



Panduan Pengguna

AWS IAM Identity Center



AWS IAM Identity Center: Panduan Pengguna

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

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

Table of Contents

Apa itu IAM Identity Center?	1
Mengapa menggunakan IAM Identity Center?	1
Ganti nama Pusat Identitas IAM	3
Ruang nama lama tetap sama	3
Memulai	4
Prasyarat dan pertimbangan IAM Identity Center	6
Memilih Wilayah AWS	7
Menggunakan Pusat Identitas IAM hanya untuk aplikasi	14
Peran IAM dibuat oleh IAM Identity Center	14
Pusat Identitas IAM dan AWS Organizations	15
Instans Pusat Identitas IAM	16
Akun AWS jenis yang dapat mengaktifkan Pusat Identitas IAM	17
Instans organisasi dari Pusat Identitas IAM	18
Instans akun Pusat Identitas IAM	21
Menghapus instance Pusat Identitas IAM Anda	26
Aktifkan Pusat Identitas IAM	28
Untuk mengaktifkan instance Pusat Identitas IAM	29
Konfirmasikan sumber identitas Anda	32
Memperbarui firewall dan gateway	35
Pertimbangan untuk mendaftarkan domain dan titik akhir URL yang diizinkan	37
Tutorial sumber identitas	39
Active Directory	40
CyberArk	42
Prasyarat	43
Pertimbangan SCIM	43
Langkah 1: Aktifkan penyediaan di IAM Identity Center	44
Langkah 2: Konfigurasi penyediaan di CyberArk	45
(Opsional) Langkah 3: Konfigurasi atribut pengguna CyberArk untuk kontrol akses (ABAC) di Pusat Identitas IAM	46
(Opsional) Melewati atribut untuk kontrol akses	46
Google Workspace	47
Pertimbangan-pertimbangan	48
Langkah 1: Google Workspace: Konfigurasi aplikasi SAML	49

Langkah 2: Pusat Identitas IAM dan Google Workspace: Mengubah sumber dan pengaturan identitas Pusat Identitas IAM Google Workspace sebagai penyedia identitas SAML	50
Langkah 3: Google Workspace: Aktifkan aplikasi	51
Langkah 4: Pusat Identitas IAM: Siapkan penyediaan otomatis Pusat Identitas IAM	52
Langkah 5: Google Workspace: Konfigurasi penyediaan otomatis	53
Melewati atribut untuk kontrol akses - Opsional	54
Tetapkan akses ke Akun AWS	55
Langkah selanjutnya	57
Pemecahan masalah	58
JumpCloud	59
Prasyarat	60
Pertimbangan SCIM	60
Langkah 1: Aktifkan penyediaan di IAM Identity Center	61
Langkah 2: Konfigurasi penyediaan di JumpCloud	61
(Opsional) Langkah 3: Konfigurasi atribut pengguna JumpCloud untuk kontrol akses di Pusat Identitas IAM	62
(Opsional) Melewati atribut untuk kontrol akses	63
Microsoft Entra ID	64
Prasyarat	64
Pertimbangan-pertimbangan	65
Langkah 1: Siapkan penyewa Microsoft Anda	67
Langkah 2: Persiapkan AWS akun	69
Langkah 3: Konfigurasi dan uji koneksi SAML Anda	71
Langkah 4: Konfigurasi dan uji sinkronisasi SCIM Anda	75
Langkah 5: Konfigurasi ABAC - Opsional	79
Tetapkan akses ke Akun AWS	81
Microsoft Entra ID konfigurasi untuk akses ke Wilayah tambahan	83
Pemecahan masalah	83
Okta	86
Pertimbangan-pertimbangan	87
Langkah 1: Okta: Dapatkan metadata SAML dari Anda Okta akun	88
Langkah 2: Pusat Identitas IAM: Konfigurasi Okta sebagai sumber identitas untuk IAM Identity Center	89
Langkah 3: Pusat Identitas IAM dan Okta: Ketentuan Okta pengguna	90
Langkah 4: Okta: Sinkronisasi pengguna dari Okta dengan Pusat Identitas IAM	91
Melewati atribut untuk kontrol akses - Opsional	93

Tetapkan akses ke Akun AWS	94
Oktakonfigurasi untuk akses ke Wilayah tambahan	96
Langkah selanjutnya	96
Pemecahan masalah	97
OneLogin	99
Prasyarat	100
Langkah 1: Aktifkan penyediaan di IAM Identity Center	100
Langkah 2: Konfigurasi penyediaan di OneLogin	101
(Opsional) Langkah 3: Konfigurasi atribut pengguna OneLogin untuk kontrol akses di Pusat Identitas IAM	103
(Opsional) Melewati atribut untuk kontrol akses	103
Pemecahan masalah	104
Identitas Ping	105
PingFederate	105
PingOne	113
Direktori Identity Center	119
Tutorial video	125
Siapkan tenaga kerja Anda	126
Pengguna, grup, dan penyediaan	126
Nama pengguna dan keunikan alamat email	126
Grup	127
Penyediaan pengguna dan grup	127
Penghapusan penyediaan pengguna dan grup	127
Kelola sumber identitas Anda	127
Pertimbangan untuk mengubah sumber identitas Anda	128
Ubah sumber identitas Anda	134
Atribut pengguna dan grup di Pusat Identitas IAM	136
Penyedia identitas eksternal	137
Microsoft AD direktori	157
Mengelola pengguna di direktori Pusat Identitas	177
Penyediaan saat pengguna berada di Pusat Identitas IAM	178
Mengubah Sumber Identitas Anda	178
Tambahkan pengguna	178
Tambahkan grup	181
Tambahkan pengguna ke grup	183
Hapus grup	184

Hapus pengguna	185
Hapus pengguna dari grup	186
Edit properti pengguna	187
Akses tenaga kerja	189
Memahami sesi otentikasi	189
Jenis sesi otentikasi	190
Cara untuk sesi pengguna akhir	191
Apa yang terjadi pada akses pengguna saat Anda mengakhiri sesi	192
Logout tunggal	197
Praktik terbaik untuk manajemen sesi	197
Konfigurasi durasi sesi	197
Sesi interaktif pengguna	198
Sesi latar belakang pengguna	199
Sesi diperpanjang untuk Kiro	200
Akhiri sesi aktif untuk pengguna tenaga kerja	201
Pertimbangan untuk sumber identitas, AWS CLI, dan SDK AWS	203
Nonaktifkan akses pengguna	206
Tolak akses pengguna	207
Mengelola akses untuk pengguna di direktori Identity Center	209
Manajemen kata sandi	209
MFA	209
Menyiapkan kata sandi pengguna	210
Otentikasi multi-faktor	213
Akses aplikasi	227
AWS aplikasi yang dikelola	228
Mengontrol akses ke aplikasi	228
Berbagi informasi identitas	229
Membatasi penggunaan AWS aplikasi yang dikelola	230
Aplikasi yang dapat Anda gunakan dengan IAM Identity Center	231
Menyiapkan Pusat Identitas IAM untuk menguji aplikasi yang AWS dikelola	236
Melihat dan mengubah detail aplikasi	242
Menonaktifkan AWS aplikasi yang dikelola	243
Mengaktifkan sesi konsol yang ditingkatkan identitas	243
Aplikasi yang dikelola pelanggan	247
Aplikasi SAML 2.0 dan OAuth 2.0	248
Pengaturan aplikasi SAML 2.0	253

Aktifkan akses akun	256
Propagasi identitas tepercaya	260
Manfaat propagasi identitas tepercaya	260
Mengaktifkan propagasi identitas tepercaya	260
Cara kerja propagasi identitas tepercaya	261
Prasyarat dan pertimbangan	262
Kasus penggunaan	264
Layanan otorisasi	290
Menyiapkan aplikasi OAuth 2.0 Anda sendiri	300
Menyiapkan aplikasi yang dikelola pelanggan	301
Tentukan aplikasi tepercaya	305
Penerbit token tepercaya	306
Putar sertifikat	321
Pertimbangan sebelum memutar sertifikat	322
Memutar sertifikat Pusat Identitas IAM	322
Indikator status kedaluwarsa sertifikat	324
Memahami properti aplikasi	325
URL mulai aplikasi	325
Status relai	326
Durasi sesi	327
Tetapkan akses pengguna ke aplikasi	327
Hapus akses pengguna ke aplikasi	328
Atribut peta	329
Akun AWS akses	330
Akun AWS tipe	331
Menugaskan Akun AWS akses	334
End-user pengalaman	334
Menegakkan dan membatasi akses	335
Mendelegasikan dan menegakkan akses	335
Membatasi akses ke penyimpanan identitas dari akun anggota	336
Administrator yang didelegasikan	336
Praktik terbaik	337
Prasyarat	342
Daftarkan akun anggota	343
Menghapus pendaftaran akun anggota	344
Lihat akun administrator yang didelegasikan	345

Akses sementara yang ditinggikan	345
Akses masuk tunggal ke Akun AWS	346
Menetapkan akses pengguna atau grup ke Akun AWS	347
Menghapus akses pengguna dan grup ke Akun AWS	350
Cabut akses pengguna	351
Mendelegasikan siapa yang dapat menetapkan akses masuk tunggal	353
Kumpulan izin	354
Membuat kumpulan izin yang menerapkan izin hak istimewa terkecil	355
Izin yang telah ditentukan	357
Izin khusus	358
Membuat, mengelola, dan menghapus set izin	361
Konfigurasi properti kumpulan izin	374
Mereferensikan kumpulan izin	380
Rekomendasi untuk menghindari gangguan akses	383
Contoh kebijakan kepercayaan khusus	383
Attribute-based kontrol akses	385
Manfaat	385
Daftar Periksa: Mengkonfigurasi ABAC di AWS menggunakan Pusat Identitas IAM	386
Atribut untuk kontrol akses	389
Service-linked peran	397
AWS portal akses	399
Memulai dengan AWS portal akses	399
Konfigurasi AWS portal akses	400
Apa yang dapat Anda konfigurasi	400
Mengaktifkan portal AWS akses	400
Menyesuaikan AWS URL portal akses	401
Konfirmasikan pengguna dapat masuk ke AWS portal akses	402
Gunakan AWS portal akses	403
Cara menggunakan AWS portal akses	404
Masuk ke AWS portal akses	404
Mengatur ulang kata sandi pengguna Anda	407
AWS CLI dan akses AWS SDK	408
Membuat tautan pintasan	413
Mendaftarkan perangkat Anda untuk MFA	416
Mengakhiri sesi aktif Anda	418
Menggunakan Pusat Identitas IAM di beberapa Wilayah AWS	420

Manfaat dukungan Multi-wilayah	420
Prasyarat dan pertimbangan	420
Memilih Wilayah Tambahan	421
Mereplikasi Pusat Identitas IAM ke Wilayah tambahan	422
Langkah 1: Buat kunci replika	422
Langkah 2: Tambahkan Wilayah	423
Langkah 3 (hanya penyedia identitas eksternal): Perbarui pengaturan IdP eksternal	424
Langkah 4: Konfirmasikan daftar izin firewall dan gateway	425
Langkah 5: Berikan informasi kepada pengguna	425
Wilayah berubah setelah menambahkan Wilayah pertama	425
Data apa yang direplikasi?	425
Akses tenaga kerja melalui Wilayah tambahan	426
Sesi pengguna di beberapa Wilayah AWS	427
AWS akses titik akhir portal di primer dan tambahan Wilayah AWS	427
Titik akhir ACS di primer dan tambahan Wilayah AWS	429
Penggunaan AWS aplikasi yang dikelola tanpa beberapa URL ACS	431
Failover ke Wilayah tambahan untuk akses Akun AWS	431
Akun AWS akses ketahanan tanpa beberapa URL ACS	432
Menyebarkan dan mengelola aplikasi di berbagai aplikasi Wilayah AWS	433
Menyebarkan dan AWS mengelola aplikasi terkelola di berbagai aplikasi Wilayah AWS	433
Menyebarkan dan mengelola aplikasi yang dikelola pelanggan di beberapa Wilayah AWS ..	435
Menghapus Wilayah dari Pusat Identitas IAM	435
Langkah 1: Perbarui konfigurasi IdP eksternal (jika ada)	436
Langkah 2: Hapus Wilayah	436
Langkah 3: Hapus kunci replika	437
API layanan didukung dalam tambahan Wilayah AWS	437
CloudTrail peristiwa di Wilayah primer dan tambahan	438
Kasus penggunaan Pusat Identitas IAM di Wilayah primer dan tambahan	438
Desain ketahanan dan perilaku Regional	442
Dirancang untuk ketersediaan	443
Mengatur akses darurat ke Konsol Manajemen AWS	443
Ringkasan konfigurasi akses darurat	444
Bagaimana merancang peran operasi penting Anda	445
Cara merencanakan model akses Anda	446
Bagaimana merancang peran darurat, akun, dan pemetaan grup	447
Cara membuat konfigurasi akses darurat Anda	447

Tugas persiapan darurat	449
Proses failover darurat	449
Kembali ke operasi normal	450
One-time pengaturan aplikasi federasi IAM langsung di Okta	450
One-time pengaturan aplikasi federasi IAM langsung dengan ADFS	453
Keamanan	460
Manajemen identitas dan akses untuk Pusat Identitas IAM	461
Autentikasi	461
Kontrol akses	461
Gambaran umum manajemen akses	462
Identity-based contoh kebijakan	466
Resource-based contoh kebijakan	474
AWS kebijakan yang dikelola	477
Menggunakan peran tertaut layanan	498
Konsol Pusat Identitas IAM dan otorisasi API	506
Tindakan API setelah November 2023	506
Tindakan API setelah Oktober 2020	507
AWS STS kunci kondisi untuk Pusat Identitas IAM	509
UserId	510
IdentityStoreArn	511
ApplicationArn	511
CredentialId	512
InstanceArn	512
Pencatatan dan Pemantauan	512
Mencatat panggilan API Pusat Identitas IAM dengan AWS CloudTrail	513
Pencatatan Pusat Identitas IAM SCIM dengan AWS CloudTrail	553
Amazon EventBridge	560
Pencatatan kesalahan sinkronisasi AD yang dapat dikonfigurasi	560
Validasi kepatuhan	563
Standar kepatuhan yang didukung	564
Ketahanan	565
Keamanan infrastruktur	566
Perlindungan data	567
Enkripsi saat bergerak	567
Privasi data	568
Retensi data	568

Enkripsi saat diam	568
Konteks enkripsi Pusat Identitas IAM	570
Menggunakan konteks enkripsi untuk mengontrol akses ke kunci yang dikelola pelanggan Anda	570
Memantau kunci enkripsi Anda untuk Pusat Identitas IAM	571
AWS penyimpanan aplikasi terkelola, enkripsi, dan penghapusan atribut identitas Pusat Identitas IAM	571
Menerapkan kunci KMS yang dikelola pelanggan	572
Kebijakan kunci KMS dasar	582
Pernyataan kebijakan utama KMS lanjutan	587
Memberikan tag ke sumber daya	596
Batasan tag	597
Kelola tag dengan konsol	597
AWS CLI contoh	598
Menetapkan tanda	598
Melihat tanda	599
Menghapus tanda	599
Menerapkan tag saat Anda membuat set izin	599
Tindakan API	600
Mengintegrasikan AWS CLI dengan IAM Identity Center	601
Bagaimana mengintegrasikan AWS CLI dengan IAM Identity Center	601
Pertimbangan untuk Akses Pribadi	602
Kuota	603
Kuota aplikasi	603
Akun AWS kuota	604
Kuota Direktori Aktif	605
Kuota penyimpanan identitas Pusat Identitas IAM	605
Batas throttle Pusat Identitas IAM	605
Kuota permintaan layanan OIDC	606
Kuota tambahan	608
Pemecahan masalah	610
Masalah saat membuat instance akun Pusat Identitas IAM	610
Anda menerima kesalahan saat mencoba melihat daftar aplikasi cloud yang telah dikonfigurasi sebelumnya untuk bekerja dengan Pusat Identitas IAM	610
Masalah mengenai isi pernyataan SAML yang dibuat oleh Pusat Identitas IAM	612

Pengguna tertentu gagal melakukan sinkronisasi ke Pusat Identitas IAM dari penyedia SCIM eksternal	612
Duplikat kesalahan pengguna atau grup saat menyediakan pengguna atau grup dengan penyedia identitas eksternal	614
Pengguna tidak dapat masuk jika nama pengguna mereka dalam format UPN	615
Saya mendapatkan kesalahan 'Tidak dapat melakukan operasi pada peran yang dilindungi 'saat memodifikasi peran IAM	615
Pengguna direktori tidak dapat mengatur ulang kata sandi mereka	616
Pengguna saya direferensikan dalam kumpulan izin tetapi tidak dapat mengakses akun atau aplikasi yang ditetapkan	616
Saya tidak dapat mengonfigurasi aplikasi saya dari katalog aplikasi dengan benar	617
Kesalahan 'Kesalahan tak terduga telah terjadi' ketika pengguna mencoba masuk menggunakan penyedia identitas eksternal	617
Kesalahan 'Atribut untuk kontrol akses gagal diaktifkan'	619
Saya mendapatkan pesan 'Browser tidak didukung' ketika saya mencoba mendaftarkan perangkat untuk MFA	619
Grup "Pengguna Domain" Direktori Aktif tidak disinkronkan dengan benar ke Pusat Identitas IAM	619
Kesalahan kredensial MFA tidak valid	619
Saya mendapatkan pesan 'Terjadi kesalahan tak terduga' ketika saya mencoba mendaftar atau masuk menggunakan aplikasi otentikator	620
Saya mendapatkan kesalahan 'Ini bukan Anda, ini kami' saat mencoba masuk ke Pusat Identitas IAM	620
Pengguna saya tidak menerima email dari Pusat Identitas IAM	621
Kesalahan: Anda tidak dapat delete/modify/remove/assign mengakses kumpulan izin yang disediakan di akun manajemen	621
Kesalahan: Token sesi tidak ditemukan atau tidak valid	621
Anggota grup dari domain tepercaya tidak disinkronkan ke Pusat Identitas IAM	621
Memecahkan masalah kunci yang dikelola pelanggan di AWS IAM Identity Center	622
Akses Ditolak: Masalah Izin Mendekripsi KMS	622
AWS kegagalan login aplikasi terkelola dengan kunci yang dikelola pelanggan diaktifkan di Pusat Identitas IAM	622
AWS kegagalan penugasan and/or pengguna instalasi aplikasi terkelola dengan kunci yang dikelola pelanggan diaktifkan di Pusat Identitas IAM	623
Masalah Izin KMS: Mengkonfigurasi Kunci yang Dikelola Pelanggan dengan AWS IAM Identity Center	623

AWS kegagalan login portal akses dengan kunci yang dikelola pelanggan di Pusat Identitas IAM	624
Memecahkan masalah pengaturan Multi-wilayah di AWS IAM Identity Center	624
Wilayah tempat saya ingin mereplikasi instance Pusat Identitas IAM saya tidak tersedia di konsol Pusat Identitas IAM	624
AWS kegagalan masuk aplikasi terkelola di Wilayah tambahan	624
Masalah yang mengaktifkan instance Pusat Identitas IAM Multi-wilayah	625
Pembuatan kunci gagal	625
Replikasi kunci gagal	625
Pembuatan instance gagal	625
Riwayat dokumen	627
AWS Glosarium	640
.....	dcxli

Apa itu IAM Identity Center?

AWS IAM Identity Center adalah AWS solusi untuk menghubungkan pengguna tenaga kerja Anda ke aplikasi AWS terkelola seperti Kiro dan Amazon Quick, dan AWS sumber daya lainnya. Anda dapat menghubungkan penyedia identitas yang ada dan menyinkronkan pengguna dan grup dari direktori Anda, atau membuat dan mengelola pengguna secara langsung di Pusat Identitas IAM. Anda kemudian dapat menggunakan Pusat Identitas IAM untuk salah satu atau kedua hal berikut:

- Akses pengguna ke aplikasi
- Akses pengguna ke Akun AWS

Sudah menggunakan IAM untuk akses ke? Akun AWS

Anda tidak perlu membuat perubahan apa pun pada alur Akun AWS kerja Anda saat ini untuk menggunakan Pusat Identitas IAM untuk akses ke aplikasi terkel AWS ola. Jika Anda menggunakan [federasi dengan IAM](#) untuk Akun AWS akses, pengguna Anda dapat terus mengakses dengan Akun AWS cara yang sama seperti biasanya, dan Anda dapat terus menggunakan alur kerja yang ada untuk mengelola akses tersebut.

Mengapa menggunakan IAM Identity Center?

Pusat Identitas IAM merampingkan dan menyederhanakan akses pengguna tenaga kerja ke aplikasi atau Akun AWS, atau keduanya, melalui kemampuan utama berikut.

Integrasi dengan aplikasi AWS terkelola

[AWS aplikasi yang dikelola](#) seperti Kiro dan ter Amazon Redshift integrasi dengan IAM Identity Center. IAM Identity Center menyediakan AWS aplikasi terkelola dengan tampilan umum pengguna dan grup.

Propagasi identitas tepercaya di seluruh aplikasi

Dengan propagasi identitas tepercaya AWS , aplikasi terkelola seperti Amazon Quick dapat dengan aman berbagi identitas pengguna dengan aplikasi AWS terkelola lainnya seperti Amazon Redshift dan mengotorisasi akses ke AWS sumber daya berdasarkan identitas pengguna. Anda dapat lebih mudah mengaudit aktivitas pengguna karena CloudTrail peristiwa dicatat berdasarkan pengguna dan tindakan yang diprakarsai pengguna. Ini membuatnya lebih mudah

untuk memahami siapa yang mengakses apa. Untuk informasi tentang kasus penggunaan yang didukung, termasuk panduan konfigurasi end-to-end, lihat [Kasus penggunaan propagasi identitas tepercaya](#).

Satu titik federasi untuk menyederhanakan akses pengguna ke AWS

Dengan menyediakan satu titik federasi, Pusat Identitas IAM mengurangi upaya administratif yang diperlukan untuk menggunakan beberapa aplikasi ter AWS kelola dan Akun AWS. Dengan IAM Identity Center, Anda hanya melakukan federasi satu kali, dan Anda hanya memiliki satu sertifikat untuk dikelola saat menggunakan penyedia [SAML 2.0](#) identitas. Pusat Identitas IAM menyediakan AWS aplikasi terkelola dengan tampilan umum pengguna dan grup untuk kasus penggunaan propagasi identitas tepercaya, atau ketika pengguna berbagi akses ke AWS sumber daya dengan orang lain.

Untuk informasi tentang cara mengonfigurasi penyedia identitas yang umum digunakan untuk bekerja dengan Pusat Identitas IAM, lihat [Tutorial sumber identitas Pusat Identitas IAM](#). Jika Anda tidak memiliki penyedia identitas yang ada, Anda dapat [membuat dan mengelola pengguna secara langsung di Pusat](#) Identitas IAM.

Kemampuan untuk mengelola akses tenaga kerja ke beberapa Akun AWS

Pusat Identitas IAM memberi Anda opsi untuk mengelola secara terpusat akses tenaga kerja Anda ke: Akun AWS

- Tim Anda dapat membuat peran IAM mereka Akun AWS dan mengelola penugasan peran secara terpusat kepada pengguna dan grup Pusat Identitas IAM menggunakan fitur pengelola akses [akun IAM](#). Lihat [Mengapa menggunakan manajer akses akun](#) di Panduan Pengguna IAM untuk informasi selengkapnya.
- Anda juga dapat menggunakan kumpulan izin Pusat Identitas IAM untuk secara terpusat membuat izin untuk fungsi pekerjaan umum seperti admin, menyediakannya di seluruh Akun AWS, dan menetapkan ke pengguna dan grup. Fitur opsional ini hanya tersedia untuk instans organisasi dari Pusat Identitas IAM.

Dua jenis contoh

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

Instans akun terikat ke Akun AWS tempat mereka diaktifkan. Gunakan instance akun Pusat Identitas IAM hanya untuk mendukung penerapan terisolasi dari aplikasi terkelola tertentu. AWS Untuk informasi selengkapnya, lihat [Instans organisasi dan akun dari Pusat Identitas IAM](#).

User-friendly akses portal web untuk pengguna Anda

Portal AWS akses adalah portal web yang ramah pengguna yang menyediakan pengguna Anda dengan akses tanpa batas ke semua aplikasi yang ditugaskan Akun AWS, atau keduanya.

Multi-Region akses ke Akun AWS dan aplikasi

Saat Anda mereplikasi instans Pusat Identitas IAM ke Wilayah tambahan, tenaga kerja Anda dapat mengakses aplikasi yang ditugaskan Akun AWS melalui semua Wilayah yang diaktifkan, dan mereka dapat menerapkan aplikasi terkel AWS ola di setiap Wilayah yang diaktifkan.

Ganti nama Pusat Identitas IAM

Pada 26 Juli 2022, AWS Single berg Sign-On anti nama menjadi AWS IAM Identity Center.

Ruang nama lama tetap sama

Ruang nama sso dan identitystore API 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 aw AWSIdentitySync alan
- [Titik akhir layanan](#) yang berisi dan sso identitystore
- [CloudFormation](#) sumber daya yang berisi AWS::SSO awalan
- [Service-linked peran](#) yang mengandung AWSServiceRoleForSSO
- URL konsol yang berisi sso dan singlesignon
- URL dokumentasi yang berisi singlesignon

Memulai dengan IAM Identity Center

Berikut ini menguraikan bagaimana Anda bisa memulai dengan IAM Identity Center.

1. Aktifkan Pusat Identitas IAM

Saat [mengaktifkan Pusat Identitas IAM](#), Anda memilih antara dua jenis instans Pusat Identitas IAM. Jenis ini adalah: inst [ans organisasi](#) (disarankan) dan inst [ans akun](#). Untuk mempelajari selengkapnya tentang berbagai kemampuan jenis instans ini, lihat instans [organisasi dan akun Pusat Identitas IAM](#).

Note

Setelah Pusat Identitas IAM diaktifkan, Anda dapat masuk dan membuka konsol Pusat Identitas [tas IAM](#) dengan melakukan salah satu dari hal berikut:

- Instans organisasi - Masuk untuk AWS menggunakan kredensial dengan izin administratif di akun manajemen.
- Instans akun - Masuk untuk AWS menggunakan kredensial dengan izin administratif di Akun AWS tempat IAM Identity Center diaktifkan.

2. Hubungkan sumber identitas Anda ke Pusat Identitas IAM

Di konsol Pusat Identitas IAM, konfirmasikan sumber identitas yang ingin Anda gunakan. Lihat berikut untuk sumber identitas:

- Penyedia identitas eksternal - Jika Anda memiliki penyedia identitas yang ada untuk mengelola pengguna tenaga kerja Anda, Anda dapat menghubungkannya ke Pusat Identitas IAM. Untuk informasi selengkapnya tentang cara mengonfigurasi penyedia identitas yang umum digunakan untuk bekerja dengan Pusat Identitas IAM, lihat [Tutorial sumber identitas Pusat Identitas IAM](#).
- Active Directory - Jika Anda menggunakan Active Directory untuk mengelola pengguna tenaga kerja Anda, Anda dapat menghubungkannya ke Pusat Identitas IAM. Untuk informasi selengkapnya, lihat [Menggunakan Active Directory sebagai sumber identitas](#).
- Pusat Identitas IAM - Atau, Anda dapat [membuat dan mengelola pengguna dan grup secara langsung di Pusat Identitas IAM](#).

 Note

Untuk memanfaatkan pengaturan Multi-wilayah, Anda harus menggunakan penyedia identitas eksternal atau direktori Pusat Identitas sebagai sumber identitas untuk Pusat Identitas IAM Anda. Multi-Region dukungan tidak tersedia untuk Active Directory. Untuk informasi selengkapnya, lihat [Menggunakan Pusat Identitas IAM di beberapa Wilayah AWS](#).

3. Menyiapkan akses pengguna ke Akun AWS (hanya instans organisasi)

Jika Anda menggunakan instance organisasi dari Pusat Identitas IAM, Anda dapat [menetapkan akses pengguna atau grup ke Akun AWS](#), menggunakan kumpulan [izin](#) untuk memberi pengguna akses ke Akun AWS dan sumber daya.

4. Mengatur akses pengguna ke aplikasi

Dengan IAM Identity Center, Anda dapat memberikan pengguna akses ke dua jenis aplikasi:

a. [AWS aplikasi yang dikelola](#)

- Anda dapat menggunakan Pusat Identitas IAM dengan aplikasi AWS terkelola seperti Amazon Q Business, AWS CLI, dan Amazon Redshift. Untuk informasi selengkapnya, lihat [AWS aplikasi yang dikelola](#) dan [Mengintegrasikan AWS CLI dengan IAM Identity Center](#).

b. [Aplikasi yang dikelola pelanggan](#)

- Anda dapat mengintegrasikan salah satu dari jenis aplikasi yang dikelola pelanggan berikut ini dengan Pusat Identitas IAM:
 - [Aplikasi yang tercantum dalam katalog Pusat Identitas IAM](#)
 - [Aplikasi kustom Anda](#)
- Setelah mengonfigurasi aplikasi Anda, Anda dapat [menetapkan akses pengguna Anda ke aplikasi](#).

5. Berikan instruksi masuk kepada pengguna Anda untuk portal AWS akses

Portal AWS akses adalah portal web yang menyediakan pengguna Anda dengan akses tanpa batas ke semua aplikasi yang ditugaskan Akun AWS, atau keduanya. Pengguna baru di Pusat Identitas IAM harus mengaktifkan kredentif pengguna mereka sebelum mereka dapat masuk ke portal AWS akses.

Untuk informasi tentang cara masuk ke portal AWS akses, lihat [Masuk ke portal AWS akses](#) di Panduan AWS Sign-In Pengguna. Untuk mempelajari tentang proses masuk untuk portal AWS akses, lihat [Masuk ke portal AWS akses](#).

Prasyarat dan pertimbangan IAM Identity Center

Anda dapat menggunakan IAM Identity Center untuk akses ke aplikasi AWS terkelola saja, Akun AWS hanya, atau keduanya. Jika Anda menggunakan federasi IAM untuk mengelola akses ke Akun AWS, Anda dapat terus melakukannya saat menggunakan IAM Identity Center untuk akses aplikasi.

Sebelum mengaktifkan IAM Identity Center, pertimbangkan hal berikut:

- AWS Wilayah

Pertama-tama Anda mengaktifkan Pusat Identitas IAM dalam satu Wilayah yang [didukung](#) untuk setiap instance Pusat Identitas IAM. Jika Anda ingin menggunakan Pusat Identitas IAM untuk akses masuk tunggal ke AWS akun, Wilayah harus dapat diakses oleh semua pengguna di organisasi Anda. Jika Anda berencana menggunakan Pusat Identitas IAM untuk akses aplikasi, ketahuilah bahwa beberapa aplikasi yang AWS dikelola, seperti Amazon SageMaker AI, hanya dapat beroperasi di Wilayah yang mereka dukung. Selain itu, sebagian besar aplikasi yang AWS dikelola memerlukan IAM Identity Center untuk tersedia di Wilayah yang sama dengan aplikasi. Ini dapat dicapai dengan menempatkannya bersama di Wilayah yang sama, atau ketika didukung, dengan mereplikasi instance Pusat Identitas IAM ke Wilayah penerapan yang diinginkan dari aplikasi terkelola. AWS Untuk informasi selengkapnya, lihat [Pertimbangan untuk memilih Wilayah AWS](#).

- Akses aplikasi saja

Anda dapat menggunakan IAM Identity Center hanya untuk akses pengguna ke aplikasi seperti Kiro, menggunakan penyedia identitas yang ada. Untuk informasi selengkapnya, lihat [Menggunakan Pusat Identitas IAM untuk akses pengguna ke aplikasi saja](#).

 Note

Akses ke sumber daya aplikasi dikelola secara independen oleh pemilik aplikasi.

- Kuota untuk peran IAM

IAM Identity Center membuat peran IAM untuk memberikan izin pengguna ke sumber daya akun. Untuk informasi selengkapnya, lihat [Peran IAM dibuat oleh IAM Identity Center](#).

- 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. Jika Anda sudah menyiapkan AWS Organizations dan akan menambahkan Pusat Identitas IAM ke organisasi Anda, pastikan semua AWS Organizations fitur diaktifkan. Untuk informasi selengkapnya, lihat [Pusat Identitas IAM dan AWS Organizations](#).

Antarmuka web IAM Identity Center, termasuk portal akses dan konsol IAM Identity Center, dimaksudkan untuk diakses oleh manusia melalui browser web yang didukung. Browser yang kompatibel mencakup tiga versi terbaru Microsoft Edge, Mozilla Firefox, Google Chrome, dan Apple Safari. Mengakses titik akhir ini menggunakan jalur berbasis non-browser tidak didukung. Untuk akses terprogram ke layanan IAM Identity Center, sebaiknya gunakan dokumentasi yang APIs tersedia di panduan referensi IAM Identity Center dan Identity Store API.

Pertimbangan untuk memilih Wilayah AWS

Anda dapat mengaktifkan Pusat Identitas IAM dalam satu, didukung Wilayah AWS pilihan Anda dan tersedia untuk pengguna secara global. Ketersediaan global ini memudahkan Anda untuk mengonfigurasi akses pengguna ke beberapa Akun AWS aplikasi. Berikut ini adalah pertimbangan utama untuk memilih Wilayah AWS.

- Lokasi geografis pengguna Anda — Saat Anda memilih Wilayah yang secara geografis paling dekat dengan sebagian besar pengguna akhir Anda, mereka akan memiliki latensi akses yang lebih rendah ke portal AWS akses dan aplikasi terkel AWS ola, seperti Amazon SageMaker AI.
- Opt-in Wilayah (Wilayah yang dinonaktifkan secara default) — Wilayah opt-in adalah wilayah Wilayah AWS yang dinonaktifkan secara default. Untuk menggunakan Wilayah opt-in, Anda harus mengaktifkannya. Untuk informasi selengkapnya, lihat [Mengelola Pusat Identitas IAM di Wilayah pilihan](#).
- Mereplikasi Pusat Identitas IAM ke Wilayah tambahan — Jika Anda berencana untuk mereplikasi Pusat Identitas IAM ke tambahan Wilayah AWS, Anda harus memilih Wilayah yang diaktifkan secara default. Untuk informasi selengkapnya, lihat [Menggunakan Pusat Identitas IAM di beberapa Wilayah AWS](#).

- Memilih Wilayah pener AWS apan untuk aplikasi ter AWS kelola — aplikasi terkelola hanya dapat beroperasi Wilayah AWS di tempat aplikasi tersebut tersedia. Banyak aplikasi AWS terkelola juga dapat beroperasi hanya di Wilayah di mana Pusat Identitas IAM diaktifkan atau direplikasi ke (Wilayah primer atau tambahan). Untuk mengonfirmasi apakah instance Pusat Identitas IAM Anda mendukung replikasi ke Wilayah tambahan, lihat [Menggunakan Pusat Identitas IAM di beberapa Wilayah AWS](#). Jika replikasi bukan pilihan, pertimbangkan untuk mengaktifkan Pusat Identitas IAM di Wilayah tempat Anda berencana untuk menggunakan aplikasi terkel AWS ola.
- Kedaulatan digital — Peraturan kedaulatan digital atau kebijakan perusahaan dapat mengamankan penggunaan tertentu Wilayah AWS. Konsultasikan dengan departemen hukum perusahaan Anda.
- Sumber identitas — Jika Anda menggunakan [AWS Managed Microsoft AD](#) atau direktori yang dikelola sendiri di [Active Directory \(AD\)](#) sebagai sumber identitas, Wilayah berandanya harus sesuai dengan tempat Wilayah AWS Anda mengaktifkan Pusat Identitas IAM.
- Cross-Region email dengan Amazon Simple Email Service — Di beberapa Wilayah, Pusat Identitas IAM dapat menghubungi [Amazon Simple Email Service \(Amazon SES\)](#) di Wilayah yang berbeda untuk mengirim email. Dalam panggilan Lintas wilayah ini, Pusat Identitas IAM mengirimkan atribut pengguna tertentu ke Wilayah lainnya. Untuk informasi selengkapnya, lihat [Cross-Region email dengan Amazon SES](#).
- AWS Control Tower— Jika Anda mengaktifkan instance organisasi dari Pusat Identitas IAM AWS Control Tower, instans akan dibuat di Wilayah yang sama dengan zona AWS Control Tower pendaratan.

Topik

- [Penyimpanan dan operasi data Wilayah Pusat Identitas IAM](#)
- [Beralih Wilayah AWS](#)
- [Menonaktifkan Wilayah AWS di mana Pusat Identitas IAM diaktifkan](#)

Penyimpanan dan operasi data Wilayah Pusat Identitas IAM

Pelajari cara IAM Identity Center menangani penyimpanan data dan operasi di seluruh Wilayah AWS area.

Memahami cara IAM Identity Center menyimpan data

Saat Anda mengaktifkan Pusat Identitas IAM, semua data yang Anda konfigurasi di Pusat Identitas IAM disimpan di Wilayah tempat Anda mengaktifkannya. Data ini mencakup konfigurasi

direktori, kumpulan izin, instance aplikasi, dan penugasan pengguna ke Akun AWS aplikasi. 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. Jika Anda mereplikasi instance Pusat Identitas IAM ke Wilayah tambahan, Pusat Identitas IAM secara otomatis mereplikasi pengguna, grup, kumpulan izin dan penetapan mereka, serta metadata dan konfigurasi lainnya ke Wilayah tersebut.

Cross-Region email dengan Amazon SES

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 peristiwa manajemen identitas dan kredensial 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 Wilayah AWS yang didukung IAM Identity Center.

Pusat Identitas IAM memanggil titik akhir lokal Amazon SES ketika Amazon SES tersedia secara lokal di Wilayah AWS. Jika Amazon SES tidak tersedia secara lokal, Pusat Identitas IAM memanggil titik akhir Amazon SES dengan cara yang berbeda Wilayah AWS, seperti yang ditunjukkan pada tabel berikut.

IAM Identity Center Kode wilayah	Nama Wilayah Pusat Identitas IAM	Amazon SES Kode wilayah	Nama wilayah Amazon SES
ap-east-1	Asia Pasifik (Hong Kong)	ap-northeast-2	Asia Pasifik (Seoul)
ap-east-2	Asia Pasifik (Taipei)	ap-northeast-1	Asia Pasifik (Tokyo)
ap-south-2	Asia Pasifik (Hyderabad)	ap-south-1	Asia Pasifik (Mumbai)
ap-southeast-4	Asia Pacific (Melbourne)	ap-southeast-2	Asia Pasifik (Sydney)
ap-southeast-5	Asia Pasifik (Malaysia)	ap-southeast-1	Asia Pasifik (Singapura)

IAM Identity Center Kode wilayah	Nama Wilayah Pusat Identitas IAM	Amazon SES Kode wilayah	Nama wilayah Amazon SES
ap-southeast-6	Asia Pasifik (Selandia Baru)	ap-southeast-2	Asia Pasifik (Sydney)
ap-southeast-7	Asia Pasifik (Thailand)	ap-northeast-3	Asia Pasifik (Osaka)
ca-west-1	Kanada Barat (Calgary)	ca-central-1	Kanada (Pusat)
eu-south-2	Eropa (Spanyol)	eu-west-3	Eropa (Paris)
eu-central-2	Europe (Zurich)	eu-central-1	Eropa (Frankfurt)
mx-central-1	Meksiko (Tengah)	us-east-2	AS Timur (Ohio)
me-central-1	Timur Tengah (UAE)	eu-central-1	Eropa (Frankfurt)
us-gov-east-1	AWS GovCloud (US-East)	us-gov-west-1	AWS GovCloud (US-West)

Dalam panggilan lintas wilayah ini, Pusat Identitas IAM mungkin mengirim 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 opt-in (Wilayah yang dinonaktifkan secara default)

Sebagian besar Wilayah AWS diaktifkan untuk operasi di semua AWS layanan secara default, tetapi Anda harus mengaktifkan Wilayah [pilihan berikut](#) jika ingin menggunakan Pusat Identitas IAM:

- Africa (Cape Town)
- Asia Pasifik (Hong Kong)
- Asia Pasifik (Taipei)
- Asia Pasifik (Hyderabad)
- Asia Pasifik (Jakarta)
- Asia Pacific (Melbourne)
- Asia Pasifik (Malaysia)
- Asia Pasifik (Selandia Baru)
- Asia Pasifik (Thailand)
- Kanada Barat (Calgary)
- Europe (Milan)
- Eropa (Spanyol)
- Europe (Zurich)
- Israel (Tel Aviv)
- Meksiko (Tengah)
- Timur Tengah (Bahrain)
- Middle East (UAE)

Jika Anda menerapkan Pusat Identitas IAM di Wilayah pilihan, maka Anda harus mengaktifkan Wilayah ini di semua akun yang ingin Anda kelola aksesnya ke Pusat Identitas IAM. Semua akun memerlukan konfigurasi ini, apakah Anda akan membuat sumber daya di Wilayah tersebut atau tidak. Anda dapat mengaktifkan Wilayah untuk akun saat ini di organisasi Anda dan Anda harus mengulangi tindakan ini saat menambahkan akun baru. Untuk petunjuk, lihat [Mengaktifkan atau menonaktifkan Wilayah di organisasi Anda](#) di Panduan AWS Organizations Pengguna. Untuk menghindari mengulangi langkah-langkah tambahan ini, Anda dapat memilih untuk menerapkan Pusat Identitas IAM Anda di Wil [ayah yang diaktifkan secara default](#).

 Note

Akun AWS anggota Anda harus dipilih ke Wilayah yang sama dengan Wilayah pilihan tempat instance Pusat Identitas IAM Anda berada, sehingga Anda dapat mengakses akun AWS anggota dari portal akses. AWS

Metadata disimpan di Wilayah opt-in

Saat Anda mengaktifkan Pusat Identitas IAM untuk akun manajemen dalam pilihan 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 oleh Pusat Identitas IAM di akun anggota

Wilayah AWS yang diaktifkan secara default

Wilayah berikut diaktifkan secara default dan Anda dapat mengaktifkan Pusat Identitas IAM di Wilayah ini.

- 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)

Beralih Wilayah AWS

Sebaiknya instal Pusat Identitas IAM di Wilayah yang ingin Anda sediakan untuk pengguna, bukan Wilayah yang mungkin perlu Anda nonaktifkan. Untuk informasi selengkapnya, lihat [Pertimbangan untuk memilih Wilayah AWS](#).

Anda dapat mengganti Wilayah Pusat Identitas IAM hanya dengan [menghapus instans Pusat Identitas IAM saat ini](#) dan membuat instance di Wilayah lain. Jika Anda sudah mengaktifkan aplikasi ter AWS kelola dengan instance Pusat Identitas IAM yang ada, nonaktifkan aplikasi sebelum menghapus Pusat Identitas IAM. Untuk petunjuk tentang menonaktifkan aplikasi AWS terkelola, lihat [Menonaktifkan AWS aplikasi yang dikelola](#).

Note

Jika Anda mempertimbangkan untuk mengalihkan Wilayah Pusat Identitas IAM untuk mengaktifkan penerapan aplikasi terkel AWS di Wilayah lain, pertimbangkan untuk mereplikasi instance Pusat Identitas IAM Anda ke Wilayah tersebut sebagai gantinya. Untuk informasi selengkapnya, lihat [Menggunakan Pusat Identitas IAM di beberapa Wilayah AWS](#).

Pertimbangan konfigurasi di Wilayah baru

Anda harus membuat ulang pengguna, grup, kumpulan izin, aplikasi, dan penugasan di instance Pusat Identitas IAM yang baru. Anda dapat menggunakan akun Pusat Identitas IAM dan [API penugasan aplikasi](#) untuk mendapatkan snapshot konfigurasi Anda dan kemudian menggunakan snapshot tersebut untuk membangun kembali konfigurasi Anda di Wilayah baru. Beralih ke Wilayah yang berbeda juga mengubah URL untuk portal [AWS akses](#), yang memberi pengguna Anda akses masuk tunggal ke aplikasi mereka Akun AWS. Anda mungkin juga perlu membuat ulang beberapa konfigurasi Pusat Identitas IAM melalui Konsol Manajemen instans baru Anda.

Menonaktifkan Wilayah AWS di mana Pusat Identitas IAM diaktifkan

Jika Anda menonaktifkan Wilayah AWS 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.

Untuk mengaktifkan kembali Pusat Identitas IAM dalam [opt-in Wilayah AWS](#), Anda harus mengaktifkan kembali Wilayah. Karena Pusat Identitas IAM harus memproses ulang semua peristiwa yang dijeda, mengaktifkan kembali Pusat Identitas IAM mungkin memerlukan waktu.

 Note

Pusat Identitas IAM dapat mengelola akses hanya ke Akun AWS yang diaktifkan untuk digunakan dalam Wilayah AWS. Untuk mengelola akses di semua akun di organisasi Anda, aktifkan Pusat Identitas IAM di akun manajemen di akun Wilayah AWS yang secara otomatis diaktifkan untuk digunakan dengan Pusat Identitas IAM.

Untuk informasi selengkapnya tentang mengaktifkan dan menonaktifkan Wilayah AWS, lihat [Mengelola Wilayah AWS](#) di Referensi Umum.

Menggunakan Pusat Identitas IAM untuk akses pengguna ke aplikasi saja

Anda dapat menggunakan IAM Identity Center untuk akses pengguna ke aplikasi seperti Kiro, Akun AWS, atau keduanya. Anda dapat menghubungkan penyedia identitas yang ada dan menyinkronkan pengguna dan grup dari direktori Anda, atau [membuat dan mengelola pengguna secara langsung di Pusat Identitas IAM](#). Untuk informasi tentang cara menghubungkan penyedia identitas Anda yang ada ke Pusat Identitas IAM, lihat [Tutorial sumber identitas Pusat Identitas IAM](#).

Sudah menggunakan IAM untuk akses ke? Akun AWS

Anda tidak perlu membuat perubahan apa pun pada alur Akun AWS kerja Anda saat ini untuk menggunakan Pusat Identitas IAM untuk akses ke aplikasi terkel AWS. Jika Anda menggunakan [federasi dengan IAM](#) untuk Akun AWS akses, pengguna Anda dapat terus mengakses dengan Akun AWS cara yang sama seperti biasanya, dan Anda dapat terus menggunakan alur kerja yang ada untuk mengelola akses tersebut.

Peran IAM dibuat oleh IAM Identity Center

Ketika Anda menetapkan pengguna ke AWS akun IAM Identity Center membuat peran IAM untuk memberikan izin pengguna ke sumber daya.

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 AWS akses atau AWS CLI. Saat Anda mengubah set izin, IAM Identity Center memastikan bahwa kebijakan dan peran IAM yang sesuai diperbarui. Mereplikasi instans Pusat Identitas IAM Anda ke Wilayah tambahan tidak memengaruhi peran IAM yang ada, dan itu tidak membuat peran IAM baru.

 Note

Set izin tidak digunakan untuk memberikan izin ke aplikasi.

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 Pusat Identitas IAM, Anda mungkin melihat nama peran yang dimulai dengan. “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 [Instans organisasi dari Pusat Identitas IAM](#).

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 Pengguna AWS Organizations .

Untuk mengaktifkan instans organisasi Pusat Identitas IAM, Anda harus masuk ke Konsol Manajemen AWS 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 yang ada). Untuk informasi selengkapnya, lihat [Membuat dan mengelola AWS Organisasi](#) di Panduan AWS Organizations Pengguna.

Saat masuk dengan kredensi administratif dari akun AWS Organizations anggota, Anda dapat mengaktifkan instance akun Pusat Identitas IAM. Instans akun memiliki kemampuan terbatas dan terikat pada satu AWS akun.

Instans organisasi dan akun dari Pusat Identitas IAM

Instance adalah penyebaran tunggal dari Pusat Identitas IAM. Ada dua jenis instans yang tersedia untuk Pusat Identitas IAM: instans organisasi dan instans akun.

- Contoh organisasi (disarankan)

Instance Pusat Identitas IAM yang Anda aktifkan di akun AWS Organizations manajemen. Instans organisasi mendukung semua fitur Pusat Identitas IAM. Sebaiknya gunakan instance organisasi ketimbang instance akun untuk meminimalkan jumlah titik manajemen.

- Contoh akun

Instance Pusat Identitas IAM yang terikat ke satu Akun AWS, dan yang hanya terlihat di dalam Akun AWS dan Wil AWS ayah di mana ia diaktifkan. Gunakan instance akun untuk skenario akun tunggal yang lebih sederhana. Anda dapat mengaktifkan instance akun dari salah satu dari berikut ini:

- Akun AWS Yang tidak dikelola oleh AWS Organizations
- Akun anggota di AWS Organizations

Akun AWS jenis yang dapat mengaktifkan Pusat Identitas IAM

Untuk mengaktifkan Pusat Identitas IAM, masuk ke Konsol Manajemen AWS dengan menggunakan salah satu kredensial berikut, tergantung pada jenis instans yang ingin Anda buat:

- Akun AWS Organizations manajemen Anda (disarankan) — Diperlukan untuk membuat instance [???](#) organisasi Pusat Identitas IAM. Gunakan instance organisasi untuk izin multi-akun dan penugasan aplikasi di seluruh organisasi.
- Akun AWS Organizations anggota Anda — Digunakan untuk membuat instance [akun Pusat Identitas IAM](#) untuk mengaktifkan penugasan aplikasi dalam akun anggota tersebut. Satu atau lebih akun dengan instance tingkat anggota dapat ada di organisasi.
- Mandiri Akun AWS — Digunakan untuk membuat instance [organisasi](#) atau instance [???](#) akun Pusat Identitas IAM. Mandiri Akun AWS tidak dikelola oleh AWS Organizations. Anda hanya dapat mengaitkan satu instance Pusat Identitas IAM dengan mandiri Akun AWS dan menggunakan instance tersebut untuk penugasan aplikasi dalam mandiri Akun AWS itu.

Gunakan tabel berikut untuk membandingkan kemampuan yang disediakan oleh jenis instans:

Kemampuan	Contoh di akun AWS Organizations manajemen (disarankan)	Instans di akun anggota	Instance dalam mandiri Akun AWS
Mengelola pengguna	✔Iya	✔Iya	✔Iya
AWS portal akses untuk akses masuk tunggal ke aplikasi terkel AWS ola Anda	✔Iya	✔Iya	✔Iya
Aplikasi yang dikelola pelanggan OAuth 2.0 (OIDC)	✔Iya	✔Iya	✔Iya
Multi-account izin	✔Iya	✘Tidak	✘Tidak
AWS akses portal untuk akses masuk	✔Iya	✘Tidak	✘Tidak

Kemampuan	Contoh di akun AWS Organizations manajemen (disarankan)	Instans di akun anggota	Instance dalam mandiri Akun AWS
tunggal ke Anda Akun AWS			
Aplikasi yang dikelola pelanggan SAML 2.0	✔Iya	✘Tidak	✘Tidak
Administrator yang didelegasikan dapat mengelola instance	✔Iya	✘Tidak	✘Tidak
Enkripsi saat diam menggunakan kunci KMS yang dikelola pelanggan	✔Iya	✘Tidak	✘Tidak
Mereplikasi Pusat Identitas IAM ke Wilayah tambahan	✔Iya	✘Tidak	✘Tidak

Untuk informasi selengkapnya tentang AWS aplikasi terkelola dan Pusat Identitas IAM, lihat [AWS aplikasi terkelola yang dapat Anda gunakan dengan IAM Identity Center](#).

