setelan durasi sesi pada set izin untuk mengontrol durasi sesi. Secara default, peran IAM yang dihasilkan oleh Pusat Identitas IAM untuk set izin hanya dapat diasumsikan oleh pengguna Pusat Identitas IAM, yang memastikan bahwa durasi sesi yang ditentukan dalam kumpulan izin Pusat Identitas IAM diberlakukan.

> **Important**
>
> Sebagai praktik keamanan terbaik, kami menyarankan Anda untuk tidak mengatur durasi sesi lebih lama dari yang diperlukan untuk menjalankan peran.

Setelah Anda membuat set izin, Anda dapat memperbaruinya untuk menerapkan durasi sesi baru. Gunakan prosedur berikut untuk mengubah panjang durasi sesi untuk set izin.

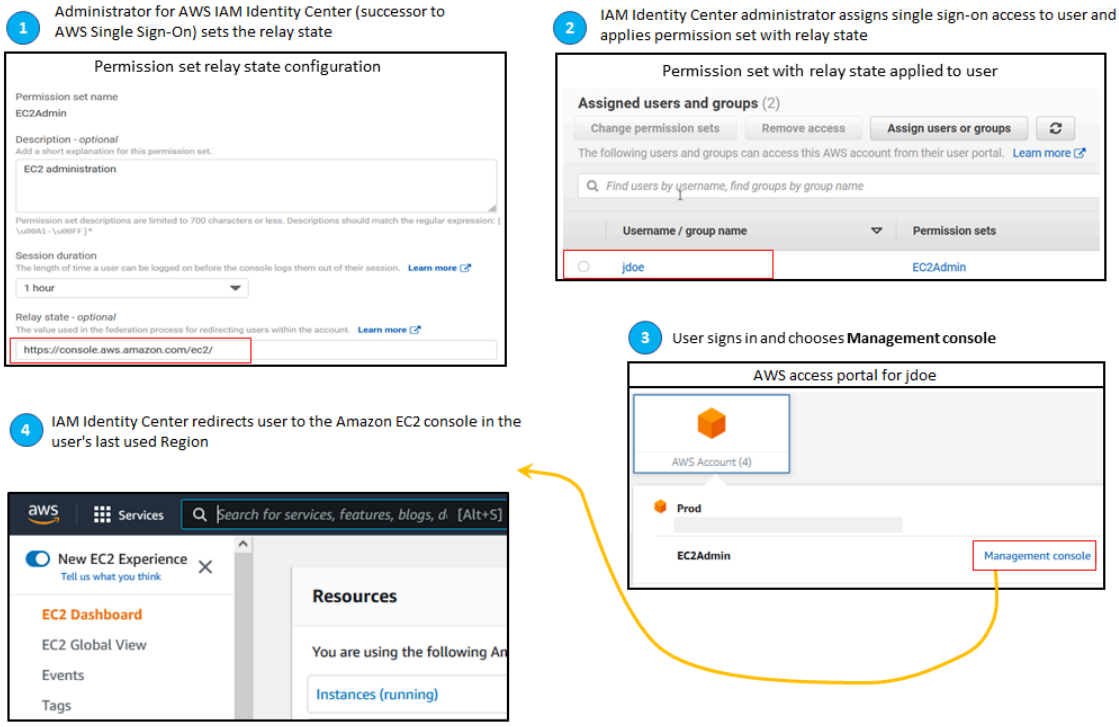
Untuk mengatur durasi sesi

1. Buka konsol Pusat Identitas IAM.
2. Di bawah Izin multi-akun, pilih Set izin.
3. Pilih nama set izin yang ingin Anda ubah durasi sesi.
4. Pada halaman detail untuk set izin, di sebelah kanan judul bagian Pengaturan umum, pilih Edit.
5. Pada halaman Edit pengaturan izin umum, pilih nilai baru untuk durasi Sesi.

6. Jika set izin disediakan di salah satu Akun AWS, nama akun akan muncul di bawah Akun AWS untuk penyediaan kembali secara otomatis. Setelah nilai durasi sesi untuk set izin diperbarui, semua Akun AWS yang menggunakan set izin akan direvisi. Ini berarti bahwa nilai baru untuk pengaturan ini diterapkan ke semua Akun AWS yang menggunakan set izin.
7. Pilih Simpan perubahan.
8. Di bagian atas Akun AWShalaman, pemberitahuan muncul.
   - Jika set izin disediakan dalam satu atau beberapa Akun AWS, notifikasi mengonfirmasi bahwa telah berhasil Akun AWS direvisi, dan set izin yang diperbarui diterapkan ke akun.
   - Jika set izin tidak disediakan dalam sebuah Akun AWS, notifikasi mengonfirmasi bahwa pengaturan untuk set izin telah diperbarui.

Atur status relai

Secara default, ketika pengguna masuk ke portal AWS akses, memilih akun, dan kemudian memilih peran yang AWS dibuat dari set izin yang ditetapkan, IAM Identity Center mengarahkan browser pengguna ke. AWS Management Console Anda dapat mengubah perilaku ini dengan menyetel status relai ke URL konsol yang berbeda. Menyetel status relai memungkinkan Anda memberi pengguna akses cepat ke konsol yang paling sesuai untuk peran mereka. Misalnya, Anda dapat menyetel status relai ke URL konsol Amazon EC2 (**`https://console.aws.amazon.com/ec2/`**) untuk mengarahkan pengguna ke konsol tersebut saat mereka memilih peran administrator Amazon EC2. Selama pengalihan ke URL default atau URL status relay, IAM Identity Center merutekan browser pengguna ke titik akhir konsol yang terakhir Wilayah AWS digunakan oleh pengguna. Misalnya, jika pengguna mengakhiri sesi konsol terakhir mereka di Wilayah Eropa (Stockholm) (eu-utara-1), pengguna dialihkan ke konsol Amazon EC2 di Wilayah tersebut.



Untuk mengonfigurasi Pusat Identitas IAM untuk mengarahkan pengguna ke konsol secara spesifik Wilayah AWS, sertakan spesifikasi Wilayah sebagai bagian dari URL. Misalnya, untuk mengarahkan pengguna ke konsol Amazon EC2 di Wilayah AS Timur (Ohio) (us-timur-2), tentukan URL untuk konsol Amazon EC2 di Wilayah tersebut (). **`https://us-east-2.console.aws.amazon.com/ec2/`** Jika Anda mengaktifkan Pusat Identitas IAM di Wilayah AS Barat (Oregon) (us-barat-2) Wilayah dan Anda ingin mengarahkan pengguna ke Wilayah itu, tentukan. **`https://us-west-2.console.aws.amazon.com`**

Gunakan prosedur berikut untuk mengonfigurasi URL status relai untuk set izin.

Untuk mengkonfigurasi status relai

1. Buka konsol Pusat Identitas IAM.
2. Di bawah Izin multi-akun, pilih Set izin.
3. Pilih nama set izin yang ingin Anda atur URL status relai baru.
4. Pada halaman detail untuk set izin, di sebelah kanan judul bagian Pengaturan umum, pilih Edit.
5. Pada halaman Edit pengaturan pengaturan izin umum, di bawah status Relay, ketik URL konsol untuk salah satu AWS layanan. Sebagai contoh:

`https://console.aws.amazon.com/ec2/`

> **Note**
>
> URL status relai harus berada di dalam file AWS Management Console.

6. Jika set izin disediakan di salah satu Akun AWS, nama akun akan muncul di bawah Akun AWS untuk penyediaan kembali secara otomatis. Setelah URL status relai untuk set izin diperbarui, semua Akun AWS yang menggunakan set izin akan direvisi. Ini berarti bahwa nilai baru untuk pengaturan ini diterapkan ke semua Akun AWS yang menggunakan set izin.
7. Pilih Simpan perubahan.
8. Di bagian atas halaman AWS Organisasi, pemberitahuan muncul.

   - Jika set izin disediakan dalam satu atau beberapa Akun AWS, notifikasi mengonfirmasi bahwa telah berhasil Akun AWS direvisi, dan set izin yang diperbarui diterapkan ke akun.
   - Jika set izin tidak disediakan dalam sebuah Akun AWS, notifikasi mengonfirmasi bahwa pengaturan untuk set izin telah diperbarui.

> **Note**
>
> Anda dapat mengotomatiskan proses ini dengan menggunakan AWS API, AWS SDK, atau AWS Command Line Interface()AWS CLI. Lihat informasi yang lebih lengkap di:
>
> - `UpdatePermissionSet`Tindakan `CreatePermissionSet` atau dalam Referensi API Pusat Identitas IAM
> - `update-permission-set`Perintah `create-permission-set` atau di sso-adminbagian Referensi AWS CLI Perintah.

Mereferensikan set izin dalam kebijakan sumber daya, Amazon EKS, dan AWS KMS

Saat Anda menetapkan izin yang disetel ke AWS akun, Pusat Identitas IAM akan membuat peran dengan nama yang dimulai dengan. `AWSReservedSSO_`

Nama lengkap dan Nama Sumber Daya Amazon (ARN) untuk peran menggunakan format berikut:

Nama	ARN
AWSReservedSSO_ *permission-set-name_unique-suffix*	arn:aws:iam:: *aws-account-ID*:role/aws-reserved/sso.amazonaws.com/ *aws-region* /AWSReservedSSO_ *permission-set-name_unique-suffix*

Misalnya, jika Anda membuat kumpulan izin yang memberikan akses AWS akun ke administrator database, peran yang sesuai akan dibuat dengan nama dan ARN berikut:

Nama	ARN
AWSReservedSSO_DatabaseAdministrator_1234567890abcdef	arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_1234567890abcdef

Jika Anda menghapus semua penetapan untuk izin ini yang ditetapkan dalam AWS akun, peran terkait yang dibuat Pusat Identitas IAM juga akan dihapus. Jika Anda membuat penugasan baru ke set izin yang sama nanti, Pusat Identitas IAM akan membuat peran baru untuk set izin. Nama dan ARN dari peran baru termasuk akhiran unik yang berbeda. Dalam contoh ini, akhiran unik adalah abcdef0123456789.

Nama	ARN
AWSReservedSSO_DatabaseAdministrator_ **abcdef0123456789**	arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/AWSReservedSSO_DatabaseAdministrator_ **abcdef0123456789**

Perubahan akhiran pada nama baru dan ARN untuk peran tersebut akan menyebabkan kebijakan apa pun yang merujuk nama asli dan ARN, yang mengganggu akses bagi individu yang menggunakan set izin yang sesuai. out-of-date Misalnya, perubahan ARN untuk peran akan mengganggu akses bagi pengguna dari set izin jika ARN asli direferensikan dalam konfigurasi berikut:

- Dalam `aws-auth ConfigMap` file untuk Amazon Elastic Kubernetes Service (Amazon EKS)
- Dalam kebijakan berbasis sumber daya untuk kunci (). AWS Key Management Service AWS KMS Kebijakan ini juga disebut sebagai kebijakan utama.

Meskipun Anda dapat memperbarui kebijakan berbasis sumber daya untuk sebagian besar AWS layanan untuk mereferensikan ARN baru untuk peran yang sesuai dengan kumpulan izin, Anda harus memiliki peran cadangan yang Anda buat di IAM untuk Amazon EKS dan jika ARN berubah. AWS KMS Untuk Amazon EKS, peran IAM cadangan harus ada di. `aws-auth ConfigMap` Karena AWS KMS, itu harus ada dalam kebijakan utama Anda. Jika Anda tidak memiliki peran IAM cadangan dalam kedua kasus, Anda harus menghubungi AWS Support.

Rekomendasi untuk menghindari gangguan akses

Untuk menghindari gangguan akses karena perubahan ARN untuk peran yang sesuai dengan set izin, kami sarankan Anda melakukan hal berikut.

- Pertahankan setidaknya satu penetapan set izin.

  Pertahankan penetapan ini di AWS akun yang berisi peran yang Anda referensikan di Amazon EKS, kebijakan utama AWS KMS, atau kebijakan berbasis sumber daya `aws-auth ConfigMap` untuk lainnya. Layanan AWS

  Misalnya, jika Anda membuat set `EKSAccess` izin dan mereferensikan peran terkait ARN dari AWS akun`111122223333`, maka tetapkan grup administratif secara permanen ke izin yang ditetapkan di akun tersebut. Karena penugasan bersifat permanen, IAM Identity Center tidak akan menghapus peran yang sesuai, yang menghilangkan risiko penggantian nama. Kelompok administratif akan selalu memiliki akses tanpa risiko eskalasi hak istimewa.
- Untuk Amazon EKS dan AWS KMS: Sertakan peran yang dibuat di IAM.

  Jika Anda mereferensikan ARN peran `aws-auth ConfigMap` untuk set izin di klaster Amazon EKS atau dalam kebijakan AWS KMS kunci untuk kunci, sebaiknya Anda juga menyertakan setidaknya satu peran yang Anda buat di IAM. Peran tersebut harus memungkinkan Anda

mengakses kluster Amazon EKS atau mengelola kebijakan AWS KMS utama. Set izin harus dapat mengambil peran ini. Dengan begitu, jika peran ARN untuk set izin berubah, Anda dapat memperbarui referensi ke ARN dalam kebijakan atau kunci. `aws-auth ConfigMap` AWS KMS Bagian selanjutnya memberikan contoh bagaimana Anda dapat membuat kebijakan kepercayaan untuk peran yang dibuat di IAM. Peran hanya dapat diasumsikan dengan set `AdministratorAccess` izin.

Contoh kebijakan kepercayaan khusus

Berikut ini adalah contoh kebijakan kepercayaan khusus yang menyediakan set `AdministratorAccess` izin dengan akses ke peran yang dibuat di IAM. Elemen kunci dari kebijakan ini meliputi:

- Elemen utama dari kebijakan kepercayaan ini menentukan pokok AWS akun. Dalam kebijakan ini, prinsipal di AWS akun `111122223333` dengan `sts:AssumeRole` izin dapat mengambil peran yang dibuat di IAM.
- Kebijakan kepercayaan ini menetapkan persyaratan tambahan untuk prinsipal yang dapat mengambil peran yang dibuat dalam IAM. `Condition element` Dalam kebijakan ini, izin yang ditetapkan dengan peran berikut ARN dapat mengambil peran tersebut.

```
arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/
AWSReservedSSO_AdministratorAccess_*"
```

> **Note**
>
> `Condition`Elemen termasuk operator `ArnLike` kondisi dan menggunakan wildcard di akhir peran set izin ARN, bukan akhiran unik. Ini berarti bahwa kebijakan akan mengizinkan set izin untuk mengambil peran yang dibuat di IAM meskipun ARN peran untuk set izin berubah.

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

```
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnLike": {
          "aws:PrincipalArn": "arn:aws:iam::111122223333:role/aws-reserved/
sso.amazonaws.com/eu-west-2/AWSReservedSSO_AdministratorAccess_*"
        }
      }
    }
  ]
}
```

Menyertakan peran yang Anda buat di IAM dalam kebijakan semacam itu akan memberi Anda akses darurat ke kluster Amazon EKS AWS KMS keys, atau AWS sumber daya lainnya jika set izin atau semua penetapan ke kumpulan izin dihapus dan dibuat ulang secara tidak sengaja.

Hapus set izin

Sebelum Anda dapat menghapus set izin dari IAM Identity Center, Anda harus menghapusnya dari semua Akun AWS yang menggunakan set izin. Untuk memeriksa akses pengguna dan grup yang ada, lihatLihat tugas pengguna dan grup.

Untuk menghapus set izin dari Akun AWS

1. Buka konsol Pusat Identitas IAM.
2. Di bawah Izin multi-akun, pilih. Akun AWS
3. Pada Akun AWShalaman, daftar tampilan pohon organisasi Anda akan muncul. Pilih nama Akun AWS dari mana Anda ingin menghapus set izin.
4. Pada halaman Ikhtisar untuk Akun AWS, pilih tab Set izin.
5. Pilih kotak centang di samping set izin yang ingin Anda hapus, lalu pilih Hapus.
6. Dalam kotak dialog Hapus set izin, konfirmasikan bahwa set izin yang benar dipilih, ketik **`Delete`** untuk mengonfirmasi penghapusan, lalu pilih Hapus akses.

Gunakan prosedur berikut untuk menghapus satu atau beberapa set izin sehingga tidak dapat lagi digunakan oleh siapa pun Akun AWS di organisasi.

> **Note**
>
> Semua pengguna dan grup yang telah diberi set izin ini, terlepas dari Akun AWS apa yang menggunakannya, tidak akan lagi dapat masuk. Untuk memeriksa akses pengguna dan grup yang ada, lihatLihat tugas pengguna dan grup.

Untuk menghapus set izin dari Akun AWS

1. Buka konsol Pusat Identitas IAM.
2. Di bawah Izin multi-akun, pilih Set izin.
3. Pilih set izin yang ingin Anda hapus, lalu pilih Hapus.
4. Di kotak dialog Hapus set izin, ketik nama set izin untuk mengonfirmasi penghapusan, lalu pilih Hapus. Nama domain tidak peka huruf besar/kecil.

Kontrol akses berbasis atribut

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Anda dapat menggunakan Pusat Identitas IAM untuk mengelola akses ke AWS sumber daya Anda di beberapa Akun AWS menggunakan atribut pengguna yang berasal dari sumber identitas Pusat Identitas IAM mana pun. Dalam AWS, atribut ini disebut tag. Menggunakan atribut pengguna sebagai tag dalam AWS membantu Anda menyederhanakan proses pembuatan izin berbutir halus AWS dan memastikan bahwa tenaga kerja Anda hanya mendapatkan akses ke sumber daya dengan tag yang cocok. AWS

Misalnya, Anda dapat menetapkan pengembang Bob dan Sally, yang berasal dari dua tim yang berbeda, ke izin yang sama yang ditetapkan di IAM Identity Center dan kemudian pilih atribut nama tim untuk kontrol akses. Ketika Bob dan Sally masuk ke mereka Akun AWS, IAM Identity Center mengirimkan atribut nama tim mereka dalam AWS sesi sehingga Bob dan Sally dapat mengakses sumber daya AWS proyek hanya jika atribut nama tim mereka cocok dengan tag nama tim pada sumber daya proyek. Jika Bob pindah ke tim Sally di masa depan, Anda dapat memodifikasi aksesnya hanya dengan memperbarui atribut nama timnya di direktori perusahaan. Ketika Bob masuk lain kali, dia akan secara otomatis mendapatkan akses ke sumber daya proyek tim barunya tanpa memerlukan izin pembaruan apa pun. AWS

Pendekatan ini juga membantu mengurangi jumlah izin berbeda yang perlu Anda buat dan kelola di IAM Identity Center karena pengguna yang terkait dengan set izin yang sama sekarang dapat

memiliki izin unik berdasarkan atribut mereka. Anda dapat menggunakan atribut pengguna ini dalam kumpulan izin IAM Identity Center dan kebijakan berbasis sumber daya untuk menerapkan ABAC ke sumber AWS daya dan menyederhanakan pengelolaan izin dalam skala besar.

Manfaat

Berikut ini adalah manfaat tambahan menggunakan ABAC di IAM Identity Center.

- ABAC memerlukan lebih sedikit set izin — Karena Anda tidak perlu membuat kebijakan yang berbeda untuk fungsi pekerjaan yang berbeda, Anda membuat lebih sedikit set izin. Ini mengurangi kompleksitas manajemen izin Anda.
- Menggunakan ABAC, tim dapat berubah dan berkembang dengan cepat — Izin untuk sumber daya baru secara otomatis diberikan berdasarkan atribut ketika sumber daya ditandai dengan tepat pada saat pembuatan.
- Gunakan atribut karyawan dari direktori perusahaan Anda dengan ABAC — Anda dapat menggunakan atribut karyawan yang ada dari sumber identitas apa pun yang dikonfigurasi di Pusat Identitas IAM untuk membuat keputusan kontrol akses. AWS
- Lacak siapa yang mengakses sumber daya — Administrator keamanan dapat dengan mudah menentukan identitas sesi dengan meninjau atribut pengguna AWS CloudTrail untuk melacak aktivitas pengguna. AWS

Untuk informasi tentang cara mengonfigurasi ABAC menggunakan konsol Pusat Identitas IAM, lihat. Atribut untuk kontrol akses Untuk informasi tentang cara mengaktifkan dan mengonfigurasi ABAC menggunakan API Pusat Identitas IAM, lihat CreateInstanceAccessControlAttributeConfigurationdi Panduan Referensi API Pusat Identitas IAM.

Topik

- Checklist: Mengkonfigurasi ABAC dalam AWS menggunakan IAM Identity Center
- Atribut untuk kontrol akses

Checklist: Mengkonfigurasi ABAC dalam AWS menggunakan IAM Identity Center

Daftar periksa ini mencakup tugas konfigurasi yang diperlukan untuk menyiapkan AWS sumber daya Anda dan untuk menyiapkan Pusat Identitas IAM untuk akses ABAC. Selesaikan tugas dalam daftar

periksa ini secara berurutan. Saat tautan referensi membawa Anda ke suatu topik, kembalilah ke topik ini sehingga Anda dapat melanjutkan tugas yang tersisa dalam daftar periksa ini.

Langka	Tugas	Referensi
1	Tinjau cara menambahkan tag ke semua AWS sumber daya Anda. Untuk mengimplementasikan ABAC di IAM Identity Center, pertama-tama Anda harus menambahk an tag ke semua AWS sumber daya yang ingin Anda terapkan ABAC.	• Sumber daya penandaan AWS
2	Tinjau cara mengonfigurasi sumber identitas Anda di Pusat Identitas IAM dengan identitas dan atribut pengguna terkait di toko identitas Anda. IAM Identity Center memungkinkan Anda menggunakan atribut pengguna dari sumber identitas IAM Identity Center yang didukung untuk ABAC di. AWS	• Kelola sumber identitas Anda
3	Berdasarkan kriteria berikut, tentukan atribut mana yang ingin Anda gunakan untuk membuat keputusan kontrol akses AWS dan kirimkan ke Pusat Identitas IAM.	• Memulai
	• Jika Anda menggunakan penyedia identitas eksternal (iDP), putuskan apakah Anda ingin menggunakan atribut yang diteruskan dari iDP atau pilih atribut dari dalam Pusat Identitas IAM.	• Memilih atribut saat menggunakan penyedia identitas eksternal sebagai sumber identitas Anda
	• Jika Anda memilih untuk mengirim atribut IDP Anda, konfigurasikan IDP Anda untuk mengirimkan atribut dalam pernyataan SAMP. Lihat `Optional` bagian dalam tutorial untuk IDP spesifik Anda.	• Memulai tutorial
	• Jika Anda menggunakan iDP sebagai sumber identitas Anda dan memilih untuk memilih atribut di IAM Identity Center, selidiki cara mengkonfigurasi SCIM sehingga nilai atribut berasal dari idP Anda. Jika Anda tidak dapat menggunakan SCIM dengan	• Penyediaan otomatis • Atribut penyedia identitas eksternal yang didukung

Langka	Tugas	Referensi
	IDP Anda, tambahkan pengguna dan atributnya menggunakan halaman Pengguna konsol Pusat Identitas IAM.	
	• Jika Anda menggunakan Active Directory atau IAM Identity Center sebagai sumber identitas Anda, atau Anda menggunakan IDP dan memilih untuk memilih atribut di IAM Identity Center, tinjau atribut yang tersedia yang dapat Anda konfigurasi. Kemudian langsung lompat ke langkah 4 untuk mulai mengonfig urasi atribut ABAC Anda menggunakan konsol IAM Identity Center.	• Memilih atribut saat menggunakan IAM Identity Center sebagai sumber identitas Anda • Memilih atribut saat menggunakan AWS Managed Microsoft AD sebagai sumber identitas Anda • Pemetaan default
4	Pilih atribut yang akan digunakan untuk ABAC menggunakan halaman Attributes for access control di konsol IAM Identity Center. Dari halaman ini Anda dapat memilih atribut untuk kontrol akses dari sumber identitas yang Anda konfigurasikan pada langkah 2. Setelah identitas Anda dan atributnya berada di Pusat Identitas IAM, Anda harus membuat pasangan nilai kunci (pemetaan) yang akan diteruskan ke Anda Akun AWS untuk digunakan dalam keputusan kontrol akses.	• Aktifkan dan konfigurasikan atribut untuk kontrol akses
5	Buat kebijakan izin khusus dalam set izin Anda dan gunakan atribut kontrol akses untuk membuat aturan ABAC sehingga pengguna hanya dapat mengakses sumber daya dengan tag yang cocok. Atribut pengguna yang Anda konfigurasikan pada langkah 4 digunakan sebagai tag AWS untuk keputusan kontrol akses. Anda dapat merujuk ke atribut kontrol akses dalam kebijakan izin menggunakan `aws:PrincipalTag/key` kondisi.	• Buat kebijakan izin untuk ABAC di IAM Identity Center

Langka	Tugas	Referensi
6	Di berbagai Anda Akun AWS, tetapkan pengguna ke set izin yang Anda buat di langkah 5. Melakukannya memastikan bahwa ketika mereka bergabung ke akun mereka dan mengakses AWS sumber daya, mereka hanya mendapatkan akses berdasarkan tag yang cocok.	• Tetapkan akses pengguna ke Akun AWS

Setelah Anda menyelesaikan langkah-langkah ini, pengguna yang bergabung ke dalam sistem masuk Akun AWS tunggal akan mendapatkan akses ke AWS sumber daya mereka berdasarkan atribut yang cocok.

Atribut untuk kontrol akses

Atribut untuk kontrol akses adalah nama halaman di konsol Pusat Identitas IAM tempat Anda memilih atribut pengguna yang ingin digunakan dalam kebijakan untuk mengontrol akses ke sumber daya. Anda dapat menetapkan pengguna ke beban kerja AWS berdasarkan atribut yang ada di sumber identitas pengguna.

Misalnya, Anda ingin menetapkan akses ke bucket S3 berdasarkan nama departemen. Saat berada di halaman Atribut untuk kontrol akses, Anda memilih atribut pengguna Departemen untuk digunakan dengan kontrol akses berbasis atribut (ABAC). Dalam set izin Pusat Identitas IAM, Anda kemudian menulis kebijakan yang memberi pengguna akses hanya jika atribut Department cocok dengan tag departemen yang ditetapkan ke bucket S3. IAM Identity Center meneruskan atribut departemen pengguna ke akun yang sedang diakses. Atribut kemudian digunakan untuk menentukan akses berdasarkan kebijakan. Untuk informasi lebih lanjut tentang ABAC, lihatKontrol akses berbasis atribut.

Memulai

Bagaimana Anda memulai mengonfigurasi atribut untuk kontrol akses tergantung pada sumber identitas yang Anda gunakan. Terlepas dari sumber identitas yang Anda pilih, setelah memilih atribut, Anda perlu membuat atau mengedit kebijakan set izin. Kebijakan ini harus memberikan akses identitas pengguna ke AWS sumber daya.

Memilih atribut saat menggunakan IAM Identity Center sebagai sumber identitas Anda

Saat Anda mengonfigurasi Pusat Identitas IAM sebagai sumber identitas, pertama-tama Anda menambahkan pengguna dan mengonfigurasi atributnya. Selanjutnya, arahkan ke halaman Attributes for access control dan pilih atribut yang ingin Anda gunakan dalam kebijakan. Terakhir, navigasikan ke Akun AWShalaman untuk membuat atau mengedit set izin untuk menggunakan atribut untuk ABAC.

Memilih atribut saat menggunakan AWS Managed Microsoft AD sebagai sumber identitas Anda

Saat Anda mengonfigurasi Pusat Identitas IAM AWS Managed Microsoft AD sebagai sumber identitas Anda, pertama-tama Anda memetakan sekumpulan atribut dari Active Directory ke atribut pengguna di IAM Identity Center. Selanjutnya, navigasikan ke halaman Attributes for access control. Kemudian pilih atribut mana yang akan digunakan dalam konfigurasi ABAC Anda berdasarkan kumpulan atribut SSO yang ada yang dipetakan dari Active Directory. Terakhir, pembuat aturan ABAC menggunakan atribut kontrol akses dalam set izin untuk memberikan akses identitas pengguna ke AWS sumber daya. Untuk daftar pemetaan default untuk atribut pengguna di Pusat Identitas IAM ke atribut pengguna di AWS Managed Microsoft AD direktori Anda, lihat. Pemetaan default

Memilih atribut saat menggunakan penyedia identitas eksternal sebagai sumber identitas Anda

Saat Anda mengonfigurasi Pusat Identitas IAM dengan penyedia identitas eksternal (iDP) sebagai sumber identitas Anda, ada dua cara untuk menggunakan atribut untuk ABAC.

- Anda dapat mengonfigurasi IDP Anda untuk mengirim atribut melalui pernyataan SAMP. Dalam hal ini, IAM Identity Center meneruskan nama atribut dan nilai dari iDP melalui evaluasi kebijakan.

  > **Note**
  >
  > Atribut dalam pernyataan SAMP tidak akan terlihat oleh Anda di halaman Atribut untuk kontrol akses. Anda harus mengetahui atribut ini terlebih dahulu dan menambahkannya ke aturan kontrol akses saat Anda membuat kebijakan. Jika Anda memutuskan untuk mempercayai atribut IdPs for eksternal Anda, maka atribut ini akan selalu diteruskan saat pengguna bergabung Akun AWS. Dalam skenario di mana atribut yang sama datang ke Pusat Identitas IAM melalui SAMP dan SCIM, nilai atribut SAMP diutamakan dalam keputusan kontrol akses.

- Anda dapat mengonfigurasi atribut yang Anda gunakan dari halaman Atribut untuk kontrol akses di konsol Pusat Identitas IAM. Nilai atribut yang Anda pilih di sini menggantikan nilai untuk setiap

atribut yang cocok yang berasal dari IDP melalui pernyataan. Tergantung pada apakah Anda menggunakan SCIM, pertimbangkan hal berikut:

- Jika menggunakan SCIM, iDP secara otomatis menyinkronkan nilai atribut ke IAM Identity Center. Atribut tambahan yang diperlukan untuk kontrol akses mungkin tidak ada dalam daftar atribut SCIM. Dalam hal ini, pertimbangkan untuk berkolaborasi dengan admin TI di IDP Anda untuk mengirim atribut tersebut ke Pusat Identitas IAM melalui pernyataan SAMP menggunakan awalan yang diperlukan. `https://aws.amazon.com/SAML/Attributes/AccessControl:` Untuk informasi tentang cara mengkonfigurasi atribut pengguna untuk kontrol akses di IDP Anda untuk dikirim melalui pernyataan SAMP, lihat untuk IDP Anda. Memulai tutorial
- Jika Anda tidak menggunakan SCIM, Anda harus menambahkan pengguna secara manual dan mengatur atribut mereka seperti jika Anda menggunakan IAM Identity Center sebagai sumber identitas. Selanjutnya, arahkan ke halaman Atribut untuk kontrol akses dan pilih atribut yang ingin Anda gunakan dalam kebijakan.

Untuk daftar lengkap atribut yang didukung untuk atribut pengguna di Pusat Identitas IAM ke atribut pengguna di eksternal Anda IdPs, lihatAtribut penyedia identitas eksternal yang didukung.

Untuk memulai ABAC di IAM Identity Center, lihat topik berikut.

Topik

- Aktifkan dan konfigurasikan atribut untuk kontrol akses
- Buat kebijakan izin untuk ABAC di IAM Identity Center

Aktifkan dan konfigurasikan atribut untuk kontrol akses

Untuk menggunakan ABAC dalam semua kasus, Anda harus terlebih dahulu mengaktifkan ABAC menggunakan konsol IAM Identity Center atau IAM Identity Center API. Jika Anda memilih untuk menggunakan IAM Identity Center untuk memilih atribut, Anda menggunakan halaman Attributes for access control di konsol IAM Identity Center atau IAM Identity Center API. Jika Anda menggunakan penyedia identitas eksternal (iDP) sebagai sumber identitas dan memilih untuk mengirim atribut melalui pernyataan SAMP, Anda mengonfigurasi idP Anda untuk meneruskan atribut. Jika pernyataan SAMP melewati salah satu atribut ini, IAM Identity Center akan mengganti nilai atribut dengan nilai dari penyimpanan identitas Pusat Identitas IAM. Hanya atribut yang dikonfigurasi di Pusat Identitas IAM yang akan dikirim untuk membuat keputusan kontrol akses saat pengguna bergabung ke akun mereka.

> **Note**
>
> Anda tidak dapat melihat atribut yang dikonfigurasi dan dikirim oleh iDP eksternal dari halaman Atribut untuk kontrol akses di konsol Pusat Identitas IAM. Jika Anda meneruskan atribut kontrol akses dalam pernyataan SAMP dari IDP eksternal Anda, maka atribut tersebut langsung dikirim ke ketika pengguna bergabung. Akun AWS Atribut tidak akan tersedia di IAM Identity Center untuk pemetaan.

Aktifkan atribut untuk kontrol akses

Gunakan prosedur berikut untuk mengaktifkan fitur kontrol atribut untuk akses (ABAC) menggunakan konsol IAM Identity Center.

> **Note**
>
> Jika Anda memiliki set izin yang ada dan Anda berencana untuk mengaktifkan ABAC di instans Pusat Identitas IAM Anda, pembatasan keamanan tambahan mengharuskan Anda untuk terlebih dahulu memiliki kebijakan tersebut`iam:UpdateAssumeRolePolicy`. Pembatasan keamanan tambahan ini tidak diperlukan jika Anda tidak memiliki set izin yang dibuat di akun Anda.

Untuk mengaktifkan Atribut untuk kontrol akses

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan
3. Pada halaman Pengaturan, cari kotak Atribut untuk informasi kontrol akses, lalu pilih Aktifkan. Lanjutkan ke prosedur berikutnya untuk mengkonfigurasinya.

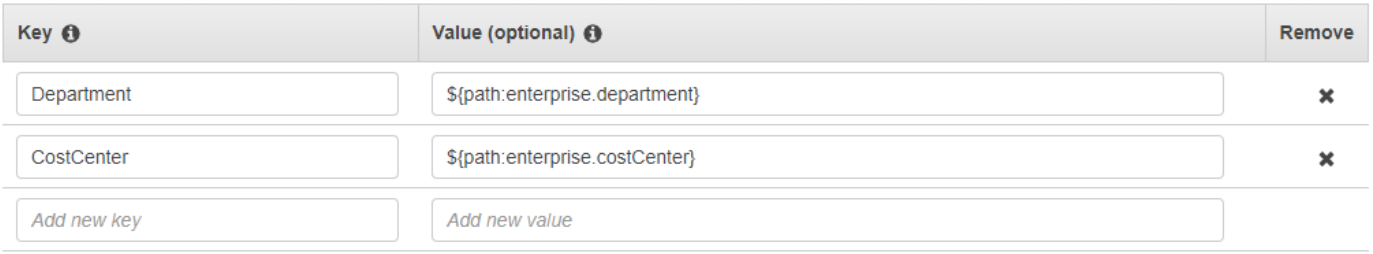
Pilih atribut Anda

Gunakan prosedur berikut untuk menyiapkan atribut untuk konfigurasi ABAC Anda.

Untuk memilih atribut Anda menggunakan konsol Pusat Identitas IAM

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan

3. Pada halaman Pengaturan, pilih tab Atribut untuk kontrol akses, lalu pilih Kelola atribut.
4. Pada halaman Atribut untuk kontrol akses, pilih Tambahkan atribut dan masukkan detail Kunci dan Nilai. Di sinilah Anda akan memetakan atribut yang berasal dari sumber identitas Anda ke atribut yang diteruskan oleh IAM Identity Center sebagai tag sesi.



Kunci mewakili nama yang Anda berikan ke atribut untuk digunakan dalam kebijakan. Ini bisa berupa nama sewenang-wenang, tetapi Anda perlu menentukan nama persis itu dalam kebijakan yang Anda buat untuk kontrol akses. Misalnya, katakanlah Anda menggunakan Okta (iDP eksternal) sebagai sumber identitas Anda dan harus meneruskan data pusat biaya organisasi Anda sebagai tag sesi. Di Key, Anda akan memasukkan nama yang sama cocok CostCenterseperti nama kunci Anda. Penting untuk dicatat bahwa nama apa pun yang Anda pilih di sini, itu juga harus diberi nama yang persis sama dalam nama Anda [Kunci syarat aws:PrincipalTag] (yaitu,). `"ec2:ResourceTag/CostCenter": "${aws:PrincipalTag/CostCenter}"`

> **Note**
>
> Gunakan atribut nilai tunggal untuk kunci Anda, misalnya,**`Manager`**. IAM Identity Center tidak mendukung atribut multi-nilai untuk ABAC, misalnya,. **`Manager, IT Systems`**

Nilai mewakili konten atribut yang berasal dari sumber identitas yang dikonfigurasi. Di sini Anda dapat memasukkan nilai apa pun dari tabel sumber identitas yang sesuai yang tercantum dalamPemetaan atribut untuk direktori AWS Managed Microsoft AD. Misalnya, menggunakan konteks yang disediakan dalam contoh yang disebutkan di atas, Anda akan meninjau daftar atribut idP yang didukung dan menentukan bahwa kecocokan terdekat dari atribut yang didukung akan menjadi **`${path:enterprise.costCenter}`**dan Anda kemudian akan memasukkannya di bidang Nilai. Lihat tangkapan layar yang disediakan di atas untuk referensi. Perhatikan, bahwa Anda tidak dapat menggunakan nilai atribut idP eksternal di luar daftar ini untuk ABAC kecuali Anda menggunakan opsi untuk meneruskan atribut melalui pernyataan SAMP.

5. Pilih Simpan perubahan.

Sekarang setelah Anda mengonfigurasi pemetaan atribut kontrol akses Anda, Anda harus menyelesaikan proses konfigurasi ABAC. Untuk melakukan ini, buat aturan ABAC Anda dan tambahkan ke set izin dan/atau kebijakan berbasis sumber daya Anda. Ini diperlukan agar Anda dapat memberikan akses identitas pengguna ke AWS sumber daya. Untuk informasi selengkapnya, lihat Buat kebijakan izin untuk ABAC di IAM Identity Center.

Nonaktifkan atribut untuk kontrol akses

Gunakan prosedur berikut untuk menonaktifkan fitur ABAC dan menghapus semua pemetaan atribut yang telah dikonfigurasi.

Untuk menonaktifkan Atribut untuk kontrol akses

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan
3. Pada halaman Pengaturan, pilih tab Atribut untuk kontrol akses, lalu pilih Nonaktifkan.
4. Dalam dialog Nonaktifkan atribut untuk kontrol akses, tinjau informasi dan saat siap masukkan DELETE, lalu pilih Konfirmasi.

> **Important**
>
> Langkah ini menghapus semua atribut yang telah dikonfigurasi. Setelah dihapus, atribut apa pun yang diterima dari sumber identitas dan atribut kustom apa pun yang telah Anda konfigurasikan sebelumnya tidak akan diteruskan.

Buat kebijakan izin untuk ABAC di IAM Identity Center

Anda dapat membuat kebijakan izin yang menentukan siapa yang dapat mengakses AWS sumber daya Anda berdasarkan nilai atribut yang dikonfigurasi. Saat Anda mengaktifkan ABAC dan menentukan atribut, Pusat Identitas IAM meneruskan nilai atribut pengguna yang diautentikasi ke IAM untuk digunakan dalam evaluasi kebijakan.

Kunci syarat aws:PrincipalTag

Anda dapat menggunakan atribut kontrol akses dalam set izin menggunakan kunci `aws:PrincipalTag` kondisi untuk membuat aturan kontrol akses. Misalnya, dalam kebijakan kepercayaan berikut, Anda dapat menandai semua sumber daya di organisasi Anda dengan pusat biaya masing-masing. Anda juga dapat menggunakan satu set izin yang memberi pengembang

akses ke sumber daya pusat biaya mereka. Sekarang, setiap kali pengembang bergabung ke akun menggunakan sistem masuk tunggal dan atribut pusat biaya mereka, mereka hanya mendapatkan akses ke sumber daya di pusat biaya masing-masing. Saat tim menambahkan lebih banyak pengembang dan sumber daya ke proyek mereka, Anda hanya perlu menandai sumber daya dengan pusat biaya yang benar. Kemudian Anda meneruskan informasi pusat biaya di AWS sesi saat pengembang bergabung Akun AWS. Akibatnya, ketika organisasi menambahkan sumber daya dan pengembang baru ke pusat biaya, pengembang dapat mengelola sumber daya yang selaras dengan pusat biaya mereka tanpa memerlukan pembaruan izin apa pun.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/CostCenter": "${aws:PrincipalTag/CostCenter}"
                }
            }
        }
    ]
}
```

Untuk informasi selengkapnya, lihat aws:PrincipalTagdan EC2: Memulai atau menghentikan instance berdasarkan pencocokan tag utama dan sumber daya di Panduan Pengguna IAM.

Jika kebijakan berisi atribut yang tidak valid dalam kondisinya, maka kondisi kebijakan akan gagal dan akses akan ditolak. Untuk informasi selengkapnya, lihat Kesalahan 'Kesalahan tak terduga telah terjadi' ketika pengguna mencoba masuk menggunakan penyedia identitas eksternal.

Penyedia identitas IAM

Saat Anda menambahkan akses masuk tunggal ke Akun AWS, Pusat Identitas IAM membuat penyedia identitas IAM di masing-masing. Akun AWS Penyedia identitas IAM membantu menjaga Akun AWS keamanan Anda karena Anda tidak perlu mendistribusikan atau menanamkan kredensil keamanan jangka panjang, seperti kunci akses, di aplikasi Anda.

Memperbaiki penyedia identitas IAM

Jika Anda secara tidak sengaja menghapus atau memodifikasi penyedia identitas Anda, Anda harus secara manual menerapkan kembali penetapan pengguna dan grup Anda. Menerapkan kembali tugas pengguna dan grup akan membuat ulang penyedia identitas. Lihat informasi yang lebih lengkap di:

- Kelola akses ke Akun AWS
- Kelola akses ke aplikasi

Peran terkait layanan

Peran terkait layanan adalah izin IAM yang telah ditentukan sebelumnya yang memungkinkan Pusat Identitas IAM untuk mendelegasikan dan menegakkan pengguna mana yang memiliki akses masuk tunggal ke spesifik di organisasi Anda. Akun AWS AWS Organizations Layanan ini memungkinkan fungsionalitas ini dengan menyediakan peran terkait layanan di setiap Akun AWS dalam organisasinya. Layanan ini kemudian memungkinkan AWS layanan lain seperti IAM Identity Center untuk memanfaatkan peran tersebut untuk melakukan tugas-tugas terkait layanan. Untuk informasi selengkapnya, lihat AWS Organizations dan peran terkait layanan.

Saat Anda mengaktifkan Pusat Identitas IAM, Pusat Identitas IAM akan membuat peran terkait layanan di semua akun dalam organisasi. AWS Organizations IAM Identity Center juga menciptakan peran terkait layanan yang sama di setiap akun yang kemudian ditambahkan ke organisasi Anda. Peran ini memungkinkan Pusat Identitas IAM untuk mengakses sumber daya setiap akun atas nama Anda. Untuk informasi selengkapnya, lihat Kelola akses ke Akun AWS.

Peran terkait layanan yang dibuat di masing-masing Akun AWS diberi nama. `AWSServiceRoleForSSO` Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk IAM Identity Center.

Kelola akses ke aplikasi

Dengan AWS IAM Identity Center, Anda dapat mengontrol siapa yang dapat memiliki akses masuk tunggal ke aplikasi Anda. Pengguna mendapatkan akses tanpa batas ke aplikasi ini setelah mereka menggunakan kredensi direktori mereka untuk masuk.

IAM Identity Center berkomunikasi dengan aman dengan aplikasi ini melalui hubungan tepercaya antara IAM Identity Center dan penyedia layanan aplikasi. Kepercayaan ini dapat dibuat dengan berbagai cara, tergantung pada jenis aplikasi.

IAM Identity Center mendukung dua jenis aplikasi: aplikasi AWS terkelola dan aplikasi yang dikelola pelanggan. AWS aplikasi terkelola dikonfigurasi langsung dari dalam konsol aplikasi yang relevan atau melalui API aplikasi. Aplikasi yang dikelola pelanggan harus ditambahkan ke konsol Pusat Identitas IAM dan dikonfigurasi dengan metadata yang sesuai untuk Pusat Identitas IAM dan penyedia layanan.

Setelah Anda mengkonfigurasi aplikasi untuk bekerja dengan IAM Identity Center, Anda dapat mengelola pengguna atau grup mana yang mengakses aplikasi. Secara default, tidak ada pengguna yang ditugaskan ke aplikasi.

Anda juga dapat memberikan karyawan Anda akses ke AWS Management Console untuk spesifik Akun AWS di organisasi Anda. Untuk informasi selengkapnya, lihat Kelola akses ke Akun AWS.

Topik

AWS aplikasi terkelola

AWS aplikasi terkelola terintegrasi dengan IAM Identity Center dan dapat menggunakannya untuk otentikasi dan layanan direktori.

Integrasi aplikasi AWS terkelola dengan IAM Identity Center memberi Anda jalur yang lebih mudah untuk menetapkan akses pengguna, tanpa perlu mengatur sinkronisasi federasi atau pengguna dan grup terpisah untuk setiap aplikasi. Anda dapat menghubungkan sumber identitas yang ingin Anda gunakan untuk otentikasi sekali, dan Anda menerima satu tampilan penugasan pengguna dan grup. Administrator aplikasi yang memungkinkan propagasi identitas tepercaya dapat menentukan dan mengaudit akses ke sumber daya aplikasi mereka berdasarkan pengguna atau keanggotaan grup pengguna, tanpa perlu memetakannya ke peran IAM.

AWS aplikasi terkelola menyediakan antarmuka pengguna administratif yang dapat Anda gunakan untuk mengelola akses ke sumber daya aplikasi. Misalnya, QuickSight administrator dapat menetapkan pengguna untuk mengakses dasbor berdasarkan keanggotaan grup mereka. Sebagian besar aplikasi yang AWS dikelola juga memberikan AWS Management Console pengalaman yang memungkinkan Anda untuk menetapkan pengguna ke aplikasi. Pengalaman konsol untuk aplikasi ini mungkin mengintegrasikan kedua fungsi, untuk menggabungkan kemampuan penetapan pengguna dengan kemampuan untuk mengelola akses ke sumber daya aplikasi.

AWS aplikasi terkelola yang terintegrasi dengan IAM Identity Center meliputi:

AWS aplikasi terkelola yang terintegrasi dengan IAM Identity Center

AWS aplikasi terkelola	Terintegrasi dengan instans organisasi IAM Identity Center	Terintegrasi dengan instans akun IAM Identity Center	Memungkinkan propagasi identitas tepercaya melalui IAM Identity Center
Amazon Athena SQL	Y	Y	Ya
Amazon CodeCatalyst	Y	Y	Tidak

AWS aplikasi terkelola	Terintegrasi dengan instans organisasi IAM Identity Center	Terintegrasi dengan instans akun IAM Identity Center	Memungkinkan propagasi identitas tepercaya melalui IAM Identity Center
Amazon CodeWhisperer	 Y	 T	 Tidak
Notebook Amazon EMR	 Y	 T	 Tidak
Amazon EMR di Amazon EC2	 Y	 Y	 Ya
Amazon EMR Studio	 Y	 Y	 Ya
Amazon Kendra	 Y	 T	 Tidak
Amazon Managed Grafana	 Y	 T	 Tidak
Amazon Monitron	 Y	 T	 Tidak

AWS aplikasi terkelola	Terintegrasi dengan instans organisasi IAM Identity Center	Terintegrasi dengan instans akun IAM Identity Center	Memungkinkan propagasi identitas tepercaya melalui IAM Identity Center
Amazon Nimble Studio	 Y	 T	 Tidak
Amazon Pinpoint	 Y	 T	 Tidak
Amazon QuickSight	 Y	 Y	 Ya
Amazon Redshift	 Y	 Y	 Ya
Hibah Akses Amazon S3	 Y	 Y	 Ya
SageMaker Studio Amazon	 Y	 T	 Tidak
WorkSpaces Web Amazon	 Y	 T	 Tidak

AWS aplikasi terkelola	Terintegrasi dengan instans organisasi IAM Identity Center	Terintegrasi dengan instans akun IAM Identity Center	Memungkinkan propagasi identitas tepercaya melalui IAM Identity Center
AWS CLI	 Y	 T	 Tidak
AWS IoT Events	 Y	 T	 Tidak
AWS IoT Fleet Hub	 Y	 T	 Tidak
AWS IoT SiteWise	 Y	 T	 Tidak
AWS Lake Formation	 Y	 Y	 Ya
Rantai Pasokan AWS	 Y	 T	 Tidak
AWS Systems Manager	 Y	 T	 Tidak

AWS aplikasi terkelola	Terintegrasi dengan instans organisasi IAM Identity Center	Terintegrasi dengan instans akun IAM Identity Center	Memungkinkan propagasi identitas tepercaya melalui IAM Identity Center
Akses Terverifikasi AWS	 Y	 T	 Tidak

Topik

- Mengendalikan akses
- Mengkoordinasikan tugas-tugas administratif
- Mengkonfigurasi IAM Identity Center untuk berbagi informasi identitas
- Pertimbangan untuk berbagi informasi identitas di Akun AWS
- Membatasi penggunaan aplikasi terkelola AWS
- Melihat detail tentang aplikasi AWS terkelola
- Menonaktifkan aplikasi terkelola AWS

Mengendalikan akses

Akses ke aplikasi yang AWS dikelola dikendalikan dengan dua cara:

- Entri awal ke aplikasi - IAM Identity Center mengelola ini melalui penugasan ke aplikasi. Secara default, penugasan diperlukan untuk aplikasi yang AWS dikelola.
- Akses ke sumber daya aplikasi — Aplikasi mengelola ini melalui penugasan sumber daya independen yang dikontrolnya.

Mengkoordinasikan tugas-tugas administratif

Jika Anda seorang administrator aplikasi, Anda dapat memilih apakah akan memerlukan tugas ke aplikasi. Jika penugasan diperlukan, saat pengguna masuk ke portal AWS akses, hanya pengguna

yang ditugaskan ke aplikasi secara langsung atau melalui penugasan grup yang dapat melihat ubin aplikasi. Atau, jika tugas tidak diperlukan, Anda dapat mengizinkan semua pengguna Pusat Identitas IAM untuk masuk ke aplikasi. Dalam hal ini, aplikasi mengelola akses ke sumber daya dan ubin aplikasi terlihat oleh semua pengguna yang mengunjungi portal AWS akses.

Jika Anda administrator Pusat Identitas IAM, Anda dapat menggunakan konsol Pusat Identitas IAM untuk menghapus tugas ke AWS aplikasi terkelola. Sebelum Anda menghapus tugas, kami sarankan Anda berkoordinasi dengan administrator aplikasi. Anda juga harus berkoordinasi dengan administrator aplikasi jika Anda berencana untuk mengubah pengaturan yang menentukan apakah penugasan diperlukan, atau mengotomatiskan penetapan aplikasi.

Mengkonfigurasi IAM Identity Center untuk berbagi informasi identitas

IAM Identity Center menyediakan penyimpanan identitas yang berisi atribut pengguna dan grup, tidak termasuk kredensi login. Anda dapat menggunakan salah satu metode berikut untuk memperbarui pengguna dan grup di toko identitas Pusat Identitas IAM Anda:

- Gunakan toko identitas IAM Identity Center sebagai sumber identitas utama Anda. Jika Anda memilih metode ini, Anda mengelola pengguna Anda, kredensi masuk mereka, dan grup dari dalam konsol Pusat Identitas IAM atau (). AWS Command Line Interface AWS CLI Untuk informasi selengkapnya, lihat Kelola identitas di Pusat Identitas IAM.
- Siapkan penyediaan (sinkronisasi) pengguna dan grup yang berasal dari salah satu sumber identitas berikut ke toko identitas Pusat Identitas IAM Anda:
  - Active Directory - Untuk informasi lebih lanjut, lihatConnect ke Microsoft AD direktori.
  - Penyedia identitas eksternal — Untuk informasi selengkapnya, lihatConnect ke penyedia identitas eksternal.

  Jika Anda memilih metode penyediaan ini, Anda terus mengelola pengguna dan grup dari dalam sumber identitas Anda, dan perubahan tersebut disinkronkan ke penyimpanan identitas Pusat Identitas IAM.

Sumber identitas mana pun yang Anda pilih, IAM Identity Center dapat berbagi informasi pengguna dan grup dengan aplikasi terkelola. AWS Dengan begitu, Anda dapat menghubungkan sumber identitas ke IAM Identity Center sekali dan kemudian berbagi informasi identitas dengan beberapa aplikasi di AWS Cloud. Ini menghilangkan kebutuhan untuk secara independen mengatur federasi dan penyediaan identitas dengan setiap aplikasi. Fitur berbagi ini juga memudahkan untuk memberi pengguna Anda akses ke banyak aplikasi yang berbeda Akun AWS.

Pertimbangan untuk berbagi informasi identitas di Akun AWS

IAM Identity Center mendukung atribut yang paling umum digunakan di seluruh aplikasi. Atribut ini termasuk nama depan dan belakang, nomor telepon, alamat email, alamat, dan bahasa pilihan. Pertimbangkan dengan cermat aplikasi mana dan akun mana yang dapat menggunakan informasi identitas pribadi ini.

Anda dapat mengontrol akses ke informasi ini dengan salah satu cara berikut. Anda dapat memilih untuk mengaktifkan akses hanya di akun AWS Organizations manajemen atau di semua akun di AWS Organizations. Atau, Anda dapat menggunakan kebijakan kontrol layanan (SCP) untuk mengontrol aplikasi mana yang dapat mengakses informasi di AWS Organizations akun mana. Misalnya, jika Anda mengaktifkan akses di akun AWS Organizations manajemen saja, maka aplikasi di akun anggota tidak memiliki akses ke informasi tersebut. Namun, jika Anda mengaktifkan akses di semua akun, Anda dapat menggunakan SCP untuk melarang akses oleh semua aplikasi kecuali yang ingin Anda izinkan.

Membatasi penggunaan aplikasi terkelola AWS

Ketika Anda mengaktifkan IAM Identity Center untuk pertama kalinya, AWS memungkinkan penggunaan aplikasi AWS terkelola secara otomatis di semua akun di AWS Organizations. Untuk membatasi aplikasi, Anda harus menerapkan SCP. Anda dapat menggunakan SCP untuk memblokir akses ke informasi pengguna dan grup Pusat Identitas IAM dan untuk mencegah aplikasi dimulai, kecuali di akun yang ditunjuk.

Melihat detail tentang aplikasi AWS terkelola

Setelah Anda menghubungkan aplikasi AWS terkelola ke IAM Identity Center dengan menggunakan konsol atau API untuk aplikasi, aplikasi terdaftar di IAM Identity Center. Setelah aplikasi terdaftar di IAM Identity Center, Anda dapat melihat informasi terperinci tentang aplikasi di konsol Pusat Identitas IAM.

Untuk melihat informasi tentang aplikasi AWS terkelola di konsol Pusat Identitas IAM

1. Buka konsol Pusat Identitas IAM.
2. Pilih Aplikasi.
3. Pilih tab aplikasi AWS terkelola.
4. Dalam daftar aplikasi, pilih nama aplikasi yang ingin Anda lihat informasi detailnya.

5. Informasi tentang aplikasi mencakup apakah penugasan pengguna dan grup diperlukan, dan jika berlaku, pengguna dan grup yang ditugaskan serta aplikasi tepercaya untuk propagasi identitas. Untuk informasi tentang propagasi identitas tepercaya, lihatPropagasi identitas tepercaya di seluruh aplikasi.

Menonaktifkan aplikasi terkelola AWS

Untuk mencegah pengguna mengautentikasi ke aplikasi yang AWS dikelola, Anda dapat menonaktifkan aplikasi di konsol Pusat Identitas IAM.

> **Warning**
>
> Menonaktifkan aplikasi menghapus semua izin pengguna ke aplikasi ini, memutus aplikasi dari IAM Identity Center, dan membuat aplikasi tidak dapat diakses. Jika Anda seorang administrator IAM Identity Center, sebaiknya Anda berkoordinasi dengan administrator aplikasi sebelum melakukan tugas ini.

Untuk menonaktifkan aplikasi AWS terkelola

1. Buka konsol Pusat Identitas IAM.
2. Pilih Aplikasi.
3. Pada halaman Aplikasi, di bawah aplikasi AWS terkelola, pilih aplikasi yang ingin Anda nonaktifkan.
4. Dengan aplikasi yang dipilih, pilih Tindakan, lalu pilih Nonaktifkan.
5. Di kotak dialog Tangguhkan aplikasi, pilih Tangguhkan.
6. Dalam daftar aplikasi AWS terkelola, status aplikasi muncul sebagai Tidak Aktif.

Aplikasi yang dikelola pelanggan

Dengan IAM Identity Center, Anda dapat membuat atau menghubungkan pengguna tenaga kerja dan mengelola akses mereka secara terpusat di semua aplikasi dan aplikasi mereka Akun AWS . IAM Identity Center bertindak sebagai layanan identitas pusat dan menyediakan berbagai cara bagi pengguna Anda untuk diautentikasi. Jika Anda sudah menggunakan penyedia identitas (iDP), IAM Identity Center dapat berintegrasi dengan IDP Anda sehingga Anda dapat menyediakan pengguna dan grup Anda ke IAM Identity Center dan menggunakan IDP Anda untuk otentikasi.

Jika Anda menggunakan aplikasi yang dikelola pelanggan yang mendukung SAMP 2.0, Anda dapat menggabungkan IDP Anda ke IAM Identity Center melalui SAMP 2.0 dan menggunakan IAM Identity Center untuk mengelola akses pengguna ke aplikasi tersebut. IAM Identity Center menyediakan katalog aplikasi yang umum digunakan yang mendukung SAMP 2.0, seperti Salesforce dan Microsoft 365. Katalog ini tersedia di konsol Pusat Identitas IAM. Anda juga dapat mengatur aplikasi SAMP 2.0 Anda sendiri.

> **Note**
>
> Jika Anda memiliki aplikasi yang dikelola pelanggan yang mendukung OAuth 2.0 dan pengguna Anda memerlukan akses dari aplikasi ini ke AWS layanan, Anda dapat menggunakan propagasi identitas tepercaya. Dengan propagasi identitas tepercaya, pengguna dapat masuk ke aplikasi, dan aplikasi itu dapat meneruskan identitas pengguna dalam permintaan untuk mengakses data dalam AWS layanan. Untuk informasi selengkapnya, lihat Menggunakan propagasi identitas tepercaya dengan aplikasi yang dikelola pelanggan.

Topik

SALL 2.0 dan OAuth 2.0

IAM Identity Center memungkinkan Anda memberi pengguna Anda akses masuk tunggal ke aplikasi SAMP 2.0 atau OAuth 2.0. Topik berikut memberikan ikhtisar tingkat tinggi SAMP 2.0 dan OAuth 2.0.

Topik

SAML 2.0

SAMP 2.0 adalah standar industri yang digunakan untuk bertukar pernyataan SAMP secara aman yang menyampaikan informasi tentang pengguna antara otoritas SAMP (disebut penyedia identitas atau iDP), dan konsumen SAMP 2.0 (disebut penyedia layanan atau SP). IAM Identity Center

menggunakan informasi ini untuk menyediakan akses masuk tunggal federasi bagi pengguna yang berwenang untuk menggunakan aplikasi dalam portal akses. AWS

OAuth 2.0

OAuth 2.0 adalah protokol yang memungkinkan aplikasi mengakses dan berbagi data pengguna dengan aman tanpa berbagi kata sandi. Kemampuan ini menyediakan cara yang aman dan terstandarisasi bagi pengguna untuk memungkinkan aplikasi mengakses sumber daya mereka. Akses difasilitasi oleh aliran hibah OAuth 2.0 yang berbeda. Aliran dasar hibah OAuth 2.0 melibatkan pengguna, aplikasi yang disebut sebagai klien, server otorisasi, dan server sumber daya.

IAM Identity Center mendukung federasi identitas berbasis OAuth 2.0 melalui layanan web OpenID Connect (OIDC). Layanan OIDC memungkinkan aplikasi, seperti AWS CLI, untuk mendaftarkan klien OAuth 2.0 publik. Untuk informasi selengkapnya, lihat Referensi API AWS IAM Identity Center OIDC. Klien terdaftar ini dapat menggunakan hibah OAuth 2.0 yang didukung untuk mendapatkan token akses dan, jika berlaku, token penyegaran setelah pengguna diautentikasi dan diotorisasi. Aplikasi kemudian dapat menggunakan token akses ini untuk mengakses sumber daya yang dilindungi OAuth 2.0, seperti titik akhir API terintegrasi IAM Identity Center, atas nama pengguna. Beberapa hibah OAuth 2.0 juga menyediakan token penyegaran, yang memiliki umur lebih lama dan dapat digunakan untuk menghasilkan token akses baru setelah token akses yang ada kedaluwarsa.

Hibah yang didukung

Spesifikasi kerangka kerja OAuth 2.0 menyediakan jenis hibah yang berbeda untuk mendukung berbagai klien, dan spesifikasi untuk membuat jenis hibah khusus. Jenis hibah mengacu pada cara aplikasi memperoleh token akses. IAM Identity Center saat ini mendukung jenis hibah berikut.

Hibah otorisasi perangkat

IAM Identity Center saat ini mendukung bagian dari Hibah Otorisasi Perangkat OAuth 2.0 (RFC 8628). Layanan OIDC memungkinkan aplikasi untuk mendaftar sebagai klien OAuth dan menggunakan alur hibah otorisasi perangkat untuk menghasilkan token akses untuk mengakses API yang dilindungi IAM Identity Center. Untuk menggunakan hibah ini, aplikasi harus terlebih dahulu mendaftarkan klien publik dengan layanan IAM Identity Center OIDC. Setelah aplikasi terdaftar, layanan OIDC menyediakan aplikasi dengan ID klien dan rahasia klien, yang dapat Anda gunakan untuk menghasilkan token menggunakan hibah otorisasi perangkat.

Ketika aplikasi perlu mengakses sumber daya yang dilindungi di masa depan, aplikasi mengirimkan permintaan ke layanan OIDC untuk memulai otorisasi perangkat. Permintaan ini mengembalikan URL verifikasi dan kode perangkat. Pengguna yang diautentikasi IAM Identity Center perlu menggunakan

kode perangkat ini dan secara eksplisit memberikan akses aplikasi ke sumber daya yang diminta. Setelah pengguna memberikan akses, aplikasi dapat menukar kode perangkat dengan token akses dan token penyegaran.

Cakupan akses

Lingkup mendefinisikan izin tertentu atau hak akses yang diminta klien OAuth dari pengguna atau server otorisasi untuk melakukan tindakan tertentu atau mengakses sumber daya tertentu atas nama pengguna. Cakupan adalah cara bagi server sumber daya untuk mengelompokkan izin yang terkait dengan tindakan dan sumber daya, dan mereka menentukan operasi kasar yang dapat diminta klien.

Klien layanan OIDC menggunakan `scope` nilai seperti yang didefinisikan dalam bagian 3.3 dari OAuth 2.0 (RFC 6749) untuk menentukan hak akses apa yang diminta untuk token akses. Cakupan yang terkait dengan token akses menentukan sumber daya apa yang akan tersedia saat digunakan untuk mengakses sumber daya yang dilindungi seperti API layanan terintegrasi IAM Identity Center.

Anda dapat menentukan maksimum 25 cakupan saat meminta token akses.

Cakupan akses yang didukung oleh layanan IAM Identity Center OIDC saat mendaftarkan klien publik

Cakupan	Deskripsi	Daerah yang didukung	Layanan yang didukung oleh
`sso:account:access`	Akses akun dan set izin yang dikelola Pusat Identitas IAM.	Semua Wilayah didukung oleh IAM Identity Center	Pusat Identitas IAM
`codewhisperer:completions`	Amazon CodeWhisperer untuk mendeteksi kerentanan keamanan dengan menganalisis kode Anda.	AS Timur (Virginia N.) (us-east-1) saja	ID AWS Builder
`codewhisperer:analysis`	Amazon CodeWhisperer untuk menghasilkan saran, dalam kode, berdasarkan kode yang ada dan komentar bahasa alami di IDE Anda.	Hanya US East (Virginia N.)	ID AWS Builder
`codecatalyst:read_write`	Baca dan tulis ke CodeCatalyst sumber daya Amazon Anda,	Hanya US East (Virginia N.)	ID AWS Builder

Cakupan	Deskripsi	Daerah yang didukung	Layanan yang didukung oleh
	memungkinkan akses ke semua sumber daya yang ada.		

Menyiapkan aplikasi SAMP 2.0 yang dikelola pelanggan

Jika Anda menggunakan aplikasi yang dikelola pelanggan yang mendukung SAMP 2.0, Anda dapat menggabungkan IDP Anda ke IAM Identity Center melalui SAMP 2.0 dan menggunakan IAM Identity Center untuk mengelola akses pengguna ke aplikasi tersebut. Anda dapat memilih aplikasi SAMP 2.0 dari katalog aplikasi yang umum digunakan di konsol IAM Identity Center, atau Anda dapat mengatur aplikasi SAMP 2.0 Anda sendiri.

> **Note**
>
> Jika Anda memiliki aplikasi yang dikelola pelanggan yang mendukung OAuth 2.0 dan pengguna Anda memerlukan akses dari aplikasi ini ke AWS layanan, Anda dapat menggunakan propagasi identitas tepercaya. Dengan propagasi identitas tepercaya, pengguna dapat masuk ke aplikasi, dan aplikasi itu dapat meneruskan identitas pengguna dalam permintaan untuk mengakses data dalam AWS layanan. Untuk informasi selengkapnya, lihat Menggunakan propagasi identitas tepercaya dengan aplikasi yang dikelola pelanggan.

Topik

- Katalog aplikasi IAM Identity Center
- Siapkan aplikasi SAFL 2.0 Anda sendiri

Katalog aplikasi IAM Identity Center

Anda dapat menggunakan katalog aplikasi di konsol IAM Identity Center untuk menambahkan banyak aplikasi SAFL 2.0 yang umum digunakan yang bekerja dengan IAM Identity Center. Contohnya termasuk Salesforce, Box, dan Microsoft 365.

Sebagian besar aplikasi memberikan informasi terperinci tentang cara mengatur kepercayaan antara IAM Identity Center dan penyedia layanan aplikasi. Informasi ini tersedia di halaman konfigurasi untuk

aplikasi, setelah Anda memilih aplikasi dalam katalog. Setelah Anda mengkonfigurasi aplikasi, Anda dapat menetapkan akses ke pengguna atau grup di IAM Identity Center sesuai kebutuhan.

Topik

- Siapkan aplikasi dari katalog aplikasi

Siapkan aplikasi dari katalog aplikasi

Gunakan prosedur ini untuk mengatur hubungan kepercayaan SAMP 2.0 antara IAM Identity Center dan penyedia layanan aplikasi Anda.

Sebelum Anda memulai prosedur ini, ada baiknya memiliki file pertukaran metadata penyedia layanan sehingga Anda dapat mengatur kepercayaan dengan lebih efisien. Jika Anda tidak memiliki file ini, Anda masih dapat menggunakan prosedur ini untuk mengonfigurasi kepercayaan secara manual.

Untuk menambah dan mengkonfigurasi aplikasi dari katalog aplikasi

1. Buka konsol Pusat Identitas IAM.
2. Pilih Aplikasi.
3. Pilih tab yang dikelola Pelanggan.
4. Pilih Tambahkan aplikasi.
5. Pada halaman Pilih jenis aplikasi, di bawah Preferensi pengaturan, pilih Saya ingin memilih aplikasi dari katalog.
6. Di bawah Katalog aplikasi, mulailah mengetik nama aplikasi yang ingin Anda tambahkan di kotak pencarian.
7. Pilih nama aplikasi dari daftar saat muncul di hasil pencarian, lalu pilih Berikutnya.
8. Pada halaman Konfigurasi aplikasi, kolom Nama Tampilan dan Deskripsi diisi sebelumnya dengan detail yang relevan untuk aplikasi. Anda dapat mengedit informasi ini.
9. Di bawah metadata IAM Identity Center, lakukan hal berikut:

    a. Di bawah file metadata SAMP Pusat Identitas IAM, pilih Unduh untuk mengunduh metadata penyedia identitas.

    b. Di bawah sertifikat Pusat Identitas IAM, pilih Unduh sertifikat untuk mengunduh sertifikat penyedia identitas.

> **Note**
>
> Anda akan memerlukan file-file ini nanti ketika Anda mengatur aplikasi dari situs web penyedia layanan. Ikuti instruksi dari penyedia itu.

10. (Opsional) Di bawah Properti aplikasi, Anda dapat menentukan URL mulai aplikasi, status Relay, dan Durasi sesi. Untuk informasi selengkapnya, lihat Konfigurasikan properti aplikasi di konsol Pusat Identitas IAM.
11. Di bawah metadata Aplikasi, lakukan salah satu hal berikut:
    a. Jika Anda memiliki file metadata, pilih Unggah file metadata SAMP aplikasi. Kemudian, pilih Pilih file untuk menemukan dan pilih file metadata.
    b. Jika Anda tidak memiliki file metadata, pilih Ketik nilai metadata Anda secara manual, lalu berikan URL ACS Aplikasi dan nilai audiens SAMP Aplikasi.
12. Pilih Kirim. Anda dibawa ke halaman detail aplikasi yang baru saja Anda tambahkan.

Siapkan aplikasi SAFL 2.0 Anda sendiri

Anda dapat mengatur aplikasi Anda sendiri yang memungkinkan federasi identitas menggunakan SAMP 2.0 dan menambahkannya ke IAM Identity Center. Sebagian besar langkah untuk menyiapkan aplikasi SAMP 2.0 Anda sendiri sama dengan menyiapkan aplikasi SAMP 2.0 dari katalog aplikasi di konsol IAM Identity Center. Namun, Anda juga harus menyediakan pemetaan atribut SALL tambahan untuk aplikasi SALL 2.0 Anda sendiri. Pemetaan ini memungkinkan IAM Identity Center untuk mengisi pernyataan SAFL 2.0 dengan benar untuk aplikasi Anda. Anda dapat memberikan pemetaan atribut SALL tambahan ini ketika Anda mengatur aplikasi untuk pertama kalinya. Anda juga dapat memberikan pemetaan atribut SAMP 2.0 pada halaman detail aplikasi di konsol Pusat Identitas IAM.

Gunakan prosedur berikut untuk mengatur hubungan kepercayaan SAMB 2.0 antara IAM Identity Center dan penyedia layanan aplikasi SAMB 2.0 Anda. Sebelum Anda memulai prosedur ini, pastikan Anda memiliki sertifikat penyedia layanan dan file pertukaran metadata sehingga Anda dapat menyelesaikan pengaturan kepercayaan.

Untuk mengatur aplikasi SAFL 2.0 Anda sendiri

1. Buka konsol Pusat Identitas IAM.
2. Pilih Aplikasi.

3. Pilih tab yang dikelola Pelanggan.
4. Pilih Tambahkan aplikasi.
5. Pada halaman Pilih jenis aplikasi, di bawah preferensi Pengaturan, pilih Saya memiliki aplikasi yang ingin saya atur.
6. Di bawah Jenis aplikasi, pilih SAFL 2.0.
7. Pilih Berikutnya.
8. Pada halaman Konfigurasi aplikasi, di bawah Konfigurasi aplikasi, masukkan nama Tampilan untuk aplikasi, seperti**`MyApp`**. Kemudian, masukkan Deskripsi.
9. Di bawah metadata IAM Identity Center, lakukan hal berikut:

    a. Di bawah file metadata SAMP Pusat Identitas IAM, pilih Unduh untuk mengunduh metadata penyedia identitas.

    b. Di bawah sertifikat Pusat Identitas IAM, pilih Unduh untuk mengunduh sertifikat penyedia identitas.

> **Note**
>
> Anda akan memerlukan file-file ini nanti ketika Anda mengatur aplikasi khusus dari situs web penyedia layanan.

10. (Opsional) Di bawah Properti aplikasi, Anda juga dapat menentukan URL mulai aplikasi, status Relay, dan Durasi sesi. Untuk informasi selengkapnya, lihat Konfigurasikan properti aplikasi di konsol Pusat Identitas IAM.
11. Di bawah Metadata aplikasi, pilih Ketik nilai metadata Anda secara manual. Kemudian, berikan URL ACS Aplikasi dan nilai audiens SALL Aplikasi.
12. Pilih Kirim. Anda dibawa ke halaman detail aplikasi yang baru saja Anda tambahkan.

Propagasi identitas tepercaya di seluruh aplikasi

Propagasi identitas tepercaya memberikan pengalaman masuk tunggal yang efisien bagi pengguna alat kueri dan aplikasi intelijen bisnis (BI) yang memerlukan akses ke data dalam layanan. AWS Manajemen akses data didasarkan pada identitas pengguna, sehingga administrator dapat memberikan akses berdasarkan keanggotaan pengguna dan grup yang ada. Akses pengguna ke AWS layanan dan peristiwa lainnya dicatat dalam log khusus layanan dan dalam CloudTrail peristiwa,

sehingga auditor mengetahui tindakan apa yang diambil pengguna dan sumber daya mana yang diakses pengguna.

Dengan propagasi identitas tepercaya, pengguna dapat masuk ke aplikasi, dan aplikasi itu dapat meneruskan identitas pengguna dalam permintaan untuk mengakses data dalam AWS layanan. Karena akses dikelola berdasarkan identitas pengguna, pengguna tidak perlu menggunakan kredensi pengguna lokal basis data atau mengambil peran IAM untuk mengakses data.

Topik

Ikhtisar propagasi identitas tepercaya

Propagasi identitas tepercaya dibangun di atas Kerangka Otorisasi OAuth 2.0, yang memungkinkan aplikasi mengakses dan berbagi data pengguna dengan aman tanpa berbagi kata sandi. OAuth 2.0 menyediakan akses terdelegasi yang aman ke sumber daya aplikasi. Akses didelegasikan karena administrator sumber daya menyetujui, atau mendelegasikan aplikasi tempat pengguna masuk, untuk mengakses aplikasi lain.

Untuk menghindari berbagi kata sandi pengguna, propagasi identitas tepercaya menggunakan token. Token menyediakan cara standar bagi aplikasi tepercaya untuk mengklaim siapa pengguna dan permintaan apa yang diizinkan antara dua aplikasi. AWS aplikasi terkelola yang terintegrasi dengan propagasi identitas tepercaya mendapatkan token dari IAM Identity Center secara langsung. IAM Identity Center juga menyediakan opsi bagi aplikasi untuk bertukar token identitas dan token akses yang berasal dari server otorisasi OAuth 2.0 eksternal. Ini memungkinkan aplikasi untuk mengautentikasi dan mendapatkan token di luar AWS, menukar token dengan token Pusat Identitas IAM, dan menggunakan token baru untuk membuat permintaan ke AWS layanan. Untuk informasi selengkapnya, lihat Menggunakan aplikasi dengan penerbit token tepercaya.

Proses OAuth 2.0 dimulai ketika pengguna masuk ke aplikasi. Aplikasi yang pengguna masuk untuk memulai permintaan untuk mengakses sumber daya aplikasi lain. Aplikasi yang memulai (meminta) dapat mengakses aplikasi penerima atas nama pengguna dengan meminta token dari server otorisasi. Server otorisasi mengembalikan token, dan aplikasi yang memulai meneruskan token itu, dengan permintaan akses, ke aplikasi penerima.

Kasus penggunaan propagasi identitas tepercaya

Sebagai administrator Pusat Identitas IAM, Anda mungkin diminta untuk membantu mengonfigurasi propagasi identitas tepercaya antara aplikasi pemula berikut yang mendukung kemampuan ini dan layanan yang terhubung. AWS Bagian berikut memberikan informasi lebih lanjut tentang kasus penggunaan spesifik yang didukung oleh aplikasi yang dapat memulai propagasi identitas tepercaya.

Topik

- Amazon EMR
- Amazon QuickSight
- Editor Kueri Pergeseran Merah Amazon v2
- Aplikasi intelijen bisnis pihak ketiga
- Aplikasi yang dikembangkan khusus

Amazon EMR

Anda dapat menggunakan Amazon EMR sebagai aplikasi inisiasi untuk kasus penggunaan propagasi identitas tepercaya berikut.

Deskripsi	AWS Layanan lain yang digunakan	Pelajari selengkapnya
Jalankan analisis interaktif dengan Spark di Amazon EMR di kluster Amazon EC2 melalui Amazon EMR Studio. Terapkan kontrol akses berdasarkan identitas tenaga kerja dan atribut terkait untuk AWS Glue Katalog melalui AWS Lake Formation dan Lokasi Amazon S3 melalui Amazon S3 Access Grants.	Amazon EMR di Amazon EC2 diotorisasi melalui, Hibah Akses AWS Lake Formation Amazon S3, Amazon S3	• Integrasikan Amazon EMR dengan IAM Identity Center di Panduan Manajemen EMR Amazon. • Hibah Akses Amazon S3 dan identitas direktori perusahaan di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon. • Menghubungkan AWS Lake Formation dengan Pusat Identitas IAM di Panduan AWS Lake Formation Pengembang

Deskripsi	AWS Layanan lain yang digunakan	Pelajari selengkapnya
Jalankan analisis adhoc dengan Trino di Athena melalui Amazon EMR Studio. Menerapkan kontrol akses berdasarkan identitas tenaga kerja dan atribut terkait untuk AWS Glue Katalog melalui AWS Lake Formation dan isolasi lokasi hasil kueri melalui Amazon S3 Access Grants.	Athena diotorisasi melalui AWS Lake Formation, Hibah Akses Amazon S3	• Integrasikan Amazon EMR dengan IAM Identity Center di Panduan Manajemen EMR Amazon. • Menggunakan Pusat Identitas IAM mengaktifkan grup kerja Athena di Panduan Pengguna Amazon Athena. • Hibah Akses Amazon S3 dan identitas direktori perusahaan di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon. • Menghubungkan AWS Lake Formation dengan Pusat Identitas IAM di Panduan AWS Lake Formation Pengembang. • Bawa identitas tenaga kerja Anda ke Amazon EMR Studio dan Athena di AWS Big Data Blog.

Amazon QuickSight

Anda dapat menggunakan Amazon QuickSight sebagai aplikasi inisiasi untuk kasus penggunaan propagasi identitas tepercaya berikut.

Deskripsi	AWS Layanan lain yang digunakan	Pelajari selengkapnya
QuickSight Pengguna Amazon dapat menanyakan data Amazon	Amazon Redshift	• Hubungkan Redshift dengan IAM Identity Center untuk

Deskripsi	AWS Layanan lain yang digunakan	Pelajari selengkapnya
Redshift. Akses data diberikan di Amazon Redshift oleh administrator Amazon Redshift.		memberi pengguna pengalaman masuk tunggal di Panduan Manajemen Pergeseran Merah Amazon. • Hubungkan Amazon Redshift dengan IAM Identity Center melalui Amazon QuickSight di Panduan Manajemen Amazon Redshift.
Amazon QuickSight dapat menanyakan Amazon Redshift Spectrum untuk data terstruktur di Amazon S3, dengan akses yang diizinkan AWS Lake Formation oleh administrator.	Amazon Redshift, data terstruktur Amazon S3 * Melalui Amazon Redshift Spectrum yang diotorisasi melalui AWS Lake Formation	• Hubungkan Redshift dengan IAM Identity Center untuk memberi pengguna pengalaman masuk tunggal di Panduan Manajemen Pergeseran Merah Amazon. • Hubungkan Amazon Redshift dengan IAM Identity Center melalui Amazon QuickSight di Panduan Manajemen Amazon Redshift. • Menghubungkan AWS Lake Formation dengan Pusat Identitas IAM di Panduan AWS Lake Formation Pengembang. • Sederhanakan manajemen akses dengan Amazon Redshift AWS Lake Formation dan untuk pengguna di Penyedia Identitas Eksternal di Blog Big AWS Data.

Deskripsi	AWS Layanan lain yang digunakan	Pelajari selengkapnya
Amazon QuickSight dapat menanyakan rangkaian data Amazon Redshift untuk data terstruktur di Amazon S3, dengan akses yang diotorisasi oleh administrator. AWS Lake Formation	Datashares Amazon Redshift, data terstruktur Amazon S3 *Diotorisasi melalui AWS Lake Formation	• Hubungkan Amazon Redshift dengan IAM Identity Center melalui Amazon QuickSight di Panduan Manajemen Amazon Redshift. • Menghubungkan AWS Lake Formation dengan Pusat Identitas IAM di Panduan AWS Lake Formation Pengembang. • Sederhanakan manajemen akses dengan Amazon Redshift AWS Lake Formation dan untuk pengguna di Penyedia Identitas Eksternal di Blog Big AWS Data.

Editor Kueri Pergeseran Merah Amazon v2

Anda dapat menggunakan Amazon Redshift Query Editor v2 sebagai aplikasi inisiasi untuk kasus penggunaan propagasi identitas tepercaya berikut.

Deskripsi	AWS Layanan lain yang digunakan	Pelajari selengkapnya
AWS Management Console pengguna dapat menggunakan Amazon Redshift Query Editor v2 untuk menanyakan data Amazon Redshift, dengan akses yang diotorisasi oleh administrator Amazon Redshift.	Amazon Redshift	• Hubungkan Redshift dengan IAM Identity Center untuk memberi pengguna pengalaman masuk tunggal di Panduan Manajemen Pergeseran Merah Amazon. • Connect ke database Amazon Redshift di Panduan Manajemen Amazon Redshift.

Deskripsi	AWS Layanan lain yang digunakan	Pelajari selengkapnya
		• Integrasikan Okta dengan Amazon Redshift Query Editor V2 menggunakan AWS IAM Identity Center Single Sign-on yang mulus di Big Data Blog.AWS
AWS Management Console pengguna dapat menggunakan Amazon Redshift Query Editor v2 untuk menanyakan Amazon Redshift Spectrum untuk data terstruktur di Amazon S3, dengan akses yang diizinkan oleh administrator. AWS Lake Formation	Amazon Redshift, data terstruktur Amazon S3 * Melalui Amazon Redshift Spectrum yang diotorisasi melalui AWS Lake Formation	• Hubungkan Redshift dengan IAM Identity Center untuk memberi pengguna pengalaman masuk tunggal di Panduan Manajemen Pergeseran Merah Amazon. • Connect ke database Amazon Redshift di Panduan Manajemen Amazon Redshift. • Menghubungkan AWS Lake Formation dengan Pusat Identitas IAM di Panduan AWS Lake Formation Pengembang.
AWS Management Console pengguna dapat menggunakan Amazon Redshift Query Editor v2 untuk menanyakan datashares Amazon Redshift untuk data terstruktur di Amazon S3, dengan akses yang diotorisasi oleh administrator. AWS Lake Formation	Datashares Amazon Redshift, data terstruktur Amazon S3 *Diotorisasi melalui AWS Lake Formation	• Connect ke database Amazon Redshift di Panduan Manajemen Amazon Redshift. • Menghubungkan AWS Lake Formation dengan Pusat Identitas IAM di Panduan AWS Lake Formation Pengembang.

Aplikasi intelijen bisnis pihak ketiga

Anda dapat menggunakan aplikasi intelijen bisnis pihak ketiga seperti Tableau, sebagai aplikasi inisiasi untuk kasus penggunaan propagasi identitas tepercaya tertentu. Aplikasi intelijen bisnis pihak ketiga yang dimodifikasi dapat meneruskan driver Amazon Redshift identitas pengguna melalui token identitas OAuth atau token akses, untuk menanyakan data Amazon Redshift, dengan akses yang disahkan oleh administrator Amazon Redshift.

Aplikasi yang dikembangkan khusus

Anda dapat menggunakan aplikasi yang dikembangkan khusus Anda sendiri sebagai aplikasi inisiasi untuk kasus penggunaan propagasi identitas tepercaya berikut.

Deskripsi	AWS Layanan lain yang digunakan	Pelajari selengkapnya
Buat aplikasi yang mengauten tikasi pengguna melalui server otorisasi OIDC, lalu gunakan AWS IAM Identity Center dan IAM untuk mendapatkan kredensi peran IAM yang disempurnakan identitas. Kredensi ini digunakan untuk meminta akses ke data tidak terstruktur di Amazon S3, dengan akses yang diotorisasi oleh administrator Amazon S3 Access Grants.	AWS IAM Identity Center, Amazon S3 data tidak terstruktur * Diotorisasi melalui Hibah Akses Amazon S3	• Hibah Akses Amazon S3 dan identitas direktori perusahaan di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon. • Cara mengembangkan aplikasi data yang dihadapi pengguna dengan IAM Identity Center dan Amazon S3 Access Grants (Bagian 1) dan (Bagian 2) di Blog Penyimpanan.AWS

Siapkan propagasi identitas tepercaya

Propagasi identitas tepercaya mendukung berbagai cara bagi aplikasi untuk mengautentikasi sehingga mereka dapat meneruskan identitas pengguna ke AWS layanan. Pengaturan untuk propagasi identitas tepercaya bervariasi, berdasarkan jenis aplikasi dan bagaimana mereka mengautentikasi.

> **Note**
>
> Anda harus menyiapkan penerbit token tepercaya jika Anda memiliki aplikasi terkelola pelanggan yang meminta akses ke aplikasi AWS terkelola, tetapi tidak menggunakan AWS API untuk terhubung.

Topik

Prasyarat dan pertimbangan

Sebelum Anda mengatur propagasi identitas tepercaya, tinjau prasyarat dan pertimbangan berikut.

Topik

Prasyarat

Untuk menggunakan propagasi identitas tepercaya, pastikan bahwa lingkungan Anda memenuhi prasyarat berikut.

- Penyebaran IAM Identity Center dengan pengguna dan grup yang disediakan

  Untuk menggunakan propagasi identitas tepercaya, Anda harus mengaktifkan Pusat Identitas IAM dan menyediakan pengguna dan grup. Untuk informasi, lihat Memulai tugas-tugas umum di IAM Identity Center.

  Instans organisasi direkomendasikan - Kami menyarankan Anda menggunakan instance organisasi dari IAM Identity Center yang Anda aktifkan di akun manajemen AWS Organizations. Jika Anda berencana untuk menggunakan propagasi identitas tepercaya untuk memungkinkan pengguna mengakses AWS layanan dan sumber daya terkait di Akun AWS dalam organisasi yang sama, Anda dapat mendelegasikan administrasi instans Pusat Identitas IAM Anda ke akun anggota.

Jika Anda berencana untuk menggunakan instans akun tunggal Pusat Identitas IAM, semua AWS layanan dan sumber daya yang Anda ingin pengguna akses melalui propagasi identitas tepercaya harus berada dalam standalone yang sama Akun AWS, atau dalam akun anggota yang sama di organisasi tempat Anda mengaktifkan Pusat Identitas IAM. Untuk informasi selengkapnya, lihat Instans akun Pusat Identitas IAM.

- Untuk aplikasi AWS terkelola; koneksi ke IAM Identity Center

  Untuk menggunakan propagasi identitas tepercaya, aplikasi yang AWS dikelola harus berintegrasi dengan IAM Identity Center.

Pertimbangan tambahan

Ingatlah pertimbangan tambahan berikut untuk menggunakan propagasi identitas tepercaya.

- Jangan mengubah pengaturan Memerlukan tugas untuk aplikasi AWS terkelola

  AWS aplikasi terkelola memiliki konfigurasi pengaturan default yang menentukan apakah penugasan diperlukan untuk pengguna dan grup. Kami menyarankan Anda untuk tidak mengubah pengaturan ini. Meskipun Anda telah mengonfigurasi izin berbutir halus yang memungkinkan pengguna mengakses sumber daya tertentu, mengubah setelan Memerlukan penetapan dapat mengakibatkan perilaku yang tidak terduga, termasuk akses pengguna yang terganggu ke sumber daya ini.
- Izin multi-akun (set izin) tidak diperlukan

  Propagasi identitas tepercaya tidak mengharuskan Anda menyiapkan izin multi-akun (set izin). Anda dapat mengaktifkan IAM Identity Center dan menggunakannya hanya untuk propagasi identitas tepercaya.

Menggunakan propagasi identitas tepercaya dengan aplikasi AWS terkelola

Propagasi identitas tepercaya memungkinkan aplikasi AWS terkelola untuk meminta akses ke data dalam AWS layanan atas nama pengguna. Manajemen akses data didasarkan pada identitas pengguna, sehingga administrator dapat memberikan akses berdasarkan keanggotaan pengguna dan grup yang ada. Identitas pengguna, tindakan yang dilakukan atas nama mereka, dan peristiwa lainnya dicatat dalam log dan CloudTrail peristiwa khusus layanan.

Propagasi identitas tepercaya didasarkan pada standar OAuth 2.0. Untuk menggunakan kemampuan ini, aplikasi yang AWS dikelola harus berintegrasi dengan IAM Identity Center. AWS Layanan analitik mungkin menyediakan antarmuka berbasis driver yang memungkinkan aplikasi yang kompatibel untuk menggunakan propagasi identitas tepercaya. Misalnya, driver JDBC, ODBC, dan Python memungkinkan alat kueri yang kompatibel untuk menggunakan propagasi identitas tepercaya tanpa perlu Anda menyelesaikan langkah penyiapan tambahan.

Topik

Siapkan aplikasi AWS terkelola untuk propagasi identitas tepercaya

AWS Layanan yang mendukung propagasi identitas tepercaya menyediakan antarmuka pengguna administratif dan API yang dapat Anda gunakan untuk mengatur kemampuan ini. Tidak diperlukan konfigurasi dalam IAM Identity Center untuk layanan ini.

Berikut ini adalah proses tingkat tinggi untuk menyiapkan AWS layanan untuk propagasi identitas tepercaya. Langkah-langkah spesifik bervariasi tergantung pada antarmuka administratif dan API yang disediakan oleh aplikasi.

1. Gunakan konsol aplikasi atau API untuk menghubungkan aplikasi ke instans Pusat Identitas IAM

   Gunakan konsol untuk aplikasi AWS terkelola atau API aplikasi untuk menghubungkan aplikasi ke instans Pusat Identitas IAM Anda. Saat Anda menggunakan konsol untuk aplikasi, antarmuka pengguna administratif menyertakan widget yang merampingkan proses penyiapan dan koneksi.
2. Menggunakan konsol aplikasi atau API untuk mengatur akses pengguna ke sumber daya aplikasi

   Selesaikan langkah ini untuk mengotorisasi sumber daya, atau data, yang dapat diakses pengguna. Akses didasarkan pada identitas pengguna atau keanggotaan grup. Model otorisasi bervariasi berdasarkan aplikasi.

> **Important**
>
> Anda harus menyelesaikan langkah ini untuk memungkinkan pengguna mengakses sumber daya AWS layanan. Jika tidak, pengguna tidak dapat mengakses sumber daya, bahkan jika aplikasi yang meminta diizinkan untuk meminta akses ke layanan.

Alur permintaan propagasi identitas tepercaya untuk aplikasi AWS terkelola

Semua aliran propagasi identitas tepercaya ke aplikasi AWS terkelola harus dimulai dengan aplikasi yang memperoleh token dari IAM Identity Center. Token ini diperlukan karena berisi referensi ke pengguna yang dikenal IAM Identity Center dan aplikasi yang terdaftar di IAM Identity Center.

Bagian berikut menjelaskan cara-cara di mana aplikasi AWS terkelola dapat memperoleh token dari IAM Identity Center untuk memulai propagasi identitas tepercaya.

Topik

- Autentikasi Pusat Identitas IAM berbasis web
- Permintaan otentikasi berbasis konsol yang diprakarsai pengguna

Autentikasi Pusat Identitas IAM berbasis web

Untuk alur ini, aplikasi AWS terkelola menyediakan pengalaman masuk tunggal berbasis web menggunakan IAM Identity Center untuk otentikasi.

Saat pengguna membuka aplikasi AWS terkelola, alur masuk tunggal yang menggunakan Pusat Identitas IAM dipicu. Jika tidak ada sesi aktif untuk pengguna di Pusat Identitas IAM, pengguna akan disajikan dengan halaman login berdasarkan sumber identitas yang telah Anda tentukan, dan Pusat Identitas IAM membuat sesi untuk pengguna.

IAM Identity Center menyediakan aplikasi AWS terkelola dengan token yang mencakup identitas pengguna dan daftar audiens (Auds) dan cakupan terkait yang aplikasi terdaftar untuk digunakan. Aplikasi kemudian dapat menggunakan token untuk membuat permintaan ke AWS layanan penerima lainnya.

Permintaan otentikasi berbasis konsol yang diprakarsai pengguna

Untuk alur ini, aplikasi AWS terkelola memberikan pengalaman konsol yang dimulai pengguna.

Dalam hal ini, aplikasi AWS terkelola dimasukkan dari Konsol AWS Manajemen setelah mengambil peran. Agar aplikasi mendapatkan token, pengguna harus memulai proses untuk memicu aplikasi untuk mengautentikasi pengguna. Ini memulai otentikasi menggunakan IAM Identity Center, yang akan mengarahkan pengguna ke sumber identitas yang telah Anda konfigurasi.

Setelah aplikasi memperoleh token

Setelah aplikasi yang meminta memperoleh token dari IAM Identity Center, aplikasi secara berkala menyegarkan token, yang dapat digunakan untuk masa pakai sesi pengguna. Selama waktu ini, aplikasi mungkin:

- Dapatkan informasi lebih lanjut tentang token untuk menentukan siapa pengguna dan cakupan mana yang dapat digunakan aplikasi dengan aplikasi AWS terkelola penerima lainnya.
- Berikan token dalam panggilan ke aplikasi AWS terkelola penerima lainnya yang mendukung penggunaan token.
- Dapatkan sesi peran IAM yang disempurnakan identitas yang dapat digunakan untuk membuat permintaan ke aplikasi AWS terkelola lainnya yang menggunakan AWS Signature Version 4.

  Sesi peran IAM yang ditingkatkan identitas adalah sesi peran IAM yang berisi identitas propagasi pengguna yang disimpan dalam token yang dibuat oleh IAM Identity Center.

Sesi peran IAM yang ditingkatkan identitas

AWS Security Token Service Ini memungkinkan aplikasi untuk mendapatkan sesi peran IAM yang ditingkatkan identitas. AWS aplikasi terkelola yang mendukung konteks pengguna dalam sesi peran dapat menggunakan informasi identitas untuk mengotorisasi akses berdasarkan pengguna yang berada dalam sesi peran. Konteks baru ini memungkinkan aplikasi untuk membuat permintaan ke aplikasi AWS terkelola yang mendukung propagasi identitas tepercaya melalui permintaan API Versi AWS Tanda Tangan 4.

Ketika aplikasi AWS terkelola menggunakan sesi peran IAM yang disempurnakan identitas untuk mengakses sumber daya, CloudTrail mencatat identitas pengguna (User-ID), sesi inisiasi, dan tindakan yang diambil.

Ketika aplikasi membuat permintaan menggunakan sesi peran IAM yang disempurnakan identitas ke aplikasi penerima, itu menambahkan konteks ke sesi sehingga aplikasi penerima dapat mengotorisasi akses berdasarkan identitas pengguna atau keanggotaan grup, atau peran IAM. Menerima aplikasi yang mendukung propagasi identitas tepercaya akan mengembalikan kesalahan

jika aplikasi penerima atau sumber daya yang diminta tidak dikonfigurasi untuk mengotorisasi akses berdasarkan identitas pengguna atau keanggotaan grup.

Untuk menghindari masalah ini, lakukan salah satu hal berikut:

- Verifikasi bahwa aplikasi penerima terhubung ke Pusat Identitas IAM.
- Gunakan konsol untuk aplikasi penerima atau API aplikasi untuk menyiapkan aplikasi guna mengotorisasi akses ke sumber daya berdasarkan identitas pengguna atau keanggotaan grup. Persyaratan pengaturan untuk ini bervariasi berdasarkan aplikasi.

Untuk informasi selengkapnya, lihat dokumentasi untuk aplikasi AWS terkelola penerima.

Jenis sesi peran IAM yang ditingkatkan identitas

Aplikasi memperoleh sesi peran IAM yang disempurnakan identitas dengan membuat permintaan ke AWS STS `AssumeRole` API dan meneruskan pernyataan konteks dalam parameter permintaan. `ProvidedContexts` `AssumeRole` Pernyataan konteks diperoleh dari `idToken` klaim yang tersedia dalam tanggapan dari permintaan. `SSO OIDC` `CreateTokenWithIAM`

AWS STS dapat membuat dua jenis sesi peran IAM yang ditingkatkan identitas, tergantung pada pernyataan konteks yang diberikan pada permintaan: `AssumeRole`

- Sesi yang hanya mencatat identitas pengguna CloudTrail.
- Sesi yang memungkinkan otorisasi berdasarkan identitas pengguna yang disebarkan dan log ke. CloudTrail

Untuk mendapatkan sesi peran IAM yang ditingkatkan identitas dari AWS STS yang hanya menyediakan informasi audit yang terdaftar dalam CloudTrail jejak, berikan nilai klaim atas permintaan tersebut`sts:audit_context`. `AssumeRole` Untuk mendapatkan sesi yang juga memungkinkan AWS layanan penerima untuk memberi wewenang kepada pengguna Pusat Identitas IAM untuk melakukan suatu tindakan, berikan nilai `sts:identity_context` klaim atas permintaan tersebut`AssumeRole`. Anda hanya dapat memberikan satu konteks.

Sesi peran IAM yang ditingkatkan identitas dibuat dengan **`sts:audit_context`**

Ketika permintaan dibuat ke AWS layanan menggunakan sesi peran IAM yang disempurnakan identitas yang dibuat dengan`sts:audit_context`, Pusat Identitas IAM pengguna `userId` dicatat dalam elemen. CloudTrail `OnBehalfOf`