Topik

- [Instans organisasi dari Pusat Identitas IAM](#)
- [Instans akun Pusat Identitas IAM](#)
- [Menghapus instance Pusat Identitas IAM Anda](#)

Instans organisasi dari Pusat Identitas IAM

Saat Anda mengaktifkan Pusat Identitas IAM bersamaan dengan AWS Organizations, Anda membuat instance organisasi Pusat Identitas IAM. 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 instance organisasi untuk setiap akun manajemen di AWS Organizations.

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

Untuk mengaktifkan instance organisasi dari Pusat Identitas IAM, lihat [Untuk mengaktifkan instance Pusat Identitas IAM](#).

Kapan menggunakan instance organisasi

Instance organisasi adalah metode utama untuk mengaktifkan Pusat Identitas IAM dan biasanya, instance organisasi direkomendasikan. Instans organisasi menawarkan manfaat berikut:

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

Untuk petunjuk tentang mengaktifkan instance organisasi dari Pusat Identitas IAM, lihat [Untuk mengaktifkan instance Pusat Identitas IAM](#).

Opsi konfigurasi instans

Bila Anda mengaktifkan instance organisasi dalam [Wilayah AWS yang diaktifkan secara default](#), Anda memilih konfigurasi instans. Di Wilayah lain, instance Anda dibuat dengan pengaturan default.

Note

Opsi Multi-Region instans dan Instans Kustom (buat kunci baru) membuat kunci KMS yang dikelola pelanggan yang ditandai dengan CreatedBy: IAM Identity Center dan mereplikasinya ke Wilayah tambahan atas nama Anda. Verifikasi bahwa prinsipal IAM Anda

memiliki `kms:CreateKey`, `kms:TagResource`, dan `kms:ReplicateKey` izin selain izin yang [diperlukan untuk mengaktifkan Pusat Identitas IAM](#).

Single-Region contoh

Instans Anda dibuat di Wilayah saat ini.

- **Enkripsi saat diam** — Data Anda dienkripsi dengan kunci yang AWS dimiliki. Anda dapat beralih ke kunci yang dikelola pelanggan nanti dari halaman Pengaturan.
- **Kumpulan izin** — Diaktifkan secara default, memungkinkan Anda mengelola Akun AWS akses untuk pengguna dan grup. Ini tidak dapat dinonaktifkan setelah diaktifkan.
- **Wilayah Utama** — Instans Anda dibuat di Wilayah saat ini. Hal ini tidak dapat diubah setelah pembuatan.
- **Wilayah Tambahan** — Tidak ada Wilayah tambahan yang dikonfigurasi. Anda dapat menambahkan Wilayah nanti dari halaman Pengaturan.

Multi-Region contoh

Instans Anda dibuat di Wilayah saat ini dan direplikasi ke Wilayah tambahan untuk akses tangguh Akun AWS dan aplikasi.

- **Enkripsi saat diam** — Data Anda dienkripsi dengan kunci Multi-wilayah yang dikelola pelanggan yang dibuat di akun Anda dengan kebijakan kunci yang mendukung replikasi. Kuncinya ditandai `CreatedBy: IAM Identity Center` sehingga Anda dapat dengan mudah mengidentifikasinya di akun Anda. Kuncinya bisa diubah nanti. AWS KMS dikenakan biaya.
- **Kumpulan izin** — Diaktifkan secara default, memungkinkan Anda mengelola Akun AWS akses untuk pengguna dan grup. Ini tidak dapat dinonaktifkan setelah diaktifkan.
- **Wilayah Utama** — Instans Anda dibuat di Wilayah saat ini. Hal ini tidak dapat diubah setelah pembuatan.
- **Wilayah Tambahan** — Instans Anda direplikasi ke Wilayah tambahan untuk akses tangguh Akun AWS dan aplikasi. Anda dapat mengubah Wilayah atau menambahkan lebih banyak Wilayah nanti.

Instans khusus

Konfigurasi instans Anda secara individual.

Enkripsi saat diam

Pilih salah satu dari berikut ini. Kunci yang dikelola pelanggan diperlukan untuk menambahkan Wilayah tambahan.

- Gunakan kunci yang AWS dimiliki — Data Anda dienkripsi dengan kunci yang dimiliki AWS dan dikelola. Tidak ada biaya tambahan yang berlaku.
- Buat kunci yang dikelola pelanggan baru — Kunci multi-wilayah dibuat di akun Anda dengan kebijakan kunci dasar yang mendukung replikasi. AWS KMS dikenakan biaya.
- Pilih kunci yang dikelola pelanggan yang ada — Gunakan kunci yang sudah ada di akun Anda. Pastikan kebijakan utama memenuhi persyaratan untuk instance Anda. AWS KMS dikenakan biaya.

Kumpulan izin

Anda dapat memilih untuk mengaktifkan kumpulan izin, memungkinkan Anda mengelola Akun AWS akses untuk pengguna dan grup. Ini tidak dapat dinonaktifkan setelah diaktifkan.

Wilayah Tambahan

Tambahkan Wilayah untuk akses tangguh Akun AWS dan aplikasi. Kunci yang dikelola AWS KMS pelanggan juga harus tersedia di Wilayah yang dipilih.

Untuk petunjuk tentang mengaktifkan instance organisasi, lihat [Aktifkan Pusat Identitas IAM](#). Untuk informasi selengkapnya tentang dukungan Multi-wilayah, lihat [Menggunakan Pusat Identitas IAM di beberapa Wilayah AWS](#).

Instans akun Pusat Identitas IAM

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

Instans akun terikat ke 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 instans akun per Akun AWS. Anda dapat membuat instance akun dari salah satu dari berikut ini: akun anggota dalam AWS Organizations atau mandiri Akun AWS yang tidak dikelola oleh AWS Organizations.

Untuk petunjuk tentang cara mengaktifkan instance akun Pusat Identitas IAM, lihat [Untuk mengaktifkan instance Pusat Identitas IAM](#) dan pilih tab Akun.

Kapan menggunakan instance akun

Dalam kebanyakan kasus, contoh [organisasi](#) direkomendasikan. Gunakan instance akun hanya jika salah satu skenario berikut berlaku:

- Anda ingin menjalankan uji coba sementara aplikasi terkel AWS ola yang didukung untuk menentukan apakah aplikasi tersebut sesuai dengan kebutuhan bisnis Anda.
- Anda tidak memiliki rencana untuk mengadopsi Pusat Identitas IAM di seluruh organisasi Anda, tetapi Anda ingin mendukung satu atau beberapa aplikasi terkel AWS ola.
- Anda memiliki instance organisasi Pusat Identitas IAM, tetapi Anda ingin menyebarkan aplikasi terkel AWS ola yang didukung ke kumpulan pengguna terisolasi yang berbeda dari pengguna dalam instans organisasi Anda.
- Anda tidak mengontrol AWS organisasi tempat Anda beroperasi. Misalnya, pihak ketiga mengontrol AWS organisasi yang mengelola Anda Akun AWS.

Important

Jika Anda berencana menggunakan Pusat Identitas IAM untuk mendukung aplikasi di beberapa akun, gunakan instance organisasi. Instans akun tidak mendukung kasus penggunaan ini.

AWS aplikasi terkelola yang mendukung instance akun

Lihat [AWS aplikasi terkelola yang dapat Anda gunakan dengan IAM Identity Center](#) untuk mempelajari aplikasi ter AWS kelola mana yang mendukung instance akun Pusat Identitas IAM. Verifikasi ketersediaan pembuatan instance akun dengan aplikasi terkel AWS ola Anda.

Batasan ketersediaan untuk akun anggota

Untuk menerapkan instance akun Pusat Identitas IAM di akun AWS Organizations anggota, salah satu kondisi berikut harus benar:

- Tidak ada instance organisasi dari Pusat Identitas IAM di organisasi Anda.

- Ada instance organisasi Pusat Identitas IAM di organisasi Anda dan administrator instans mengizinkan pembuatan instance akun Pusat Identitas IAM (untuk instans organisasi yang dibuat setelah 15 November 2023).
- Ada instance organisasi Pusat Identitas IAM di organisasi Anda dan administrator instans mengaktifkan pembuatan instans akun secara manual oleh akun anggota di organisasi (untuk instans organisasi yang dibuat sebelum 15 November 2023). Untuk petunjuk, lihat [Izinkan pembuatan instance akun di akun anggota](#).

Setelah salah satu kondisi sebelumnya terpenuhi, semua kondisi berikut harus benar:

- Administrator Anda belum membuat Kebijakan Kontrol [Layanan](#) yang mencegah akun anggota membuat instance akun.
- Anda belum memiliki instance Pusat Identitas IAM di akun yang sama ini, terlepas dari Wilayah AWS itu.
- Anda bekerja di tempat di Wilayah AWS mana Pusat Identitas IAM tersedia. Untuk informasi tentang Wilayah, lihat [Penyimpanan dan operasi data Wilayah Pusat Identitas IAM](#).

Pertimbangan instance akun

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

- Instans akun tidak mendukung kumpulan izin dan karenanya tidak mendukung akses ke Akun AWS.
- Anda tidak dapat mengonversi atau menggabungkan instance akun menjadi instance organisasi.
- Hanya pilih aplikasi [AWS terkelola](#) yang mendukung instance akun.
- Gunakan instance akun untuk pengguna terisolasi yang akan menggunakan aplikasi dalam satu akun saja dan selama masa pakai aplikasi yang digunakan.
- Aplikasi yang dilampirkan ke instance akun harus tetap dilampirkan ke instance akun sampai Anda menghapus aplikasi dan sumber dayanya.
- Instance akun harus tetap berada di Akun AWS tempat pembuatannya.

Izinkan pembuatan instance akun di akun anggota

Jika Anda mengaktifkan Pusat Identitas IAM sebelum 15 November 2023, Anda memiliki instance [organisasi Pusat Identitas IAM](#) dengan kemampuan akun anggota untuk membuat instance akun dinonaktifkan secara default. Anda dapat memilih apakah akun anggota Anda dapat membuat instance akun dengan mengaktifkan fitur instance akun di konsol Pusat Identitas IAM.

Untuk mengaktifkan pembuatan instance akun oleh akun anggota di organisasi Anda

Important

Mengaktifkan instance akun Pusat Identitas IAM untuk akun anggota adalah operasi satu kali. Ini berarti bahwa operasi ini tidak dapat dibalik. Setelah diaktifkan, Anda dapat membatasi pembuatan instance akun dengan membuat kebijakan kontrol layanan (SCP). Untuk petunjuk, lihat [Mengontrol pembuatan instance akun dengan Kebijakan Kontrol Layanan](#).

1. Buka konsol [Pusat Identitas IAM](#).
2. Pilih Pengaturan, lalu pilih tab Manajemen.
3. Di bagian Instance akun Pusat Identitas IAM, pilih Aktifkan instance akun Pusat Identitas IAM.
4. Di kotak dialog Aktifkan instance akun Pusat Identitas IAM, konfirmasi bahwa Anda ingin mengizinkan akun anggota di organisasi Anda membuat instance akun dengan memilih Aktifkan.

Gunakan Kebijakan Kontrol Layanan untuk mengontrol pembuatan instance akun

Kemampuan akun anggota untuk membuat instance akun tergantung pada saat Anda mengaktifkan Pusat Identitas IAM:

- Sebelum November 2023 — Anda harus [mengizinkan pembuatan instance akun di akun anggota](#), yang merupakan tindakan yang tidak dapat dibatalkan.
- Setelah 15 November 2023 — Akun anggota dapat membuat instance akun secara default.

Dalam kedua kasus tersebut, Anda dapat menggunakan Kebijakan Kontrol Layanan (SCP) untuk:

- Mencegah semua akun anggota membuat instance akun.
- Izinkan hanya akun anggota tertentu untuk membuat instance akun.

Mencegah instans akun

Gunakan prosedur berikut untuk membuat SCP yang mencegah akun anggota membuat instance akun Pusat Identitas IAM.

1. Buka konsol [Pusat Identitas IAM](#).
2. Di Dasbor, di bagian Manajemen pusat, pilih tombol Cegah instans akun.
3. Dalam 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. SCP adalah fitur dari AWS Organizations. Untuk petunjuk tentang melampirkan SCP, lihat [Melampirkan dan melepaskan kebijakan kontrol layanan](#) di Panduan AWS Organizations Pengguna.

Batasi instance akun

Alih-alih mencegah semua pembuatan instance akun, kebijakan ini menolak setiap upaya untuk membuat instance akun Pusat Identitas IAM untuk semua Akun AWS kecuali yang tercantum secara eksplisit di "**<ALLOWED-ACCOUNT-ID>**" placeholder.

Example: Kebijakan tolak untuk membatasi pembuatan instance akun

JSON

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

}

- Ganti ["**<ALLOWED-ACCOUNT-ID>**"] dengan Akun AWS ID aktual yang ingin Anda izinkan untuk membuat instance akun Pusat Identitas IAM.
- Anda dapat mencantumkan beberapa ID akun yang diizinkan dalam format array: ["**111122223333**", "**444455556666**"].
- Lampirkan kebijakan ini ke SCP organisasi Anda untuk menerapkan kontrol terpusat atas pembuatan instance akun Pusat Identitas IAM.

Untuk petunjuk tentang melampirkan SCP, lihat Mel [ampirkan dan melepaskan kebijakan kontrol layanan](#) di Panduan AWS Organizations Pengguna.

Menghapus instance Pusat Identitas IAM Anda

Ketika instance Pusat Identitas IAM dihapus, semua data dalam instance tersebut dihapus dan tidak dapat dipulihkan. Tabel berikut menjelaskan data apa yang dihapus berdasarkan jenis direktori yang dikonfigurasi di Pusat Identitas IAM.

Data apa yang akan dihapus	Direktori terhubung - AWS Managed Microsoft AD, Konektor AD, atau penyedia identitas eksternal	Toko identitas Pusat Identitas IAM	
Semua set izin yang telah Anda konfigurasi Akun AWS	☑Ya	☑Iya	
Semua aplikasi yang telah Anda konfigurasi di Pusat Identitas IAM	☑Ya	☑Iya	
Semua tugas pengguna yang telah Anda konfigurasi	☑Ya	☑Iya	

Data apa yang akan dihapus	Direktori terhubung - AWS Managed Microsoft AD, Konektor AD, atau penyedia identitas eksternal	Toko identitas Pusat Identitas IAM	
sikan Akun AWS dan aplikasi			
Semua pengguna dan grup di direktori atau toko	N/A	☑Ya	

Jika Anda mereplikasi instance Pusat Identitas IAM ke Wilayah tambahan, Anda harus menghapus Wilayah tersebut sebelum menghapus instans.

Gunakan prosedur berikut untuk menghapus instans Pusat Identitas IAM Anda.

Untuk menghapus instans Pusat Identitas IAM Anda

1. Buka konsol [Pusat Identi](#) tas IAM.
2. Pada panel navigasi kiri, pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Manajemen.
4. Di bagian konfigurasi Hapus Pusat Identitas IAM, pilih H apus.
5. Dalam dialog konfigurasi Hapus Pusat Identitas IAM, pilih setiap kotak centang untuk mengetahui bahwa Anda memahami bahwa data Anda akan dihapus. Ketik instance Pusat Identitas IAM Anda di kotak teks, lalu pilih Kon firmasi.

Aktifkan Pusat Identitas IAM

Ketika Anda mengaktifkan Pusat Identitas IAM, Anda memilih jenis AWS IAM Identity Center instans untuk diaktifkan. Instance layanan adalah penyebaran tunggal layanan dalam AWS lingkungan Anda. Ada dua jenis instans yang tersedia untuk Pusat Identitas IAM: instans organisasi dan instans akun. Jenis instans yang tersedia untuk Anda aktifkan tergantung pada jenis akun yang Anda masuki.

Daftar berikut mengidentifikasi jenis instance Pusat Identitas IAM yang dapat Anda aktifkan untuk setiap jenis: Akun AWS

- Akun AWS Organizations manajemen Anda (disarankan) — Diperlukan untuk membuat instance [organisasi](#) dari Pusat Identitas IAM. Gunakan instance organisasi untuk izin multi-akun dan penugasan aplikasi di seluruh organisasi. Anda dapat mereplikasi jenis instans ini ke Wilayah tambahan untuk meningkatkan ketahanan akses akun dan fleksibilitas dalam memilih Wilayah pener AWS apa aplikasi.
- Akun AWS Organizations anggota Anda — Digunakan untuk membuat instance [akun Pusat Identitas IAM](#) untuk mengaktifkan penugasan aplikasi dalam akun anggota tersebut. Satu atau lebih akun dengan instance tingkat anggota dapat ada di organisasi.
- Mandiri Akun AWS — Digunakan untuk membuat instance [organisasi](#) atau instance [??? akun](#) Pusat Identitas IAM. Mandiri Akun AWS tidak dikelola oleh AWS Organizations. Anda hanya dapat mengaitkan satu instance Pusat Identitas IAM dengan mandiri Akun AWS dan menggunakan instance tersebut untuk penugasan aplikasi dalam mandiri Akun AWS itu.

Important

Akun manajemen organisasi dapat mengontrol apakah akun anggota [organisasi dapat membuat instance akun Pusat Identitas IAM](#) dengan menggunakan Kebijakan Kontrol Layanan.

Jika Anda menggunakan akun tingkat gratis, membuat AWS organisasi secara otomatis meningkatkan akun Anda ke paket berbayar dengan harga bayar sesuai penggunaan. Kredit tingkat gratis Anda segera kedaluwarsa. Untuk informasi selengkapnya, lihat [FAQ Tingkat AWS Gratis](#).

Untuk perbandingan kemampuan berbeda yang disediakan oleh jenis instans yang berbeda, lihat [Instans organisasi dan akun dari Pusat Identitas IAM](#).

Sebelum mengaktifkan Pusat Identitas IAM, kami sarankan Anda meninjaunya. [Prasyarat dan pertimbangan IAM Identity Center](#)

Untuk mengaktifkan instance Pusat Identitas IAM

Pilih tab untuk jenis instance Pusat Identitas IAM yang ingin Anda aktifkan, baik instans organisasi atau akun:

Organization (recommended)

1. Lakukan salah satu hal berikut untuk masuk ke Konsol Manajemen AWS.
 - Baru untuk AWS (pengguna root) - Masuk sebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.
 - Sudah menggunakan AWS dengan mandiri Akun AWS (kredenSIAL IAM) - Masuk menggunakan kredenSIAL IAM Anda dengan izin administratif.
 - Sudah menggunakan AWS Organizations (kredenSIAL IAM) - Masuk menggunakan kredenSIAL akun manajemen Anda.
2. Buka konsol [Pusat Identi](#) tas IAM.
3. Langkah ini hanya berlaku untuk [Wilayah AWS yang diaktifkan secara default](#). Jika Anda mengaktifkan Pusat Identitas IAM di Wilayah lain, lewati ke Langkah 4.

Di bawah Konfigurasi instans, pilih salah satu opsi berikut:

- Single-Region instance — Instans Anda dibuat di Wilayah saat ini.
- Multi-Region instance — Instans Anda dibuat di Wilayah saat ini dan direplikasi ke Wilayah tambahan untuk akses tangguh Akun AWS dan aplikasi. Kunci KMS Multi-wilayah yang dikelola pelanggan dibuat secara otomatis untuk mendukung Multi-wilayah. AWS KMS dikenakan biaya.
- Instans kustom — Konfigurasikan setelan instans Anda secara individual.

Untuk informasi selengkapnya tentang setiap opsi, lihat [Opsi konfigurasi instans](#).

Pilih **Aktif** kan untuk membuat instance Anda.

4. (Opsional) Jika Anda ingin menggunakan kunci KMS yang dikelola pelanggan untuk enkripsi saat diam daripada kunci terkel AWS ola default, konfigurasi kunci yang dikelola

pelanggan di bagian Kunci untuk mengenkripsi data Pusat Identitas IAM saat istirahat. Untuk informasi lebih lanjut, lihat [Menerapkan kunci KMS yang dikelola pelanggan di AWS IAM Identity Center](#).

 Important

Lakukan langkah ini hanya jika Anda telah mengonfigurasi izin yang diperlukan untuk penggunaan kunci yang dikelola pelanggan KMS. Tanpa izin yang tepat, langkah ini dapat gagal atau mengganggu administrasi Pusat Identitas IAM dan aplikasi yang AWS dikelola.

5. (Opsional) Secara default, instans Anda memiliki izin multi-akun yang diaktifkan. Jika Anda berencana menggunakan Pusat Identitas IAM hanya untuk otentikasi aplikasi dan manajemen pengguna, matikan sakelar Aktifkan izin multi-akun.

Jika Anda memilih untuk tidak mengaktifkan izin multi-akun sekarang, Akun AWS bagian tersebut tidak muncul di konsol Pusat Identitas IAM. Pusat Identitas IAM tidak menerapkan peran terkait layanan ke akun anggota. Anda dapat mengaktifkan izin multi-akun nanti dari tab Manajemen pada halaman Pengaturan.

6. Di bawah Aktifkan Pusat Identitas IAM, pilih Aktifkan.
 - Jika Anda masuk ke akun manajemen organisasi yang ada, Pusat Identitas IAM mulai mengaktifkan. Lanjutkan untuk mengatur lingkungan Anda.
 - Jika Anda memiliki mandiri Akun AWS (bukan bagian dari organisasi), Anda akan melihat AWS Organizations halaman Aktifkan Pusat Identitas IAM dengan. Opsi ini membuat organisasi baru dengan akun Anda sebagai akun manajemen. Tinjau informasi dan pilih Aktifkan untuk menyelesaikan proses.

 Note

AWS Organizations dapat mengaktifkan Pusat Identitas IAM hanya di satu Wilayah AWS. Setelah mengaktifkan Pusat Identitas IAM, jika Anda perlu mengubah Wilayah tempat Pusat Identitas IAM diaktifkan, Anda harus [menghapus](#) instans saat ini dan membuat instance di Wilayah lainnya.

 Tip

Jika Anda memiliki akun mandiri dan ingin membuat instance akun alih-alih instance organisasi, lihat tab Akun.

Setelah mengaktifkan instance organisasi Anda, kami sarankan Anda melakukan langkah-langkah berikut untuk menyelesaikan pengaturan lingkungan Anda:

- Konfirmasikan bahwa Anda menggunakan sumber identitas pilihan Anda. Jika Anda sudah memiliki sumber identitas yang ditetapkan, Anda dapat terus menggunakannya. Untuk informasi selengkapnya, lihat [Konfirmasikan sumber identitas Anda di Pusat Identitas IAM](#).
- Daftarkan akun anggota sebagai administrator yang didelegasikan. Untuk informasi selengkapnya, lihat [Administrator yang didelegasikan](#).
- IAM Identity Center memberi Anda portal akses ke AWS sumber daya. 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 Gateway (SWG), lihat [Perbarui firewall dan gateway untuk memungkinkan akses ke Portal akses AWS](#)

Account

1. Lakukan salah satu hal berikut untuk masuk ke Konsol Manajemen AWS.
 - Baru untuk AWS (pengguna root) - Masuk sebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.
 - Sudah menggunakan AWS (kredenSIAL IAM) - Masuk menggunakan kredenSIAL IAM Anda dengan izin administratif.
 - Sudah menggunakan AWS Organizations (kredenSIAL IAM) - Masuk menggunakan kredenSIAL administratif akun anggota Anda.
2. Buka konsol [Pusat Identitas IAM](#).
3. Jika Anda baru menggunakan AWS atau memiliki aplikasi mandiri Akun AWS, di bawah Aktifkan Pusat Identitas IAM, pilih Aktifkan.

Anda melihat AWS Organizations halaman **Aktifkan Pusat Identitas IAM** dengan. Ini membuat instance organisasi, yang kami rekomendasikan. Namun, jika Anda lebih memilih instance akun sebagai gantinya, pilih tautan **mengaktifkan instance akun Pusat Identitas IAM**.

4. Jika Anda adalah administrator akun AWS Organizations anggota, di bawah **Aktifkan instance akun Pusat Identitas IAM**, pilih **Aktifkan instance akun**.
5. Pada halaman **Aktifkan instance akun Pusat Identitas IAM**, tinjau informasi dan secara opsional tambahkan tag yang ingin Anda kaitkan dengan instance akun ini. Kemudian pilih **Aktifkan** untuk menyelesaikan proses.

 Note

Jika AWS akun Anda adalah anggota organisasi, mungkin ada batasan pada kemampuan Anda untuk mengaktifkan instance akun Pusat Identitas IAM.

- Jika organisasi Anda mengaktifkan Pusat Identitas IAM sebelum 15 November 2023, kemampuan akun anggota untuk membuat instans akun dinonaktifkan secara default dan harus diaktifkan oleh akun manajemen organisasi.
- Jika organisasi Anda mengaktifkan Pusat Identitas IAM setelah 15 November 2023, kemampuan akun anggota untuk membuat instans akun diaktifkan secara default. Namun, kebijakan kontrol layanan dapat digunakan untuk mencegah pembuatan instance akun Pusat Identitas IAM dalam organisasi.

Lihat informasi yang lebih lengkap di [the section called “Izinkan pembuatan instance akun di akun anggota”](#) dan [the section called “SCP untuk pembuatan instance akun”](#).

Konfirmasikan sumber identitas Anda di Pusat Identitas IAM

Sumber identitas Anda di Pusat Identitas IAM menentukan di mana pengguna dan grup Anda dikelola. Setelah mengaktifkan Pusat Identitas IAM, konfirmasikan bahwa Anda menggunakan sumber identitas pilihan Anda. Jika Anda sudah memiliki sumber identitas yang ditetapkan, Anda dapat terus menggunakannya.

Jika Anda sudah mengelola pengguna dan grup di Active Directory atau IdP eksternal, sebaiknya pertimbangkan 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 penugasan pengguna dan grup yang Anda konfigurasi di Pusat Identitas IAM. Jika ini terjadi, semua pengguna, termasuk pengguna administratif di Pusat Identitas IAM, akan kehilangan akses masuk tunggal ke aplikasi mereka Akun AWS . Untuk informasi selengkapnya, lihat [Pertimbangan untuk mengubah sumber identitas Anda](#).

Untuk mengonfirmasi sumber identitas Anda

1. Buka konsol [Pusat Identitas](#) IAM.
2. Pada halaman Dasbor, di bawah bagian Langkah pengaturan yang disarankan, pilih Konfirmasikan sumber identitas Anda. 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 Identity Center

Saat Anda mengaktifkan Pusat Identitas IAM untuk pertama kalinya, itu secara otomatis dikonfigurasi dengan direktori Identity Center 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 Anda Akun AWS . Untuk tutorial menggunakan sumber identitas ini, lihat [Konfigurasi akses pengguna dengan direktori IAM Identity Center default](#).

Active Directory

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

penyimpanan identitas Pusat Identitas IAM. Untuk informasi selengkapnya, lihat [Microsoft AD direktori](#).

 Note

Pusat Identitas IAM tidak mendukung Sim SAMBA4-based ple AD sebagai sumber identitas.

Penyedia identitas eksternal

Untuk penyedia identitas eksternal (IdPs) seperti Okta atau Microsoft Entra ID, Anda dapat menggunakan Pusat Identitas IAM untuk mengotentikasi identitas dari IdPs melalui standar Security Assertion Markup Language (SAML) 2.0. Protokol SAML tidak menyediakan cara untuk menanyakan IdP untuk mempelajari tentang pengguna dan grup. Anda membuat Pusat Identitas IAM mengetahui pengguna dan grup tersebut dengan menyediakan mereka 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 cara menyiapkan sumber identitas Anda, lihat [Tutorial sumber identitas Pusat Identitas IAM](#).

 Note

Jika Anda berencana menggunakan penyedia identitas eksternal, perhatikan bahwa IdP eksternal, bukan Pusat Identitas IAM, mengelola setelan otentikasi multi-faktor (MFA). MFA di Pusat Identitas IAM tidak didukung untuk digunakan oleh penyedia identitas eksternal. Untuk informasi selengkapnya, lihat [Meminta pengguna untuk MFA](#).

 Note

Jika Anda berencana untuk mereplikasi Pusat Identitas IAM ke Wilayah tambahan, Anda harus menggunakan penyedia identitas eksternal atau direktori Pusat Identitas sebagai sumber identitas Anda. Multi-Region dukungan tidak tersedia untuk Active Directory. Untuk

detail lebih lanjut termasuk prasyarat, lihat [Menggunakan Pusat Identitas IAM di beberapa Wilayah AWS](#).

Perbarui firewall dan gateway untuk memungkinkan akses ke Portal akses AWS

Portal AWS akses memberi pengguna 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.

Note

AWS aplikasi terkelola terintegrasi dengan Pusat Identitas IAM dan menggunakannya untuk otentikasi dan layanan direktori, tetapi mungkin tidak menggunakan portal AWS akses untuk akses aplikasi.

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 Gateway (SWG), Anda harus mengizinkan daftar domain dan titik akhir URL yang terkait dengan portal akses. AWS

Daftar berikut menyediakan domain IPv4 dan dual-stack serta titik akhir URL untuk ditambahkan ke daftar izin solusi pemfilteran konten web Anda.

Daftar izin IPv4

- *[Directory ID or alias].awsapps.com*
- *[Identity Center instance ID].[Region].portal.amazonaws.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]*.prod.pr.panorama.console.api.aws/panoramamaroute
- *[Region]*.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com

Dual-stack Izinkan daftar

- *[Identity Center instance ID]*.portal.*[Region]*.app.aws
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.api.aws
- sso.*[Region]*.api.aws
- portal.sso.*[Region]*.api.aws
- *[Region]*.sso.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- cdn.us-east-1.threat-mitigation.aws.amazon.com
- us-east-1.threat-mitigation.aws.amazon.com
- amcs-captcha-prod-us-east-1.s3.dualstack.us-east-1.amazonaws.com

Daftar izin gabungan (IPv4+ Dual-stack dengan kompatibilitas mundur)

- *[Directory ID or alias]*.awsapps.com
- *[Identity Center instance ID]*.*[Region]*.portal.amazonaws.com
- *[Identity Centers instance ID]*.portal.*[Region]*.app.aws

- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.[Region].amazonaws.com
- oidc.[Region].api.aws
- *.sso.amazonaws.com
- *.sso.[Region].amazonaws.com
- sso.[Region].api.aws
- *.sso-portal.[Region].amazonaws.com
- portal.sso.[Region].api.aws
- [Region].prod.pr.panorama.console.api.aws/panoramamaroute
- [Region].signin.aws
- [Region].sso.signin.aws
- [Region].signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com
- cdn.us-east-1.threat-mitigation.aws.amazon.com
- us-east-1.threat-mitigation.aws.amazon.com
- amcs-captcha-prod-us-east-1.s3.dualstack.us-east-1.amazonaws.com

Pertimbangan untuk mendaftarkan domain dan titik akhir URL yang diizinkan

Selain persyaratan allowlist untuk portal AWS akses, layanan dan aplikasi lain yang Anda gunakan mungkin memerlukan daftar domain yang diizinkan.

- Untuk mengakses Akun AWS Konsol Manajemen AWS, dan konsol Pusat Identitas IAM dari portal AWS akses Anda, Anda harus mengizinkan daftar domain tambahan. Lihat [Pemecahan Masalah Konsol Manajemen AWS](#) di Panduan Memulai untuk daftar Konsol Manajemen AWS domain.
- Untuk mengakses aplikasi AWS terkelola dari portal AWS akses Anda, Anda harus mengizinkan daftar domain masing-masing. Lihat dokumentasi layanan masing-masing untuk panduan.

- Jika Anda menggunakan perangkat lunak eksternal, seperti eksternal IdPs (misalnya, Okta dan Microsoft Entra ID), Anda harus menyertakan domain mereka dalam daftar izin Anda.

Tutorial sumber identitas Pusat Identitas IAM

Anda dapat menghubungkan sumber identitas yang ada di akun AWS Organizations manajemen Anda ke [instans organisasi Pusat Identitas IAM](#). Jika Anda tidak memiliki penyedia identitas yang ada, Anda dapat membuat dan mengelola pengguna secara langsung di direktori Pusat Identitas IAM default. Anda dapat memiliki satu sumber identitas per organisasi.

Tutorial di bagian ini menjelaskan cara mengatur instance organisasi IAM Identity Center dengan sumber identitas yang umum digunakan, membuat pengguna administratif, dan jika Anda menggunakan IAM Identity Center untuk mengelola akses ke Akun AWS, membuat dan mengkonfigurasi set izin. Jika Anda menggunakan IAM Identity Center untuk akses aplikasi saja, Anda tidak perlu menggunakan set izin.

Tutorial ini tidak menjelaskan cara mengatur instance akun IAM Identity Center. Anda dapat menggunakan instans akun untuk menetapkan pengguna dan grup ke aplikasi, tetapi Anda tidak dapat menggunakan jenis instans ini untuk mengelola akses pengguna. Akun AWS Untuk informasi selengkapnya, lihat [Instans akun Pusat Identitas IAM](#).

Note

Sebelum memulai salah satu tutorial ini, aktifkan IAM Identity Center. Untuk informasi selengkapnya, lihat [Aktifkan Pusat Identitas IAM](#).

Topik

- [Menggunakan Active Directory sebagai sumber identitas](#)
- [Setting up SCIM provisioning between CyberArk and IAM Identity Center](#)
- [Konfigurasi SAML dan SCIM dengan Google Workspace dan Pusat Identitas IAM](#)
- [Menggunakan IAM Identity Center untuk terhubung dengan Platform JumpCloud Direktori](#)
- [Konfigurasi SAML dan SCIM dengan Microsoft Entry ID dan Pusat Identitas IAM](#)
- [Konfigurasi SAML dan SCIM dengan Okta dan Pusat Identitas IAM](#)
- [Menyiapkan penyedia SCIM antara OneLogin dan IAM Identity Center](#)
- [Menggunakan Ping Identity produk dengan IAM Identity Center](#)
- [Konfigurasi akses pengguna dengan direktori IAM Identity Center default](#)
- [Tutorial video](#)

Menggunakan Active Directory sebagai sumber identitas

Jika Anda mengelola pengguna di AWS Managed Microsoft AD direktori menggunakan 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 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. Untuk informasi lebih lanjut, lihat:

- [Connect direktori di AWS Managed Microsoft AD ke Pusat Identitas IAM](#)
- [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 untuk menghubungkan direktori Anda ke IAM Identity Center.

Note

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 di [Microsoft AD direktori](#).
2. Ikuti langkah-langkah di [Connect direktori di AWS Managed Microsoft AD ke Pusat Identitas IAM](#).
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 di [Microsoft AD direktori](#).
2. Ikuti langkah-langkah 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. Lihat informasi yang lebih lengkap di [Membuat kumpulan 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. Untuk informasi selengkapnya, lihat [Menggunakan federasi identitas SAMP dan SCIM dengan penyedia identitas eksternal](#).

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](#)
- [Pertimbangan SCIM](#)
- [Langkah 1: Aktifkan penyediaan di IAM Identity Center](#)
- [Langkah 2: Konfigurasi penyediaan di CyberArk](#)
- [\(Opsional\) Langkah 3: Konfigurasi atribut pengguna CyberArk untuk kontrol akses \(ABAC\) di Pusat Identitas IAM](#)
- [\(Opsional\) Melewati atribut untuk kontrol akses](#)

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 [CyberArk dokumentasi 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. Di kotak dialog Inbound automatic provisioning, salin endpoint SCIM dan token akses. Anda harus menempelkannya nanti saat mengonfigurasi penyediaan di iDP Anda.
 - a. Titik akhir SCIM - Misalnya, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
 - b. Access token - Pilih Tampilkan token untuk menyalin nilainya.

Warning

Ini adalah satu-satunya waktu di mana Anda dapat memperoleh titik akhir SCIM dan token akses. Pastikan Anda menyalin nilai-nilai ini sebelum bergerak maju. Anda akan

memasukkan nilai-nilai ini untuk mengkonfigurasi penyediaan otomatis di IDP Anda nanti dalam tutorial ini.

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, lihat [Prasyarat](#), 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.
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: Konfigurasi 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 [Mengaktifkan dan mengonfigurasi 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 dari CyberArk.
 - 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 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 `tagCostCenter = 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.

Konfigurasi SAML dan SCIM dengan Google Workspace dan Pusat Identitas IAM

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

Note

Google Workspacesaat ini tidak mendukung URL SAML multiple assertion konsumsi service (ACS) dalam aplikasi. AWS IAM Identity Center Fitur SAML ini diperlukan untuk sepenuhnya memanfaatkan dukungan [Multi-wilayah](#) di Pusat Identitas IAM. Jika Anda berencana untuk mereplikasi Pusat Identitas IAM ke Wilayah tambahan, ketahuilah bahwa menggunakan URL ACS tunggal dapat memengaruhi pengalaman pengguna di Wilayah tambahan tersebut. Wilayah utama Anda akan terus berfungsi secara normal. Kami menyarankan Anda bekerja dengan vendor IdP Anda untuk mengaktifkan fitur ini. Untuk informasi selengkapnya tentang pengalaman pengguna di Wilayah tambahan dengan URL ACS tunggal, lihat [the section called “Penggunaan AWS aplikasi yang dikelola tanpa beberapa URL ACS”](#) dan [the section called “Akun AWS akses ketahanan tanpa beberapa URL ACS”](#).

Informasi pengguna dari Google Workspace disinkronkan ke Pusat Identitas IAM menggunakan protokol [System for Cross-domain Identity Management \(SCIM\) 2.0](#). Untuk informasi selengkapnya, lihat [Menggunakan federasi identitas SAMP dan SCIM dengan penyedia identitas eksternal](#).

Anda mengonfigurasi koneksi ini dengan Google Workspace menggunakan titik akhir SCIM Anda untuk Pusat Identitas IAM 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 Pusat Identitas IAM dan Google Workspace. Untuk melakukan ini, Anda perlu mengatur Google Workspace sebagai penyedia identitas dan terhubung dengan Pusat Identitas IAM Anda.

Tujuan

Langkah-langkah dalam tutorial ini membantu memandu Anda melalui membangun koneksi SAML antara Google Workspace dan AWS. Nantinya, 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 dalam tutorial ini. Setelah menyelesaikan tutorial ini, pengguna Anda akan dapat mengakses portal AWS akses dengan Google Workspace kredensial Anda.

Note

Untuk mendaftar uji coba gratis, Google Workspace kunjungi [Google Workspace](#) situs Google's web.

Jika Anda belum mengaktifkan Pusat Identitas IAM, lihat [Aktifkan Pusat Identitas IAM](#).

Pertimbangan-pertimbangan

- Sebelum mengonfigurasi penyediaan SCIM antara Google Workspace dan Pusat Identitas IAM, sebaiknya tinjau terlebih dahulu. [Pertimbangan untuk menggunakan penyediaan otomatis](#)
- Sinkronisasi otomatis SCIM dari saat Google Workspace ini terbatas pada penyediaan pengguna. Penyediaan grup otomatis tidak didukung saat ini. Grup dapat dibuat secara manual dengan [perintah](#) Create-group AWS CLI Identity Store atau AWS Identity and Access Management (IAM) API. [CreateGroup](#) Atau, Anda dapat menggunakan [ssosync](#) untuk menyinkronkan Google Workspace pengguna dan grup ke Pusat Identitas IAM.

- Setiap Google Workspace pengguna harus memiliki nama depan, nama belakang, nama pengguna dan nilai 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 beberapa 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.
- 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 diganti dan disinkronkan menggunakan SCIM from. Google Workspace
- Ada pertimbangan tambahan saat mengubah sumber identitas Anda. Untuk informasi selengkapnya, lihat [the section called “Mengubah dari Pusat Identitas IAM ke IdP eksternal”](#).

Langkah 1: Google Workspace: Konfigurasi aplikasi SAML

1. Masuk ke konsol Google Admin menggunakan akun dengan hak administrator super.
2. Di panel navigasi kiri konsol Google Admin Anda, pilih Aplikasi dan kemudian pilih Aplikasi Web dan Seluler.
3. Di daftar tar ik- turun Tambah aplikasi, pilih Cari aplikasi.
4. Di kotak pencarian masukkan Amazon Web Services, lalu pilih aplikasi Amazon Web Services (SAML) dari daftar.
5. Pada halaman Google Detail Penyedia Identitas - Amazon Web Services, Anda dapat melakukan salah satu dari hal berikut:
 - a. Unduh metadata IdP.
 - b. Salin URL SSO, URL ID Entitas, dan informasi Sertifikat.

Anda akan memerlukan file XML atau informasi URL di Langkah 2.

6. Sebelum pindah ke langkah berikutnya di konsol Google Admin, biarkan halaman ini terbuka dan pindah ke konsol Pusat Identitas IAM.

Langkah 2: Pusat Identitas IAM dan Google Workspace: Mengubah sumber dan pengaturan identitas Pusat Identitas IAM Google Workspace sebagai penyedia identitas SAML

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.
 - Jika Anda belum mengaktifkan Pusat Identitas IAM, lihat [Aktifkan Pusat Identitas IAM](#) untuk informasi selengkapnya. Setelah mengaktifkan dan mengakses Pusat Identitas IAM untuk pertama kalinya, Anda akan tiba di Dashboard di mana Anda dapat memilih Pilih sumber identitas Anda.
4. Pada halaman Pilih sumber identitas, pilih Penyedia identitas eksternal, lalu pilih Berikutnya.
5. Halaman Konfigurasi penyedia identitas eksternal terbuka. Untuk menyelesaikan halaman ini dan Google Workspace halaman di Langkah 1, Anda harus menyelesaikan hal berikut:
 - Di bawah bagian metadata Penyedia Identitas di konsol Pusat Identitas IAM, Anda perlu melakukan salah satu dari hal berikut:
 - i. Unggah metadata Google SAML sebagai metadata IdP SAML di konsol Pusat Identitas IAM.
 - ii. Salin dan tempel URL Google SSO ke bidang URL IdP, Sign-in URL Penerbit ke bidang URL Google penerbit IdP, dan unggah Google Sertifikat sebagai sertifikat IdP.
6. Setelah memberikan Google metadata di bagian metadata Penyedia Identitas pada konsol Pusat Identitas IAM, di bawah Metadata penyedia layanan, pilih Default IPv4 atau Dual-stack. Jika Anda menyesuaikan URL portal AWS akses Anda, pilih Default IPv4. Salin URL Layanan Konsumen Penegakan Identitas IAM (ACS) dan URL penerbit Pusat Identitas IAM. Anda memerlukan URL ini untuk menyelesaikan konfigurasi konsol Google Admin di langkah berikutnya. Untuk informasi selengkapnya tentang URL ACS, lihat [Titik akhir ACS di primer dan tambahan Wilayah AWS](#).
7. Biarkan halaman terbuka dengan konsol IAM Identity Center dan kembali ke konsol Google Admin. Anda harus berada di halaman detail Amazon Web Services - Service Provider. Pilih Lanjutkan.

8. Pada halaman detail penyedia layanan, masukkan nilai URL ACS dan ID Entity. Anda menyalin nilai-nilai ini di langkah sebelumnya dan nilai-nilai tersebut dapat ditemukan di konsol Pusat Identitas IAM.
 - Tempelkan URL IAM Identity Center Assertion Consumer Service (ACS) ke bidang URL ACS
 - Tempelkan URL penerbit Pusat Identitas IAM ke bidang ID Entitas.
9. Pada 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
10. Pilih Lanjutkan.
11. Pada halaman Pemetaan Atribut, di bawah Atribut, pilih TAMBAH PEMETAAN, lalu konfigurasi bidang ini di bawah Atribut Google Direktori:
 - Untuk atribut `https://aws.amazon.com/SAML/Attributes/RoleSessionName` aplikasi, pilih bidang Informasi Dasar, Email Utama dari Google Directory atribut.
 - Untuk atribut `https://aws.amazon.com/SAML/Attributes/Role` aplikasi, pilih Google Directory atribut apa saja. Atribut Google Direktori bisa menjadi Departemen.
12. Pilih Selanjutnya
13. Kembali ke konsol Pusat Identitas IAM dan pilih Berikutnya. Pada halaman Tinjau dan Konfirmasi, tinjau informasi dan kemudian masukkan ACCEPT ke dalam ruang yang disediakan. Pilih Ubah sumber identitas.

Anda sekarang siap untuk mengaktifkan aplikasi Amazon Web Services Google Workspace sehingga pengguna Anda dapat disediakan ke Pusat Identitas IAM.

Langkah 3: Google Workspace: Aktifkan aplikasi

1. Kembali ke Konsol Google Admin dan AWS IAM Identity Center aplikasi Anda yang dapat ditemukan di bawah Aplikasi dan Aplikasi Web dan Seluler.
2. Di panel Akses pengguna di sebelah Akses pengguna, pilih panah bawah untuk memperluas Akses pengguna untuk menampilkan panel status Layanan.
3. Di panel status layanan, pilih AKTIF untuk semua orang, lalu pilih SIMPAN.

 Note

Untuk membantu mempertahankan prinsip hak istimewa terkecil, kami sarankan bahwa setelah Anda menyelesaikan tutorial ini, Anda mengubah status Layanan menjadi OFF untuk semua orang. Hanya pengguna yang memerlukan 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 4: Pusat Identitas IAM: Siapkan penyediaan otomatis Pusat Identitas IAM

1. Kembali ke konsol Pusat Identitas IAM.
2. Pada halaman Pengaturan, cari kotak informasi penyediaan otomatis, lalu pilih Aktifkan. Ini segera memungkinkan penyediaan otomatis di Pusat Identitas IAM dan menampilkan titik akhir SCIM yang diperlukan dan informasi token akses.
3. Di kotak dialog Penyediaan otomatis masuk, salin setiap nilai untuk opsi berikut. Pada Langkah 5 dari tutorial ini, Anda akan memasukkan nilai-nilai ini untuk mengkonfigurasi penyediaan Google Workspace otomatis.
 - a. Titik akhir SCIM - Misalnya,
 - IPv4 `https://scim.Region.amazonaws.com/1111111111-2222-3333-4444-555555555555/scim/v2`
 - Dual-stack `https://scim.Region.api.aws/1111111111-2222-3333-4444-555555555555/scim/v2`
 - b. Token akses - Pilih Tampilkan token untuk menyalin nilainya.

 Warning

Ini adalah satu-satunya waktu di mana Anda dapat memperoleh titik akhir SCIM dan token akses. Pastikan Anda menyalin nilai-nilai ini sebelum bergerak maju.

4. Pilih Tutup.

Sekarang setelah Anda mengatur penyedia di konsol IAM Identity Center, pada langkah berikutnya Anda akan mengonfigurasi penyedia otomatis di Google Workspace

Langkah 5: Google Workspace: Konfigurasi penyedia otomatis

1. Kembali ke konsol Google Admin dan AWS IAM Identity Center aplikasi Anda yang dapat ditemukan di bawah Aplikasi dan Aplikasi Web dan Seluler. Di bagian Penyediaan otomatis, pilih Konfigurasi penyedia otomatis.
2. Pada prosedur sebelumnya, Anda menyalin nilai token Akses di konsol Pusat Identitas IAM. Tempelkan nilai itu ke bidang token Akses dan pilih Lanjutkan. Juga, dalam prosedur sebelumnya, Anda menyalin nilai titik akhir SCIM di konsol Pusat Identitas IAM. Tempelkan nilai itu ke bidang URL Endpoint dan pilih Lanjutkan.
3. 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.
4. Di bagian Cakupan penyedia, Anda dapat memilih grup dengan Google Workspace direktori Anda untuk menyediakan akses ke aplikasi Amazon Web Services. Lewati langkah ini dan pilih Lanjutkan.
5. Di bagian Deprovisioning, Anda dapat memilih cara merespons berbagai peristiwa yang menghapus akses dari pengguna. Untuk setiap situasi, Anda dapat menentukan jumlah waktu sebelum deprovisioning dimulai:
 - dalam waktu 24 jam
 - setelah satu hari
 - setelah tujuh hari
 - setelah 30 hari

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

Tip

Selalu tetapkan lebih banyak waktu sebelum menghapus akun pengguna daripada untuk menangguhkan akun pengguna.

6. Pilih Selesai. Anda dikembalikan ke halaman aplikasi Amazon Web Services.
7. Di Auto-provisioning bagian ini, nyalakan sakelar sakelar untuk mengubahnya dari Tidak Aktif ke Aktif.

Note

Penggeser aktivasi dinonaktifkan jika Pusat Identitas IAM tidak diaktifkan untuk pengguna. Pilih Akses pengguna dan nyalakan aplikasi untuk mengaktifkan slider.

8. Di kotak dialog konfirmasi, pilih Aktifkan.
9. 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 harus sesuai dengan informasi di Google Workspace direktori.

Selamat!

Anda telah berhasil mengatur koneksi SAML antara Google Workspace dan AWS dan telah memverifikasi bahwa penyediaan otomatis berfungsi. Anda sekarang dapat menetapkan pengguna ini ke akun dan aplikasi di Pusat Identitas IAM. Untuk tutorial ini, pada langkah selanjutnya mari kita tunjuk salah satu pengguna sebagai administrator Pusat Identitas IAM dengan memberi mereka izin administratif ke akun manajemen.

Melewati atribut untuk kontrol akses - Opsional

Anda dapat secara opsional menggunakan [Atribut untuk kontrol akses](#) fitur di Pusat Identitas IAM untuk meneruskan Attribute elemen dengan Name atribut 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 Meneruskan 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 `tagCostCenter = 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.

Tetapkan akses ke Akun AWS

Langkah-langkah berikut hanya diperlukan untuk memberikan akses ke Akun AWS saja. Langkah-langkah ini tidak diperlukan untuk memberikan akses ke AWS aplikasi.

Note

Untuk menyelesaikan langkah ini, Anda memerlukan instance Organisasi dari Pusat Identitas IAM. Untuk informasi selengkapnya, lihat [Instans organisasi dan akun dari Pusat Identitas IAM](#).

Langkah 1: Pusat Identitas IAM: Hibah Google Workspace akses pengguna ke akun

1. Kembali ke konsol Pusat Identitas IAM. Di panel navigasi Pusat Identitas IAM, di bawah `Multi-account izin`, pilih `Akun AWS`.
2. Pada Akun AWS halaman `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. Alur kerja `Tetapkan pengguna dan grup` ditampilkan. 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 kumpulan izin` pilih `Buat kumpulan izin` untuk membuka tab baru yang memandu Anda melalui tiga sub-langkah yang terlibat dalam membuat kumpulan izin.

- i. Untuk Langkah 1: Pilih jenis kumpulan izin, leng kapi yang berikut:
 - Di Jenis kumpulan izin, pilih Set izin yang telah ditentukan sebelumnya.
 - Di Kebijakan untuk kumpulan izin yang telah ditentukan sebelumnya, pilih `AdministratorAccess`.