```
"userIdentity": {
      "type": "AssumedRole",
      "principalId": "AROAEXAMPLE:MyRole",
      "arn": "arn:aws:sts::111111111111:assumed-role/MyRole/MySession",
      "accountId": "111111111111",
      "accessKeyId": "ASIAEXAMPLE",
      "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "AROAEXAMPLE",
            "arn": "arn:aws:iam::111111111111:role/MyRole",
            "accountId": "111111111111",
            "userName": "MyRole"
        },
        "attributes": {
            "creationDate": "2023-12-12T13:55:22Z",
            "mfaAuthenticated": "false"
        }
    },
    "onBehalfOf": {
        "userId": "11111111-1111-1111-1111-1111111111",
        "identityStoreArn": "arn:aws:identitystore::111111111111:identitystore/
d-111111111"
    }
}
```

> **Note**
>
> Sesi ini tidak dapat digunakan untuk mengotorisasi pengguna Pusat Identitas. Mereka masih dapat digunakan untuk mengotorisasi peran IAM.

Untuk mendapatkan jenis sesi peran ini AWS STS, berikan nilai `sts:audit_context` bidang ke `AssumeRole` permintaan dalam parameter `ProvidedContexts` permintaan. Gunakan `arn:aws:iam::aws:contextProvider/IdentityStore` sebagai nilai untuk`ProviderArn`.

Sesi peran IAM yang ditingkatkan identitas dibuat dengan **`sts:identity_context`**

Ketika pengguna membuat permintaan ke AWS layanan menggunakan sesi peran IAM yang disempurnakan identitas yang dibuat dengan`sts:identity_context`, Pusat Identitas IAM

pengguna `userId` dicatat CloudTrail dalam `onBehalfOf` elemen dengan cara yang sama seperti sesi yang dibuat dengan. `sts:audit_context`

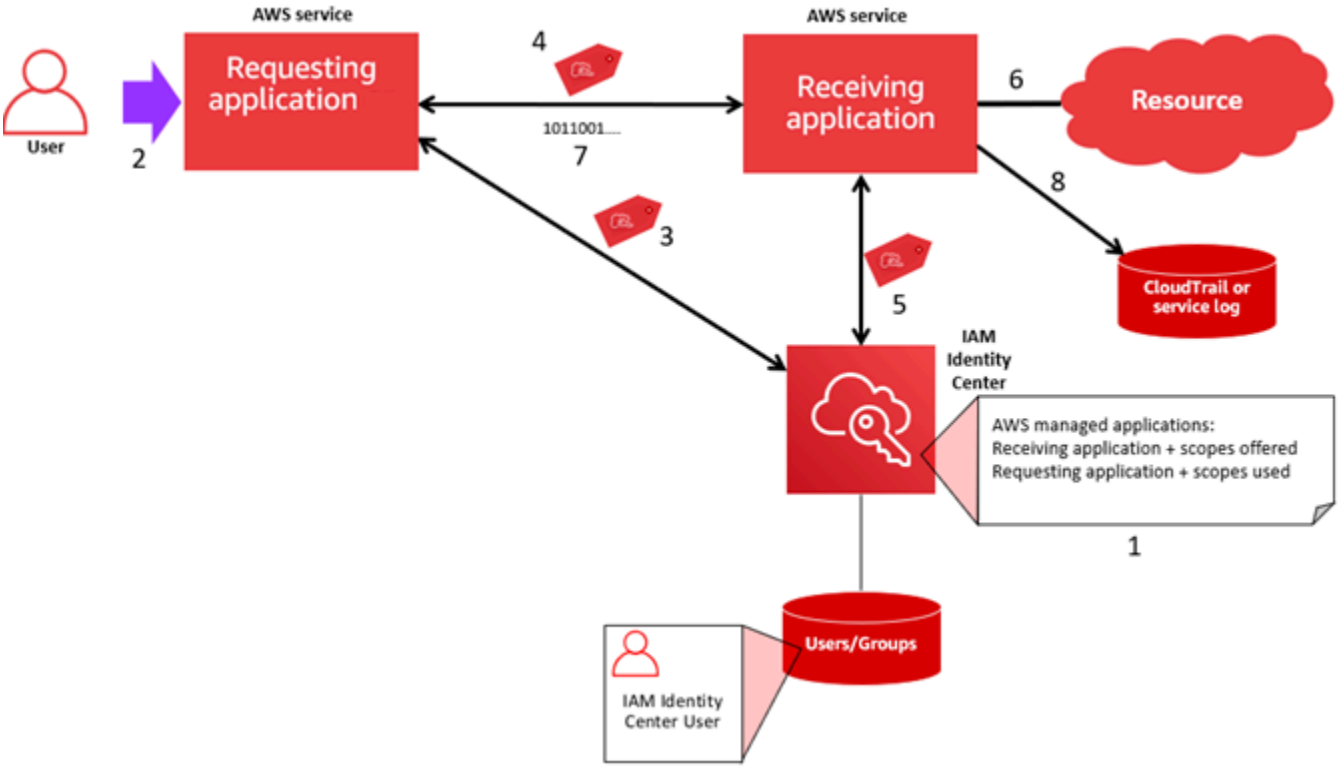
Selain mencatat pengguna IAM Identity Center CloudTrail, jenis sesi ini juga digunakan oleh API yang didukung untuk mengotorisasi tindakan berdasarkan identitas pengguna yang disebarkan. `userId` Untuk daftar tindakan IAM untuk API yang didukung, lihat kebijakan `AWSIAMIdentityCenterAllowListForIdentityContext` AWS terkelola. Kebijakan AWS terkelola ini disediakan sebagai kebijakan sesi saat sesi peran IAM yang ditingkatkan identitas dibuat dengan. `sts:identity_context` Kebijakan ini mencegah Anda menggunakan sesi peran dengan AWS layanan yang tidak didukung.

Untuk mendapatkan jenis sesi peran ini AWS STS, berikan nilai `sts:identity_context` bidang ke `AssumeRole` permintaan dalam parameter `ProvidedContexts` permintaan. Gunakan `arn:aws:iam::aws:contextProvider/IdentityStore` sebagai nilai untuk`ProviderArn`.

Proses penyiapan dan alur permintaan untuk aplikasi AWS terkelola

Bagian ini menjelaskan proses penyiapan dan alur permintaan untuk aplikasi AWS terkelola yang menggunakan propagasi identitas tepercaya dan yang memberikan pengalaman masuk tunggal berbasis web.

Diagram berikut memberikan gambaran umum tentang proses ini.



Langkah-langkah berikut memberikan informasi tambahan tentang proses ini.

1. Gunakan konsol untuk aplikasi AWS terkelola atau API aplikasi untuk melakukan hal berikut:
   a. Connect aplikasi ke instans IAM Identity Center Anda.
   b. Siapkan izin untuk mengotorisasi sumber daya aplikasi mana yang dapat diakses pengguna.
2. Alur permintaan dimulai ketika pengguna membuka aplikasi AWS terkelola yang dapat meminta akses ke sumber daya (aplikasi yang meminta).
3. Untuk mendapatkan token untuk mengakses aplikasi AWS terkelola penerima, aplikasi AWS terkelola yang meminta memulai permintaan masuk ke Pusat Identitas IAM.

   Jika pengguna tidak masuk, IAM Identity Center akan memicu alur autentikasi pengguna ke sumber identitas yang telah Anda tentukan. Ini menciptakan sesi portal AWS akses baru untuk pengguna dengan durasi yang Anda konfigurasikan di IAM Identity Center. IAM Identity Center kemudian menghasilkan token yang terkait dengan sesi, dan aplikasi dapat beroperasi selama durasi sesi portal AWS akses pengguna yang tersisa. Jika pengguna keluar dari aplikasi mereka, atau jika Anda menghapus sesi mereka, sesi secara otomatis berakhir dalam waktu dua jam.
4. Aplikasi yang AWS dikelola memulai permintaan ke aplikasi penerima dan menyediakan tokennya.
5. Aplikasi penerima melakukan panggilan ke IAM Identity Center untuk mendapatkan identitas pengguna dan cakupan yang dikodekan dalam token. Aplikasi penerima juga dapat membuat permintaan untuk mendapatkan atribut pengguna atau keanggotaan grup pengguna dari direktori Pusat Identitas.
6. Aplikasi penerima menggunakan konfigurasi otorisasi untuk menentukan apakah pengguna berwenang untuk mengakses sumber daya aplikasi yang diminta.
7. Jika pengguna berwenang untuk mengakses sumber daya aplikasi yang diminta, aplikasi penerima menanggapi permintaan tersebut.
8. Identitas pengguna, tindakan yang dilakukan atas nama mereka, dan peristiwa lain yang dicatat dalam log dan AWS CloudTrail peristiwa aplikasi penerima. Cara spesifik di mana informasi ini dicatat bervariasi berdasarkan aplikasi.

Menggunakan propagasi identitas tepercaya dengan aplikasi yang dikelola pelanggan

Propagasi identitas tepercaya memungkinkan aplikasi yang dikelola pelanggan untuk meminta akses ke data dalam AWS layanan atas nama pengguna. Manajemen akses data didasarkan pada identitas pengguna, sehingga administrator dapat memberikan akses berdasarkan keanggotaan pengguna

dan grup yang ada. Identitas pengguna, tindakan yang dilakukan atas nama mereka, dan peristiwa lainnya dicatat dalam log dan CloudTrail peristiwa khusus layanan.

Dengan propagasi identitas tepercaya, pengguna dapat masuk ke aplikasi yang dikelola pelanggan, dan aplikasi itu dapat meneruskan identitas pengguna dalam permintaan untuk mengakses data dalam AWS layanan.

> **Important**
>
> Untuk mengakses AWS layanan, aplikasi yang dikelola pelanggan harus mendapatkan token dari penerbit token tepercaya, yang berada di luar Pusat Identitas IAM. Penerbit token tepercaya adalah server otorisasi OAuth 2.0 yang membuat token yang ditandatangani. Token ini mengotorisasi aplikasi yang memulai permintaan akses ke AWS layanan (menerima aplikasi). Untuk informasi selengkapnya, lihat Menggunakan aplikasi dengan penerbit token tepercaya.

Topik

Siapkan aplikasi OAuth 2.0 yang dikelola pelanggan untuk propagasi identitas tepercaya

Untuk menyiapkan aplikasi OAuth 2.0 yang dikelola pelanggan untuk propagasi identitas tepercaya, Anda harus terlebih dahulu menambahkannya ke IAM Identity Center. Gunakan prosedur berikut untuk menambahkan aplikasi Anda ke IAM Identity Center.

Topik

Langkah 1: Pilih jenis aplikasi

1. Buka konsol Pusat Identitas IAM.

2. Pilih Aplikasi.
3. Pilih tab yang dikelola Pelanggan.
4. Pilih Tambahkan aplikasi.
5. Pada halaman Pilih jenis aplikasi, di bawah preferensi Pengaturan, pilih Saya memiliki aplikasi yang ingin saya atur.
6. Di bawah Jenis aplikasi, pilih OAuth 2.0.
7. Pilih Berikutnya untuk melanjutkan ke halaman berikutnya,Langkah 2: Tentukan detail aplikasi.

Langkah 2: Tentukan detail aplikasi

1. Pada halaman Tentukan detail aplikasi, di bawah Nama dan deskripsi aplikasi, masukkan nama Tampilan untuk aplikasi, seperti**`MyApp`**. Kemudian, masukkan Deskripsi.
2. Di bawah Metode penetapan pengguna dan grup, pilih salah satu opsi berikut:

   - Memerlukan tugas - Izinkan hanya pengguna dan grup Pusat Identitas IAM yang ditugaskan ke aplikasi ini untuk mengakses aplikasi.

     Visibilitas ubin aplikasi —Hanya pengguna yang ditugaskan ke aplikasi secara langsung atau melalui penugasan grup yang dapat melihat ubin aplikasi di portal AWS akses, asalkan visibilitas Aplikasi di portal AWS akses diatur ke Visible.
   - Tidak memerlukan tugas - Izinkan semua pengguna dan grup Pusat Identitas IAM yang berwenang untuk mengakses aplikasi ini.

     Visibilitas ubin aplikasi — Ubin aplikasi terlihat oleh semua pengguna yang masuk ke portal AWS akses, kecuali visibilitas Aplikasi di portal AWS akses diatur ke Tidak terlihat.
3. Di bawah portal AWS akses, masukkan URL tempat pengguna dapat mengakses aplikasi dan menentukan apakah ubin aplikasi akan terlihat atau tidak terlihat di portal AWS akses. Jika Anda memilih Tidak terlihat, bahkan pengguna yang ditetapkan tidak dapat melihat ubin aplikasi.
4. Di bawah Tag (opsional), pilih Tambahkan tag baru, lalu tentukan nilai untuk Kunci dan Nilai (opsional).

   Untuk informasi tentang tanda, lihat Penandaan pada sumber daya AWS IAM Identity Center.
5. Pilih Berikutnya, dan lanjutkan ke halaman berikutnya,Langkah 3: Tentukan pengaturan otentikasi.

Langkah 3: Tentukan pengaturan otentikasi

Untuk menambahkan aplikasi terkelola pelanggan yang mendukung OAuth 2.0 ke IAM Identity Center, Anda harus menentukan penerbit token tepercaya. Penerbit token tepercaya adalah server otorisasi OAuth 2.0 yang membuat token yang ditandatangani. Token ini mengotorisasi aplikasi yang memulai permintaan (meminta aplikasi) untuk akses ke aplikasi yang AWS dikelola (menerima aplikasi).

1. Pada halaman Tentukan pengaturan otentikasi, di bawah Penerbit token tepercaya, lakukan salah satu hal berikut:

   - Untuk menggunakan penerbit token tepercaya yang ada:

     Pilih kotak centang di samping nama penerbit token tepercaya yang ingin Anda gunakan.

   - Untuk menambahkan penerbit token tepercaya baru:

     1. Pilih Buat penerbit token tepercaya.
     2. Tab browser baru terbuka. Ikuti langkah 5 hingga 8 inciCara menambahkan penerbit token tepercaya ke konsol IAM Identity Center.
     3. Setelah Anda menyelesaikan langkah-langkah ini, kembali ke jendela browser yang Anda gunakan untuk pengaturan aplikasi Anda dan pilih penerbit token tepercaya yang baru saja Anda tambahkan.
     4. Dalam daftar penerbit token tepercaya, pilih kotak centang di sebelah nama penerbit token tepercaya yang baru saja Anda tambahkan.

        Setelah Anda memilih penerbit token tepercaya, bagian Konfigurasikan penerbit token tepercaya yang dipilih akan muncul.

2. Di bawah Konfigurasi penerbit token tepercaya yang dipilih, masukkan klaim Aud. Klaim Aud mengidentifikasi audiens yang dituju (penerima) untuk token yang dihasilkan oleh penerbit token tepercaya. Untuk informasi selengkapnya, lihat Klaim Aud.
3. Untuk mencegah pengguna Anda mengautentikasi ulang saat mereka menggunakan aplikasi ini, pilih Segarkan otentikasi pengguna secara otomatis untuk sesi aplikasi aktif. Saat dipilih, opsi ini menyegarkan token akses untuk sesi setiap 60 menit, hingga sesi berakhir atau pengguna mengakhiri sesi.
4. Pilih Berikutnya, dan lanjutkan ke halaman berikutnya,Langkah 4: Tentukan kredensil aplikasi.

Langkah 4: Tentukan kredensil aplikasi

Selesaikan langkah-langkah dalam prosedur ini untuk menentukan kredensil yang digunakan aplikasi Anda untuk melakukan tindakan pertukaran token dengan aplikasi tepercaya. Kredensi ini digunakan dalam kebijakan berbasis sumber daya. Kebijakan tersebut mengharuskan Anda menentukan prinsipal yang memiliki izin untuk melakukan tindakan yang ditentukan dalam kebijakan. Anda harus menentukan prinsipal, bahkan jika aplikasi tepercaya sama Akun AWS.

> **Note**
>
> Saat Anda menetapkan izin dengan kebijakan, berikan hanya izin yang diperlukan untuk melakukan tugas. Anda melakukan ini dengan menentukan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, juga dikenal sebagai izin hak akses paling rendah.

Kebijakan ini membutuhkan `sso-oauth:CreateTokenWithIAM` tindakan.

1. Pada halaman Specify application credentials, lakukan salah satu hal berikut:

   - Untuk menentukan satu atau lebih peran IAM dengan cepat:
     1. Pilih Masukkan satu atau beberapa peran IAM.
     2. Di bawah Masukkan peran IAM, tentukan Nama Sumber Daya Amazon (ARN) dari peran IAM yang ada. Untuk menentukan ARN, gunakan sintaks berikut. Bagian Wilayah ARN kosong karena sumber daya IAM bersifat global.

        ```
        arn:aws:iam::account:role/role-name-with-path
        ```

        Untuk informasi selengkapnya, lihat Akses lintas akun menggunakan kebijakan berbasis sumber daya dan ARN IAM di Panduan Pengguna.AWS Identity and Access Management
   - Untuk mengedit kebijakan secara manual (diperlukan jika Anda menentukan AWS non-kredensional):
     1. Pilih Edit kebijakan aplikasi.
     2. Ubah kebijakan Anda dengan mengetik atau menempelkan teks di kotak teks JSON.
     3. Mengatasi peringatan keamanan, kesalahan, atau peringatan umum yang dihasilkan selama validasi kebijakan. Untuk informasi selengkapnya, lihat Memvalidasi kebijakan IAM di AWS Identity and Access Management Panduan Pengguna.

2. Pilih Berikutnya dan lanjutkan ke halaman berikutnyaLangkah 5: Tinjau dan konfigurasikan.

Langkah 5: Tinjau dan konfigurasikan

1. Pada halaman Tinjau dan konfigurasi, tinjau pilihan yang Anda buat. Untuk membuat perubahan, pilih bagian konfigurasi yang Anda inginkan, pilih Edit, lalu buat perubahan yang diperlukan.
2. Setelah selesai, pilih Tambah aplikasi.
3. Aplikasi yang Anda tambahkan muncul di daftar aplikasi yang dikelola Pelanggan.
4. Setelah menyiapkan aplikasi yang dikelola pelanggan di IAM Identity Center, Anda harus menentukan satu atau beberapa AWS layanan, atau aplikasi tepercaya, untuk propagasi identitas. Ini memungkinkan pengguna untuk masuk ke aplikasi yang dikelola pelanggan Anda dan mengakses data di aplikasi tepercaya.

   Untuk informasi selengkapnya, lihat Tentukan aplikasi tepercaya .

Tentukan aplikasi tepercaya

Setelah menyiapkan aplikasi yang dikelola pelanggan, Anda harus menentukan satu atau lebih AWS layanan tepercaya, atau aplikasi tepercaya, untuk propagasi identitas. Tentukan AWS layanan yang memiliki data yang perlu diakses oleh pengguna aplikasi yang dikelola pelanggan Anda. Ketika pengguna Anda masuk ke aplikasi yang dikelola pelanggan Anda, aplikasi itu akan meneruskan identitas pengguna Anda ke aplikasi tepercaya.

Gunakan prosedur berikut untuk memilih layanan, dan kemudian tentukan aplikasi individual untuk dipercaya untuk layanan itu.

1. Buka konsol Pusat Identitas IAM.
2. Pilih Aplikasi.
3. Pilih tab yang dikelola Pelanggan.
4. Dalam daftar aplikasi yang dikelola Pelanggan, pilih aplikasi OAuth 2.0 yang ingin Anda mulai permintaan akses. Ini adalah aplikasi tempat pengguna Anda masuk.
5. Pada halaman Detail, di bawah Aplikasi tepercaya untuk propagasi identitas, pilih Tentukan aplikasi tepercaya.
6. Di bawah Jenis pengaturan, pilih Aplikasi individual dan tentukan akses, lalu pilih Berikutnya.
7. Pada halaman Pilih layanan, pilih AWS layanan yang memiliki aplikasi yang dapat dipercaya oleh aplikasi yang dikelola pelanggan Anda untuk propagasi identitas, lalu pilih Berikutnya.

Layanan yang Anda pilih mendefinisikan aplikasi yang dapat dipercaya. Anda akan memilih aplikasi di langkah berikutnya.

8. Pada halaman Pilih aplikasi, pilih Aplikasi individual, pilih kotak centang untuk setiap aplikasi yang dapat menerima permintaan akses, lalu pilih Berikutnya.
9. Pada halaman Configure access, di bawah metode Configuration, lakukan salah satu hal berikut:
   - Pilih akses per aplikasi — Pilih opsi ini untuk mengonfigurasi tingkat akses yang berbeda untuk setiap aplikasi. Pilih aplikasi yang ingin Anda konfigurasikan tingkat aksesnya, lalu pilih Edit akses. Di Tingkat akses untuk diterapkan, ubah tingkat akses sesuai kebutuhan, lalu pilih Simpan perubahan.
   - Terapkan tingkat akses yang sama ke semua aplikasi — Pilih opsi ini jika Anda tidak perlu mengonfigurasi tingkat akses per aplikasi.
10. Pilih Berikutnya.
11. Pada halaman konfigurasi Tinjauan, tinjau pilihan yang Anda buat. Untuk membuat perubahan, pilih bagian konfigurasi yang Anda inginkan, pilih Edit akses, lalu buat perubahan yang diperlukan.
12. Setelah selesai, pilih aplikasi Trust.

Menggunakan aplikasi dengan penerbit token tepercaya

Penerbit token tepercaya memungkinkan Anda menggunakan propagasi identitas tepercaya dengan aplikasi yang mengautentikasi di luar. AWS Dengan penerbit token tepercaya, Anda dapat mengotorisasi aplikasi ini untuk membuat permintaan atas nama pengguna mereka untuk mengakses aplikasi AWS terkelola.

Topik berikut menjelaskan cara kerja penerbit token tepercaya dan memberikan panduan penyiapan.

Topik

Ikhtisar penerbit token tepercaya

Propagasi identitas tepercaya menyediakan mekanisme yang memungkinkan aplikasi yang mengautentikasi di luar AWS untuk membuat permintaan atas nama penggunanya dengan menggunakan penerbit token tepercaya. Penerbit token tepercaya adalah server otorisasi OAuth 2.0 yang membuat token yang ditandatangani. Token ini mengotorisasi aplikasi yang memulai permintaan (meminta aplikasi) untuk akses ke AWS layanan (menerima aplikasi). Meminta aplikasi memulai permintaan akses atas nama pengguna yang diautentikasi oleh penerbit token tepercaya. Pengguna diketahui oleh penerbit token tepercaya dan Pusat Identitas IAM.

AWS layanan yang menerima permintaan mengelola otorisasi berbutir halus ke sumber daya mereka berdasarkan pengguna dan keanggotaan grup mereka sebagaimana diwakili dalam direktori Pusat Identitas. AWS layanan tidak dapat menggunakan token dari penerbit token eksternal secara langsung.

Untuk mengatasi hal ini, IAM Identity Center menyediakan cara bagi aplikasi yang meminta, atau AWS driver yang digunakan aplikasi yang meminta, untuk menukar token yang dikeluarkan oleh penerbit token tepercaya dengan token yang dihasilkan oleh IAM Identity Center. Token yang dihasilkan oleh IAM Identity Center mengacu pada pengguna IAM Identity Center yang sesuai. Aplikasi yang meminta, atau driver, menggunakan token baru untuk memulai permintaan ke aplikasi penerima. Karena token baru mereferensikan pengguna terkait di Pusat Identitas IAM, aplikasi penerima dapat mengotorisasi akses yang diminta berdasarkan pengguna atau keanggotaan grup mereka sebagaimana diwakili dalam Pusat Identitas IAM.

> **Important**
>
> Memilih server otorisasi OAuth 2.0 untuk ditambahkan sebagai penerbit token tepercaya adalah keputusan keamanan yang memerlukan pertimbangan cermat. Hanya pilih penerbit token tepercaya yang Anda percayai untuk melakukan tugas-tugas berikut:
>
> - Otentikasi pengguna yang ditentukan dalam token.
> - Otorisasi akses pengguna tersebut ke aplikasi penerima.
> - Hasilkan token yang dapat ditukar oleh IAM Identity Center dengan token yang dibuat IAM Identity Center.

Prasyarat dan pertimbangan untuk emiten token tepercaya

Sebelum Anda menyiapkan penerbit token tepercaya, tinjau prasyarat dan pertimbangan berikut.

- Konfigurasi penerbit token tepercaya

  Anda harus mengonfigurasi server otorisasi OAuth 2.0 (penerbit token tepercaya). Meskipun penerbit token tepercaya biasanya penyedia identitas yang Anda gunakan sebagai sumber identitas Anda untuk IAM Identity Center, itu tidak harus demikian. Untuk informasi tentang cara menyiapkan penerbit token tepercaya, lihat dokumentasi untuk penyedia identitas yang relevan.

  > **Note**
  >
  > Anda dapat mengonfigurasi hingga 10 penerbit token tepercaya untuk digunakan dengan IAM Identity Center, selama Anda memetakan identitas setiap pengguna di penerbit token tepercaya ke pengguna yang sesuai di IAM Identity Center.

- Server otorisasi OAuth 2.0 (penerbit token tepercaya) yang membuat token harus memiliki titik akhir penemuan OpenID Connect (OIDC) yang dapat digunakan IAM Identity Center untuk mendapatkan kunci publik guna memverifikasi tanda tangan token. Untuk informasi selengkapnya, lihat URL titik akhir penemuan OIDC (URL penerbit).
- Token yang dikeluarkan oleh penerbit token tepercaya

  Token dari penerbit token tepercaya harus memenuhi persyaratan berikut:

  - Token harus ditandatangani dan dalam format JSON Web Token (JWT) menggunakan algoritma RS256.
  - Token harus berisi klaim berikut:
    - Penerbit (iss) — Entitas yang mengeluarkan token. Nilai ini harus sesuai dengan nilai yang dikonfigurasi di titik akhir penemuan OIDC (URL penerbit) di penerbit token tepercaya.
    - Subjek (sub) - Pengguna yang diautentikasi.
    - Audiens (aud) — Penerima token yang dituju. Ini adalah AWS layanan yang akan diakses setelah token ditukar dengan token dari IAM Identity Center. Untuk informasi selengkapnya, lihat Klaim Aud.
    - Waktu Kedaluwarsa (exp) — Waktu setelah token kedaluwarsa.
    -
  - Token dapat berupa token identitas atau token akses.
  - Token harus memiliki atribut yang dapat dipetakan secara unik ke satu pengguna IAM Identity Center.
- Klaim opsional

IAM Identity Center mendukung semua klaim opsional yang didefinisikan dalam RFC 7523. Untuk informasi lebih lanjut, lihat Bagian 3: Format JWT dan Persyaratan Pemrosesan RFC ini.

Misalnya, token dapat berisi klaim JTI (JWT ID). Klaim ini, jika ada, mencegah token yang memiliki JTI yang sama digunakan kembali untuk pertukaran token. Untuk informasi lebih lanjut tentang klaim JTI, lihatRincian klaim JTI.

- Konfigurasi IAM Identity Center untuk bekerja dengan penerbit token tepercaya

  Anda juga harus mengaktifkan Pusat Identitas IAM, mengonfigurasi sumber identitas untuk Pusat Identitas IAM, dan menyediakan pengguna yang sesuai dengan pengguna di direktori penerbit token tepercaya.

  Untuk melakukan ini, Anda harus melakukan salah satu dari yang berikut:

  - Sinkronisasi pengguna ke IAM Identity Center dengan menggunakan protokol System for Cross-domain Identity Management (SCIM) 2.0.
  - Buat pengguna langsung di IAM Identity Center.

> **Note**
>
> Penerbit token tepercaya tidak didukung jika Anda menggunakan Layanan Domain Direktori Aktif sebagai sumber identitas Anda.

Rincian klaim JTI

Jika IAM Identity Center menerima permintaan untuk menukar token yang telah dipertukarkan oleh IAM Identity Center, permintaan gagal. Untuk mendeteksi dan mencegah penggunaan kembali token untuk pertukaran token, Anda dapat menyertakan klaim JTI. IAM Identity Center melindungi terhadap pemutaran ulang token berdasarkan klaim dalam token.

Tidak semua server otorisasi OAuth 2.0 menambahkan klaim JTI ke token. Beberapa server otorisasi OAuth 2.0 mungkin tidak mengizinkan Anda menambahkan JTI sebagai klaim khusus. Server otorisasi OAuth 2.0 yang mendukung penggunaan klaim JTI dapat menambahkan klaim ini hanya ke token identitas, token akses saja, atau keduanya. Untuk informasi selengkapnya, lihat dokumentasi untuk server otorisasi OAuth 2.0 Anda.

Untuk informasi tentang membangun aplikasi yang bertukar token, lihat dokumentasi API Pusat Identitas IAM. Untuk informasi tentang mengonfigurasi aplikasi yang dikelola pelanggan untuk mendapatkan dan menukar token yang benar, lihat dokumentasi untuk aplikasi tersebut.

Pengaturan konfigurasi penerbit token tepercaya

Bagian berikut menjelaskan pengaturan yang diperlukan untuk mengatur dan menggunakan penerbit token tepercaya.

Topik

URL titik akhir penemuan OIDC (URL penerbit)

Saat menambahkan penerbit token tepercaya ke konsol Pusat Identitas IAM, Anda harus menentukan URL titik akhir penemuan OIDC. URL ini biasanya disebut dengan URL relatifnya,`/.well-known/openid-configuration`. Di konsol IAM Identity Center, URL ini disebut URL penerbit.

> **Note**
>
> Anda harus menempelkan URL titik akhir penemuan hingga dan tanpa`.well-known/openid-configuration`. Jika `.well-known/openid-configuration` disertakan dalam URL, konfigurasi penerbit token tepercaya tidak akan berfungsi. Karena IAM Identity Center tidak memvalidasi URL ini, jika URL tidak dibentuk dengan benar, penyiapan penerbit token tepercaya akan gagal tanpa pemberitahuan.

IAM Identity Center menggunakan URL ini untuk mendapatkan informasi tambahan tentang penerbit token tepercaya. Misalnya, IAM Identity Center menggunakan URL ini untuk mendapatkan informasi yang diperlukan untuk memverifikasi token yang dihasilkan oleh penerbit token tepercaya. Saat Anda menambahkan penerbit token tepercaya ke Pusat Identitas IAM, Anda harus menentukan URL ini. Untuk menemukan URL, lihat dokumentasi untuk penyedia server otorisasi OAuth 2.0 yang Anda gunakan untuk menghasilkan token untuk aplikasi Anda, atau hubungi penyedia secara langsung untuk mendapatkan bantuan.

Pemetaan atribut

Pemetaan atribut memungkinkan Pusat Identitas IAM untuk mencocokkan pengguna yang diwakili dalam token yang dikeluarkan oleh penerbit token tepercaya kepada satu pengguna di Pusat Identitas IAM. Anda harus menentukan pemetaan atribut saat menambahkan penerbit token tepercaya ke Pusat Identitas IAM. Pemetaan atribut ini digunakan dalam klaim dalam token yang dihasilkan oleh penerbit token tepercaya. Nilai dalam klaim digunakan untuk mencari Pusat Identitas IAM. Pencarian menggunakan atribut yang ditentukan untuk mengambil satu pengguna di IAM Identity Center, yang akan digunakan sebagai pengguna di dalamnya. AWS Klaim yang Anda pilih harus dipetakan ke satu atribut dalam daftar tetap atribut yang tersedia di penyimpanan identitas Pusat Identitas IAM. Anda dapat memilih salah satu atribut penyimpanan identitas IAM Identity Center berikut: nama pengguna, email, dan ID eksternal. Nilai untuk atribut yang Anda tentukan di Pusat Identitas IAM harus unik untuk setiap pengguna.

Klaim Aud

Klaim aud mengidentifikasi audiens (penerima) yang menjadi tujuan token. Ketika aplikasi yang meminta akses mengautentikasi melalui penyedia identitas yang tidak terfederasi ke IAM Identity Center, penyedia identitas tersebut harus diatur sebagai penerbit token tepercaya. Aplikasi yang menerima permintaan akses (aplikasi penerima) harus menukar token yang dihasilkan oleh penerbit token tepercaya untuk token yang dihasilkan oleh IAM Identity Center.

Untuk informasi tentang cara mendapatkan nilai klaim aud untuk aplikasi penerima saat terdaftar di penerbit token tepercaya, lihat dokumentasi untuk penerbit token tepercaya Anda atau hubungi administrator penerbit token tepercaya untuk bantuan.

Menyiapkan penerbit token tepercaya

Untuk mengaktifkan propagasi identitas tepercaya untuk aplikasi yang mengautentikasi secara eksternal ke IAM Identity Center, satu atau beberapa administrator harus menyiapkan penerbit token tepercaya. Penerbit token tepercaya adalah server otorisasi OAuth 2.0 yang mengeluarkan token ke aplikasi yang memulai permintaan (meminta aplikasi). Token mengotorisasi aplikasi ini untuk memulai permintaan atas nama pengguna mereka ke aplikasi penerima (AWS layanan).

Topik

- Mengkoordinasikan peran dan tanggung jawab administratif
- Tugas untuk menyiapkan penerbit token tepercaya
- Cara menambahkan penerbit token tepercaya ke konsol IAM Identity Center
- Cara melihat atau mengedit pengaturan penerbit token tepercaya di konsol Pusat Identitas IAM

- Proses penyiapan dan alur permintaan untuk aplikasi yang menggunakan penerbit token tepercaya

Mengkoordinasikan peran dan tanggung jawab administratif

Dalam beberapa kasus, satu administrator mungkin melakukan semua tugas yang diperlukan untuk menyiapkan penerbit token tepercaya. Jika beberapa administrator melakukan tugas-tugas ini, koordinasi yang erat diperlukan. Tabel berikut menjelaskan bagaimana beberapa administrator dapat berkoordinasi untuk menyiapkan penerbit token tepercaya dan mengonfigurasi AWS layanan untuk menggunakannya.

> **Note**
>
> Aplikasi ini dapat berupa AWS layanan apa pun yang terintegrasi dengan IAM Identity Center dan mendukung propagasi identitas tepercaya.

Untuk informasi selengkapnya, lihat Tugas untuk menyiapkan penerbit token tepercaya.

Peran	Melakukan tugas-tugas ini	Koordinat dengan
Administrator Pusat Identitas IAM	Menambahkan iDP eksternal sebagai penerbit token tepercaya ke konsol IAM Identity Center. Membantu mengatur pemetaan atribut yang benar antara IAM Identity Center dan iDP eksternal. Memberi tahu administrator AWS layanan saat penerbit token tepercaya ditambahkan ke konsol Pusat Identitas IAM.	Administrator IDP eksternal (penerbit token tepercaya) AWS administrator layanan
Administrator IDP eksternal (penerbit token tepercaya)	Mengkonfigurasi iDP eksternal untuk mengeluarkan token. Membantu mengatur pemetaan atribut yang benar antara IAM Identity Center dan iDP eksternal.	Administrator Pusat Identitas IAM AWS administrator layanan

Peran	Melakukan tugas-tugas ini	Koordinat dengan
	Memberikan nama audiens (klaim Aud) kepada administrator AWS layanan.	
AWS administrator layanan	Memeriksa konsol AWS layanan untuk penerbit token tepercaya . Penerbit token tepercaya akan terlihat di konsol AWS layanan setelah administrator Pusat Identitas IAM menambahkannya ke konsol Pusat Identitas IAM. Mengkonfigurasi AWS layanan untuk menggunakan penerbit token tepercaya.	Administrator Pusat Identitas IAM Administrator IDP eksternal (penerbit token tepercaya)

Tugas untuk menyiapkan penerbit token tepercaya

Untuk menyiapkan penerbit token tepercaya, administrator Pusat Identitas IAM, administrator IDP eksternal (penerbit token tepercaya), dan administrator aplikasi harus menyelesaikan tugas-tugas berikut.

> **Note**
>
> Aplikasi ini dapat berupa AWS layanan apa pun yang terintegrasi dengan IAM Identity Center dan mendukung propagasi identitas tepercaya.

1. Tambahkan penerbit token tepercaya ke IAM Identity Center — Administrator IAM Identity Center menambahkan penerbit token tepercaya dengan menggunakan konsol IAM Identity Center atau API. Konfigurasi ini membutuhkan penentuan yang berikut:
   - Nama untuk penerbit token tepercaya
   - URL titik akhir penemuan OIDC (di konsol Pusat Identitas IAM, URL ini disebut URL penerbit).
   - Pemetaan atribut untuk pencarian pengguna. Pemetaan atribut ini digunakan dalam klaim dalam token yang dihasilkan oleh penerbit token tepercaya. Nilai dalam klaim digunakan untuk

mencari Pusat Identitas IAM. Pencarian menggunakan atribut tertentu untuk mengambil satu pengguna di IAM Identity Center.

2. Connect AWS layanan ke IAM Identity Center — Administrator AWS layanan harus menghubungkan aplikasi ke IAM Identity Center dengan menggunakan konsol untuk aplikasi atau API aplikasi.

   Setelah penerbit token tepercaya ditambahkan ke konsol Pusat Identitas IAM, itu juga terlihat di konsol AWS layanan dan tersedia untuk dipilih oleh administrator AWS layanan.

3. Konfigurasikan penggunaan pertukaran token — Di konsol AWS layanan, administrator AWS layanan mengonfigurasi AWS layanan untuk menerima token yang dikeluarkan oleh penerbit token tepercaya. Token ini ditukar dengan token yang dihasilkan oleh IAM Identity Center. Ini memerlukan penentuan nama penerbit token tepercaya dari Langkah 1, dan nilai klaim Aud yang sesuai dengan layanan. AWS

   Penerbit token tepercaya menempatkan nilai klaim Aud dalam token yang dikeluarkannya untuk menunjukkan bahwa token dimaksudkan untuk digunakan oleh AWS layanan. Untuk mendapatkan nilai ini, hubungi administrator untuk penerbit token tepercaya.

Cara menambahkan penerbit token tepercaya ke konsol IAM Identity Center

Dalam organisasi yang memiliki beberapa administrator, tugas ini dilakukan oleh administrator Pusat Identitas IAM. Jika Anda adalah administrator Pusat Identitas IAM, Anda harus memilih IDP eksternal mana yang akan digunakan sebagai penerbit token tepercaya.

Untuk menambahkan penerbit token tepercaya ke konsol Pusat Identitas IAM

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Otentikasi.
4. Di bawah Penerbit token tepercaya, pilih Buat penerbit token tepercaya.
5. Pada halaman Siapkan IDP eksternal untuk menerbitkan token tepercaya, di bawah detail penerbit token tepercaya, lakukan hal berikut:

   - Untuk URL Penerbit, tentukan URL penemuan OIDC dari IDP eksternal yang akan mengeluarkan token untuk propagasi identitas tepercaya. Anda harus menentukan URL titik akhir penemuan hingga dan tanpa `.well-known/openid-configuration`. Administrator iDP eksternal dapat memberikan URL ini.

> **Note**
>
> Catatan URL ini harus cocok dengan URL dalam klaim Penerbit (iss) dalam token yang dikeluarkan untuk propagasi identitas tepercaya.

- Untuk nama penerbit token Tepercaya, masukkan nama untuk mengidentifikasi penerbit token tepercaya ini di IAM Identity Center dan di konsol aplikasi.

6. Di bawah atribut Peta, lakukan hal berikut:
   - Untuk atribut penyedia Identity, pilih atribut dari daftar untuk dipetakan ke atribut di penyimpanan identitas Pusat Identitas IAM.
   - Untuk atribut IAM Identity Center, pilih atribut yang sesuai untuk pemetaan atribut.
7. Di bawah Tag (opsional), pilih Tambahkan tag baru, tentukan nilai untuk Kunci, dan opsional untuk Nilai.

   Untuk informasi tentang tanda, lihat Penandaan pada sumber daya AWS IAM Identity Center.
8. Pilih Buat penerbit token tepercaya.
9. Setelah Anda selesai membuat penerbit token tepercaya, hubungi administrator aplikasi untuk memberi tahu mereka nama penerbit token tepercaya, sehingga mereka dapat mengonfirmasi bahwa penerbit token tepercaya terlihat di konsol yang berlaku.
10. Administrator aplikasi harus memilih penerbit token tepercaya ini di konsol yang berlaku untuk mengaktifkan akses pengguna ke aplikasi dari aplikasi yang dikonfigurasi untuk propagasi identitas tepercaya.