Pilih Berikutnya.

- ii. Untuk Langkah 2: Tentukan detail kumpulan izin, pertahankan pengaturan default, dan pilih Ber ikutnya.

Pengaturan default membuat kumpulan izin bernama `AdministratorAccess` dengan durasi sesi disetel ke satu jam.

- iii. Untuk Langkah 3: Tinjau dan buat, verifikasi bahwa jenis kumpulan izin menggunakan kebijakan ter AWS kelola `AdministratorAccess`. Pilih Buat. Pada halaman Kumpulan izin muncul pemberitahuan yang memberi tahu Anda bahwa kumpulan izin telah dibuat. Anda dapat menutup tab ini di browser web Anda sekarang.
 - iv. Pada tab browser Tet apkan pengguna dan grup, Anda masih menggunakan Langkah 2: Pilih kumpulan izin tempat Anda memulai alur kerja buat kumpulan izin.
 - v. Di area Perizinan set, pilih tombol Refresh. Kum `AdministratorAccess` pulan izin yang Anda buat muncul dalam daftar. Pilih kotak centang untuk kumpulan izin tersebut, lalu pilih Ber ikutnya.
- c. Untuk Langkah 3: Tinjau dan kirimkan ulasan pengguna dan kumpulan izin yang dipilih, lalu pilih K irim.

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 Anda Akun AWS telah disediakan ulang dan kumpulan izin yang diperbarui diterapkan. Ketika pengguna masuk, mereka akan memiliki opsi untuk memilih `AdministratorAccess` peran.

 Note

Sinkronisasi otomatis SCIM dari Google Workspace hanya mendukung pengguna penyediaan. Penyediaan grup otomatis tidak didukung saat ini. Anda tidak

dapat membuat grup untuk Google Workspace pengguna menggunakan Konsol Manajemen AWS. Setelah menyediakan pengguna, Anda dapat membuat grup menggunakan [perintah](#) `Create- AWS CLI group Identity Store` atau IAM API [CreateGroup](#).

Langkah 2: Google Workspace: Konfirmasikan Google Workspace akses pengguna ke AWS sumber daya

1. Masuk untuk Google menggunakan akun pengguna uji. Untuk mempelajari cara menambahkan pengguna ke Google Workspace, lihat [Google Workspace dokumentasi](#).
2. Pilih ikon pel Google apps uncur (wafel).
3. Gulir ke bagian bawah daftar aplikasi tempat Google Workspace aplikasi khusus Anda berada. Aplikasi Amazon Web Services ditampilkan.
4. Pilih aplikasi Amazon Web Services. Anda masuk ke portal AWS akses dan dapat melihat Akun AWS ikon. 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 menunjukkan satu akun.
5. Pilih akun untuk menampilkan kumpulan izin yang tersedia bagi pengguna. Dalam tutorial ini Anda membuat kum AdministratorAccess pulan izin.
6. Di sebelah kumpulan izin terdapat tautan untuk jenis akses yang tersedia untuk kumpulan izin tersebut. Ketika Anda membuat kumpulan izin, Anda menentukan konsol manajemen dan akses terprogram diaktifkan, sehingga kedua opsi tersebut hadir. Pilih Konsol manajemen untuk membuka Konsol Manajemen AWS.
7. Pengguna masuk ke konsol.

Langkah selanjutnya

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

- Gunakan [perintah](#) `Create-group AWS CLI Identity Store` atau IAM API [CreateGroup](#) untuk membuat grup bagi pengguna Anda.

Grup berguna saat menetapkan akses ke Akun AWS dan aplikasi. Alih-alih menetapkan setiap pengguna secara individual, Anda memberikan izin ke grup. Kemudian, saat Anda menambahkan

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 kumpulan izin](#).

Kumpulan izin menentukan tingkat akses yang dimiliki pengguna dan grup ke Akun AWS.

Kumpulan izin disimpan di Pusat Identitas IAM dan dapat disediakan untuk satu atau lebih. Akun AWS Anda dapat menetapkan lebih dari satu set izin untuk pengguna.

Note

Sebagai administrator Pusat Identitas IAM, terkadang Anda perlu mengganti sertifikat IdP yang lebih lama dengan yang lebih baru. Misalnya, Anda mungkin perlu mengganti sertifikat IdP saat tanggal kedaluwarsa pada sertifikat mendekati. Proses penggantian sertifikat yang lebih lama dengan yang lebih baru disebut sebagai rotasi sertifikat. Pastikan untuk meninjau cara [mengelola sertifikat SAML](#) untuk Google Workspace.

Pemecahan masalah

Untuk pemecahan masalah SCIM dan SAML umum dengan Google Workspace, lihat bagian berikut:

- [Pengguna tertentu gagal melakukan sinkronisasi ke Pusat Identitas IAM dari penyedia SCIM eksternal](#)
- [Masalah mengenai isi pernyataan SAML yang dibuat oleh Pusat Identitas IAM](#)
- [Duplikat kesalahan pengguna atau grup saat menyediakan pengguna atau grup dengan penyedia identitas eksternal](#)
- Untuk pem Google Workspace echan masalah, lihat [Google Workspace dokumentasi](#).

Sumber daya berikut dapat membantu Anda memecahkan masalah saat Anda bekerja dengan AWS:

- [AWS re:Post](#)- Temukan FAQ dan tautan ke sumber daya lain untuk membantu Anda memecahkan masalah.
- [AWS Dukungan](#)- Dapatkan dukungan teknis

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 [Security Assertion Markup Language \(SAMP\) 2.0](#). Untuk informasi selengkapnya, lihat [Menggunakan federasi identitas SAMP dan SCIM dengan penyedia identitas eksternal](#).

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 dan JumpCloud.

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](#)
- [Pertimbangan SCIM](#)
- [Langkah 1: Aktifkan penyediaan di IAM Identity Center](#)
- [Langkah 2: Konfigurasikan penyediaan di JumpCloud](#)
- [\(Opsional\) Langkah 3: Konfigurasikan atribut pengguna JumpCloud untuk kontrol akses di Pusat Identitas IAM](#)
- [\(Opsional\) Melewati atribut untuk kontrol akses](#)

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](#).
- Jika Anda mereplikasi Pusat Identitas IAM ke Wilayah tambahan, Anda harus memperbarui konfigurasi penyedia identitas Anda untuk mengaktifkan akses ke aplikasi AWS terkelola dan Akun AWS dari Wilayah tersebut. Untuk detail selengkapnya, lihat [the section called “Langkah 3 \(hanya penyedia identitas eksternal\): Perbarui pengaturan IdP eksternal”](#). Lihat JumpCloud dokumentasi untuk detail tambahan.
- 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.

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. Di kotak dialog Inbound automatic provisioning, salin endpoint SCIM dan token akses. Anda harus menempelkannya nanti saat mengonfigurasi penyediaan di iDP Anda.
 - a. Titik akhir SCIM - Misalnya, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
 - b. Access token - Pilih Tampilkan token untuk menyalin nilainya.

Warning

Ini adalah satu-satunya waktu di mana Anda dapat memperoleh titik akhir SCIM dan token akses. Pastikan Anda menyalin nilai-nilai ini sebelum bergerak maju. Anda akan memasukkan nilai-nilai ini untuk mengkonfigurasi penyediaan otomatis di IDP Anda nanti dalam tutorial ini.

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, lihat [Prasyarat](#), 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.
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 mengonfigurasi 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 `tagCostCenter = 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.

Konfigurasi SAML dan SCIM dengan Microsoft Entra ID dan Pusat Identitas IAM

AWS IAM Identity Center mendukung integrasi dengan [Security Assertion Markup Language \(SAML\) 2.0](#) serta penyediaan [otomatis](#) (sinkronisasi) informasi pengguna dan grup dari Microsoft Entra ID (sebelumnya dikenal sebagai Azure Active Directory atau Azure AD) ke IAM Identity Center menggunakan protokol [System for Cross-domain Identity Management \(SCIM\) 2.0](#). Untuk informasi selengkapnya, lihat [Menggunakan federasi identitas SAMP dan SCIM dengan penyedia identitas eksternal](#).

Tujuan

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

Microsoft Entra ID

Prasyarat

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

- Penye Microsoft Entra ID wa. Untuk informasi selengkapnya, lihat [Mulai Cepat: Menyiapkan penyewa](#) dalam Microsoft dokumentasi.
- Akun AWS IAM Identity Center yang diaktifkan. Untuk informasi selengkapnya, lihat [Mengaktifkan Pusat Identitas IAM](#) di Panduan AWS IAM Identity Center Pengguna.

Pertimbangan-pertimbangan

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

Penyediaan Otomatis

Sebelum Anda mulai menerapkan SCIM, sebaiknya tinjau 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 di Microsoft Entra ID, atribut tersebut tidak akan dihapus dari pengguna terkait di Pusat Identitas IAM. Ini adalah batasan yang diketahui di Microsoft 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 ditugaskan secara eksplisit yang dapat dibaca dan disediakan. Microsoft Entra ID tidak secara rekursif membongkar keanggotaan grup dari pengguna atau grup yang ditugaskan secara tidak langsung (pengguna atau grup yang merupakan anggota grup yang ditugaskan secara langsung). Untuk informasi selengkapnya, lihat [Assignment-based ingkupan](#) dalam Microsoft dokumentasi. Atau, Anda dapat menggunakan sinkronisasi AD yang dapat dikonfigurasi [IAM Identity Center](#) untuk mengintegrasikan Active Directory grup dengan Pusat Identitas IAM.

Grup Dinamis

Layanan penyediaan Microsoft Entra ID pengguna dapat membaca dan menyediakan pengguna dalam grup <https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-create-rule> 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 ke 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 ke Pusat Identitas IAM melalui SCIM, strukturnya akan menjadi 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 menyertakan 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 menyertakan anggota langsung grup A (yaitu, ua1). Itu tidak akan secara rekursif memasukkan anggota grup B.

- Grup dinamis tidak dapat berisi grup dinamis lainnya. Untuk informasi selengkapnya, lihat [Batasan pratinjau](#) dalam Microsoft dokumentasi.

Langkah 1: Siapkan penyewa Microsoft Anda

Pada langkah ini, Anda akan mempelajari cara menginstal dan mengkonfigurasi aplikasi AWS IAM Identity Center perusahaan Anda dan menetapkan akses ke pengguna Microsoft Entra ID pengujian 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 di Microsoft Entra ID. Anda akan memerlukan aplikasi ini nanti untuk mengkonfigurasi koneksi SAML Anda dengan AWS.

1. Masuk ke pusat admin [Microsoft Entra setidaknya](#) sebagai Administrator Aplikasi Cloud.
2. Arahkan ke Identitas > Aplikasi > Aplikasi perusahaan, lalu pilih Aplikasi baru.
3. Pada halaman Browse Microsoft Entra Gallery, masukkan **AWS IAM Identity Center** di kotak pencarian.
4. Pilih AWS IAM Identity Center dari 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 pengujian Anda yang akan Anda buat dalam prosedur ini.

1. Di [konsol tengah admin](#) Microsoft Entra, navigasikan ke Identitas > Pengguna > Semua pengguna.
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 Tinjauan + buat, lalu pilih Buat.

Step 1.3

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

Dalam prosedur ini, Anda akan memverifikasi apa yang Nikki berhasil masuk ke portal [Akun Saya](#) Microsoft miliknya.

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 Tindakan Diperlukan, pilih Tindakan nanti untuk melewati prompt untuk metode keamanan tambahan.
4. Pada halaman Akun saya, di panel navigasi kiri, pilih Aplikasi Saya. Perhatikan bahwa selain itu Add-ins, tidak ada aplikasi yang ditampilkan saat ini. Anda akan menambahkan AWS IAM Identity Center aplikasi 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 penggunaannya ke AWS IAM Identity Center aplikasi.

1. Di [konsol tengah admin](#) Microsoft Entra, navigasikan ke Identitas > Aplikasi > Aplikasi perusahaan dan kemudian pilih AWS IAM Identity Center dari daftar.
2. Di sebelah kiri, pilih Pengguna dan grup.
3. Pilih Tambahkan user/group. Anda dapat mengabaikan pesan yang menyatakan bahwa grup tidak tersedia untuk penugasan. Tutorial ini tidak menggunakan grup untuk tugas.
4. Pada halaman Tambah Tugas, di bawah Pengguna, pilih Tidak Ada yang Dipilih.
5. Pilih NikkiWolf, lalu pilih Pilih.
6. Pada halaman Tambah Tugas, pilih Tetapkan. NikkiWolf sekarang muncul dalam daftar pengguna yang ditugaskan ke AWS IAM Identity Center aplikasi.

Langkah 2: Persiapkan AWS akun

Pada langkah ini, Anda akan mempelajari cara menggunakan IAM Identity Center untuk mengonfigurasi izin akses (melalui kumpulan izin), secara manual membuat pengguna Nikki Wolf yang sesuai, dan menetapkan izin yang diperlukan untuk mengelola sumber daya di AWS.

Step 2.1 >

Langkah 2.1: Buat set RegionalAdmin izin di IAM Identity Center

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

1. Buka konsol [Pusat Identi](#) tas IAM.
2. Di bawah Multi-account izin, pilih Kumpulan izin.
3. Pilih Buat kumpulan izin.
4. Pada halaman Pilih jenis kumpulan izin, pilih Kumpulan izin khusus, lalu pilih Berikutnya.
5. Pilih Kebijakan sebaris untuk mengembangkannya, lalu buat kebijakan untuk kumpulan 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 Tambah sumber daya, di bawah Jenis sumber daya, pilih Semua Sumber Daya, lalu pilih Tambahkan sumber daya. Pastikan 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 kumpulan izin, di bawah Nama kumpulan izin, masukkan **RegionalAdmin**, lalu pilih Berikutnya.
8. Pada halaman Tinjau dan buat, pilih Buat. Anda akan melihat RegionalAdmin ditampilkan dalam daftar kumpulan izin.

Step 2.2 >

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

Karena protokol SAML tidak menyediakan mekanisme untuk menanyakan IdP (Microsoft Entra ID) dan secara otomatis membuat pengguna di sini di Pusat Identitas IAM, gunakan prosedur berikut untuk membuat pengguna secara manual di Pusat Identitas IAM yang mencerminkan atribut inti dari pengguna Nikki Wolfs di Microsoft Entra ID

1. Buka konsol [Pusat Identitas IAM](#).
2. Pilih Pengguna, pilih Tambah pengguna, lalu berikan informasi berikut:
 - a. Untuk Nama Pengguna dan Alamat Email — Masukkan **NikkiWolf** @ yang sama ***yourcompanydomain.extension*** yang Anda gunakan saat membuat Microsoft Entra ID pengguna Anda. Misalnya, NikkiWolf @***example.org***.
 - b. Konfirmasi alamat email — Re-enter alamat email dari langkah sebelumnya
 - c. Nama depan — Masukkan **Nikki**
 - d. Nama belakang — Masukkan **Wolf**
 - e. Nama tampilan — Masukkan **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 di IAM Identity Center

Di sini Anda menemukan Akun AWS tempat di mana Nikki akan mengelola Wilayah, dan kemudian menetapkan izin yang diperlukan baginya untuk berhasil mengakses portal AWS akses.

1. Buka konsol [Pusat Identitas](#) IAM.
2. Di bawah Multi-account izin, pilih Akun AWS.
3. Pilih kotak centang di sebelah nama akun (misalnya, *Sandbox*) tempat Anda ingin memberikan akses Nikki untuk mengelola Wilayah, lalu pilih Tetapkan pengguna dan grup.
4. Pada halaman Tetapkan pengguna dan grup, pilih tab Pengguna, cari dan centang kotak di sebelah Nikki, lalu pilih Berikutnya.

5. Example

<caption>On the Pilih kumpulan izin page, choose the RegionalAdmin permission set created in Step 2.1, and then choose Selanjutnya.</caption>

6. Pada halaman Tinjau dan kirim, tinjau pilihan Anda, lalu pilih Kirim.

Langkah 3: Konfigurasi dan uji koneksi SAML Anda

Pada langkah ini, Anda mengonfigurasi koneksi SAML menggunakan aplikasi AWS IAM Identity Center perusahaan Microsoft Entra ID bersama dengan pengaturan IdP eksternal di Pusat Identitas IAM.

Step 3.1 >

Langkah 3.1: Kumpulkan metadata penyedia layanan yang diperlukan dari Pusat Identitas IAM

Pada langkah ini, Anda akan meluncurkan wizard 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 Microsoft Entra ID di langkah berikutnya.

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 Penyelesaian identitas eksternal, lalu pilih Berikutnya.
4. Pada halaman Konfigurasi penyedia identitas eksternal, di bawah Metadata penyedia layanan, pilih Default IPv4 atau Dual-stack. Anda dapat mengunduh file metadata penyedia layanan setelah menyelesaikan perubahan sumber identitas.
5. Di bagian yang sama, cari nilai URL masuk portal AWS akses dan salin. Anda harus memasukkan nilai ini ketika diminta pada langkah berikutnya.
6. Biarkan halaman ini terbuka, dan pindah ke langkah berikutnya (**Step 3.2**) untuk mengkonfigurasi aplikasi AWS IAM Identity Center perusahaan di Microsoft Entra ID. Kemudian, Anda akan kembali ke halaman ini untuk menyelesaikan prosesnya.

Step 3.2 >

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

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

1. Di [konsol tengah admin](#) Microsoft Entra, navigasikan ke Identitas > Aplikasi > Aplikasi perusahaan, lalu pilih AWS IAM Identity Center.
2. Di sebelah kiri, pilih 2. Siapkan Single sign-on.
3. Pada halaman Set up Single Sign-On with SAML, pilih SAML. Kemudian pilih Unggah file metadata, pilih ikon folder, pilih file metadata penyedia layanan yang Anda unduh pada langkah sebelumnya, lalu pilih Tambah.
4. Pada halaman Konfigurasi SAML Dasar, verifikasi bahwa nilai Identifier dan Reply URL (Assertion Consumer Service URL) sekarang menunjuk ke titik akhir di AWS
 - Identifier - Ini adalah URL Penerbit dari Pusat Identitas IAM. Nilai yang sama berlaku terlepas dari apakah Anda menggunakan IPv4-only atau titik akhir tumpukan ganda.
 - URL Balas (URL Layanan Konsumen Penegasan) - Nilai di sini mencakup kedua IPv4-only dan titik akhir tumpukan ganda dari semua Wilayah yang diaktifkan di Pusat Identitas IAM Anda. Anda dapat menggunakan URL ACS Wilayah utama sebagai URL default sehingga pengguna diarahkan ke Wilayah utama saat mereka meluncurkan aplikasi Amazon Web

Services dari Microsoft Entra ID. Untuk informasi selengkapnya tentang URL ACS, lihat [Titik akhir ACS di primer dan tambahan Wilayah AWS](#).

- (Opsional) Jika Anda mereplikasi Pusat Identitas IAM ke Wilayah tambahan, Anda juga dapat membuat aplikasi bookmark Microsoft Entra ID untuk portal AWS akses di setiap Wilayah tambahan. Ini memungkinkan pengguna Anda untuk mengakses portal AWS akses di Wilayah tambahan dari Microsoft Entra ID. Pastikan untuk memberikan izin kepada pengguna Anda untuk mengakses aplikasi bookmark di Microsoft Entra ID. Lihat [Microsoft Entra ID dokumentasi](#) untuk lebih jelasnya. Jika Anda berencana untuk mereplikasi Pusat Identitas IAM ke Wilayah tambahan nanti, kunjungi [Microsoft Entra ID konfigurasi untuk akses ke Wilayah tambahan](#) untuk panduan cara mengaktifkan akses ke Wilayah tambahan setelah penyiapan awal ini.
5. Di bawah **Sign on URL** (Opsional), tempel nilai URL masuk portal AWS akses yang Anda salin pada langkah sebelumnya (**Step 3.1**), pilih **Simpan**, lalu pilih **X** untuk menutup jendela.
 6. Jika diminta untuk menguji sistem masuk tunggal dengan AWS 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 SAML**, di bagian **Sertifikat SAML**, di sebelah **Federation Metadata XML**, pilih **Unduh** untuk menyimpan file metadata ke sistem Anda. Anda harus mengunggah file ini ketika 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 SAML 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 SAML**, pilih tombol **Pilih file**, dan pilih file metadata penyedia identitas yang Anda unduh Microsoft Entra ID di langkah sebelumnya, lalu pilih **Buka**.
3. Pilih **Berikutnya**.
4. Setelah Anda membaca penafian dan siap untuk melanjutkan, masukkan **ACCEPT**.
5. Pilih **Ubah sumber identitas** untuk menerapkan perubahan Anda.

Step 3.4 >

Langkah 3.4: Uji bahwa Nikki dialihkan ke portal AWS akses

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

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. Pada halaman Akun saya, di panel 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 kredensial NikkiWolf Anda. Jika diminta untuk kedua kalinya untuk otentikasi, pilih NikkiWolf kredensi 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. Pastikan Akun AWS tampilan Anda.

Tip

Jika halaman kosong dan tidak ada Akun AWS tampilan, konfirmasi bahwa Nikki berhasil ditugaskan ke grup RegionalAdmin dengan izin (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 untuknya Akun AWS. Nikki seharusnya hanya memiliki hak administrator yang cukup untuk mengelola Wilayah dari halaman Akun.

1. Di portal AWS akses, pilih tab Akun untuk menampilkan daftar akun. Nama akun, ID akun, dan alamat email yang terkait dengan akun mana pun yang telah Anda tetapkan kumpulan izin muncul.
2. Pilih nama akun (misalnya, *Sandbox*) tempat Anda menerapkan kumpulan izin (lihat **Step 2.3**). Ini akan memperluas daftar kumpulan izin yang dapat dipilih Nikki untuk mengelola akunnya.
3. Selanjutnya RegionalAdmin pilih Konsol manajemen untuk mengambil peran yang Anda tetapkan dalam kum RegionalAdmin pulan izin. Ini akan mengarahkan Anda ke halaman Konsol Manajemen AWS 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 Wil AWS ayah. Pilih kotak centang untuk Wilayah yang tersedia dalam tabel. Perhatikan bahwa Nikki memang memiliki izin yang diperlukan untuk Meng aktifkan atau Men onaktifkan daftar Wilayah untuk akunnya seperti yang dimaksudkan.

 Dilakukan dengan baik!

Langkah 1 hingga 3 membantu Anda berhasil menerapkan dan menguji koneksi SAML 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 dengan Microsoft Entra ID menggunakan titik akhir SCIM untuk Pusat Identitas IAM dan token pembawa yang dibuat secara otomatis oleh Pusat Identitas IAM.

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 Pusat Identitas IAM dan Microsoft Entra ID.

Langkah-langkah berikut memandu Anda melalui cara mengaktifkan penyediaan otomatis pengguna yang terutama berada di Pusat Identi Microsoft Entra ID tas 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 apakah pengguna ini dan semua atribut yang relevan berhasil disinkronkan ke Pusat Identitas IAM.

1. Di [konsol tengah admin](#) Microsoft Entra, navigasikan ke Identitas > Pengguna > Semua pengguna.
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 - Masukkan **Marketing Lead**
 - Departemen - Masuk **Sales**
 - ID Karyawan - Masukkan **12345**
7. Pilih Tinjauan + buat, lalu pilih Buat.

Step 4.2 >

Langkah 4.2: Aktifkan penyediaan otomatis di Pusat Identitas IAM

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. Cari kotak informasi penyediaan otomatis, lalu pilih Aktifkan. Ini segera memungkinkan penyediaan otomatis di Pusat Identitas IAM dan menampilkan titik akhir SCIM yang diperlukan dan informasi token akses.
4. Di kotak dialog Penyediaan otomatis masuk, salin setiap nilai untuk opsi berikut. Anda harus menempelkannya di langkah berikutnya saat Anda mengonfigurasi penyediaan Microsoft Entra ID.
 - a. Titik akhir SCIM - Misalnya,
 - IPv4: `https://scim.aws-region.amazonaws.com/1111111111-2222-3333-4444-555555555555/scim/v2`
 - Tumpukan ganda: `https://scim.aws-region.api.aws/1111111111-2222-3333-4444-555555555555/scim/v2`
 - b. Token akses - Pilih Tampilkan token untuk menyalin nilainya.

 Warning

Ini adalah satu-satunya waktu di mana Anda dapat memperoleh titik akhir SCIM dan token akses. Pastikan Anda menyalin nilai-nilai ini sebelum bergerak maju.

5. Pilih Tutup.
6. Di bawah tab Sumber identitas, perhatikan bahwa metode Penyediaan sekarang diatur ke SCIM.

Step 4.3 >

Langkah 4.3: Konfigurasi penyediaan otomatis di Microsoft Entra ID

Sekarang setelah Anda memiliki pengguna RichRoe pengujian Anda di tempat dan telah mengaktifkan SCIM di Pusat Identitas IAM, Anda dapat melanjutkan dengan mengonfigurasi pengaturan sinkronisasi SCIM di Microsoft Entra ID

1. Di [konsol tengah admin](#) Microsoft Entra, navigasikan ke Identitas > Aplikasi > Aplikasi perusahaan, lalu 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 nilai URL titik akhir SCIM yang Anda salin **Step 4.2** sebelumnya. Di Token Rahasia, tempel nilai token Akses.
5. Pilih Uji Koneksi. Anda akan melihat pesan yang menunjukkan bahwa kredensial yang diuji berhasil diotorisasi untuk mengaktifkan penyediaan.
6. Pilih Simpan.
7. Di bawah Kelola, pilih Pengguna dan grup, lalu pilih Tambah user/group.
8. Pada halaman Tambah Tugas, di bawah Pengguna, pilih Tidak Ada yang Dipilih.
9. Pilih RichRoe, lalu pilih Pilih.
10. Pada halaman Tambah Tugas, pilih Tetapkan.
11. Pilih Ihtisar, 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 RichRoe pengguna Anda ditampilkan. Perhatikan bahwa di kolom Dibuat oleh nilainya diatur ke SCIM.
3. Pilih RichRoe, di bawah Profil, verifikasi bahwa atribut berikut disalin dari Microsoft Entra ID.
 - Nama depan - **Richard**
 - Nama belakang - **Roe**
 - Departemen - **Sales**
 - Judul - **Marketing Lead**
 - Nomor Karyawan - **12345**

Sekarang pengguna Richard telah dibuat di Pusat Identitas IAM, Anda dapat menentukannya ke kumpulan izin apa pun sehingga Anda dapat mengontrol tingkat akses yang dimilikinya ke AWS sumber daya Anda. Misalnya, Anda dapat menetapkan RichRoe ke kumpulan **RegionalAdmin** izin yang Anda gunakan sebelumnya untuk memberi Nikki izin untuk mengelola Wilayah (lihat **Step 2.3**) dan kemudian menguji tingkat aksesnya menggunakan **Step 3.5**.

 Selamat!

Anda telah berhasil mengatur koneksi SAML antara Microsoft 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.

Langkah 5: Konfigurasikan ABAC - Opsional

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

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

Configure user attributes in Microsoft Entry ID for access control in IAM Identity Center

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 Pusat Identitas IAM untuk mengelola akses ke AWS sumber daya Anda. Setelah ditentukan, ke Microsoft Entra ID atribut ini ke Pusat Identitas IAM melalui pernyataan SAML. Anda kemudian perlu [Membuat kumpulan izin](#) di Pusat Identitas IAM untuk mengelola akses berdasarkan atribut yang Anda lewati. Microsoft Entra ID

Sebelum Anda memulai prosedur ini, Anda harus terlebih dahulu mengaktifkan [Atribut untuk kontrol akses](#) fitur ini. Untuk informasi selengkapnya tentang cara melakukan ini, lihat [Mengaktifkan dan mengonfigurasi atribut untuk kontrol akses](#).

1. Di [konsol tengah admin](#) Microsoft Entra, navigasikan ke Identitas > Aplikasi > Aplikasi perusahaan, lalu 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 Pusat Identitas IAM. Misalnya, `AccessControl:Department`.
 - c. Untuk Namespace, masukkan `https://aws.amazon.com/SAML/Attributes`.
 - d. Untuk Sumber, pilih Atribut.
 - e. Untuk atribut Sumber, gunakan daftar drop-down untuk memilih atribut Microsoft Entra ID pengguna. Misalnya, `user.department`.
5. Ulangi langkah sebelumnya untuk setiap atribut yang perlu Anda kirim ke Pusat Identitas IAM dalam pernyataan SAML.
6. Pilih Simpan.

Configure ABAC using IAM Identity Center

Konfigurasikan ABAC menggunakan Pusat Identitas IAM

Dengan metode ini, Anda menggunakan [Atribut untuk kontrol akses](#) fitur di Pusat Identitas IAM untuk meneruskan Attribute elemen dengan Name atribut disetel ke `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Anda dapat menggunakan elemen ini untuk meneruskan atribut sebagai tag sesi dalam pernyataan SAML. Untuk informasi selengkapnya tentang tag sesi, [lihat Meneruskan 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 `tagDepartment=billing`, gunakan atribut berikut:

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

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

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

Tetapkan akses ke Akun AWS

Langkah-langkah berikut hanya diperlukan untuk memberikan akses ke Akun AWS saja. Langkah-langkah ini tidak diperlukan untuk memberikan akses ke AWS aplikasi.

Note

Untuk menyelesaikan langkah ini, Anda memerlukan instance Organisasi dari Pusat Identitas IAM. Untuk informasi selengkapnya, lihat [Instans organisasi dan akun dari Pusat Identitas IAM](#).

Langkah 1: Pusat Identitas IAM: Hibah Microsoft Entry ID akses pengguna ke akun

1. Kembali ke konsol Pusat Identitas IAM. Di panel navigasi Pusat Identitas IAM, di bawah `Multi-account` izin, pilih `Akun AWS`.
2. Pada Akun AWS halaman `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. Alur kerja `Tetapkan pengguna dan grup` ditampilkan. 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 kumpulan izin` pilih `Buat kumpulan izin` untuk membuka tab baru yang memandu Anda melalui tiga sub-langkah yang terlibat dalam membuat kumpulan izin.
 - i. Untuk `Langkah 1: Pilih jenis kumpulan izin`, leng kapi yang berikut:
 - Di `Jenis kumpulan izin`, pilih `Set izin` yang telah ditentukan sebelumnya.
 - Di `Kebijakan untuk kumpulan izin` yang telah ditentukan sebelumnya, pilih `AdministratorAccess`.

Pilih Berikutnya.

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

Pengaturan default membuat kumpulan izin bernama *AdministratorAccess* dengan durasi sesi disetel ke satu jam.

- iii. Untuk Langkah 3: Tinjau dan buat, verifikasi bahwa jenis kumpulan izin menggunakan kebijakan ter AWS kelola AdministratorAccess. Pilih Buat. Pada halaman Kumpulan izin muncul pemberitahuan yang memberi tahu Anda bahwa kumpulan izin telah dibuat. Anda dapat menutup tab ini di browser web Anda sekarang.
 - iv. Pada tab browser Tetapkan pengguna dan grup, Anda masih menggunakan Langkah 2: Pilih kumpulan izin tempat Anda memulai alur kerja buat kumpulan izin.
 - v. Di area Perizinan set, pilih tombol Refresh. Kumpulan *AdministratorAccess* izin yang Anda buat muncul dalam daftar. Pilih kotak centang untuk kumpulan izin tersebut, lalu pilih Berikutnya.
- c. Untuk Langkah 3: Tinjau dan kirimkan ulasan pengguna dan kumpulan 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 Anda Akun AWS telah disediakan ulang dan kumpulan izin yang diperbarui diterapkan. Ketika pengguna masuk, mereka akan memiliki opsi untuk memilih *AdministratorAccess* peran.

Langkah 2: Microsoft Entra ID: Konfirmasikan Microsoft Entra ID akses pengguna ke AWS sumber daya

1. Kembali ke Microsoft Entra ID konsol dan navigasikan ke SAML-based Sign-on aplikasi Pusat Identitas IAM Anda.
2. Pilih Pengguna dan grup dan pilih Tambahkan pengguna atau grup. Anda akan menambahkan pengguna yang Anda buat dalam tutorial ini di Langkah 4 ke Microsoft Entra ID aplikasi. Dengan menambahkan pengguna, Anda akan mengizinkan mereka untuk AWS masuk. Cari pengguna yang Anda buat di Langkah 4. Jika Anda mengikuti langkah ini, itu akan terjadi **RichardRoe**.

- Untuk demo, lihat Menggabungkan [instans Pusat Identitas IAM yang ada dengan Microsoft Entra ID](#)

Microsoft Entry ID konfigurasi untuk akses ke Wilayah tambahan Pusat Identitas IAM - Opsional

Jika Anda mereplikasi Pusat Identitas IAM ke Wilayah tambahan, Anda harus memperbarui konfigurasi penyedia identitas untuk mengaktifkan akses ke aplikasi terkel AWS dan Akun AWS melalui Wilayah tambahan. Langkah-langkah di bawah ini memandu Anda melalui prosedur. Untuk detail lebih lanjut tentang topik ini termasuk prasyarat, lihat [Menggunakan Pusat Identitas IAM di beberapa Wilayah AWS](#).

1. Ambil URL ACS untuk wilayah tambahan dari konsol Pusat Identitas IAM seperti yang diuraikan dalam [Titik akhir ACS di primer dan tambahan Wilayah AWS](#).
2. Di [konsol tengah admin](#) Microsoft Entra, navigasikan ke Identitas > Aplikasi > Aplikasi perusahaan, lalu pilih AWS IAM Identity Center.
3. Di sebelah kiri, pilih 2. Siapkan Single sign-on.
4. Pada halaman Konfigurasi SAML Dasar, di bawah bagian URL Balas (URL Layanan Konsumen Penegasan), pilih Tambahkan URL balasan untuk setiap URL ACS Wilayah penambahan. Anda dapat menyimpan URL ACS Wilayah utama sebagai URL default sehingga pengguna terus diarahkan ke Wilayah utama saat mereka meluncurkan AWS IAM Identity Center aplikasi dari Microsoft Entra ID.
5. Setelah selesai menambahkan URL ACS, simpan AWS IAM Identity Center aplikasi.
6. Anda dapat membuat aplikasi bookmark Microsoft Entra ID untuk portal AWS akses di setiap Wilayah tambahan. Ini memungkinkan pengguna Anda untuk mengakses portal AWS akses di Wilayah tambahan dari Microsoft Entra ID. Pastikan untuk memberikan izin kepada pengguna Anda untuk mengakses aplikasi bookmark di Microsoft Entra ID. Lihat [Microsoft Entra ID dokumentasi](#) untuk lebih jelasnya.
7. Pastikan Anda dapat masuk ke portal AWS akses di setiap Wilayah tambahan. Arahkan ke URL portal [AWS akses](#) atau luncurkan aplikasi bookmark dari Microsoft Entra ID.

Pemecahan masalah

Untuk pemecahan masalah SCIM dan SAML umum dengan Microsoft Entra ID, lihat bagian berikut:

- [Masalah sinkronisasi dengan Microsoft Entry ID dan Pusat Identitas IAM](#)
- [Pengguna tertentu gagal melakukan sinkronisasi ke Pusat Identitas IAM dari penyedia SCIM eksternal](#)
- [Masalah mengenai isi pernyataan SAML yang dibuat oleh Pusat Identitas IAM](#)
- [Duplikat kesalahan pengguna atau grup saat menyediakan pengguna atau grup dengan penyedia identitas eksternal](#)
- [Sumber daya tambahan](#)

Masalah sinkronisasi dengan Microsoft Entry ID dan Pusat Identitas IAM

Jika Anda mengalami masalah dengan Microsoft Entra ID pengguna yang tidak menyinkronkan ke Pusat Identitas IAM, itu mungkin karena masalah sintaks yang ditandai oleh Pusat Identitas IAM saat pengguna baru ditambahkan ke Pusat Identitas IAM. Anda dapat mengonfirmasi hal ini dengan memeriksa log Microsoft Entra ID audit untuk kejadian 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 peristiwa yang gagal. Ini dapat dilakukan dengan mencari di konsol Riwayat Acara CloudTrail menggunakan filter berikut:

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

Kesalahan dalam CloudTrail acara akan menyatakan sebagai berikut:

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

Pada akhirnya, pengecualian ini berarti bahwa salah satu nilai yang diteruskan Microsoft Entra ID berisi lebih banyak nilai daripada yang diantisipasi. Solusinya adalah meninjau atribut pengguna di Microsoft 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, kantor, dan faks. Meskipun nilai-nilai terpisah, semuanya diteruskan ke Pusat Identitas IAM di bawah atribut induk tunggal Phone Numbers.

Untuk tips pemecahan masalah SCIM umum, lihat [Pemecahan Masalah](#).

Microsoft Entra ID Sinkronisasi Akun Tamu

Jika Anda ingin menyinkronkan pengguna Microsoft Entra ID tamu ke Pusat Identitas IAM, lihat prosedur berikut.

Microsoft Entra ID email pengguna tamu berbeda dari Microsoft Entra ID pengguna. Perbedaan ini menyebabkan masalah saat mencoba menyinkronkan pengguna Microsoft Entra ID tamu dengan Pusat Identitas IAM. Misalnya, lihat alamat email berikut untuk pengguna tamu:

`exampleuser_domain.com#EXT#@domain.onmicrosoft.com`.

Pusat Identitas IAM tidak mengharapkan alamat email berisi `#EXT#@domain` format.

1. Masuk ke pusat admin [Microsoft Entra](#) dan arahkan ke Identitas > Aplikasi > Aplikasi perusahaan, lalu pilih AWS IAM Identity Center
2. Arahkan ke tab Single Sign On di panel kiri.
3. Pilih Edit yang muncul di sebelah Atribut & Klaim Pengguna.
4. Pilih Pen gidentifikasi Pengguna Unik (ID Nama) setelah Klaim yang Diperlukan.
5. Anda akan membuat dua kondisi klaim untuk Microsoft Entra ID pengguna dan pengguna tamu Anda:
 - a. Untuk Microsoft Entra ID pengguna, buat tipe pengguna untuk anggota dengan atribut sumber disetel ke `user.userprincipalname`.
 - b. Untuk pengguna Microsoft Entra ID tamu, buat jenis pengguna untuk tamu eksternal dengan atribut sumber disetel ke `user.mail`.
 - c. Pilih Simpan dan coba masuk lagi sebagai pengguna Microsoft Entra ID tamu.

Sumber daya tambahan

- Untuk tips pemecahan masalah SCIM umum, lihat [Memecahkan masalah Pusat Identitas IAM](#).
- Untuk pem Microsoft Entra ID ecahan masalah, lihat [Microsoft dokumentasi](#).
- Untuk mempelajari lebih lanjut tentang federasi di beberapa Akun AWS, lihat Meng [amankan Akun AWS dengan Azure Active Directory Federation](#).

Sumber daya berikut dapat membantu Anda memecahkan masalah saat Anda bekerja dengan AWS:

- [AWS re:Post](#)- Temukan FAQ dan tautan ke sumber daya lain untuk membantu Anda memecahkan masalah.
- [AWS Dukungan](#)- Dapatkan dukungan teknis

Konfigurasi SAFL dan SCIM dengan Okta dan Pusat Identitas IAM

Anda dapat secara otomatis menyediakan atau menyinkronkan informasi pengguna dan grup dari Okta ke Pusat Identitas IAM menggunakan protokol [System for Cross-domain Identity Management \(SCIM\) 2.0](#). Untuk informasi selengkapnya, lihat [Menggunakan federasi identitas SAMP dan SCIM dengan penyedia identitas eksternal](#).

Untuk mengonfigurasi koneksi ini, 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 akun Anda Okta.

Okta mendukung 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.

- Impor pengguna - Pengguna dapat diimpor dari IAM Identity Center ke Okta.

Objektif

Dalam tutorial ini, Anda akan berjalan melalui pengaturan koneksi SAFL dengan Okta IAM Identity Center. Nanti, Anda akan menyinkronkan pengguna dari Okta, menggunakan SCIM. Dalam skenario ini, Anda mengelola semua pengguna dan grup Okta. 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.

Fitur-fitur berikut didukung saat menghubungkan Okta ke IAM Identity Center melalui SALL:

- IdP-initiated Masuk SAMM — Pengguna masuk melalui Okta portal dan mendapatkan akses ke Pusat Identitas IAM.
- SP-initiated Masuk SAMP — Pengguna mengakses portal AWS akses, yang mengarahkan mereka untuk masuk melalui portal. Okta

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.

Jika Anda belum mengaktifkan IAM Identity Center, lihat [Aktifkan Pusat Identitas IAM](#).

Pertimbangan-pertimbangan

- Sebelum Anda mengonfigurasi penyediaan SCIM antara Okta dan IAM Identity Center, kami sarankan Anda meninjau terlebih dahulu. [Pertimbangan untuk menggunakan penyediaan otomatis](#)
- 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.

- Saat menggunakan Okta dengan IAM Identity Center, IAM Identity Center umumnya dikonfigurasi sebagai Aplikasi di. Okta Hal ini memungkinkan Anda untuk mengkonfigurasi beberapa instance IAM Identity Center sebagai beberapa aplikasi, mendukung akses ke beberapa AWS Organizations, dalam satu instance. Okta
- 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 konfigurasi untuk mendorong grup ke Pusat Identitas IAM.
- Jika Anda mereplikasi Pusat Identitas IAM ke Wilayah tambahan, Anda harus memperbarui konfigurasi penyedia identitas Anda untuk mengaktifkan akses ke aplikasi AWS terkelola dan Akun AWS melalui Wilayah tambahan. Untuk detail lebih lanjut termasuk prasyarat, lihat. [Menggunakan Pusat Identitas IAM di beberapa Wilayah AWS](#) Okta-specific langkah-langkah dijelaskan dalam [Oktakonfigurasi untuk akses ke Wilayah tambahan](#)

Langkah 1: Okta: Dapatkan metadata SAFL dari Anda Okta akun

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 ini di langkah selanjutnya.

Langkah 2: Pusat Identitas IAM: Konfigurasi 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, salin item berikut ke file teks agar mudah diakses:
 - URL IAM Identity Center Assertion Consumer Service (ACS) — Anda memiliki pilihan antara IPv4-only dan URL ACS dual-stack. Selain itu, jika instans Pusat Identitas IAM Anda diaktifkan di beberapa Wilayah, setiap Wilayah tambahan memiliki URL ACS masing-masing IPv4-only dan dual-stack. Untuk informasi selengkapnya tentang URL ACS, lihat [Titik akhir ACS di primer dan tambahan Wilayah AWS](#).
 - URL penerbit Pusat Identitas IAM

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

- b. Di bawah Metadata penyedia identitas, di bawah metadata IDP SAMP, pilih Pilih file lalu pilih file yang Anda buat di langkah sebelumnya `metadata.xml`.
 - 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 ini di langkah berikutnya.

8. Kembali ke Okta admin dashboard dan pilih tab Masuk AWS IAM Identity Center aplikasi, lalu pilih Edit.
9. Di bawah Sign-on Pengaturan Lanjutan masukkan yang berikut ini:
 - Untuk URL ACS, masukkan nilai yang Anda salin untuk URL IAM Identity Center Assertion Consumer Service (ACS). Anda dapat menggunakan URL ACS Wilayah utama sebagai URL default sehingga pengguna diarahkan ke Wilayah utama saat mereka meluncurkan aplikasi Amazon Web Services dari Okta.

- (Opsional) Jika Anda mereplikasi Pusat Identitas IAM ke Wilayah tambahan, Anda juga dapat membuat aplikasi bookmark Okta untuk portal AWS akses di setiap Wilayah tambahan. Ini memungkinkan pengguna Anda untuk mengakses portal AWS akses di Wilayah tambahan dari Okta. Pastikan untuk memberikan izin kepada pengguna Anda untuk mengakses aplikasi bookmark di Okta. Lihat [Okta dokumentasi](#) untuk lebih jelasnya. Jika Anda berencana untuk mereplikasi Pusat Identitas IAM ke Wilayah tambahan nanti, kunjungi [Okta konfigurasi untuk akses ke Wilayah tambahan](#) panduan cara mengaktifkan akses ke Wilayah tambahan setelah penyiapan awal ini.
- 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.

Pastikan 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 Okta Pusat Identitas IAM. Biarkan Okta admin dashboard terbuka, dan kembali ke konsol IAM Identity Center untuk langkah selanjutnya.

Langkah 3: Pusat Identitas IAM dan Okta: Ketentuan Okta pengguna

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:
 - a. Endpoint SCIM - Format endpoint tergantung pada konfigurasi Anda:
 - IPv4: `.amazonaws.com//https://scim.us-east-211111111111-2222-3333-4444-555555555555scim/v2`
 - Dual-stack: `https://scim.us-east-211111111111-2222-3333-4444-555555555555 .api.aws/scim/v2`
 - b. Access token - Pilih Tampilkan token untuk menyalin nilainya.

 Warning

Ini adalah satu-satunya waktu di mana Anda dapat memperoleh titik akhir SCIM dan token akses. Pastikan Anda menyalin nilai-nilai ini sebelum bergerak maju. Anda akan memasukkan nilai-nilai ini untuk mengkonfigurasi penyediaan otomatis Okta nanti dalam tutorial ini.

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 otomatis.
7. Konfigurasikan Okta dengan nilai penyediaan SCIM dari AWS IAM Identity Center yang Anda salin sebelumnya di langkah ini:
 - a. Di bidang URL Dasar, masukkan nilai titik akhir SCIM.
 - b. Di bidang Token API, masukkan nilai token Access.
8. Pilih Test API Credentials untuk memverifikasi kredensyal yang dimasukkan valid.

Pesan berhasil AWS IAM Identity Center diverifikasi! menampilkan.
9. Pilih Simpan. Anda dipindahkan ke bagian 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: Okta: Sinkronisasi pengguna dari Okta dengan Pusat Identitas IAM

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 AWS 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 ingin disinkronkan dengan IAM Identity Center. Pilih Simpan.

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

3. Kembali ke tab Tugas.
4. Untuk menambahkan Okta pengguna individu ke Pusat Identitas IAM, gunakan langkah-langkah berikut:
 - a. Di halaman Penugasan, pilih Tetapkan, lalu pilih Tetapkan ke Orang.
 - b. 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.

5. 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.

Melewati atribut untuk kontrol akses - Opsional

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 `tagCostCenter = 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.

Tetapkan akses ke Akun AWS

Langkah-langkah berikut hanya diperlukan untuk memberikan akses ke Akun AWS saja. Langkah-langkah ini tidak diperlukan untuk memberikan akses ke AWS aplikasi.

Note

Untuk menyelesaikan langkah ini, Anda memerlukan instance Organisasi dari IAM Identity Center. Untuk informasi selengkapnya, lihat [Instans organisasi dan akun dari Pusat Identitas IAM](#).

Langkah 1: Pusat Identitas IAM: Hibah Okta akses pengguna ke akun

1. Di panel navigasi Pusat Identitas IAM, di bawah Multi-accountizin, 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 kirim, tinjau pengguna yang dipilih dan set izin, 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*

Langkah 2: Okta: Konfirmasikan Okta akses pengguna ke AWS sumber daya

1. Masuk menggunakan akun uji ke fileOkta dashboard.
2. Di bawah Aplikasi Saya, pilih AWS IAM Identity Center ikon.
3. Anda harus 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 menentukan akses ke akses terprogram Konsol Manajemen AWS dan akses terprogram. Pilih Konsol manajemen untuk membuka Konsol Manajemen AWS.

6. Pengguna masuk ke Konsol Manajemen AWS.

Anda juga dapat menggunakan portal AWS akses. Ini mengarahkan Anda untuk masuk melalui Okta portal sebelum membawa Anda ke portal AWS akses. Jalur ini mengikuti alur masuk SP-initiated SAFL.

Okta konfigurasi untuk akses ke Wilayah tambahan Pusat Identitas IAM - Opsional

Jika Anda mereplikasi Pusat Identitas IAM ke Wilayah tambahan, Anda harus memperbarui konfigurasi penyedia identitas Anda untuk mengaktifkan akses ke aplikasi AWS terkelola dan Akun AWS melalui Wilayah tambahan. Langkah-langkah di bawah ini memandu Anda melalui prosedur ini. Untuk detail lebih lanjut tentang topik ini termasuk prasyarat, lihat. [Menggunakan Pusat Identitas IAM di beberapa Wilayah AWS](#)

1. Ambil URL ACS untuk wilayah tambahan dari konsol Pusat Identitas IAM seperti yang diuraikan dalam. [Titik akhir ACS di primer dan tambahan Wilayah AWS](#)
2. Di panel navigasi dasbor Okta admin, pilih Aplikasi, lalu Aplikasi lagi di daftar yang diperluas.
3. Pilih AWS IAM Identity Centeraplikasinya.
4. Pilih tab Masuk.
5. Di bawah Sign-on Pengaturan Lanjutan, dan URL SSO Lainnya yang Dapat Diminta, pilih Tambahkan yang lain untuk setiap URL ACS Wilayah tambahan, dan tempel URL ACS ke bidang teks.
6. Setelah selesai menambahkan URL ACS, simpan AWS IAM Identity Centeraplikasi.
7. Anda dapat membuat aplikasi bookmark Okta untuk portal AWS akses di setiap Wilayah tambahan. Ini memungkinkan pengguna Anda untuk mengakses portal AWS akses di Wilayah tambahan dariOkta. Pastikan untuk memberikan izin kepada pengguna Anda untuk mengakses aplikasi bookmark di. Okta Lihat [Okta dokumentasi](#) untuk lebih jelasnya.
8. Verifikasi bahwa Anda dapat masuk ke portal AWS akses di setiap Wilayah tambahan. Arahkan ke [URL portal AWS akses](#) atau luncurkan aplikasi bookmark dari. Okta

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, lihat [Menetapkan akses pengguna atau grup ke Akun AWS](#).
- Berikan akses ke aplikasi cloud, lihat [Menetapkan akses pengguna ke aplikasi di konsol Pusat Identitas IAM](#).
- Mengkonfigurasi izin berdasarkan fungsi pekerjaan, lihat [Membuat set izin](#).