Cara melihat atau mengedit pengaturan penerbit token tepercaya di konsol Pusat Identitas IAM

Setelah menambahkan penerbit token tepercaya ke konsol Pusat Identitas IAM, Anda dapat melihat dan mengedit pengaturan yang relevan.

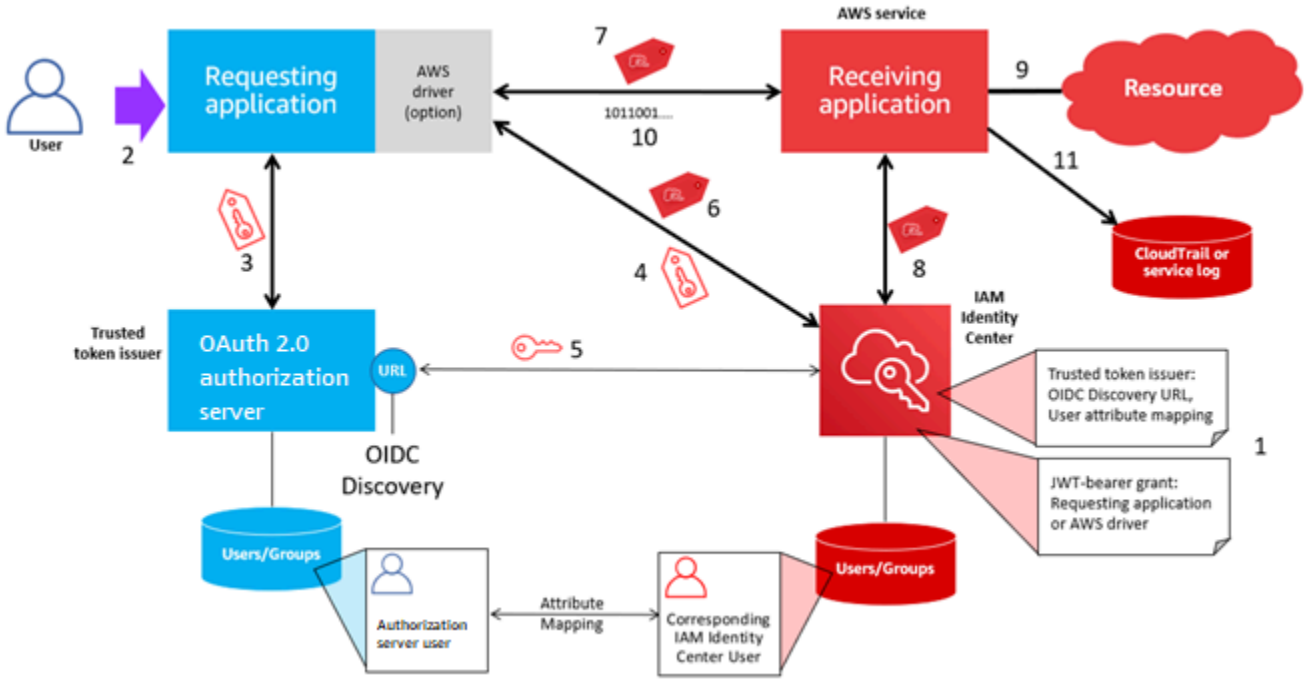
Jika Anda berencana untuk mengedit pengaturan penerbit token tepercaya, perlu diingat bahwa hal itu dapat menyebabkan pengguna kehilangan akses ke aplikasi apa pun yang dikonfigurasi untuk menggunakan penerbit token tepercaya. Untuk menghindari gangguan akses pengguna, sebaiknya Anda berkoordinasi dengan administrator untuk aplikasi apa pun yang dikonfigurasi untuk menggunakan penerbit token tepercaya sebelum Anda mengedit pengaturan.

Untuk melihat atau mengedit setelan penerbit token tepercaya di konsol Pusat Identitas IAM

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Otentikasi.
4. Di bawah Penerbit token tepercaya, pilih penerbit token tepercaya yang ingin Anda lihat atau edit.
5. Pilih Tindakan, dan kemudian pilih Edit.
6. Pada halaman Edit penerbit token tepercaya, lihat atau edit pengaturan sesuai kebutuhan. Anda dapat mengedit nama penerbit token tepercaya, pemetaan atribut, dan tag.
7. Pilih Simpan perubahan.
8. Di kotak dialog Edit penerbit token tepercaya, Anda diminta untuk mengonfirmasi bahwa Anda ingin melakukan perubahan. Pilih Konfirmasi.

Proses penyiapan dan alur permintaan untuk aplikasi yang menggunakan penerbit token tepercaya

Bagian ini menjelaskan proses penyiapan dan alur permintaan untuk aplikasi yang menggunakan penerbit token tepercaya untuk propagasi identitas tepercaya. Diagram berikut memberikan gambaran umum tentang proses ini.



Langkah-langkah berikut memberikan informasi tambahan tentang proses ini.

1. Siapkan Pusat Identitas IAM dan aplikasi AWS terkelola penerima untuk menggunakan penerbit token tepercaya. Untuk informasi, lihat Tugas untuk menyiapkan penerbit token tepercaya.
2. Alur permintaan dimulai ketika pengguna membuka aplikasi yang meminta.
3. Aplikasi yang meminta meminta token dari penerbit token tepercaya untuk memulai permintaan ke aplikasi terkelola penerima AWS . Jika pengguna belum mengautentikasi, proses ini memicu alur otentikasi. Token berisi informasi berikut:
   - Subjek (Sub) pengguna.
   - Atribut yang digunakan IAM Identity Center untuk mencari pengguna yang sesuai di IAM Identity Center.
   - Klaim audiens (Aud) yang berisi nilai yang dikaitkan dengan penerbit token tepercaya dengan aplikasi AWS terkelola penerima. Jika ada klaim lain, klaim tersebut tidak digunakan oleh IAM Identity Center.
4. Aplikasi yang meminta, atau AWS driver yang digunakannya, meneruskan token ke IAM Identity Center dan meminta agar token ditukar dengan token yang dihasilkan oleh IAM Identity Center. Jika Anda menggunakan AWS driver, Anda mungkin perlu mengkonfigurasi driver untuk kasus penggunaan ini. Untuk informasi selengkapnya, lihat dokumentasi untuk aplikasi AWS terkelola yang relevan.
5. IAM Identity Center menggunakan endpoint OIDC Discovery untuk mendapatkan kunci publik yang dapat digunakan untuk memverifikasi keaslian token. IAM Identity Center kemudian melakukan hal berikut:
   - Memverifikasi token.
   - Mencari direktori Pusat Identitas. Untuk melakukan ini, IAM Identity Center menggunakan atribut yang dipetakan yang ditentukan dalam token.
   - Memverifikasi bahwa pengguna berwenang untuk mengakses aplikasi penerima. Jika aplikasi AWS terkelola dikonfigurasi untuk meminta penugasan kepada pengguna dan grup, pengguna harus memiliki penugasan langsung atau berbasis grup ke aplikasi; jika tidak, permintaan ditolak. Jika aplikasi AWS terkelola dikonfigurasi agar tidak memerlukan penugasan pengguna dan grup, pemrosesan dilanjutkan.

   > **Note**
   >
   > AWS layanan memiliki konfigurasi pengaturan default yang menentukan apakah penugasan diperlukan untuk pengguna dan grup. Kami menyarankan Anda untuk tidak mengubah pengaturan Memerlukan tugas untuk aplikasi ini jika Anda berencana untuk menggunakannya dengan propagasi identitas tepercaya. Meskipun Anda telah

mengonfigurasi izin berbutir halus yang memungkinkan pengguna mengakses sumber daya aplikasi tertentu, mengubah setelan Memerlukan penetapan dapat mengakibatkan perilaku yang tidak terduga, termasuk akses pengguna yang terganggu ke sumber daya ini.

- Memverifikasi bahwa aplikasi yang meminta dikonfigurasi untuk menggunakan cakupan yang valid untuk aplikasi terkelola penerima AWS .

6. Jika langkah verifikasi sebelumnya berhasil, IAM Identity Center membuat token baru. Token baru adalah token buram (terenkripsi) yang mencakup identitas pengguna yang sesuai di Pusat Identitas IAM, audiens (Aud) dari aplikasi AWS terkelola penerima, dan cakupan yang dapat digunakan aplikasi yang meminta saat membuat permintaan ke aplikasi terkelola penerima. AWS
7. Aplikasi yang meminta, atau driver yang digunakannya, memulai permintaan sumber daya ke aplikasi penerima dan meneruskan token yang dihasilkan IAM Identity Center ke aplikasi penerima.
8. Aplikasi penerima melakukan panggilan ke IAM Identity Center untuk mendapatkan identitas pengguna dan cakupan yang dikodekan dalam token. Mungkin juga membuat permintaan untuk mendapatkan atribut pengguna atau keanggotaan grup pengguna dari direktori Pusat Identitas.
9. Aplikasi penerima menggunakan konfigurasi otorisasi untuk menentukan apakah pengguna berwenang untuk mengakses sumber daya aplikasi yang diminta.
10. Jika pengguna berwenang untuk mengakses sumber daya aplikasi yang diminta, aplikasi penerima menanggapi permintaan tersebut.
11. Identitas pengguna, tindakan yang dilakukan atas nama mereka, dan peristiwa lain yang dicatat dalam log dan CloudTrail peristiwa aplikasi penerima. Cara spesifik di mana informasi ini dicatat bervariasi berdasarkan aplikasi.

Mengelola sertifikat IAM Identity Center

IAM Identity Center menggunakan sertifikat untuk mengatur hubungan kepercayaan SAMP antara IAM Identity Center dan penyedia layanan aplikasi Anda. Saat Anda menambahkan aplikasi di IAM Identity Center, sertifikat IAM Identity Center secara otomatis dibuat untuk digunakan dengan aplikasi tersebut selama proses penyiapan. Secara default, sertifikat IAM Identity Center yang dibuat secara otomatis ini berlaku untuk jangka waktu lima tahun.

Sebagai administrator Pusat Identitas IAM, Anda kadang-kadang perlu mengganti sertifikat lama dengan yang lebih baru untuk aplikasi tertentu. Misalnya, Anda mungkin perlu mengganti sertifikat

saat tanggal kedaluwarsa sertifikat mendekati. Proses penggantian sertifikat yang lebih lama dengan yang lebih baru disebut sebagai rotasi sertifikat.

Topik

Pertimbangan sebelum memutar sertifikat

Sebelum Anda memulai proses memutar sertifikat di IAM Identity Center, pertimbangkan hal berikut:

- Proses rotasi sertifikasi mengharuskan Anda membangun kembali kepercayaan antara IAM Identity Center dan penyedia layanan. Untuk membangun kembali kepercayaan, gunakan prosedur yang disediakan diMemutar sertifikat Pusat Identitas IAM.
- Memperbarui sertifikat dengan penyedia layanan dapat menyebabkan gangguan layanan sementara bagi pengguna Anda sampai kepercayaan telah berhasil dibangun kembali. Rencanakan operasi ini dengan hati-hati selama jam sibuk di luar jika memungkinkan.

Memutar sertifikat Pusat Identitas IAM

Memutar sertifikat IAM Identity Center adalah proses multistep yang melibatkan hal-hal berikut:

- Menghasilkan sertifikat baru
- Menambahkan sertifikat baru ke situs web penyedia layanan
- Mengatur sertifikat baru menjadi aktif
- Menghapus sertifikat yang tidak aktif

Gunakan semua prosedur berikut dalam urutan berikut untuk menyelesaikan proses rotasi sertifikat untuk aplikasi tertentu.

Langkah 1: Buat sertifikat baru.

Sertifikat Pusat Identitas IAM baru yang Anda hasilkan dapat dikonfigurasi untuk menggunakan properti berikut:

- Masa berlaku - Menentukan waktu yang diberikan (dalam bulan) sebelum sertifikat IAM Identity Center baru berakhir.
- Ukuran kunci — Menentukan jumlah bit yang harus digunakan kunci dengan algoritma kriptografinya. Anda dapat mengatur nilai ini ke RSA 1024-bit atau RSA 2048-bit. Untuk informasi umum tentang cara kerja ukuran kunci dalam kriptografi, lihat Ukuran kunci.
- Algoritma - Menentukan algoritma yang digunakan IAM Identity Center saat menandatangani pernyataan/respons SAMP. Anda dapat mengatur nilai ini ke SHA-1 atau SHA-256. AWS merekomendasikan penggunaan SHA-256 jika memungkinkan, kecuali penyedia layanan Anda memerlukan SHA-1. Untuk informasi umum tentang cara kerja algoritma kriptografi, lihat Kriptografi kunci publik.

1. Buka konsol Pusat Identitas IAM.
2. Pilih Aplikasi.
3. Dalam daftar aplikasi, pilih aplikasi yang ingin Anda hasilkan sertifikat baru.
4. Pada halaman detail aplikasi, pilih tab Konfigurasi. Di bawah metadata Pusat Identitas IAM, pilih Kelola sertifikat. Jika Anda tidak memiliki tab Konfigurasi atau pengaturan konfigurasi tidak tersedia, Anda tidak perlu memutar sertifikat untuk aplikasi ini.
5. Pada halaman sertifikat Pusat Identitas IAM, pilih Hasilkan sertifikat baru.
6. Dalam kotak dialog Hasilkan sertifikat Pusat Identitas IAM baru, tentukan nilai yang sesuai untuk Periode validitas, Algoritma, dan Ukuran kunci. Kemudian pilih Hasilkan.

Langkah 2: Perbarui situs web penyedia layanan.

Gunakan prosedur berikut untuk membangun kembali kepercayaan dengan penyedia layanan aplikasi.

> **Important**
>
> Saat Anda mengunggah sertifikat baru ke penyedia layanan, pengguna Anda mungkin tidak dapat diautentikasi. Untuk memperbaiki situasi ini, atur sertifikat baru sebagai aktif seperti yang dijelaskan pada langkah berikutnya.

1. Di konsol Pusat Identitas IAM, pilih aplikasi yang baru saja Anda buat sertifikat baru.
2. Pada halaman detail aplikasi, pilih Edit konfigurasi.

3. Pilih Lihat petunjuk, lalu ikuti petunjuk untuk situs web penyedia layanan aplikasi spesifik Anda untuk menambahkan sertifikat yang baru dibuat.

Langkah 3: Atur sertifikat baru menjadi aktif.

Aplikasi dapat memiliki hingga dua sertifikat yang ditetapkan untuk itu. IAM Identity Center akan menggunakan sertifikasi yang ditetapkan sebagai aktif untuk menandatangani semua pernyataan SAMP.

1. Buka konsol Pusat Identitas IAM.
2. Pilih Aplikasi.
3. Dalam daftar aplikasi, pilih aplikasi Anda.
4. Pada halaman detail aplikasi, pilih tab Konfigurasi. Di bawah metadata Pusat Identitas IAM, pilih Kelola sertifikat.
5. Pada halaman sertifikat Pusat Identitas IAM, pilih sertifikat yang ingin disetel ke aktif, pilih Tindakan, lalu pilih Setel sebagai aktif.
6. Dalam dialog Setel sertifikat yang dipilih sebagai aktif, konfirmasikan bahwa Anda memahami bahwa menyetel sertifikat menjadi aktif mungkin mengharuskan Anda untuk membangun kembali kepercayaan, lalu pilih Aktif.

Langkah 4: Hapus sertifikat lama.

Gunakan prosedur berikut untuk menyelesaikan proses rotasi sertifikat untuk aplikasi Anda. Anda hanya dapat menghapus sertifikat yang berada dalam keadaan tidak aktif.

1. Buka konsol Pusat Identitas IAM.
2. Pilih Aplikasi.
3. Dalam daftar aplikasi, pilih aplikasi Anda.
4. Pada halaman detail aplikasi, pilih tab Konfigurasi. Di bawah metadata Pusat Identitas IAM, pilih Kelola sertifikat.
5. Pada halaman sertifikat Pusat Identitas IAM, pilih sertifikat yang ingin Anda hapus. Pilih Tindakan dan kemudian pilih Hapus.
6. Di kotak dialog Hapus sertifikat, pilih Hapus.

Indikator status kedaluwarsa sertifikat

Saat berada di halaman Aplikasi di properti aplikasi, Anda mungkin melihat ikon indikator status berwarna. Ikon ini muncul di kolom Kedaluwarsa di samping setiap sertifikat dalam daftar. Berikut ini menjelaskan kriteria yang digunakan IAM Identity Center untuk menentukan ikon mana yang ditampilkan untuk setiap sertifikat.

- Merah - Menunjukkan bahwa sertifikat saat ini kedaluwarsa.
- Kuning - Menunjukkan bahwa sertifikat akan kedaluwarsa dalam 90 hari atau kurang.
- Hijau - Menunjukkan bahwa sertifikat saat ini valid dan akan tetap berlaku setidaknya selama 90 hari lagi.

Untuk memeriksa status sertifikat saat ini

1. Buka konsol Pusat Identitas IAM.
2. Pilih Aplikasi.
3. Dalam daftar aplikasi, tinjau status sertifikat dalam daftar seperti yang ditunjukkan dalam kolom Kedaluwarsa pada.

Konfigurasikan properti aplikasi di konsol Pusat Identitas IAM

Di Pusat Identitas IAM, Anda dapat menyesuaikan pengalaman pengguna dengan mengonfigurasi URL mulai aplikasi, status relai, dan durasi sesi.

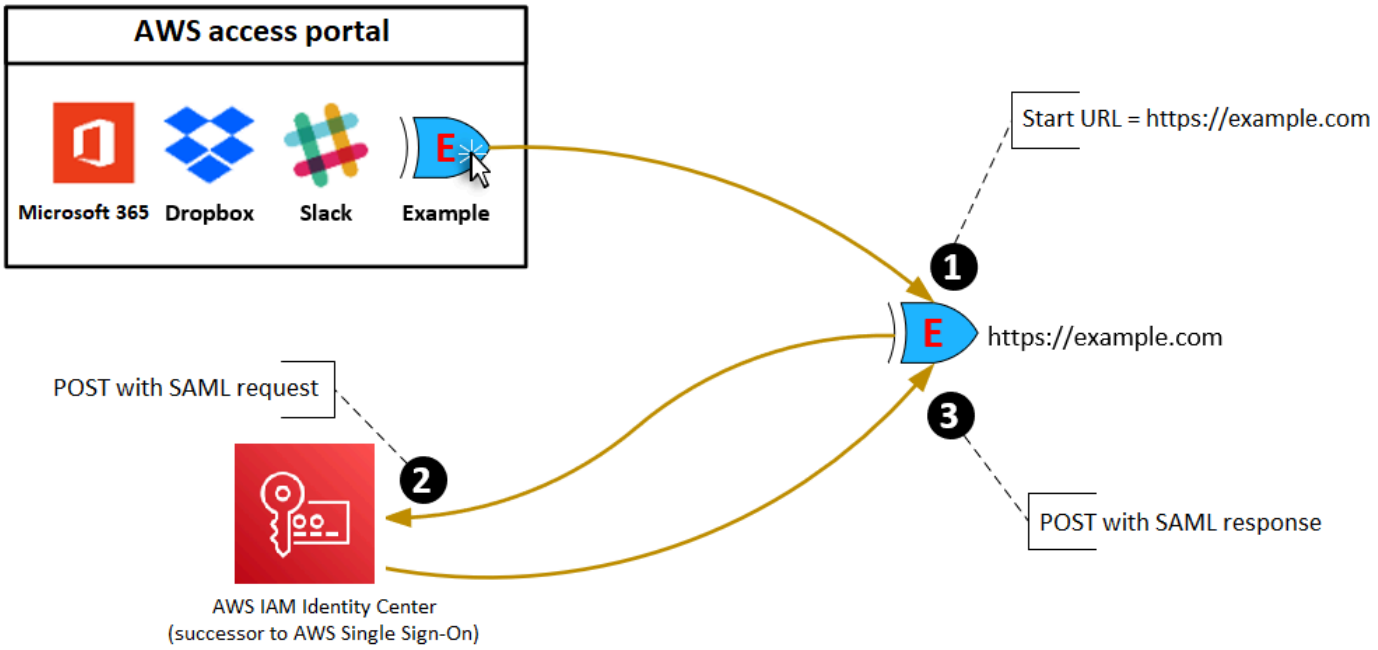
URL mulai aplikasi

Anda menggunakan URL awal aplikasi untuk memulai proses federasi dengan aplikasi Anda. Penggunaan umum adalah untuk aplikasi yang hanya mendukung pengikatan yang dimulai oleh penyedia layanan (SP).

Langkah-langkah dan diagram berikut menggambarkan alur kerja otentikasi URL awal aplikasi saat pengguna memilih aplikasi di portal akses: AWS

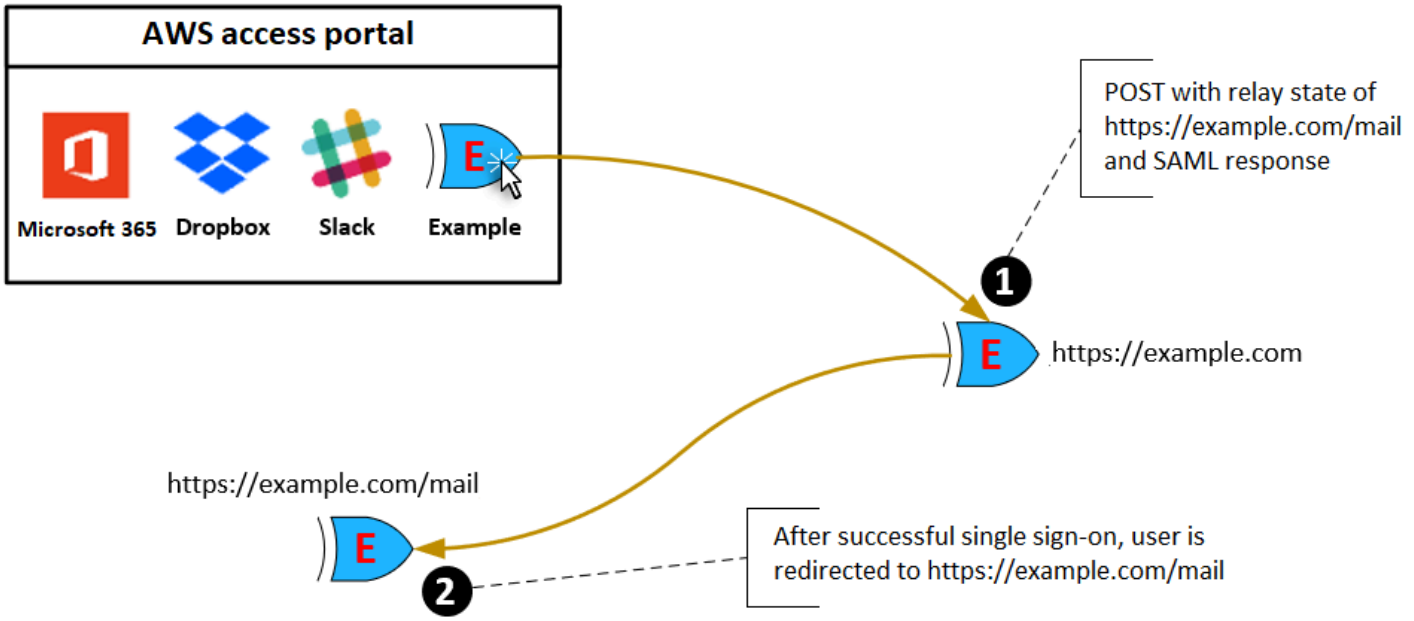
1. Browser pengguna mengalihkan permintaan otentikasi menggunakan nilai untuk URL awal aplikasi (dalam hal ini https://example.com).
2. Aplikasi mengirimkan `HTML POST` dengan `SAMLRequest` ke IAM Identity Center.

3. IAM Identity Center kemudian mengirimkan `HTML POST` dengan `SAMLResponse` kembali ke aplikasi.



Status relai

Selama proses otentikasi federasi, status relai mengarahkan pengguna dalam aplikasi. Untuk SALL 2.0, nilai ini diteruskan, tidak dimodifikasi, ke aplikasi. Setelah properti aplikasi dikonfigurasi, IAM Identity Center mengirimkan nilai status relai bersama dengan respons SAMP ke aplikasi.



Durasi sesi

Durasi sesi adalah lamanya waktu sesi pengguna aplikasi valid. Untuk SAFL 2.0, ini digunakan untuk mengatur `SessionNotOnOrAfter` tanggal elemen pernyataan SAMB. `saml2:AuthNStatement`

Durasi sesi dapat ditafsirkan oleh aplikasi dengan salah satu cara berikut:

- Aplikasi dapat menggunakannya untuk menentukan waktu maksimum yang diizinkan untuk sesi pengguna. Aplikasi mungkin menghasilkan sesi pengguna dengan durasi yang lebih pendek. Ini dapat terjadi ketika aplikasi hanya mendukung sesi pengguna dengan durasi yang lebih pendek dari panjang sesi yang dikonfigurasi.
- Aplikasi dapat menggunakannya sebagai durasi yang tepat dan mungkin tidak mengizinkan administrator untuk mengonfigurasi nilai. Ini dapat terjadi ketika aplikasi hanya mendukung panjang sesi tertentu.

Untuk informasi selengkapnya tentang cara durasi sesi digunakan, lihat dokumentasi aplikasi spesifik Anda.

Tetapkan akses pengguna ke aplikasi di konsol Pusat Identitas IAM

Anda dapat menetapkan pengguna akses masuk tunggal ke aplikasi SAMP 2.0 di katalog aplikasi atau ke aplikasi SAMP 2.0 khusus.

Pertimbangan untuk tugas kelompok:

- Tetapkan akses langsung ke grup. Untuk membantu menyederhanakan administrasi izin akses, kami sarankan Anda menetapkan akses langsung ke grup daripada ke pengguna individu. Dengan grup, Anda dapat memberikan atau menolak izin ke grup pengguna, alih-alih menerapkan izin tersebut ke setiap individu. Jika pengguna pindah ke organisasi yang berbeda, Anda cukup memindahkan pengguna tersebut ke grup yang berbeda. Pengguna kemudian secara otomatis menerima izin yang diperlukan untuk organisasi baru.
- Grup bersarang tidak didukung. Saat menetapkan akses pengguna ke aplikasi, IAM Identity Center tidak mendukung pengguna yang ditambahkan ke grup bersarang. Jika pengguna ditambahkan ke grup bersarang, mereka mungkin menerima pesan “Anda tidak memiliki aplikasi apa pun” saat masuk. Penugasan harus dilakukan terhadap grup langsung di mana pengguna menjadi anggota.

Untuk menetapkan akses pengguna atau grup ke aplikasi

> **Important**
>
> Untuk aplikasi AWS terkelola, Anda harus menambahkan pengguna langsung dari dalam konsol aplikasi yang relevan atau melalui API.

1. Buka konsol Pusat Identitas IAM.

   > **Note**
   >
   > Jika Anda mengelola pengguna AWS Managed Microsoft AD, pastikan konsol IAM Identity Center menggunakan AWS Wilayah tempat AWS Managed Microsoft AD direktori Anda berada sebelum mengambil langkah berikutnya.

2. Pilih Aplikasi.
3. Dalam daftar aplikasi, pilih nama aplikasi yang ingin Anda tetapkan aksesnya.
4. Pada halaman detail aplikasi, di bagian Pengguna yang ditugaskan, pilih Tetapkan pengguna.
5. Dalam kotak dialog Tetapkan pengguna, masukkan nama pengguna atau grup. Anda juga dapat mencari pengguna dan grup. Anda dapat menentukan beberapa pengguna atau grup dengan memilih akun yang berlaku saat muncul di hasil penelusuran.
6. Pilih Tetapkan pengguna.

Hapus akses pengguna di konsol Pusat Identitas IAM

Gunakan prosedur ini untuk menghapus akses pengguna ke aplikasi SAMP 2.0 dalam katalog aplikasi atau aplikasi SAMP 2.0 kustom.

Untuk menghapus akses pengguna ke aplikasi

1. Buka konsol Pusat Identitas IAM.
2. Pilih Aplikasi.
3. Dalam daftar aplikasi, pilih aplikasi dari mana Anda ingin menghapus akses pengguna.
4. Pada halaman detail aplikasi, di bagian Pengguna yang ditugaskan, pilih pengguna atau grup yang ingin Anda hapus lalu pilih tombol Hapus akses.

5. Dalam kotak dialog Hapus akses, verifikasi nama pengguna atau grup. Kemudian pilih Hapus akses.

Petakan atribut dalam aplikasi Anda ke atribut IAM Identity Center

Beberapa penyedia layanan memerlukan pernyataan SAM khusus untuk meneruskan data tambahan tentang login pengguna Anda. Dalam hal ini, gunakan prosedur berikut untuk menentukan bagaimana atribut pengguna aplikasi Anda harus dipetakan ke atribut yang sesuai di IAM Identity Center.

Untuk memetakan atribut aplikasi ke atribut di IAM Identity Center

1. Buka konsol Pusat Identitas IAM.
2. Pilih Aplikasi.
3. Dalam daftar aplikasi, pilih aplikasi tempat Anda ingin memetakan atribut.
4. Pada halaman detail aplikasi, pilih Tindakan dan kemudian pilih Edit pemetaan atribut.
5. Pilih Tambahkan pemetaan atribut baru.
6. Di kotak teks pertama, masukkan atribut aplikasi.
7. Di kotak teks kedua, masukkan atribut di Pusat Identitas IAM yang ingin Anda petakan ke atribut aplikasi. Misalnya, Anda mungkin ingin memetakan atribut aplikasi **`Username`** ke atribut **`email`** pengguna IAM Identity Center. Untuk melihat daftar atribut pengguna yang diizinkan di Pusat Identitas IAM, lihat tabel diPemetaan atribut untuk direktori AWS Managed Microsoft AD.
8. Di kolom ketiga tabel, pilih format yang sesuai untuk atribut dari menu.
9. Pilih Simpan perubahan.

Desain ketahanan dan perilaku Regional

Layanan IAM Identity Center dikelola sepenuhnya dan menggunakan layanan yang sangat tersedia dan tahan lamaAWS, seperti Amazon S3 dan Amazon EC2. Untuk memastikan ketersediaan jika terjadi gangguan zona ketersediaan, IAM Identity Center beroperasi di beberapa zona ketersediaan. Untuk informasi tentang tujuan desain ketersediaan untuk Pusat Identitas IAM, lihat Lampiran A: Dirancang-Untuk Ketersediaan untuk AWS Layanan Tertentu dalam Panduan Pilar Keandalan.

Anda mengaktifkan Pusat Identitas IAM di akun AWS Organizations manajemen Anda. Ini diperlukan agar Pusat Identitas IAM dapat menyediakan, menghilangkan penyediaan, dan memperbarui peran di semua peran Anda. Akun AWS Ketika Anda mengaktifkan IAM Identity Center, itu diterapkan ke Wilayah AWS yang saat ini dipilih. Jika Anda ingin menerapkan ke spesifikWilayah AWS, ubah pilihan wilayah sebelum mengaktifkan Pusat Identitas IAM.

> **Note**
>
> IAM Identity Center mengontrol akses ke set izin dan aplikasi dari Wilayah utamanya saja. Kami menyarankan Anda mempertimbangkan risiko yang terkait dengan kontrol akses ketika IAM Identity Center beroperasi di satu Wilayah.

Meskipun IAM Identity Center menentukan akses dari Wilayah tempat Anda mengaktifkan layanan, Akun AWS bersifat global. Ini berarti bahwa setelah pengguna masuk ke Pusat Identitas IAM, mereka dapat beroperasi di Wilayah mana pun ketika mereka mengakses Akun AWS melalui Pusat Identitas IAM. Sebagian besar aplikasi yang AWS dikelola seperti Amazon SageMaker, bagaimanapun, harus diinstal di Wilayah yang sama dengan Pusat Identitas IAM bagi pengguna untuk mengautentikasi dan menetapkan akses ke aplikasi ini. Untuk informasi tentang kendala Regional saat menggunakan aplikasi dengan IAM Identity Center, lihat dokumentasi untuk aplikasi.

Anda juga dapat menggunakan IAM Identity Center untuk mengautentikasi dan mengotorisasi akses ke aplikasi berbasis SAMP yang dapat dijangkau melalui URL publik, terlepas dari platform atau cloud tempat aplikasi dibangun.

Kami tidak menyarankan menggunakan Instans akun Pusat Identitas IAM sebagai sarana untuk menerapkan ketahanan karena menciptakan titik kontrol terisolasi kedua yang tidak terhubung ke instans organisasi Anda.

Mengatur akses darurat ke AWS Management Console

IAM Identity Center dibangun dari AWS infrastruktur yang sangat tersedia dan menggunakan arsitektur Availability Zone untuk menghilangkan satu titik kegagalan. Untuk lapisan perlindungan tambahan jika terjadi Pusat Identitas IAM atau Wilayah AWS gangguan, kami menyarankan Anda menyiapkan konfigurasi yang dapat Anda gunakan untuk menyediakan akses sementara ke. AWS Management Console

Daftar Isi

Ikhtisar

AWSmemungkinkan Anda untuk:

- Hubungkan iDP pihak ketiga Anda ke IAM Identity Center.
- Hubungkan IDP pihak ketiga Anda ke individu Akun AWS dengan menggunakan federasi berbasis SAMP 2.0.

Jika Anda menggunakan Pusat Identitas IAM, Anda dapat menggunakan kemampuan ini untuk membuat konfigurasi akses darurat yang dijelaskan di bagian berikut. Konfigurasi ini memungkinkan Anda untuk menggunakan IAM Identity Center sebagai mekanisme untuk Akun AWS akses. Jika Pusat Identitas IAM terganggu, pengguna operasi darurat Anda dapat masuk ke federasi langsung AWS Management Console melalui, dengan menggunakan kredensil yang sama yang mereka

gunakan untuk mengakses akun mereka. Konfigurasi ini berfungsi ketika Pusat Identitas IAM tidak tersedia, tetapi bidang data IAM dan penyedia identitas eksternal Anda (iDP) tersedia.

> **Important**
>
> Kami menyarankan Anda menerapkan konfigurasi ini sebelum gangguan terjadi karena Anda tidak dapat membuat konfigurasi jika akses Anda untuk membuat peran IAM yang diperlukan juga terganggu. Juga, uji konfigurasi ini secara berkala untuk memastikan bahwa tim Anda memahami apa yang harus dilakukan jika IAM Identity Center terganggu.

Ringkasan konfigurasi akses darurat

Untuk mengkonfigurasi akses darurat, Anda harus menyelesaikan tugas-tugas berikut:

1. Buat akun operasi darurat di organisasi Anda di AWS Organizations.
2. Hubungkan IDP Anda ke akun operasi darurat dengan menggunakan federasi berbasis SAMP 2.0.
3. Di akun operasi darurat, buat peran untuk federasi penyedia identitas pihak ketiga. Selain itu, buat peran operasi darurat di setiap akun beban kerja Anda, dengan izin yang diperlukan.
4. Delegasikan akses ke akun beban kerja Anda untuk peran IAM yang Anda buat di akun operasi darurat. Untuk mengotorisasi akses ke akun operasi darurat Anda, buat grup operasi darurat di IDP Anda, tanpa anggota.
5. Aktifkan grup operasi darurat di IDP Anda untuk menggunakan peran operasi darurat dengan membuat aturan di IDP Anda yang memungkinkan akses federasi SAMP 2.0 ke. AWS Management Console

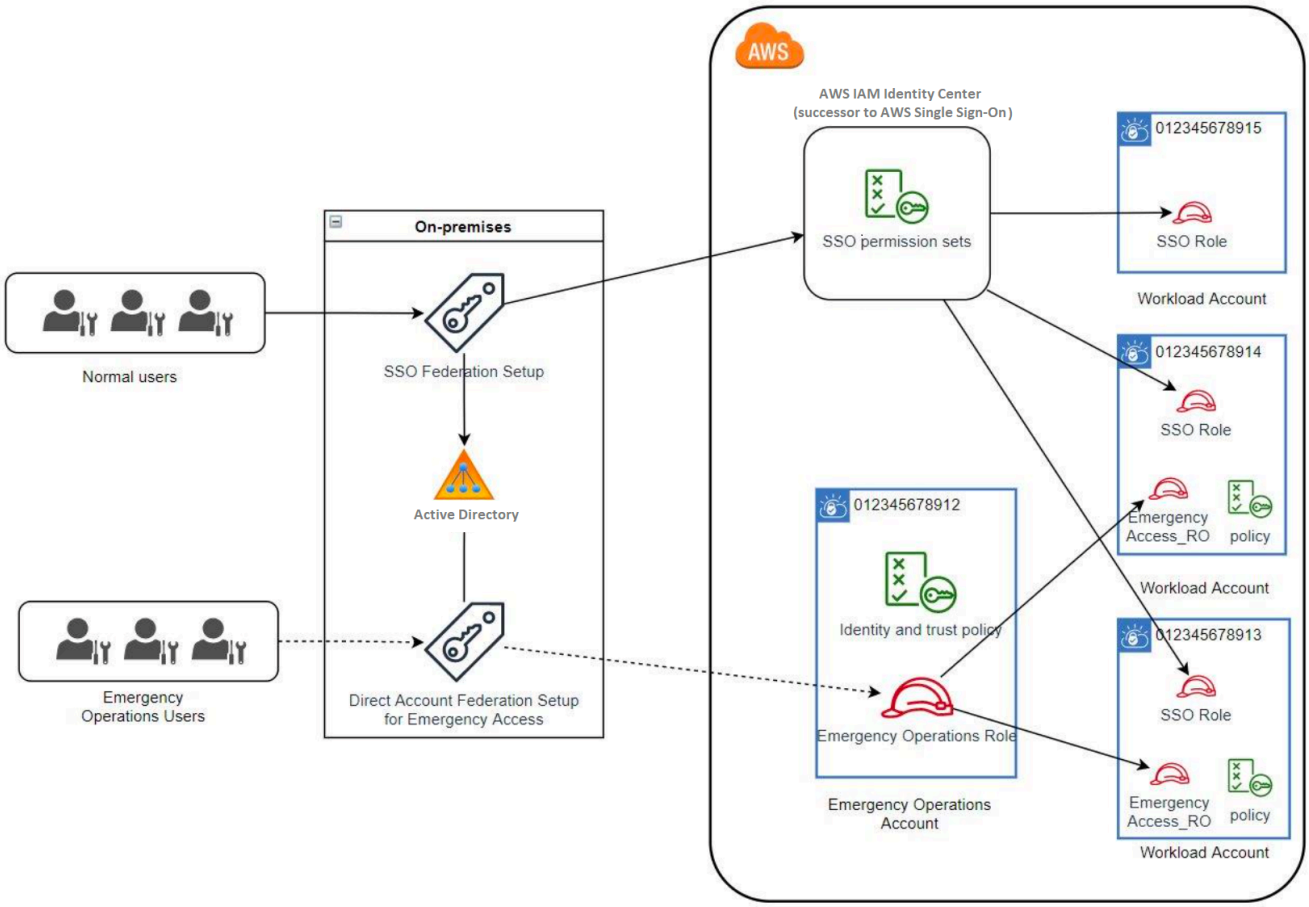
Selama operasi normal, tidak ada yang memiliki akses ke akun operasi darurat karena grup operasi darurat di IDP Anda tidak memiliki anggota. Jika terjadi gangguan Pusat Identitas IAM, gunakan IDP Anda untuk menambahkan pengguna tepercaya ke grup operasi darurat di IDP Anda. Pengguna ini kemudian dapat masuk ke IDP Anda, menavigasi keAWS Management Console, dan mengambil peran operasi darurat di akun operasi darurat. Dari sana, pengguna ini dapat beralih peran ke peran akses darurat di akun beban kerja Anda di mana mereka perlu melakukan pekerjaan operasi.

Bagaimana merancang peran operasi penting Anda

Dengan desain ini, Anda mengonfigurasi satu Akun AWS di mana Anda berfederasi melalui IAM, sehingga pengguna dapat mengambil peran operasi penting. Peran operasi penting memiliki

kebijakan kepercayaan yang memungkinkan pengguna untuk mengambil peran yang sesuai dalam akun beban kerja Anda. Peran dalam akun beban kerja memberikan izin yang diperlukan pengguna untuk melakukan pekerjaan penting.

Diagram berikut memberikan gambaran desain.



Cara merencanakan model akses Anda

Sebelum Anda mengonfigurasi akses darurat, buat rencana bagaimana model akses akan bekerja. Gunakan proses berikut untuk membuat rencana ini.

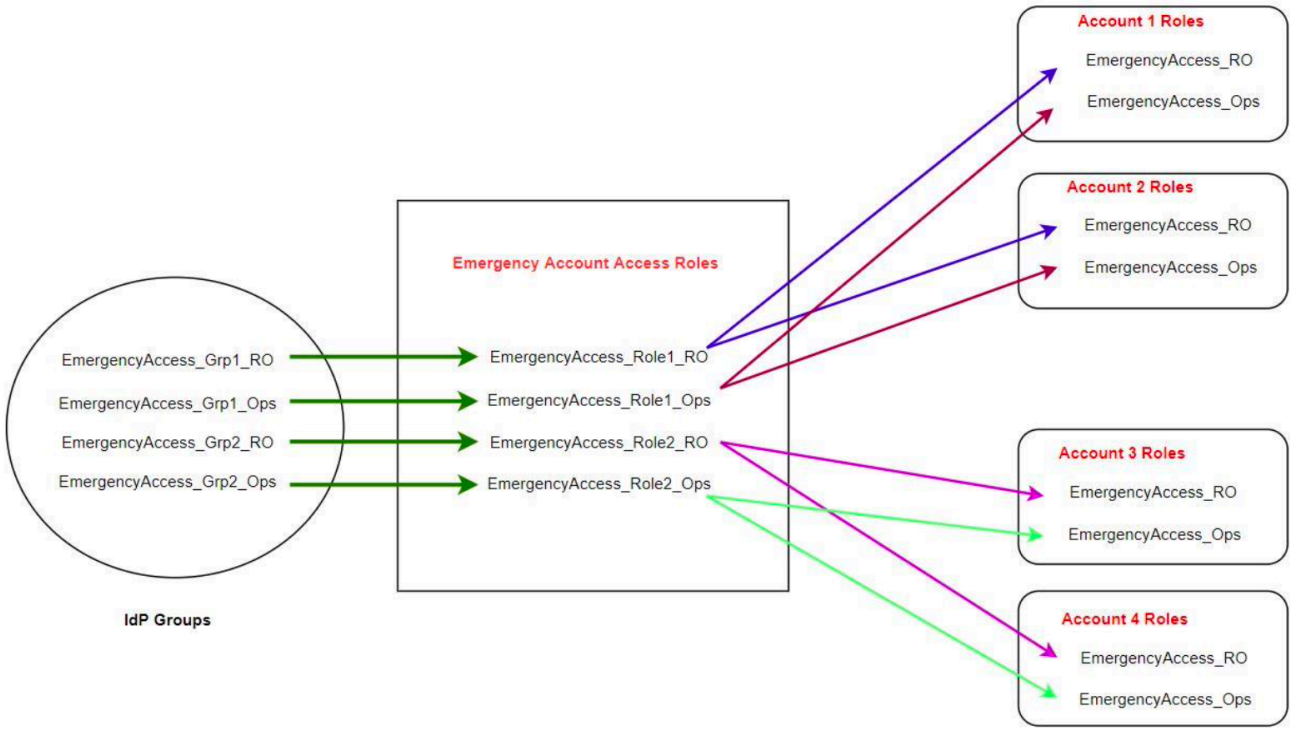
1. Identifikasi di Akun AWS mana akses operator darurat sangat penting selama gangguan ke Pusat Identitas IAM. Misalnya, akun produksi Anda mungkin penting, tetapi akun pengembangan dan pengujian Anda mungkin tidak.
2. Untuk pengumpulan akun tersebut, identifikasi peran penting spesifik yang Anda butuhkan di akun Anda. Di seluruh akun ini, konsisten dalam mendefinisikan apa yang dapat dilakukan peran. Ini

menyederhanakan pekerjaan di akun akses darurat tempat Anda membuat peran lintas akun. Kami menyarankan Anda memulai dengan dua peran berbeda dalam akun ini: Read Only (RO) dan Operations (Ops). Jika diperlukan, Anda dapat membuat lebih banyak peran dan memetakan peran ini ke grup pengguna akses darurat yang lebih berbeda dalam pengaturan Anda.

3. Identifikasi dan buat grup akses darurat di IDP Anda. Anggota grup adalah pengguna kepada siapa Anda mendelegasikan akses ke peran akses darurat.
4. Tentukan peran mana yang dapat diasumsikan oleh kelompok-kelompok ini dalam akun akses darurat. Untuk melakukannya, tentukan aturan di IDP Anda yang menghasilkan klaim yang mencantumkan peran mana yang dapat diakses grup. Grup ini kemudian dapat mengambil peran Baca Saja atau Operasi Anda di akun akses darurat. Dari peran tersebut, mereka dapat mengambil peran yang sesuai di akun beban kerja Anda.

Bagaimana merancang peran darurat, akun, dan pemetaan grup

Diagram berikut menunjukkan cara memetakan grup akses darurat Anda ke peran di akun akses darurat Anda. Diagram juga menunjukkan hubungan kepercayaan peran lintas akun yang memungkinkan peran akun akses darurat untuk mengakses peran terkait di akun beban kerja Anda. Kami menyarankan agar desain rencana darurat Anda menggunakan pemetaan ini sebagai titik awal.



Cara membuat konfigurasi akses darurat Anda

Gunakan tabel pemetaan berikut untuk membuat konfigurasi akses darurat Anda. Tabel ini mencerminkan rencana yang mencakup dua peran dalam akun beban kerja: Hanya Baca (RO) dan Operasi (Ops), dengan kebijakan kepercayaan dan kebijakan izin yang sesuai. Kebijakan kepercayaan memungkinkan peran akun akses darurat untuk mengakses peran akun beban kerja individu. Peran akun beban kerja individual juga memiliki kebijakan izin untuk peran yang dapat dilakukan di akun. Kebijakan izin dapat berupa kebijakan AWSterkelola atau kebijakan yang dikelola pelanggan.

Akun	Peran untuk membuat	Kebijakan kepercaya an	Kebijakan izin
Akun 1	Emergency Access_RO	Emergency Access_Role1_RO	arn:aws:iam::aws:p olicy/ReadOnlyAccess
Akun 1	Emergency Access_Ops	Emergency Access_Role1_Ops	arn:aws:iam::aws:p olicy/job-function/ SystemAdministrator
Akun 2	Emergency Access_RO	Emergency Access_Role2_RO	arn:aws:iam: :aws:poli cy/ ReadOnlyAccess
Akun 2	Emergency Access_Ops	Emergency Access_Role2_Ops	arn:aws:iam::aws:p olicy/job-function/ SystemAdministrator
Akun akses darurat	Emergency Access_Role1_RO Emergency Access_Role1_Ops Emergency Access_Role2_RO Emergency Access_Role2_Ops	IdP	AssumeRole untuk sumber daya peran dalam akun

Dalam rencana pemetaan ini, akun akses darurat berisi dua peran hanya-baca dan dua peran operasi. Peran ini mempercayai IDP Anda untuk mengautentikasi dan mengotorisasi grup yang Anda pilih untuk mengakses peran dengan meneruskan nama peran dalam pernyataan. Ada peran read-only dan operasi yang sesuai dalam beban kerja Akun 1 dan Akun 2. Untuk beban kerja Akun 1, `EmergencyAccess_R0` peran mempercayai `EmergencyAccess_Role1_R0` peran yang berada di akun akses darurat. Tabel menentukan pola kepercayaan serupa antara peran read-only akun beban kerja dan peran operasi dan peran akses darurat yang sesuai.

Tugas persiapan darurat

Untuk menyiapkan konfigurasi akses darurat Anda, kami sarankan Anda melakukan tugas-tugas berikut sebelum keadaan darurat terjadi.

1. Siapkan aplikasi federasi IAM langsung di IDP Anda. Untuk informasi selengkapnya, lihat Pengaturan satu kali aplikasi federasi IAM langsung di Okta.
2. Buat koneksi IDP di akun akses darurat yang dapat diakses selama acara berlangsung.
3. Buat peran akses darurat di akun akses darurat seperti yang dijelaskan dalam tabel pemetaan di atas.
4. Buat peran operasi sementara dengan kebijakan kepercayaan dan izin di setiap akun beban kerja.
5. Buat grup operasi sementara di IDP Anda. Nama grup akan tergantung pada nama-nama peran operasi sementara.
6. Uji federasi IAM langsung.
7. Nonaktifkan aplikasi federasi iDP di IDP Anda untuk mencegah penggunaan reguler.

Proses failover darurat

Jika instans Pusat Identitas IAM tidak tersedia dan Anda menentukan bahwa Anda harus menyediakan akses darurat ke Konsol AWS Manajemen, kami merekomendasikan proses failover berikut.

1. Administrator iDP mengaktifkan aplikasi federasi IAM langsung di IDP Anda.
2. Pengguna meminta akses ke grup operasi sementara melalui mekanisme yang ada, seperti permintaan email, saluran Slack, atau bentuk komunikasi lainnya.
3. Pengguna yang Anda tambahkan ke grup akses darurat masuk ke IDP, pilih akun akses darurat, dan, pengguna memilih peran yang akan digunakan di akun akses darurat. Dari peran ini, mereka

dapat mengambil peran dalam akun beban kerja terkait yang memiliki kepercayaan lintas akun dengan peran akun darurat.

Kembali ke operasi normal

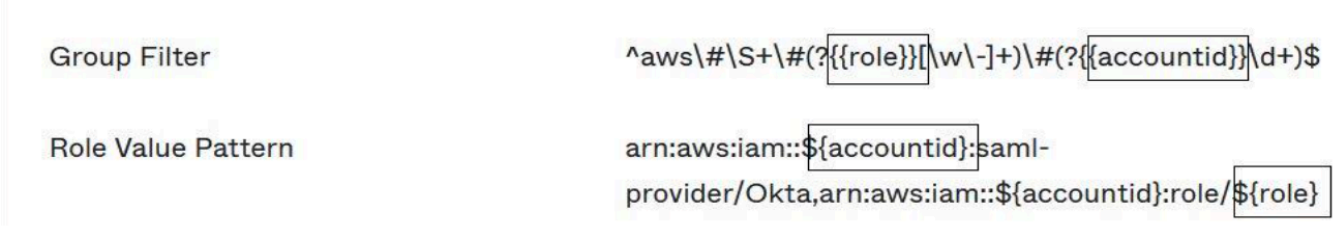
Periksa Dasbor AWS Kesehatan untuk mengonfirmasi kapan kesehatan layanan IAM Identity Center dipulihkan. Untuk kembali ke operasi normal, lakukan langkah-langkah berikut.

1. Setelah ikon status untuk layanan IAM Identity Center menunjukkan bahwa layanan tersebut sehat, masuk ke IAM Identity Center.
2. Jika Anda berhasil masuk ke Pusat Identitas IAM, komunikasikan kepada pengguna akses darurat bahwa Pusat Identitas IAM tersedia. Instruksikan pengguna ini untuk keluar dan menggunakan portal AWS akses untuk masuk kembali ke Pusat Identitas IAM.
3. Setelah semua pengguna akses darurat keluar, di iDP, nonaktifkan aplikasi federasi iDP. Kami menyarankan Anda melakukan tugas ini setelah jam kerja.
4. Hapus semua pengguna dari grup akses darurat di IDP.

Infrastruktur peran akses darurat Anda tetap ada sebagai rencana akses cadangan, tetapi sekarang dinonaktifkan.

Pengaturan satu kali aplikasi federasi IAM langsung di Okta

1. Masuk ke Okta akun Anda sebagai pengguna dengan izin administratif.
2. Di Konsol Okta Admin, di bawah Aplikasi, pilih Aplikasi.
3. Pilih Jelajahi Katalog Aplikasi. Cari dan pilih Federasi AWS Akun. Kemudian pilih Tambahkan integrasi.
4. Siapkan federasi IAM langsung AWS dengan mengikuti langkah-langkah di Cara Mengkonfigurasi SAMP 2.0 untuk Federasi AWS Akun.
5. Pada tab Sign-On Options, pilih SAMP 2.0 dan masukkan pengaturan Group Filter dan Role Value Pattern. Nama grup untuk direktori pengguna tergantung pada filter yang Anda konfigurasikan.



Pada gambar di atas, `role` variabelnya adalah untuk peran operasi darurat di akun akses darurat Anda. Misalnya, jika Anda membuat `EmergencyAccess_Role1_RO` peran (seperti yang dijelaskan dalam tabel pemetaan) di Akun AWS`123456789012`, dan jika setelan filter grup Anda dikonfigurasi seperti yang ditunjukkan pada gambar di atas, nama grup Anda seharusnya`aws#EmergencyAccess_Role1_RO#123456789012`.

6. Di direktori Anda (misalnya, direktori Anda di Active Directory), buat grup akses darurat dan tentukan nama untuk direktori (misalnya,`aws#EmergencyAccess_Role1_RO#123456789012`). Tetapkan pengguna Anda ke grup ini dengan menggunakan mekanisme penyediaan yang ada.
7. Di akun akses darurat, konfigurasikan kebijakan kepercayaan khusus yang memberikan izin yang diperlukan untuk peran akses darurat yang akan diasumsikan selama gangguan. Berikut ini adalah contoh pernyataan untuk kebijakan kepercayaan khusus yang dilampirkan pada `EmergencyAccess_Role1_RO` peran. Untuk ilustrasi, lihat akun darurat pada diagram di bawahBagaimana merancang peran darurat, akun, dan pemetaan grup.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
         "Effect":"Allow",
         "Principal":{
            "Federated":"arn:aws:iam::123456789012:saml-provider/Okta"
         },
         "Action":[
            "sts:AssumeRoleWithSAML",
            "sts:SetSourceIdentity",
            "sts:TagSession"
         ],
         "Condition":{
            "StringEquals":{
               "SAML:aud":"https:~/~/signin.aws.amazon.com/saml"
            }
         }
```

```
      }
   ]
}
```

8. Berikut ini adalah pernyataan contoh untuk kebijakan izin yang dilampirkan ke `EmergencyAccess_Role1_RO` peran. Untuk ilustrasi, lihat akun darurat pada diagram di bawahBagaimana merancang peran darurat, akun, dan pemetaan grup.

```
{
    "Version": "2012-10-17",
    "Statement":[
      {
         "Effect":"Allow",
         "Action":"sts:AssumeRole",
         "Resource":[
            "arn:aws:iam::<account 1>:role/EmergencyAccess_RO",
            "arn:aws:iam::<account 2>:role/EmergencyAccess_RO"
         ]
      }
   ]
}
```

9. Pada akun beban kerja, konfigurasikan kebijakan kepercayaan khusus. Berikut ini adalah contoh pernyataan untuk kebijakan kepercayaan yang melekat pada `EmergencyAccess_RO` peran tersebut. Dalam contoh ini, akun `123456789012` adalah akun akses darurat. Untuk ilustrasi, lihat akun beban kerja dalam diagram di bawah. Bagaimana merancang peran darurat, akun, dan pemetaan grup

```
{
    "Version": "2012-10-17",
    "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::123456789012:root"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

> **Note**
>
> Sebagian besar IdPs memungkinkan Anda untuk menjaga integrasi aplikasi dinonaktifkan sampai diperlukan. Kami menyarankan agar Anda tetap menonaktifkan aplikasi federasi IAM langsung di IDP Anda hingga diperlukan untuk akses darurat.

Keamanan di AWS IAM Identity Center

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 IAM Identity Center, 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 IAM Identity Center. Topik berikut menunjukkan cara mengonfigurasi Pusat Identitas IAM untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Pusat Identitas IAM Anda.

Topik

Manajemen identitas dan akses untuk IAM Identity Center

Akses ke Pusat Identitas IAM memerlukan kredensi yang AWS dapat digunakan untuk mengautentikasi permintaan Anda. Kredensi tersebut harus memiliki izin untuk mengakses AWS sumber daya, seperti aplikasi yang AWS dikelola.

Otentikasi ke portal AWS akses dikendalikan oleh direktori yang telah Anda sambungkan ke Pusat Identitas IAM. Namun, otorisasi untuk Akun AWS yang tersedia bagi pengguna dari dalam portal AWS akses ditentukan oleh dua faktor:

1. Siapa yang telah diberi akses ke mereka yang ada Akun AWS di konsol Pusat Identitas IAM. Untuk informasi selengkapnya, lihat Akses masuk tunggal ke Akun AWS.
2. Tingkat izin apa yang telah diberikan kepada pengguna di konsol Pusat Identitas IAM untuk memungkinkan mereka mengakses yang sesuai dengan itu. Akun AWS Untuk informasi selengkapnya, lihat Membuat, mengelola, dan menghapus set izin.

Bagian berikut menjelaskan bagaimana Anda sebagai administrator dapat mengontrol akses ke konsol Pusat Identitas IAM atau dapat mendelegasikan akses administratif untuk day-to-day tugas dari konsol Pusat Identitas IAM.

- Autentikasi
- Kontrol akses

Autentikasi

Pelajari cara mengakses AWS menggunakan identitas IAM.

Kontrol akses

Anda dapat memiliki kredensi yang valid untuk mengautentikasi permintaan Anda, tetapi kecuali Anda memiliki izin, Anda tidak dapat membuat atau mengakses sumber daya Pusat Identitas IAM. Misalnya, Anda harus memiliki izin untuk membuat direktori yang terhubung Pusat Identitas IAM.

Bagian berikut menjelaskan cara mengelola izin untuk IAM Identity Center. Anda disarankan untuk membaca gambaran umum terlebih dahulu.

- Ikhtisar mengelola izin akses ke sumber daya Pusat Identitas IAM Anda

- Contoh kebijakan berbasis identitas untuk IAM Identity Center
- Menggunakan peran terkait layanan untuk IAM Identity Center

Ikhtisar mengelola izin akses ke sumber daya Pusat Identitas IAM Anda

Setiap AWS sumber daya dimiliki oleh Akun AWS, dan izin untuk membuat atau mengakses sumber daya diatur oleh kebijakan izin. Untuk menyediakan akses, administrator akun dapat menambahkan izin ke identitas IAM (yaitu, pengguna, grup, dan peran). Beberapa layanan (seperti AWS Lambda) juga mendukung penambahan izin ke sumber daya.

> **Note**
>
> Administrator akun (atau pengguna administrator) adalah pengguna dengan hak akses administrator. Untuk informasi selengkapnya, lihat Praktik terbaik IAM dalam Panduan Pengguna IAM.

Topik

- Sumber daya dan operasi Pusat Identitas IAM
- Memahami kepemilikan sumber daya
- Mengelola akses ke sumber daya
- Menentukan elemen kebijakan: tindakan, efek, sumber daya, dan prinsip
- Menentukan kondisi dalam kebijakan

Sumber daya dan operasi Pusat Identitas IAM

Di IAM Identity Center, sumber daya utama adalah instance aplikasi, profil, dan set izin.

Memahami kepemilikan sumber daya

Pemilik sumber daya adalah Akun AWS yang menciptakan sumber daya. Artinya, pemilik sumber daya adalah entitas utama (akun, pengguna, atau peran IAM) yang mengautentikasi permintaan yang membuat sumber daya. Akun AWS Contoh berikut menggambarkan cara kerjanya:

- Jika Pengguna root akun AWS membuat sumber daya Pusat Identitas IAM, seperti instance aplikasi atau set izin, Anda Akun AWS adalah pemilik sumber daya tersebut.

- Jika Anda membuat pengguna di AWS akun Anda dan memberikan izin pengguna tersebut untuk membuat sumber daya Pusat Identitas IAM, pengguna kemudian dapat membuat sumber daya Pusat Identitas IAM. Namun, AWS akun Anda, tempat pengguna berada, memiliki sumber daya.
- Jika Anda membuat peran IAM di AWS akun Anda dengan izin untuk membuat sumber daya Pusat Identitas IAM, siapa pun yang dapat mengambil peran tersebut dapat membuat sumber daya Pusat Identitas IAM. Anda Akun AWS, yang menjadi milik peran tersebut, memiliki sumber daya Pusat Identitas IAM.

Mengelola akses ke sumber daya

Kebijakan izin menjelaskan siapa yang memiliki akses ke suatu objek. Bagian berikut menjelaskan opsi yang tersedia untuk membuat kebijakan izin.

> **Note**
>
> Bagian ini membahas penggunaan IAM dalam konteks IAM Identity Center. Bagian ini tidak memberikan informasi yang mendetail tentang layanan IAM. Untuk dokumentasi lengkap IAM, lihat Apa yang Dimaksud dengan IAM? dalam Panduan Pengguna IAM. Untuk informasi tentang sintaksis dan penjelasan kebijakan IAM, lihat AWS Referensi Kebijakan IAM dalam 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. Pusat Identitas IAM hanya mendukung kebijakan berbasis identitas (kebijakan IAM).

Topik

- Kebijakan berbasis identitas (kebijakan IAM)
- Kebijakan berbasis sumber daya

Kebijakan berbasis identitas (kebijakan IAM)

Anda dapat menambahkan izin ke identitas IAM. Misalnya, Anda dapat melakukan hal berikut:

- Lampirkan kebijakan izin ke pengguna atau grup di Anda Akun AWS — Administrator akun dapat menggunakan kebijakan izin yang dikaitkan dengan pengguna tertentu untuk memberikan izin bagi pengguna tersebut untuk menambahkan sumber daya Pusat Identitas IAM, seperti aplikasi baru.

- Melampirkan kebijakan izin pada peran (memberikan izin lintas akun) – Anda dapat melampirkan kebijakan izin berbasis identitas ke peran IAM untuk memberikan izin lintas akun.

  Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mendelegasikan izin, lihat Manajemen Akses dalam Panduan Pengguna IAM.

Kebijakan izin berikut memberikan izin kepada pengguna untuk menjalankan semua tindakan yang dimulai dengan `List`. Tindakan ini menampilkan informasi tentang sumber daya Pusat Identitas IAM, seperti instance aplikasi atau set izin. Perhatikan bahwa karakter wildcard (*) dalam `Resource` elemen menunjukkan bahwa tindakan diizinkan untuk semua sumber daya Pusat Identitas IAM yang dimiliki oleh akun.

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

Untuk informasi selengkapnya tentang penggunaan kebijakan berbasis identitas dengan IAM Identity Center, lihat. Contoh kebijakan berbasis identitas untuk IAM Identity Center Untuk informasi lebih lanjut tentang pengguna, kelompok, peran, dan izin, lihat Identitas (Pengguna, Grup, dan Peran) dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Layanan lain, seperti Amazon S3, juga mendukung kebijakan izin berbasis sumber daya. Misalnya, Anda dapat melampirkan kebijakan ke bucket S3 untuk mengelola izin akses ke bucket tersebut. IAM Identity Center tidak mendukung kebijakan berbasis sumber daya.

Menentukan elemen kebijakan: tindakan, efek, sumber daya, dan prinsip

Untuk setiap sumber daya Pusat Identitas IAM (lihatSumber daya dan operasi Pusat Identitas IAM), layanan mendefinisikan satu set operasi API. Untuk memberikan izin untuk operasi API ini, IAM Identity Center mendefinisikan serangkaian tindakan yang dapat Anda tentukan dalam kebijakan. Perhatikan bahwa melakukan operasi API bisa memerlukan izin untuk lebih dari satu tindakan.

Berikut ini adalah elemen-elemen kebijakan dasar:

- Sumber Daya – Dalam kebijakan, Anda menggunakan Amazon Resource Name (ARN) untuk mengidentifikasi sumber daya yang diberlakukan oleh kebijakan tersebut.
- Tindakan – Anda menggunakan kata kunci tindakan untuk mengidentifikasi operasi sumber daya yang ingin Anda izinkan atau tolak. Misalnya, `sso:DescribePermissionsPolicies` izin memungkinkan izin pengguna untuk melakukan operasi Pusat `DescribePermissionsPolicies` Identitas IAM.
- Efek – Anda menentukan efek ketika pengguna meminta tindakan tertentu—baik mengizinkan maupun menolak. Jika Anda tidak secara eksplisit memberikan akses ke (mengizinkan) sumber daya, akses akan ditolak secara implisit. Anda juga dapat secara eksplisit menolak akses ke sumber daya, yang mungkin Anda lakukan untuk memastikan bahwa pengguna tidak dapat mengaksesnya, meskipun kebijakan yang berbeda memberikan akses.
- Principal – Dalam kebijakan berbasis identitas (Kebijakan IAM), pengguna yang kebijakannya terlampir adalah principal yang implisit. Untuk kebijakan berbasis sumber daya, Anda menentukan pengguna, akun, layanan, atau entitas lain yang diinginkan untuk menerima izin (berlaku hanya untuk kebijakan berbasis sumber daya). IAM Identity Center tidak mendukung kebijakan berbasis sumber daya.

Untuk mempelajari lebih lanjut tentang sintaks dan deskripsi kebijakan IAM, lihat referensi kebijakan AWS IAM di Panduan Pengguna IAM.

Menentukan kondisi dalam kebijakan

Saat memberikan izin, Anda dapat menggunakan bahasa kebijakan akses untuk menentukan kondisi yang diperlukan agar kebijakan diterapkan. Misalnya, Anda mungkin ingin kebijakan diterapkan hanya setelah tanggal tertentu. Untuk informasi selengkapnya tentang menentukan kondisi dalam bahasa kebijakan, lihat Kondisi dalam Panduan Pengguna IAM.

Untuk menyatakan kondisi, Anda menggunakan kunci kondisi standar. Tidak ada kunci kondisi khusus untuk IAM Identity Center. Namun, ada tombol AWS kondisi yang dapat Anda gunakan sesuai kebutuhan. Untuk daftar lengkap AWS kunci, lihat Kunci kondisi global yang tersedia di Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk IAM Identity Center

Topik ini memberikan contoh kebijakan IAM yang dapat Anda buat untuk memberikan izin kepada pengguna dan peran untuk mengelola Pusat Identitas IAM.

> **Important**
>
> Kami menyarankan Anda terlebih dahulu meninjau topik pengantar yang menjelaskan konsep dasar dan opsi yang tersedia bagi Anda untuk mengelola akses ke sumber daya Pusat Identitas IAM Anda. Untuk informasi selengkapnya, lihat Ikhtisar mengelola izin akses ke sumber daya Pusat Identitas IAM Anda.

Bagian dalam topik ini mencakup hal berikut:

- Contoh kebijakan kustom
- Izin diperlukan untuk menggunakan konsol Pusat Identitas IAM

Contoh kebijakan kustom

Bagian ini memberikan contoh kasus penggunaan umum yang memerlukan kebijakan IAM khusus. Contoh kebijakan ini adalah kebijakan berbasis identitas, yang tidak menentukan elemen Utama. Ini karena dengan kebijakan berbasis identitas, Anda tidak menentukan kepala sekolah yang mendapat izin. Sebaliknya, Anda melampirkan kebijakan ke kepala sekolah. Saat Anda melampirkan kebijakan izin berbasis identitas ke peran IAM, prinsipal yang diidentifikasi dalam kebijakan kepercayaan peran akan mendapatkan izin. Anda dapat membuat kebijakan berbasis identitas di IAM dan melampirkannya ke pengguna, grup, dan/atau peran. Anda juga dapat menerapkan kebijakan ini ke pengguna Pusat Identitas IAM saat Anda membuat izin yang ditetapkan di Pusat Identitas IAM.

> **Note**
>
> Gunakan contoh ini saat Anda membuat kebijakan untuk lingkungan Anda dan pastikan untuk menguji kasus pengujian positif (“akses diberikan”) dan negatif (“akses ditolak”) sebelum menerapkan kebijakan ini di lingkungan produksi Anda. Untuk informasi selengkapnya tentang pengujian kebijakan IAM, lihat Menguji kebijakan IAM dengan simulator kebijakan IAM di Panduan Pengguna IAM.

Topik

- Contoh 1: Izinkan pengguna untuk melihat Pusat Identitas IAM
- Contoh 2: Izinkan pengguna untuk mengelola izin ke Pusat Akun AWS Identitas IAM
- Contoh 3: Izinkan pengguna untuk mengelola aplikasi di IAM Identity Center

- Contoh 4: Izinkan pengguna mengelola pengguna dan grup di direktori Pusat Identitas

Contoh 1: Izinkan pengguna untuk melihat Pusat Identitas IAM

Kebijakan izin berikut memberikan izin hanya-baca kepada pengguna sehingga mereka dapat melihat semua pengaturan dan informasi direktori yang dikonfigurasi di Pusat Identitas IAM.

> **Note**
>
> Kebijakan ini disediakan untuk tujuan contoh saja. Dalam lingkungan produksi, kami menyarankan Anda menggunakan kebijakan `ViewOnlyAccess` AWS terkelola untuk IAM Identity Center.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ds:DescribeDirectories",
                "ds:DescribeTrusts",
                "iam:ListPolicies",
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:ListAccountsForParent",
                "organizations:ListOrganizationalUnitsForParent",
                "sso:ListManagedPoliciesInPermissionSet",
                "sso:ListPermissionSetsProvisionedToAccount",
                "sso:ListAccountAssignments",
                "sso:ListAccountsForProvisionedPermissionSet",
                "sso:ListPermissionSets",
                "sso:DescribePermissionSet",
                "sso:GetInlinePolicyForPermissionSet",
                "sso-directory:DescribeDirectory",
                "sso-directory:SearchUsers",
```

```
                "sso-directory:SearchGroups"
            ],
            "Resource": "*"
        }
    ]
}
```

Contoh 2: Izinkan pengguna untuk mengelola izin ke Pusat Akun AWS Identitas IAM

Kebijakan izin berikut memberikan izin untuk memungkinkan pengguna membuat, mengelola, dan menerapkan set izin untuk Anda. Akun AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:AttachManagedPolicyToPermissionSet",
                "sso:CreateAccountAssignment",
                "sso:CreatePermissionSet",
                "sso:DeleteAccountAssignment",
                "sso:DeleteInlinePolicyFromPermissionSet",
                "sso:DeletePermissionSet",
                "sso:DetachManagedPolicyFromPermissionSet",
                "sso:ProvisionPermissionSet",
                "sso:PutInlinePolicyToPermissionSet",
                "sso:UpdatePermissionSet"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IAMListPermissions",
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles",
                "iam:ListPolicies"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AccessToSSOProvisionedRoles",
            "Effect": "Allow",
```

```
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:GetRole",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",
                "iam:PutRolePolicy",
                "iam:UpdateRole",
                "iam:UpdateRoleDescription"
            ],
            "Resource": "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetSAMLProvider"
            ],
            "Resource": "arn:aws:iam::*:saml-provider/AWSSSO_*_DO_NOT_DELETE"
        }
    ]
}
```

> **Note**
>
> Izin tambahan yang tercantum di bawah`"Sid": "IAMListPermissions"`, dan `"Sid": "AccessToSSOProvisiondRoles"` bagian diperlukan hanya untuk memungkinkan pengguna membuat tugas di akun AWS Organizations manajemen. Dalam kasus tertentu, Anda mungkin juga perlu menambahkan `iam:UpdateSAMLProvider` ke bagian ini.

Contoh 3: Izinkan pengguna untuk mengelola aplikasi di IAM Identity Center

Kebijakan izin berikut memberikan izin untuk memungkinkan pengguna melihat dan mengonfigurasi aplikasi di Pusat Identitas IAM, termasuk aplikasi SaaS pra-terintegrasi dari dalam katalog Pusat Identitas IAM.

> **Note**
>
> `sso:AssociateProfile`Operasi yang digunakan dalam contoh kebijakan berikut diperlukan untuk pengelolaan penugasan pengguna dan grup untuk aplikasi. Ini juga memungkinkan pengguna untuk menetapkan pengguna dan grup Akun AWS dengan menggunakan set izin yang ada. Jika pengguna harus mengelola Akun AWS akses dalam Pusat Identitas IAM, dan memerlukan izin yang diperlukan untuk mengelola set izin, lihat. Contoh 2: Izinkan pengguna untuk mengelola izin ke Pusat Akun AWS Identitas IAM

Pada Oktober 2020, banyak dari operasi ini hanya tersedia melalui AWS konsol. Kebijakan contoh ini mencakup tindakan “baca” seperti daftar, dapatkan, dan pencarian, yang relevan dengan pengoperasian konsol yang bebas kesalahan untuk kasus ini.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:AssociateProfile",
                "sso:CreateApplicationInstance",
                "sso:ImportApplicationInstanceServiceProviderMetadata",
                "sso:DeleteApplicationInstance",
                "sso:DeleteProfile",
                "sso:DisassociateProfile",
                "sso:GetApplicationTemplate",
                "sso:UpdateApplicationInstanceServiceProviderConfiguration",
                "sso:UpdateApplicationInstanceDisplayData",
                "sso:DeleteManagedApplicationInstance",
                "sso:UpdateApplicationInstanceStatus",
                "sso:GetManagedApplicationInstance",
                "sso:UpdateManagedApplicationInstanceStatus",
                "sso:CreateManagedApplicationInstance",
                "sso:UpdateApplicationInstanceSecurityConfiguration",
                "sso:UpdateApplicationInstanceResponseConfiguration",
                "sso:GetApplicationInstance",
                "sso:CreateApplicationInstanceCertificate",
                "sso:UpdateApplicationInstanceResponseSchemaConfiguration",
                "sso:UpdateApplicationInstanceActiveCertificate",
                "sso:DeleteApplicationInstanceCertificate",
```

```
                "sso:ListApplicationInstanceCertificates",
                "sso:ListApplicationTemplates",
                "sso:ListApplications",
                "sso:ListApplicationInstances",
                "sso:ListDirectoryAssociations",
                "sso:ListProfiles",
                "sso:ListProfileAssociations",
                "sso:ListInstances",
                "sso:GetProfile",
                "sso:GetSSOStatus",
                "sso:GetSsoConfiguration",
                "sso-directory:DescribeDirectory",
                "sso-directory:DescribeUsers",
                "sso-directory:ListMembersInGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Contoh 4: Izinkan pengguna mengelola pengguna dan grup di direktori Pusat Identitas

Kebijakan izin berikut memberikan izin untuk memungkinkan pengguna membuat, melihat, memodifikasi, dan menghapus pengguna dan grup di Pusat Identitas IAM.

Dalam beberapa kasus, modifikasi langsung ke pengguna dan grup di IAM Identity Center dibatasi. Misalnya, ketika Active Directory, atau penyedia identitas eksternal dengan Penyediaan Otomatis diaktifkan, dipilih sebagai sumber identitas.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso-directory:ListGroupsForUser",
                "sso-directory:DisableUser",
                "sso-directory:EnableUser",
                "sso-directory:SearchGroups",
                "sso-directory:DeleteGroup",
                "sso-directory:AddMemberToGroup",
```

```
                "sso-directory:DescribeDirectory",
                "sso-directory:UpdateUser",
                "sso-directory:ListMembersInGroup",
                "sso-directory:CreateUser",
                "sso-directory:DescribeGroups",
                "sso-directory:SearchUsers",
                "sso:ListDirectoryAssociations",
                "sso-directory:RemoveMemberFromGroup",
                "sso-directory:DeleteUser",
                "sso-directory:DescribeUsers",
                "sso-directory:UpdateGroup",
                "sso-directory:CreateGroup"
            ],
            "Resource": "*"
        }
    ]
}
```

Izin diperlukan untuk menggunakan konsol Pusat Identitas IAM

Agar pengguna dapat bekerja dengan konsol Pusat Identitas IAM tanpa kesalahan, izin tambahan diperlukan. Jika kebijakan IAM telah dibuat yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana dimaksudkan untuk pengguna dengan kebijakan tersebut. Contoh berikut mencantumkan kumpulan izin yang mungkin diperlukan untuk memastikan operasi bebas kesalahan dalam konsol Pusat Identitas IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:DescribeAccountAssignmentCreationStatus",
                "sso:DescribeAccountAssignmentDeletionStatus",
                "sso:DescribePermissionSet",
                "sso:DescribePermissionSetProvisioningStatus",
                "sso:DescribePermissionsPolicies",
                "sso:DescribeRegisteredRegions",
                "sso:GetApplicationInstance",
                "sso:GetApplicationTemplate",
                "sso:GetInlinePolicyForPermissionSet",
                "sso:GetManagedApplicationInstance",
                "sso:GetMfaDeviceManagementForDirectory",
```

```
                "sso:GetPermissionSet",
                "sso:GetPermissionsPolicy",
                "sso:GetProfile",
                "sso:GetSharedSsoConfiguration",
                "sso:GetSsoConfiguration",
                "sso:GetSSOStatus",
                "sso:GetTrust",
                "sso:ListAccountAssignmentCreationStatus",
                "sso:ListAccountAssignmentDeletionStatus",
                "sso:ListAccountAssignments",
                "sso:ListAccountsForProvisionedPermissionSet",
                "sso:ListApplicationInstanceCertificates",
                "sso:ListApplicationInstances",
                "sso:ListApplications",
                "sso:ListApplicationTemplates",
                "sso:ListDirectoryAssociations",
                "sso:ListInstances",
                "sso:ListManagedPoliciesInPermissionSet",
                "sso:ListPermissionSetProvisioningStatus",
                "sso:ListPermissionSets",
                "sso:ListPermissionSetsProvisionedToAccount",
                "sso:ListProfileAssociations",
                "sso:ListProfiles",
                "sso:ListTagsForResource",
                "sso-directory:DescribeDirectory",
                "sso-directory:DescribeGroups",
                "sso-directory:DescribeUsers",
                "sso-directory:ListGroupsForUser",
                "sso-directory:ListMembersInGroup",
                "sso-directory:SearchGroups",
                "sso-directory:SearchUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS kebijakan terkelola untuk Pusat Identitas IAM

Untuk membuat kebijakan terkelola pelanggan IAM yang memberi tim Anda hanya izin yang mereka butuhkan membutuhkan waktu dan keahlian. Untuk memulai dengan cepat, Anda dapat menggunakan kebijakan AWS terkelola. Kebijakan ini mencakup kasus penggunaan umum dan

tersedia di Akun AWS Anda. Untuk informasi lebih lanjut tentang kebijakan yang dikelola AWS , lihat kebijakan yang dikelola AWS di Panduan Pengguna IAM.