Pemecahan masalah

Untuk pemecahan masalah SCIM dan SAFL umum dengan Okta, lihat bagian berikut:

- [Penyediaan ulang pengguna dan grup dihapus dari IAM Identity Center](#)
- [Kesalahan Penyediaan Otomatis di Okta](#)
- [Pengguna tertentu gagal melakukan sinkronisasi ke Pusat Identitas IAM dari penyedia SCIM eksternal](#)
- [Masalah mengenai isi pernyataan SAML yang dibuat oleh Pusat Identitas IAM](#)
- [Duplikat kesalahan pengguna atau grup saat menyediakan pengguna atau grup dengan penyedia identitas eksternal](#)
- [Sumber daya tambahan](#)

Penyediaan ulang pengguna dan grup dihapus dari IAM Identity Center

- Anda dapat menerima pesan galat berikut di Okta Konsol, jika Anda mencoba mengubah pengguna atau grup yang pernah disinkronkan dan kemudian dihapus dari Pusat Identitas IAM: Okta
 - Dorongan profil otomatis pengguna *Jane Doe* ke aplikasi AWS IAM Identity Center gagal: Kesalahan saat mencoba mendorong pembaruan profil untuk *jane_doe@example.com*: Tidak ada pengguna yang dikembalikan untuk pengguna *xxxxx-xxxxxx-xxxxx-xxxxxxx*
 - Grup tertaut tidak ada di AWS IAM Identity Center. Ubah grup tertaut untuk melanjutkan mendorong keanggotaan grup.
- Anda juga dapat menerima pesan galat berikut di Log Sistem untuk pengguna atau grup Pusat Identitas IAM yang disinkronkan dan dihapus: Okta
 - Kesalahan Okta: Eventfailed application.provision.user.push_profile: Tidak ada pengguna yang dikembalikan untuk pengguna *xxxxx-xxxxxx-xxxxx-xxxxxxx*

- Kesalahan Okta: `application.provision.group_push.mapping.update.or.delete.failed.with.error:` Grup tertaut tidak ada di. AWS IAM Identity Center Ubah grup tertaut untuk melanjutkan mendorong keanggotaan grup.

Warning

Pengguna dan grup harus dihapus dari Okta bukan IAM Identity Center jika Anda telah menyinkronkan Okta dan IAM Identity Center menggunakan SCIM.

Pemecahan masalah Pengguna Pusat Identitas IAM yang dihapus

Untuk mengatasi masalah ini dengan pengguna Pusat Identitas IAM yang dihapus, pengguna harus dihapus dari Okta. Jika perlu, pengguna ini juga perlu dibuat ulang. Okta Ketika pengguna dibuat ulang Okta, itu juga akan direvisi ke Pusat Identitas IAM melalui SCIM. Untuk informasi selengkapnya tentang menghapus pengguna, lihat [Okta dokumentasi](#).

Note

Jika Anda perlu menghapus akses Okta pengguna ke Pusat Identitas IAM, Anda harus terlebih dahulu menghapusnya dari Push Grup mereka dan kemudian Grup Penugasan mereka masuk. Okta Ini memastikan pengguna dihapus dari keanggotaan grup terkait mereka di IAM Identity Center. [Untuk informasi selengkapnya tentang pemecahan masalah Group Push, lihat Okta dokumentasi.](#)

Pemecahan masalah Grup Pusat Identitas IAM yang dihapus

Untuk mengatasi masalah ini dengan grup Pusat Identitas IAM yang dihapus, grup harus dihapus dari Okta. Jika perlu, grup ini juga perlu dibuat ulang di Okta menggunakan Group Push. Ketika pengguna dibuat ulang di Okta, itu juga akan direvisi ke Pusat Identitas IAM melalui SCIM. Untuk informasi selengkapnya tentang menghapus grup, lihat dokumentasi [Okta](#).

Kesalahan Penyediaan Otomatis di Okta

Jika Anda menerima pesan galat berikut di Okta:

Penyediaan otomatis pengguna Jane Doe ke aplikasi AWS IAM Identity Center gagal: Pengguna yang cocok tidak ditemukan

Lihat [Oktadokumentasi](#) untuk informasi lebih lanjut.

Sumber daya tambahan

- Untuk tips pemecahan masalah SCIM umum, lihat. [Memecahkan masalah Pusat Identitas IAM](#)

Sumber daya berikut dapat membantu Anda memecahkan masalah saat Anda bekerja dengan: AWS

- [AWS re:Post](#)- Temukan FAQ dan tautan ke sumber daya lain untuk membantu Anda memecahkan masalah.
- [AWS Dukungan](#)- Dapatkan dukungan teknis

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. Untuk informasi selengkapnya, lihat [Menggunakan federasi identitas SAMP dan SCIM dengan penyedia identitas eksternal](#).

Note

OneLoginsaat ini tidak mendukung layanan konsumsi pernyataan ganda SAMP (ACS) URLs dalam aplikasi. AWS IAM Identity Center Fitur SAMP ini diperlukan untuk sepenuhnya memanfaatkan [dukungan Multi-wilayah](#) di IAM Identity Center. Jika Anda berencana untuk mereplikasi Pusat Identitas IAM ke Wilayah tambahan, ketahuilah bahwa menggunakan satu URL ACS dapat memengaruhi pengalaman pengguna di Wilayah tambahan tersebut. Wilayah utama Anda akan terus berfungsi secara normal. Kami menyarankan Anda bekerja dengan vendor IDP Anda untuk mengaktifkan fitur ini. Untuk informasi selengkapnya tentang pengalaman pengguna di Wilayah tambahan dengan satu URL ACS, lihat [the section called “Penggunaan AWS aplikasi yang dikelola tanpa beberapa URL ACS”](#) dan [the section called “Akun AWS akses ketahanan tanpa beberapa URL ACS”](#).

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 dan OneLogin.

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](#)
- [Langkah 1: Aktifkan penyediaan di IAM Identity Center](#)
- [Langkah 2: Konfigurasi penyediaan di OneLogin](#)
- [\(Opsional\) Langkah 3: Konfigurasi atribut pengguna OneLogin untuk kontrol akses di Pusat Identitas IAM](#)
- [\(Opsional\) Melewati atribut untuk kontrol akses](#)
- [Pemecahan masalah](#)

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. Di kotak dialog Inbound automatic provisioning, salin endpoint SCIM dan token akses. Anda harus menempelkannya nanti saat mengonfigurasi penyediaan di iDP Anda.
 - a. Titik akhir SCIM - Misalnya, `https://scim.us-east-2.amazonaws.com/ /scim/v2111111111-2222-3333-4444-5555555555`
 - b. Access token - Pilih Tampilkan token untuk menyalin nilainya.

Warning

Ini adalah satu-satunya waktu di mana Anda dapat memperoleh titik akhir SCIM dan token akses. Pastikan Anda menyalin nilai-nilai ini sebelum bergerak maju. Anda akan memasukkan nilai-nilai ini untuk mengkonfigurasi penyediaan otomatis di IDP Anda nanti dalam tutorial ini.

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 dengan OneLogin, lihat [Mengaktifkan Single Sign-On Between OneLogin dan AWS di Blog Jaringan Mitra](#). AWS

Untuk mengonfigurasi penyediaan di OneLogin

1. Masuk ke OneLogin, 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 panel navigasi.
3. Pada prosedur sebelumnya, Anda menyalin nilai endpoint SCIM di IAM Identity Center. Tempelkan nilai itu ke bidang URL Dasar SCIM di OneLogin. 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 panel navigasi, pilih Penyediaan.
6. Pilih kotak centang untuk Aktifkan penyediaan, Buat pengguna, Hapus pengguna, dan Perbarui pengguna, lalu pilih Simpan.
7. Di panel navigasi, pilih Users (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 kemajuannya. 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 pilih Buat Pengguna, Hapus Pengguna, and/or Perbarui Pengguna, dan klik Simpan.

(Opsional) Langkah 3: Konfigurasi 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 [Mengaktifkan dan mengonfigurasi atribut untuk kontrol akses](#).

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

1. Masuk ke OneLogin, 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 panel navigasi.
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 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 `tagCostCenter = 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.

Pemecahan 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 grup OneLogin, 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 tindakan OneLogin, 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 Pusat Identitas IAM tanpa terlebih dahulu menghapusnya OneLogin dan sekarang saya mengalami user/group masalah sinkronisasi

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](#)
- [PingOne](#)

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. Untuk informasi selengkapnya, lihat [Menggunakan federasi identitas SAMP dan SCIM dengan penyedia identitas eksternal](#).

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 dan PingFederate.

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

- [Prasyarat](#)
- [Pertimbangan-pertimbangan](#)
- [Langkah 1: Aktifkan penyediaan di IAM Identity Center](#)
- [Langkah 2: Konfigurasi penyediaan di PingFederate](#)
- [\(Opsional\) Langkah 3: Konfigurasi atribut pengguna di PingFederate untuk kontrol akses di IAM Identity Center](#)
- [\(Opsional\) Melewati atribut untuk kontrol akses](#)
- [Pemecahan masalah](#)

Prasyarat

Anda 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 Ping Identity situs web.

- [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 SAMP antara dan IAM Identity Center. PingFederate
- Jika Anda mereplikasi Pusat Identitas IAM ke Wilayah tambahan, Anda harus memperbarui konfigurasi penyedia identitas Anda untuk mengaktifkan akses ke aplikasi AWS terkelola dan Akun AWS dari Wilayah tersebut. Untuk detail selengkapnya, lihat [the section called “Langkah 3 \(hanya penyedia identitas eksternal\): Perbarui pengaturan IdP eksternal”](#). Lihat PingFederate dokumentasi untuk detail tambahan.

Pertimbangan-pertimbangan

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 dikonfigurasi PingFederate, 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. Di kotak dialog penyediaan otomatis masuk, salin titik akhir SCIM dan token akses. Anda harus menempelkannya nanti saat mengonfigurasi penyediaan di iDP Anda.
 - a. Titik akhir SCIM - Misalnya, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-55555555555`
 - b. Access token - Pilih Tampilkan token untuk menyalin nilainya.

 Warning

Ini adalah satu-satunya waktu di mana Anda dapat memperoleh titik akhir SCIM dan token akses. Pastikan Anda menyalin nilai-nilai ini sebelum bergerak maju. Anda akan memasukkan nilai-nilai ini untuk mengkonfigurasi penyediaan otomatis di IDP Anda nanti dalam tutorial ini.

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: Konfigurasi 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, lihat [Prasyarat](#), 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.properties` file 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. PingFederate

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. Juga, dalam prosedur sebelumnya Anda menyalin nilai token Access di IAM Identity Center. Tempelkan nilai itu ke bidang Access Token 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 data PingFederate.

11. Pada halaman Pengaturan Sumber, konfirmasi 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: Konfigurasi atribut pengguna di PingFederate 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 [Mengaktifkan dan mengonfigurasi 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 data PingFederate.

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

Pemecahan masalah

Untuk pemecahan masalah SCIM dan SAMP umum dengan PingFederate, lihat bagian berikut:

- [Pengguna tertentu gagal melakukan sinkronisasi ke Pusat Identitas IAM dari penyedia SCIM eksternal](#)
- [Masalah mengenai isi pernyataan SAML yang dibuat oleh Pusat Identitas IAM](#)
- [Duplikat kesalahan pengguna atau grup saat menyediakan pengguna atau grup dengan penyedia identitas eksternal](#)
- Untuk informasi lebih lanjut tentang PingFederate, lihat [PingFederatedokumentasi](#).

Sumber daya berikut dapat membantu Anda memecahkan masalah saat Anda bekerja dengan: AWS

- [AWS re:Post](#)- Temukan FAQs dan tautkan ke sumber daya lain untuk membantu Anda memecahkan masalah.
- [AWS Dukungan](#)- Dapatkan dukungan teknis

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 dan PingOne.

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](#)
- [Pertimbangan-pertimbangan](#)

- [Langkah 1: Aktifkan penyedia di IAM Identity Center](#)
- [Langkah 2: Konfigurasikan penyedia di PingOne](#)
- [\(Opsional\) Langkah 3: Konfigurasikan atribut pengguna PingOne untuk kontrol akses di Pusat Identitas IAM](#)
- [\(Opsional\) Melewati atribut untuk kontrol akses](#)
- [Pemecahan masalah](#)

Prasyarat

Anda memerlukan yang berikut ini sebelum Anda dapat memulai:

- PingOneLangganan atau uji coba gratis, dengan otentikasi federasi dan kemampuan penyedia. Untuk informasi lebih lanjut tentang cara mendapatkan uji coba gratis, lihat situs [Ping Identity](#)web.
- [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 SAMP 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.
- Jika Anda mereplikasi Pusat Identitas IAM ke Wilayah tambahan, Anda harus memperbarui konfigurasi penyedia identitas Anda untuk mengaktifkan akses ke aplikasi AWS terkelola dan Akun AWS dari Wilayah tersebut. Untuk detail selengkapnya, lihat [the section called “Langkah 3 \(hanya penyedia identitas eksternal\): Perbarui pengaturan IdP eksternal”](#). Lihat PingOne dokumentasi untuk detail tambahan.

Pertimbangan-pertimbangan

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

- PingOne tidak mendukung penyediaan kelompok melalui SCIM. Hubungi Ping untuk informasi terbaru tentang dukungan grup di SCIM untuk PingOne.
- Pengguna dapat terus disediakan PingOne setelah menonaktifkan penyediaan di portal admin. PingOne Jika Anda perlu segera menghentikan penyediaan, hapus token pembawa SCIM yang relevan, and/or nonaktifkan [Menyediakan pengguna dan grup dari penyedia identitas eksternal menggunakan SCIM](#) di Pusat Identitas IAM.
- Jika atribut untuk pengguna dihapus dari penyimpanan data yang dikonfigurasi PingOne, 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 di PingOne:
 - IAM Identity Center hanya mendukung emailaddress sebagai NameId format. Ini berarti Anda harus memilih atribut pengguna yang unik dalam direktori Anda di PingOne, 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, di PingOne, 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:emailAddress dalam 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. Di kotak dialog penyediaan otomatis masuk, salin titik akhir SCIM dan token akses. Anda harus menempelkannya nanti saat mengonfigurasi penyediaan di iDP Anda.
 - a. Titik akhir SCIM - Misalnya, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
 - b. Access token - Pilih Tampilkan token untuk menyalin nilainya.

 Warning

Ini adalah satu-satunya waktu di mana Anda dapat memperoleh titik akhir SCIM dan token akses. Pastikan Anda menyalin nilai-nilai ini sebelum bergerak maju. Anda akan memasukkan nilai-nilai ini untuk mengkonfigurasi penyediaan otomatis di IDP Anda nanti dalam tutorial ini.

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: Konfigurasi 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, lihat [Prasyarat](#), 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 SAMP 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. 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-pertimbangan](#) 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: Konfigurasi 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 [Mengaktifkan dan mengonfigurasi 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 SAMP 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 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.

Pemecahan masalah

Untuk pemecahan masalah SCIM dan SAMP umum dengan PingOne, lihat bagian berikut:

- [Pengguna tertentu gagal melakukan sinkronisasi ke Pusat Identitas IAM dari penyedia SCIM eksternal](#)
- [Masalah mengenai isi pernyataan SAML yang dibuat oleh Pusat Identitas IAM](#)
- [Duplikat kesalahan pengguna atau grup saat menyediakan pengguna atau grup dengan penyedia identitas eksternal](#)
- Untuk informasi lebih lanjut tentang PingOne, lihat [PingOne dokumentasi](#).

Sumber daya berikut dapat membantu Anda memecahkan masalah saat Anda bekerja dengan: AWS

- [AWS re:Post](#)- Temukan FAQs dan tautkan ke sumber daya lain untuk membantu Anda memecahkan masalah.
- [AWS Dukungan](#)- Dapatkan dukungan teknis

Konfigurasi akses pengguna dengan direktori IAM Identity Center default

Ketika Anda mengaktifkan Pusat Identitas IAM 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 Microsoft Active Directory, Microsoft Entra ID, atau Okta pertimbangkan untuk mengintegrasikan sumber identitas tersebut dengan Pusat Identitas IAM alih-alih menggunakan konfigurasi default.

Tujuan

Dalam tutorial ini, Anda akan menggunakan direktori default sebagai sumber identitas Anda dan instance organisasi Pusat Identitas IAM untuk mengatur dan menguji pengguna administratif. Pengguna administratif ini membuat dan mengelola pengguna dan grup serta memberikan AWS akses dengan kumpulan izin. Pada langkah selanjutnya, Anda akan membuat yang berikut:

- Pengguna administratif bernama *Nikki Wolf*
- Sebuah kelompok bernama *Admin team*

- Kumpulan 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 Pusat Identitas IAM, membuat kumpulan izin tambahan, dan mengatur akses organisasi ke aplikasi. Atau, jika Anda ingin memberi pengguna akses ke aplikasi, Anda dapat mengikuti [langkah 1](#) dari prosedur ini dan [mengonfigurasi akses aplikasi](#).

Prasyarat

Prasyarat berikut diperlukan untuk menyelesaikan tutorial ini:

- [Aktifkan Pusat Identitas IAM](#) dan memiliki instance [organisasi dari Pusat](#) Identitas IAM.
 - Jika Anda memiliki instance [???](#) akun Pusat Identitas IAM, Anda dapat membuat pengguna dan grup serta memberi mereka akses ke aplikasi. Untuk informasi selengkapnya, lihat [Akses aplikasi](#).
- Masuk ke Konsol Manajemen AWS dan akses konsol Pusat Identitas IAM sebagai:
 - Baru untuk AWS (pengguna root) - Masuk sebagai pemilik akun dengan memilih pengguna Akun AWS root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.
 - Sudah menggunakan AWS (kredensial IAM) - Masuk menggunakan kredensial IAM Anda dengan izin administratif.
 - Untuk bantuan lebih lanjut untuk masuk ke Konsol Manajemen AWS, lihat [AWS Sign-In Panduan](#).
- Anda dapat mengonfigurasi otentikasi multi-faktor untuk pengguna Pusat Identitas IAM Anda. Untuk informasi selengkapnya, lihat [Konfigurasi MFA di Pusat Identitas IAM](#).

Langkah 1: Tambahkan pengguna

1. Buka konsol [Pusat Identitas IAM](#).
2. Di panel navigasi Pusat Identitas IAM, pilih Pengguna, lalu pilih Tambah pengguna.
3. 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 (Direkomendasikan).

Opsi ini mengirimkan alamat email kepada pengguna dari Amazon Web Services, dengan baris subjek Undangan untuk bergabung dengan Pusat Identitas IAM. 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.
4. Pilih Berikutnya. Halaman Tambahkan pengguna ke grup akan muncul. Kita akan membuat grup untuk menetapkan izin administratif alih-alih memberikannya secara langsung *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 *Admin team*.
 - b. Pilih Buat grup
 - c. Tutup tab browser Grup untuk kembali ke tab Tambah browser pengguna
5. Di area Grup, pilih tombol Refresh. *Admin team* Grup muncul dalam daftar.

Pilih kotak centang di sebelah *Admin team*, lalu pilih Berikutnya.

6. Pada halaman Tinjau dan tambahkan pengguna, konfirmasi 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 Tambah pengguna.

Pesan notifikasi memberi tahu Anda bahwa pengguna telah ditambahkan.

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

Langkah 2: Tambahkan izin administratif

Important

Ikuti langkah-langkah ini hanya jika Anda mengaktifkan instance [organisasi dari Pusat Identitas IAM](#).

1. Di panel navigasi Pusat Identitas IAM, di bawah Multi-account izin, pilih Akun AWS.
2. Pada Akun AWS halaman 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. Alur kerja Tetapkan pengguna dan grup ditampilkan. Ini terdiri dari tiga langkah:
 - a. Untuk Langkah 1: Pilih pengguna dan grup pilih *Admin team* grup yang Anda buat. Lalu pilih Selanjutnya.
 - b. Untuk Langkah 2: Pilih kumpulan izin pilih Buat kumpulan izin untuk membuka tab baru yang memandu Anda melalui tiga sub-langkah yang terlibat dalam membuat kumpulan izin.
 - i. Untuk Langkah 1: Pilih jenis kumpulan izin, lengkapi yang berikut:
 - Di Jenis kumpulan izin, pilih Set izin yang telah ditentukan sebelumnya.

- Di Kebijakan untuk kumpulan izin yang telah ditentukan sebelumnya, pilih `AdministratorAccess`.

Pilih Berikutnya.

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

Pengaturan default membuat kumpulan izin bernama `AdministratorAccess` dengan durasi sesi disetel ke satu jam. Anda dapat mengubah nama kumpulan izin dengan memasukkan nama baru di bidang Nama kumpulan izin.

- iii. Untuk Langkah 3: Tinjau dan buat, verifikasi bahwa jenis kumpulan izin menggunakan kebijakan ter AWS kelola `AdministratorAccess`. Pilih Buat. Pada halaman Kumpulan izin muncul pemberitahuan yang memberi tahu Anda bahwa kumpulan izin telah dibuat. Anda dapat menutup tab ini di browser web Anda sekarang.

Pada tab browser Tetapkan pengguna dan grup, Anda masih menggunakan Langkah 2: Pilih kumpulan izin tempat Anda memulai alur kerja buat kumpulan izin.

Di area Perizinan set, pilih tombol Refresh. Kumpulan `AdministratorAccess` izin yang Anda buat muncul dalam daftar. Pilih kotak centang untuk kumpulan izin tersebut, lalu pilih Berikutnya.

- c. Pada halaman Langkah 3: Tinjau dan kirim tugas, konfirmasi `Admin team` bahwa grup dipilih dan kumpulan `AdministratorAccess` izin dipilih, lalu pilih Kirim.

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

Anda dikembalikan ke Akun AWS halaman. Pesan notifikasi memberi tahu Anda bahwa Akun AWS telah disediakan ulang dan kumpulan izin yang diperbarui diterapkan.

 Selamat!

Anda telah berhasil mengatur pengguna, grup, dan kumpulan izin pertama Anda.

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

Langkah 3: Uji akses pengguna

Sekarang *Nikki Wolf* pengguna di organisasi Anda, mereka dapat masuk dan mengakses sumber daya yang diberi izin sesuai dengan kumpulan izin mereka. Untuk memverifikasi bahwa pengguna dikonfigurasi dengan benar, pada langkah berikutnya Anda akan menggunakan *Nikki's* kredensial untuk masuk dan mengatur kata sandi mereka. Ketika Anda menambahkan pengguna *Nikki Wolf* di Langkah 1, Anda memilih untuk *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 juga menyertakan nama *Nikki's* pengguna 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 *Nikki's* kata sandi dan men [daftarkan perangkat](#) MFA mereka.

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

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

Setiap kumpulan izin memiliki dua metode manajemen yang dapat Anda gunakan, baik tombol Peran atau Akses.

- Peran, misalnya *AdministratorAccess* - Membuka AWS Console Home.
- Kunci akses - Menyediakan kredensial yang dapat Anda gunakan dengan AWS CLI atau dan AWS SDK. Termasuk informasi untuk menggunakan kredensial jangka pendek yang secara otomatis menyegarkan atau kunci akses jangka pendek. Untuk informasi

selengkapnya, lihat [Mendapatkan kredensial pengguna Pusat Identitas IAM untuk AWS CLI atau AWS SDK](#).

4. Pilih tautan Peran untuk masuk ke AWS Console Home.

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

Langkah selanjutnya

Sekarang setelah Anda membuat pengguna administratif di Pusat Identitas IAM, Anda dapat:

- [Tetapkan aplikasi](#)
- [Tambahkan pengguna lain](#)
- [Menetapkan pengguna ke akun](#)
- [Konfigurasi kumpulan izin tambahan](#)

Note

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

Setelah pengguna [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 ditugaskan untuk mereka.

Tutorial video

Sebagai sumber daya tambahan, Anda dapat menggunakan tutorial video ini untuk mempelajari lebih lanjut tentang pengaturan penyedia identitas eksternal:

- [Migrasi antar penyedia identitas eksternal di AWS IAM Identity Center](#)
- [Menggabungkan AWS IAM Identity Center instance Anda yang ada dengan Microsoft Entra ID](#)

Siapkan tenaga kerja Anda di Pusat Identitas IAM

IAM Identity Center adalah AWS solusi untuk menghubungkan pengguna tenaga kerja Anda ke aplikasi ter AWS kelola seperti Kiro dan Amazon Quick, dan sumber daya lainnya AWS . Anda dapat menghubungkan penyedia identitas yang ada dan menyinkronkan pengguna dan grup dari direktori Anda, atau membuat dan mengelola pengguna secara langsung di Pusat Identitas IAM.

Sudah menggunakan IAM untuk akses ke? Akun AWS

Anda tidak perlu membuat perubahan apa pun pada alur Akun AWS kerja Anda saat ini untuk menggunakan Pusat Identitas IAM untuk akses ke aplikasi terkel AWS ola. Jika Anda menggunakan [federasi dengan IAM](#) untuk Akun AWS akses, pengguna Anda dapat terus mengakses dengan Akun AWS cara yang sama seperti biasanya, dan Anda dapat terus menggunakan alur kerja yang ada untuk mengelola akses tersebut.

Pilih pendekatan yang paling sesuai dengan strategi manajemen identitas organisasi Anda dan infrastruktur yang ada.

Topik

- [Pengguna, grup, dan penyediaan di Pusat Identitas IAM](#)
- [Kelola sumber identitas Anda](#)
- [Mengelola pengguna di direktori Pusat Identitas](#)

Pengguna, grup, dan penyediaan di Pusat Identitas IAM

IAM Identity Center memungkinkan Anda mengontrol siapa yang dapat masuk dan sumber daya apa yang dapat mereka akses. Pengguna harus disediakan untuk masuk. Anda kemudian dapat menetapkan akses hanya untuk pengguna atau grup yang disediakan. Pelajari tentang pengguna, grup, dan penyediaan di Pusat Identitas IAM.

Nama pengguna dan keunikan alamat email

Pusat Identitas IAM mengharuskan setiap pengguna memiliki nama pengguna yang unik. Nama pengguna adalah pengidentifikasi utama pengguna. Nama pengguna tidak harus cocok dengan alamat email pengguna. Pusat Identitas IAM mengharuskan semua nama pengguna dan alamat email untuk pengguna Anda tidak 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 grup bersarang (Grup dalam grup). Grup berguna saat menetapkan akses ke Akun AWS dan aplikasi. Alih-alih menetapkan setiap pengguna secara individual, Anda memberikan izin ke grup. Kemudian, saat Anda menambahkan 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

Penyediaan adalah proses membuat informasi pengguna dan grup tersedia untuk digunakan oleh Pusat Identitas IAM dan aplikasi yang dikelola atau aplikasi yang AWS dikelola pelanggan. Anda dapat membuat pengguna dan grup secara langsung di Pusat Identitas IAM atau menghubungkan sumber identitas Anda ke Pusat Identitas IAM. Dengan IAM Identity Center, Anda dapat menetapkan pengguna dan grup akses ke aplikasi yang terhubung dan Akun AWS.

Penyediaan di Pusat Identitas IAM bervariasi berdasarkan sumber identitas yang Anda gunakan. Untuk informasi selengkapnya, lihat [Kelola sumber identitas Anda](#).

Penghapusan penyediaan pengguna dan grup

Deprovisioning adalah proses menghapus pengguna dan informasi grup dari Pusat Identitas IAM.

Jika Anda menggunakan Active Directory atau penyedia identitas eksternal dengan Pusat Identitas IAM, Anda harus menghapus pengguna dan grup dari sumber identitas ini daripada Pusat Identitas IAM. Menghapus pengguna dan grup IAM Identity Center tidak akan sepenuhnya menghapusnya jika sumber identitas Anda adalah Active Directory atau penyedia identitas eksternal.

Jika Anda perlu menghentikan penyediaan pengguna atau grup Pusat Identitas IAM, Anda harus terlebih dahulu [menghapus penugasan kumpulan izin](#) atau aplikasi ke pengguna atau grup yang ingin Anda hapus penyediaan. Jika tidak, Anda akan memiliki kumpulan izin dan penugasan aplikasi yang tidak ditetapkan di Pusat Identitas IAM 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 Akun AWS, aplikasi, atau keduanya.

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

- [Penyedia identitas eksternal](#) — Pilih opsi ini jika Anda ingin mengelola pengguna di penyedia identitas eksternal (iDP) seperti Okta atau Microsoft Entra ID
- [Direktori Aktif Anda di tempat atau AWS terkelola](#) — Pilih opsi ini jika Anda ingin menghubungkan Active Directory (AD).
- [Direktori Pusat Identitas](#) - Ketika Anda mengaktifkan Pusat Identitas IAM untuk pertama kalinya, secara otomatis dikonfigurasi dengan direktori Pusat Identitas sebagai sumber identitas default. Anda kecuali Anda memilih sumber identitas yang berbeda. Dengan direktori Pusat Identitas, Anda membuat pengguna dan grup, dan menetapkan tingkat akses mereka ke aplikasi Akun AWS dan Anda.

 Note

IAM Identity Center tidak mendukung Simple AD SAMBA4 berbasis sebagai sumber identitas.

Topik

- [Pertimbangan untuk mengubah sumber identitas Anda](#)
- [Ubah sumber identitas Anda](#)
- [Atribut pengguna dan grup yang didukung di Pusat Identitas IAM](#)
- [Penyedia identitas eksternal](#)
- [Microsoft AD direktori](#)

Pertimbangan untuk mengubah sumber identitas Anda

Meskipun Anda dapat mengubah sumber identitas kapan saja, sebaiknya 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 penugasan pengguna dan grup yang Anda konfigurasi di Pusat Identitas IAM. Jika ini terjadi, semua pengguna, termasuk pengguna administratif di Pusat Identitas IAM, akan kehilangan akses masuk tunggal ke aplikasi mereka Akun AWS .

Sebelum Anda mengubah sumber identitas untuk Pusat Identitas IAM, tinjau pertimbangan berikut sebelum melanjutkan. Jika Anda ingin melanjutkan dengan mengubah sumber identitas Anda, lihat [Ubah sumber identitas Anda](#) untuk informasi selengkapnya.

Mengubah antara direktori Pusat Identitas IAM dan Direktori Aktif

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

Important

Saat mengubah jenis sumber identitas Anda di Pusat Identitas IAM ke atau dari Active Directory, ketahuilah bahwa Identity Store ID akan berubah. Ini dapat memiliki implikasi sebagai berikut:

- URL portal AWS akses default Anda akan berubah. Anda perlu mengkomunikasikan URL baru kepada tenaga kerja Anda dan memperbarui bookmark, daftar izin gateway atau firewall, dan konfigurasi tempat URL ini direferensikan. Kami menyarankan Anda melakukan perubahan ini di jendela pemeliharaan terjadwal untuk meminimalkan gangguan pada pengguna Anda.
- Jika Anda menggunakan kunci KMS yang dikelola pelanggan untuk enkripsi saat diam di Pusat Identitas IAM, dan telah mengonfigurasi kebijakan kunci KMS dengan konteks enkripsi, ketahuilah bahwa konteks enkripsi untuk Identity Store akan berubah. Misalnya, di Identity Store ARN `"arn:aws:identitystore: :123456789012: -922763e9b3", "d-922763e9b3"` adalah Identity Store ID. `identitystore/d` Untuk mencegah gangguan layanan selama transisi ini, ubah sementara kebijakan kunci KMS Anda untuk menggunakan pola wildcard: `"arn:aws:identitystore: :123456789012:identitystore/*"`.

Jika Anda sudah mengelola pengguna dan grup di direktori Identity Center default, pertimbangkan hal berikut:

- Tugas dihapus dan pengguna serta grup dihapus — Mengubah sumber identitas Anda ke Active Directory akan 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, lalu menerapkan kembali penugasannya.

Jika memilih untuk tidak menggunakan Active Directory, Anda harus membuat pengguna dan grup di direktori Pusat Identitas, lalu membuat penugasan.

- Tugas 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 [Buat, Perbarui, dan Hapus](#) API dengan hati-hati. Pusat Identitas IAM tidak mendukung sinkronisasi keluar, sehingga sumber identitas Anda tidak secara otomatis memperbarui dengan perubahan yang Anda buat pada pengguna atau grup menggunakan API ini.
- URL portal akses akan berubah — Mengubah sumber identitas Anda antara Pusat Identitas IAM dan Direktori Aktif juga mengubah URL untuk portal AWS akses.
- Jika pengguna dihapus atau dinonaktifkan di konsol Pusat Identitas IAM menggunakan API Identity Store, pengguna dengan sesi aktif dapat terus mengakses aplikasi dan akun terintegrasi. Untuk informasi tentang durasi sesi otentikasi dan perilaku pengguna, lihat [Memahami sesi otentikasi di Pusat Identitas IAM](#).
- Multi-Region dukungan — Jika Anda telah mereplikasi Pusat Identitas IAM ke Wilayah tambahan atau berencana untuk melakukannya, Anda harus menggunakan penyedia identitas eksternal atau direktori Pusat Identitas sebagai sumber identitas. Multi-Region dukungan tidak tersedia untuk Active Directory. Untuk informasi lebih lanjut termasuk prasyarat lainnya, lihat [Menggunakan Pusat Identitas IAM di beberapa Wilayah AWS](#).

Untuk informasi tentang cara IAM Identity Center menyediakan pengguna dan grup, lihat [Microsoft AD direktori](#).

Mengubah dari Pusat Identitas IAM ke IdP eksternal

Jika Anda mengubah sumber identitas Anda dari Pusat Identitas IAM menjadi penyedia identitas eksternal (IdP), pertimbangkan hal berikut:

- Tugas dan keanggotaan bekerja dengan pernyataan yang benar — tugas pengguna, tugas grup, dan keanggotaan grup Anda terus berfungsi selama IdP baru mengirimkan pernyataan yang benar

(misalnya, SAML NameID). Pernyataan ini harus sesuai 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 memperbarui 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 ke menggunakan Pusat Identitas IAM kapan saja. Lihat [Mengubah dari IdP eksternal ke Pusat Identitas IAM](#).
- Sesi pengguna yang ada dicabut saat durasi sesi berakhir — Setelah Anda mengubah sumber identitas Anda menjadi penyedia identitas eksternal, sesi pengguna aktif akan bertahan selama sisa durasi sesi maksimum yang dikonfigurasi di konsol. Misalnya, jika durasi sesi portal AWS akses diatur ke delapan jam, dan Anda mengubah sumber identitas pada jam keempat, sesi pengguna aktif akan bertahan selama empat jam tambahan. Untuk mencabut sesi pengguna, lihat [the section called “Akhir sesi aktif untuk pengguna tenaga kerja”](#).

Jika pengguna dihapus atau dinonaktifkan di konsol Pusat Identitas IAM menggunakan API Identity Store, pengguna dengan sesi aktif dapat terus mengakses aplikasi dan akun terintegrasi. Untuk informasi tentang durasi sesi otentikasi dan perilaku pengguna, lihat [Memahami sesi otentikasi di Pusat Identitas IAM](#).

Note

Anda tidak dapat mencabut sesi pengguna dari konsol Pusat Identitas IAM setelah Anda menghapus pengguna.

Untuk informasi tentang cara IAM Identity Center menyediakan pengguna dan grup, lihat [Penyedia identitas eksternal](#).

Mengubah dari IdP eksternal ke Pusat Identitas IAM

Jika Anda mengubah sumber identitas Anda dari penyedia identitas eksternal (IdP) ke Pusat Identitas IAM, pertimbangkan hal berikut:

- Pusat Identitas IAM mempertahankan semua tugas Anda.
- Paksa reset kata sandi — Pengguna yang memiliki kata sandi di Pusat Identitas IAM dapat terus 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.
- Sesi pengguna yang ada dicabut pada durasi sesi berakhir — Setelah Anda mengubah sumber identitas Anda ke Pusat Identitas IAM, sesi pengguna aktif akan bertahan selama sisa durasi sesi maksimum yang dikonfigurasi di konsol. Misalnya, jika durasi sesi portal AWS akses adalah delapan jam, dan Anda mengubah sumber identitas pada jam keempat, sesi pengguna aktif terus berjalan selama empat jam tambahan. Untuk mencabut sesi pengguna, lihat [the section called “Akhiri sesi aktif untuk pengguna tenaga kerja”](#).

Jika pengguna dihapus atau dinonaktifkan di konsol Pusat Identitas IAM menggunakan API Identity Store, pengguna dengan sesi aktif dapat terus mengakses aplikasi dan akun terintegrasi. Untuk informasi tentang durasi sesi otentikasi dan perilaku pengguna, lihat [Memahami sesi otentikasi di Pusat Identitas IAM](#).

 Note

Anda tidak akan dapat mencabut sesi pengguna dari konsol Pusat Identitas IAM setelah Anda menghapus pengguna.

Untuk informasi tentang cara IAM Identity Center menyediakan pengguna dan grup, lihat [Mengelola pengguna di direktori Pusat Identitas](#).

Mengubah dari satu IdP eksternal ke IdP eksternal lainnya

Jika Anda sudah menggunakan IdP eksternal sebagai sumber identitas untuk Pusat Identitas IAM dan Anda mengubah ke IdP eksternal yang berbeda, pertimbangkan hal berikut:

- Tugas dan keanggotaan bekerja dengan pernyataan yang benar — Pusat Identitas IAM mempertahankan semua tugas Anda. Tugas pengguna, penugasan grup, dan keanggotaan grup terus berfungsi selama IdP baru mengirimkan pernyataan yang benar (misalnya, SAML NameID).

Pernyataan ini harus cocok dengan nama pengguna di Pusat Identitas IAM saat pengguna Anda melakukan otentikasi melalui IdP eksternal baru.

- Penyediaan SCIM — Jika Anda menggunakan SCIM untuk penyediaan ke Pusat Identitas IAM, kami sarankan Anda meninjau IdP-specific informasi dalam panduan ini dan dokumentasi yang

disediakan oleh IdP untuk memastikan bahwa penyedia baru mencocokkan pengguna dan grup dengan benar saat SCIM diaktifkan.

- Sesi pengguna yang ada dicabut pada durasi sesi berakhir — Setelah Anda mengubah sumber identitas Anda ke penyedia identitas eksternal yang berbeda, sesi pengguna aktif akan bertahan selama sisa durasi sesi maksimum yang dikonfigurasi di konsol. Misalnya, jika durasi sesi portal AWS akses adalah delapan jam, dan Anda mengubah sumber identitas pada jam keempat, sesi pengguna aktif akan bertahan selama empat jam tambahan. Untuk mencabut sesi pengguna, lihat [the section called “Akhiri sesi aktif untuk pengguna tenaga kerja”](#).

Jika pengguna dihapus atau dinonaktifkan di konsol Pusat Identitas IAM menggunakan API Identity Store, pengguna dengan sesi aktif dapat terus mengakses aplikasi dan akun terintegrasi. Untuk informasi tentang durasi sesi otentikasi dan perilaku pengguna, lihat [Memahami sesi otentikasi di Pusat Identitas IAM](#).

Note

Anda tidak dapat mencabut sesi pengguna dari konsol Pusat Identitas IAM setelah Anda menghapus pengguna.

Untuk informasi tentang cara IAM Identity Center menyediakan pengguna dan grup, lihat [Penyedia identitas eksternal](#).

Mengubah antara Active Directory dan IdP eksternal

Jika Anda mengubah sumber identitas Anda 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 Active Directory.
- Penyediaan pengguna — Jika Anda mengubah ke IdP eksternal, Anda harus mengonfigurasi Pusat Identitas IAM untuk menyediakan pengguna Anda. Atau, Anda harus menyediakan pengguna dan grup untuk IdP eksternal secara manual sebelum Anda dapat mengonfigurasi tugas.
- Membuat 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.

- Jika pengguna dihapus atau dinonaktifkan di konsol Pusat Identitas IAM menggunakan API Identity Store, pengguna dengan sesi aktif dapat terus mengakses aplikasi dan akun terintegrasi. Untuk informasi tentang durasi sesi otentikasi dan perilaku pengguna, lihat [Memahami sesi otentikasi di Pusat Identitas IAM](#).
- Multi-Region dukungan — Jika Anda telah mereplikasi Pusat Identitas IAM ke Wilayah tambahan atau berencana untuk melakukannya, Anda harus menggunakan penyedia identitas eksternal atau direktori Pusat Identitas sebagai sumber identitas. Multi-Region dukungan tidak tersedia untuk Active Directory. Untuk informasi lebih lanjut termasuk prasyarat lainnya, lihat [Menggunakan Pusat Identitas IAM di beberapa Wilayah AWS](#).

Untuk informasi tentang cara IAM Identity Center menyediakan pengguna dan grup, lihat [Microsoft AD direktori](#).

Ubah sumber identitas Anda

Prosedur berikut menjelaskan cara mengubah dari direktori yang disediakan IAM Identity Center (direktori Identity Center default) ke Active Directory atau penyedia identitas eksternal, atau sebaliknya. Sebelum Anda melanjutkan, tinjau informasi di [Pertimbangan untuk mengubah sumber identitas Anda](#). Untuk menyelesaikan prosedur ini, Anda memerlukan instance Organisasi dari Pusat Identitas IAM. Untuk informasi selengkapnya, lihat [Instans organisasi dan akun dari Pusat Identitas IAM](#).

Warning

Bergantung pada penerapan Anda saat ini, perubahan ini menghapus tugas pengguna dan grup yang Anda konfigurasi di Pusat Identitas IAM. Perubahan ini juga akan menghapus peran IAM set izin dari Anda Akun AWS. Akibatnya, Anda mungkin perlu memperbarui kebijakan sumber daya Anda, dan harus memastikan ini tidak akan mengganggu akses Anda ke AWS KMS kunci dan cluster Amazon EKS. Untuk mempelajari selengkapnya, lihat [Mereferensikan kumpulan izin dalam kebijakan sumber daya, peta konfigurasi Cluster Amazon EKS, dan AWS KMS kebijakan utama](#).

Jika hal ini terjadi, semua pengguna dan grup, termasuk pengguna administratif di Pusat Identitas IAM, akan kehilangan akses masuk tunggal ke aplikasi mereka Akun AWS .

Untuk mengubah sumber identitas Anda

1. Buka konsol [Pusat Identi](#) tas IAM.
2. Pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Sumber identitas. Pilih Tindakan, lalu pilih Ubah sumber identitas.
4. Di bawah Pilih sumber identitas, pilih sumber yang ingin Anda ubah, lalu pilih Berikutnya.

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 akan menghapus pengguna dan grup dari direktori Pusat Identitas. Perubahan ini juga menghapus tugas yang Anda konfigurasi di Pusat Identitas IAM.

Note

Jika Anda mereplikasi Pusat Identitas IAM ke Wilayah tambahan dan ingin mengubah sumber identitas Anda ke Active Directory, Anda harus menghapus semua Wilayah tambahan terlebih dahulu. Multi-Region dukungan tidak tersedia untuk instans yang menggunakan Active Directory sebagai sumber identitas. Untuk informasi selengkapnya, lihat [Menggunakan Pusat Identitas IAM di beberapa Wilayah AWS](#)

Jika Anda beralih ke penyedia identitas eksternal, kami sarankan Anda mengikuti langkah-langkah di [Cara terhubung ke penyedia identitas eksternal](#).

5. Setelah Anda membaca penafian dan siap untuk melanjutkan, ketik **ACCEPT**.
6. Pilih Ubah 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 ke halaman Pengaturan. Pada halaman Pengaturan, lakukan salah satu hal berikut:
 - Pilih Mulai pengaturan yang dipandu. Untuk informasi tentang cara menyelesaikan proses penyiapan yang dipandu, lihat [Pengaturan terpandu](#).

- Di bagian Sumber identitas, pilih Tindakan, lalu pilih Kelola sinkronisasi untuk mengonfigurasi cakupan sinkronisasi Anda, daftar pengguna dan grup yang akan disinkronkan.

Atribut pengguna dan grup yang didukung di Pusat Identitas IAM

Panduan ini memberikan referensi untuk dukungan atribut SCIM di IAM Identity Center. Ini mencantumkan atribut pengguna dan grup mana dari spesifikasi SCIM yang didukung di penyimpanan identitas Pusat Identitas IAM, dan mengidentifikasi atribut dan sub-atribut tertentu yang tidak didukung.

Atribut adalah potongan informasi yang membantu Anda menentukan dan mengidentifikasi pengguna individu atau objek grup, seperti `name`, `email`, atau `members`. IAM Identity Center mendukung atribut yang paling umum digunakan melalui entri manual dan penyediaan SCIM otomatis.

- Untuk informasi tentang spesifikasi Sistem untuk Manajemen Identitas Lintas Domain (SCIM), lihat <https://tools.ietf.org/html/rfc7642>.
- Untuk informasi tentang penyediaan manual dan otomatis, lihat [Penyediaan saat pengguna berasal dari iDP eksternal](#)
- Untuk informasi tentang pemetaan atribut, lihat [Pemetaan atribut antara Pusat Identitas IAM dan direktori Penyedia Identitas 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 tidak didukung

Semua atribut dari skema pengguna SCIM (<https://tools.ietf.org/html/rfc7643#section-8.3>) didukung di penyimpanan identitas Pusat Identitas IAM, kecuali 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 tidak didukung

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`).

Penyedia identitas eksternal

Dengan IAM Identity Center, Anda dapat menghubungkan identitas tenaga kerja yang ada dari penyedia identitas eksternal (IdPs) melalui protokol Security Assertion Markup Language (SAMP) 2.0 dan System for Cross-Domain Identity Management (SCIM). Ini memungkinkan pengguna Anda untuk masuk ke portal AWS akses dengan kredensial 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 atau Microsoft 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 kredensial jangka pendek otomatis.

Jika Anda menggunakan direktori yang dikelola sendiri di Direktori Aktif atau direktori AWS Managed Microsoft AD, lihat [Microsoft AD direktori](#).

 Note

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 [Menyediakan pengguna dan grup dari penyedia identitas eksternal menggunakan SCIM](#) untuk pengguna dan grup Anda, atau gunakan [Penyediaan manual](#). Terlepas dari bagaimana Anda menyediakan pengguna, IAM Identity Center mengalihkan, antarmuka baris perintah Konsol Manajemen AWS, 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](#)

Topik

- [Cara terhubung ke penyedia identitas eksternal](#)
- [Cara mengubah metadata penyedia identitas eksternal di IAM Identity Center](#)
- [Menggunakan federasi identitas SAMP dan SCIM dengan penyedia identitas eksternal](#)
- [Profil SCIM dan implementasi SAMP 2.0](#)

Cara terhubung ke penyedia identitas eksternal

Ada berbagai prasyarat, pertimbangan, dan prosedur penyediaan untuk eksternal yang didukung. IdPs Ada tutorial langkah demi langkah yang tersedia untuk beberapa IdPs:

- [CyberArk](#)
- [Google Workspace](#)
- [JumpCloud](#)
- [Microsoft Entra ID](#)
- [Okta](#)
- [OneLogin](#)

- [Identitas Ping](#)

Untuk informasi lebih lanjut tentang pertimbangan eksternal IdPs yang didukung IAM Identity Center, lihat. [Menggunakan federasi identitas SAMP dan SCIM dengan penyedia identitas eksternal](#)

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.

 Note

File metadata SAMP yang Anda unduh berisi URL dual-stack assertion consumer service (ACS). IPv4-only Selanjutnya, jika Pusat Identitas IAM Anda direplikasi ke Wilayah tambahan, file metadata berisi URL ACS untuk setiap Wilayah tambahan. Jika IDP eksternal Anda memiliki batasan jumlah URL ACS, Anda harus menghapus URL ACS yang tidak perlu. Misalnya, jika organisasi Anda telah sepenuhnya mengadopsi titik akhir dual-stack dan tidak lagi menggunakannya, Anda dapat menghapus IPv4-only yang terakhir. Pendekatan alternatif adalah tidak menggunakan file metadata tetapi untuk menyalin dan menempelkan URL ACS ke IDP eksternal.

- 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.

Cara mengubah metadata penyedia identitas eksternal di IAM Identity Center

Anda dapat mengubah metadata penyedia identitas eksternal yang sebelumnya Anda berikan ke Pusat Identitas IAM. Perubahan ini memengaruhi kemampuan pengguna Anda untuk masuk dan mengakses AWS sumber daya melalui Pusat Identitas IAM. Prosedur berikut menjelaskan cara memperbarui metadata eksternal IDP Anda yang disimpan di IAM Identity Center. Untuk menyelesaikan prosedur ini, Anda memerlukan instance Organisasi dari IAM Identity Center. Untuk informasi selengkapnya, lihat [Instans organisasi dan akun dari Pusat Identitas IAM](#).

Untuk mengubah metadata penyedia identitas eksternal

1. Buka [konsol Pusat Identitas IAM](#).
2. Pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Sumber identitas. Pilih Tindakan dan kemudian pilih Kelola Otentikasi.
4. Di bagian metadata penyedia identitas, pilih Edit metadata iDP. Anda dapat membuat perubahan pada URL masuk IDP dan atau URL penerbit iDP untuk iDP eksternal Anda di halaman ini. Pilih Simpan perubahan ketika Anda telah membuat semua perubahan yang diperlukan.

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>) sesuai spesifikasi `addr-(" ") (#section -3.4.1). name@domain.com` <https://tools.ietf.org/html/rfc2822>
 - SubjectNameIDNilai pernyataan SAMP harus sama persis dengan Nama Pengguna pengguna yang disediakan di Pusat Identitas IAM. Sign-in gagal jika IAM Identity Center tidak dapat mencocokkan NameID ke Nama Pengguna, bahkan ketika IDP eksternal berhasil mengautentikasi pengguna.
 - 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.
 - IAM Identity Center tidak mendukung penandatanganan permintaan otentikasi SAMP yang dikirim ke eksternal. IdPs
 - IDP harus mendukung beberapa URL layanan konsumen assertion (ACS) jika Anda berencana untuk mereplikasi Pusat Identitas IAM ke Wilayah tambahan, dan sepenuhnya memanfaatkan manfaat Pusat Identitas IAM Multi-wilayah. Untuk informasi selengkapnya, lihat [Menggunakan Pusat Identitas IAM di beberapa Wilayah AWS](#). Menggunakan satu URL ACS dapat memengaruhi pengalaman pengguna di Wilayah tambahan. Wilayah utama Anda akan terus berfungsi secara normal. Untuk informasi selengkapnya tentang pengalaman pengguna di Wilayah tambahan dengan satu URL ACS, lihat [the section called “Penggunaan AWS aplikasi yang dikelola tanpa beberapa URL ACS”](#) dan [the section called “Akun AWS akses ketahanan tanpa beberapa URL ACS”](#).
- SCIM
 - Implementasi IAM Identity Center SCIM didasarkan pada SCIM RFC 7642 (<https://tools.ietf.org/html/rfc7642>), 7643 (), dan 7644 (<https://tools.ietf.org/html/rfc7643><https://tools.ietf.org/html/>

[rfc7644](#)), dan persyaratan interoperabilitas yang ditetapkan dalam draf Maret 2020 dari Profil SCIM Dasar 1.0 ([#rfc .section.4](#)). FastFed https://openid.net/specs/fastfed-scim-1_0-02.html

Setiap perbedaan antara dokumen-dokumen ini dan implementasi saat ini di IAM Identity Center dijelaskan di bagian [Operasi API yang Didukung](#) dari IAM Identity Center SCIM Implementation Developer Guide.

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 acara ExternalIdPDirectoryLogin
- IdP-specific log and/or debug log
- [Memecahkan masalah Pusat Identitas IAM](#)

Note

Beberapa IdPs, seperti yang ada di [Tutorial sumber identitas Pusat Identitas IAM](#), 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 generik serupa “AWS” dapat menggunakan and/or titik akhir pendekatan federasi 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 Konsol Manajemen AWS dan pihak ketiga seperti Microsoft 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, lihat [Menyediakan pengguna dan grup dari penyedia identitas eksternal menggunakan SCIM](#). Untuk detail tambahan tentang implementasi SCIM IAM Identity Center, lihat Panduan Pengembang Implementasi [SCIM Pusat Identitas IAM](#).

Topik

- [Menyediakan pengguna dan grup dari penyedia identitas eksternal menggunakan SCIM](#)
- [Putar sertifikat SAMP 2.0](#)

Menyediakan pengguna dan grup dari penyedia identitas eksternal menggunakan SCIM

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](#)
- [IdentityStore Akses API dengan penyediaan SCIM](#)
- [Cara memantau kedaluwarsa token akses](#)
- [Menghasilkan token akses](#)
- [Aktifkan penyediaan otomatis](#)
- [Hapus token akses](#)
- [Nonaktifkan penyediaan otomatis](#)
- [Putar token akses](#)
- [Audit dan rekonsiliasi sumber daya yang disediakan secara otomatis](#)
- [Penyediaan manual](#)

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 [Tutorial sumber identitas Pusat Identitas IAM](#) 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 pengenalan masuk unik non-Null pengguna ke atribut nama pengguna IAM Identity Center. Periksa untuk melihat apakah IDP Anda memiliki nilai tunggal yang merupakan pengenalan 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.
- Untuk SCIM-provisioned pengguna, pastikan atribut yang dikirim idP Anda karena SAMP Subject NameID adalah atribut yang sama dengan yang Anda petakan ke Nama Pengguna dalam konfigurasi SCIM Anda. Jika berbeda, login gagal.
- 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 pengenalan 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.
- Setelah menyiapkan penyediaan otomatis dengan SCIM untuk IDP Anda, Anda tidak dapat lagi menambahkan atau mengedit pengguna di konsol Pusat Identitas IAM. Jika Anda perlu menambahkan atau memodifikasi pengguna, Anda harus melakukannya dari IDP eksternal atau sumber identitas Anda.

Untuk informasi selengkapnya tentang implementasi SCIM IAM Identity Center, lihat Panduan Pengembang Implementasi [IAM Identity Center SCIM](#).

IdentityStore Akses API dengan penyediaan SCIM

Saat Anda mengonfigurasi penyediaan SCIM dari iDP eksternal, API Identity Store yang memungkinkan untuk mengubah pengguna dan keanggotaan grup tetap dapat diakses. Prinsipal di akun manajemen dan akun administrator yang didelegasikan dapat memanggil mereka.

Ada alasan yang valid untuk menggunakan API ini bersama SCIM. Misalnya, beberapa IdPs seperti Google Workspace tidak mendukung penyediaan grup SCIM, dan mengharuskan Anda [membuat dan mengelola grup secara manual](#) melalui Identity Store API. Kasus penggunaan lainnya termasuk menonaktifkan pengguna yang cepat dan grup pra-penyediaan sebelum sinkronisasi IDP.

Important

Jika organisasi Anda tidak memerlukan akses API langsung, ketahuilah bahwa menggunakan mutasi Identity Store API pada SCIM-provisioned direktori dapat menyebabkan direktori di IAM Identity Center hanyut dari iDP eksternal Anda. Sinkronisasi SCIM beroperasi pada delta dari sumber iDP. Ini berarti perubahan yang dilakukan melalui API mungkin tidak diperbaiki oleh sinkronisasi SCIM berikutnya. Hal ini dapat mengakibatkan:

- Pengguna atau keanggotaan grup di IAM Identity Center yang tidak cocok dengan IDP eksternal Anda, melanggar harapan bahwa iDP adalah satu-satunya sumber kebenaran.
- Eskalasi hak istimewa yang tidak diinginkan jika kepala sekolah menambahkan diri mereka sendiri atau orang lain ke grup yang memberikan akses atau aplikasi. Akun AWS
- Kesenjangan audit dan kepatuhan, karena tinjauan hak yang dilakukan terhadap IDP eksternal mungkin tidak mencerminkan keadaan aktual akses. AWS

Jika Anda ingin mencegah API-based mutasi, lampirkan kebijakan kontrol layanan (SCP) ke akun administrator yang didelegasikan. Perhatikan bahwa SCP tidak berlaku untuk akun manajemen itu sendiri.

Contoh SCP berikut menyangkal semua tindakan Identity Store yang bermutasi:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyIdentityStoreMutations",
      "Effect": "Deny",
```

```
"Action": [  
  "identitystore:Create*",  
  "identitystore:Update*",  
  "identitystore:Delete*"  
],  
"Resource": "*" ]  
}
```

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.

Menghasilkan token akses

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 [Aktifkan 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.

Aktifkan 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 [Tutorial sumber identitas Pusat Identitas IAM](#) 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. Di kotak dialog penyediaan otomatis masuk, salin titik akhir SCIM dan token akses. Anda harus menempelkannya nanti saat mengonfigurasi penyediaan di iDP Anda.
 - a. Titik akhir SCIM - Misalnya, `.amazonaws.com//https://scim.us-east-211111111111-2222-3333-4444-555555555555scim/v2`
 - b. Token akses - Pilih Tampilkan token untuk menyalin nilainya.

Warning

Ini adalah satu-satunya waktu di mana Anda dapat memperoleh titik akhir SCIM dan token akses. Pastikan Anda menyalin nilai-nilai ini sebelum bergerak maju. Anda akan

memasukkan nilai-nilai ini untuk mengkonfigurasi penyediaan otomatis di IDP Anda nanti dalam tutorial ini.

5. Pilih Tutup.

Setelah Anda menyelesaikan prosedur ini, Anda harus mengonfigurasi penyediaan otomatis di IDP Anda. Untuk informasi selengkapnya, lihat [Tutorial sumber identitas Pusat Identitas IAM](#) untuk IDP Anda.

Hapus 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.

Nonaktifkan 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 [Hapus 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.

Putar 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 [Menghasilkan token akses](#) 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 konfigurasi 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 [Hapus token akses](#) untuk menghapus token akses lama yang Anda catat sebelumnya. Anda juga dapat menggunakan tanggal pembuatan token sebagai petunjuk token mana yang akan dihapus.

Audit dan rekonsiliasi sumber daya yang disediakan secara otomatis

SCIM memungkinkan Anda untuk secara otomatis menyediakan pengguna, grup, dan keanggotaan grup dari sumber identitas Anda ke IAM Identity Center. Panduan ini membantu Anda memverifikasi dan mendamaikan sumber daya ini untuk mempertahankan sinkronisasi yang akurat.

Mengapa mengaudit sumber daya Anda?

Audit rutin membantu memastikan kontrol akses Anda tetap akurat dan penyedia identitas (IDP) Anda tetap disinkronkan dengan Pusat Identitas IAM dengan benar. Ini sangat penting untuk kepatuhan keamanan dan manajemen akses.

Sumber daya yang dapat Anda audit:

- Pengguna
- Grup
- Keanggotaan grup

Anda dapat menggunakan AWS Identity Store [API](#) atau [perintah CLI](#) untuk melakukan audit dan rekonsiliasi. Contoh berikut menggunakan AWS CLI perintah. Untuk alternatif API, lihat [operasi terkait](#) dalam referensi Identity Store API.

Cara mengaudit sumber daya

Berikut adalah contoh cara mengaudit sumber daya ini menggunakan AWS CLI perintah.

Sebelum Anda mulai, pastikan Anda memiliki:

- Akses administrator ke Pusat Identitas IAM.
- AWS CLI diinstal dan dikonfigurasi. Untuk selengkapnya, lihat [Panduan Pengguna Antarmuka Baris AWS Perintah](#).
- Izin IAM yang diperlukan untuk perintah Identity Store.

Langkah 1: Daftar sumber daya saat ini

Anda dapat melihat sumber daya Anda saat ini menggunakan AWS CLI.

Note

Saat menggunakan AWS CLI, pagination ditangani secara otomatis kecuali Anda menentukan. `--no-paginate` Jika Anda memanggil API secara langsung (misalnya, dengan SDK atau skrip khusus), tangani `NextToken` respons tersebut. Ini memastikan Anda mengambil semua hasil di beberapa halaman.

Example untuk pengguna

```
aws identitystore list-users \  
  --region REGION \  
  --identity-store-id IDENTITY_STORE_ID
```


Example untuk kelompok

```
aws identitystore list-groups \  
  --region REGION \  
  --identity-store-id IDENTITY_STORE_ID
```

Example untuk keanggotaan grup

```
aws identitystore list-group-memberships \  
  --region REGION \  
  --identity-store-id IDENTITY_STORE_ID \  
  --group-id GROUP_ID
```

Langkah 2: Bandingkan dengan sumber identitas Anda

Bandinkan sumber daya yang terdaftar dengan sumber identitas Anda untuk mengidentifikasi perbedaan apa pun, seperti:

- Sumber daya yang hilang yang harus disediakan di Pusat Identitas IAM.
- Sumber daya tambahan yang harus dihapus dari IAM Identity Center.

Example untuk pengguna

```
# Create missing users  
aws identitystore create-user \  
  --identity-store-id IDENTITY_STORE_ID \  
  --user-name USERNAME \  
  --display-name DISPLAY_NAME \  
  --name GivenName=FIRST_NAME,FamilyName=LAST_NAME \  
  --emails Value=EMAIL,Primary=true  
  
# Delete extra users  
aws identitystore delete-user \  
  --identity-store-id IDENTITY_STORE_ID \  
  --user-id USER_ID
```

Example untuk kelompok

```
# Create missing groups  
aws identitystore create-group \  
  --identity-store-id IDENTITY_STORE_ID \  
  --group-name GROUP_NAME
```

```
--identity-store-id IDENTITY_STORE_ID \  
[group attributes]  
  
# Delete extra groups  
aws identitystore delete-group \  
  --identity-store-id IDENTITY_STORE_ID \  
  --group-id GROUP_ID
```

Example untuk keanggotaan grup

```
# Add missing members  
aws identitystore create-group-membership \  
  --identity-store-id IDENTITY_STORE_ID \  
  --group-id GROUP_ID \  
  --member-id '{"UserId": "USER_ID"}'  
  
# Remove extra members  
aws identitystore delete-group-membership \  
  --identity-store-id IDENTITY_STORE_ID \  
  --membership-id MEMBERSHIP_ID
```

Pertimbangan-pertimbangan

- Perintah tunduk pada [kuota layanan dan pembatasan API](#).
- Ketika Anda menemukan banyak perbedaan selama rekonsiliasi, buat perubahan kecil dan bertahap ke Identity Store. AWS Ini membantu Anda menghindari kesalahan yang memengaruhi banyak pengguna.
- Sinkronisasi SCIM dapat mengganti perubahan manual Anda. Periksa pengaturan IDP Anda untuk memahami perilaku ini.

Penyediaan manual

Beberapa IdPs tidak memiliki dukungan Sistem untuk Manajemen Cross-domain Identitas (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 [Nama pengguna dan keunikan 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](#).

Putar 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 X.509 sertifikat SAMP 2.0 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](#)
- [Indikator status kedaluwarsa sertifikat](#)

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 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

Halaman Kelola sertifikat SAMP 2.0 menampilkan ikon indikator status berwarna di kolom Kedaluwarsa pada 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 kedaluwarsa.
- Kuning - Menunjukkan bahwa sertifikat kedaluwarsa dalam 90 hari atau kurang.
- Hijau - Menunjukkan bahwa sertifikat valid dan tetap berlaku setidaknya 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.

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 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 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 Directory Service berada AWS Managed Microsoft AD dalam akun manajemen Anda. AWS Organizations
- IAM Identity Center tidak mendukung Simple AD berbasis SAMBA 4 sebagai direktori yang terhubung.
- IAM Identity Center tidak dapat menyinkronkan Prinsipal Keamanan Asing (FSP). Jika grup AWS Managed Microsoft AD berisi anggota dari domain tepercaya sebagai FSP, anggota tersebut tidak akan disinkronkan.

Untuk demonstrasi tentang proses menggunakan Active Directory sebagai sumber identitas untuk IAM Identity Center, lihat video berikut: [YouTube](#)

[Menggunakan Active Directory sebagai sumber identitas untuk AWS IAM Identity Center | Amazon Web Services](#)

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. Untuk informasi lebih lanjut, lihat:

- [Connect direktori di AWS Managed Microsoft AD ke Pusat Identitas IAM](#)
- [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 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.

 Note

IAM Identity Center tidak mendukung SAMBA4-based Simple AD sebagai sumber identitas.

AWS Managed Microsoft AD

1. Tinjau panduan di [Microsoft AD direktori](#).
2. Ikuti langkah-langkah di [Connect direktori di AWS Managed Microsoft AD ke Pusat Identitas IAM](#).
3. Konfigurasi 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](#).

Self-managed direktori di Active Directory

1. Tinjau panduan di [Microsoft AD direktori](#).
2. Ikuti langkah-langkah di [Connect direktori yang dikelola sendiri di Active Directory ke IAM Identity Center](#).
3. Konfigurasi 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 di [Penyedia identitas eksternal](#).
2. Ikuti langkah-langkah di [Cara terhubung ke penyedia identitas eksternal](#).
3. Konfigurasi 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 Active Directory ke IAM Identity Center, Anda dapat menentukan pengguna kepada siapa Anda ingin memberikan izin administratif, dan kemudian menyinkronkan pengguna tersebut dari direktori Anda ke IAM Identity Center.

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 [Membuat kumpulan izin](#).

Penyediaan saat pengguna berasal dari Active Directory

IAM Identity Center menggunakan koneksi yang disediakan oleh 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 di AWS Managed Microsoft AD ke Pusat Identitas IAM](#)
- [Connect direktori yang dikelola sendiri di Active Directory ke IAM Identity Center](#)
- [Pemetaan atribut antara Pusat Identitas IAM dan direktori Penyedia Identitas Eksternal](#)
- [Pusat Identitas IAM sinkronisasi AD yang dapat dikonfigurasi](#)

Connect direktori di AWS Managed Microsoft AD ke Pusat Identitas IAM

Gunakan prosedur berikut untuk menghubungkan direktori yang dikelola oleh AWS Directory Service IAM Identity Center. AWS Managed Microsoft AD

Untuk menghubungkan 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 kredensial perusahaan mereka ke berbagai layanan dan aplikasi bisnis. AWS One-way trust 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 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 Panduan AWS Directory Service Administrasi.

Note

Untuk menggunakan AWS aplikasi, seperti IAM Identity Center untuk membaca pengguna Directory Service direktori dari domain terpercaya, Directory Service akun memerlukan izin ke AccountControl atribut pengguna pada pengguna terpercaya. Tanpa izin baca untuk atribut ini, AWS aplikasi tidak dapat menentukan apakah akun diaktifkan atau dinonaktifkan.

Akses baca ke atribut ini disediakan secara default saat trust dibuat. Jika Anda menolak akses ke atribut ini (tidak disarankan), Anda akan merusak aplikasi seperti Identity Center agar tidak dapat membaca pengguna terpercaya. Solusinya adalah dengan secara khusus mengizinkan akses Baca ke userAccountControl atribut pada akun AWS layanan di bawah OU AWS Cadangan (diawali dengan AWS_).

- **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 Panduan AWS Directory Service Administrasi. Berikut ini adalah pertimbangan saat menggunakan AD Connector:
 - 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 Directory Service untuk Microsoft Active Directory.

Note

IAM Identity Center tidak bekerja dengan direktori SAMBA4-based Simple AD.

Pemetaan atribut antara Pusat Identitas IAM dan direktori Penyedia Identitas Eksternal

Pemetaan atribut digunakan untuk memetakan tipe atribut yang ada di Pusat Identitas IAM dengan atribut serupa di sumber identitas eksternal Anda seperti Google Workspace,, Microsoft Active Directory (AD) dan. Okta IAM Identity Center mengambil atribut pengguna dari sumber identitas Anda dan memetakannya ke atribut pengguna IAM Identity Center.

Jika Pusat Identitas IAM Anda disinkronkan untuk menggunakan penyedia identitas eksternal (iDP), seperti Google Workspace, Okta, atau Ping sebagai sumber identitas, Anda harus memetakan atribut Anda di IDP Anda.

IAM Identity Center mengisi ulang sekumpulan atribut untuk Anda di bawah tab pemetaan Atribut yang ditemukan di halaman konfigurasinya. IAM Identity Center menggunakan atribut pengguna ini untuk mengisi pernyataan SAMP (sebagai atribut SAMP) yang dikirim ke aplikasi. Atribut pengguna ini pada gilirannya diambil dari sumber identitas Anda. Setiap aplikasi menentukan daftar atribut SAMP 2.0 yang dibutuhkan untuk proses masuk tunggal yang berhasil. Untuk informasi selengkapnya, lihat [Memetakan atribut dalam aplikasi Anda ke atribut Pusat Identitas IAM](#).

IAM Identity Center juga mengelola serangkaian atribut untuk Anda di bawah bagian pemetaan Atribut dari halaman konfigurasi Active Directory jika Anda menggunakan Active Directory sebagai sumber identitas. Untuk informasi selengkapnya, lihat [Memetakan atribut pengguna antara IAM Identity Center dan Microsoft AD direktori](#).

Atribut penyedia identitas eksternal yang didukung

Tabel berikut mencantumkan semua atribut penyedia identitas eksternal (iDP) yang didukung dan 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}
```

Atribut yang didukung di IDP

```
${path:addresses[type eq "work"].region}
```

```
${path:addresses[type eq "work"].postalCode}
```

```
${path:addresses[type eq "work"].country}
```

```
${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 antara IAM Identity Center dan Microsoft AD

Tabel berikut mencantumkan pemetaan default untuk atribut pengguna di Pusat Identitas IAM ke atribut pengguna di direktori Anda. Microsoft AD Pusat Identitas IAM hanya mendukung daftar atribut dalam atribut Pengguna di kolom Pusat Identitas IAM.

Atribut pengguna di Pusat Identitas IAM	Peta ke atribut ini di Active Directory
displayname	\${displayname}
emails[?primary].value *	\${mail}
externalid	\${objectguid}
name.givenname	\${givenname}
name.familyname	\${sn}
name.middlename	\${initials}
sid	\${objectsid}
username	\${userprincipalname}

* Atribut email di IAM Identity Center harus unik dalam direktori.

Atribut grup di Pusat Identitas IAM	Peta ke atribut ini di Active Directory
externalid	\${objectguid}
description	\${description}
displayname	\${samaccountname}@{associateddomain}

Pertimbangan-pertimbangan

- Jika Anda tidak memiliki tugas untuk pengguna dan grup di Pusat Identitas IAM saat Anda mengaktifkan sinkronisasi AD yang dapat dikonfigurasi, pemetaan default di tabel sebelumnya akan digunakan. Untuk informasi tentang cara menyesuaikan pemetaan ini, lihat. [Konfigurasi pemetaan atribut untuk sinkronisasi Anda](#)
- 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, konfirmasi alur Pusat Identitas IAM dengan ketergantungan pada “nama pengguna” akan terus berfungsi seperti yang diharapkan, sebelum melakukan perubahan.

Didukung Microsoft AD atribut untuk Pusat Identitas IAM

Tabel berikut mencantumkan semua atribut Microsoft AD direktori yang didukung dan yang dapat dipetakan ke atribut pengguna di IAM Identity Center.

Atribut yang didukung di direktori Microsoft AD

`${samaccountname}`

`${description}`

`${objectguid}`

`${givenname}`

`${sn}`

`${initials}`

`${mail}`

`${userprincipalname}`

`${displayname}`

`${distinguishedname}`

`${proxyaddresses[?type == "SMTP"].value}`

`${proxyaddresses[?type == "smtp"].value}`

`${useraccountcontrol}`

Pertimbangan-pertimbangan

- Anda dapat menentukan kombinasi atribut Microsoft AD direktori yang didukung untuk dipetakan ke atribut tunggal yang dapat berubah di Pusat Identitas IAM.

Atribut Pusat Identitas IAM yang didukung untuk Microsoft AD

Tabel berikut mencantumkan semua atribut IAM Identity Center yang didukung dan yang dapat dipetakan ke atribut pengguna di direktori Anda 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 untuk Direktori Aktif

`${user:AD_GUID}`

`${user:AD_SID}`

`${user:email}`

`${user:familyName}`

`${user:givenName}`

`${user:middleName}`

`${user:name}`

`${user:preferredUsername}`

`${user:subject}`

Memetakan atribut pengguna antara IAM Identity Center dan Microsoft AD direktori

Anda dapat menggunakan prosedur berikut untuk menentukan bagaimana atribut pengguna Anda di Pusat Identitas IAM harus dipetakan ke atribut yang sesuai di Microsoft AD direktori 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 **mail** direktori Microsoft AD.
5. Pilih Simpan perubahan.

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.

- 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 AWS atau 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.

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 IAM Identity Center 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 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).

- 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 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](#)

Topik

- [Cara kerja sinkronisasi AD yang dapat dikonfigurasi](#)
- [Konfigurasi pemetaan atribut untuk sinkronisasi Anda](#)
- [First-time Pengaturan sinkronisasi Direktori Aktif ke Pusat Identitas IAM](#)
- [Menambahkan pengguna dan grup ke cakupan sinkronisasi](#)
- [Hapus pengguna dan grup dari cakupan sinkronisasi Anda](#)
- [Jeda dan lanjutkan sinkronisasi](#)
- [Otomatiskan konfigurasi sinkronisasi Anda untuk sinkronisasi AD yang dapat dikonfigurasi](#)

Cara kerja sinkronisasi AD yang dapat dikonfigurasi

IAM Identity Center menyegarkan data AD-based identitas di toko identitas dengan menggunakan proses berikut. Untuk mempelajari lebih lanjut tentang prasyarat, lihat. [Prasyarat dan pertimbangan](#)

Pembuatan

Setelah menghubungkan direktori yang dikelola sendiri di Active Directory atau AWS Managed Microsoft AD direktori yang dikelola oleh 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.

Anda hanya dapat menetapkan akses ke pengguna atau grup baru setelah mereka disinkronkan ke dalam 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.

Konfigurasi pemetaan atribut untuk sinkronisasi Anda

Untuk informasi selengkapnya tentang atribut yang tersedia, lihat [Pemetaan atribut antara Pusat Identitas IAM dan direktori Penyedia Identitas Eksternal](#).

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, konfigurasi 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.

First-time Pengaturan sinkronisasi Direktori Aktif ke Pusat Identitas IAM

Jika Anda menyinkronkan pengguna dan grup dari Active Directory ke IAM Identity Center untuk pertama kalinya, ikuti langkah-langkah ini. Atau, Anda dapat mengikuti langkah-langkah yang diuraikan [Ubah sumber identitas Anda](#) untuk mengubah sumber identitas Anda dari IAM Identity Center ke Active Directory.

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: Konfigurasi 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: Konfigurasi 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, konfirmasi 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

 Note

Saat menambahkan grup ke cakupan sinkronisasi Anda, sinkronkan grup langsung dari domain lokal tepercaya, bukan dari grup di AWS Managed Microsoft AD domain. Grup yang disinkronkan langsung dari domain tepercaya berisi objek pengguna aktual yang dapat diakses dan disinkronkan oleh IAM Identity Center dengan sukses.

Tambahkan pengguna dan grup Active Directory Anda ke IAM Identity Center dengan mengikuti langkah-langkah ini.

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 Users (Pengguna). Jika pengguna yang Anda tentukan tidak ditampilkan 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. Jika grup yang Anda tentukan tidak ditampilkan 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, lihat [Cara 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.

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 IAMIdentityCenterAllUsersAndGroups.
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.

Mengelola pengguna di direktori Pusat Identitas

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 Directory Service. Untuk informasi lebih lanjut, lihat pertimbangan untuk [Mengubah antara direktori Pusat Identitas IAM dan Direktori Aktif](#).

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 untuk [Mengubah dari Pusat Identitas IAM ke IdP eksternal](#).

Topik

- [Tambahkan pengguna ke direktori Pusat Identitas Anda](#)
- [Tambahkan grup ke direktori Pusat Identitas Anda](#)
- [Tambahkan pengguna ke grup](#)
- [Hapus grup di Pusat Identitas IAM](#)
- [Hapus pengguna di Pusat Identitas IAM](#)
- [Hapus pengguna dari grup](#)
- [Edit properti pengguna direktori Pusat Identitas](#)

Tambahkan pengguna ke direktori Pusat Identitas Anda

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. Atau, Anda dapat memanggil operasi AWS API [CreateUser](#) untuk menambahkan pengguna.

Console

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. Email mengundang pengguna atas nama perusahaan Anda untuk mengakses portal AWS akses Pusat Identitas IAM, dan mendaftarkan kata sandi. Undangan email akan kedaluwarsa dalam tujuh hari. Jika ini terjadi, Anda dapat mengirim ulang email dengan memilih Setel ulang kata sandi, lalu memilih Kirim email ke pengguna dengan instruksi untuk mengatur ulang kata sandi. Sebelum pengguna menerima undangan, Anda akan melihat tautan verifikasi email Kirim, yang dimaksudkan untuk memverifikasi alamat email mereka. Namun, langkah ini opsional dan akan hilang setelah pengguna menerima undangan dan mendaftarkan kata sandi.

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, lihat [Cross-Region email dengan Amazon SES](#).

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. Pengguna perlu memverifikasi alamat email mereka. Anda dapat memulai proses dengan memilih tautan Kirim verifikasi email. Tautan verifikasi email akan kedaluwarsa dalam tujuh hari. Jika ini terjadi, Anda dapat mengirim ulang tautan verifikasi email dengan memilih Setel ulang kata sandi, lalu memilih Buat kata sandi satu kali dan bagikan kata sandi dengan pengguna.
- 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 [Menyediakan pengguna dan grup dari penyedia identitas eksternal menggunakan SCIM](#).
- 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.

AWS CLI

Untuk menambahkan pengguna

`create-user` Perintah berikut membuat pengguna baru di direktori Pusat Identitas Anda.

```
aws identitystore create-user \  
  --identity-store-id d-1234567890 \  
  --user-name johndoe \  
  --name "GivenName=John,FamilyName=Doe" \  
  --display-name "John Doe" \  
  --emails "Type=work,Value=johndoe@example.com"
```

Output:

```
{  
  "UserId": "1234567890-abcdef",  
  "IdentityStoreId": "d-1234567890"  
}
```

Note

Saat Anda membuat pengguna dengan perintah `create-user` CLI atau operasi [CreateUser](#) API, pengguna tidak memiliki kata sandi. Anda dapat memperbarui pengaturan di Pusat Identitas IAM untuk mengirim email verifikasi kepada pengguna ini setelah upaya pertama mereka untuk masuk sehingga mereka dapat mengatur kata sandi. Jika Anda tidak mengaktifkan pengaturan ini, Anda harus membuat kata sandi satu kali dan membagikannya dengan pengguna. Untuk informasi selengkapnya, lihat [Email kata sandi satu kali ke pengguna yang dibuat dengan API atau CLI](#).

Tambahkan grup ke direktori Pusat Identitas Anda

Gunakan prosedur berikut untuk menambahkan grup ke direktori Pusat Identitas Anda. Atau, Anda dapat memanggil operasi AWS API [CreateGroup](#) untuk menambahkan grup.

Console

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.

AWS CLI

Untuk menambahkan grup

`create-group` Perintah berikut membuat grup baru di direktori Pusat Identitas Anda.

```
aws identitystore create-group \  
  --identity-store-id d-1234567890 \  
  --display-name "Developers" \  
  --description "Group that contains all developers"
```

Output:

```
{  
  "GroupId": "1a2b3c4d-5e6f-7g8h-9i0j-1k2l3m4n5o6p",  
  "IdentityStoreId": "d-1234567890"  
}
```

Setelah menambahkan grup ini ke direktori Pusat Identitas, Anda dapat menetapkan akses masuk tunggal ke grup. Untuk informasi selengkapnya, lihat [Menetapkan akses pengguna atau grup ke Akun AWS](#).

Tambahkan pengguna ke grup

Gunakan prosedur berikut untuk menambahkan pengguna sebagai anggota grup yang sebelumnya Anda buat di direktori Pusat Identitas Anda. Atau, Anda dapat memanggil operasi AWS API [CreateGroupMembership](#) untuk menambahkan pengguna sebagai anggota grup.

Console

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).

AWS CLI

Untuk menambahkan pengguna sebagai anggota grup

`create-group-membership` Perintah berikut menambahkan pengguna ke grup di direktori Pusat Identitas Anda.

```
aws identitystore create-group-membership \
  --identity-store-id d-1234567890 \
  --group-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222 \
  --member-id UserId=a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Output:

```
{
  "MembershipId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
  "IdentityStoreId": "d-1234567890"
```


}

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.

Important

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

Console

Untuk menghapus grup

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, konfirmasi maksud Anda dengan mengetikkan **Delete** kotak dialog Hapus grup.
 - Jika Anda menghapus satu grup yang berisi pengguna, konfirmasi 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.

AWS CLI

Untuk menghapus grup

`delete-group` Perintah berikut menghapus grup tertentu dari direktori Pusat Identitas Anda.

```
aws identitystore delete-group \  
  --identity-store-id d-1234567890 \  
  --group-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222
```

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 menghapus pengguna, Anda tidak dapat membatalkan tindakan ini. Gunakan prosedur berikut untuk menghapus pengguna di direktori Pusat Identitas Anda.

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 [Memahami sesi otentikasi 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 kredensial pengguna IAM Identity Center berbeda dari pengguna IAM, grup, dan kredensial pengguna IAM. Jika Anda mencari petunjuk tentang menghapus pengguna di IAM, lihat [Menghapus pengguna IAM di Panduan Pengguna](#). AWS Identity and Access Management

Console

Untuk menghapus kluster

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, konfirmasi maksud Anda dengan mengetikkan **Delete** kotak dialog Hapus pengguna.
5. Pilih Hapus pengguna. Jika Anda memilih beberapa pengguna untuk dihapus, pilih Hapus # pengguna.

AWS CLI

Untuk menghapus kluster

`delete-user` Perintah berikut menghapus pengguna dari direktori Pusat Identitas Anda.

```
aws identitystore delete-user \  
  --identity-store-id d-1234567890 \  
  --user-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Hapus pengguna dari grup

Gunakan prosedur berikut untuk menghapus anggota dari grup. Atau, Anda dapat memanggil operasi AWS API [DeleteGroupMembership](#) untuk menghapus pengguna dari grup.

Console

Untuk menghapus pengguna dari grup

1. Buka [konsol Pusat Identitas IAM](#).
2. Pilih Grup.
3. Pilih grup yang ingin Anda perbarui.
4. Pada halaman detail grup, di bawah Pengguna dalam grup ini, pilih pengguna yang akan dihapus.

5. Pilih Hapus pengguna dari grup.
6. Pada kotak dialog Hapus pengguna, pilih Hapus pengguna dari grup untuk memverifikasi bahwa Anda ingin menghapus akses pengguna ke akun dan aplikasi yang ditetapkan ke grup.

AWS CLI

Untuk menghapus pengguna dari grup

`delete-group-membership` Perintah berikut menghapus keanggotaan dari grup.

```
aws identitystore delete-group-membership
--identity-store-id d-1234567890 \
--membership-id a1b2c3d4-5678-90ab-cdef-EXAMPLE33333
```

Edit properti pengguna direktori Pusat Identitas

Gunakan prosedur berikut untuk mengedit properti pengguna di direktori Pusat Identitas Anda. Atau, Anda dapat memanggil operasi AWS API [UpdateUser](#) untuk memperbarui properti pengguna.

Console

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.

AWS CLI

Untuk mengedit properti pengguna di Pusat Identitas IAM

`update-user` Perintah berikut memperbarui nama panggilan pengguna.

```
aws identitystore update-user \  
  --identity-store-id d-1234567890 \  
  --user-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
  --operations '{"AttributePath":"nickName","AttributeValue":"Johnny"}'
```

Menyiapkan akses tenaga kerja ke AWS sumber daya

Atur cara pengguna tenaga kerja Anda mengotentikasi dan mengakses AWS sumber daya melalui Pusat Identitas IAM. Bagian ini mencakup komponen-komponen berikut yang mengatur akses pengguna tenaga kerja ke AWS lingkungan Anda:

- Sesi otentikasi — Memahami bagaimana Pusat Identitas IAM mengelola berbagai jenis sesi pengguna, mulai dari sesi portal interaktif hingga sesi aplikasi latar belakang, dan bagaimana mereka berinteraksi satu sama lain.
- Manajemen akses pengguna — Konfigurasi durasi sesi, nonaktifkan akun pengguna, dan terapkan blok akses di seluruh organisasi untuk menjaga keamanan dan kepatuhan.
- Manajemen kata sandi — Untuk pengguna yang dibuat di direktori Identity Center, tetapkan persyaratan kata sandi, tangani pengaturan kredensi pengguna, dan kelola pengaturan ulang kata sandi untuk pengguna.
- Multi-factor otentikasi — Untuk pengguna yang dibuat di direktori Identity Center, tingkatkan keamanan dengan MFA menggunakan aplikasi otentikator, kunci keamanan, atau autentikator bawaan untuk melindungi login pengguna.

Topik

- [Memahami sesi otentikasi di Pusat Identitas IAM](#)
- [Mengkonfigurasi durasi sesi di Pusat Identitas IAM](#)
- [Nonaktifkan akses pengguna ke Akun AWS dan aplikasi di Pusat Identitas IAM](#)
- [Tolak akses pengguna dengan Kebijakan Kontrol Layanan](#)
- [Mengelola akses untuk pengguna di direktori Identity Center](#)

Memahami sesi otentikasi di Pusat Identitas IAM

Saat pengguna masuk ke portal [AWS akses](#), Pusat Identitas IAM membuat sesi otentikasi yang mewakili identitas terverifikasi pengguna.

Setelah diautentikasi, pengguna dapat mengakses semua aplikasi yang ditugaskan Akun AWS, [AWS dikelola](#), dan aplikasi [yang dikelola](#) pelanggan yang telah diberikan administrator izin untuk digunakan, tanpa login tambahan.

Jenis sesi otentikasi

Sesi interaktif pengguna

Setelah pengguna masuk ke portal AWS akses, Pusat Identitas IAM membuat sesi interaktif pengguna. Sesi ini mewakili status autentikasi pengguna dalam Pusat Identitas IAM dan berfungsi sebagai dasar untuk membuat jenis sesi lainnya. Sesi interaktif pengguna dapat berlangsung selama durasi yang dikonfigurasi di Pusat Identitas IAM, yang bisa hingga 90 hari.

Sesi interaktif pengguna adalah mekanisme otentikasi utama. Mereka berakhir ketika pengguna keluar atau ketika administrator mengakhiri sesi mereka. Durasi sesi ini harus dikonfigurasi dengan hati-hati berdasarkan persyaratan keamanan organisasi Anda.

Untuk informasi tentang mengonfigurasi durasi sesi interaktif pengguna, lihat [the section called “Konfigurasi durasi sesi”](#).

Sesi aplikasi

Sesi aplikasi adalah koneksi yang diautentikasi antara pengguna dan aplikasi AWS terkelola (seperti Kiro atau Amazon Quick) yang dibuat oleh Pusat Identitas IAM melalui sistem masuk tunggal.

Secara default, sesi aplikasi memiliki masa pakai satu jam, tetapi secara otomatis diperbarui selama sesi interaktif pengguna yang mendasarinya tetap valid. Mekanisme penyegaran ini memberikan pengalaman yang mulus bagi pengguna sambil mempertahankan kontrol keamanan. Ketika sesi interaktif pengguna berakhir, baik melalui proses keluar pengguna atau tindakan administrator, sesi aplikasi akan berakhir pada upaya penyegaran berikutnya, biasanya dalam waktu 30 menit.

Jika Anda menggunakan manajer akses [akun](#) untuk akses ke Akun AWS, portal penggunaanya tersedia sebagai aplikasi akses AWS akun di portal AWS akses. Sesi aplikasi akses AWS akun dikelola oleh IAM Identity Center sebagai sesi aplikasi.

Sesi latar belakang pengguna

Sesi latar belakang pengguna adalah sesi durasi diperpanjang yang dirancang untuk aplikasi yang perlu menjalankan proses selama berjam-jam atau sehari-hari tanpa gangguan. Saat ini, jenis sesi ini berlaku terutama untuk [Amazon SageMaker Studio](#), di mana ilmuwan data dapat menjalankan pekerjaan pelatihan pembelajaran mesin yang membutuhkan waktu berjam-jam untuk menyelesaikannya.

Untuk informasi tentang mengonfigurasi durasi sesi latar belakang pengguna, lihat [Sesi latar belakang pengguna](#).

Sesi Kiro

Anda dapat memperpanjang sesi Kiro untuk memungkinkan pengembang yang menggunakan Kiro di IDE untuk mempertahankan otentikasi hingga 90 hari. Fitur ini mengurangi gangguan login saat Anda mengerjakan kode.

Sesi ini tidak bergantung pada jenis sesi lain dan tidak memengaruhi sesi interaktif pengguna atau aplikasi terkel AWS lainnya. Tergantung kapan Anda mengaktifkan Pusat Identitas IAM, fitur ini mungkin diaktifkan secara default.

Untuk informasi tentang mengkonfigurasi sesi Kiro yang diperpanjang, lihat [????](#).

Sesi peran IAM

Sesi peran IAM berbasis set izin

Pusat Identitas IAM membuat jenis sesi yang berbeda saat pengguna mengakses Konsol Manajemen AWS atau AWS CLI. Dalam kasus ini, Pusat Identitas IAM menggunakan sesi masuk untuk mendapatkan sesi IAM dengan mengasumsikan peran IAM yang ditentukan dalam kumpulan izin pengguna.

Sesi peran IAM yang dibuat oleh manajer akses akun

Jika Anda menggunakan manajer akses akun untuk akses ke Akun AWS, manajer akses akun mengambil peran IAM yang ditetapkan dan dengan demikian memulai sesi peran IAM.

Important

Tidak seperti sesi aplikasi, sesi peran IAM beroperasi secara independen setelah ditetapkan. Mereka bertahan selama durasi yang dikonfigurasi dalam kumpulan izin (atau peran IAM saat menggunakan pengelola akses akun), yang dapat bertahan hingga 12 jam, terlepas dari status sesi masuk asli. Perilaku ini memastikan bahwa operasi CLI yang berjalan lama atau sesi konsol tidak berakhir secara tak terduga.

Cara untuk mengakhiri sesi pengguna di Pusat Identitas IAM

User-initiated

Saat pengguna keluar dari portal AWS akses, sesi masuk berakhir, mencegah pengguna mengakses sumber daya baru.

Sesi aplikasi yang ada, bagaimanapun, tidak berakhir secara instan. Sebaliknya, mereka akan berakhir dalam waktu sekitar 30 menit, ketika mereka mencoba penyegaran berikutnya dan menemukan sesi masuk tidak lagi valid. Sesi peran IAM yang ada berlanjut hingga kedaluwarsa berdasarkan konfigurasi kumpulan izin (atau konfigurasi peran IAM saat menggunakan manajer akses akun), yang bisa sampai 12 jam kemudian.

Administrator-initiated

Siapa pun yang memiliki izin administratif Pusat Identitas IAM di organisasi Anda, biasanya administrator TI atau tim keamanan, dapat meng [akhiri sesi](#) pengguna. Tindakan ini bekerja dengan cara yang sama seperti jika pengguna keluar sendiri, memungkinkan administrator meminta pengguna untuk masuk lagi bila diperlukan. Kemampuan ini berguna ketika kebijakan keamanan berubah atau ketika aktivitas mencurigakan terdeteksi.

Ketika administrator Pusat Identitas IAM [menghapus pengguna](#) atau [menonaktifkan akses pengguna](#), pengguna kehilangan akses ke portal AWS akses dan dicegah masuk kembali untuk memulai aplikasi baru atau sesi peran IAM. Pengguna akan kehilangan akses ke sesi aplikasi yang ada dalam waktu 30 menit. Setiap sesi peran IAM yang ada akan berlanjut berdasarkan durasi sesi yang dikonfigurasi dalam kumpulan izin Pusat Identitas IAM (atau peran IAM saat menggunakan manajer akses akun). Durasi sesi maksimum bisa 12 jam.

Apa yang terjadi pada akses pengguna saat Anda mengakhiri sesi

Referensi ini memberikan informasi terperinci tentang bagaimana sesi Pusat Identitas IAM berperilaku saat tindakan administratif diambil. Tabel di bagian ini menunjukkan durasi dan efek tindakan manajemen pengguna dan perubahan izin pada akses ke portal AWS akses, aplikasi, dan Akun AWS sesi.

Manajemen pengguna

Tabel ini merangkum bagaimana perubahan manajemen pengguna memengaruhi akses ke AWS sumber daya, sesi aplikasi, dan sesi AWS akun.

Tindakan	Pengguna kehilangan akses Pusat Identitas IAM	Pengguna tidak dapat membuat sesi aplikasi baru	Pengguna tidak dapat mengakses sesi aplikasi yang ada	Pengguna kehilangan akses ke Akun AWS sesi yang ada
Akses pengguna dinonaktifkan	Efektif segera	Efektif segera	Dalam 30 menit	Dalam waktu 12 jam atau kurang. Durasi tergantung pada durasi kedaluwarsa sesi peran IAM yang dikonfigurasi untuk kumpulan izin (atau peran IAM saat menggunakan manajer akses akun).
Pengguna dihapus	Efektif segera	Efektif segera	Dalam 30 menit	Dalam waktu 12 jam atau kurang. Durasi tergantung pada durasi kedaluwarsa sesi peran IAM yang dikonfigurasi untuk kumpulan izin (atau peran IAM saat menggunakan manajer akses akun).
Sesi pengguna dicabut	Pengguna harus masuk lagi untuk	Efektif segera	Dalam 30 menit	Dalam waktu 12 jam atau kurang. Durasi tergantung

Tindakan	Pengguna kehilangan akses Pusat Identitas IAM	Pengguna tidak dapat membuat sesi aplikasi baru	Pengguna tidak dapat mengakses sesi aplikasi yang ada	Pengguna kehilangan akses ke Akun AWS sesi yang ada
	mendapatkan kembali akses			g pada durasi kedaluwarsa sesi peran IAM yang dikonfigurasi untuk kumpulan izin (atau peran IAM saat menggunakan manajer akses akun).
Pengguna keluar	Pengguna harus masuk lagi untuk mendapatkan kembali akses	Efektif segera	Dalam 30 menit	Dalam waktu 12 jam atau kurang. Durasi tergantung pada durasi kedaluwarsa sesi peran IAM yang dikonfigurasi untuk kumpulan izin (atau peran IAM saat menggunakan manajer akses akun).

Keanggotaan grup

Tabel ini merangkum bagaimana perubahan pada izin pengguna dan keanggotaan grup memengaruhi akses ke AWS sumber daya, sesi aplikasi, dan sesi AWS akun.

Tindakan	Pengguna kehilangan akses Pusat Identitas IAM	Pengguna tidak dapat membuat sesi aplikasi baru	Pengguna tidak dapat mengakses sesi aplikasi yang ada	Pengguna kehilangan akses ke Akun AWS sesi yang ada
Aplikasi atau Akun AWS akses dihapus dari pengguna	Tidak - Pengguna dapat terus mengakses Pusat Identitas IAM	Efektif segera	Dalam 30 menit	Dalam waktu 12 jam atau kurang. Durasi tergantung pada durasi kedaluwarsa sesi peran IAM yang dikonfigurasi untuk kumpulan izin (atau peran IAM saat menggunakan manajer akses akun).
Pengguna dihapus dari grup yang memiliki aplikasi yang ditugaskan atau Akun AWS	Tidak - Pengguna dapat terus mengakses Pusat Identitas IAM	Efektif segera	Dalam 30 menit	Dalam waktu 12 jam atau kurang. Durasi tergantung pada durasi kedaluwarsa sesi peran IAM yang dikonfigurasi untuk kumpulan izin (atau peran IAM saat menggunakan manajer akses akun).
Aplikasi atau Akun AWS	Tidak - Pengguna dapat terus mengakses	Efektif segera	Dalam 30 menit	Dalam waktu 12 jam atau kurang. Durasi tergantung

Tindakan	Pengguna kehilangan akses Pusat Identitas IAM	Pengguna tidak dapat membuat sesi aplikasi baru	Pengguna tidak dapat mengakses sesi aplikasi yang ada	Pengguna kehilangan akses ke Akun AWS sesi yang ada
akses dihapus dari grup	Pusat Identitas IAM			g pada durasi kedaluwarsa sesi peran IAM yang dikonfigurasi untuk kumpulan izin (atau peran IAM saat menggunakan manajer akses akun).

Note

Portal AWS akses dan AWS CLI akan mencerminkan izin pengguna yang diperbarui segera setelah Anda menambahkan atau menghapus pengguna dari grup tersebut. Jika Anda menggunakan penyedia identitas eksternal, perubahan akan berlaku setelah penyedia Anda menyinkronkan pembaruan ke Pusat Identitas IAM.

Memahami perbedaan waktu

- Efektif segera — Pusat Identitas IAM mengevaluasi keanggotaan grup dan perubahan izin secara real time. Lain kali pengguna mencoba membuat sesi baru, perubahan diterapkan.
- Dalam 30 menit — Sesi aplikasi yang ada berakhir pada upaya penyegaran berikutnya, biasanya dalam waktu 30 menit.
- Dalam waktu 12 jam atau kurang — sesi peran IAM beroperasi secara independen dan hanya berakhir ketika durasi yang dikonfigurasi berakhir.

Logout tunggal

Pusat Identitas IAM tidak mendukung SAML Single Logout (protokol yang secara otomatis menandatangani pengguna dari semua aplikasi yang terhubung saat mereka keluar dari satu aplikasi) yang diprakarsai oleh penyedia identitas yang bertindak sebagai sumber identitas Anda. Selain itu, tidak mengirim SAML Single Logout ke aplikasi [SAML 2.0](#) yang menggunakan IAM Identity Center sebagai penyedia identitas.

Praktik terbaik untuk manajemen sesi

Manajemen sesi yang efektif membutuhkan konfigurasi dan pemantauan yang bijaksana. Organisasi harus mengkonfigurasi durasi sesi yang sesuai dengan persyaratan keamanan mereka, umumnya menggunakan durasi yang lebih pendek untuk aplikasi dan lingkungan sensitif.

Menerapkan proses untuk mengakhiri sesi ketika pengguna mengubah peran atau meninggalkan organisasi sangat penting untuk menjaga batas-batas keamanan. Tinjauan rutin sesi aktif harus dimasukkan ke dalam praktik pemantauan keamanan untuk mendeteksi perilaku anomali yang mungkin mengindikasikan masalah keamanan, seperti pola akses yang tidak biasa, waktu atau lokasi login yang tidak terduga, atau akses ke sumber daya di luar fungsi pekerjaan normal.

Mengkonfigurasi durasi sesi di Pusat Identitas IAM

Anda dapat mengonfigurasi durasi sesi untuk pengguna tenaga kerja Anda saat mereka menggunakan aplikasi Portal akses AWS dan yang bekerja dengan Pusat Identitas IAM, termasuk Kiro. IAM Identity Center menyediakan jenis sesi berikut: sesi interaktif pengguna, sesi latar belakang pengguna, dan sesi diperpanjang untuk Kiro.

Topik

- [Sesi interaktif pengguna](#)
- [Sesi latar belakang pengguna](#)
- [Sesi diperpanjang untuk Kiro](#)
- [Melihat dan mengakhiri sesi aktif untuk pengguna tenaga kerja Anda](#)
- [Pertimbangan durasi sesi untuk menggunakan sumber identitas, AWS CLI, dan AWS SDK](#)

Sesi interaktif pengguna

Sesi interaktif pengguna adalah sesi yang terkait dengan login pengguna ke portal AWS akses atau akses ke aplikasi [yang](#) AWS dikelola. Durasi sesi otentikasi ke aplikasi Portal akses AWS dan adalah lamanya waktu maksimum pengguna dapat masuk tanpa autentikasi ulang. Jika Anda mengakhiri sesi portal AWS akses aktif, ini juga mengakhiri sesi apa pun untuk aplikasi terkelola ini.

Durasi sesi default untuk sesi interaktif pengguna adalah 8 jam. Anda dapat menentukan durasi yang berbeda, dari minimal 15 menit hingga maksimum 90 hari. Nilai durasi khusus harus dimasukkan dalam menit dan antara 15 menit dan 129.600 menit (90 hari). Untuk informasi selengkapnya, lihat [Memahami sesi otentikasi di Pusat Identitas IAM](#).

Untuk pertimbangan seperti bagaimana sumber identitas Pusat Identitas IAM dapat memengaruhi durasi sesi interaktif pengguna, lihat [the section called “Pertimbangan untuk sumber identitas, AWS CLI, dan SDK AWS”](#).

Untuk mengkonfigurasi durasi sesi interaktif pengguna

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan.
3. Pada halaman Peng aturan, pilih tab Oten tikasi.
4. Di bawah O tentikasi, di samping Durasi sesi, pilih Konfigurasi. Kotak dialog Konfigurasikan durasi sesi muncul.
5. Di kotak dialog Konfigurasikan durasi sesi, di bawah Sesi interaktif pengguna, pilih durasi sesi maksimum untuk pengguna Anda dengan memilih panah drop-down. Pilih panjang sesi, lalu pilih S impan.

Note

Perubahan durasi sesi hanya berlaku untuk sesi baru. Sesi saat ini mempertahankan durasi aslinya.

6. Anda dikembalikan ke tab O tentikasi. Pesan pemberitahuan hijau muncul di atas tab menunjukkan bahwa pengaturan sesi berhasil diperbarui.

Sesi latar belakang pengguna

Sesi latar belakang pengguna memungkinkan pengguna untuk memulai pekerjaan yang berjalan lama pada AWS aplikasi terkelola seperti [Amazon SageMaker Studio](#), tanpa pengguna tersebut harus tetap masuk saat pekerjaan berjalan. Pekerjaan berjalan segera dan menggunakan [kemampuan propag](#) asi identitas tepercaya dari Pusat Identitas IAM untuk memastikan bahwa izin pengguna dipertahankan saat pekerjaan dijalankan di latar belakang. Pekerjaan dapat terus berjalan meskipun pengguna mematikan komputer mereka, sesi masuk Pusat Identitas IAM berakhir, atau pengguna keluar dari portal AWS akses. Kemampuan ini memungkinkan ilmuwan data, insinyur pembelajaran mesin, dan lainnya untuk memulai alur kerja analitik dan pembelajaran mesin yang berjalan di latar belakang tanpa keterlibatan pengguna aktif.

Sesi latar belakang pengguna diaktifkan secara default untuk aplikasi AWS terkelola yang didukung seperti Amazon SageMaker Studio. Namun, untuk menggunakan kemampuan ini, Anda harus mengaktifkan propagasi identitas tepercaya di Amazon SageMaker Studio saat membuat atau memperbarui domain. Untuk informasi selengkapnya, lihat [Mengaktifkan propagasi identitas tepercaya di domain SageMaker AI Amazon Anda](#).

Durasi sesi default untuk sesi latar belakang pengguna adalah 7 hari. Anda dapat menentukan durasi yang berbeda, dari minimal 15 menit hingga maksimum 90 hari. Nilai durasi khusus harus dimasukkan dalam menit dan antara 15 menit dan 129.600 menit (90 hari).

Ingatlah pertimbangan berikut untuk sesi latar belakang pengguna:

- Sesi latar belakang pengguna hanya dapat dibuat ketika pengguna memulai pekerjaan secara manual di Amazon SageMaker Studio. Kemampuan ini tidak didukung untuk alur kerja terjadwal otomatis.
- Untuk daftar Wilayah AWS yang mendukung sesi latar belakang pengguna, lihat Wilayah yang [Di AWS dukung](#).
- Anda dapat melihat sesi latar belakang pengguna di CloudTrail. Untuk informasi, lihat [Mengidentifikasi rincian sesi latar belakang pengguna](#).
- Anda juga dapat mengakhiri sesi aktif untuk pengguna di organisasi Anda. Untuk selengkapnya, lihat [Mengakhiri sesi aktif untuk pengguna tenaga kerja Anda](#).

Untuk mengkonfigurasi durasi sesi latar belakang pengguna

1. Buka konsol Pusat Identitas IAM.

2. Pilih Pengaturan.
3. Pada halaman Pengaturan, pilih tab Otentikasi.
4. Di bawah Otentikasi, di samping Durasi sesi, pilih Konfigurasi. Kotak dialog Konfigurasi durasi sesi muncul.
5. Di kotak dialog Konfigurasi durasi sesi, jika kotak centang Aktifkan sesi latar belakang pengguna belum dipilih, pilih. Kosongkan kotak centang untuk menonaktifkan sesi latar belakang pengguna.

 Note

Sesi saat ini tidak terpengaruh jika Anda menonaktifkan sesi latar belakang pengguna.

6. Di bawah Sesi latar belakang pengguna, pilih durasi sesi maksimum dengan memilih panah drop-down. Pilih panjang sesi, lalu pilih Simpan.

 Note

Perubahan durasi sesi hanya berlaku untuk sesi baru. Sesi saat ini mempertahankan durasi aslinya.

7. Anda dikembalikan ke tab Otentikasi. Pesan pemberitahuan hijau muncul di atas tab menunjukkan bahwa pengaturan sesi berhasil diperbarui.

 Note

Aplikasi yang dikelola pelanggan tidak dapat membuat sesi latar belakang pengguna.

Sesi diperpanjang untuk Kiro

Jika pengembang Anda menggunakan Kiro sebagai bagian dari lingkungan pengembangan terintegrasi (IDE), Anda dapat mengatur durasi sesi untuk Kiro menjadi 90 hari. Tergantung kapan Anda mengaktifkan Pusat Identitas IAM, durasi sesi yang diperpanjang untuk Kiro mungkin diaktifkan secara default. Sesi yang diperpanjang ini tidak memengaruhi durasi sesi portal AWS akses atau aplikasi terkel AWS lainnya.

Untuk pertimbangan seperti bagaimana sumber identitas Pusat Identitas IAM dapat memengaruhi durasi sesi yang diperpanjang, lihat [the section called “Pertimbangan untuk sumber identitas, AWS CLI, dan SDK AWS”](#).

 Note

Kiro dapat diakses dari konsol yang diatur ke komersial Wilayah AWS yang diaktifkan secara default. Jika instance Pusat Identitas IAM Anda berada di Wilayah di mana Kiro saat ini tidak dapat diakses, mengaktifkan durasi sesi diperpanjang 90 hari tidak akan mengesampingkan setelan default. Ini berarti bahwa durasi sesi Anda tetap tidak berubah, apakah Anda mengaktifkan durasi sesi diperpanjang 90 hari atau tidak. Untuk informasi, Wil AWS ayah [yang Didukung untuk Kiro](#).

Untuk memperpanjang sesi untuk Kiro

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengaturan.
3. Pada halaman Peng aturan, pilih tab Oten tikasi.
4. Di bawah O tentikasi, di samping Durasi sesi, pilih Konfigurasi. Kotak dialog Konfigurasikan durasi sesi muncul.
5. Di kotak dialog Konfigurasikan durasi sesi, pilih kotak centang Aktifkan sesi yang diperpanjang untuk Kiro. Kosongkan kotak centang untuk menonaktifkan sesi sesi yang diperpanjang untuk Kiro.
6. Pilih Simpan untuk kembali ke halaman Pengaturan.

Melihat dan mengakhiri sesi aktif untuk pengguna tenaga kerja Anda

Sebagai administrator Pusat Identitas IAM, Anda dapat melihat daftar sesi aktif pengguna tenaga kerja Anda, dan jika diperlukan, mengakhiri satu sesi atau lebih untuk pengguna. Misalnya, Anda mungkin perlu mengakhiri sesi pengguna saat:

- Pengguna tidak lagi membutuhkan sesi.
- Pengguna tidak boleh mempertahankan status otentikasi mereka saat ini. Ini dapat terjadi ketika mereka meninggalkan perusahaan atau izin mereka berubah.

Anda dapat melihat dan mengakhiri sesi ini dengan menggunakan konsol Pusat Identitas IAM. Pengguna Anda juga dapat melihat dan mengakhiri sesi mereka sendiri dengan menggunakan portal AWS akses. Untuk informasi tentang bagaimana pengguna tenaga kerja Anda dapat melihat dan mengakhiri sesi mereka tanpa bantuan dari administrator, lihat [Melihat dan mengakhiri sesi aktif Anda](#).

 Note

Mengakhiri sesi aktif untuk pengguna Pusat Identitas IAM tidak mengakhiri sesi peran IAM yang aktif di Konsol Manajemen AWS atau AWS CLI. Untuk informasi selengkapnya, lihat [Memahami sesi otentikasi di Pusat Identitas IAM](#).

Untuk mengakhiri sesi aktif untuk pengguna tenaga kerja (konsol Pusat Identitas IAM)

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengguna.
3. Pada halaman Pengguna, pilih nama 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 untuk pengguna ini.
5. Cari sesi latar belakang pengguna (opsional)

Untuk mencari sesi berdasarkan Nama Sumber Daya Amazon (ARN) dari pekerjaan yang menggunakan sesi, dalam daftar Jenis sesi, pilih Sesi latar belakang pengguna, lalu masukkan ARN pekerjaan di kotak pencarian.

 Note

Anda hanya dapat mengakhiri sesi aktif yang dimuat. Jika pengguna memiliki banyak sesi, pilih Muat sesi yang lebih aktif untuk menampilkan sesi tambahan.

6. Pilih kotak centang di samping setiap sesi yang ingin Anda akhiri, lalu pilih Akhiri sesi.
7. Kotak dialog muncul yang mengonfirmasi bahwa Anda mengakhiri sesi aktif untuk pengguna ini. Tinjau informasi, dan jika Anda ingin melanjutkan, ketik `confirm`, lalu pilih Akhiri sesi.
8. Anda akan kembali ke halaman pengguna. Pesan pemberitahuan hijau muncul untuk menunjukkan bahwa sesi yang dipilih berhasil diakhiri.

Pertimbangan durasi sesi untuk menggunakan sumber identitas, AWS CLI, dan AWS SDK

Berikut ini adalah pertimbangan untuk mengonfigurasi durasi sesi jika Anda menggunakan Microsoft Active Directory (AD) atau penyedia identitas eksternal (IdP) sebagai sumber identitas, atau, AWS Perangkat Peng AWS Command Line Interface embangan Perangkat Lunak (SDK), atau alat AWS pengembangan lainnya untuk mengakses AWS layanan secara terprogram.

Microsoft Active Directory, sesi interaktif pengguna, dan sesi diperpanjang untuk Kiro

Jika Anda menggunakan Microsoft Active Directory (AD) sebagai sumber identitas dan Anda mengonfigurasi durasi sesi untuk sesi interaktif pengguna atau sesi yang diperpanjang untuk Kiro, ingatlah pertimbangan berikut.

Note

Pertimbangan ini tidak berlaku untuk sesi latar belakang pengguna.

Baik Anda menggunakan AWS Managed Microsoft AD atau AD Connector dikonfigurasi di AWS Directory Service, masa pakai maksimum tiket Kerberos pengguna yang ditentukan dalam Microsoft AD dapat memengaruhi berapa lama sesi interaktif pengguna dan sesi diperpanjang untuk Kiro valid. Untuk informasi selengkapnya tentang pengaturan ini, lihat [Masa pakai maksimum untuk tiket pengguna](#) di situs web Microsoft.

- **AWS Managed Microsoft AD:** Jika Anda menggunakan AWS Managed Microsoft AD konfigurasi di AWS Directory Service, masa pakai maksimum untuk tiket Kerberos pengguna ditetapkan pada 10 jam. Oleh karena itu, durasi sesi interaktif pengguna diatur ke pengaturan Pusat Identitas IAM yang lebih pendek dan 10 jam. Misalnya, jika Anda mengatur durasi sesi interaktif pengguna menjadi 12 jam, pengguna Anda harus melakukan autentikasi ulang di portal AWS akses setelah 10 jam. Batas 10 jam yang sama berlaku untuk sesi yang diperpanjang untuk Kiro.
- **Konektor AD:** Jika Anda menggunakan Konektor AD yang dikonfigurasi di AWS Directory Service, masa pakai maksimum tiket Kerberos pengguna ditentukan di Microsoft AD di belakang Konektor AD. Nilai defaultnya adalah 10 jam, dan memiliki efek yang sama pada sesi interaktif pengguna dan sesi diperpanjang seperti untuk AWS Managed Microsoft AD. Meskipun batas ini mungkin dapat dikonfigurasi di Microsoft AD, sebaiknya Anda bekerja sama dengan administrator TI untuk mempertimbangkan risikonya, terutama karena pengaturan ini dapat memengaruhi durasi sesi untuk aplikasi klien Microsoft AD lainnya.

Penyedia identitas eksternal, sesi interaktif pengguna, dan sesi diperpanjang untuk Kiro

Jika Anda menggunakan penyedia identitas eksternal (IdP) dan mengonfigurasi durasi sesi untuk sesi interaktif pengguna atau sesi yang diperpanjang untuk Kiro, ingatlah pertimbangan berikut.

Note

Pertimbangan ini tidak berlaku untuk sesi latar belakang pengguna.

Pusat Identitas IAM menggunakan `SessionNotOnOrAfter` atribut dari pernyataan SAML untuk membantu menentukan berapa lama sesi dapat valid.

- Jika tidak `SessionNotOnOrAfter` diteruskan dalam pernyataan SAML, durasi sesi portal AWS akses (interaktif pengguna) dan sesi yang diperpanjang tidak terpengaruh oleh durasi sesi IdP eksternal Anda. Misalnya, jika durasi sesi IdP Anda adalah 24 jam dan Anda menetapkan durasi sesi 18 jam di Pusat Identitas IAM, pengguna Anda harus melakukan autentikasi ulang di portal AWS akses setelah 18 jam. Demikian pula, jika Anda menetapkan sesi diperpanjang 90 hari untuk Kiro, pengguna Kiro Anda perlu melakukan autentikasi ulang setelah 90 hari.
- Jika `SessionNotOnOrAfter` diteruskan dalam pernyataan SAML, nilai durasi sesi disetel ke sesi portal AWS akses (interaktif pengguna) yang lebih pendek atau durasi sesi yang diperpanjang dan durasi sesi SAML IdP Anda. Jika Anda menetapkan durasi sesi 72 jam di Pusat Identitas IAM dan IdP Anda memiliki durasi sesi 18 jam, pengguna Anda akan memiliki akses ke AWS sumber daya selama 18 jam yang ditentukan di IdP Anda. Demikian pula, jika Anda mengatur sesi diperpanjang 90 hari untuk Kiro, pengguna Kiro Anda perlu melakukan autentikasi ulang di Kiro setelah 18 jam.
- Jika durasi sesi IdP Anda lebih lama dari yang ditetapkan di Pusat Identitas IAM, pengguna Anda dapat memulai sesi Pusat Identitas IAM baru tanpa memasukkan kembali kredensialnya, berdasarkan sesi login mereka yang masih valid dengan IdP Anda.

AWS CLI dan sesi SDK

Jika Anda menggunakan AWS CLI, AWS SDK, atau alat AWS pengembangan lainnya untuk mengakses AWS layanan secara terprogram, prasyarat berikut harus dipenuhi untuk mengatur durasi sesi untuk portal AWS akses dan aplikasi yang dikelola. AWS

- 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 Konfigur [asi penyedia token SS](#) O di Panduan Referensi AWS SDK dan 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 manajemen sesi AWS CLI yang mendukung.

- AWS CLI V2 2.9 atau yang lebih baru
- AWS CLI V1 1.27.10 atau yang lebih baru

 Note

Untuk kasus penggunaan akses akun, jika pengguna menjalankan AWS CLI, jika Anda menyegarkan kumpulan izin tepat sebelum sesi Pusat Identitas IAM disetel kedaluwarsa dan durasi sesi disetel ke 20 jam sementara durasi set izin diatur ke 12 jam, AWS CLI sesi berjalan maksimal 20 jam ditambah 12 jam dengan total 32 jam. Untuk informasi selengkapnya tentang IAM Identity Center CLI, lihat Referensi Per [AWS CLI intah](#).

Versi minimum SDK yang mendukung manajemen sesi Pusat Identitas IAM

Berikut ini adalah versi minimum SDK yang mendukung manajemen sesi Pusat Identitas IAM.

SDK	Versi minimum
Python	1.26.10
PHP	3.245.0
Ruby	aws-sdk-inti 3.167.0
Java V2	AWS SDK untuk Java v2 (2.18.13)

SDK	Versi minimum
Pergi V2	Seluruh SDK: rilis-2022-11-11 dan modul Go tertentu: .13.0, .18.0 credentials/v1 config/v1
JSV2	2.1253.0
JSV3	v3.210.0
C++	1.9.372
.NET	v3.7.400.0

Nonaktifkan akses pengguna ke Akun AWS dan aplikasi di Pusat Identitas IAM

Saat menonaktifkan akses pengguna di direktori Pusat Identitas IAM, Anda tidak dapat mengedit detail pengguna, mengatur ulang kata sandi mereka, menambahkan pengguna ke grup, atau melihat keanggotaan grup mereka. Menonaktifkan akses pengguna mencegah mereka masuk ke portal AWS akses dan mereka tidak akan lagi memiliki akses ke aplikasi Akun AWS dan yang ditugaskan. Gunakan nonaktifkan akses pengguna untuk penghapusan akses sementara ketika Anda mungkin perlu memulihkan akses nanti.

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 [Memahami sesi otentikasi di Pusat Identitas IAM](#).

Untuk menonaktifkan akses pengguna di Pusat Identitas IAM

1. Buka konsol [Pusat Identitas IAM](#).

 Important

Instruksi di halaman ini berlaku untuk [AWS IAM Identity Center](#). Mereka tidak berlaku untuk [AWS Identity and Access Management](#) (IAM). Pengguna, grup, dan kredensial pengguna IAM Identity Center berbeda dari pengguna IAM, grup, dan kredensial pengguna IAM. Jika Anda mencari petunjuk tentang menonaktifkan pengguna di IAM, lihat [M engelola 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 bawah nama pengguna pengguna yang aksesnya ingin Anda nonaktifkan, di bagian Informasi umum, pilih Non aktifkan akses pengguna.
5. Di kotak dialog Nonaktifkan akses pengguna, pilih N onaktifkan akses pengguna.

Tolak akses pengguna dengan Kebijakan Kontrol Layanan

Untuk segera menolak akses untuk melakukan panggilan API resmi saat akses pengguna Pusat Identitas IAM dinonaktifkan atau pengguna dihapus, Anda dapat:

1. [Tambahkan atau](#) perbarui [kebijakan sebaris](#) dari kumpulan izin (atau kebijakan peran IAM saat menggunakan manajer akses [akun](#)) yang ditetapkan ke pengguna dengan menambahkan Deny efek eksplisit untuk semua tindakan pada semua sumber daya.
2. Tentukan kunci `identitystore:user_id` kondisi `aws:user_id` atau.

Atau, Anda dapat menggunakan Kebijakan Kontrol [Layanan](#) untuk menolak akses pengguna di semua akun anggota di organisasi Anda.

Example Contoh SCP untuk menolak akses

Kebijakan penolakan ini memblokir semua AWS tindakan untuk pengguna tertentu, terlepas dari izin lain yang mungkin diberikan di tempat lain. Kebijakan ini mengesampingkan Allow kebijakan apa pun.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "aws:UserId": "*:deleteduser@domain.com"
        }
      }
    }
  ]
}
```