AWS layanan memelihara dan memperbarui kebijakan AWS terkelola. Anda tidak dapat mengubah izin dalam kebijakan AWS terkelola. Layanan terkadang menambahkan izin tambahan ke kebijakan yang dikelola AWS untuk mendukung fitur-fitur baru. Jenis pembaruan ini akan memengaruhi semua identitas (pengguna, grup, dan peran) di mana kebijakan tersebut dilampirkan. Layanan kemungkinan besar akan memperbarui kebijakan yang dikelola AWS saat ada fitur baru yang diluncurkan atau saat ada operasi baru yang tersedia. Layanan tidak menghapus izin dari kebijakan AWS terkelola, sehingga pembaruan kebijakan tidak akan merusak izin yang ada.

Selain itu, AWS mendukung kebijakan terkelola untuk fungsi pekerjaan yang mencakup beberapa layanan. Misalnya, kebijakan ReadOnlyAccess AWS terkelola menyediakan akses hanya-baca ke semua AWS layanan dan sumber daya. Saat layanan meluncurkan fitur baru, AWS tambahkan izin hanya-baca untuk operasi dan sumber daya baru. Untuk melihat daftar dan deskripsi dari kebijakan fungsi tugas, lihat kebijakan yang dikelola AWS untuk fungsi tugas di Panduan Pengguna IAM.

Tindakan baru yang memungkinkan Anda membuat daftar dan menghapus sesi pengguna tersedia di bawah namespace `identitystore-auth` baru. Setiap izin tambahan untuk tindakan di namespace ini akan diperbarui di halaman ini. Saat membuat kebijakan IAM kustom Anda, hindari penggunaan * after `identitystore-auth` karena ini berlaku untuk semua tindakan yang ada di namespace hari ini atau di masa mendatang.

AWS kebijakan terkelola: AWSSSOMasterAccountAdministrator

`AWSSSOMasterAccountAdministrator`Kebijakan tersebut memberikan tindakan administratif yang diperlukan kepada kepala sekolah. Kebijakan ini ditujukan untuk kepala sekolah yang melakukan peran pekerjaan sebagai administrator. AWS IAM Identity Center Seiring waktu, daftar tindakan yang diberikan akan diperbarui agar sesuai dengan fungsionalitas IAM Identity Center yang ada dan tindakan yang diperlukan sebagai administrator.

Anda dapat melampirkan kebijakan `AWSSSOMasterAccountAdministrator` ke identitas IAM Anda. Saat Anda melampirkan `AWSSSOMasterAccountAdministrator` kebijakan ke identitas, Anda memberikan AWS IAM Identity Center izin administratif. Prinsipal dengan kebijakan ini dapat mengakses Pusat Identitas IAM dalam akun AWS Organizations manajemen dan semua akun anggota. Prinsipal ini dapat sepenuhnya mengelola semua operasi Pusat Identitas IAM, termasuk kemampuan untuk membuat instans Pusat Identitas IAM, pengguna, set izin, dan tugas. Kepala sekolah juga dapat membuat instance penugasan tersebut di seluruh akun anggota AWS organisasi

dan membangun koneksi antara direktori AWS Directory Service terkelola dan Pusat Identitas IAM. Saat fitur administratif baru dirilis, administrator akun akan diberikan izin ini secara otomatis.

Pengelompokan izin

Kebijakan ini dikelompokkan ke dalam pernyataan berdasarkan kumpulan izin yang diberikan.

- `AWSSSOMasterAccountAdministrator`— Memungkinkan IAM Identity Center untuk meneruskan peran layanan bernama `AWSServiceRoleforSSO` IAM Identity Center sehingga nantinya dapat mengambil peran dan melakukan tindakan atas nama mereka. Hal ini diperlukan ketika orang atau aplikasi mencoba untuk mengaktifkan IAM Identity Center. Untuk informasi selengkapnya, lihat Kelola akses ke Akun AWS.
- `AWSSSOMemberAccountAdministrator`— Memungkinkan IAM Identity Center untuk melakukan tindakan administrator akun di lingkungan multi-akun AWS . Untuk informasi selengkapnya, lihat AWS kebijakan terkelola: AWSSSOMemberAccountAdministrator.
- `AWSSSOManageDelegatedAdministrator`— Memungkinkan IAM Identity Center untuk mendaftar dan membatalkan pendaftaran administrator yang didelegasikan untuk organisasi Anda.

```
{
   "Version":"2012-10-17",
   "Statement":[
     {
         "Sid": "AWSSSOCreateSLR",
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
         "Resource": "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
         "Condition": {
            "StringLike": {
               "iam:AWSServiceName": "sso.amazonaws.com"
            }
         }
     },
     {
         "Sid":"AWSSSOMasterAccountAdministrator",
         "Effect":"Allow",
         "Action":"iam:PassRole",
         "Resource":"arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
         "Condition":{
```

```
            "StringLike":{
              "iam:PassedToService":"sso.amazonaws.com"
            }
         }
      },
      {
         "Sid":"AWSSSOMemberAccountAdministrator",
         "Effect":"Allow",
         "Action":[
            "ds:DescribeTrusts",
            "ds:UnauthorizeApplication",
            "ds:DescribeDirectories",
            "ds:AuthorizeApplication",
            "iam:ListPolicies",
            "organizations:EnableAWSServiceAccess",
            "organizations:ListRoots",
            "organizations:ListAccounts",
            "organizations:ListOrganizationalUnitsForParent",
            "organizations:ListAccountsForParent",
            "organizations:DescribeOrganization",
            "organizations:ListChildren",
            "organizations:DescribeAccount",
            "organizations:ListParents",
            "organizations:ListDelegatedAdministrators",
            "sso:*",
            "sso-directory:*",
            "identitystore:*",
            "identitystore-auth:*",
            "ds:CreateAlias",
            "access-analyzer:ValidatePolicy"
         ],
         "Resource":"*"
      },
      {
         "Sid": "AWSSSOManageDelegatedAdministrator",
         "Effect": "Allow",
         "Action": [
            "organizations:RegisterDelegatedAdministrator",
            "organizations:DeregisterDelegatedAdministrator"
         ],
         "Resource": "*",
         "Condition": {
            "StringEquals": {
               "organizations:ServicePrincipal": "sso.amazonaws.com"
```

```
        }
            }
        }

   ]
}
```

Informasi tambahan tentang kebijakan ini

Ketika Pusat Identitas IAM diaktifkan untuk pertama kalinya, layanan Pusat Identitas IAM membuat peran layanan yang ditautkan di akun AWS Organizations manajemen (sebelumnya akun master) sehingga Pusat Identitas IAM dapat mengelola sumber daya di akun Anda. Tindakan yang diperlukan adalah `iam:CreateServiceLinkedRole` dan`iam:PassRole`, yang ditampilkan dalam cuplikan berikut.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "AWSSSOCreateSLR",
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
         "Resource": "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
         "Condition": {
            "StringLike": {
               "iam:AWSServiceName": "sso.amazonaws.com"
            }
         }
      },
      {
         "Sid":"AWSSSOMasterAccountAdministrator",
         "Effect":"Allow",
         "Action":"iam:PassRole",
         "Resource":"arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO",
         "Condition":{
             "StringLike":{
               "iam:PassedToService":"sso.amazonaws.com"
             }
         }
      },
   ]
```

```
}
```

AWS kebijakan terkelola: AWSSSOMemberAccountAdministrator

`AWSSSOMemberAccountAdministrator`Kebijakan tersebut memberikan tindakan administratif yang diperlukan kepada kepala sekolah. Kebijakan ini ditujukan untuk kepala sekolah yang melakukan peran pekerjaan sebagai administrator Pusat Identitas IAM. Seiring waktu, daftar tindakan yang diberikan akan diperbarui agar sesuai dengan fungsionalitas IAM Identity Center yang ada dan tindakan yang diperlukan sebagai administrator.

Anda dapat melampirkan kebijakan `AWSSSOMemberAccountAdministrator` ke identitas IAM Anda. Saat Anda melampirkan `AWSSSOMemberAccountAdministrator` kebijakan ke identitas, Anda memberikan AWS IAM Identity Center izin administratif. Prinsipal dengan kebijakan ini dapat mengakses Pusat Identitas IAM dalam akun AWS Organizations manajemen dan semua akun anggota. Prinsipal ini dapat sepenuhnya mengelola semua operasi Pusat Identitas IAM, termasuk kemampuan untuk membuat pengguna, set izin, dan tugas. Kepala sekolah juga dapat membuat instance penugasan tersebut di seluruh akun anggota AWS organisasi dan membangun koneksi antara direktori AWS Directory Service terkelola dan Pusat Identitas IAM. Saat fitur administratif baru dirilis, administrator akun diberikan izin ini secara otomatis.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSSSOMemberAccountAdministrator",
      "Effect": "Allow",
      "Action": [
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "ds:UnauthorizeApplication",
        "ds:DescribeTrusts",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:DescribeAccount",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
```

```
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSSSOManageDelegatedAdministrator",
      "Effect": "Allow",
      "Action": [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource": "*",
        "Condition": {
           "StringEquals": {
              "organizations:ServicePrincipal": "sso.amazonaws.com"
        }
            }
        }
  ]
}
```

Informasi tambahan tentang kebijakan ini

Administrator IAM Identity Center mengelola pengguna, grup, dan kata sandi di toko direktori Pusat Identitas mereka (sso-direktori). Peran admin akun mencakup izin untuk tindakan berikut:

- `"sso:*"`
- `"sso-directory:*"`

Administrator Pusat Identitas IAM memerlukan izin terbatas untuk AWS Directory Service tindakan berikut untuk melakukan tugas sehari-hari.

- `"ds:DescribeTrusts"`
- `"ds:UnauthorizeApplication"`
- `"ds:DescribeDirectories"`

- "ds:AuthorizeApplication"
- “ds:CreateAlias”

Izin ini memungkinkan administrator IAM Identity Center untuk mengidentifikasi direktori yang ada dan mengelola aplikasi sehingga mereka dapat dikonfigurasi untuk digunakan dengan IAM Identity Center. Untuk informasi selengkapnya tentang setiap tindakan ini, lihat Izin AWS Directory Service API: Referensi tindakan, sumber daya, dan kondisi.

IAM Identity Center menggunakan kebijakan IAM untuk memberikan izin kepada pengguna IAM Identity Center. Administrator IAM Identity Center membuat set izin dan melampirkan kebijakan padanya. Administrator Pusat Identitas IAM harus memiliki izin untuk membuat daftar kebijakan yang ada sehingga mereka dapat memilih kebijakan mana yang akan digunakan dengan set izin yang mereka buat atau perbarui. Untuk menetapkan izin aman dan fungsional, administrator Pusat Identitas IAM harus memiliki izin untuk menjalankan validasi kebijakan IAM Access Analyzer.

- "iam:ListPolicies"
- "access-analyzer:ValidatePolicy"

Administrator IAM Identity Center memerlukan akses terbatas ke AWS Organizations tindakan berikut untuk melakukan tugas sehari-hari:

- "organizations:EnableAWSServiceAccess"
- "organizations:ListRoots"
- "organizations:ListAccounts"
- "organizations:ListOrganizationalUnitsForParent"
- "organizations:ListAccountsForParent"
- "organizations:DescribeOrganization"
- "organizations:ListChildren"
- "organizations:DescribeAccount"
- "organizations:ListParents"
- "organizations:ListDelegatedAdministrators"
- "organizations:RegisterDelegatedAdministrator"
- "organizations:DeregisterDelegatedAdministrator"

Izin ini memungkinkan administrator IAM Identity Center kemampuan untuk bekerja dengan sumber daya organisasi (akun) untuk tugas administratif Pusat Identitas IAM dasar seperti berikut:

- Mengidentifikasi akun manajemen milik organisasi
- Mengidentifikasi akun anggota yang menjadi milik organisasi
- Mengaktifkan akses AWS layanan untuk akun
- Menyiapkan dan mengelola administrator yang didelegasikan

Untuk informasi selengkapnya tentang menggunakan administrator yang didelegasikan dengan IAM Identity Center, lihat. Administrator yang didelegasikan Untuk informasi selengkapnya tentang cara izin ini digunakan AWS Organizations, lihat Menggunakan AWS Organizations dengan AWS layanan lain.

AWS kebijakan terkelola: AWSSSODirectoryAdministrator

Anda dapat melampirkan kebijakan `AWSSSODirectoryAdministrator` ke identitas IAM Anda.

Kebijakan ini memberikan izin administratif atas pengguna dan grup Pusat Identitas IAM. Prinsipal dengan kebijakan ini terlampir dapat melakukan pembaruan apa pun kepada pengguna dan grup IAM Identity Center. Isi dari pernyataan kebijakan ini ditampilkan di potongan berikut.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSSSODirectoryAdministrator",
            "Effect": "Allow",
            "Action": [
                "sso-directory:*",
                "identitystore:*",
                "identitystore-auth:*",
                "sso:ListDirectoryAssociations"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS kebijakan terkelola: AWSSSOReadOnly

Anda dapat melampirkan kebijakan `AWSSSOReadOnly` ke identitas IAM Anda.

Kebijakan ini memberikan izin hanya-baca yang memungkinkan pengguna melihat informasi di Pusat Identitas IAM. Prinsipal dengan kebijakan ini terlampir tidak dapat melihat pengguna atau grup Pusat Identitas IAM secara langsung. Prinsipal dengan kebijakan ini terlampir tidak dapat melakukan pembaruan apa pun di Pusat Identitas IAM. Misalnya, prinsipal dengan izin ini dapat melihat pengaturan Pusat Identitas IAM, tetapi tidak dapat mengubah nilai pengaturan apa pun. Isi dari pernyataan kebijakan ini ditampilkan di potongan berikut.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSSSOReadOnly",
            "Effect": "Allow",
            "Action": [
                "ds:DescribeDirectories",
                "ds:DescribeTrusts",
                "iam:ListPolicies",
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount",
                "organizations:ListParents",
                "organizations:ListChildren",
                "organizations:ListAccounts",
                "organizations:ListRoots",
                "organizations:ListAccountsForParent",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListDelegatedAdministrators",
                "sso:Describe*",
                "sso:Get*",
                "sso:List*",
                "sso:Search*",
                "sso-directory:DescribeDirectory",
                "access-analyzer:ValidatePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS kebijakan terkelola: AWSSSODirectoryReadOnly

Anda dapat melampirkan kebijakan `AWSSSODirectoryReadOnly` ke identitas IAM Anda.

Kebijakan ini memberikan izin hanya-baca yang memungkinkan pengguna melihat pengguna dan grup di Pusat Identitas IAM. Prinsipal dengan kebijakan ini terlampir tidak dapat melihat penetapan Pusat Identitas IAM, set izin, aplikasi, atau setelan. Prinsipal dengan kebijakan ini terlampir tidak dapat melakukan pembaruan apa pun di Pusat Identitas IAM. Misalnya, prinsipal dengan izin ini dapat melihat pengguna Pusat Identitas IAM, tetapi mereka tidak dapat mengubah atribut pengguna apa pun atau menetapkan perangkat MFA. Isi dari pernyataan kebijakan ini ditampilkan di potongan berikut.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSSSODirectoryReadOnly",
            "Effect": "Allow",
            "Action": [
                "sso-directory:Search*",
                "sso-directory:Describe*",
                "sso-directory:List*",
                "sso-directory:Get*",
                "identitystore:Describe*",
                "identitystore:List*",
                "identitystore-auth:ListSessions",
                "identitystore-auth:BatchGetSession"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS kebijakan terkelola: AWSIdentitySyncFullAccess

Anda dapat melampirkan kebijakan `AWSIdentitySyncFullAccess` ke identitas IAM Anda.

Prinsipal dengan kebijakan ini terlampir memiliki izin akses penuh untuk membuat dan menghapus profil sinkronisasi, mengaitkan atau memperbarui profil sinkronisasi dengan target sinkronisasi, membuat, mencantumkan, dan menghapus filter sinkronisasi, serta memulai atau menghentikan sinkronisasi.

Detail izin

Kebijakan ini mencakup izin berikut saat mengakses Active Directory.

- `ds:AuthorizeApplication`— Memungkinkan sinkronisasi identitas untuk memberikan akses ke aplikasi selama proses pembuatan profil sinkronisasi.
- `ds:UnauthorizeApplication`— Memungkinkan sinkronisasi identitas untuk menghapus akses ke aplikasi selama proses penghapusan profil sinkronisasi.

Isi dari pernyataan kebijakan ini ditampilkan di potongan berikut.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ds:AuthorizeApplication",
                "ds:UnauthorizeApplication"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "identity-sync:DeleteSyncProfile",
                "identity-sync:CreateSyncProfile",
                "identity-sync:GetSyncProfile",
                "identity-sync:StartSync",
                "identity-sync:StopSync",
                "identity-sync:CreateSyncFilter",
                "identity-sync:DeleteSyncFilter",
                "identity-sync:ListSyncFilters",
                "identity-sync:CreateSyncTarget",
                "identity-sync:DeleteSyncTarget",
                "identity-sync:GetSyncTarget",
                "identity-sync:UpdateSyncTarget"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS kebijakan terkelola: AWSIdentitySyncReadOnlyAccess

Anda dapat melampirkan kebijakan `AWSIdentitySyncReadOnlyAccess` ke identitas IAM Anda.

Kebijakan ini memberikan izin hanya-baca yang memungkinkan pengguna melihat informasi tentang profil sinkronisasi identitas, filter, dan setelan target. Prinsipal dengan kebijakan ini terlampir tidak dapat melakukan pembaruan apa pun pada setelan sinkronisasi. Misalnya, prinsipal dengan izin ini dapat melihat setelan sinkronisasi identitas, tetapi tidak dapat mengubah profil atau nilai filter apa pun. Isi dari pernyataan kebijakan ini ditampilkan di potongan berikut.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "identity-sync:GetSyncProfile",
                "identity-sync:ListSyncFilters",
                "identity-sync:GetSyncTarget",
            ],
            "Resource": "*"
        }
    ]
}
```

AWS kebijakan terkelola: AWSSSOServiceRolePolicy

Anda tidak dapat melampirkan `AWSSSOServiceRolePolicy` kebijakan ke identitas IAM Anda.

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan Pusat Identitas IAM untuk mendelegasikan dan menegakkan pengguna mana yang memiliki akses masuk tunggal ke pengguna tertentu. Akun AWS AWS Organizations Saat Anda mengaktifkan IAM, peran terkait layanan dibuat di semua bagian dalam organisasi Anda. Akun AWS IAM Identity Center juga menciptakan peran terkait layanan yang sama di setiap akun yang kemudian ditambahkan ke organisasi Anda. Peran ini memungkinkan Pusat Identitas IAM untuk mengakses sumber daya setiap akun atas nama Anda. Peran terkait layanan yang dibuat di masing-masing Akun AWS diberi nama. `AWSServiceRoleForSSO` Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk IAM Identity Center.

AWS kebijakan terkelola: AWSIAMIdentityCenterAllowListForIdentityContext

Saat mengambil peran dengan konteks identitas Pusat Identitas IAM, AWS Security Token Service (AWS STS) secara otomatis melampirkan `AWSIAMIdentityCenterAllowListForIdentityContext` kebijakan ke peran tersebut.

Kebijakan ini menyediakan daftar tindakan yang diizinkan saat Anda menggunakan propagasi identitas tepercaya dengan peran yang diasumsikan dengan konteks identitas Pusat Identitas IAM. Semua tindakan lain yang dipanggil dengan konteks ini diblokir. Konteks identitas diteruskan sebagai`ProvidedContext`. Isi dari pernyataan kebijakan ini ditampilkan di potongan berikut.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TrustedIdentityPropagation",
            "Effect": "Deny",
            "NotAction": [
                "athena:BatchGetNamedQuery",
                "athena:BatchGetPreparedStatement",
                "athena:BatchGetQueryExecution",
                "athena:CreateNamedQuery",
                "athena:CreatePreparedStatement",
                "athena:DeleteNamedQuery",
                "athena:DeletePreparedStatement",
                "athena:GetNamedQuery",
                "athena:GetPreparedStatement",
                "athena:GetQueryExecution",
                "athena:GetQueryResults",
                "athena:GetQueryResultsStream",
                "athena:GetQueryRuntimeStatistics",
                "athena:GetWorkGroup",
                "athena:ListNamedQueries",
                "athena:ListPreparedStatements",
                "athena:ListQueryExecutions",
                "athena:StartQueryExecution",
                "athena:StopQueryExecution",
                "athena:UpdateNamedQuery",
                "athena:UpdatePreparedStatement",
                "athena:GetDatabase",
                "athena:GetDataCatalog",
                "athena:GetTableMetadata",
                "athena:ListDatabases",
```

```
                "athena:ListDataCatalogs",
                "athena:ListTableMetadata",
                "athena:ListWorkGroups",
                "elasticmapreduce:GetClusterSessionCredentials",
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:GetTable",
                "glue:GetTables",
                "glue:GetTableVersions",
                "glue:GetPartition",
                "glue:GetPartitions",
                "glue:BatchGetPartition",
                "glue:GetColumnStatisticsForPartition",
                "glue:GetColumnStatisticsForTable",
                "glue:SearchTables",
                "glue:CreateDatabase",
                "glue:UpdateDatabase",
                "glue:DeleteDatabase",
                "glue:CreateTable",
                "glue:DeleteTable",
                "glue:BatchDeleteTable",
                "glue:UpdateTable",
                "glue:BatchCreatePartition",
                "glue:CreatePartition",
                "glue:DeletePartition",
                "glue:BatchDeletePartition",
                "glue:UpdatePartition",
                "glue:BatchUpdatePartition",
                "glue:DeleteColumnStatisticsForPartition",
                "glue:DeleteColumnStatisticsForTable",
                "glue:UpdateColumnStatisticsForPartition",
                "glue:UpdateColumnStatisticsForTable",
                "lakeformation:GetDataAccess",
                "s3:GetAccessGrantsInstanceForPrefix",
                "s3:GetDataAccess"
            ],
            "Resource": "*"
        }
    ]
}
```

Pusat Identitas IAM memperbarui kebijakan AWS terkelola

Tabel berikut menjelaskan pembaruan kebijakan AWS terkelola untuk Pusat Identitas IAM sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman riwayat Dokumen Pusat Identitas IAM.

Perubahan	Deskripsi	Tanggal
AWSIAMIdentityCenterAllowListForIdentityContext	Kebijakan ini sekarang mencakup `s3:GetAccessGrantsInstanceForPrefix` dan `s3:GetDataAccess` tindakan.	26 November 2023
AWSIAMIdentityCenterAllowListForIdentityContext	Kebijakan ini menyediakan daftar tindakan yang diizinkan saat Anda menggunakan propagasi identitas tepercaya dengan peran yang diasumsikan dengan konteks identitas Pusat Identitas IAM.	15 November 2023
AWSSSODirectoryReadOnly	Kebijakan ini sekarang menyertakan namespace baru `identitystore-auth` dengan izin baru untuk memungkinkan pengguna membuat daftar dan mendapatkan sesi.	21 Februari 2023
AWSSSOServiceRolePolicy	Kebijakan ini sekarang memungkinkan `UpdateSAMLProvider` tindakan diambil pada akun manajemen .	20 Oktober 2022
AWSSSOMasterAccountAdministrator	Kebijakan ini sekarang menyertakan namespace	20 Oktober 2022

Perubahan	Deskripsi	Tanggal
	baru `identitystore-auth` dengan izin baru untuk memungkinkan admin membuat daftar dan menghapus sesi untuk pengguna.	
AWSSSOMemberAccountAdministrator	Kebijakan ini sekarang menyertakan namespace baru `identitystore-auth` dengan izin baru untuk memungkinkan admin membuat daftar dan menghapus sesi untuk pengguna.	20 Oktober 2022
AWSSSODirectoryAdministrator	Kebijakan ini sekarang menyertakan namespace baru `identitystore-auth` dengan izin baru untuk memungkinkan admin membuat daftar dan menghapus sesi untuk pengguna.	20 Oktober 2022

Perubahan	Deskripsi	Tanggal
AWSSSOMasterAccountAdministrator	Kebijakan ini sekarang menyertakan izin baru untuk menelepon`ListDelegatedAdministrators`. AWS Organizations Kebijakan ini juga sekarang menyertakan subset izin `AWSSSOManageDelegatedAdministrator` yang mencakup izin untuk memanggil dan. `RegisterDelegatedAdministrator` `DeregisterDelegatedAdministrator`	Agustus 16, 2022
AWSSSOMemberAccountAdministrator	Kebijakan ini sekarang menyertakan izin baru untuk menelepon`ListDelegatedAdministrators`. AWS Organizations Kebijakan ini juga sekarang menyertakan subset izin `AWSSSOManageDelegatedAdministrator` yang mencakup izin untuk memanggil dan. `RegisterDelegatedAdministrator` `DeregisterDelegatedAdministrator`	Agustus 16, 2022
AWSSSOReadOnly	Kebijakan ini sekarang menyertakan izin baru untuk menelepon`ListDelegatedAdministrators`. AWS Organizations	Agustus 11, 2022

Perubahan	Deskripsi	Tanggal
AWSSSOServiceRolePolicy	Kebijakan ini sekarang menyertakan izin baru untuk menelepon DeleteRolePermissionsBoundary dan PutRolePermisionsBoundary .	14 Juli 2022
AWSSSOServiceRolePolicy	Kebijakan ini sekarang menyertakan izin baru yang memungkinkan panggilan ListAWSServiceAccessForOrganization and ListDelegatedAdministrators masuk AWS Organizations.	Mei 11, 2022
AWSSSOMasterAccountAdministrator AWSSSOMemberAccountAdministrator AWSSSOReadOnly	Tambahkan izin IAM Access Analyzer yang memungkinkan prinsipal menggunakan pemeriksaan kebijakan untuk validasi.	28 April 2022
AWSSSOMasterAccountAdministrator	Kebijakan ini sekarang memungkinkan semua tindakan layanan IAM Identity Center Identity Store. Untuk informasi tentang tindakan yang tersedia di layanan IAM Identity Center Identity Store, lihat Referensi API IAM Identity Center Identity Store.	29 Maret 2022

Perubahan	Deskripsi	Tanggal
AWSSSOMemberAccountAdministrator	Kebijakan ini sekarang memungkinkan semua tindakan layanan IAM Identity Center Identity Store.	29 Maret 2022
AWSSSODirectoryAdministrator	Kebijakan ini sekarang memungkinkan semua tindakan layanan IAM Identity Center Identity Store.	29 Maret 2022
AWSSSODirectoryReadOnly	Kebijakan ini sekarang memberikan akses ke tindakan baca layanan IAM Identity Center Identity Store. Akses ini diperlukan untuk mengambil informasi pengguna dan grup dari layanan IAM Identity Center Identity Store.	29 Maret 2022
AWSIdentitySyncFullAccess	Kebijakan ini memungkinkan akses penuh ke izin sinkronisasi identitas.	3 Maret 2022
AWSIdentitySyncReadOnlyAccess	Kebijakan ini memberikan izin hanya-baca yang memungkinkan prinsipal untuk melihat setelan sinkronisasi identitas.	3 Maret 2022
AWSSSOReadOnly	Kebijakan ini memberikan izin hanya-baca yang memungkinkan prinsipal untuk melihat setelan konfigurasi Pusat Identitas IAM.	4 Agustus 2021

Perubahan	Deskripsi	Tanggal
Pusat Identitas IAM mulai melacak perubahan	Pusat Identitas IAM mulai melacak perubahan untuk kebijakan AWS terkelola.	4 Agustus 2021

Menggunakan peran terkait layanan untuk IAM Identity Center

AWS IAM Identity Center menggunakan AWS Identity and Access Management peran terkait layanan (IAM). Peran terkait layanan adalah jenis peran IAM unik yang ditautkan langsung ke Pusat Identitas IAM. Ini telah ditentukan oleh IAM Identity Center dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda. Untuk informasi selengkapnya, lihat Peran terkait layanan.

Peran terkait layanan membuat pengaturan IAM Identity Center lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Pusat Identitas IAM mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya Pusat Identitas IAM yang dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas IAM lainnya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat Layanan AWS yang Berfungsi dengan IAM dan cari layanan yang memiliki Ya di kolom Peran Terkait Layanan. Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Izin peran terkait layanan untuk Pusat Identitas IAM

Pusat Identitas IAM menggunakan peran terkait layanan yang diberi nama AWSServiceRoleForSSOuntuk memberikan izin Pusat Identitas IAM untuk mengelola AWS sumber daya, termasuk peran IAM, kebijakan, dan IDP SAMP atas nama Anda.

Peran AWSServiceRoleForSSO terkait layanan mempercayai layanan berikut untuk mengambil peran:

- `IAM Identity Center`

Kebijakan izin peran AWSServiceRoleForSSO terkait layanan memungkinkan Pusat Identitas IAM menyelesaikan peran berikut di jalur “/aws-reserved/sso.amazonaws.com/” dan dengan awalan nama “_”: AWSReservedSSO

- iam:AttachRolePolicy
- iam:CreateRole
- iam:DeleteRole
- iam:DeleteRolePermissionsBoundary
- iam:DeleteRolePolicy
- iam:DetachRolePolicy
- iam:GetRole
- iam:ListRolePolicies
- iam:PutRolePolicy
- iam:PutRolePermissionsBoundary
- iam:ListAttachedRolePolicies

Kebijakan izin peran AWSServiceRoleForSSO terkait layanan memungkinkan Pusat Identitas IAM untuk menyelesaikan hal berikut pada penyedia SAMP dengan awalan nama sebagai "_": AWSSSO

- iam:CreateSAMLProvider
- iam:GetSAMLProvider
- iam:UpdateSAMLProvider
- iam:DeleteSAMLProvider

Kebijakan izin peran AWSServiceRoleForSSO terkait layanan memungkinkan Pusat Identitas IAM menyelesaikan hal-hal berikut di semua organisasi:

- organizations:DescribeAccount
- organizations:DescribeOrganization
- organizations:ListAccounts
- organizations:ListAWSServiceAccessForOrganization
- organizations:ListDelegatedAdministrators

Kebijakan izin peran AWSServiceRoleForSSO terkait layanan memungkinkan Pusat Identitas IAM menyelesaikan hal berikut pada semua peran IAM (*):

- iam:listRoles

Kebijakan izin peran AWSServiceRoleForSSO terkait layanan memungkinkan Pusat Identitas IAM untuk menyelesaikan hal berikut di “arn:aws:iam: :*:role/ /sso.amazonaws.com/”: aws-service-role AWSServiceRoleForSSO

- `iam:GetServiceLinkedRoleDeletionStatus`
- `iam:DeleteServiceLinkedRole`

Kebijakan izin peran memungkinkan Pusat Identitas IAM menyelesaikan tindakan berikut pada sumber daya.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"IAMRoleProvisioningActions",
         "Effect":"Allow",
         "Action":[
            "iam:AttachRolePolicy",
            "iam:CreateRole",
            "iam:DeleteRolePermissionsBoundary",
            "iam:PutRolePermissionsBoundary",
            "iam:PutRolePolicy",
            "iam:UpdateRole",
            "iam:UpdateRoleDescription",
            "iam:UpdateAssumeRolePolicy"
         ],
         "Resource":[
            "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
         ],
         "Condition":{
            "StringNotEquals":{
               "aws:PrincipalOrgMasterAccountId":"${aws:PrincipalAccount}"
            }
         }
      },
      {
         "Sid":"IAMRoleReadActions",
         "Effect":"Allow",
         "Action":[
            "iam:GetRole",
            "iam:ListRoles"
         ],
```

```
         "Resource":[
            "*"
         ]
      },
      {
         "Sid":"IAMRoleCleanupActions",
         "Effect":"Allow",
         "Action":[
            "iam:DeleteRole",
            "iam:DeleteRolePolicy",
            "iam:DetachRolePolicy",
            "iam:ListRolePolicies",
            "iam:ListAttachedRolePolicies"
         ],
         "Resource":[
            "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
         ]
      },
      {
         "Sid":"IAMSLRCleanupActions",
         "Effect":"Allow",
         "Action":[
            "iam:DeleteServiceLinkedRole",
            "iam:GetServiceLinkedRoleDeletionStatus",
            "iam:DeleteRole",
            "iam:GetRole"
         ],
         "Resource":[
            "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO"
         ]
      },
      {
        "Sid": "IAMSAMLProviderCreationAction",
        "Effect": "Allow",
        "Action": [
          "iam:CreateSAMLProvider"
      ],
      "Resource": [
         "arn:aws:iam::*:saml-provider/AWSSSO_*"
       ],
      "Condition": {
         "StringNotEquals": {
            "aws:PrincipalOrgMasterAccountId": "${aws:PrincipalAccount}"
```

```
          }
        }
      },
      {
        "Sid": "IAMSAMLProviderUpdateAction",
        "Effect": "Allow",
        "Action": [
          "iam:UpdateSAMLProvider"
        ],
        "Resource": [
           "arn:aws:iam::*:saml-provider/AWSSSO_*"
        ]
      },
      {
         "Sid":"IAMSAMLProviderCleanupActions",
         "Effect":"Allow",
         "Action":[
            "iam:DeleteSAMLProvider",
            "iam:GetSAMLProvider"
         ],
         "Resource":[
            "arn:aws:iam::*:saml-provider/AWSSSO_*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "organizations:DescribeAccount",
            "organizations:DescribeOrganization",
            "organizations:ListAccounts",
            "organizations:ListAWSServiceAccessForOrganization",
            "organizations:ListDelegatedAdministrators"
         ],
         "Resource":[
            "*"
         ]
      },
      {
         "Sid":"AllowUnauthAppForDirectory",
         "Effect":"Allow",
         "Action":[
            "ds:UnauthorizeApplication"
         ],
         "Resource":[
```