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "identitystore:UserId": "DELETEDUSER_ID"
        }
      }
    }
  ]
}
```

Mengelola akses untuk pengguna di direktori Identity Center

Pelajari cara mengelola kata sandi dan otentikasi multi-faktor (MFA) untuk pengguna di direktori Pusat Identitas IAM. Fitur keamanan ini membantu melindungi akun pengguna.

Note

Fitur-fitur ini tidak berlaku untuk pengguna Active Directory atau pengguna penyedia identitas eksternal.

Administrator dapat mengelola kata sandi dan MFA melalui konsol Pusat Identitas IAM. Fitur keamanan ini hanya berfungsi dengan direktori Identity Center bawaan.

Manajemen kata sandi

Manajemen kata sandi mencakup kemampuan ini:

- Setel ulang kata sandi dengan instruksi email
- Hasilkan kata sandi satu kali
- Konfigurasi verifikasi email otomatis untuk API-created pengguna

AWS memberlakukan persyaratan keamanan tetap, termasuk aturan kompleksitas dan pembatasan penggunaan kembali kata sandi.

MFA

MFA diaktifkan secara default dan mendukung hingga delapan perangkat per pengguna.

Jenis perangkat yang didukung meliputi:

- Aplikasi autentikator
- Kunci keamanan
- Built-in otentikator biometrik

Administrator dapat mendaftarkan dan mengelola perangkat MFA untuk pengguna.

Topik

- [Menyiapkan kata sandi pengguna](#)
- [MFA untuk pengguna direktori Pusat Identitas](#)

Menyiapkan kata sandi pengguna

Untuk pengguna yang dibuat di direktori Identity Center, administrator dapat mengelola kebijakan kata sandi, menangani pengguna tanpa kata sandi awal, dan mengatur ulang kata sandi bila diperlukan. Fitur manajemen kata sandi ini hanya berlaku untuk pengguna di direktori Pusat Identitas bawaan. Jika Anda menggunakan Active Directory atau penyedia identitas eksternal, Anda harus mengelola kata sandi di sistem tersebut.

Opsi manajemen kata sandi

- **Persyaratan kata sandi** — Persyaratan keamanan yang harus dipenuhi pengguna saat mengatur atau mengubah kata sandi. Ini termasuk aturan kompleksitas dan pembatasan penggunaan kembali.
- **One-time pengaturan kata sandi** — Konfigurasi verifikasi email untuk pengguna yang dibuat melalui API atau CLI yang tidak memiliki kata sandi awal. Anda juga dapat membuat kata sandi sementara untuk akses langsung.
- **Reset kata sandi** — Reset kata sandi untuk pengguna yang terkunci atau membutuhkan kredensial baru. Anda dapat mengirim instruksi reset menggunakan email atau membuat kata sandi satu kali.

Topik

- [Persyaratan kata sandi saat mengelola identitas di Pusat Identitas IAM](#)
- [Email kata sandi satu kali ke pengguna yang dibuat dengan API atau CLI](#)
- [Setel ulang kata sandi pengguna Pusat Identitas IAM untuk pengguna akhir](#)

Persyaratan kata sandi saat mengelola identitas di Pusat Identitas IAM

Note

Persyaratan ini hanya berlaku untuk pengguna yang dibuat di direktori Identity Center. Jika Anda telah mengonfigurasi sumber identitas selain Pusat Identitas IAM untuk otentikasi, seperti [Active Directory](#) atau penyedia identitas [eksternal](#), kebijakan kata sandi untuk pengguna Anda ditentukan dan diberlakukan di sistem tersebut, bukan di Pusat Identitas IAM.

Jika sumber identitas Anda adalah AWS Managed Microsoft AD, lihat Mengel [ola kebijakan kata sandi AWS Managed Microsoft AD](#) untuk informasi selengkapnya.

Saat Anda menggunakan Pusat Identitas IAM 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 antara 8 dan 64 karakter panjangnya.
- Kata sandi harus berisi setidaknya satu karakter dari masing-masing dari empat kategori berikut:
 - Huruf kecil (a-z)
 - Huruf besar (A-Z)
 - Angka (0-9)
 - Non-alphanumeric karakter (~! @\$%^&* _-+=`| \ () { } [] ; : " ' < > , . ? /)
- Tiga kata sandi terakhir tidak dapat digunakan kembali.
- Kata sandi yang diketahui publik melalui kumpulan data yang bocor dari pihak ketiga tidak dapat digunakan.

Email kata sandi satu kali ke pengguna yang dibuat dengan API atau CLI

Saat Anda membuat pengguna dengan operasi [CreateUser](#) API atau perintah `create-user` CLI, pengguna tidak memiliki kata sandi. Anda dapat memperbarui pengaturan di Pusat Identitas IAM untuk mengirim email verifikasi kepada pengguna ini setelah upaya pertama mereka untuk masuk, jika Anda telah menentukan email untuk pengguna saat mereka dibuat. Setelah menerima email verifikasi, pengguna harus mengatur kata sandi untuk masuk.

Jika Anda tidak mengaktifkan pengaturan ini, Anda harus [membuat kata sandi satu kali](#) dan membagikannya dengan pengguna yang Anda buat menggunakan perintah `CreateUser` API atau `create-user` CLI.

Untuk mengirim email verifikasi alamat email ke pengguna yang dibuat dengan `CreateUser` API atau perintah **CLI `create-user`**

1. Buka konsol [Pusat Identi](#) tas IAM.
2. Pilih Pengaturan.
3. Pada halaman Peng aturan, pilih tab Oten tikasi.

4. Di bagian Otentikasi standar, pilih Konfigurasi.
5. Di kotak dialog Konfigurasi otentikasi standar, pilih kotak centang Kirim email OTP. Lalu, pilih Simpan. Status diperbarui dari Dinonaktifkan ke Diaktifkan.

Setel ulang kata sandi pengguna Pusat Identitas IAM untuk pengguna akhir

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

Pertimbangan untuk penyedia identitas dan jenis pengguna

- MicrosoftDirektori Aktif atau penyedia eksternal — Jika Anda menghubungkan Pusat Identitas IAM 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 adalah pengguna Pusat Identitas IAM, Anda dapat mengatur ulang kata sandi Pusat Identitas IAM Anda sendiri, lihat. [Mengatur ulang AWS akses kata sandi pengguna portal](#)

Untuk mengatur ulang kata sandi untuk pengguna akhir Pusat Identitas IAM

Important

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

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

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

 Warning

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

- 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.

MFA untuk pengguna direktori Pusat Identitas

 Important

MFA di Pusat Identitas IAM saat ini tidak didukung untuk penyedia identitas [eksternal](#).

IAM Identity Center hadir dengan otentikasi multi-faktor (MFA) yang dihidupkan secara default sehingga semua pengguna harus masuk dengan MFA selain nama pengguna dan kata sandi mereka. Ini memastikan bahwa pengguna harus masuk ke portal AWS akses menggunakan dua faktor berikut:

- 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](#).

Topik

- [Tersedia tipe MFA untuk IAM Identity Center](#)
- [Konfigurasi MFA di Pusat Identitas IAM](#)
- [Daftarkan perangkat MFA untuk pengguna](#)
- [Mengganti nama dan menghapus perangkat MFA di IAM Identity Center](#)

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.

- [FIDO2 autentikator](#), termasuk autentikator bawaan dan kunci keamanan
- [Aplikasi otentikator virtual](#)
- [RADIUS MFA](#) Implementasi 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 AWS Anda juga dapat mengonfigurasi pengaturan MFA untuk meminta MFA setiap kali mereka mencoba masuk dari perangkat atau browser baru, atau saat masuk dari alamat IP yang tidak dikenal. Untuk informasi selengkapnya tentang cara mengonfigurasi setelan MFA untuk pengguna Anda, lihat [Pilih jenis MFA untuk otentikasi pengguna](#) dan [Konfigurasi penegakan perangkat MFA](#).

FIDO2 autentikator

[FIDO2](#) adalah standar yang mencakup CTAP2 dan [WebAuthn](#) dan didasarkan pada kriptografi kunci publik. Kredensi FIDO tahan terhadap phishing karena unik untuk situs web tempat kredensialnya dibuat. AWS

AWS mendukung 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 kredensial 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 kredensial 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
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. Directory Service termasuk 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 untuk pengguna yang masuk ke portal akses. AWS Namun, RADIUS MFA terus menantang pengguna ketika mereka masuk ke semua aplikasi lain yang bekerja dengannya Directory Service, seperti Amazon RDS for SQL Server.

Jika MFA Anda Dinonaktifkan pada konsol Pusat Identitas IAM dan Anda telah mengonfigurasi RADIUS MFA dengan Directory Service RADIUS MFA mengatur akses masuk portal. AWS Ini berarti bahwa IAM Identity Center kembali ke konfigurasi RADIUS MFA jika MFA dinonaktifkan.

Konfigurasi MFA di Pusat Identitas IAM

Anda dapat mengonfigurasi kemampuan otentikasi Multi-faktor (MFA) di Pusat Identitas IAM ketika sumber identitas Anda dikonfigurasi dengan penyimpanan identitas IAM Identity Center, atau AD Connector. AWS Managed Microsoft AD MFA di Pusat Identitas IAM saat ini tidak didukung untuk penyedia identitas [eksternal](#).

Berikut ini adalah rekomendasi MFA umum, tergantung pada pengaturan Pusat Identitas IAM dan preferensi organisasi Anda.

- 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 [Konfigurasi penegakan perangkat MFA](#).

- Jika Anda sudah menggunakan RADIUS MFA yang Anda konfigurasi dengan 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](#).
- YouTube Video berikut memberikan gambaran umum tentang MFA dan IAM Identity Center:

[Pusat Identitas IAM: Autentikasi multi-faktor default untuk instance baru](#)

Topik

- [Meminta pengguna untuk MFA](#)
- [Pilih jenis MFA untuk otentikasi pengguna](#)
- [Konfigurasi penegakan perangkat MFA](#)
- [Memungkinkan pengguna untuk mendaftarkan perangkat MFA mereka sendiri](#)

Meminta pengguna untuk MFA

Anda dapat menggunakan langkah-langkah berikut untuk menentukan seberapa sering pengguna tenaga kerja diminta untuk otentikasi multi-faktor (MFA) setiap kali mereka mencoba masuk ke portal akses. AWS Sebelum Anda mulai, kami sarankan Anda memahami [Tersedia tipe MFA untuk IAM Identity Center](#).

Important

Instruksi di bagian ini berlaku untuk [AWS IAM Identity Center](#). Mereka tidak berlaku untuk [AWS Identity and Access Management](#) (IAM). Pengguna IAM Identity Center, grup, dan kredensial pengguna berbeda dari pengguna IAM, grup, dan kredensial pengguna IAM. Jika Anda mencari petunjuk tentang menonaktifkan MFA untuk pengguna IAM, lihat Menonaktifkan perangkat [MFA](#) di Panduan Pengguna AWS Identity and Access Management

 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 mengkonfigurasi 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:

- Setiap kali mereka masuk (selalu aktif)

Dalam mode ini (pengaturan default), IAM Identity Center mengharuskan pengguna dengan perangkat MFA terdaftar akan diminta setiap kali mereka masuk. Ini adalah pengaturan yang paling aman dan memastikan bahwa kebijakan organisasi atau kepatuhan Anda diberlakukan dengan mengharuskan MFA digunakan setiap kali mereka masuk ke portal akses AWS . Misalnya, PCI DSS sangat merekomendasikan MFA selama setiap login untuk mengakses aplikasi yang mendukung transaksi pembayaran berisiko tinggi.

- Hanya ketika konteks masuk mereka berubah (sadar konteks)

Dalam mode ini, 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 tetapi kurang aman daripada opsi selalu aktif. Pengguna hanya diminta untuk MFA jika konteks masuk mereka berubah.

- 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 dan tidak disarankan.

Meskipun MFA dinonaktifkan untuk direktori Pusat Identitas Anda untuk pengguna, Anda tidak dapat mengelola perangkat MFA dalam detail pengguna mereka, dan pengguna direktori Pusat Identitas tidak dapat mengelola perangkat MFA dari portal akses. AWS

 Note

Jika Anda sudah menggunakan RADIUS MFA dengan 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 Simpan perubahan.

Topik Terkait

- [Pilih jenis MFA untuk otentikasi pengguna](#)
- [Konfigurasi penegakan perangkat MFA](#)
- [Memungkinkan pengguna untuk mendaftarkan perangkat MFA mereka sendiri](#)

Pilih jenis MFA untuk otentikasi pengguna

Gunakan prosedur berikut untuk memilih jenis perangkat yang dapat diautentikasi oleh pengguna Anda saat diminta autentikasi multi-faktor (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](#).
 - Kunci keamanan dan autentikator bawaan
 - Aplikasi Authenticator
6. Pilih Simpan perubahan.

Konfigurasi penegakan perangkat MFA

Gunakan prosedur berikut untuk menentukan apakah pengguna Anda harus memiliki perangkat MFA terdaftar saat masuk ke portal AWS akses.

Untuk informasi selengkapnya tentang MFA di IAM, lihat Autentikasi [AWS multi-faktor](#) di IAM.

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 untuk 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

Administrator IAM Identity Center dapat memungkinkan pengguna untuk 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 Anda mengatur pendaftaran mandiri untuk pengguna Anda, Anda mungkin ingin mengirimkan mereka tautan ke prosedur [Mendaftarkan perangkat Anda untuk MFA](#). Topik ini memberikan instruksi tentang cara mengatur perangkat MFA mereka sendiri.

Daftarkan perangkat MFA untuk pengguna

Administrator IAM Identity Center dapat menyiapkan perangkat MFA baru untuk diakses oleh pengguna tertentu di konsol Pusat Identitas IAM. Administrator 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 mengonfigurasi 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

Kirimkan 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.

Mengganti nama dan menghapus perangkat MFA di IAM Identity Center

Administrator IAM Identity Center dapat menggunakan prosedur berikut untuk 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.

Konfigurasi 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 kredensial direktori mereka untuk masuk.

IAM Identity Center berkomunikasi dengan aman dengan aplikasi ini melalui hubungan tepercaya antara Pusat Identitas IAM dan penyedia layanan aplikasi. Kepercayaan ini dapat dibuat dengan cara yang berbeda, tergantung pada jenis aplikasi.

IAM Identity Center mendukung dua jenis aplikasi: aplikasi terkel [AWS ola](#) dan aplikasi yang dikelola [pelanggan](#). AWS aplikasi yang dikelola 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 mengonfigurasi aplikasi untuk bekerja dengan Pusat Identitas IAM, 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 Konsol Manajemen AWS untuk yang spesifik Akun AWS di organisasi Anda. Untuk informasi selengkapnya, lihat [Konfigurasi akses ke Akun AWS](#).

Topik

- [AWS aplikasi yang dikelola](#)
- [Aplikasi yang dikelola pelanggan](#)
- [Ikhtisar propagasi identitas tepercaya](#)
- [Menyiapkan aplikasi OAuth 2.0 Anda sendiri](#)
- [Putar sertifikat Pusat Identitas IAM](#)
- [Memahami properti aplikasi di konsol Pusat Identitas IAM](#)
- [Menetapkan akses pengguna ke aplikasi di konsol Pusat Identitas IAM](#)
- [Hapus akses pengguna ke aplikasi SAML 2.0](#)
- [Memetakan atribut dalam aplikasi Anda ke atribut Pusat Identitas IAM](#)

AWS aplikasi yang dikelola

AWS IAM Identity Center merampingkan dan menyederhanakan tugas menghubungkan pengguna tenaga kerja Anda ke aplikasi AWS terkelola seperti Kiro dan Amazon Quick. Dengan IAM Identity Center, Anda dapat menghubungkan penyedia identitas yang ada satu kali dan menyinkronkan pengguna dan grup dari direktori Anda, atau membuat dan mengelola pengguna Anda secara langsung di Pusat Identitas IAM. Dengan menyediakan satu titik federasi, Pusat Identitas IAM menghilangkan kebutuhan untuk mengatur federasi atau sinkronisasi pengguna dan grup untuk setiap aplikasi dan mengurangi upaya administratif Anda. Anda juga mendapatkan [pandangan umum tentang tugas pengguna dan grup](#).

Untuk tabel AWS aplikasi yang bekerja dengan Pusat Identitas IAM, lihat [AWS aplikasi terkelola yang dapat Anda gunakan dengan IAM Identity Center](#).

Mengontrol akses ke AWS aplikasi yang dikelola

Akses ke AWS aplikasi terkelola dikendalikan dengan dua cara:

- Entri awal ke aplikasi

IAM Identity Center mengelola ini melalui penugasan ke aplikasi. Secara default, penugasan diperlukan untuk aplikasi AWS yang dikelola. Jika Anda seorang administrator aplikasi, Anda dapat memilih apakah akan memerlukan penugasan ke aplikasi.

Jika penugasan diperlukan, saat pengguna masuk ke Portal akses AWS, hanya pengguna yang ditugaskan ke aplikasi secara langsung atau melalui penugasan grup yang dapat melihat ubin aplikasi.

Jika penugasan 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 akses AWS.

Important

Jika Anda adalah administrator Pusat Identitas IAM, Anda dapat menggunakan konsol Pusat Identitas IAM untuk menghapus penugasan ke aplikasi yang AWS dikelola. Sebelum Anda menghapus tugas, sebaiknya Anda berkoordinasi dengan administrator aplikasi. Anda juga harus berkoordinasi dengan administrator aplikasi jika Anda berencana untuk

mengubah pengaturan yang menentukan apakah tugas diperlukan, atau mengotomatiskan penugasan aplikasi.

- Akses ke sumber daya aplikasi

Aplikasi mengelola ini melalui penugasan sumber daya independen yang dikendalikannya.

AWS aplikasi terkelola menyediakan antarmuka pengguna administratif yang dapat Anda gunakan untuk mengelola akses ke sumber daya aplikasi. Misalnya, administrator Cepat dapat menetapkan pengguna untuk mengakses dasbor berdasarkan keanggotaan grup mereka. Sebagian AWS besar aplikasi terkelola juga memberikan Konsol Manajemen AWS pengalaman yang memungkinkan Anda untuk menetapkan pengguna ke aplikasi. Pengalaman konsol untuk aplikasi ini mungkin mengintegrasikan kedua fungsi, untuk menggabungkan kemampuan penugasan pengguna dengan kemampuan untuk mengelola akses ke sumber daya aplikasi.

Berbagi informasi identitas

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 hanya di akun AWS Organizations manajemen, maka aplikasi di akun anggota tidak memiliki akses ke informasi. Namun, jika Anda mengaktifkan akses di semua akun, Anda dapat menggunakan SCP untuk melarang akses oleh semua aplikasi kecuali yang ingin Anda izinkan.

Kebijakan kontrol layanan adalah fitur dari AWS Organizations. Untuk petunjuk tentang melampirkan SCP, lihat Mel [ampirkan dan melepaskan kebijakan kontrol layanan](#) di Panduan AWS Organizations Pengguna.

Mengkonfigurasi Pusat Identitas IAM untuk berbagi informasi identitas

Pusat Identitas IAM menyediakan penyimpanan identitas yang berisi atribut pengguna dan grup, tidak termasuk kredentif masuk. Anda dapat menggunakan salah satu metode berikut untuk memperbarui pengguna dan grup di penyimpanan identitas Pusat Identitas IAM Anda:

- Gunakan penyimpanan identitas Pusat Identitas IAM sebagai sumber identitas utama Anda. Jika Anda memilih metode ini, Anda mengelola pengguna, kredentif masuk mereka, dan grup dari dalam konsol Pusat Identitas IAM atau AWS Command Line Interface (AWS CLI). Untuk informasi selengkapnya, lihat [Mengelola pengguna di direktori Pusat Identitas](#).
- Mengatur penyediaan (sinkronisasi) pengguna dan grup yang berasal dari salah satu sumber identitas berikut ke penyimpanan identitas Pusat Identitas IAM Anda:
 - Active Directory — Untuk informasi selengkapnya, lihat [Microsoft AD direktori](#).
 - Penyedia identitas eksternal — Untuk informasi selengkapnya, lihat [Penyedia identitas eksternal](#).

Jika Anda memilih metode penyediaan ini, Anda akan terus mengelola pengguna dan grup dari dalam sumber identitas Anda, dan perubahan tersebut disinkronkan ke penyimpanan identitas Pusat Identitas IAM.

Sumber identitas apa pun yang Anda pilih, Pusat Identitas IAM dapat berbagi informasi pengguna dan grup dengan aplikasi terkel AWS ola. Dengan begitu, Anda dapat menghubungkan sumber identitas ke Pusat Identitas IAM sekali dan kemudian berbagi informasi identitas dengan beberapa aplikasi di AWS Cloud. Ini menghilangkan kebutuhan untuk mengatur federasi dan penyediaan identitas secara independen dengan setiap aplikasi. Fitur berbagi ini juga memudahkan untuk memberi pengguna Anda akses ke banyak aplikasi yang berbeda Akun AWS.

Membatasi penggunaan AWS aplikasi yang dikelola

Saat pertama kali mengaktifkan Pusat Identitas IAM, itu akan tersedia sebagai sumber identitas untuk aplikasi terkel AWS ola di semua akun di akun Anda AWS Organizations. Untuk membatasi aplikasi, Anda harus menerapkan kebijakan kontrol layanan (SCP). SCP adalah fitur AWS Organizations yang dapat Anda gunakan untuk mengontrol izin maksimum yang dapat dimiliki identitas (pengguna dan peran) dalam organisasi Anda secara terpusat. 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. Untuk informasi selengkapnya, lihat [Kebijakan Kontrol Layanan \(SCP\)](#) di Panduan Pengguna AWS Organizations .

Contoh SCP berikut memblokir akses ke informasi pengguna dan grup Pusat Identitas IAM dan mencegah aplikasi dimulai, kecuali di akun yang ditunjuk (111111111111 dan 222222222222):