```
            "*"
         ]
      },
      {
         "Sid":"AllowDescribeForDirectory",
         "Effect":"Allow",
         "Action":[
            "ds:DescribeDirectories",
            "ds:DescribeTrusts"
         ],
         "Resource":[
            "*"
         ]
      },
      {
         "Sid":"AllowDescribeAndListOperationsOnIdentitySource",
         "Effect":"Allow",
         "Action":[
            "identitystore:DescribeUser",
            "identitystore:DescribeGroup",
            "identitystore:ListGroups",
            "identitystore:ListUsers"
         ],
         "Resource":[
            "*"
         ]
      }
   ]
}
```

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran tertaut layanan dalam Panduan Pengguna IAM.

Membuat peran terkait layanan untuk IAM Identity Center

Anda tidak perlu membuat peran terkait layanan secara manual. Setelah diaktifkan, IAM Identity Center membuat peran terkait layanan di semua akun dalam organisasi di Organizations. AWS IAM Identity Center juga menciptakan peran terkait layanan yang sama di setiap akun yang kemudian ditambahkan ke organisasi Anda. Peran ini memungkinkan Pusat Identitas IAM untuk mengakses sumber daya setiap akun atas nama Anda.

Catatan

- Jika Anda masuk ke akun AWS Organizations manajemen, akun tersebut akan menggunakan peran Anda yang saat ini masuk dan bukan peran terkait layanan. Ini mencegah eskalasi hak istimewa.
- Ketika IAM Identity Center melakukan operasi IAM apa pun di akun AWS Organizations manajemen, semua operasi terjadi dengan menggunakan kredensi prinsipal IAM. Ini memungkinkan log in CloudTrail untuk memberikan visibilitas siapa yang membuat semua perubahan hak istimewa di akun manajemen.

Important

Jika Anda menggunakan layanan IAM Identity Center sebelum 7 Desember 2017, ketika mulai mendukung peran terkait layanan, maka IAM Identity Center membuat AWSServiceRoleForSSO peran di akun Anda. Untuk mempelajari lebih lanjut, lihat Peran Baru yang Muncul di Akun IAM Saya.

Jika Anda menghapus peran tautan layanan ini dan kemudian perlu membuatnya lagi, Anda dapat menggunakan proses yang sama untuk membuat ulang peran di akun Anda.

Mengedit peran terkait layanan untuk IAM Identity Center

Pusat Identitas IAM tidak mengizinkan Anda mengedit peran AWSServiceRoleForSSO terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin merujuk peran tersebut. Namun, Anda dapat mengedit deskripsi peran ini menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit peran terkait layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk IAM Identity Center

Anda tidak perlu menghapus AWSServiceRoleForSSO peran secara manual. Ketika Akun AWS dihapus dari AWS organisasi, IAM Identity Center secara otomatis membersihkan sumber daya dan menghapus peran terkait layanan dari itu. Akun AWS

Anda juga dapat menggunakan konsol IAM, IAM CLI, atau IAM API untuk menghapus peran terkait layanan secara manual. Untuk melakukannya, Anda harus membersihkan sumber daya untuk peran tertaut layanan terlebih dahulu, lalu Anda dapat menghapusnya secara manual.

> **Note**
>
> Jika layanan Pusat Identitas IAM menggunakan peran saat Anda mencoba menghapus sumber daya, maka penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus sumber daya Pusat Identitas IAM yang digunakan oleh AWSServiceRoleForSSO

1. Hapus akses pengguna dan grupuntuk semua pengguna dan grup yang memiliki akses ke Akun AWS.
2. Hapus set izinyang telah Anda kaitkan dengan Akun AWS

Untuk menghapus peran terkait layanan secara manual menggunakan IAM

Gunakan konsol IAM, IAM CLI, atau IAM API untuk menghapus peran terkait layanan. AWSServiceRoleForSSO Untuk informasi selengkapnya, silakan lihat Menghapus Peran Terkait Layanan di Panduan Pengguna IAM.

Konsol IAM Identity Center dan otorisasi API

API konsol IAM Identity Center yang ada mendukung otorisasi ganda, yang memungkinkan Anda mempertahankan penggunaan operasi API yang ada saat API yang lebih baru tersedia. Jika Anda memiliki instans Pusat Identitas IAM yang telah dibuat sebelum 15 November 2023 dan 15 Oktober 2020, Anda dapat menggunakan tabel berikut untuk menentukan operasi API mana yang sekarang dipetakan ke operasi API yang lebih baru yang dirilis setelah tanggal tersebut.

Topik

- Tindakan API setelah November 2023
- Tindakan API setelah Oktober 2020

Tindakan API setelah November 2023

Instans Pusat Identitas IAM yang dibuat sebelum 15 November 2023 menghormati tindakan API lama dan baru selama tidak ada penolakan eksplisit pada tindakan apa pun. Instans yang dibuat setelah 15 November 2023 menggunakan tindakan API yang lebih baru untuk otorisasi di konsol Pusat Identitas IAM.

Nama operasi konsol digunakan sebelum 15 November 2023	Tindakan API digunakan setelah 15 November 2023
AssociateProfile	CreateApplicationAssignment
CreateManagedApplicationInstance | CreateApplicationInstance	CreateApplication
CreateManagedApplicationInstance	PutApplicationAuthenticationMethod
DeleteApplicationInstance | DeleteManagedApplicationInstance	DeleteApplication
DeleteSSO	DeleteInstance
DisassociateProfile	DeleteApplicationAssignment
GetApplicationTemplate	DescribeApplicationProvider
GetManagedApplicationInstance	DescribeApplication
GetSharedSsoConfiguration	DescribeInstance
ListApplicationInstances	ListApplications
ListApplicationTemplates	ListApplicationProviders
ListDirectoryAssociations	DescribeInstance
ListProfileAssociations	ListApplicationAssignments

Nama operasi konsol digunakan sebelum 15 November 2023	Tindakan API digunakan setelah 15 November 2023
UpdateApplicationInstanceDisplayData | UpdateApplicationInstanceStatus | UpdateManagedApplicationInstanceStatus	UpdateApplication

Tindakan API setelah Oktober 2020

Contoh Pusat Identitas IAM yang dibuat sebelum 15 Oktober 2020 menghormati tindakan API lama dan baru selama tidak ada penolakan eksplisit pada tindakan apa pun. Instans yang dibuat setelah 15 Oktober 2020 menggunakan tindakan API yang lebih baru untuk otorisasi di konsol Pusat Identitas IAM.

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
AssociateProfile	AssociateProfile	CreateAccountAssignment
AttachManagedPolicy	PutPermissionsPolicy	AttachManagedPolicyToPermissionSet
CreatePermissionSet	CreatePermissionSet	CreatePermissionSet
DeleteApplicationInstanceForAWsAccount	DeleteApplicationInstance | DeleteTrust	DeleteAccountAssignment
DeleteApplicationProfileForAwsAccount	DeleteProfile	DeleteAccountAssignment
DeletePermissionsPolicy	DeletePermissionsPolicy	DeleteInlinePolicyFromPermissionSet
DeletePermissionSet	DeletePermissionSet	DeletePermissionSet
DescribePermissionsPolicies	DescribePermissionsPolicies	ListManagedPoliciesInPermissionSet

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
DetachManagedPolicy	DeletePermissionsPolicy	DetachManagedPolicyFromPermissionSet
DisassociateProfile	DisassociateProfile	DeleteAccountAssignment
GetApplicationInstanceForAWSAccount	GetApplicationInstance	ListAccountAssignments
GetAWSAccountProfileStatus	GetProfile	ListPermissionSetsProvisionedToAccount
GetPermissionSet	GetPermissionSet	DescribePermissionSet
GetPermissionsPolicy	GetPermissionsPolicy	GetInlinePolicyForPermissionSet
ListAccountsWithProvisionedPermissionSet	ListApplicationInstances | GetApplicationInstance	ListAccountsForProvisionedPermissionSet
ListAWSAccountProfiles	ListProfiles | GetProfile	ListPermissionSetsProvisionedToAccount
ListPermissionSets	ListPermissionSets	ListPermissionSets
ListProfileAssociations	ListProfileAssociations	ListAccountAssignments
ProvisionApplicationInstanceForAWSAccount	GetApplicationInstance | CreateApplicationInstance	CreateAccountAssignment
ProvisionApplicationProfileForAWSAccountInstance	GetProfile | CreateProfile | UpdateProfile	CreateAccountAssignment
ProvisionSAMLProvider	GetTrust | CreateTrust | UpdateTrust	CreateAccountAssignment
PutPermissionsPolicy	PutPermissionsPolicy	PutInlinePolicyToPermissionSet

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
UpdatePermissionSet	UpdatePermissionSet	UpdatePermissionSet

AWS STS kunci konteks kondisi untuk Pusat Identitas IAM

Ketika kepala sekolah membuat permintaan AWS, AWS mengumpulkan informasi permintaan ke dalam konteks permintaan, yang digunakan untuk mengevaluasi dan mengotorisasi permintaan. Anda dapat menggunakan elemen `Condition` dari kebijakan JSON untuk membandingkan kunci dalam konteks permintaan dengan nilai kunci yang Anda tentukan dalam kebijakan Anda. Informasi permintaan disediakan oleh sumber yang berbeda, termasuk prinsipal yang membuat permintaan, sumber daya, permintaan yang dibuat terhadapnya, dan metadata tentang permintaan itu sendiri. Kunci kondisi khusus layanan didefinisikan untuk digunakan dengan layanan individual AWS .

IAM Identity Center mencakup penyedia AWS STS konteks yang memungkinkan aplikasi AWS terkelola dan aplikasi pihak ketiga untuk menambahkan nilai untuk kunci kondisi yang ditentukan oleh IAM Identity Center. Kunci-kunci ini termasuk dalam peran IAM. Nilai-nilai kunci ditetapkan ketika aplikasi meneruskan token ke AWS STS. Aplikasi memperoleh token yang diteruskan dengan salah satu AWS STS cara berikut:

- Selama otentikasi dengan IAM Identity Center.
- Setelah pertukaran token dengan penerbit token tepercaya untuk propagasi identitas tepercaya. Dalam hal ini, aplikasi memperoleh token dari penerbit token tepercaya dan menukar token itu dengan token dari IAM Identity Center.

Kunci ini biasanya digunakan oleh aplikasi yang terintegrasi dengan propagasi identitas tepercaya. Dalam beberapa kasus, ketika nilai kunci hadir, Anda dapat menggunakan kunci ini dalam kebijakan IAM yang Anda buat untuk mengizinkan atau menolak izin.

Misalnya, Anda mungkin ingin memberikan akses bersyarat ke sumber daya berdasarkan nilai`UserId`. Nilai ini menunjukkan pengguna IAM Identity Center mana yang menggunakan peran tersebut. Contohnya mirip dengan menggunakan`SourceId`. Tidak seperti`SourceId`, bagaimanapun, nilai untuk `UserId` mewakili pengguna tertentu yang diverifikasi dari toko identitas. Nilai ini hadir dalam token yang diperoleh aplikasi dan kemudian diteruskan ke AWS STS. Ini bukan string tujuan umum yang dapat berisi nilai arbitrer.

Topik

toko identitas: UserId

Kunci konteks ini adalah pengguna IAM Identity Center yang merupakan subjek dari pernyataan konteks yang dikeluarkan oleh IAM Identity Center. `UserId` Pernyataan konteks diteruskan ke. AWS STS Anda dapat menggunakan kunci ini untuk membandingkan pengguna Pusat Identitas IAM atas nama siapa permintaan dibuat dengan pengenal untuk pengguna yang Anda tentukan dalam kebijakan. `UserId`

- Ketersediaan — Kunci ini disertakan dalam konteks permintaan setelah pernyataan konteks yang dikeluarkan oleh IAM Identity Center disetel, ketika peran diasumsikan menggunakan AWS STS `assume-role` perintah apa pun dalam operasi AWS CLI atau AWS STS `AssumeRole` API.
- Tipe data - String
- Jenis nilai - Bernilai tunggal

toko identitas: IdentityStoreArn

Kunci konteks ini adalah ARN dari penyimpanan identitas yang dilampirkan pada instance IAM Identity Center yang mengeluarkan pernyataan konteks. Ini juga merupakan toko identitas tempat Anda dapat mencari atribut`identitystore:UserID`. Anda dapat menggunakan kunci ini dalam kebijakan untuk menentukan apakah `identitystore:UserID` berasal dari ARN toko identitas yang diharapkan.

- Ketersediaan — Kunci ini disertakan dalam konteks permintaan setelah pernyataan konteks yang dikeluarkan oleh IAM Identity Center disetel, ketika peran diasumsikan menggunakan AWS STS `assume-role` perintah apa pun dalam operasi AWS CLI atau AWS STS `AssumeRole` API.
- Tipe data - Arn, String
- Jenis nilai - Bernilai tunggal

pusat identitas: ApplicationArn

Kunci konteks ini adalah ARN dari aplikasi yang IAM Identity Center mengeluarkan pernyataan konteks. Anda dapat menggunakan kunci ini dalam kebijakan untuk menentukan apakah `identitycenter:ApplicationArn` berasal dari aplikasi yang diharapkan. Menggunakan kunci ini dapat membantu mencegah peran IAM diakses oleh aplikasi yang tidak terduga.

- Ketersediaan — Kunci ini disertakan dalam konteks permintaan operasi AWS STS `AssumeRole` API. Konteks permintaan mencakup pernyataan konteks yang dikeluarkan oleh IAM Identity Center.
- Tipe data - Arn, String
- Jenis nilai - Bernilai tunggal

pusat identitas: CredentialId

Kunci konteks ini adalah ID acak untuk kredensi peran yang disempurnakan identitas dan hanya digunakan untuk pencatatan. Karena nilai kunci ini tidak dapat diprediksi, sebaiknya Anda tidak menggunakannya untuk pernyataan konteks dalam kebijakan.

- Ketersediaan — Kunci ini disertakan dalam konteks permintaan operasi AWS STS `AssumeRole` API. Konteks permintaan mencakup pernyataan konteks yang dikeluarkan oleh IAM Identity Center.
- Tipe data - String
- Jenis nilai - Bernilai tunggal

pusat identitas: InstanceArn

Kunci konteks ini adalah ARN dari instance IAM Identity Center yang mengeluarkan pernyataan konteks untuk. `identitystore:UserID` Anda dapat menggunakan kunci ini untuk menentukan apakah pernyataan `identitystore:UserID` dan konteks berasal dari ARN misalnya IAM Identity Center yang diharapkan.

- Ketersediaan — Kunci ini disertakan dalam konteks permintaan operasi AWS STS `AssumeRole` API. Konteks permintaan mencakup pernyataan konteks yang dikeluarkan oleh IAM Identity Center.
- Tipe data - Arn, String

- Jenis nilai - Bernilai tunggal

Logging dan monitoring di IAM Identity Center

Sebagai praktik terbaik, Anda harus memantau organisasi Anda untuk memastikan bahwa perubahan dicatat. Ini membantu Anda memastikan bahwa setiap perubahan tak terduga dapat diselidiki dan perubahan yang tidak diinginkan dapat dibatalkan. AWS IAM Identity Center Saat ini mendukung dua AWS layanan yang membantu Anda memantau organisasi Anda dan aktivitas yang terjadi di dalamnya.

Topik

- Mencatat panggilan API Pusat Identitas IAM dengan AWS CloudTrail
- CloudWatch Acara Amazon
- Pencatatan sinkronisasi AD dan kesalahan sinkronisasi AD yang dapat dikonfigurasi

Mencatat panggilan API Pusat Identitas IAM dengan AWS CloudTrail

AWS IAM Identity Center terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di IAM Identity Center. CloudTrail menangkap panggilan API untuk IAM Identity Center sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari konsol Pusat Identitas IAM dan panggilan kode ke operasi API Pusat Identitas IAM. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara berkelanjutan ke bucket Amazon S3, termasuk acara untuk Pusat Identitas IAM. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat ke Pusat Identitas IAM, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

Topik

- Informasi Pusat Identitas IAM di CloudTrail
- Memahami entri berkas log Pusat Identitas IAM
- Memahami peristiwa masuk Pusat Identitas IAM

Informasi Pusat Identitas IAM di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi di Pusat Identitas IAM, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di situs Anda Akun AWS. Untuk informasi selengkapnya, lihat Melihat peristiwa dengan riwayat CloudTrail acara.

Untuk catatan acara yang sedang berlangsung di Anda Akun AWS, termasuk acara untuk IAM Identity Center, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol tersebut, jejak diterapkan ke semua Wilayah AWS . Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- Gambaran umum untuk membuat jejak
- CloudTrail layanan dan integrasi yang didukung
- Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima file CloudTrail log dari beberapa Wilayah dan Menerima file CloudTrail log dari beberapa akun

Saat CloudTrail logging diaktifkan di Anda Akun AWS, panggilan API yang dilakukan ke tindakan IAM Identity Center dilacak dalam file log. Catatan IAM Identity Center ditulis bersama dengan catatan AWS layanan lainnya dalam file log. CloudTrail menentukan kapan harus membuat dan menulis ke file baru berdasarkan periode waktu dan ukuran file.

CloudTrail Operasi Pusat Identitas IAM berikut didukung:

Operasi API konsol	Operasi API publik
`AssociateDirectory`	`AttachManagedPolicyToPermissionSet`
`AssociateProfile`	`CreateAccountAssignment`

Operasi API konsol	Operasi API publik
BatchDeleteSession	CreateInstanceAccessControlAttributeConfiguration
BatchGetSession	CreatePermissionSet
CreateApplicationInstance	DeleteAccountAssignment
CreateApplicationInstanceCertificate	DeleteInlinePolicyFromPermissionSet
CreatePermissionSet	DeleteInstanceAccessControlAttributeConfiguration
CreateProfile	DeletePermissionSet
DeleteApplicationInstance	DescribeAccountAssignmentCreationStatus
DeleteApplicationInstanceCertificate	DescribeAccountAssignmentDeletionStatus
DeletePermissionsPolicy	DescribeInstanceAccessControlAttributeConfiguration
DeletePermissionSet	DescribePermissionSet
DeleteProfile	DescribePermissionSetProvisioningStatus
DescribePermissionsPolicies	DetachManagedPolicyFromPermissionSet
DisassociateDirectory	GetInlinePolicyForPermissionSet
DisassociateProfile	ListAccountAssignmentCreationStatus

Operasi API konsol	Operasi API publik
GetApplicationInstance	ListAccountAssignmentDeletionStatus
GetApplicationTemplate	ListAccountAssignments
GetMfaDeviceManagementForDirectory	ListAccountsForProvisionedPermissionSet
GetPermissionSet	ListInstances
GetSSOStatus	ListManagedPoliciesInPermissionSet
ImportApplicationInstanceServiceProviderMetadata	ListPermissionSetProvisioningStatus
ListApplicationInstances	ListPermissionSets
ListApplicationInstanceCertificates	ListPermissionSetsProvisionedToAccount
ListApplicationTemplates	ListTagsForResource
ListDirectoryAssociations	ProvisionPermissionSet
ListPermissionSets	PutInlinePolicyToPermissionSet
ListProfileAssociations	TagResource
ListProfiles	UntagResource
ListSessions	UpdateInstanceAccessControlAttributeConfiguration
PutMfaDeviceManagementForDirectory	UpdatePermissionSet
PutPermissionsPolicy	

Operasi API konsol	Operasi API publik
StartSSO	
UpdateApplicationInstanceActiveCertificate	
UpdateApplicationInstanceDisplayData	
UpdateApplicationInstanceServiceProviderConfiguration	
UpdateApplicationInstanceStatus	
UpdateApplicationInstanceResponseConfiguration	
UpdateApplicationInstanceResponseSchemaConfiguration	
UpdateApplicationInstanceSecurityConfiguration	
UpdateDirectoryAssociation	
UpdateProfile	

Untuk informasi selengkapnya tentang operasi API publik IAM Identity Center, lihat Panduan Referensi API Pusat Identitas IAM.

CloudTrail Operasi IAM Identity Center Identity Store berikut didukung:

- AddMemberToGroup
- CompleteVirtualMfaDeviceRegistration
- CompleteWebAuthnDeviceRegistration
- CreateAlias
- CreateExternalIdPConfigurationForDirectory

- CreateGroup
- CreateUser
- DeleteExternalIdPConfigurationForDirectory
- DeleteGroup
- DeleteMfaDeviceForUser
- DeleteUser
- DescribeDirectory
- DescribeGroups
- DescribeUsers
- DisableExternalIdPConfigurationForDirectory
- DisableUser
- EnableExternalIdPConfigurationForDirectory
- EnableUser
- GetAWSSPConfigurationForDirectory
- ListExternalIdPConfigurationsForDirectory
- ListGroupsForUser
- ListMembersInGroup
- ListMfaDevicesForUser
- PutMfaDeviceManagementForDirectory
- RemoveMemberFromGroup
- SearchGroups
- SearchUsers
- StartVirtualMfaDeviceRegistration
- StartWebAuthnDeviceRegistration
- UpdateExternalIdPConfigurationForDirectory
- UpdateGroup
- UpdateMfaDeviceForUser
- UpdatePassword
- UpdateUser
- VerifyEmail

CloudTrail Tindakan OIDC Pusat Identitas IAM berikut didukung:

- `CreateToken`
- `RegisterClient`
- `StartDeviceAuthorization`

CloudTrail Tindakan Portal Pusat Identitas IAM berikut didukung:

- `Authenticate`
- `Federate`
- `ListApplications`
- `ListProfilesForApplication`
- `ListAccounts`
- `ListAccountRoles`
- `GetRoleCredentials`
- `Logout`

Setiap peristiwa atau entri log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut:

- Apakah permintaan dibuat dengan pengguna root atau kredenal pengguna AWS Identity and Access Management (IAM).
- Apakah permintaan dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat elemen CloudTrail UserIdentity.

Memahami entri berkas log Pusat Identitas IAM

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah

jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log untuk administrator (samadams@example.com) yang berlangsung di konsol Pusat Identitas IAM:


```
{
   "Records":[
      {
         "eventVersion":"1.05",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":"AIDAJAIENLMexample",
            "arn":"arn:aws:iam::08966example:user/samadams",
            "accountId":"08966example",
            "accessKeyId":"AKIAIIJM2K4example",
            "userName":"samadams"
         },
         "eventTime":"2017-11-29T22:39:43Z",
         "eventSource":"sso.amazonaws.com",
         "eventName":"DescribePermissionsPolicies",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"203.0.113.0",
         "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
         "requestParameters":{
            "permissionSetId":"ps-79a0dde74b95ed05"
         },
         "responseElements":null,
         "requestID":"319ac6a1-d556-11e7-a34f-69a333106015",
         "eventID":"a93a952b-13dd-4ae5-a156-d3ad6220b071",
         "readOnly":true,
         "resources":[

         ],
         "eventType":"AwsApiCall",
         "recipientAccountId":"08966example"
      }
   ]
}
```


Contoh berikut menunjukkan entri CloudTrail log untuk tindakan pengguna akhir (bobsmith@example.com) yang terjadi di portal AWS akses:

```
{
   "Records":[
      {
         "eventVersion":"1.05",
         "userIdentity":{
            "type":"Unknown",
            "principalId":"example.com//
S-1-5-21-1122334455-3652759393-4233131409-1126",
            "accountId":"08966example",
            "userName":"bobsmith@example.com"
         },
         "eventTime":"2017-11-29T18:48:28Z",
         "eventSource":"sso.amazonaws.com",
         "eventName":"ListApplications",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"203.0.113.0",
         "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
         "requestParameters":null,
         "responseElements":null,
         "requestID":"de6c0435-ce4b-49c7-9bcc-bc5ed631ce04",
         "eventID":"e6e1f3df-9528-4c6d-a877-6b2b895d1f91",
         "eventType":"AwsApiCall",
         "recipientAccountId":"08966example"
      }
   ]
}
```

Contoh berikut menunjukkan entri CloudTrail log untuk tindakan pengguna akhir (bobsmith@example.com) yang terjadi di IAM Identity Center OIDC:

```
{
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "Unknown",
        "principalId": "example.com//S-1-5-21-1122334455-3652759393-4233131409-1126",
        "accountId": "08966example",
        "userName": "bobsmith@example.com"
      },
      "eventTime": "2020-06-16T01:31:15Z",
      "eventSource": "sso.amazonaws.com",
      "eventName": "CreateToken",
      "awsRegion": "us-east-1",
```

```
      "sourceIPAddress": "203.0.113.0",
      "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
      "requestParameters": {
        "clientId": "clientid1234example",
        "clientSecret": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "grantType": "urn:ietf:params:oauth:grant-type:device_code",
        "deviceCode": "devicecode1234example"
      },
      "responseElements": {
        "accessToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "tokenType": "Bearer",
        "expiresIn": 28800,
        "refreshToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "idToken": "HIDDEN_DUE_TO_SECURITY_REASONS"
      },
      "eventID": "09a6e1a9-50e5-45c0-9f08-e6ef5089b262",
      "readOnly": false,
      "resources": [
        {
          "accountId": "08966example",
          "type": "IdentityStoreId",
          "ARN": "d-1234example"
        }
      ],
      "eventType": "AwsApiCall",
      "recipientAccountId": "08966example"
}
```


Memahami peristiwa masuk Pusat Identitas IAM

AWS CloudTrail mencatat peristiwa login yang berhasil dan tidak berhasil untuk semua sumber AWS IAM Identity Center identitas. Identitas sumber SSO dan Active Directory (AD Connector dan AWS Managed Microsoft AD) asli akan mencakup peristiwa masuk tambahan yang ditangkap setiap kali pengguna diminta untuk memecahkan tantangan atau faktor kredenal tertentu, serta status permintaan verifikasi kredenal tertentu. Hanya setelah pengguna menyelesaikan semua tantangan kredensi yang diperlukan, pengguna akan masuk, yang akan mengakibatkan `UserAuthentication` peristiwa dicatat.

Tabel berikut menangkap masing-masing nama CloudTrail acara masuk Pusat Identitas IAM, tujuan, dan penerapannya ke sumber identitas yang berbeda.

Nama peristiwa	Tujuan acara	Penerapan sumber identitas
`CredentialChallenge`	Digunakan untuk memberi tahu bahwa IAM Identity Center telah meminta pengguna untuk memecahkan tantangan kredensyal tertentu dan menentukan `CredentialType` yang diperlukan (Misalnya, PASSWORD atau TOTP).	Pengguna Pusat Identitas IAM asli, AD Connector, dan AWS Managed Microsoft AD
`CredentialVerification`	Digunakan untuk memberi tahu bahwa pengguna telah mencoba untuk memecahkan `CredentialChallenge` permintaan tertentu dan menentukan apakah kredensi itu berhasil atau gagal.	Pengguna Pusat Identitas IAM asli, AD Connector, dan AWS Managed Microsoft AD
`UserAuthentication`	Digunakan untuk memberi tahu bahwa semua persyaratan otentikasi yang ditantang pengguna telah berhasil diselesaikan dan bahwa pengguna berhasil masuk. Pengguna yang gagal menyelesaikan tantangan kredensi yang diperlukan tidak akan menghasilkan *`UserAuthentication`* peristiwa yang dicatat.	Semua sumber identitas

Tabel berikut menangkap bidang data peristiwa berguna tambahan yang terdapat dalam peristiwa login CloudTrail tertentu.

Nama peristiwa	Tujuan acara	Penerapan acara masuk	Contoh nilai
`AuthWorkflowID`	Digunakan untuk mengkorelasikan semua peristiwa yang dipancarkan di seluruh urutan masuk. Untuk setiap login pengguna, beberapa peristiwa dapat dipancarkan oleh IAM Identity Center.	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	“AuthWorkflowID”: “9de74b32-8362-4a01-a524-de21df59fd83"
`CredentialType`	Digunakan untuk menentukan kredensi atau faktor yang ditantang . `UserAuthentication` event akan mencakup semua `CredentialType` nilai yang berhasil diverifikasi di seluruh urutan login pengguna.	`CredentialChallenge` , `CredentialVerification` , `UserAuthentication`	CredentialType“: “PASSWORD” atau "CredentialType“: “PASSWORD, TOTP” (nilai yang mungkin termasuk: PASSWORD, TOTP, WEBAUTHN, EXTERNAL_IDP, RESYNC_TOTP)
`DeviceEnrollmentRequired`	Digunakan untuk menentukan bahwa pengguna diminta untuk mendaftarkan perangkat MFA selama login, dan bahwa pengguna	`UserAuthentication`	“DeviceEnrollmentRequired“: “benar”

Nama peristiwa	Tujuan acara	Penerapan acara masuk	Contoh nilai
	berhasil menyelesaikan permintaan itu.		
`LoginTo`	Digunakan untuk menentukan lokasi pengalihan mengikuti urutan login yang berhasil.	`UserAuthentication`	“LoginTo“:" https://mydirectory.awsapps.com/start/...”

Contoh peristiwa untuk skenario masuk Pusat Identitas IAM

Contoh berikut menunjukkan urutan CloudTrail peristiwa yang diharapkan untuk skenario masuk yang berbeda.

Topik

- Masuk berhasil saat mengautentikasi hanya dengan kata sandi
- Login berhasil saat mengautentikasi dengan penyedia identitas eksternal
- Login berhasil saat mengautentikasi dengan kata sandi dan aplikasi autentikator TOTP
- Masuk yang berhasil saat mengautentikasi dengan kata sandi dan pendaftaran MFA paksa diperlukan
- Gagal masuk saat mengautentikasi hanya dengan kata sandi

Masuk berhasil saat mengautentikasi hanya dengan kata sandi

Urutan peristiwa berikut menangkap contoh login hanya kata sandi yang berhasil.

CredentialChallenge (Kata Sandi)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
```

```
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-07T20:33:58Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "CredentialType":"PASSWORD"
   },
   "requestID":"5be44ffb-6946-4f47-acaf-1adebd4afead",
   "eventID":"27ea7725-c1fd-4355-bdba-d0e628e0e604",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```


Sukses CredentialVerification (Kata Sandi)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
```

```
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "CredentialType":"PASSWORD"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"c49640f6-0c8a-43d3-a6e0-900e3bb188d4",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```

Berhasil UserAuthentication (Hanya Kata Sandi)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
```

```
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?
state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
BshlIc5OBAA6ftz73M6LsfLWDlfOxviO2K3wet946lC30f_iWdilx-
zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7TqziOLiBLBUSx
east-1",
      "CredentialType":"PASSWORD"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"e959a95a-2b33-478d-906c-4fe303e8a9f1",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```


Login berhasil saat mengautentikasi dengan penyedia identitas eksternal

Urutan peristiwa berikut menangkap contoh login yang berhasil saat diautentikasi melalui protokol SAMP menggunakan penyedia identitas eksternal.

Sukses UserAuthentication (Penyedia Identitas Eksternal)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":""
   },
   "eventTime":"2020-12-07T20:34:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
```

```
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?
state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
BshlIc5OBAA6ftz73M6LsfLWDlfOxviO2K3wet946lC30f_iWdilx-
zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7TqziOLiBLBUSx
east-1",
      "CredentialType":"EXTERNAL_IDP"
   },
   "requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
   "eventID":"e959a95a-2b33-478d-906c-4fe303e8a9f1",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```


Login berhasil saat mengautentikasi dengan kata sandi dan aplikasi autentikator TOTP

Urutan peristiwa berikut menangkap contoh di mana otentikasi multi-faktor diperlukan selama login dan pengguna berhasil masuk menggunakan kata sandi dan aplikasi autentikator TOTP.

CredentialChallenge (Kata Sandi)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:13Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
```

```
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"PASSWORD"
   },
   "requestID":"e454ea66-1027-4d00-9912-09c0589649e1",
   "eventID":"d89cc0b5-a23a-4b88-843a-89329aeaef2e",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```


Sukses CredentialVerification (Kata Sandi)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:20Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
```

```
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"PASSWORD"
   },
   "requestID":"92c4ac90-0d9b-452d-95d5-728487612f5e",
   "eventID":"4533fd49-6669-4d0b-b272-a0b2139309a8",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```


CredentialChallenge (TOTP)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:20Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"TOTP"
   },
   "requestID":"92c4ac90-0d9b-452d-95d5-728487612f5e",
   "eventID":"29202f08-f240-40cc-b789-c0cea8a27847",
```

```
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```

Sukses CredentialVerification (TOTP)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:27Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"TOTP"
   },
   "requestID":"c40a691f-eeb1-4352-b286-5e909f96f318",
   "eventID":"e889ff1d-fcaf-454f-805d-7132cf2362a4",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
```

```
      "CredentialVerification":"Success"
   }
}
```

Berhasil UserAuthentication (Kata Sandi+TOTP)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T20:40:27Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVLeFhWeDRmZFJmMmxHcWYwdzhZck5RQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
\u003d11Fir1mCVJ-4Y5UY6RI10UCXvRePCHd6195xvYg1rwo1Pj7B-7UGIGlYUUVe31Nkzd7ihxKn6DMdnFfO01O8qc3RF
Sx-pjBXKG_jUcvBk_UILdGytV4o1u97h42B-
TA_6uwdmJiw1dcCz_Rv44d_BS0PkulW-5LVJy1oeP1H0FPPMeheyuk5Uy48d5of9-c\u0026wdc_csrf_token
\u003dNMlui44guoVnxRd0qu2tYJIdyyFPX6SDRNTspIScfMM0AgFbho1nvvCaxPTghHbgHCRIXdffFtzH0sL1ow419Bobn
\u0026organization\u003dd-9067230c03\u0026region\u003dus-east-1",
      "CredentialType":"PASSWORD,TOTP"
   },
   "requestID":"c40a691f-eeb1-4352-b286-5e909f96f318",
   "eventID":"7a8c8725-db2f-488d-a43e-788dc6c73a4a",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
```

```
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
}
```

Masuk yang berhasil saat mengautentikasi dengan kata sandi dan pendaftaran MFA paksa diperlukan

Urutan peristiwa berikut menangkap contoh login kata sandi yang berhasil, tetapi pengguna diminta dan berhasil menyelesaikan pendaftaran perangkat MFA sebelum menyelesaikan proses masuk mereka.

CredentialChallenge (Kata Sandi)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-09T01:24:02Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "CredentialType":"PASSWORD"
   },
   "requestID":"321f4b13-42b5-4005-a0f7-826cad26d159",
   "eventID":"8c707b0f-e45a-4a9c-bee2-ff68638d2f1b",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
```

```
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```


Sukses CredentialVerification (Kata Sandi)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-09T01:24:09Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "CredentialType":"PASSWORD"
   },
   "requestID":"12b57efa-0a92-4479-91a3-5b6641817c21",
   "eventID":"783b0c89-7142-4942-8b84-6ee0de1b992e",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Success"
   }
}
```

Berhasil UserAuthentication (Sandi+Pendaftaran MFA Diperlukan)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-09T01:24:14Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"UserAuthentication",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVGQ3VqdHF5aW9CUDdrNXRTVTJUaWNnQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
\u003d11eZ80S_maUsZ7ABETjeQhyWfvIHYz52rgR28sYAKN1oEk2G07czrwzXvE9HLlN2K9De8LyBEV83SFeDQfrWpkwXf
FJyJqkoGrt_w6rm_MpAn0uyrVq8udY EgU3fhOL3QWvWiquYnDPMyPmmy_qkZgR9rz__BI
\u0026wdc_csrf_token
\u003dJih9U62o5LQDtYLNqCK8a6xj0gJg5BRWq2tbl75y8vAmwZhAqrgrgbxXat2M646UZGp93krw7WYQdHIgi5OYI9QSc
\u003dd-9067230c03\u0026region\u003dus-east-1",
      "CredentialType":"PASSWORD",
      "DeviceEnrollmentRequired":"true"
   },
   "requestID":"74d24604-a365-4237-8c4a-350795494b92",
   "eventID":"a15bf257-7f37-46c0-b67c-fea5fa6166be",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "UserAuthentication":"Success"
   }
```

```
}
```

Gagal masuk saat mengautentikasi hanya dengan kata sandi

Urutan peristiwa berikut menangkap contoh login hanya kata sandi yang gagal.

CredentialChallenge (Kata Sandi)

```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T18:56:15Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialChallenge",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"adbf67c4-8188-4e2b-8527-fe539e328fa7",
      "CredentialType":"PASSWORD"
   },
   "requestID":"f54848ea-b1aa-402f-bf0d-a54561a2ffcc",
   "eventID":"d96f1d6c-dbd9-4a0b-9a45-6a2b66078c78",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialChallenge":"Success"
   }
}
```

Gagal CredentialVerification (Kata Sandi)


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"Unknown",
      "principalId":"111122223333",
      "arn":"",
      "accountId":"111122223333",
      "accessKeyId":"",
      "userName":"user1"
   },
   "eventTime":"2020-12-08T18:56:21Z",
   "eventSource":"signin.amazonaws.com",
   "eventName":"CredentialVerification",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"203.0.113.0",
   "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
   "requestParameters":null,
   "responseElements":null,
   "additionalEventData":{
      "AuthWorkflowID":"adbf67c4-8188-4e2b-8527-fe539e328fa7",
      "CredentialType":"PASSWORD"
   },
   "requestID":"04528c82-a678-4a1f-a56d-ea2c6445a72a",
   "eventID":"9160fe06-fc2a-474f-9b78-000ee067a09d",
   "readOnly":false,
   "eventType":"AwsServiceEvent",
   "managementEvent":true,
   "eventCategory":"Management",
   "recipientAccountId":"111122223333",
   "serviceEventDetails":{
      "CredentialVerification":"Failure"
   }
}
```


CloudWatch Acara Amazon

IAM Identity Center dapat bekerja dengan CloudWatch Acara untuk meningkatkan 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 aturan CloudWatch Peristiwa 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 AWS Lambda fungsi yang mencatat detail tindakan untuk ditinjau nanti.

Untuk mempelajari lebih lanjut tentang CloudWatch Acara, termasuk cara mengonfigurasi dan mengaktifkannya, lihat Panduan Pengguna CloudWatch Acara Amazon.

Pencatatan sinkronisasi AD dan kesalahan sinkronisasi AD yang dapat dikonfigurasi

Anda dapat mengaktifkan pencatatan pada sinkronisasi Direktori Aktif (AD) dan konfigurasi sinkronisasi AD yang dapat dikonfigurasi untuk menerima log dengan informasi tentang kesalahan yang dapat terjadi selama proses sinkronisasi. Dengan log ini, Anda dapat memantau jika ada masalah dengan sinkronisasi AD dan sinkronisasi AD yang dapat dikonfigurasi dan mengambil tindakan jika berlaku. Anda dapat mengirim log ke grup CloudWatch log Amazon Log, bucket Amazon Simple Storage Service (Amazon S3), atau Amazon Data Firehose dengan pengiriman lintas akun yang didukung untuk bucket Amazon S3 dan Firehose.

Untuk informasi selengkapnya tentang batasan, izin, dan log vended, lihat Mengaktifkan logging dari. Layanan AWS

> **Note**
>
> Anda dikenakan biaya untuk logging. Untuk informasi selengkapnya, lihat Log Terjual di halaman CloudWatch Harga Amazon.

Untuk mengaktifkan sinkronisasi AD dan log kesalahan sinkronisasi AD yang dapat dikonfigurasi

1. Masuk ke konsol Pusat Identitas IAM.
2. Pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Sumber identitas, pilih Tindakan, lalu pilih Kelola log.
4. Pilih Tambahkan pengiriman log dan salah satu jenis tujuan berikut.

a. Pilih Ke Amazon CloudWatch Log. Kemudian pilih atau masukkan grup log tujuan.
b. Pilih Ke Amazon S3. Kemudian pilih atau masukkan ember tujuan.
c. Pilih Untuk Firehose. Kemudian pilih atau masukkan aliran pengiriman tujuan.

5. Pilih Kirim.

Untuk menonaktifkan sinkronisasi AD dan log kesalahan sinkronisasi AD yang dapat dikonfigurasi

1. Masuk ke konsol Pusat Identitas IAM.
2. Pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Sumber identitas, pilih Tindakan, lalu pilih Kelola log.
4. Pilih Hapus untuk tujuan yang ingin Anda hapus.
5. Pilih Kirim.

Bidang log kesalahan sinkronisasi AD dan sinkronisasi AD yang dapat dikonfigurasi

Lihat daftar berikut untuk kemungkinan bidang log kesalahan.

`sync_profile_name`

Nama profil sinkronisasi.

`error_code`

Kode kesalahan yang mewakili jenis kesalahan apa yang telah terjadi.

`error_message`

Pesan yang berisi informasi rinci tentang kesalahan yang terjadi.

`sync_source`

Sumber sinkronisasi adalah tempat entitas disinkronkan. Untuk IAM Identity Center, ini adalah Active Directory (AD) yang dikelola oleh AWS Directory Service. Sumber sinkronisasi berisi domain dan ARN dari direktori yang terpengaruh.

`sync_target`

Target sinkronisasi adalah tujuan tempat entitas disimpan. Untuk IAM Identity Center, ini adalah Toko Identitas. Target sinkronisasi berisi ARN Toko Identitas yang terpengaruh.

`source_entity_id`

Pengidentifikasi unik untuk entitas yang menyebabkan kesalahan. Untuk IAM Identity Center, ini adalah SID entitas.

`source_entity_type`

Jenis entitas yang menyebabkan kesalahan. Nilai dapat berupa `USER` atau `GROUP`.

`eventTimestamp`

Stempel waktu saat kesalahan terjadi.

Contoh log kesalahan sinkronisasi AD dan sinkronisasi AD yang dapat dikonfigurasi

Contoh 1: Log kesalahan untuk kata sandi kedaluwarsa untuk direktori AD

```
{
    "sync_profile_name": "EXAMPLE-PROFILE-NAME",
    "error" : {
        "error_code": "InvalidDirectoryCredentials",
        "error_message": "The password for your AD directory has expired. Please reset
 the password to allow Identity Sync to access the directory."
    },
    "sync_source": {
        "arn": "arn:aws:ds:us-east-1:123456789:directory/d-123456",
        "domain": "EXAMPLE.com"
    },
    "eventTimestamp": "1683355579981"
}
```

Contoh 2: Log kesalahan untuk pengguna dengan nama pengguna yang tidak unik

```
{
    "sync_profile_name": "EXAMPLE-PROFILE-NAME",
    "error" : {
        "error_code": "ConflictError",
        "error_message": "The source entity has a username conflict with the sync
 target. Please verify that the source identity has a unique username in the target."
    },
    "sync_source": {
        "arn": "arn:aws:ds:us-east-1:111122223333:directory/d-123456",
        "domain": "EXAMPLE.com"
```

```
    },
    "sync_target": {
        "arn": "arn:aws:identitystore::111122223333:identitystore/d-123456"
    },
    "source_entity_id": "SID-1234",
    "source_entity_type": "USER",
    "eventTimestamp": "1683355579981"
}
```

Validasi kepatuhan untuk Pusat Identitas IAM

Auditor pihak ketiga menilai keamanan dan kepatuhan Layanan AWS seperti AWS IAM Identity Center sebagai bagian dari beberapa program AWS kepatuhan.

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 mengevaluasi sumber daya AWS Anda dan memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- 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.

Standar kepatuhan yang didukung

IAM Identity Center telah menjalani audit untuk standar berikut dan memenuhi syarat untuk digunakan sebagai bagian dari solusi yang Anda perlukan untuk mendapatkan sertifikasi kepatuhan.

AWS telah memperluas program kepatuhan Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA) untuk memasukkan IAM Identity Center sebagai layanan yang memenuhi syarat HIPAA.

AWS menawarkan whitepaper yang berfokus pada HIPAA untuk pelanggan yang ingin mempelajari lebih lanjut tentang bagaimana mereka dapat menggunakan Layanan AWS untuk memproses dan menyimpan informasi kesehatan. Untuk informasi selengkapnya, lihat Kepatuhan HIPAA.

	Program Penilai Terdaftar Keamanan Informasi (IRAP) memungkinkan pelanggan Pemerintah Australia untuk memastikan bahwa kontrol kepatuhan yang tepat telah diterapkan dan menentukan model tanggung jawab yang sesuai untuk memenuhi persyaratan Manual Keamanan Informasi Pemerintah Australia (ISM) yang diproduksi oleh Australian Cyber Security Centre (ACSC). Untuk informasi lebih lanjut, lihat Sumber Daya IRAP.
	IAM Identity Center memiliki Atestation of Compliance for Payment Card Industry (PCI) Data Security Standard (DSS) versi 3.2 di Service Provider Level 1. Pelanggan yang menggunakan AWS produk dan layanan untuk menyimpan, memproses, atau mengirimkan data pemegang kartu dapat menggunakan sumber identitas berikut di IAM Identity Center untuk mengelola sertifikasi kepatuhan PCI DSS mereka sendiri: • Direktori Aktif • Penyedia identitas eksternal Sumber identitas IAM Identity Center saat ini tidak sesuai dengan PCI DSS. Untuk informasi selengkapnya tentang PCI DSS, termasuk cara meminta salinan PCI AWS Compliance Package, lihat PCI DSS level 1.

Laporan System & Organization Control (SOC) adalah laporan pemeriksaan pihak ketiga independen yang menunjukkan bagaimana IAM Identity Center mencapai kontrol dan tujuan kepatuhan utama. Laporan ini membantu Anda dan auditor memahami bagaimana kontrol mendukung operasi dan kepatuhan. Ada tiga jenis laporan SOC:

- AWS Laporan SOC 1 - Unduh dengan AWS Artifak
- AWS SOC 2: Laporan Keamanan, Ketersediaan, & Kerahasiaan - Unduh dengan Artifak AWS
- AWS SOC 3: Laporan Keamanan, Ketersediaan, & Kerahasiaan

IAM Identity Center berada dalam lingkup untuk AWS laporan SOC 1, SOC 2, dan SOC 3. Untuk informasi selengkapnya, lihat Kepatuhan SOC.

Ketahanan di Pusat Identitas IAM

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang dan mengoperasikan aplikasi dan basis data yang melakukan secara otomatis pinda saat gagal/failover di antara zona-zona tanpa terputus. Zona Ketersediaan lebih sangat tersedia, lebih toleran kesalahan, dan lebih dapat diskalakan daripadai infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang AWS Wilayah dan Availability Zone, lihat infrastruktur AWS global.

Untuk mempelajari lebih lanjut tentang AWS IAM Identity Center ketahanan, lihat. Desain ketahanan dan perilaku Regional

Keamanan infrastruktur di Pusat Identitas IAM

Sebagai layanan terkelola, AWS IAM Identity Center dilindungi oleh prosedur keamanan jaringan AWS global yang dijelaskan dalam Praktik Terbaik untuk Keamanan, Identitas, & Kepatuhan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses Pusat Identitas IAM melalui jaringan. Klien harus mendukung Keamanan Lapisan Pengangkutan (TLS) 1.0 atau versi yang lebih baru. Kami merekomendasikan TLS 1.2 atau versi yang lebih baru. Klien juga harus mendukung suite cipher dengan perfect forward secrecy (PFS) seperti Ephemeral Diffie-Hellman (DHE) atau Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Sebagian besar sistem modern seperti Java 7 dan sistem yang lebih baru mendukung mode ini.

Selain itu, permintaan harus ditandatangani dengan menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan pengguna utama IAM. Atau Anda bisa menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

Penandaan pada sumber daya AWS IAM Identity Center

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 sebuah string kosong.

Tag membantu Anda mengidentifikasi dan mengatur sumber daya AWS. Banyak layanan AWS yang mendukung penandaan, sehingga Anda dapat menetapkan tag yang sama ke sumber daya dari layanan yang berbeda untuk menunjukkan bahwa sumber daya tersebut terkait. Misalnya, Anda dapat menetapkan tag yang sama ke izin tertentu yang ditetapkan dalam instance Pusat Identitas IAM Anda. Untuk informasi selengkapnya tentang strategi penandaan, lihat Menandai AWS Sumber Daya di Referensi Umum AWSPanduan dan Menandai Praktik Terbaik.

Selain mengidentifikasi, mengatur, dan melacak AWS sumber daya Anda dengan tag, Anda dapat menggunakan tag dalam kebijakan IAM untuk membantu mengontrol siapa yang dapat melihat dan berinteraksi dengan sumber daya Anda. Untuk mempelajari lebih lanjut tentang menggunakan tag untuk mengontrol akses, lihat Mengontrol akses ke AWS sumber daya menggunakan tag di Panduan Pengguna IAM. Misalnya, Anda dapat mengizinkan pengguna untuk memperbarui set izin Pusat Identitas IAM, tetapi hanya jika set izin Pusat Identitas IAM memiliki `owner` tag dengan nilai nama pengguna tersebut.

Saat ini, Anda dapat menerapkan tag ke set izin saja. Anda tidak dapat menerapkan tag ke peran terkait yang dibuat oleh IAM Identity Center. Akun AWS Anda dapat menggunakan konsol Pusat Identitas IAM, AWS CLI atau API Pusat Identitas IAM untuk menambahkan, mengedit, atau menghapus tag untuk set izin.

Bagian berikut memberikan informasi lebih lanjut tentang tag untuk IAM Identity Center.

Pembatasan tanda

Pembatasan dasar berikut berlaku untuk tag pada sumber daya Pusat Identitas IAM:

- Jumlah maksimum tag yang dapat Anda tetapkan ke sumber daya adalah 50.
- Panjang kunci maksimum adalah 128 karakter Unicode.
- Panjang nilai maksimum adalah 256 karakter Unicode.
- Karakter yang valid untuk kunci tag dan nilai adalah:

  a-z, A-Z, 0-9, spasi, dan karakter berikut: _.:/= + - dan @
- Kunci dan nilai peka huruf besar dan kecil.
- Jangan gunakan `aws:` sebagai prefiks untuk kunci; ini dicadangkan untuk penggunaan AWS

Mengelola tag dengan menggunakan konsol IAM Identity Center

Anda dapat menggunakan konsol Pusat Identitas IAM untuk menambahkan, mengedit, dan menghapus tag yang terkait dengan instans atau set izin Anda.

Untuk mengelola tag set izin untuk konsol Pusat Identitas IAM

1. Buka konsol Pusat Identitas IAM.
2. Pilih set Izin.
3. Pilih nama set izin yang memiliki tag yang ingin Anda kelola.
4. Pada tab Izin, di bawah Tag, lakukan salah satu hal berikut, lalu lanjutkan ke langkah berikutnya:

   a. Jika tag sudah ditetapkan untuk set izin ini, pilih Edit tag.

   b. Jika tidak ada tag yang ditetapkan ke set izin ini, pilih Tambahkan tag.
5. Untuk setiap tag baru, ketikkan nilai di kolom Kunci dan Nilai (opsional). Setelah selesai, pilih Simpan perubahan.

Untuk menghapus tag, pilih X di kolom Hapus di sebelah tag yang ingin Anda hapus.

Untuk mengelola tag untuk instance IAM Identity Center

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan.

3. Pilih tab Tag (Tanda).
4. Untuk setiap tag, ketikkan nilai di bidang Kunci dan Nilai (opsional). Setelah selesai, pilih tombol Tambahkan tag baru.

Untuk menghapus tag, pilih tombol Hapus di sebelah tag yang ingin Anda hapus.

Contoh AWS CLI

AWS CLIIni menyediakan perintah yang dapat Anda gunakan untuk mengelola tag yang Anda tetapkan ke set izin Anda.

Menetapkan tanda

Gunakan perintah berikut untuk menetapkan tag ke set izin Anda.

Example **`tag-resource`**Perintah untuk set izin

Tetapkan tag ke set izin dengan menggunakan `tag-resource`dalam `sso` kumpulan perintah:

```
$ aws sso-admin tag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tags Stage=Test
```

Perintah ini mencakup parameter-parameter berikut ini:

- `instance-arn`— Nama Sumber Daya Amazon (ARN) dari instans Pusat Identitas IAM di mana operasi akan berjalan.
- `resource-arn`— ARN sumber daya dengan tag yang akan dicantumkan.
- `tags` — Pasangan nilai kunci tanda.

Untuk menetapkan beberapa tanda sekaligus, tentukan tanda tersebut dalam daftar yang dipisahkan koma:

```
$ aws sso-admin tag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tags Stage=Test,CostCenter=80432,Owner=SysEng
```

Melihat tanda

Gunakan perintah berikut untuk melihat tag yang telah Anda tetapkan ke set izin Anda.

Example **`list-tags-for-resource`**Perintah untuk set izin

Lihat tag yang ditetapkan ke set izin dengan menggunakan `list-tags-for-resource`dalam `sso` kumpulan perintah:

```
$ aws sso-admin list-tags-for-resource --resource-arn sso-resource-arn
```

Menghapus tanda

Gunakan perintah berikut untuk menghapus tag dari set izin.

Example **`untag-resource`**Perintah untuk set izin

Hapus tag dari set izin dengan menggunakan `untag-resource`dalam `sso` kumpulan perintah:

```
$ aws sso-admin untag-resource \
> --instance-arn sso-instance-arn \
> --resource-arn sso-resource-arn \
> --tag-keys Stage CostCenter Owner
```

Untuk parameter `--tag-keys`, menentukan satu atau lebih kunci tanda, dan tidak termasuk nilai tanda.

Menerapkan tag saat Anda membuat set izin

Gunakan perintah berikut untuk menetapkan tag pada saat Anda membuat set izin.

Example **`create-permission-set`**Perintah dengan tag

Saat Anda membuat set izin dengan menggunakan `create-permission-set`perintah, Anda dapat menentukan tag dengan `--tags` parameter:

```
$ aws sso-admin create-permission-set \
> --instance-arn sso-instance-arn \
> --name permission=set-name \
> --tags Stage=Test,CostCenter=80432,Owner=SysEng
```

Mengelola tag menggunakan IAM Identity Center API

Anda dapat menggunakan tindakan berikut di API Pusat Identitas IAM untuk mengelola tag untuk set izin Anda.

Tindakan API untuk tag instance IAM Identity Center

Gunakan tindakan API berikut untuk menetapkan, melihat, dan menghapus tag untuk set izin atau instance Pusat Identitas IAM.

- TagResource
- ListTagsForResource
- UntagResource
- CreatePermissionSet
- CreateInstance

IntegrasiAWSCLI dengan IAM Identity Center

AWSIntegrasi Command Line Interface (CLI) versi 2 dengan IAM Identity Center menyederhanakan proses login. Pengembang dapat masuk langsung keAWS CLImenggunakan kredensi Active Directory atau IAM Identity Center yang sama yang biasanya mereka gunakan untuk masuk ke IAM Identity Center, dan mengakses akun dan peran yang ditetapkan. Misalnya, setelah administrator mengkonfigurasi IAM Identity Center untuk menggunakan Active Directory untuk otentikasi, pengembang dapat masuk keAWS CLIlangsung menggunakan kredensi Active Directory mereka.

AWSIntegrasi CLI dengan IAM Identity Center menawarkan manfaat sebagai berikut:

- Perusahaan dapat memungkinkan pengembang mereka untuk masuk menggunakan kredensi dari IAM Identity Center atau Active Directory dengan menghubungkan IAM Identity Center ke Active Directory mereka menggunakanAWS Directory Service.
- Pengembang dapat masuk dari CLI untuk akses yang lebih cepat.
- Pengembang dapat membuat daftar dan beralih di antara akun dan peran yang telah mereka tetapkan aksesnya.
- Pengembang dapat membuat dan menyimpan profil peran bernama dalam konfigurasi CLI mereka secara otomatis dan mereferensikannya di CLI untuk menjalankan perintah di akun dan peran yang diinginkan.
- CLI mengelola kredensi jangka pendek secara otomatis sehingga pengembang dapat memulai dan tetap berada di CLI dengan aman tanpa gangguan, dan menjalankan skrip yang berjalan lama.

Bagaimana cara mengintegrasikanAWSCLI dengan IAM Identity Center

Untuk menggunakanAWSIntegrasi CLI dengan IAM Identity Center, Anda perlu mengunduh, menginstal, dan mengonfigurasiAWS Command Line Interfaceversi 2. Untuk langkah-langkah terperinci tentang cara mengunduh dan mengintegrasikanAWS CLIdengan IAM Identity Center, lihatMengonfigurasiAWSCLI untuk menggunakan IAM Identity Centerdi dalamAWS Command Line InterfacePanduan Pengguna.

AWS IAM Identity Center Ketersediaan wilayah

IAM Identity Center tersedia dalam beberapa yang umum digunakan Wilayah AWS. Ketersediaan ini memudahkan Anda untuk mengonfigurasi akses pengguna ke beberapa Akun AWS aplikasi bisnis. Ketika pengguna Anda masuk ke portal AWS akses, mereka dapat memilih izin yang mereka miliki, dan kemudian mengakses. Akun AWS AWS Management Console Untuk daftar lengkap yang didukung Pusat Identitas IAM, lihat titik akhir dan kuota Pusat Identitas IAM. Wilayah AWS

Data Wilayah Pusat Identitas IAM

Saat pertama kali mengaktifkan IAM Identity Center, semua data yang Anda konfigurasikan di IAM Identity Center disimpan di Wilayah tempat Anda mengonfigurasinya. Data ini mencakup konfigurasi direktori, set izin, instance aplikasi, dan penugasan pengguna ke aplikasi. Akun AWS Jika Anda menggunakan penyimpanan identitas Pusat Identitas IAM, semua pengguna dan grup yang Anda buat di Pusat Identitas IAM juga disimpan di Wilayah yang sama. Kami menyarankan Anda menginstal Pusat Identitas IAM di Wilayah yang ingin Anda tetap tersedia bagi pengguna, bukan Wilayah yang mungkin perlu Anda nonaktifkan.

AWS Organizations hanya mendukung satu Wilayah AWS per satu. Untuk mengaktifkan Pusat Identitas IAM di Wilayah yang berbeda, Anda harus terlebih dahulu menghapus konfigurasi Pusat Identitas IAM Anda saat ini. Beralih ke Wilayah lain juga mengubah URL untuk portal AWS akses, dan Anda harus mengkonfigurasi ulang semua set izin dan penetapan.

Panggilan Lintas Wilayah

IAM Identity Center menggunakan Amazon Simple Email Service (Amazon SES) untuk mengirim email ke pengguna akhir ketika mereka mencoba masuk dengan kata sandi satu kali (OTP) sebagai faktor otentikasi kedua. Email ini juga dikirim untuk acara manajemen identitas dan kredensi tertentu, seperti ketika pengguna diundang untuk mengatur kata sandi awal, untuk memverifikasi alamat email, dan mengatur ulang kata sandi mereka. Amazon SES tersedia dalam subset yang didukung Pusat Identitas IAM. Wilayah AWS

Pusat Identitas IAM memanggil titik akhir lokal Amazon SES saat Amazon SES tersedia secara lokal di file. Wilayah AWS Jika Amazon SES tidak tersedia secara lokal, Pusat Identitas IAM memanggil titik akhir Amazon SES secara berbeda Wilayah AWS, seperti yang ditunjukkan dalam tabel berikut.

Kode Wilayah Amazon SES tercantum dalam tabel berikut.

Kode Wilayah Pusat Identitas IAM	Nama Wilayah Pusat Identitas IAM	Kode Wilayah Amazon SES	Nama wilayah Amazon SES
us-gov-east-1	AWS GovCloud (AS-Timur)	us-gov-west-1	AWS GovCloud (AS-Barat)
ap-east-1	Asia Pasifik (Hong Kong)	ap-northeast-2	Asia Pasifik (Seoul)
ap-southeast-4	Asia Pasifik (Melbourne)	ap-southeast-2	Asia Pasifik (Sydney)
ap-south-2	Asia Pasifik (Hyderabad)	ap-south-1	Asia Pasifik (Mumbai)
eu-central-2	Eropa (Zürich)	eu-central-1	Eropa (Frankfurt)
eu-south-2	Eropa (Spanyol)	eu-west-3	Eropa (Paris)
me-central-1	Timur Tengah (UEA)	eu-central-1	Eropa (Frankfurt)

Dalam panggilan Lintas wilayah ini, Pusat Identitas IAM mungkin mengirimkan atribut pengguna berikut:

- Alamat Email
- Nama depan
- Nama belakang
- Akun di AWS Organizations
- AWS URL portal akses
- nama pengguna
- ID Direktori
- ID Pengguna

Mengelola Pusat Identitas IAM di Wilayah keikutsertaan (Wilayah yang dinonaktifkan secara default)

Sebagian Wilayah AWS besar diaktifkan untuk operasi di semua AWS layanan secara default. Mereka Wilayah secara otomatis diaktifkan untuk digunakan dengan IAM Identity Center. Berikut ini Wilayah AWS adalah Wilayah keikutsertaan dan Anda harus mengaktifkannya:

- Afrika (Cape Town)
- Asia Pasifik (Hong Kong)
- Asia Pasifik (Jakarta)
- Asia Pasifik (Melbourne)
- Asia Pasifik (Hyderabad)
- Eropa (Milan)
- Eropa (Zürich)
- Eropa (Spanyol)
- Israel (Tel Aviv)
- Timur Tengah (Bahrain)
- Middle East (UAE)

Saat Anda mengaktifkan Pusat Identitas IAM untuk akun manajemen dalam keikutsertaan Wilayah AWS, metadata Pusat Identitas IAM berikut untuk setiap akun anggota disimpan di Wilayah.

- ID Akun
- Nama akun
- Email akun
- Nama Sumber Daya Amazon (ARN) dari peran IAM yang dibuat Pusat Identitas IAM di akun anggota

Jika Anda menonaktifkan Wilayah di mana Pusat Identitas IAM diinstal, Pusat Identitas IAM juga dinonaktifkan. Setelah Pusat Identitas IAM dinonaktifkan di Wilayah, pengguna di Wilayah tersebut tidak akan memiliki akses masuk tunggal ke Akun AWS dan aplikasi. AWS menyimpan data dalam konfigurasi Pusat Identitas IAM Anda setidaknya selama 10 hari. Jika Anda mengaktifkan kembali Pusat Identitas IAM dalam jangka waktu ini, data konfigurasi Pusat Identitas IAM Anda akan tetap tersedia di Wilayah.

Untuk mengaktifkan kembali Pusat Identitas IAM dalam keikutsertaan Wilayah AWS, Anda harus mengaktifkan kembali Wilayah. Karena IAM Identity Center harus memproses ulang semua peristiwa yang dijeda lagi, mengaktifkan kembali IAM Identity Center mungkin membutuhkan waktu.

> **Note**
>
> Pusat Identitas IAM hanya dapat mengelola akses ke Akun AWS yang diaktifkan untuk digunakan dalam file Wilayah AWS. Untuk mengelola akses di semua akun di organisasi Anda, aktifkan Pusat Identitas IAM di akun manajemen Wilayah AWS yang diaktifkan secara otomatis untuk digunakan dengan Pusat Identitas IAM.

Untuk informasi selengkapnya tentang mengaktifkan dan menonaktifkan Wilayah AWS, lihat Mengelola Wilayah AWS di Referensi Umum.AWS

Hapus konfigurasi Pusat Identitas IAM

Ketika konfigurasi Pusat Identitas IAM dihapus, semua data dalam konfigurasi itu dihapus dan tidak dapat dipulihkan. Tabel berikut menjelaskan data apa yang dihapus berdasarkan jenis direktori yang saat ini dikonfigurasi di IAM Identity Center.

Data apa yang akan dihapus	Direktori yang terhubung (AWS Managed Microsoft AD atau AD Connector)	Toko identitas Pusat Identitas IAM
Semua set izin yang telah Anda konfigurasikan Akun AWS	✓	✓
Semua aplikasi yang telah Anda konfigurasikan di IAM Identity Center	✓	✓
Semua tugas pengguna yang telah Anda konfigurasikan untuk Akun AWS dan aplikasi	✓	✓

Data apa yang akan dihapus	Direktori yang terhubung (AWS Managed Microsoft AD atau AD Connector)	Toko identitas Pusat Identitas IAM
Semua pengguna dan grup di direktori atau toko	N/A	✓

Gunakan prosedur berikut ketika Anda perlu menghapus konfigurasi Pusat Identitas IAM Anda saat ini.

Untuk menghapus konfigurasi Pusat Identitas IAM

1. Buka konsol Pusat Identitas IAM.
2. Pada panel navigasi kiri, pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Manajemen.
4. Di bagian konfigurasi Delete IAM Identity Center, pilih Delete.
5. Dalam dialog konfigurasi Delete IAM Identity Center, pilih setiap kotak centang untuk mengetahui bahwa Anda memahami bahwa data Anda akan dihapus. Ketik instans Pusat Identitas IAM Anda di kotak teks, lalu pilih Konfirmasi.

AWS IAM Identity Center kuota

Tabel berikut menjelaskan kuota dalam IAM Identity Center. Permintaan peningkatan kuota harus berasal dari manajemen atau akun administrator yang didelegasikan. Untuk menambah kuota, lihat Meminta kenaikan kuota.

> **Note**
>
> Sebaiknya gunakan AWS CLI dan API jika Anda memiliki lebih dari 50.000 pengguna, 10.000 grup, atau 500 set izin. Untuk informasi lebih lanjut tentang CLI, lihat. IntegrasiAWSCLI dengan IAM Identity Center Untuk informasi selengkapnya tentang API, lihat Selamat datang di Referensi API Pusat Identitas IAM.

Kuota aplikasi

Sumber daya	Kuota bawaan	Dapat ditingkatkan
Ukuran file sertifikat SAML penyedia layanan (dalam format PEM)	2 KB	Tidak
Batas pernyataan SAMP	50.000 karakter	Tidak
Batas ukuran file sertifikat iDP yang diunggah ke IAM Identity Center	2500 (UTF-8) karakter	Tidak
Akses cakupan per aplikasi	25	Tidak

Akun AWS kuota

Sumber daya	Kuota bawaan	Dapat ditingkatkan
Jumlah set izin yang diizinkan di Pusat Identitas IAM	2000	Ya

Sumber daya	Kuota bawaan	Dapat ditingkatkan
Jumlah set izin yang disediakan yang diizinkan per Akun AWS	250	Ya
Jumlah kebijakan inline per set izin	1	Tidak
Jumlah kebijakan AWS terkelola dan terkelola pelanggan per set izin	20 [1]	Tidak
Ukuran maksimum kebijakan inline per set izin	32.768 byte. Ukuran maksimum karakter non-spasi dalam kebijakan sebaris per set izin adalah 10.240 byte.	Tidak
Jumlah peran IAM (set izin) dalam Akun AWS yang dapat diperbarui sekaligus	1	Tidak

[1]AWS Identity and Access Management (IAM) menetapkan kuota 10 kebijakan terkelola per peran. Untuk memanfaatkan kuota ini, minta peningkatan kuota IAM Kebijakan terkelola yang dilampirkan ke peran IAM di konsol Service Quotas untuk setiap Akun AWS tempat Anda ingin menerapkan set izin.

> **Note**
>
> Set izindisediakan Akun AWS sebagai peran IAM, atau menggunakan peran IAM yang ada di Akun AWS, dan oleh karena itu mengikuti kuota IAM. Untuk informasi selengkapnya tentang kuota yang terkait dengan peran IAM, lihat kuota IAM dan STS.

Kuota Direktori Aktif

Sumber daya	Kuota bawaan	Dapat ditingkatkan
Jumlah direktori terhubung yang dapat Anda miliki sekaligus	1	Tidak

Kuota toko identitas IAM Identity Center

Sumber daya	Kuota bawaan	Dapat ditingkatkan
Jumlah pengguna yang didukung di IAM Identity Center	100000	Ya
Jumlah grup yang didukung di Pusat Identitas IAM	100000	Tidak
Jumlah grup unik yang dapat digunakan untuk mengevalu asi izin pengguna	1000	Tidak

Batas throttle IAM Identity Center

Sumber daya	Kuota bawaan
API Pusat Identitas IAM	IAM Identity Center API memiliki throttle kolektif maksimum 20 transaksi per detik (TPS). Ini CreateAccountAssignmentmemiliki tingkat maksimum 10 panggilan asinkron yang luar biasa. Kuota-kuota ini tidak dapat diubah.

Kuota tambahan

Sumber daya	Kuota bawaan	Dapat ditingkatkan
Jumlah total Akun AWS atau aplikasi yang dapat dikonfigurasi*	3000	Ya
Jumlah total instans Pusat Identitas IAM per akun	1	Tidak
Jumlah total emiten token tepercaya	10	Tidak

* Hingga 3000 Akun AWS atau aplikasi (total gabungan) didukung. Misalnya, Anda dapat mengonfigurasi 2750 akun dan 250 aplikasi, menghasilkan total 3000 akun dan aplikasi.

Memecahkan masalah Pusat Identitas IAM

Berikut ini dapat membantu Anda memecahkan masalah umum yang mungkin Anda temui saat menyiapkan atau menggunakan konsol Pusat Identitas IAM.

Masalah saat membuat instance akun IAM Identity Center

Beberapa batasan mungkin berlaku saat membuat instance akun IAM Identity Center. Jika Anda tidak dapat membuat instance akun melalui konsol Pusat Identitas IAM, atau pengalaman penyiapan aplikasi AWS terkelola yang didukung, verifikasi kasus penggunaan berikut:

- Periksa yang lain Wilayah AWS Akun AWS di mana Anda mencoba membuat instance akun. Anda terbatas pada satu contoh IAM Identity Center perAkun AWS. Untuk mengaktifkan aplikasi, baik beralih ke Wilayah AWS dengan instance dari IAM Identity Center atau beralih ke akun tanpa instance dari IAM Identity Center.
- Jika organisasi Anda mengaktifkan Pusat Identitas IAM sebelum 14 September 2023, administrator Anda mungkin perlu ikut serta dalam pembuatan instans akun. Bekerja dengan administrator Anda untuk mengaktifkan pembuatan instans akun dari konsol Pusat Identitas IAM di akun manajemen.
- Administrator Anda mungkin telah membuat Kebijakan Kontrol Layanan untuk membatasi pembuatan instance akun Pusat Identitas IAM. Bekerja dengan administrator Anda menambahkan akun Anda ke daftar izinkan.

Anda menerima kesalahan saat mencoba melihat daftar aplikasi cloud yang telah dikonfigurasi sebelumnya untuk bekerja dengan IAM Identity Center

Kesalahan berikut ini terjadi ketika Anda memiliki kebijakan yang mengizinkan `sso:ListApplications` tetapi tidak API Pusat Identitas IAM lainnya. Perbarui kebijakan Anda untuk mengatasi kesalahan ini.

`ListApplications`Izin tersebut mengotorisasi beberapa API:

- `ListApplications`API.
- API internal yang mirip dengan `ListApplicationProviders` API yang digunakan di konsol IAM Identity Center.

Untuk membantu menyelesaikan duplikasi, API internal sekarang juga mengotorisasi penggunaan tindakan. `ListApplicationProviders` Untuk mengizinkan `ListApplications` API publik tetapi menolak API internal, kebijakan Anda harus menyertakan pernyataan yang menolak `ListApplicationProviders` tindakan:

```
      "Statement": [
    {
         "Effect": "Deny",
         "Action": "ListApplicationProviders",
         "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": "ListApplications",
        "Resource": "<instanceArn>" // (or "*" for all instances)
    }
]
```

Untuk mengizinkan API internal tetapi menolak`ListApplications`, kebijakan hanya perlu mengizinkan`ListApplicationProviders`. `ListApplications`API ditolak jika tidak diizinkan secara eksplisit.

```
      "Statement": [
    {
         "Effect": "Allow",
         "Action": "ListApplicationProviders",
         "Resource": "*"
    }
]
```

Saat kebijakan Anda diperbarui, hubungi AWS Support agar tindakan proaktif ini dihapus.

Masalah mengenai isi pernyataan SAMP yang dibuat oleh IAM Identity Center

IAM Identity Center menyediakan pengalaman debug berbasis web untuk pernyataan SAMP yang dibuat dan dikirim oleh IAM Identity Center, termasuk atribut dalam pernyataan ini, saat mengakses dan aplikasi SAMP dari portal akses. Akun AWS AWS Untuk melihat detail pernyataan SAMP yang dihasilkan oleh IAM Identity Center, gunakan langkah-langkah berikut.

1. Masuk ke portal AWS akses.
2. Saat Anda masuk ke portal, tahan tombol Shift ke bawah, pilih ubin aplikasi, lalu lepaskan tombol Shift.
3. Periksa informasi pada halaman berjudul Anda sekarang dalam mode administrator. Untuk menyimpan informasi ini untuk referensi future, pilih Copy XHTML, dan paste konten di tempat lain.
4. Pilih Kirim untuk <application>melanjutkan. Opsi ini mengirimkan pernyataan ke penyedia layanan.

> **Note**
>
> Beberapa konfigurasi browser dan sistem operasi mungkin tidak mendukung prosedur ini. Prosedur ini telah diuji pada Windows 10 menggunakan browser Firefox, Chrome, dan Edge.

Pengguna tertentu gagal melakukan sinkronisasi ke Pusat Identitas IAM dari penyedia SCIM eksternal

Jika sinkronisasi SCIM berhasil untuk subset pengguna yang dikonfigurasi di iDP Anda untuk penyediaan ke Pusat Identitas IAM tetapi gagal untuk orang lain, Anda mungkin melihat kesalahan yang mirip dengan dari penyedia identitas Anda. `'Request is unparsable, syntactically incorrect, or violates schema'` Anda juga dapat melihat pesan kegagalan penyediaan terperinci di. AWS CloudTrail

Masalah ini sering menunjukkan bahwa pengguna di IDP Anda dikonfigurasi sedemikian rupa sehingga IAM Identity Center tidak mendukung. Rincian lengkap implementasi IAM Identity Center SCIM, termasuk spesifikasi parameter dan operasi yang diperlukan, opsional, dan terlarang untuk

objek pengguna, dapat ditemukan di Panduan Pengembang Implementasi SCIM Pusat Identitas IAM. Panduan Pengembang SCIM harus dianggap otoritatif untuk informasi seputar persyaratan SCIM. Namun, berikut ini adalah beberapa alasan umum untuk kesalahan ini:

1. Objek pengguna di iDP tidak memiliki nama pertama (diberikan), nama terakhir (keluarga), dan/atau nama tampilan.

   - Solusi: Tambahkan nama pertama (diberikan), terakhir (keluarga), dan tampilan untuk objek pengguna. Selain itu, pastikan bahwa pemetaan penyediaan SCIM untuk objek pengguna di idP Anda dikonfigurasi untuk mengirim nilai nonempty untuk semua atribut ini.

2. Lebih dari satu nilai untuk satu atribut sedang dikirim untuk pengguna (juga dikenal sebagai “atribut multi-nilai”). Misalnya, pengguna mungkin memiliki nomor telepon kantor dan rumah yang ditentukan dalam iDP, atau beberapa email atau alamat fisik, dan idP Anda dikonfigurasi untuk mencoba menyinkronkan beberapa atau semua nilai untuk atribut tersebut.

   - Opsi solusi:

     i. Perbarui pemetaan penyediaan SCIM Anda untuk objek pengguna di idP Anda untuk mengirim hanya satu nilai untuk atribut yang diberikan. Misalnya, konfigurasikan pemetaan yang hanya mengirimkan nomor telepon kerja untuk setiap pengguna.

     ii. Jika atribut tambahan dapat dihapus dengan aman dari objek pengguna di IDP, Anda dapat menghapus nilai tambahan, meninggalkan salah satu atau nol nilai ditetapkan untuk atribut tersebut untuk pengguna.

     iii. Jika atribut tidak diperlukan untuk tindakan apa punAWS, hapus pemetaan untuk atribut tersebut dari pemetaan penyediaan SCIM untuk objek pengguna di idP Anda.

3. IDP Anda mencoba mencocokkan pengguna di target (Pusat Identitas IAM, dalam hal ini) berdasarkan beberapa atribut. Karena nama pengguna dijamin unik dalam instance Pusat Identitas IAM tertentu, Anda hanya perlu menentukan `username` sebagai atribut yang digunakan untuk pencocokan.

   - Solusi: Pastikan konfigurasi SCIM Anda di IDP Anda hanya menggunakan satu atribut untuk pencocokan dengan pengguna di IAM Identity Center. Misalnya, pemetaan `username` atau `userPrincipalName` di IDP ke atribut di SCIM untuk `userName` penyediaan ke IAM Identity Center akan benar dan cukup untuk sebagian besar implementasi.

Pengguna tidak dapat masuk ketika nama pengguna mereka dalam format UPN

Pengguna mungkin tidak dapat masuk ke portal AWS akses berdasarkan format yang mereka gunakan untuk memasukkan nama pengguna mereka di halaman masuk. Untuk sebagian besar, pengguna dapat masuk ke portal pengguna menggunakan nama pengguna biasa mereka, nama logon tingkat bawah (DOMAIN\UserName) atau nama logon UPN mereka (). `UserName@Corp.Example.com` Pengecualian untuk ini adalah ketika IAM Identity Center menggunakan direktori terhubung yang telah diaktifkan dengan MFA dan mode verifikasi telah diatur ke Context-aware atau Always-on. Dalam skenario ini, pengguna harus masuk dengan nama logon tingkat bawah (DOMAIN\). UserName Untuk informasi selengkapnya, lihat Otentikasi multi-faktor untuk pengguna Pusat Identitas. Untuk informasi umum tentang format nama pengguna yang digunakan untuk masuk ke Active Directory, lihat Format Nama Pengguna di situs web dokumentasi Microsoft.

Saya mendapatkan kesalahan 'Tidak dapat melakukan operasi pada peran yang dilindungi' saat memodifikasi peran IAM

Saat meninjau Peran IAM di akun, Anda mungkin melihat nama peran yang diawali dengan '_'AWSReservedSSO. Ini adalah peran yang dibuat oleh layanan Pusat Identitas IAM di akun, dan mereka berasal dari menetapkan izin yang ditetapkan ke akun. Mencoba memodifikasi peran ini dari dalam konsol IAM akan menghasilkan kesalahan berikut:

```
'Cannot perform the operation on the protected role 'AWSReservedSSO_RoleName_Here' -
 this role is only modifiable by AWS'
```

Peran ini hanya dapat dimodifikasi dari konsol Administrator Pusat Identitas IAM, yang ada di akun manajemen. AWS Organizations Setelah dimodifikasi, Anda kemudian dapat menekan perubahan ke AWS akun yang ditetapkan.

Pengguna direktori tidak dapat mengatur ulang kata sandi mereka

Ketika pengguna direktori mengatur ulang kata sandi mereka menggunakan Lupa Kata Sandi? opsi saat masuk portal AWS akses, kata sandi baru mereka harus mematuhi kebijakan kata sandi default seperti yang dijelaskan dalamPersyaratan kata sandi saat mengelola identitas di IAM Identity Center.

Jika pengguna memasukkan kata sandi yang mematuhi kebijakan dan kemudian menerima kesalahan`We couldn't update your password`, periksa untuk melihat apakah AWS CloudTrail tercatat kegagalan tersebut. Ini dapat dilakukan dengan mencari di konsol Riwayat Acara CloudTrail menggunakan filter berikut:

```
"UpdatePassword"
```

Jika pesan menyatakan hal berikut, maka Anda mungkin perlu menghubungi dukungan:

```
"errorCode": "InternalFailure",
      "errorMessage": "An unknown error occurred“
```

Kemungkinan penyebab lain dari masalah ini adalah dalam konvensi penamaan yang diterapkan pada nilai nama pengguna. Konvensi penamaan harus mengikuti pola tertentu seperti 'Surname.givenName'. Namun, beberapa nama pengguna bisa sangat panjang, atau mengandung karakter khusus, dan ini dapat menyebabkan karakter dijatuhkan dalam panggilan API, sehingga mengakibatkan kesalahan. Anda mungkin ingin mencoba pengaturan ulang kata sandi dengan pengguna uji dengan cara yang sama untuk memverifikasi apakah ini masalahnya.

Jika masalah berlanjut, hubungi Pusat AWS Dukungan.

Pengguna saya direferensikan dalam set izin tetapi tidak dapat mengakses akun atau aplikasi yang ditetapkan

Masalah ini dapat terjadi jika Anda menggunakan System for Cross-domain Identity Management (SCIM) untuk Penyediaan Otomatis dengan penyedia identitas eksternal. Secara khusus, ketika pengguna, atau grup yang menjadi anggotanya, dihapus kemudian dibuat ulang menggunakan nama pengguna yang sama (untuk pengguna) atau nama (untuk grup) di penyedia identitas, pengidentifikasi internal unik baru dibuat untuk pengguna atau grup baru di Pusat Identitas IAM. Namun, IAM Identity Center masih memiliki referensi ke identifier lama dalam database izinnya, sehingga nama pengguna atau grup masih muncul di UI, tetapi akses gagal. Ini karena ID pengguna atau grup yang mendasari yang dirujuk UI tidak ada lagi.

Untuk memulihkan Akun AWS akses dalam kasus ini, Anda dapat menghapus akses untuk pengguna atau grup lama dari Akun AWS (s) tempat awalnya ditetapkan, dan kemudian menetapkan kembali akses ke pengguna atau grup. Ini memperbarui set izin dengan pengenal yang benar untuk pengguna atau grup baru. Demikian pula, untuk memulihkan akses aplikasi, Anda dapat menghapus

akses untuk pengguna atau grup dari daftar pengguna yang ditetapkan untuk aplikasi itu, lalu menambahkan pengguna atau grup kembali lagi.

Anda juga dapat memeriksa untuk melihat apakah AWS CloudTrail tercatat kegagalan dengan mencari CloudTrail log Anda untuk peristiwa sinkronisasi SCIM yang mereferensikan nama pengguna atau grup yang dimaksud.

Saya tidak bisa mendapatkan aplikasi saya dari katalog aplikasi yang dikonfigurasi dengan benar

Jika Anda menambahkan aplikasi dari katalog aplikasi di IAM Identity Center, ketahuilah bahwa setiap penyedia layanan menyediakan dokumentasi terperinci mereka sendiri. Anda dapat mengakses informasi ini dari tab Konfigurasi untuk aplikasi di konsol Pusat Identitas IAM.

Jika masalah terkait dengan pengaturan kepercayaan antara aplikasi penyedia layanan dan IAM Identity Center, pastikan untuk memeriksa instruksi manual untuk langkah-langkah pemecahan masalah.

Kesalahan 'Kesalahan tak terduga telah terjadi' ketika pengguna mencoba masuk menggunakan penyedia identitas eksternal

Kesalahan ini dapat terjadi karena beberapa alasan, tetapi salah satu alasan umum adalah ketidakcocokan antara informasi pengguna yang dibawa dalam permintaan SAMP, dan informasi untuk pengguna di Pusat Identitas IAM.

Agar pengguna IAM Identity Center berhasil masuk saat menggunakan iDP eksternal sebagai sumber identitas, berikut ini harus benar:

- Format NameID SAMP (dikonfigurasi di penyedia identitas Anda) harus 'email'
- Nilai nameId harus berupa string yang diformat dengan benar (RFC2822) (user@domain.com)
- Nilai NameID harus sama persis dengan nama pengguna pengguna yang ada di Pusat Identitas IAM (tidak masalah apakah alamat email di Pusat Identitas IAM cocok atau tidak - kecocokan masuk didasarkan pada nama pengguna)
- Implementasi IAM Identity Center dari federasi SAMP 2.0 hanya mendukung 1 pernyataan dalam tanggapan SAMP antara penyedia identitas dan IAM Identity Center. Itu tidak mendukung pernyataan SAMP terenkripsi.

- Pernyataan berikut berlaku jika Atribut untuk kontrol akses diaktifkan di akun Pusat Identitas IAM Anda:
  - Jumlah atribut yang dipetakan dalam permintaan SAMP harus 50 atau kurang.
  - Permintaan SAMP tidak boleh berisi atribut multi-nilai.
  - Permintaan SAMP tidak boleh berisi beberapa atribut dengan nama yang sama.
  - Atribut tidak boleh berisi XHTML terstruktur sebagai nilainya.
  - Format Nama harus berupa format yang ditentukan SAMP, bukan format generik.

> **Note**
>
> IAM Identity Center tidak melakukan pembuatan “tepat waktu” pengguna atau grup untuk pengguna atau grup baru melalui federasi SAMP. Ini berarti bahwa pengguna harus dibuat sebelumnya di Pusat Identitas IAM, baik secara manual atau melalui penyediaan otomatis, untuk masuk ke Pusat Identitas IAM.

Kesalahan ini juga dapat terjadi ketika titik akhir Assertion Consumer Service (ACS) yang dikonfigurasi di penyedia identitas Anda tidak cocok dengan URL ACS yang disediakan oleh instans IAM Identity Center Anda. Pastikan kedua nilai ini sama persis.

Selain itu, Anda dapat memecahkan masalah kegagalan masuk penyedia identitas eksternal lebih lanjut dengan membuka AWS CloudTrail dan memfilter nama acara P. ExternalId DirectoryLogin

Kesalahan 'Atribut untuk kontrol akses gagal diaktifkan'

Kesalahan ini dapat terjadi jika pengguna yang mengaktifkan ABAC tidak memiliki `iam:UpdateAssumeRolePolicy` izin yang diperlukan untuk mengaktifkan. Atribut untuk kontrol akses

Saya mendapatkan pesan 'Browser tidak didukung' ketika saya mencoba mendaftarkan perangkat untuk MFA

WebAuthn Saat ini didukung di browser web Google Chrome, Mozilla Firefox, Microsoft Edge dan Apple Safari, serta platform Windows 10 dan Android. Beberapa komponen WebAuthn dukungan dapat bervariasi, seperti dukungan autentikator platform di browser macOS dan iOS. Jika pengguna

mencoba mendaftarkan WebAuthn perangkat pada browser atau platform yang tidak didukung, mereka akan melihat opsi tertentu berwarna abu-abu yang tidak didukung, atau mereka akan menerima kesalahan bahwa semua metode yang didukung tidak didukung. Dalam kasus ini, silakan merujuk ke FIDO2: Web Authentication (WebAuthn) untuk informasi lebih lanjut tentang dukungan browser/platform. Untuk informasi lebih lanjut tentang Pusat WebAuthn Identitas IAM, lihatOtentikator FIDO2.

Grup Active Directory “Pengguna Domain” tidak disinkronkan dengan benar ke Pusat Identitas IAM

Grup Pengguna Domain Direktori Aktif adalah “grup utama” default untuk objek pengguna AD. Grup utama Active Directory dan keanggotaannya tidak dapat dibaca oleh IAM Identity Center. Saat menetapkan akses ke sumber daya atau aplikasi Pusat Identitas IAM, gunakan grup selain grup Pengguna Domain (atau grup lain yang ditetapkan sebagai grup utama) agar keanggotaan grup tercermin dengan benar di penyimpanan identitas Pusat Identitas IAM.

Kesalahan kredensial MFA tidak valid

Kesalahan ini dapat terjadi ketika pengguna mencoba masuk ke Pusat Identitas IAM menggunakan akun dari penyedia identitas eksternal (misalnya, Okta atauMicrosoft Entra ID) sebelum akun mereka sepenuhnya disediakan ke Pusat Identitas IAM menggunakan protokol SCIM. Setelah akun pengguna disediakan ke Pusat Identitas IAM, masalah ini harus diselesaikan. Konfirmasikan bahwa akun telah disediakan ke Pusat Identitas IAM. Jika tidak, periksa log penyediaan di penyedia identitas eksternal.

Saya mendapatkan pesan 'Kesalahan tak terduga telah terjadi' ketika saya mencoba mendaftar atau masuk menggunakan aplikasi autentikator

Sistem kata sandi satu kali berbasis waktu (TOTP), seperti yang digunakan oleh IAM Identity Center dalam kombinasi dengan aplikasi autentikator berbasis kode, bergantung pada sinkronisasi waktu antara klien dan server. Pastikan perangkat tempat aplikasi autentikator diinstal disinkronkan dengan benar ke sumber waktu yang andal, atau setel waktu di perangkat secara manual agar sesuai dengan sumber terpercaya, seperti NIST (https://www.time.gov/) atau setara lokal/regional lainnya.

Pengguna saya tidak menerima email dari IAM Identity Center

Semua email yang dikirim oleh layanan IAM Identity Center akan berasal dari alamat `no-reply@signin.aws` atau`no-reply@login.awsapps.com`. Sistem surat Anda harus dikonfigurasi sehingga menerima email dari alamat email pengirim ini dan tidak menanganinya sebagai sampah atau spam.

Kesalahan: Anda tidak dapat menghapus/memodifikasi/menghapus/menetapkan akses ke set izin yang disediakan di akun manajemen

Pesan ini menunjukkan bahwa Administrator yang didelegasikan fitur telah diaktifkan dan bahwa operasi yang Anda coba sebelumnya hanya dapat berhasil dilakukan oleh seseorang yang memiliki hak istimewa akun manajemen. AWS Organizations Untuk mengatasi masalah ini, masuk sebagai pengguna yang memiliki hak istimewa ini dan coba lakukan tugas lagi atau tetapkan tugas ini kepada seseorang yang memiliki izin yang benar. Untuk informasi selengkapnya, lihat Daftarkan akun anggota.

Riwayat dokumen

Tabel berikut menjelaskan penambahan penting pada AWS IAM Identity Center dokumentasi. Kami juga rutin memperbarui dokumentasi untuk menjawab umpan balik yang Anda kirimkan kepada kami.

- Pembaruan dokumentasi utama terbaru: 23 September 2022

Perubahan	Deskripsi	Tanggal
Pembaruan untuk kebijakan AWS terkelola	Izin yang diperbarui untuk kebijakan `AWSIAMIdentityCenterAllowListForIdentityContext` AWS terkelola.	26 November 2023
Topik kebijakan AWS terkelola baru	Menambahkan detail untuk kebijakan `AWSIAMIdentityCenterAllowListForIdentityContext` AWS terkelola.	15 November 2023
Panduan yang disempurnakan untuk memulai dengan IAM Identity Center	Menambahkan konten baru untuk memulai dengan IAM Identity Center dan membuat pengguna administratif	September 23, 2022
Pengguna dan grup yang diperbarui di Referensi API Pusat Identitas	Pembaruan ini mencakup referensi ke API Buat, Perbarui, dan Hapus baru di Panduan Referensi API Pusat Identitas.	31 Agustus 2022
AWSSingle Sign-On (AWSSSO) berganti nama menjadi IAM Identity Center AWS	AWSmemperkenalkan. AWS IAM Identity Center IAM Identity Center memperluas kemampuan AWS Identity and Access Managemen	Juli 26, 2022

	t (IAM) untuk membantu Anda mengelola akun secara terpusat dan akses ke aplikasi untuk pengguna tenaga kerja Anda. Fitur IAM Identity Center meliputi penugasan aplikasi, izin multi-akun, dan portal akses. AWS	
Dukungan untuk batas izin dan kebijakan yang dikelola pelanggan dalam set izin	Menambahkan konten untuk menggunakan kebijakan terkelola dan AWS dikelola pelanggan AWS Identity and Access Management (IAM) dengan set izin.	14 Juli 2022
Support untuk AWS Wilayah yang diaktifkan secara manual	Menambahkan konten untuk menggunakan Pusat Identitas IAM di Wilayah yang diaktifkan secara manual.	Juni 15, 2022
Pembaruan untuk kebijakan AWS terkelola	Izin yang diperbarui untuk kebijakan `AWSSSOServiceRolePolicy` AWS terkelola.	Mei 11, 2022
Support untuk administrasi yang didelegasikan	Menambahkan konten untuk fitur administrasi yang didelegasikan.	Mei 11, 2022
Pembaruan untuk kebijakan AWS terkelola	Izin yang diperbaru i untuk`AWSSSOMasterAccountAdministrator` ,`AWSSSOMemberAccountAdministrator` , dan kebijakan `AWSSSOReadOnly` AWS terkelola.	28 April 2022

Dukungan untuk sinkronisasi AD yang dapat dikonfigurasi	Menambahkan konten untuk fitur sinkronisasi AD yang dapat dikonfigurasi.	April 14, 2022
Topik kebijakan AWS terkelola baru	Menambahkan detail untuk kebijakan `AWSSSOMasterAccountAdministrator` AWS terkelola.	4 Agustus 2021
Pembaruan untuk kuota	Penyesuaian tabel kuota.	21 Desember 2020
Contoh kebijakan baru	Menambahkan contoh kebijakan terkelola pelanggan baru dan pembaruan ke bagian yang diperlukan izin.	21 Desember 2020
Support untuk kontrol akses berbasis atribut (ABAC)	Menambahkan konten untuk fitur ABAC.	24 November 2020
Support untuk pendaftaran paksa MFA	Pembaruan untuk mengharuskan pengguna mendaftarkan perangkat MFA saat masuk.	23 November 2020
Support untuk WebAuthn	Menambahkan konten untuk WebAuthn fitur baru.	20 November 2020
Support untuk Ping Identity	Menambahkan konten untuk diintegrasikan dengan Ping Identity produk sebagai penyedia identitas eksternal yang didukung.	26 Oktober 2020
Support untuk OneLogin	Menambahkan konten untuk diintegrasikan OneLogin sebagai penyedia identitas eksternal yang didukung.	31 Juli 2020

Support untuk Okta	Menambahkan konten untuk diintegrasikan Okta sebagai penyedia identitas eksternal yang didukung.	28 Mei 2020
Support untuk penyedia identitas eksternal	Referensi diubah dari direktori ke sumber identitas, menambahkan konten untuk mendukung penyedia identitas eksternal.	26 November 2019
Pengaturan MFA baru	Menghapus topik verifikasi dua langkah dan menambahk an topik MFA baru sebagai gantinya.	24 Oktober 2019
Pengaturan baru untuk menambahkan verifikasi dua langkah	Menambahkan konten tentang cara mengaktifkan verifikasi dua langkah untuk pengguna.	16 Januari 2019
Support untuk durasi sesi pada AWS akun	Menambahkan konten tentang cara mengatur durasi sesi untuk AWS akun.	30 Oktober 2018
Opsi baru untuk menggunakan direktori Pusat Identitas	Menambahkan konten untuk memilih direktori Pusat Identitas atau menghubun gkan ke direktori yang ada di Direktori Aktif.	17 Oktober 2018
Support untuk status relai dan durasi sesi pada aplikasi	Menambahkan konten tentang status relai dan durasi sesi untuk aplikasi.	10 Oktober 2018

Dukungan tambahan untuk aplikasi baru	Ditambahkan 4me, BambooHR, Bonusly, Citrix ShareFile, ClickTime, Convo, Deputy, Deskpro, Dome9, DruvaInSync, Egnyte, Engagedly, Expensify, Freshdesk, IdeaScale, Igloo, Jitbit, Kudos, LiquidFiles, Lucidchart, PurelyHR, Samanage, ScreenSteps, Sli.do, SmartSheet, Syncplicity, TalentLMS, Trello, UserVoice, Zoho, OpsGenie, DigiCert, WeekDone, ProdPad, dan UserEcho ke katalog aplikasi.	3 Agustus 2018
Support untuk akses multi-akun ke akun manajemen	Menambahkan konten tentang cara mendelegasikan akses multi-akun ke pengguna di akun manajemen.	9 Juli 2018
Support untuk aplikasi baru	Ditambahkan DocuSign, Keeper Security, dan SugarCRM ke katalog aplikasi.	Maret 16, 2018
Dapatkan kredensi sementara untuk akses CLI	Menambahkan informasi tentang cara mendapatkan kredensi sementara untuk menjalankan AWS CLI perintah.	22 Februari 2018
Panduan baru	Ini adalah rilis pertama dari Panduan Pengguna Pusat Identitas IAM.	7 Desember 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.