```
{
  "Sid": "DenyIdCExceptInDesignatedAWSAccounts",
  "Effect": "Deny",
  "Action": [
    "identitystore:*",
    "sso:*",
    "sso-directory:*",
    "sso-oauth:*"
  ],
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "aws:PrincipalAccount": [
        "111111111111",
        "222222222222"
      ]
    }
  }
}
```

AWS aplikasi terkelola yang dapat Anda gunakan dengan IAM Identity Center

IAM Identity Center memungkinkan Anda menghubungkan sumber identitas yang ada atau membuat pengguna satu kali. Hal ini memungkinkan administrator aplikasi untuk mengelola akses ke aplikasi terkel AWS ola berikut tanpa federasi terpisah atau sinkronisasi pengguna dan grup.

AWS aplikasi terkelola yang terintegrasi dengan IAM Identity Center

Semua aplikasi terkel AWS ola dalam tabel berikut terintegrasi dengan instans [organisasi dari Pusat Identitas IAM](#). Tabel ini juga menyediakan informasi tentang hal berikut untuk aplikasi terkel AWS ola yang didukung:

- Apakah aplikasi juga terintegrasi dengan instance akun IAM Identity Center
- Apakah aplikasi dapat mengaktifkan propagasi identitas tepercaya melalui Pusat Identitas IAM

- Apakah aplikasi mendukung Pusat Identitas IAM yang dikonfigurasi dengan kunci KMS yang dikelola pelanggan
- Apakah aplikasi mendukung penerapan di Wilayah tambahan Pusat Identitas IAM

Note

Aplikasi yang mendukung penerapan di Wilayah tambahan Pusat Identitas IAM juga mendukung Pusat Identitas IAM yang dikonfigurasi dengan kunci KMS yang dikelola pelanggan. Setiap aplikasi AWS terkelola yang tercantum di sini mendukung penerapan di Wilayah utama. Untuk informasi selengkapnya, lihat [the section called “Menyebarkan dan AWS mengelola aplikasi terkelola di berbagai aplikasi Wilayah AWS”](#).

AWS aplikasi yang dikelola	Terintegrasi dengan instans akun IAM Identity Center	Memungkinkan penyebaran identitas tepercaya melalui Pusat Identitas IAM	Mendukung Pusat Identitas IAM yang dikonfigurasi dengan kunci K MS yang dikelola pelanggan	Mendukung penerapan di Wilayah tambahan Pusat Identitas IAM
Amazon Athena SQL	Ya	Ya	Ya	Ya
Amazon CodeCatalyst	Ya	Tidak	Ya	Tidak
Amazon DataZone	Ya	Ya	Ya	Tidak
Kemampuan Amazon EKS	Ya	Ya	Ya	Tidak
Amazon EMR pada EC2	Ya	Ya	Ya	Ya
Amazon EMR di EKS	Ya	Ya	Ya	Ya
Amazon EMR Tanpa Server	Ya	Ya	Ya	Ya

AWS aplikasi yang dikelola	Terintegrasi dengan instans akun IAM Identity Center	Memungkinkan penyebaran identitas tepercaya melalui Pusat Identitas IAM	Mendukung Pusat Identitas IAM yang dikonfigurasi dengan kunci K MS yang dikelola pelanggan	Mendukung penerapan di Wilayah tambahan Pusat Identitas IAM
Amazon EMR Studio	Ya	Ya	Ya	Ya
Amazon Kendra	Tidak	Tidak	Ya	Tidak
Amazon Managed Grafana	Tidak	Tidak	Ya	Tidak
Amazon Monitor	Tidak	Tidak	Ya	Tidak
OpenSearch Layanan Amazon	Ya	Ya	Ya	Tidak
OpenSearch Layanan Amazon Serverless Service	Ya	Ya	Ya	Tidak
Bisnis Amazon Q	Ya	Ya	Ya	Tidak
Amazon Quick	Ya	Ya	Ya	Tidak
Amazon Redshift	Ya ²	Ya	Ya	Ya
Amazon S3 Access Grants	Ya	Ya	Ya	Ya
SageMaker Studio Amazon	Tidak	Ya	Ya	Tidak
Studio SageMaker Terpadu Amazon	Ya	Ya	Ya	Ya

AWS aplikasi yang dikelola	Terintegrasi dengan instans akun IAM Identity Center	Memungkinkan penyebaran identitas tepercaya melalui Pusat Identitas IAM	Mendukung Pusat Identitas IAM yang dikonfigurasi dengan kunci K MS yang dikelola pelanggan	Mendukung penerapan di Wilayah tambahan Pusat Identitas IAM
Amazon WorkMail	Ya	Ya	Ya	Tidak
Amazon WorkSpaces	Ya	Tidak	Ya	Tidak
Amazon WorkSpaces Secure Browser	Tidak	Tidak	Ya	Tidak
AWS akses akun (manajer akses akun)	Tidak	Ya	Ya	No. ³
AWS App Studio	Ya	Tidak	Tidak	Tidak
AWS Deadline Cloud	Ya	Tidak	Ya	Ya
Agen AWS DevOps	Ya	Ya	Ya	Ya
AWS Glue	Ya	Ya	Ya	Ya
AWS IoT Events	Tidak	Tidak	Tidak	Tidak
AWS IoT SiteWise	Tidak	Tidak	Tidak	Tidak
AWS Lake Formation	Ya	Ya	Ya	Ya
AWS re:Post Privat	Ya	Tidak	Ya	Tidak
Rantai Pasokan AWS	Ya	Tidak	Ya	Tidak
AWS Agen Keamanan	Ya	Ya	Ya	Tidak

AWS aplikasi yang dikelola	Terintegrasi dengan instans akun IAM Identity Center	Memungkinkan penyebaran identitas tepercaya melalui Pusat Identitas IAM	Mendukung Pusat Identitas IAM yang dikonfigurasi dengan kunci K MS yang dikelola pelanggan	Mendukung penerapan di Wilayah tambahan Pusat Identitas IAM
AWS Systems Manager	Tidak	Tidak	Ya	Ya - Desktop Jarak Jauh Manajer Armada
AWS Transfer Family aplikasi web	Ya	Ya	Ya	Ya
AWS Transformasi	Ya	Tidak	Ya	Tidak
Akses Terverifikasi AWS	Tidak	Tidak	Ya	Tidak
Kiro	Ya ¹	Ya	Ya	Tidak
Multi-party persetujuan	Tidak	Ya	Ya	Tidak
OpenSearch user interface (Dashboards)	Ya	Ya	Ya	Tidak

¹ Untuk Kiro, instance akun IAM Identity Center didukung kecuali pengguna Anda memerlukan akses ke rangkaian lengkap fitur Kiro di situs web. AWS Untuk informasi selengkapnya, lihat [Menyiapkan Kiro](#) di Panduan Pengguna Kiro.

² Untuk Amazon Redshift, instance akun IAM Identity Center didukung kecuali untuk aplikasi seperti Query Editor v2 yang memerlukan kumpulan izin, yang tidak didukung oleh instans akun.

³ Anda mengaktifkan manajer akses akun di Wilayah utama Pusat Identitas IAM, yang membuat aplikasi akses AWS akun tersedia di sana. Anda dapat mereplikasi instance pengelola akses akun ke Wilayah tambahan Pusat Identitas IAM untuk membuat aplikasi akses AWS akun tersedia di Wilayah tambahan tersebut.

 Note

Beberapa AWS layanan seperti Connect Custom AWS Client VPN er dan tidak tercantum dalam tabel ini meskipun Anda dapat menggunakannya dengan Pusat Identitas IAM. Ini karena mereka berintegrasi dengan IAM Identity Center secara eksklusif menggunakan SAML dan oleh karena itu dikategorikan sebagai aplikasi yang dikelola [pelanggan](#).

Mulai cepat: Menyiapkan Pusat Identitas IAM untuk menguji AWS aplikasi yang dikelola

Jika administrator belum memberi Anda akses ke Pusat Identitas IAM, Anda dapat menggunakan langkah-langkah dalam topik ini untuk mengatur Pusat Identitas IAM untuk menguji aplikasi yang AWS dikelola. Anda akan mempelajari cara mengaktifkan Pusat Identitas IAM, membuat pengguna langsung di Pusat Identitas IAM, dan menetapkan pengguna tersebut ke aplikasi terkel AWS ola.

Topik ini menyediakan langkah-langkah awal cepat tentang cara mengaktifkan Pusat Identitas IAM dengan salah satu cara berikut:

- Dengan AWS Organizations — Jika Anda memilih opsi ini, instance organisasi dari Pusat Identitas IAM akan dibuat.
- Hanya di spesifik Anda Akun AWS — Jika Anda memilih opsi ini, instance akun Pusat Identitas IAM akan dibuat.

Untuk informasi tentang jenis instance ini, lihat [Instans organisasi dan akun dari Pusat Identitas IAM](#).

Prasyarat

Sebelum Anda mengaktifkan Pusat Identitas IAM, konfirmasi hal berikut:

- Anda memiliki Akun AWS — Jika Anda tidak memiliki Akun AWS, lihat Mem [ulai dengan an Akun AWS](#) di Panduan Referensi Manajemen AWS Akun.
- Aplikasi AWS terkelola bekerja dengan Pusat Identitas IAM — Tinjau daftar [AWS aplikasi terkelola yang dapat Anda gunakan dengan IAM Identity Center](#) untuk mengonfirmasi bahwa aplikasi terkel AWS ola yang ingin Anda uji berfungsi dengan Pusat Identitas IAM.

- Anda telah meninjau Pertimbangan Regional — Pastikan AWS aplikasi terkelola yang ingin Anda uji didukung di Wilayah AWS tempat Anda mengaktifkan Pusat Identitas IAM. Untuk informasi selengkapnya, lihat dokumentasi untuk aplikasi AWS terkelola.

 Note

Anda harus menerapkan aplikasi ter AWS kelola di Wilayah yang sama tempat Anda berencana mengaktifkan Pusat Identitas IAM.

Menyiapkan instance organisasi dari Pusat Identitas IAM untuk diuji AWS aplikasi yang dikelola

 Note

Topik ini menjelaskan cara mengaktifkan Pusat Identitas IAM dengan AWS Organizations, yang merupakan cara yang disarankan untuk mengaktifkan Pusat Identitas IAM.

Konfirmasikan izin Anda

Untuk mengaktifkan Pusat Identitas IAM dengan AWS Organizations, Anda harus masuk ke Konsol AWS Manajemen sebagai salah satu dari berikut ini:

- Pengguna dengan izin administratif di Akun AWS tempat IAM Identity Center akan diaktifkan. AWS Organizations
- Pengguna root (tidak disarankan kecuali tidak ada pengguna administratif lain).

 Important

Pengguna root memiliki akses ke semua AWS layanan dan sumber daya di akun. Sebagai praktik terbaik keamanan, kecuali Anda tidak memiliki kredenSIAL lain, jangan gunakan kredenSIAL root akun Anda untuk mengakses AWS sumber daya. KredenSIAL ini menyediakan akses akun tidak terbatas dan sulit untuk dicabut.

Langkah 1. Aktifkan Pusat Identitas IAM dengan AWS Organizations

1. Lakukan salah satu hal berikut untuk masuk ke Konsol Manajemen AWS.
 - Baru untuk AWS (pengguna root) - Masuk sebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.
 - Sudah menggunakan AWS dengan mandiri Akun AWS (kredensial IAM) - Masuk menggunakan kredensial IAM Anda dengan izin administratif.
2. Pada halaman Beranda Konsol AWS Manajemen, pilih layanan Pusat Identitas IAM atau navigasikan ke konsol Pusat Identitas IAM [tas IAM](#).
3. Pilih Aktifkan, dan aktifkan Pusat Identitas IAM dengan AWS Organizations. Ketika Anda melakukan ini, Anda membuat instance [organisasi](#) dari Pusat Identitas IAM.

Langkah 2. Membuat pengguna administratif di Pusat Identitas IAM

Prosedur ini menjelaskan cara membuat pengguna secara langsung di direktori Pusat Identitas bawaan. Direktori ini tidak terhubung ke direktori lain yang mungkin digunakan administrator Anda untuk mengelola pengguna tenaga kerja. Setelah Anda membuat pengguna di Pusat Identitas IAM, Anda akan menentukan kredensial baru untuk pengguna ini. Saat Anda masuk sebagai pengguna ini untuk menguji aplikasi terkelola AWS Anda, Anda akan masuk dengan kredensial baru, bukan dengan kredensial yang ada yang Anda gunakan untuk mengakses sumber daya perusahaan.

Note

Sebaiknya gunakan metode ini untuk membuat pengguna hanya untuk tujuan pengujian.

1. Di panel navigasi konsol Pusat Identitas IAM, pilih Pengguna, lalu pilih Tambah pengguna.
2. Ikuti panduan di konsol untuk menambahkan pengguna. Tetapkan Kirim email ke pengguna ini dengan instruksi pengaturan kata sandi yang dipilih dan pastikan Anda menentukan alamat email yang dapat Anda akses.
3. Di panel navigasi, pilih Akun AWS, pilih kotak centang di sebelah akun Anda, lalu pilih Tetapkan pengguna atau grup.
4. Pilih tab Pengguna, pilih kotak centang di sebelah pengguna yang baru saja Anda tambahkan, dan pilih Berikutnya.

5. Pilih **Buat kumpulan izin**, dan ikuti panduan di konsol untuk membuat kumpulan izin yang **AdministratorAccess** telah ditentukan sebelumnya.
6. Setelah selesai, kumpulan izin baru muncul dalam daftar. Tutup tab **Kumpulan izin** di jendela browser Anda, kembali ke tab **Tetapkan pengguna dan grup**, dan pilih ikon refresh di samping **Buat kumpulan izin**.
7. Pada tab browser **Tetapkan pengguna dan grup**, kumpulan izin baru muncul dalam daftar. Pilih kotak centang di samping nama kumpulan izin, pilih **Berikutnya**, lalu pilih **Kirim**.
8. Keluar dari konsol.

Langkah 3. Masuk ke AWS akses portal sebagai pengguna administratif

Portal AWS akses adalah portal web yang menyediakan pengguna yang Anda buat dengan akses ke konsol AWS Manajemen. Sebelum Anda dapat masuk ke portal AWS akses, Anda harus menerima undangan untuk bergabung dengan Pusat Identitas IAM dan mengaktifkan kredentif pengguna Anda.

1. Periksa email Anda untuk baris subjek **Undangan untuk bergabung dengan Pusat Identitas AWS IAM**.
2. Pilih **Terima undangan**, dan ikuti panduan di halaman pendaftaran untuk menetapkan kata sandi baru, masuk, dan mendaftarkan perangkat MFA untuk pengguna Anda.
3. Setelah Anda mendaftarkan perangkat MFA Anda, portal AWS akses terbuka.
4. Di portal AWS akses, pilih **Anda Akun AWS** dan pilih **AdministratorAccess**. Anda akan diarahkan ke Konsol AWS Manajemen.

Langkah 4. Konfigurasi AWS aplikasi yang dikelola untuk menggunakan Pusat Identitas IAM

1. Saat Anda masuk ke Konsol AWS Manajemen, buka konsol untuk aplikasi ter AWS kelola yang akan Anda gunakan.
2. Ikuti panduan di konsol untuk mengonfigurasi aplikasi terkel AWS ola untuk menggunakan Pusat Identitas IAM. Selama proses ini, Anda dapat menetapkan pengguna yang Anda buat ke aplikasi.

Menyiapkan instance akun Pusat Identitas IAM untuk diuji AWS aplikasi yang dikelola

Note

Instance akun IAM Identity Center membatasi penerapan Anda menjadi satu Akun AWS. Anda harus mengaktifkan instance ini Wilayah AWS sama dengan AWS aplikasi yang ingin Anda uji.

Konfirmasikan aplikasi Anda

Semua aplikasi AWS terkelola yang bekerja dengan Pusat Identitas IAM dapat digunakan dengan instans organisasi Pusat Identitas IAM. Namun, hanya beberapa aplikasi ini yang dapat digunakan dengan instance akun IAM Identity Center. Tinjau daftar [AWS aplikasi terkelola yang dapat Anda gunakan dengan IAM Identity Center](#).

Langkah1. Mengaktifkan instance akun Pusat Identitas IAM

1. Lakukan salah satu hal berikut untuk masuk ke Konsol Manajemen AWS.
 - Baru untuk AWS (pengguna root) - Masuk sebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.
 - Sudah menggunakan AWS dengan mandiri Akun AWS (kredenSIAL IAM) - Masuk menggunakan kredenSIAL IAM Anda dengan izin administratif.
2. Pada halaman Beranda Konsol AWS Manajemen, pilih layanan Pusat Identitas IAM atau navigasikan ke konsol Pusat Identi [tas IAM](#).
3. Pilih Aktifkan.
4. Pada AWS Organizations halaman Aktifkan Pusat Identitas IAM dengan, pilih aktifkan instance akun Pusat Identitas IAM.
5. Pada halaman Aktifkan instance akun Pusat Identitas IAM, tinjau informasi dan secara opsional tambahkan tag yang ingin Anda kaitkan dengan instance akun ini. Kemudian pilih Aktifkan.

Langkah 2. Membuat pengguna di Pusat Identitas IAM

Prosedur ini menjelaskan cara membuat pengguna secara langsung di direktori Pusat Identitas bawaan. Direktori ini tidak terhubung ke direktori lain yang mungkin digunakan administrator Anda

untuk mengelola pengguna tenaga kerja. Setelah Anda membuat pengguna di Pusat Identitas IAM, Anda akan menentukan kredensial baru untuk pengguna ini. Saat Anda masuk sebagai pengguna ini untuk menguji aplikasi ter AWS kelola Anda, Anda akan masuk dengan kredensial baru. Kredensial baru tidak akan memungkinkan Anda mengakses sumber daya perusahaan lainnya.

 Note

Kami menyarankan Anda menggunakan metode ini untuk membuat pengguna hanya untuk tujuan pengujian.

1. Di panel navigasi konsol Pusat Identitas IAM, pilih **Pengguna**, lalu pilih **Tambah pengguna**.
2. Ikuti panduan di konsol untuk menambahkan pengguna. Setiap Kirim email ke pengguna ini dengan instruksi pengaturan kata sandi yang dipilih dan pastikan Anda menentukan alamat email yang dapat Anda akses.
3. Keluar dari konsol.

Langkah 3. Masuk ke AWS akses portal sebagai pengguna Pusat Identitas IAM Anda

Portal AWS akses adalah portal web yang menyediakan pengguna yang Anda buat dengan akses ke konsol AWS Manajemen. Sebelum Anda dapat masuk ke portal AWS akses, Anda harus menerima undangan untuk bergabung dengan Pusat Identitas IAM dan mengaktifkan kredensial pengguna Anda.

1. Periksa email Anda untuk baris subjek **Undangan untuk bergabung dengan Pusat Identitas AWS**.
2. Pilih **Terima undangan**, dan ikuti panduan di halaman pendaftaran untuk menetapkan kata sandi baru, masuk, dan mendaftarkan perangkat MFA untuk pengguna Anda.
3. Setelah Anda mendaftarkan perangkat MFA Anda, portal AWS akses terbuka. Ketika aplikasi tersedia untuk Anda, Anda akan menemukannya di bawah **Aplikasi**.

 Note

AWS aplikasi yang mendukung instance akun memungkinkan pengguna untuk masuk ke aplikasi tanpa memerlukan izin tambahan. Oleh karena itu, **Akun** akan tetap kosong.

Langkah 4. Konfigurasi AWS aplikasi yang dikelola untuk menggunakan Pusat Identitas IAM

1. Saat Anda masuk ke Konsol AWS Manajemen, buka konsol untuk aplikasi ter AWS kelola yang akan Anda gunakan.
2. Ikuti panduan di konsol untuk mengonfigurasi aplikasi terkel AWS ola untuk menggunakan Pusat Identitas IAM. Selama proses ini, Anda dapat menetapkan pengguna yang Anda buat ke aplikasi.

Melihat dan mengubah detail tentang AWS aplikasi yang dikelola

Setelah Anda menghubungkan aplikasi AWS terkelola ke Pusat Identitas IAM dengan menggunakan konsol atau API untuk aplikasi, aplikasi terdaftar di Pusat Identitas IAM. Setelah aplikasi terdaftar di Pusat Identitas IAM, Anda dapat melihat dan mengubah detail tentang aplikasi di konsol Pusat Identitas IAM.

Informasi tentang aplikasi mencakup apakah tugas pengguna dan grup diperlukan, dan jika berlaku, pengguna dan grup yang ditugaskan serta aplikasi tepercaya untuk propagasi identitas. Untuk informasi tentang propagasi identitas tepercaya, lihat [Ikhtisar propagasi identitas tepercaya](#).

Untuk melihat dan mengubah informasi tentang AWS aplikasi yang dikelola di konsol Pusat Identitas IAM

1. Buka konsol [Pusat Identi](#) tas IAM.
2. Pilih Aplikasi.
3. Pilih tab yang AWS dikelola.
4. Pilih tautan untuk aplikasi terkelola yang ingin Anda buka dan lihat.
5. Jika Anda ingin mengubah informasi tentang aplikasi terkel AWS ola, pilih T indakan, lalu pilih Edit Detail.
6. Anda dapat mengubah nama tampilan aplikasi, deskripsi, serta metode penugasan pengguna dan grup.
 - a. Untuk mengubah nama tampilan, masukkan nama yang diinginkan di bidang Nama tampilan dan pilih S impan perubahan.
 - b. Untuk mengubah deskripsi, masukkan deskripsi yang diinginkan di bidang Deskripsi dan pilih S impan perubahan.

- c. Untuk mengubah metode penugasan pengguna dan grup, buat perubahan yang diinginkan dan pilih Simpan perubahan. Untuk informasi selengkapnya, lihat [the section called “Pengguna, grup, dan penyedia”](#).

Menonaktifkan AWS aplikasi yang dikelola

Untuk mencegah pengguna melakukan otentikasi ke aplikasi ter AWS kelola, Anda dapat menonaktifkan aplikasi di konsol Pusat Identitas IAM.

Untuk menonaktifkan AWS aplikasi yang dikelola

1. Buka konsol [Pusat Identitas IAM](#).
2. Pilih Aplikasi.
3. Pada halaman Aplikasi, di bawah AWS aplikasi ter kelola, pilih aplikasi yang ingin Anda nonaktifkan.
4. Dengan aplikasi yang dipilih, pilih Tindakan, lalu pilih Non aktifkan.
5. Di kotak dialog Nonaktifkan aplikasi, pilih Non aktifkan.
6. Dalam daftar AWS aplikasi terkelola, status aplikasi muncul sebagai Tidak aktif.

Note

Jika aplikasi ter AWS kelola dinonaktifkan, Anda dapat memulihkan kemampuan pengguna untuk melakukan otentikasi ke aplikasi dengan memilih Tindakan lalu Aktifkan.

Mengaktifkan sesi konsol yang ditingkatkan identitas

Sesi yang disempurnakan identitas untuk konsol meningkatkan sesi AWS konsol pengguna dengan menyediakan beberapa konteks pengguna tambahan untuk mempersonalisasi pengalaman pengguna tersebut. Kemampuan ini saat ini didukung untuk pengguna Amazon Q Developer Pro [Amazon Q di AWS aplikasi dan situs web](#).

Anda dapat mengaktifkan sesi konsol yang ditingkatkan identitas tanpa membuat perubahan apapun pada pola akses atau federasi yang ada ke AWS konsol. Jika pengguna Anda masuk ke AWS konsol dengan IAM (misalnya, jika mereka masuk sebagai pengguna IAM atau melalui akses federasi

dengan IAM), mereka dapat terus menggunakan metode ini. Jika pengguna Anda masuk ke portal AWS akses, mereka dapat terus menggunakan kredentif pengguna Pusat Identitas IAM mereka.

Topik

- [Prasyarat dan pertimbangan](#)
- [Cara mengaktifkan sesi konsol yang ditingkatkan identitas](#)
- [Cara kerja sesi konsol yang ditingkatkan identitas](#)

Prasyarat dan pertimbangan

Sebelum Anda mengaktifkan sesi konsol yang ditingkatkan identitas, tinjau prasyarat dan pertimbangan berikut:

- Jika pengguna mengakses Amazon Q di AWS aplikasi dan situs web melalui langganan Amazon Q Developer Pro, Anda harus mengaktifkan sesi konsol yang ditingkatkan identitas.

Note

Pengguna Amazon Q Developer dapat mengakses Amazon Q tanpa sesi yang ditingkatkan identitas, tetapi mereka tidak akan memiliki akses ke langganan Amazon Q Developer Pro mereka.

- Identity-enhanced sesi konsol memerlukan instance [organisasi](#) dari Pusat Identitas IAM.
- Integrasi dengan Amazon Q tidak didukung jika Anda mengaktifkan Pusat Identitas IAM dalam pilihan. Wilayah AWS
- Untuk mengaktifkan sesi konsol yang ditingkatkan identitas, Anda harus memiliki izin berikut:
 - `sso:CreateApplication`
 - `sso:GetSharedSsoConfiguration`
 - `sso:ListApplications`
 - `sso:PutApplicationAssignmentConfiguration`
 - `sso:PutApplicationAuthenticationMethod`
 - `sso:PutApplicationGrant`
 - `sso:PutApplicationAccessScope`
 - `signin:CreateTrustedIdentityPropagationApplicationForConsole`
 - `signin:ListTrustedIdentityPropagationApplicationsForConsole`

- Untuk memungkinkan pengguna menggunakan sesi konsol yang ditingkatkan identitas, Anda harus memberi mereka `sts:setContext` izin dalam kebijakan berbasis identitas. Untuk selengkapnya, lihat [Memberikan izin kepada pengguna untuk menggunakan sesi konsol yang ditingkatkan identitas](#).

Cara mengaktifkan sesi konsol yang ditingkatkan identitas

Anda dapat mengaktifkan sesi konsol yang ditingkatkan identitas di konsol Amazon Q atau di konsol Pusat Identitas IAM.

Aktifkan sesi konsol yang ditingkatkan identitas di konsol Amazon Q

Sebelum mengaktifkan sesi konsol yang disempurnakan identitas, Anda harus memiliki instance organisasi Pusat Identitas IAM dengan sumber identitas yang terhubung. Jika Anda telah mengonfigurasi Pusat Identitas IAM, lewati ke langkah 3.

1. Buka konsol Pusat Identitas IAM. Pilih **Aktifkan**, dan buat instance organisasi dari Pusat Identitas IAM. Untuk informasi, lihat [Aktifkan Pusat Identitas IAM](#).
2. Hubungkan sumber identitas Anda ke Pusat Identitas IAM dan sediakan pengguna ke Pusat Identitas IAM. Anda dapat menghubungkan sumber identitas yang ada ke Pusat Identitas IAM atau menggunakan direktori Pusat Identitas jika Anda belum menggunakan sumber identitas lain. Untuk informasi selengkapnya, lihat [Tutorial sumber identitas Pusat Identitas IAM](#).
3. Setelah Anda selesai menyiapkan Pusat Identitas IAM, buka konsol Amazon Q dan ikuti langkah-langkah di [Lang 3](#) di Panduan Pengguna Pengembang Amazon Q. Pastikan untuk mengaktifkan sesi konsol yang ditingkatkan identitas.

Note

Jika Anda tidak memiliki izin yang cukup untuk mengaktifkan sesi konsol yang ditingkatkan identitas, Anda mungkin perlu meminta administrator Pusat Identitas IAM untuk melakukan tugas ini untuk Anda di konsol Pusat Identitas IAM. Untuk informasi selengkapnya, lihat prosedur berikutnya.

Aktifkan sesi konsol yang ditingkatkan identitas di konsol Pusat Identitas IAM

Jika Anda adalah administrator Pusat Identitas IAM, Anda mungkin diminta oleh administrator lain untuk mengaktifkan sesi konsol yang disempurnakan identitas di konsol Pusat Identitas IAM.

1. Buka konsol Pusat Identitas IAM.
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Di bawah Aktifkan sesi yang disempurnakan identitas, pilih Aktifkan.
4. Di pesan kedua, pilih Aktifkan.
5. Setelah Anda selesai mengaktifkan sesi konsol yang ditingkatkan identitas, pesan konfirmasi muncul di bagian atas halaman Peng aturan.
6. Di bagian Detail, status untuk Identity-enhanced sesi adalah Di aktifkan.

Cara kerja sesi konsol yang ditingkatkan identitas

Pusat Identitas IAM meningkatkan sesi konsol pengguna saat ini untuk menyertakan ID pengguna Pusat Identitas IAM yang aktif dan ID sesi Pusat Identitas IAM.

Identity-enhanced sesi konsol mencakup tiga nilai berikut:

- Identity store user ID ([toko identitas: UserId](#)) - Nilai ini digunakan untuk mengidentifikasi pengguna secara unik di sumber identitas yang terhubung ke Pusat Identitas IAM.
- Direktori penyimpanan identitas ARN ([toko identitas: IdentityStoreArn](#)) - Nilai ini adalah ARN dari penyimpanan identitas yang terhubung ke Pusat Identitas IAM, dan tempat Anda dapat mencari atribut untuk `identitystore:UserId`.
- ID sesi Pusat Identitas IAM - Nilai ini menunjukkan apakah sesi Pusat Identitas IAM pengguna masih valid.

Nilai-nilainya sama, tetapi diperoleh dengan cara yang berbeda dan ditambahkan pada titik proses yang berbeda, tergantung pada bagaimana pengguna masuk:

- Pusat Identitas IAM (portal AWS akses): Dalam hal ini, ID pengguna penyimpanan identitas pengguna dan nilai ARN sudah disediakan dalam sesi Pusat Identitas IAM yang aktif. IAM Identity Center meningkatkan sesi saat ini dengan hanya menambahkan ID sesi.
- Metode masuk lainnya: Jika pengguna masuk AWS sebagai pengguna IAM, dengan peran IAM, atau sebagai pengguna federasi dengan IAM, tidak ada nilai ini yang disediakan. IAM Identity Center meningkatkan sesi saat ini dengan menambahkan ID pengguna penyimpanan identitas, direktori penyimpanan identitas ARN, dan ID sesi.

Aplikasi yang dikelola pelanggan

Pusat Identitas IAM bertindak sebagai layanan identitas pusat untuk pengguna dan grup tenaga kerja Anda. Jika Anda sudah menggunakan penyedia identitas (IdP), Pusat Identitas IAM dapat mengintegrasikan dengan IdP Anda sehingga Anda dapat menyediakan pengguna dan grup ke Pusat Identitas IAM dan menggunakan IdP Anda untuk otentikasi. Dengan satu koneksi, Pusat Identitas IAM mewakili IdP Anda di depan beberapa Layanan AWS dan memungkinkan aplikasi OAuth 2.0 Anda untuk meminta akses ke data dalam layanan ini atas nama pengguna Anda. Anda juga dapat menggunakan Pusat Identitas IAM untuk menetapkan akses pengguna Anda ke aplikasi [SAML 2.0](#). Ini termasuk AWS layanan seperti Connect Customer dan AWS Client VPN, yang terintegrasi dengan IAM Identity Center secara eksklusif menggunakan SAML dan oleh karena itu dikategorikan sebagai aplikasi yang dikelola pelanggan.

- Jika aplikasi Anda mendukung Token Web JSON (JWT), Anda dapat menggunakan fitur propagasi identitas tepercaya dari Pusat Identitas IAM untuk memungkinkan aplikasi Anda meminta akses ke data Layanan AWS atas nama pengguna Anda. Propagasi identitas tepercaya dibangun di atas Kerangka OAuth 2.0 Otorisasi dan mencakup opsi untuk aplikasi untuk bertukar token identitas yang berasal dari server otorisasi OAuth 2.0 eksternal untuk token yang dikeluarkan oleh IAM Identity Center dan diakui oleh. Layanan AWS Untuk informasi selengkapnya, lihat [Kasus penggunaan propagasi identitas tepercaya](#).
- Jika aplikasi Anda mendukung SAML 2.0, Anda dapat menghubungkannya ke instance [organisasi Pusat Identitas IAM](#). Anda dapat menggunakan Pusat Identitas IAM untuk menetapkan akses ke aplikasi SAML 2.0 Anda.

Note

Saat mengintegrasikan aplikasi yang dikelola pelanggan dengan instance Pusat Identitas IAM yang menggunakan kunci KMS yang dikelola [pelanggan](#), verifikasi apakah aplikasi memanggil API layanan Pusat Identitas IAM. Jika ya, lihat kebijakan kunci [KMS dasar](#) untuk izin yang diperlukan.

Topik

- [Akses masuk tunggal ke aplikasi SAML 2.0 dan OAuth 2.0](#)
- [Menyiapkan aplikasi SAML 2.0 yang dikelola pelanggan](#)
- [Aktifkan AWS akses akun untuk aplikasi yang dikelola pelanggan](#)

Akses masuk tunggal ke aplikasi SAML 2.0 dan OAuth 2.0

IAM Identity Center memungkinkan Anda untuk memberi pengguna akses masuk tunggal ke aplikasi SAML 2.0 atau OAuth 2.0. Topik berikut memberikan ikhtisar tingkat tinggi tentang SAML 2.0 dan OAuth 2.0.

Topik

- [SAML 2.0](#)
- [OAuth 2.0](#)

SAML 2.0

SAML 2.0 adalah standar industri yang digunakan untuk bertukar pernyataan SAML dengan aman yang menyampaikan informasi tentang pengguna antara otoritas SAML (disebut penyedia identitas atau IdP), dan konsumen SAML 2.0 (disebut penyedia layanan atau SP). Pusat Identitas IAM menggunakan informasi ini untuk menyediakan akses masuk tunggal federasi bagi pengguna yang berwenang untuk menggunakan aplikasi dalam portal akses. AWS

Note

Pusat Identitas IAM tidak mendukung validasi tanda tangan permintaan otentikasi SAML masuk dari aplikasi SAML.

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.

IAM Identity Center memungkinkan aplikasi yang berjalan pada klien publik untuk mengambil kredentif sementara untuk mengakses Akun AWS dan melayani secara terprogram atas nama pengguna mereka. Klien publik biasanya desktop, laptop, atau perangkat seluler lainnya yang digunakan untuk menjalankan aplikasi secara lokal. Contoh AWS aplikasi yang berjalan pada klien publik termasuk AWS Command Line Interface (AWS CLI), AWS Toolkit, dan AWS Perangkat Pengembangan Perangkat Lunak (SDK). Untuk mengaktifkan aplikasi ini untuk mendapatkan kredensial, Pusat Identitas IAM mendukung bagian dari alur OAuth 2.0 berikut:

- Pemberian Kode Otorisasi dengan Kunci Bukti untuk Pertukaran Kode (PKCE) ([RFC 6749 dan RFC 7636](#)) <https://www.rfc-editor.org/rfc/rfc7636>
- Hibah Otorisasi Perangkat ([RFC 86](#) 28)

Note

Jenis hibah ini hanya dapat digunakan dengan Layanan AWS mendukung kemampuan ini. Layanan ini mungkin tidak mendukung jenis hibah ini sama sekali Wilayah AWS. Lihat dokumentasi yang relevan Layanan AWS untuk perbedaan regional.

OpenID Connect (OIDC) adalah protokol otentikasi yang didasarkan pada Kerangka OAuth 2.0. OIDC menentukan cara menggunakan OAuth 2.0 untuk otentikasi. Melalui API layanan OIDC Pusat Identitas [IAM](#), aplikasi mendaftarkan klien OAuth 2.0 dan menggunakan salah satu alur ini untuk mendapatkan token akses yang memberikan izin ke API yang dilindungi IAM Identity Center. Aplikasi menentukan cakupan [akses](#) untuk mendeklarasikan pengguna API yang dituju. Setelah Anda, sebagai administrator Pusat Identitas IAM, mengonfigurasi sumber identitas Anda, pengguna akhir aplikasi Anda harus menyelesaikan proses masuk, jika mereka belum melakukannya. Pengguna akhir Anda kemudian harus memberikan persetujuan mereka untuk mengizinkan aplikasi melakukan panggilan API. Panggilan API ini dilakukan menggunakan izin pengguna. Sebagai tanggapan, Pusat Identitas IAM mengembalikan token akses ke aplikasi yang berisi cakupan akses yang disetujui pengguna.

Menggunakan aliran hibah OAuth 2.0

Alur hibah OAuth 2.0 hanya tersedia melalui aplikasi terkel AWS ola yang mendukung alur. Untuk menggunakan alur OAuth 2.0, instance Pusat Identitas IAM Anda dan aplikasi terkelola yang AWS didukung yang Anda gunakan harus digunakan dalam satu aplikasi. Wilayah AWS Lihat dokumentasi untuk masing-masing Layanan AWS untuk menentukan ketersediaan regional aplikasi terkel AWS ola dan instance Pusat Identitas IAM yang ingin Anda gunakan.

Untuk menggunakan aplikasi yang menggunakan aliran OAuth 2.0, pengguna akhir harus memasukkan URL tempat aplikasi akan terhubung dan mendaftar dengan instance Pusat Identitas IAM Anda. Bergantung pada aplikasi, sebagai administrator, Anda harus memberi pengguna Anda URL portal AWS akses atau URL Pener bit instans Pusat Identitas IAM Anda. Anda dapat menemukan dua pengaturan ini di halaman Peng <https://console.aws.amazon.com/singlesignon/>

aturan konsol Pusat Identitas IAM. Untuk informasi tambahan tentang mengonfigurasi aplikasi klien, lihat dokumentasi aplikasi tersebut.

Pengalaman pengguna akhir untuk masuk ke aplikasi dan memberikan persetujuan tergantung pada apakah aplikasi menggunakan [Pemberian Kode Otorisasi dengan PKCE](#) atau [Hibah Otorisasi Perangkat](#).

Pemberian Kode Otorisasi dengan PKCE

Alur ini digunakan oleh aplikasi yang berjalan pada perangkat yang memiliki browser.

1. Jendela browser terbuka.
2. Jika pengguna belum diautentikasi, browser mengalihkan mereka untuk menyelesaikan otentikasi pengguna.
3. Setelah otentikasi, pengguna disajikan dengan layar persetujuan yang menampilkan informasi berikut:
 - Nama aplikasi
 - Cakupan akses yang diminta aplikasi untuk digunakan
4. Pengguna dapat membatalkan proses persetujuan atau mereka dapat memberikan persetujuan mereka dan aplikasi melanjutkan dengan akses berdasarkan izin pengguna.

Hibah Otorisasi Perangkat

Alur ini dapat digunakan oleh aplikasi yang berjalan pada perangkat dengan atau tanpa browser. Ketika aplikasi memulai alur, aplikasi menyajikan URL dan kode pengguna yang harus diverifikasi pengguna nanti dalam alur. Kode pengguna diperlukan karena aplikasi yang memulai alur mungkin berjalan pada perangkat yang berbeda dari perangkat tempat pengguna memberikan persetujuan. Kode memastikan bahwa pengguna menyetujui aliran yang mereka mulai pada perangkat lain.

Note

Jika Anda memiliki klien yang menggunakan `device.sso.region.amazonaws.com`, Anda harus memperbarui alur otorisasi untuk menggunakan Proof Key for Code Exchange (PKCE). Untuk informasi selengkapnya, lihat [Mengonfigurasi otentikasi Pusat Identitas IAM dengan AWS CLI](#) dalam Panduan AWS Command Line Interface Pengguna.

1. Ketika aliran dimulai dari perangkat dengan browser, jendela browser terbuka. Ketika aliran dimulai dari perangkat tanpa browser, pengguna harus membuka browser di perangkat yang berbeda dan pergi ke URL yang disajikan aplikasi.
2. Dalam kedua kasus tersebut, jika pengguna belum diautentikasi, browser mengalihkan mereka untuk menyelesaikan otentikasi pengguna.
3. Setelah otentikasi, pengguna disajikan dengan layar persetujuan yang menampilkan informasi berikut:
 - Nama aplikasi
 - Cakupan akses yang diminta aplikasi untuk digunakan
 - Kode pengguna yang disajikan aplikasi kepada pengguna
4. Pengguna dapat membatalkan proses persetujuan atau mereka dapat memberikan persetujuan mereka dan aplikasi melanjutkan dengan akses berdasarkan izin pengguna.

Cakupan akses

Lingkup mendefinisikan akses untuk layanan yang dapat diakses melalui aliran OAuth 2.0. Cakupan adalah cara bagi layanan, juga disebut server sumber daya, untuk mengelompokkan izin yang terkait dengan tindakan dan sumber daya layanan, dan mereka menentukan operasi kasar yang dapat diminta klien OAuth 2.0. Ketika klien OAuth 2.0 mendaftar dengan layanan OIDC Pusat Identitas [IAM](#), klien menentukan cakupan untuk menyatakan tindakan yang dimaksudkan, yang pengguna harus memberikan persetujuan.

Klien OAuth 2.0 menggunakan scope nilai seperti yang didefinisikan dalam [bagian 3.3 dari OAuth 2.0 \(RFC 6749\)](#) untuk menentukan izin apa yang diminta untuk token akses. Klien dapat menentukan maksimal 25 cakupan saat meminta token akses. Ketika pengguna memberikan persetujuan selama Pemberian Kode Otorisasi dengan aliran PKCE atau Pemberian Otorisasi Perangkat, Pusat Identitas IAM mengkodekan cakupan ke dalam token akses yang dikembalikan.

AWS menambahkan cakupan ke Pusat Identitas IAM untuk didukung Layanan AWS. Tabel berikut mencantumkan cakupan yang didukung layanan OIDC Pusat Identitas IAM saat Anda mendaftarkan klien publik.

Cakupan akses yang didukung oleh layanan OIDC Pusat Identitas IAM saat mendaftarkan klien publik

Lingkup	Deskripsi	Layanan yang didukung oleh
<code>sso:account:access</code>	Akses akun terkelola Pusat Identitas IAM dan kumpulan izin.	Pusat Identitas IAM
<code>codewhisperer:analysis</code>	Aktifkan akses ke analisis kode Kiro.	ID AWS Builder dan Pusat Identitas IAM
<code>codewhisperer:completions</code>	Aktifkan akses ke saran kode inline Kiro.	ID AWS Builder dan Pusat Identitas IAM
<code>codewhisperer:conversations</code>	Aktifkan akses ke obrolan Kiro.	ID AWS Builder dan Pusat Identitas IAM
<code>codewhisperer:taskassist</code>	Aktifkan akses ke Kiro Agent untuk pengembangan perangkat lunak.	ID AWS Builder dan Pusat Identitas IAM
<code>codewhisperer:transformations</code>	Aktifkan akses ke Kiro Agent untuk transformasi kode.	ID AWS Builder dan Pusat Identitas IAM
<code>codecatalyst:read_write</code>	Baca dan tulis ke CodeCatalyst sumber daya Amazon Anda, memungkinkan akses ke semua sumber daya yang ada.	ID AWS Builder dan Pusat Identitas IAM
<code>verified_access:application:connect</code>	Aktifkan Akses Terverifikasi AWS	Akses Terverifikasi AWS
<code>redshift:connect</code>	Hubungkan ke Amazon Redshift	Amazon Redshift

Lingkup	Deskripsi	Layanan yang didukung oleh
<code>datazone:domain:access</code>	Akses Peran DataZone Eksekusi Domain	Amazon DataZone
<code>nosqlworkbench:datamodeladviser</code>	Membuat dan membaca model data	NoSQL Workbench
<code>transform:read_write</code>	Aktifkan akses ke AWS Transform Agent untuk transformasi kode	AWS Transformasi

Menyiapkan aplikasi SAML 2.0 yang dikelola pelanggan

Jika Anda menggunakan aplikasi yang dikelola pelanggan yang mendukung [SAML 2.0](#), Anda dapat menyatukan IdP ke Pusat Identitas IAM melalui SAML 2.0 dan menggunakan Pusat Identitas IAM untuk mengelola akses pengguna ke aplikasi tersebut. Anda dapat memilih aplikasi SAML 2.0 dari katalog aplikasi yang umum digunakan di konsol IAM Identity Center, atau Anda dapat mengatur aplikasi SAML 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 Layanan AWS, Anda dapat menggunakan propagasi identitas tepercaya. Dengan propagasi identitas tepercaya, pengguna dapat masuk ke aplikasi, dan aplikasi tersebut dapat meneruskan identitas pengguna dalam permintaan untuk mengakses data masuk Layanan AWS.

Topik

- [Menyiapkan aplikasi dari katalog aplikasi Pusat Identitas IAM](#)
- [Siapkan aplikasi SAML 2.0 Anda sendiri](#)

Menyiapkan aplikasi dari katalog aplikasi Pusat Identitas IAM

Anda dapat menggunakan katalog aplikasi di konsol IAM Identity Center untuk menambahkan banyak aplikasi SAML 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 Pusat Identitas IAM dan penyedia layanan aplikasi. Informasi ini tersedia di halaman konfigurasi untuk aplikasi, setelah Anda memilih aplikasi di katalog. Setelah mengonfigurasi aplikasi, Anda dapat menetapkan akses ke pengguna atau grup di Pusat Identitas IAM sesuai kebutuhan.

Gunakan prosedur ini untuk mengatur hubungan kepercayaan SAML 2.0 antara Pusat Identitas IAM dan penyedia layanan aplikasi Anda.

Sebelum Anda memulai prosedur ini, akan sangat membantu untuk 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 menambahkan dan mengonfigurasi aplikasi dari katalog aplikasi

1. Buka konsol [Pusat Identitas IAM](#).
2. Pilih Aplikasi.
3. Pilih tab Customer managed.
4. Pilih Tambah aplikasi.
5. Pada halaman Pilih jenis aplikasi, di bawah preferensi Setup, 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 ketika muncul di hasil pencarian, lalu pilih Berikutnya.
8. Pada halaman Konfigurasi aplikasi, bidang Nama tampilan dan Deskripsi telah diisi sebelumnya dengan detail yang relevan untuk aplikasi. Anda dapat mengedit informasi ini.
9. Di bawah metadata Pusat Identitas IAM, lakukan hal berikut:
 - a. Di bawah file metadata SAML 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 tersebut.

10. (Opsional) Di bawah Properti aplikasi, Anda dapat menentukan URL mulai Aplikasi, Status Relay, dan Durasi sesi. Untuk informasi selengkapnya, lihat [Memahami 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 SAML aplikasi. Kemudian, pilih Pilih file untuk menemukan dan memilih file metadata.
 - b. Jika Anda tidak memiliki file metadata, pilih Ketik nilai metadata secara manual, lalu berikan URL ACS Aplikasi dan nilai audiens SAML Aplikasi.
12. Pilih Kirim. Anda akan dibawa ke halaman detail aplikasi yang baru saja Anda tambahkan.

Siapkan aplikasi SAML 2.0 Anda sendiri

Anda dapat mengatur aplikasi Anda sendiri yang memungkinkan federasi identitas menggunakan SAML 2.0 dan menambahkannya ke Pusat Identitas IAM. Sebagian besar langkah untuk menyiapkan aplikasi SAML 2.0 Anda sendiri sama dengan menyiapkan aplikasi SAML 2.0 dari katalog aplikasi di konsol IAM Identity Center. Namun, Anda juga harus menyediakan pemetaan atribut SAML tambahan untuk aplikasi SAML 2.0 Anda sendiri. Pemetaan ini memungkinkan Pusat Identitas IAM untuk mengisi pernyataan SAML 2.0 dengan benar untuk aplikasi Anda. Anda dapat memberikan pemetaan atribut SAML tambahan ini saat Anda mengatur aplikasi untuk pertama kalinya. Anda juga dapat menyediakan pemetaan atribut SAML 2.0 pada halaman detail aplikasi di konsol Pusat Identitas IAM.

Gunakan prosedur berikut untuk mengatur hubungan kepercayaan SAML 2.0 antara Pusat Identitas IAM dan penyedia layanan aplikasi SAML 2.0 Anda. Sebelum memulai prosedur ini, pastikan Anda memiliki sertifikat penyedia layanan dan file pertukaran metadata sehingga Anda dapat menyelesaikan pengaturan kepercayaan.

Untuk mengatur aplikasi SAML 2.0 Anda sendiri

1. Buka konsol [Pusat Identi](#) tas IAM.
 2. Pilih Aplikasi.
 3. Pilih tab Customer managed.
 4. Pilih Tambah aplikasi.
 5. Pada halaman Pilih jenis aplikasi, di bawah preferensi Setup, pilih Saya memiliki aplikasi yang ingin saya atur.
 6. Di bawah Jenis aplikasi, pilih SAML 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 Pusat Identitas IAM, lakukan hal berikut:
 - a. Di bawah file metadata SAML 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 [Memahami properti aplikasi di konsol Pusat Identitas IAM](#).
 11. Di bawah Metadata aplikasi, pilih Ketik nilai metadata secara manual. Kemudian, berikan nilai pemir sa Application ACS dan Appl ication SAML.
 12. Pilih Kirim. Anda akan dibawa ke halaman detail aplikasi yang baru saja Anda tambahkan.

Aktifkan AWS akses akun untuk aplikasi yang dikelola pelanggan

Anda dapat mengaktifkan akses AWS akun untuk aplikasi yang dikelola pelanggan di IAM Identity Center dengan mengonfigurasi penerbit [token tepercaya](#). Penerbit token tepercaya adalah server

otorisasi OAuth 2.0 yang mengeluarkan token yang ditandatangani atas nama pengguna yang diautentikasi. IAM Identity Center menukar token ini dengan kredensi yang memungkinkan aplikasi Anda mengakses AWS akun dan peran yang ditetapkan secara terprogram kepada pengguna tersebut. Penerbit token tepercaya juga dapat digunakan untuk akses ke aplikasi yang AWS dikelola. Untuk informasi selengkapnya, lihat [Menggunakan aplikasi dengan penerbit token tepercaya](#).

Note

Anda dapat mengaktifkan fitur ini hanya untuk [instance organisasi](#) IAM Identity Center. Hanya administrator akun manajemen atau administrator yang didelegasikan yang dapat mengaktifkan `sso:account:access` ruang lingkup untuk aplikasi yang dikelola pelanggan. Jika Anda adalah pembuat aplikasi di akun anggota, hubungi administrator Pusat Identitas IAM Anda untuk mengaktifkan cakupan ini untuk aplikasi Anda.

Cara kerjanya

Setelah administrator mengaktifkan `sso:account:access` ruang lingkup untuk aplikasi yang dikelola pelanggan, alur kerja berikut akan terjadi:

1. Pengguna masuk ke aplikasi Anda melalui penyedia identitas eksternal (iDP).
2. Aplikasi Anda menerima token JWT yang ditandatangani dari iDP.
3. Aplikasi Anda menukar token ini dengan token IAM Identity Center dengan memanggil `CreateTokenWithIAM` API dengan JWT bearer grant type (`urn:ietf:params:oauth:grant-type:jwt-bearer`). Panggilan ini memerlukan otentikasi Signature Version 4 (SigV4). Untuk informasi selengkapnya, lihat [CreateTokenWithIAM](#) di Referensi API OIDC Pusat Identitas IAM.
4. Aplikasi Anda menggunakan token IAM Identity Center untuk memanggil [operasi API portal](#) (`ListAccounts`, `ListAccountRoles`, `GetRoleCredentials`) untuk menemukan akun dan peran yang ditetapkan kepada pengguna dan mengambil AWS kredensi sementara atas nama mereka.
5. Pengguna mengakses AWS sumber daya melalui aplikasi Anda tanpa langkah masuk tambahan.

Jika Anda mengaktifkan hibah token penyegaran saat menyiapkan aplikasi, kembalikan `CreateTokenWithIAM` juga token penyegaran bersama token akses. Aplikasi Anda dapat menggunakan token penyegaran ini untuk mendapatkan token akses baru tanpa mengulangi

pertukaran token JWT Bearer penuh. Untuk me-refresh token akses, panggil `CreateTokenWithIAM` dengan jenis `refresh_token` hibah.

Prasyarat

Sebelum Anda mengaktifkan akses akun untuk aplikasi yang dikelola pelanggan, Anda perlu:

- [Aplikasi yang dikelola pelanggan](#) yang dikonfigurasi di IAM Identity Center yang mendukung JSON Web Tokens (JWTs). Aplikasi harus memiliki komponen server backend yang dapat menyimpan kredensial dengan aman. Browser-based Aplikasi, seperti aplikasi halaman tunggal (SPA), dan klien publik lainnya tidak didukung untuk fitur ini.
- [Penerbit token terpercaya](#) yang melekat pada aplikasi Anda.
- Akses ke akun AWS Organizations manajemen atau akun administrator yang didelegasikan untuk Pusat Identitas IAM. Pembangun aplikasi di akun anggota tidak dapat mengaktifkan cakupan ini secara langsung.

Aktifkan akses akun

Untuk mengaktifkan cakupan **sso:account:access** untuk aplikasi yang dikelola pelanggan

1. Masuk ke Konsol Manajemen AWS menggunakan akun manajemen organisasi atau akun administrator yang didelegasikan.
2. Buka [konsol Pusat Identitas IAM](#).
3. Pada panel navigasi, pilih Aplikasi.
4. Pilih tab yang dikelola Pelanggan.
5. Pilih nama aplikasi yang ingin Anda konfigurasikan.
6. Di bagian akses AWS akun, nyalakan Aktifkan akses AWS akun.

Setelah Anda mengaktifkan akses akun, aplikasi dapat memanggil operasi API portal Identity secara terprogram untuk mencantumkan akun dan peran, dan mengambil AWS kredensi sementara untuk peran yang diizinkan diakses oleh pengguna yang diautentikasi.

Important

Saat Anda mengaktifkan **sso:account:access** cakupan untuk aplikasi, aplikasi tersebut dapat mengakses semua akun dan peran yang tersedia untuk pengguna yang diautentikasi

melalui penetapan set izin mereka. Anda tidak dapat membatasi aplikasi ke akun atau peran tertentu. Pastikan Anda memahami tingkat akses ini sebelum mengaktifkan fitur ini.

Akses terprogram

Anda dapat menggunakan `PutApplicationAccessScope` API untuk mengaktifkan `sso:account:access` cakupan aplikasi yang dikelola pelanggan secara terprogram. Anda harus memanggil API dari akun manajemen organisasi atau akun administrator yang didelegasikan.

AWS CLI

```
aws sso-admin put-application-access-scope \
  --application-arn
  arn:aws:sso::123456789012:application/ssoins-1234567890abcdef/apl-1234567890abcdef \
  --scope "sso:account:access"
```

Permintaan API:

```
{
  "ApplicationArn":
  "arn:aws:sso::123456789012:application/ssoins-1234567890abcdef/apl-1234567890abcdef",
  "Scope": "sso:account:access"
}
```

Untuk menonaktifkan akses akun, gunakan `DeleteApplicationAccessScope` API dengan ARN aplikasi dan nilai cakupan yang sama.

Untuk informasi selengkapnya, lihat [PutApplicationAccessScope](#) dan [DeleteApplicationAccessScope](#) di Referensi API Pusat Identitas IAM.

Praktik terbaik keamanan

- Ruang `sso:account:access` lingkup memberikan akses aplikasi ke semua akun dan peran yang tersedia untuk pengguna yang diautentikasi. Anda tidak dapat membatasi akses ke akun atau peran tertentu. Hanya aktifkan ruang lingkup ini untuk aplikasi yang memerlukan tingkat akses ini.
- Simpan token akses IAM Identity Center dan refresh token di server backend Anda. Jangan pernah mengeksposnya ke kode sisi klien.
- Jangan mencatat token atau kredensi di log aplikasi, pesan kesalahan, atau output debugging.

- Jangan lewatkan token dalam parameter kueri URL. Gunakan `x-amz-sso_bearer_token` header untuk token akses.
- Gunakan [AWS CloudTrail](#) untuk memantau panggilan API yang dilakukan oleh aplikasi Anda.

Informasi Terkait

- [Aplikasi yang dikelola pelanggan](#)
- [Menggunakan aplikasi dengan penerbit token terpercaya](#)
- [AWS akses Portal API Referensi](#)

Ikhtisar propagasi identitas terpercaya

Propagasi identitas terpercaya adalah fitur Pusat Identitas IAM yang memungkinkan administrator Layanan AWS untuk memberikan izin berdasarkan atribut pengguna seperti asosiasi grup. Dengan propagasi identitas terpercaya, konteks identitas ditambahkan ke peran IAM untuk mengidentifikasi pengguna yang meminta akses ke AWS sumber daya. Konteks ini disebarkan ke yang lain Layanan AWS.

Konteks identitas terdiri dari informasi yang Layanan AWS digunakan untuk membuat keputusan otorisasi ketika mereka menerima permintaan akses. Informasi ini mencakup metadata yang mengidentifikasi pemohon (misalnya, pengguna Pusat Identitas IAM), Layanan AWS akses yang diminta (misalnya, Amazon Redshift), dan ruang lingkup akses (misalnya, akses baca saja). Penerima Layanan AWS menggunakan konteks ini, dan izin apa pun yang diberikan kepada pengguna, untuk mengotorisasi akses ke sumber dayanya.

Manfaat propagasi identitas terpercaya

Penyebaran identitas terpercaya memungkinkan administrator Layanan AWS untuk memberikan izin ke sumber daya, seperti data, menggunakan identitas perusahaan tenaga kerja Anda. Selain itu, mereka dapat mengaudit siapa yang mengakses data apa dengan melihat log layanan atau AWS CloudTrail. Jika Anda adalah administrator Pusat Identitas IAM, Anda mungkin diminta oleh Layanan AWS administrator lain untuk mengaktifkan propagasi identitas terpercaya.

Mengaktifkan propagasi identitas terpercaya

Proses mengaktifkan propagasi identitas terpercaya melibatkan dua langkah berikut:

1. Aktifkan Pusat Identitas IAM dan hubungkan sumber identitas Anda yang ada ke Pusat Identitas IAM - Anda akan terus mengelola identitas tenaga kerja Anda di sumber identitas Anda yang ada; menghubungkannya ke Pusat Identitas IAM akan membuat referensi ke tenaga kerja Anda yang dapat dibagikan oleh semua orang Layanan AWS dalam kasus penggunaan Anda. Ini juga tersedia bagi pemilik data untuk digunakan dalam kasus penggunaan di masa mendatang.
2. Hubun Layanan AWS gkan kasus penggunaan Anda ke Pusat Identitas IAM - Administrator masing-masing Layanan AWS dalam kasus penggunaan propagasi identitas tepercaya mengikuti panduan dalam dokumentasi layanan masing-masing untuk menghubungkan layanan ke Pusat Identitas IAM.

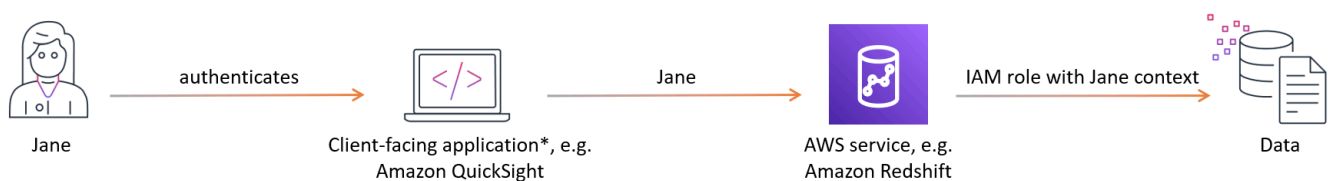
Note

Jika kasus penggunaan melibatkan aplikasi pihak ketiga atau yang dikembangkan pelanggan, Anda mengaktifkan penyebaran identitas tepercaya dengan mengonfigurasi hubungan kepercayaan antara penyedia identitas yang mengotentikasi pengguna aplikasi dan Pusat Identitas IAM. Hal ini memungkinkan aplikasi Anda memanfaatkan aliran propagasi identitas tepercaya yang dijelaskan sebelumnya.

Untuk informasi selengkapnya, lihat [Menggunakan aplikasi dengan penerbit token tepercaya](#).

Cara kerja propagasi identitas tepercaya

Diagram berikut menunjukkan alur kerja tingkat tinggi untuk propagasi identitas tepercaya:



1. Pengguna mengotentikasi dengan aplikasi yang menghadap klien, misalnya Quick.
2. Aplikasi yang Layanan AWS menghadap klien meminta akses untuk menggunakan data kueri dan menyertakan informasi tentang pengguna.

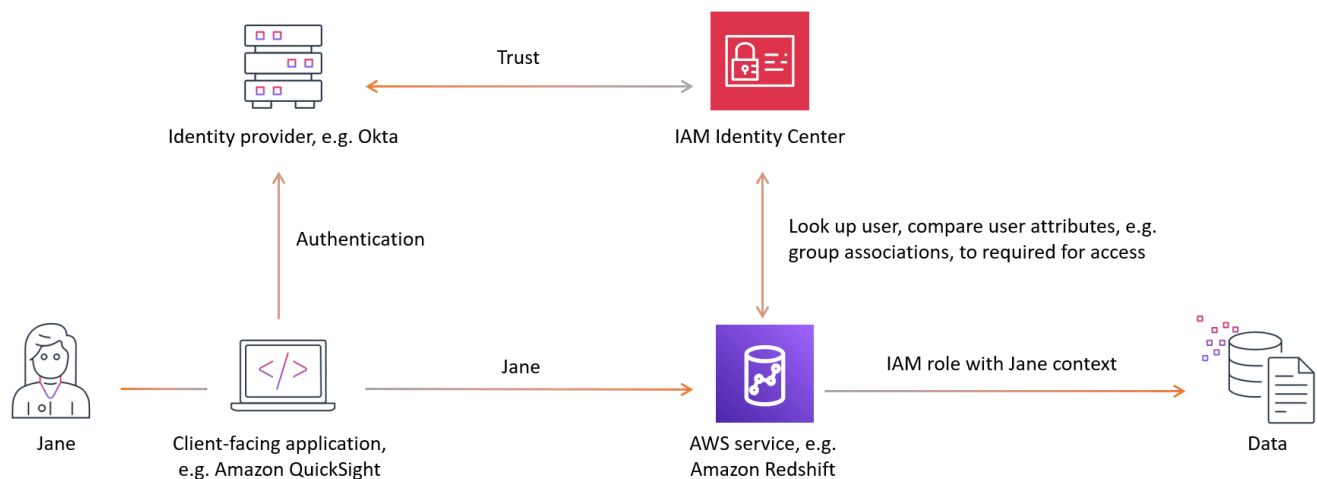
Note

Beberapa kasus penggunaan propagasi identitas tepercaya melibatkan alat yang berinteraksi dengan Layanan AWS menggunakan driver layanan. Anda dapat

mengetahui apakah ini berlaku untuk kasus penggunaan Anda dalam panduan kasus [penggunaan](#).

3. Mem Layanan AWS verifikasi identitas pengguna dengan Pusat Identitas IAM dan membandingkan atribut pengguna, seperti asosiasi grup mereka, dengan yang diperlukan untuk akses. Men Layanan AWS gotorisasi akses selama pengguna atau grup mereka memiliki izin yang diperlukan.
4. Layanan AWS dapat memasukkan pengenalan pengguna di AWS CloudTrail dan di log layanan mereka. Periksa dokumentasi layanan untuk detailnya.

Gambar berikut memberikan ikhtisar langkah-langkah yang dijelaskan sebelumnya dalam alur kerja propagasi identitas terpercaya:



Topik

- [Prasyarat dan pertimbangan](#)
- [Kasus penggunaan propagasi identitas terpercaya](#)
- [Layanan otorisasi](#)

Prasyarat dan pertimbangan

Sebelum Anda mengatur propagasi identitas terpercaya, tinjau prasyarat dan pertimbangan berikut.

Topik

- [Prasyarat](#)

- [Pertimbangan-pertimbangan](#)
- [Pertimbangan untuk aplikasi yang dikelola pelanggan](#)

Prasyarat

Untuk menggunakan propagasi identitas tepercaya, pastikan lingkungan Anda memenuhi prasyarat berikut:

- Mengaktifkan dan menyediakan Pusat Identitas IAM
 - Untuk menggunakan propagasi identitas tepercaya, Anda harus mengaktifkan Pusat Identitas IAM di tempat yang sama Wilayah AWS di mana AWS aplikasi dan layanan yang akan diakses pengguna Anda diaktifkan. Untuk informasi, lihat [Aktifkan Pusat Identitas IAM](#).
 - Instans Organisasi Pusat Identitas IAM direkomendasikan - Sebaiknya gunakan instance [???](#) organisasi Pusat Identitas IAM yang Anda aktifkan di akun manajemen. AWS Organizations Anda dapat [mendelegasikan administ](#)asi instans organisasi Pusat Identitas IAM ke akun anggota. Jika Anda memilih instance [akun Pusat Identi](#)tas IAM, semua Layanan AWS yang ingin Anda akses pengguna dengan propagasi identitas tepercaya harus berada di Akun AWS tempat yang sama di mana Anda mengaktifkan Pusat Identitas IAM. Untuk informasi selengkapnya, lihat [Instans akun Pusat Identitas IAM](#).
 - Hubungkan penyedia identitas Anda yang ada ke Pusat Identitas IAM dan sediakan pengguna dan grup Anda ke Pusat Identitas IAM. Untuk informasi selengkapnya, lihat [Tutorial sumber identitas Pusat Identitas IAM](#).
- Hubungkan AWS aplikasi dan layanan terkelola dalam kasus penggunaan propagasi identitas tepercaya Anda ke Pusat Identitas IAM. Untuk menggunakan propagasi identitas tepercaya, AWS aplikasi terkelola harus terhubung ke Pusat Identitas IAM.

Pertimbangan-pertimbangan

Ingatlah pertimbangan berikut saat mengonfigurasi dan menggunakan propagasi identitas tepercaya:

- Instans organisasi vs akun dari Pusat Identitas IAM
 - Inst [ance organisasi](#) dari Pusat Identitas IAM akan memberi Anda kontrol dan fleksibilitas paling besar untuk mengembangkan kasus penggunaan Anda ke banyak pengguna Akun AWS, dan Layanan AWS. Jika Anda tidak dapat menggunakan instance organisasi, kasus penggunaan Anda mungkin didukung dengan instans akun Pusat Identitas IAM. Untuk mempelajari lebih lanjut tentang instance akun IAM Identity Center yang Layanan AWS mendukung kasus

penggunaan Anda, lihat [AWS aplikasi terkelola yang dapat Anda gunakan dengan IAM Identity Center](#).

- Multi-account izin (kumpulan izin) tidak diperlukan
 - Penyebaran identitas tepercaya tidak mengharuskan Anda menyiapkan izin [multi-akun](#) (kumpulan izin). Anda dapat mengaktifkan Pusat Identitas IAM dan menggunakannya hanya untuk propagasi identitas tepercaya.

Pertimbangan untuk aplikasi yang dikelola pelanggan

Tenaga kerja Anda dapat memperoleh manfaat dari penyebaran identitas tepercaya bahkan jika pengguna Anda berinteraksi dengan aplikasi yang menghadap klien yang tidak dikelola oleh AWS, misalnya, Tableau atau aplikasi yang dikembangkan khusus Anda. Pengguna aplikasi ini mungkin tidak disediakan di Pusat Identitas IAM. Untuk mengaktifkan pengenalan dan otorisasi akses pengguna ke AWS sumber daya yang lancar, Pusat Identitas IAM memungkinkan Anda mengonfigurasi hubungan tepercaya antara penyedia identitas yang mengautentikasi pengguna Anda dan Pusat Identitas IAM. Untuk informasi selengkapnya, lihat [Menggunakan aplikasi dengan penerbit token tepercaya](#).

Selain itu, mengonfigurasi propagasi identitas tepercaya untuk aplikasi Anda akan memerlukan:

- Aplikasi Anda harus menggunakan kerangka kerja OAuth 2.0 untuk otentikasi. Propagasi identitas tepercaya tidak mendukung integrasi SAML 2.0.
- Aplikasi Anda harus diakui oleh Pusat Identitas IAM. Ikuti panduan khusus untuk kasus [penggunaan Anda](#).

Kasus penggunaan propagasi identitas tepercaya

Sebagai administrator Pusat Identitas IAM, Anda mungkin diminta untuk membantu mengonfigurasi propagasi identitas tepercaya dari aplikasi yang menghadap pengguna ke Layanan AWS. Untuk mendukung permintaan ini, Anda memerlukan informasi berikut:

- Aplikasi yang menghadap ke klien apa yang akan digunakan pengguna Anda?
- Yang Layanan AWS digunakan untuk menanyakan data dan untuk mengotorisasi akses ke data?
- Yang Layanan AWS mengizinkan akses ke data?

Peran Anda dalam mengaktifkan kasus penggunaan propagasi identitas tepercaya yang tidak melibatkan aplikasi pihak ketiga atau aplikasi yang dikembangkan khusus adalah untuk:

1. [Aktifkan Pusat](#) Identitas IAM.
2. [Hubungkan sumber identitas Anda yang ada ke Pusat](#) Identitas IAM.

Langkah-langkah yang tersisa dari konfigurasi identitas tepercaya untuk kasus penggunaan ini dilakukan dalam aplikasi yang terhubung Layanan AWS . Administrator yang terhubung Layanan AWS atau aplikasi harus merujuk ke panduan pengguna masing-masing untuk panduan khusus layanan yang komprehensif.

Peran Anda dalam mengaktifkan kasus penggunaan propagasi identitas tepercaya yang melibatkan aplikasi pihak ketiga atau aplikasi yang dikembangkan khusus mencakup langkah-langkah [Aktifkan Pusat Identitas IAM](#) dan [menghubungkan sumber identitas Anda](#) serta:

1. Mengkonfigurasi koneksi penyedia identitas (IdP) Anda ke pihak ketiga atau aplikasi yang dikembangkan khusus.
2. Mengaktifkan Pusat Identitas IAM untuk mengenali pihak ketiga atau aplikasi yang dikembangkan khusus.
3. Mengkonfigurasi IdP Anda sebagai penerbit token tepercaya di Pusat Identitas IAM. Untuk informasi selengkapnya, lihat [Menggunakan aplikasi dengan penerbit token tepercaya](#).

Administrator aplikasi yang terhubung dan Layanan AWS harus merujuk ke panduan pengguna masing-masing untuk panduan khusus layanan yang komprehensif.

Analisis, data lake house, dan kasus penggunaan pembelajaran mesin

Anda dapat mengaktifkan kasus penggunaan propagasi tepercaya dengan layanan analisis dan pembelajaran mesin berikut:

- Amazon Redshift - Untuk panduan, lihat [Propagasi identitas tepercaya dengan Amazon Redshift](#).
- Amazon EMR - Untuk panduan, lihat [Propagasi identitas tepercaya dengan Amazon EMR](#).
- Amazon Athena - Untuk panduan, lihat [Propagasi identitas tepercaya dengan Amazon Athena](#).
- SageMaker Studio - Untuk panduan, lihat [Propagasi identitas tepercaya dengan Amazon SageMaker Studio](#).

Kasus penggunaan tambahan

Anda dapat mengaktifkan Pusat Identitas IAM dan propagasi identitas tepercaya dengan tambahan berikut: Layanan AWS

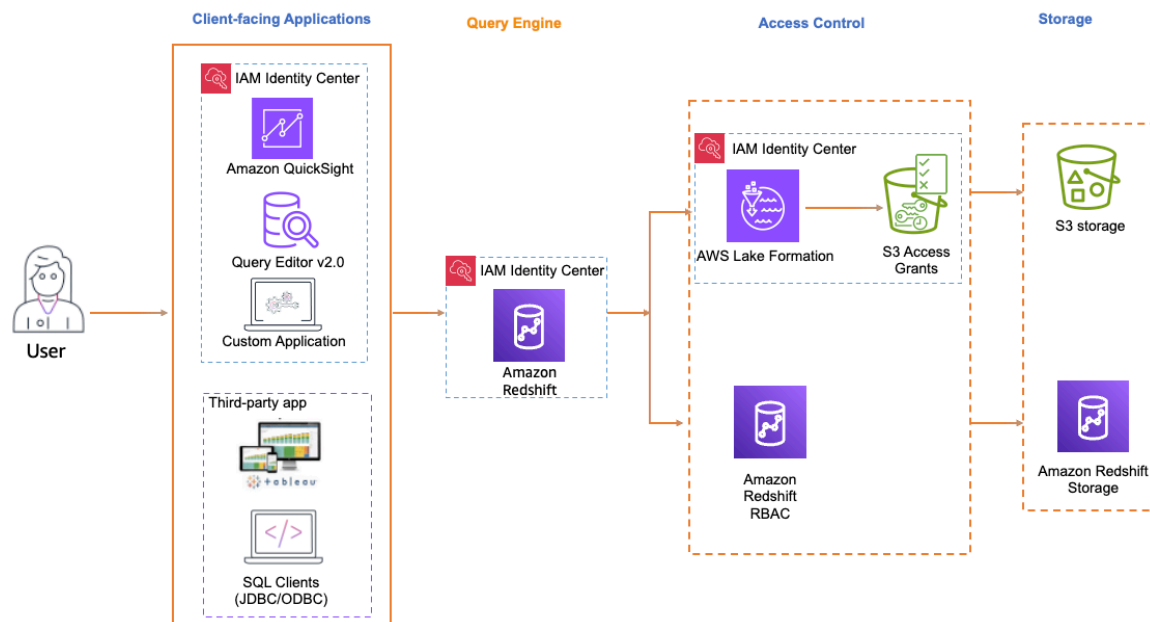
- Amazon Q Business - untuk panduan, lihat:
 - [Alur kerja admin untuk aplikasi yang menggunakan Pusat Identitas IAM.](#)
 - [Mengkonfigurasi aplikasi Amazon Q Business menggunakan Pusat Identitas IAM.](#)
 - [Konfigurasi Amazon Q Business dengan propagasi identitas tepercaya IAM Identity Center.](#)
- OpenSearch Layanan Amazon - untuk panduan, lihat:
 - [Dukungan Propagasi Identitas Tepercaya Pusat Identitas IAM untuk OpenSearch Layanan Amazon.](#)
 - [Antar OpenSearch muka pengguna terpusat \(Dasbor\) dengan OpenSearch Layanan Amazon.](#)
- AWS Transfer Family- untuk panduan, lihat:
 - [Transfer aplikasi web Keluarga.](#)

Topik

- [Propagasi identitas tepercaya dengan Amazon Redshift](#)
- [Propagasi identitas tepercaya dengan Amazon EMR](#)
- [Propagasi identitas tepercaya dengan Amazon Athena](#)
- [Propagasi identitas tepercaya dengan Amazon SageMaker Studio](#)

Propagasi identitas tepercaya dengan Amazon Redshift

Langkah-langkah untuk mengaktifkan propagasi identitas tepercaya bergantung pada apakah pengguna berinteraksi dengan aplikasi ter AWS kelola atau aplikasi yang dikelola pelanggan. Diagram berikut menunjukkan konfigurasi propagasi identitas tepercaya untuk aplikasi yang menghadap klien - baik AWS dikelola atau eksternal AWS - yang menanyakan data Amazon Redshift dengan kontrol akses yang disediakan oleh Amazon Redshift atau oleh layanan otorisasi, seperti AWS Lake Formation atau Amazon S3. Access Grants



Ketika propagasi identitas terpercaya ke Amazon Redshift diaktifkan, administrator Redshift dapat mengonfigurasi Redshift untuk [secara otomatis membuat peran](#) untuk Pusat Identitas IAM sebagai penyedia identitas, memetakan peran Redshift ke grup di Pusat Identitas IAM, dan menggunakan kontrol akses berbasis peran [Redshift untuk memberikan akses](#).

Aplikasi yang menghadap klien yang didukung

AWS aplikasi yang dikelola

Aplikasi terkel AWS ola yang menghadap klien berikut ini mendukung propagasi identitas terpercaya ke Amazon Redshift:

- [Pergeseran Merah Amazon Query Editor V2](#)
- [Quick](#)

Note

Jika Anda menggunakan Amazon Redshift Spectrum untuk mengakses database atau tabel eksternal di AWS Glue Data Catalog, pertimbangkan untuk menyiapkan [Lake Formation](#) dan [Amazon S3 Access Grants](#) untuk menyediakan kontrol akses halus.

Aplikasi yang dikelola pelanggan

Aplikasi yang dikelola pelanggan berikut mendukung propagasi identitas tepercaya ke Amazon Redshift:

- Tableau termasuk Tableau Desktop, Tableau Server, dan Tableau Prep
 - Untuk mengaktifkan penyebaran identitas tepercaya bagi pengguna Tableau, lihat [Integrasi Tableau dan Okta dengan Amazon Redshift menggunakan Pusat Identitas IAM](#) di Blog Data AWS Besar.
- Klien SQL (DBeaver dan DBVisualizer)
 - Untuk mengaktifkan propagasi identitas tepercaya bagi pengguna Klien SQL (DBeaver dan DBVisualizer), lihat Integrasi [Penyedia Identitas \(IdP\) dengan Amazon Redshift Query Editor V2 dan Klien SQL menggunakan Pusat Identitas IAM untuk Single yang mulus Sign-On](#) di Blog AWS Big Data.

Menyiapkan propagasi identitas tepercaya dengan Amazon Redshift Query Editor V2

Prosedur berikut memandu Anda melalui cara mencapai propagasi identitas tepercaya dari Amazon Redshift Query Editor V2 ke Amazon Redshift.

Prasyarat

Sebelum Anda dapat memulai dengan tutorial ini, Anda harus menyiapkan yang berikut:

1. [Aktifkan Pusat](#) Identitas IAM. [Instance organisasi](#) direkomendasikan. Untuk informasi selengkapnya, lihat [Prasyarat dan pertimbangan](#).
2. [Menyediakan pengguna dan grup dari sumber identitas Anda ke Pusat](#) Identitas IAM.

Mengaktifkan propagasi identitas tepercaya mencakup tugas yang dilakukan oleh administrator Pusat Identitas IAM di konsol Pusat Identitas IAM dan tugas yang dilakukan oleh administrator Amazon Redshift di konsol Amazon Redshift.

Tugas yang dilakukan oleh administrator Pusat Identitas IAM

Tugas berikut harus diselesaikan oleh administrator Pusat Identitas IAM:

1. Buat peran [IAM](#) di akun tempat cluster Amazon Redshift atau instans Tanpa Server ada dengan kebijakan izin berikut. Untuk informasi selengkapnya, lihat [Pembuatan Peran IAM](#).
 - Contoh kebijakan berikut mencakup izin yang diperlukan untuk menyelesaikan tutorial ini. Untuk menggunakan kebijakan ini, ganti kebijakan *italicized placeholder text*

dalam contoh dengan informasi Anda sendiri. Untuk petunjuk tambahan, lihat [Membuat kebijakan](#) atau [Mengedit kebijakan](#).

Kebijakan izin:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRedshiftApplication",
      "Effect": "Allow",
      "Action": [
        "redshift:DescribeQev2IdcApplications",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowIDCPpermissions",
      "Effect": "Allow",
      "Action": [
        "sso:DescribeApplication",
        "sso:DescribeInstance"
      ],
      "Resource": [
        "arn:aws:sso:::instance/Your-IAM-Identity-Center-Instance-ID",
        "arn:aws:sso:::111122223333:application/Your-IAM-Identity-Center-Instance-ID/*"
      ]
    }
  ]
}
```

Kebijakan kepercayaan:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "redshift-serverless.amazonaws.com",
          "redshift.amazonaws.com"
        ]
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetContext"
      ]
    }
  ]
}
```

2. Buat kumpulan izin di akun AWS Organizations manajemen tempat Pusat Identitas IAM diaktifkan. Anda akan menggunakannya pada langkah berikutnya untuk mengizinkan pengguna federasi mengakses Redshift Query Editor V2.
 - a. Buka konsol Pusat Identitas IAM, di bawah Multi-Account izin, pilih Set izin.
 - b. Pilih Buat kumpulan izin.
 - c. Pilih Set izin khusus dan kemudian pilih Berikutnya.
 - d. Di bawah AWS kebijakan terkelola, pilih **AmazonRedshiftQueryEditorV2ReadSharing**.
 - e. Di bawah Kebijakan sebaris, tambahkan kebijakan berikut:

JSON

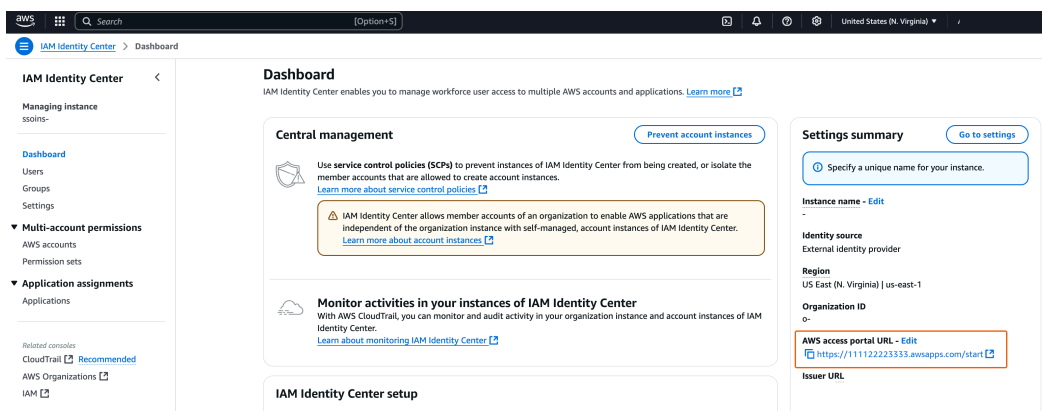
```
{
  "Version": "2012-10-17",
  "Statement": [
```

```

{
  "Sid": "Statement1",
  "Effect": "Allow",
  "Action": [
    "redshift:DescribeQev2IdcApplications",
    "redshift-serverless:ListNamespaces",
    "redshift-serverless:ListWorkgroups",
    "redshift-serverless:GetWorkgroup"
  ],
  "Resource": "*"
}

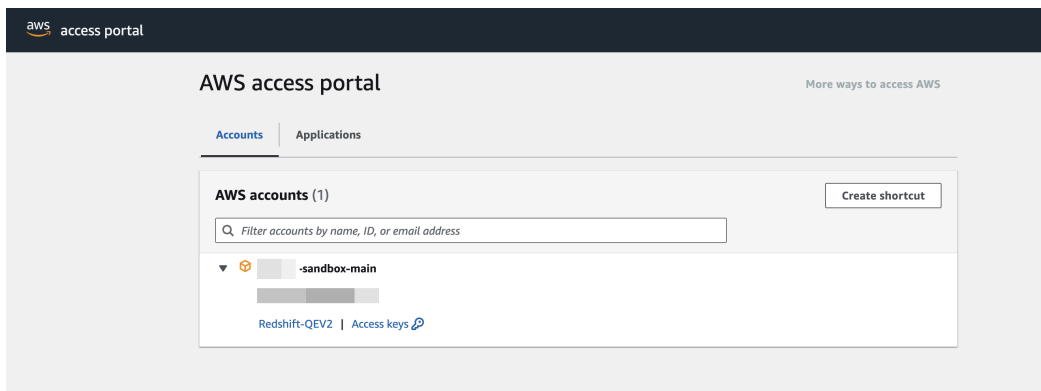
```

- f. Pilih Berikutnya dan kemudian berikan nama untuk nama kumpulan izin. Misalnya, **Redshift-Query-Editor-V2**.
- g. Di bawah Status Relay — opsional, atur status relai default ke URL Query Editor V2, menggunakan format: `https://your-region.console.aws.amazon.com/sqlworkbench/home`.
- h. Tinjau pengaturan dan pilih Buat.
- i. Arahkan ke Dasbor Pusat Identitas IAM dan salin URL portal AWS akses dari bagian Ringkasan Pengaturan.



- j. Buka Jendela Browser Penyamaran baru dan tempel URL.

Ini akan membawa Anda ke portal AWS akses Anda, memastikan Anda masuk dengan pengguna Pusat Identitas IAM.



Untuk informasi selengkapnya tentang kumpulan izin, lihat [Kelola Akun AWS dengan set izin](#).

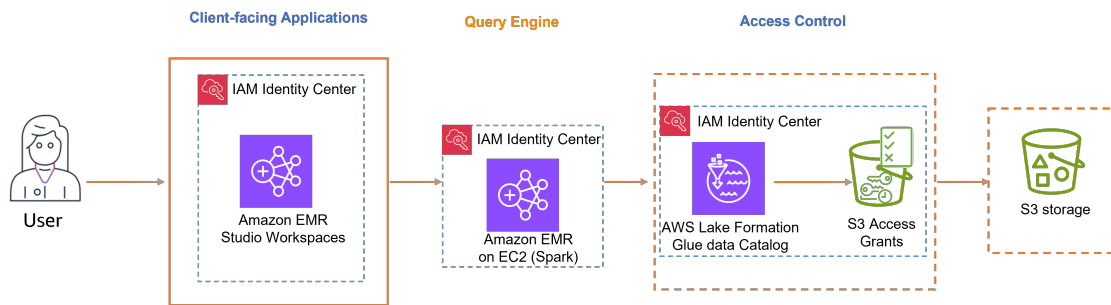
3. Aktifkan akses pengguna federasi ke Redshift Query Editor V2.
 - a. Di akun AWS Organizations manajemen, buka konsol Pusat Identitas IAM.
 - b. Di panel navigasi, di bawah Multi-account izin, pilih Akun AWS.
 - c. Pada Akun AWS halaman, pilih Akun AWS yang ingin Anda tetapkan akses.
 - d. Pilih Tetapkan pengguna atau grup.
 - e. Pada halaman Tetapkan pengguna dan grup, pilih pengguna dan/atau grup yang ingin Anda buat kumpulan izin. Lalu, pilih Selanjutnya.
 - f. Pada halaman Tetapkan kumpulan izin, pilih kumpulan izin yang Anda buat pada langkah sebelumnya. Lalu, pilih Selanjutnya.
 - g. Pada halaman Tinjau dan kirim tugas, tinjau pilihan Anda dan pilih Kirim.

Tugas yang dilakukan oleh administrator Amazon Redshift

Mengaktifkan propagasi identitas tepercaya ke Amazon Redshift memerlukan administrator cluster Amazon Redshift atau administrator Amazon Redshift Serverless untuk melakukan sejumlah tugas di konsol Amazon Redshift. Untuk informasi selengkapnya, lihat Meng [integrasikan Identity Provider \(IdP\) dengan Amazon Redshift Query Editor V2 dan SQL Client menggunakan IAM Identity Center untuk Single yang mulus Sign-On](#) di Blog AWS Big Data.

Propagasi identitas tepercaya dengan Amazon EMR

Diagram berikut menunjukkan konfigurasi propagasi identitas tepercaya untuk Amazon EMR Studio menggunakan Amazon EMR di Amazon EC2 dengan kontrol akses yang disediakan oleh AWS Lake Formation dan Amazon S3. Access Grants



Aplikasi yang menghadap klien yang didukung

- EMR Amazon Studio

Untuk mengaktifkan propagasi identitas terpercaya, ikuti langkah-langkah berikut:

- [Siapkan Amazon EMR Studio](#) sebagai aplikasi yang menghadap klien untuk cluster Amazon EMR.
- Siapkan [Amazon EMR Cluster di Amazon EC2 dengan. Apache Spark](#)
- Direkomendasikan: [AWS Lake Formation](#) dan [Amazon S3 Access Grants](#) untuk menyediakan kontrol akses yang halus ke AWS Glue Data Catalog dan lokasi data yang mendasarinya di S3.

Menyiapkan propagasi identitas terpercaya dengan Amazon EMR Studio

Prosedur berikut memandu Anda melalui pengaturan Amazon EMR Studio untuk propagasi identitas terpercaya dalam kueri terhadap grup kerja Amazon Athena atau cluster Amazon EMR yang sedang berjalan. Apache Spark

Prasyarat

Sebelum Anda dapat memulai dengan tutorial ini, Anda harus menyiapkan yang berikut:

1. [Aktifkan Pusat](#) Identitas IAM. [Instance organisasi](#) direkomendasikan. Untuk informasi selengkapnya, lihat [Prasyarat dan pertimbangan](#).
2. [Menyediakan pengguna dan grup dari sumber identitas Anda ke Pusat](#) Identitas IAM.

Untuk menyelesaikan penyiapan propagasi identitas terpercaya dari Amazon EMR Studio, administrator EMR Studio harus melakukan langkah-langkah berikut.

Langkah 1. Buat peran IAM yang diperlukan untuk EMR Studio

Pada langkah ini, Studio administrator Amazon EMR membuat peran layanan IAM dan peran pengguna IAM untuk EMR. Studio

1. [Buat peran layanan EMR Studio](#) - EMR Studio mengambil peran IAM ini untuk mengelola ruang kerja dan notebook dengan aman, terhubung ke cluster, dan menangani interaksi data.
 - a. Arahkan ke konsol IAM (<https://console.aws.amazon.com/iam/>) dan buat peran IAM.
 - b. Pilih Layanan AWS sebagai entitas tepercaya dan kemudian pilih Amazon EMR. Lampirkan kebijakan berikut untuk menentukan izin peran dan hubungan kepercayaan.

Untuk menggunakan kebijakan ini, ganti kebijakan *italicized placeholder text* dalam contoh dengan informasi Anda sendiri. Untuk petunjuk tambahan, lihat [Membuat kebijakan](#) atau [Mengedit kebijakan](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ObjectActions",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::Your-S3-Bucket-For-EMR-Studio/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "Your-AWS-Account-ID"
        }
      }
    },
    {
      "Sid": "BucketActions",
      "Effect": "Allow",

```

```

    "Action": [
      "s3:ListBucket",
      "s3:GetEncryptionConfiguration"
    ],
    "Resource": [
      "arn:aws:s3:::Your-S3-Bucket-For-EMR-Studio"
    ],
    "Condition": {
      "StringEquals": {
        "aws:ResourceAccount": "Your-AWS-Account-ID"
      }
    }
  }
]
}

```

Untuk referensi semua izin peran layanan, lihat izin [peran layanan](#) EMR Studio.

2. [Buat peran pengguna EMR Studio untuk otentikasi Pusat Identitas IAM](#) - EMR Studio mengambil peran ini ketika pengguna masuk melalui Pusat Identitas IAM untuk mengelola ruang kerja, cluster EMR, pekerjaan, repositori git. Peran ini digunakan untuk memulai alur kerja propagasi identitas tepercaya.

Note

Peran pengguna EMR Studio tidak perlu menyertakan izin untuk mengakses lokasi Amazon S3 tabel di AWS Glue Katalog. AWS Lake Formation izin dan lokasi danau terdaftar akan digunakan untuk menerima izin sementara.

Kebijakan contoh berikut dapat digunakan dalam peran yang memungkinkan pengguna EMR Studio menggunakan kelompok kerja Athena untuk menjalankan kueri.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowDefaultEC2SecurityGroupsCreationInVPCWithEMRTags",

```

```

        "Effect": "Allow",
        "Action": [
            "ec2:CreateSecurityGroup"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:vpc/*"
        ],
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/for-use-with-amazon-emr-managed-
policies": "true"
            }
        }
    },
    {
        "Sid": "AllowAddingEMRTagsDuringDefaultSecurityGroupCreation",
        "Effect": "Allow",
        "Action": [
            "ec2:CreateTags"
        ],
        "Resource": "arn:aws:ec2:*:*:security-group/*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/for-use-with-amazon-emr-managed-
policies": "true",
                "ec2:CreateAction": "CreateSecurityGroup"
            }
        }
    },
    {
        "Sid": "AllowSecretManagerListSecrets",
        "Action": [
            "secretsmanager:ListSecrets"
        ],
        "Resource": "*",
        "Effect": "Allow"
    },
    {
        "Sid": "AllowSecretCreationWithEMRTagsAndEMRStudioPrefix",
        "Effect": "Allow",
        "Action": "secretsmanager:CreateSecret",
        "Resource": "arn:aws:secretsmanager:*:*:secret:emr-studio-*",
        "Condition": {
            "StringEquals": {

```

```

        "aws:RequestTag/for-use-with-amazon-emr-managed-
policies": "true"
    }
},
{
    "Sid": "AllowAddingTagsOnSecretsWithEMRStudioPrefix",
    "Effect": "Allow",
    "Action": "secretsmanager:TagResource",
    "Resource": "arn:aws:secretsmanager:*:*:secret:emr-studio-*"
},
{
    "Sid": "AllowPassingServiceRoleForWorkspaceCreation",
    "Action": "iam:PassRole",
    "Resource": [
        "arn:aws:iam::111122223333:role/service-
role/AmazonEMRStudio_ServiceRole_Name"
    ],
    "Effect": "Allow"
},
{
    "Sid": "AllowS3ListAndLocationPermissions",
    "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws:s3:::*",
    "Effect": "Allow"
},
{
    "Sid": "AllowS3ReadOnlyAccessToLogs",
    "Action": [
        "s3:GetObject"
    ],
    "Resource": [
        "arn:aws:s3:::aws-logs-Your-AWS-Account-ID-Region/
elasticmapreduce/*"
    ],
    "Effect": "Allow"
},
{
    "Sid": "AllowAthenaQueryExecutions",
    "Effect": "Allow",

```

```

        "Action": [
            "athena:StartQueryExecution",
            "athena:GetQueryExecution",
            "athena:GetQueryResults",
            "athena:StopQueryExecution",
            "athena:ListQueryExecutions",
            "athena:GetQueryResultsStream",
            "athena:ListWorkGroups",
            "athena:GetWorkGroup",
            "athena:CreatePreparedStatement",
            "athena:GetPreparedStatement",
            "athena>DeletePreparedStatement"
        ],
        "Resource": "*"
    },
    {
        "Sid": "AllowGlueSchemaManipulations",
        "Effect": "Allow",
        "Action": [
            "glue:GetDatabase",
            "glue:GetDatabases",
            "glue:GetTable",
            "glue:GetTables",
            "glue:GetPartition",
            "glue:GetPartitions"
        ],
        "Resource": "*"
    },
    {
        "Sid": "AllowQueryEditorToAccessWorkGroup",
        "Effect": "Allow",
        "Action": "athena:GetWorkGroup",
        "Resource": "arn:aws:athena:*:111122223333:workgroup*"
    },
    {
        "Sid": "AllowConfigurationForWorkspaceCollaboration",
        "Action": [
            "elasticmapreduce:UpdateEditor",
            "elasticmapreduce:PutWorkspaceAccess",
            "elasticmapreduce>DeleteWorkspaceAccess",
            "elasticmapreduce:ListWorkspaceAccessIdentities"
        ],
        "Resource": "*",
        "Effect": "Allow",
    }

```

```

        "Condition": {
            "StringEquals": {
                "elasticmapreduce:ResourceTag/creatorUserId":
"${aws:userId}"
            }
        },
        {
            "Sid": "DescribeNetwork",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ListIAMRoles",
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AssumeRole",
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Resource": "*"
        }
    ]
}

```

Kebijakan kepercayaan berikut memungkinkan EMR Studio untuk mengambil peran:

Note

Izin tambahan diperlukan untuk memanfaatkan Ruang Kerja EMR Studio dan Notebook EMR. Lihat [Membuat kebijakan izin untuk pengguna EMR Studio](#) untuk informasi selengkapnya.

Anda dapat menemukan informasi lebih lanjut dengan tautan berikut:

- [Tentukan izin IAM khusus dengan kebijakan yang dikelola pelanggan](#)
- [Izin peran layanan EMR Studio](#)

Langkah 2. Buat dan konfigurasi EMR Studio Anda

Pada langkah ini, Anda akan membuat Amazon EMR Studio di konsol EMR Studio dan menggunakan peran IAM yang Anda buat. [Langkah 1. Buat peran IAM yang diperlukan untuk EMR Studio](#)

1. Arahkan ke konsol EMR Studio, pilih **Create Studio** dan opsi **Custom Setup**. Anda dapat membuat bucket S3 baru atau menggunakan bucket yang sudah ada. Anda dapat mencentang kotak untuk Enkripsi file ruang kerja dengan kunci KMS Anda sendiri. Untuk informasi selengkapnya, lihat [AWS Key Management Service](#).

The screenshot shows the 'Create a Studio' page in the Amazon EMR Studio console. The 'Setup options' section has three radio buttons: 'Interactive workloads', 'Batch jobs', and 'Custom' (which is selected). The 'Studio settings' section includes a text input for 'Studio name' containing 'Studio_1', a description field, and an 'S3 location for Workspace storage' section. In the S3 section, 'Create new bucket' is selected, and a note indicates that a new bucket will be created with a specific S3 location. There is also an option to 'Encrypt Workspace files with your own AWS KMS key'.

2. Di bawah **Peran layanan** untuk membiarkan Studio mengakses sumber daya Anda, pilih peran layanan yang dibuat [Langkah 1. Buat peran IAM yang diperlukan untuk EMR Studio](#) dari menu.

3. Pilih Pusat Identitas IAM di bawah Oten tifikasi. Pilih peran pengguna yang dibuat di [Langkah 1. Buat peran IAM yang diperlukan untuk EMR Studio.](#)

The screenshot shows the 'Create Studio' page in the AWS IAM Identity Center console. The top navigation bar includes the AWS logo, a search bar, and the text '[Option+S]'. The breadcrumb trail is 'Amazon EMR > EMR Studio: Studios > Create Studio'. The main content area is divided into several sections:

- Service role to let Studio access your AWS resources:** A dropdown menu shows 'AmazonEMRStudio' with a 'View permission details' link and a refresh icon.
- Authentication:** A section titled 'Choose an authentication method for your Studio.' with two options:
 - ☐ AWS Identity and Access Management (IAM): Authenticate with single sign-on using IAM identity federation or IAM credentials.
 - ☒ IAM Identity Center (AWS Single Sign-On): Authenticate with single sign-on using IAM Identity Center (recommended to centrally manage access permissions for multiple AWS accounts).
- User role:** A section titled 'Each Studio will have a default set of user roles. You can further refine user permissions once you have created a Studio. To create an additional set of permission use [AWS IAM](#).' A dropdown menu shows 'emrstudio-userrole-ids' with a refresh icon and a 'Create IAM role' button.
- Connect EMR Studio to IAM Identity Center:** A section titled 'Instance of IAM Identity Center' with the text 'Manage access to EMR Studio by assigning users and groups from your Identity Center directory.' and a dropdown menu showing 'arn:aws:sso::instance/ssoins-'.

4. Centang kotak Propagasi identitas tepercaya. Pilih Hanya pengguna dan grup yang ditugaskan di bawah bagian Akses aplikasi, yang akan memungkinkan Anda untuk hanya memberikan pengguna dan grup yang berwenang untuk mengakses studio ini.
5. (Opsional) - Anda dapat mengkonfigurasi VPC dan subnet jika Anda menggunakan Studio ini dengan cluster EMR.

The screenshot shows the 'Create Studio' page with the 'Trusted identity propagation' and 'Application access' sections expanded. The top navigation bar and breadcrumb trail are the same as in the previous screenshot.

- Trusted identity propagation:** A section titled 'Control and log the access that a user has across connected applications.' with a checkbox 'Enable trusted identity propagation' that is checked. Below the checkbox is a note: 'When users make requests to applications that are connected through Identity Center, share their user identity information from EMR Studio. This setting applies for the lifetime of the Studio. You can't turn it off later.' A blue box contains a note: 'The following features aren't supported from a Studio with trusted identity propagation: creating EMR on EC2 clusters without a template, using EMR Serverless applications, launching EMR on EKS clusters, using a runtime role, and enabling SQL Explorer or Workspace collaboration.'
- Application access:** A section titled 'Choose who can access your application' with a dropdown menu showing 'Only assigned users and groups'. Below the dropdown is a note: 'Only the users and groups that you specify from your Identity Center directory can access this application.' There is also an option for 'All users and groups' with a note: 'Any user or group from your IAM Identity Center directory can access this application.'
- Networking and security - optional:** A section with two sub-sections:
 - VPC:** A section titled 'Select a VPC for your Studio to use when it communicates with EMR clusters. To use condition keys like those in the example [service role policies for Amazon EMR](#), you must tag the VPC with the `for-use-with-amazon-emr-managed-policies` key and value `true`. To manage tags, use [VPC Dashboard](#).' A dropdown menu shows 'Select a VPC' with a refresh icon.
 - Subnets:** A section titled 'Select the subnets that your Studio can use when it communicates with EMR clusters. To use condition keys like those in the example [service role policies for Amazon EMR](#), you must tag each subnet with the `for-use-with-amazon-emr-managed-policies` key and value `true`. To manage tags, use [VPC Dashboard](#).'

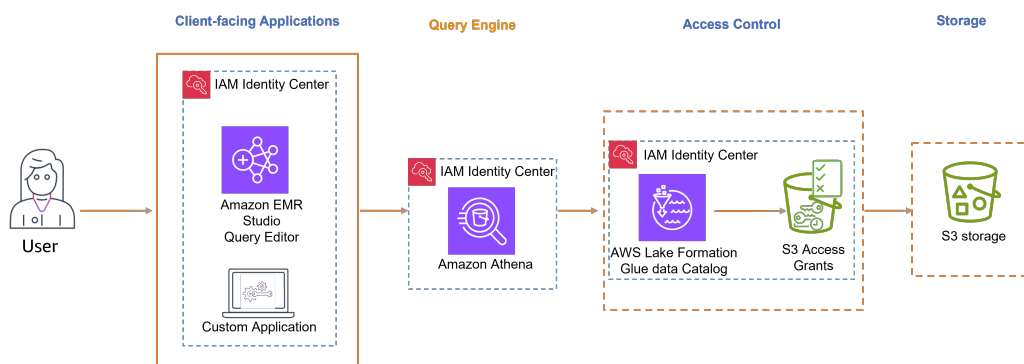
6. Tinjau semua detail dan pilih Buat Studio.
7. Setelah mengonfigurasi cluster Athena WorkGroup atau EMR, masuk ke URL Studio untuk:
 - a. Jalankan query Athena dengan Query Editor.
 - b. Jalankan pekerjaan Spark di ruang kerja menggunakan Jupyter notebook.

Propagasi identitas terpercaya dengan Amazon Athena

Langkah-langkah untuk mengaktifkan propagasi identitas terpercaya bergantung pada apakah pengguna berinteraksi dengan aplikasi ter AWS kelola atau aplikasi yang dikelola pelanggan. Diagram berikut menunjukkan konfigurasi propagasi identitas terpercaya untuk aplikasi yang menghadap klien - baik AWS dikelola atau eksternal AWS - yang menggunakan Amazon Athena untuk menanyakan data Amazon S3 dengan kontrol akses yang disediakan oleh AWS Lake Formation dan Amazon S3. Access Grants

Note

- Penyebaran identitas terpercaya dengan Amazon Athena memerlukan penggunaan Trino.
- Klien Apache Spark dan SQL yang terhubung ke Amazon Athena melalui driver ODBC dan JDBC tidak didukung.



AWS aplikasi yang dikelola

Aplikasi terkel AWS ola yang menghadap klien berikut ini mendukung propagasi identitas terpercaya dengan Athena:

- EMR Amazon Studio

Untuk mengaktifkan propagasi identitas terpercaya, ikuti langkah-langkah berikut:

- [Siapkan Amazon EMR Studio](#) sebagai aplikasi yang menghadap klien untuk Athena. Editor Kueri di EMR Studio diperlukan untuk menjalankan Athena Queries saat propagasi identitas terpercaya diaktifkan.
- [Siapkan Athena Work](#) group.

- [Siapkan AWS Lake Formation](#) untuk mengaktifkan kontrol akses halus untuk AWS Glue tabel berdasarkan pengguna atau grup di Pusat Identitas IAM.
- [Siapkan Amazon S3 Access Grants](#) untuk mengaktifkan akses sementara ke lokasi data yang mendasarinya di S3.

 Note

Baik Lake Formation maupun Amazon S3 Access Grants diperlukan untuk kontrol akses ke AWS Glue Data Catalog dan untuk hasil kueri Athena di Amazon S3.

Aplikasi yang dikelola pelanggan

Untuk mengaktifkan propagasi identitas tepercaya bagi pengguna aplikasi yang dikembangkan khusus, lihat [Akses secara ter Layanan AWS program menggunakan propagasi identitas tepercaya](#) di Blog Keamanan. AWS

Menyiapkan propagasi identitas tepercaya dengan kelompok kerja Amazon Athena

Prosedur berikut memandu Anda menyiapkan grup kerja Amazon Athena untuk propagasi identitas tepercaya.

Prasyarat

Sebelum Anda dapat memulai dengan tutorial ini, Anda harus menyiapkan yang berikut:

1. [Aktifkan Pusat](#) Identitas IAM. [Instance organisasi](#) direkomendasikan. Untuk informasi selengkapnya, lihat [Prasyarat dan pertimbangan](#).
2. [Menyediakan pengguna dan grup dari sumber identitas Anda ke Pusat](#) Identitas IAM.
3. Konfigurasi ini memerlukan [Amazon EMR Studio](#), [AWS Lake Formation](#), dan [Amazon S3 Access Grants](#).

Menyiapkan propagasi identitas tepercaya dengan Athena

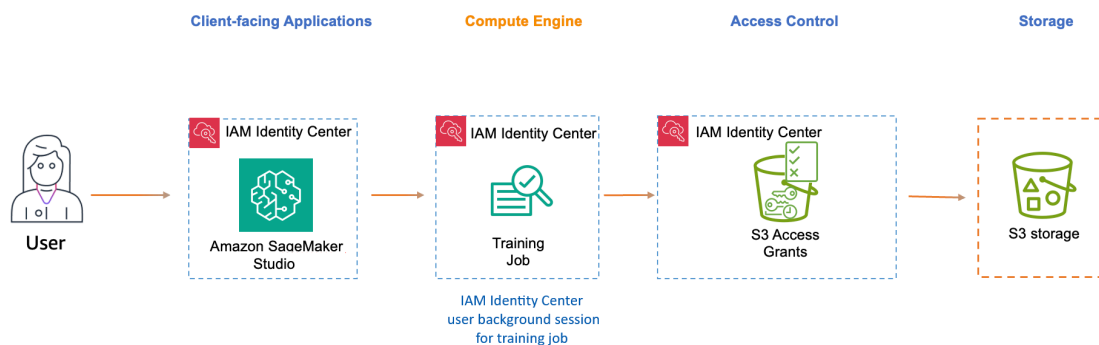
Untuk mengatur propagasi identitas tepercaya dengan Athena, administrator Athena harus:

1. Tinjau [Pertimbangan dan batasan dalam menggunakan kelompok kerja Athena yang diaktifkan IAM Identity Center](#).
2. [Buat grup kerja Athena yang diaktifkan Pusat Identitas IAM](#).

Propagasi identitas tepercaya dengan Amazon SageMaker Studio

[Amazon SageMaker Studio](#) terintegrasi dengan Pusat Identitas IAM, dan mendukung sesi latar belakang [pengguna](#) dan propagasi identitas tepercaya. Sesi latar belakang pengguna memungkinkan pengguna untuk memulai pekerjaan yang berjalan lama di SageMaker Studio, tanpa pengguna tersebut harus tetap masuk saat pekerjaan berjalan. Pekerjaan berjalan segera dan di latar belakang, menggunakan izin pengguna yang memulai pekerjaan. Pekerjaan dapat terus berjalan meskipun pengguna mematikan komputer mereka, sesi masuk Pusat Identitas IAM berakhir, atau pengguna keluar dari portal AWS akses. Durasi sesi default untuk sesi latar belakang pengguna adalah 7 hari, tetapi Anda dapat menentukan durasi maksimum 90 hari. Propagasi identitas tepercaya memungkinkan akses halus disediakan ke AWS sumber daya seperti bucket Amazon S3 berdasarkan identitas pengguna atau keanggotaan grup.

Diagram berikut menunjukkan konfigurasi propagasi identitas tepercaya untuk SageMaker Studio, dengan akses ke data yang disimpan dalam bucket Amazon S3. Sesi latar belakang pengguna diaktifkan untuk Pusat Identitas IAM, yang memungkinkan pekerjaan pelatihan SageMaker Studio berjalan di latar belakang. Kontrol akses untuk data pelatihan disediakan oleh Amazon S3Access Grants.



AWS aplikasi yang dikelola

Aplikasi terkel AWS ola yang menghadap klien berikut ini mendukung propagasi identitas tepercaya:

- [SageMaker Studio Amazon](#)

Untuk mengaktifkan propagasi identitas tepercaya dan sesi latar belakang pengguna, ikuti langkah-langkah berikut:

- [Siapkan SageMaker Studio sebagai aplikasi yang menghadap ke klien.](#)

- [Siapkan Amazon S3 Access Grants](#) untuk mengaktifkan akses sementara ke lokasi data yang mendasarinya di Amazon S3.

Menyiapkan propagasi identitas tepercaya dengan SageMaker Studio

Prosedur berikut memandu Anda melalui pengaturan SageMaker Studio untuk propagasi identitas tepercaya dan sesi latar belakang pengguna.

Prasyarat

Sebelum Anda dapat memulai dengan tutorial ini, Anda harus menyelesaikan tugas-tugas berikut:

1. [Aktifkan Pusat](#) Identitas IAM. Instance organisasi diperlukan. Untuk informasi selengkapnya, lihat [Prasyarat dan pertimbangan](#).
2. [Menyediakan pengguna dan grup dari sumber identitas Anda ke Pusat](#) Identitas IAM.
3. [Konfirmasikan bahwa sesi latar belakang pengguna diaktifkan](#) di konsol Pusat Identitas IAM. Secara default, sesi latar belakang pengguna diaktifkan dan durasi sesi diatur ke 7 hari. Anda dapat mengubah durasi ini.

Untuk mengatur propagasi identitas tepercaya dari SageMaker SageMaker Studio, administrator Studio harus melakukan langkah-langkah berikut.

Langkah 1: Aktifkan propagasi identitas tepercaya di domain SageMaker Studio baru atau yang sudah ada

SageMaker Studio menggunakan domain untuk mengatur profil pengguna, aplikasi, dan sumber daya terkaitnya. Untuk mengaktifkan propagasi identitas tepercaya, Anda harus membuat domain SageMaker Studio atau memodifikasi domain yang ada seperti yang dijelaskan dalam prosedur berikut.

1. Buka konsol SageMaker AI, navigasikan ke Domain, dan lakukan salah satu dari hal berikut.
 - Buat domain SageMaker Studio baru dengan menggunakan [Setup untuk organisasi](#).

Pilih [Siapkan untuk organisasi](#), lalu lakukan hal berikut:

- Pilih Pusat AWS Identitas sebagai metode otentikasi.
- Pilih kotak centang Aktifkan propagasi identitas tepercaya untuk semua pengguna di domain ini.

- Ubah domain SageMaker Studio yang ada.
- Pilih domain yang ada yang menggunakan Pusat Identitas IAM untuk otentikasi.

 Important

Propagasi identitas tepercaya hanya didukung di domain SageMaker Studio yang menggunakan Pusat Identitas IAM untuk otentikasi. Jika domain menggunakan IAM untuk otentikasi, Anda tidak dapat mengubah metode otentikasi, dan karenanya Anda tidak dapat mengaktifkan propagasi identitas tepercaya.

- [Edit pengaturan domain](#). Edit pengaturan Otentikasi dan izin untuk mengaktifkan propagasi identitas tepercaya.
2. Lanjutkan ke [Langkah 2: Konfigurasi peran eksekusi domain default](#). Peran ini diperlukan bagi pengguna domain SageMaker Studio untuk mengakses AWS layanan lain seperti Amazon S3.

Langkah 2: Konfigurasi peran eksekusi domain default dan kebijakan kepercayaan peran

Peran eksekusi domain adalah peran [IAM](#) yang diasumsikan oleh domain SageMaker Studio atas nama semua pengguna di domain. Izin yang Anda tetapkan untuk peran ini menentukan tindakan apa yang dapat dilakukan SageMaker Studio.

1. Untuk membuat atau memilih peran eksekusi domain, lakukan salah satu dari hal berikut:
 - Buat atau pilih peran dengan menggunakan [Setup untuk organisasi](#).
 - Buka konsol SageMaker AI dan ikuti panduan konsol di [Langkah 2: Konfigurasi peran dan aktivitas ML](#) untuk membuat peran eksekusi domain baru atau pilih peran yang ada.
 - Selesaikan langkah-langkah penyiapan lainnya untuk membuat domain SageMaker Studio Anda.
 - Buat peran eksekusi secara manual.
 - Buka konsol IAM dan [buat peran eksekusi sendiri](#).
2. [Perbarui kebijakan kepercayaan](#) yang dilampirkan ke peran eksekusi domain sehingga mencakup dua tindakan berikut: [sts:AssumeRole](#) dan [sts:SetContext](#). Untuk informasi tentang cara menemukan peran eksekusi untuk domain SageMaker Studio Anda, lihat [Mendapatkan peran eksekusi domain](#).

Kebijakan kepercayaan menentukan identitas yang dapat mengambil peran. Kebijakan ini diperlukan untuk mengizinkan layanan SageMaker Studio mengambil peran eksekusi domain. Tambahkan kedua tindakan ini sehingga muncul sebagai berikut dalam kebijakan Anda.

```
{  
  
  "Version": "2012-10-17",  
  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "Service": [  
          "sagemaker.amazonaws.com"  
        ]  
      },  
      "Action": [  
        "sts:AssumeRole",  
        "sts:SetContext"  
      ]  
    }  
  ]  
}
```

Langkah 3: Verifikasi izin Amazon S3 Access Grant yang diperlukan untuk peran eksekusi domain

Untuk menggunakan Amazon S3 Access Grants, Anda harus memiliki kebijakan izin yang dilampirkan (baik sebagai kebijakan sebaris atau kebijakan yang dikelola pelanggan) ke peran eksekusi domain SageMaker Studio yang berisi izin berikut.

```
{  
  
  "Version": "2012-10-17",  
  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "s3:GetDataAccess",  
        "s3:GetAccessGrantsInstanceForPrefix"  
      ]  
    }  
  ]  
}
```



```

    ],
    "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
  }
]
}

```

Jika Anda tidak memiliki kebijakan yang berisi izin ini, ikuti petunjuk di Men [tambahkan dan menghapus izin identitas IAM](#) di Panduan AWS Identity and Access Management Pengguna.

Langkah 4: Tetapkan grup dan pengguna ke domain

Tetapkan grup dan pengguna ke domain SageMaker Studio dengan mengikuti langkah-langkah di [Tambahkan grup dan pengguna](#).

Langkah 5: Siapkan Amazon S3 Access Grants

Untuk mengatur Amazon S3 Access Grants, ikuti langkah-langkah di Mengon [figurasi Amazon S3 Access Grants untuk propagasi identitas tepercaya melalui Pusat](#) Identitas IAM. Gunakan petunjuk langkah demi langkah untuk menyelesaikan tugas-tugas berikut:

1. Buat instance Amazon S3 Access Grants.
2. Daftarkan lokasi dalam contoh itu.
3. Buat hibah untuk mengizinkan pengguna atau grup Pusat Identitas IAM tertentu mengakses lokasi atau subset Amazon S3 yang ditunjuk (misalnya, awalan tertentu) di dalam lokasi tersebut.

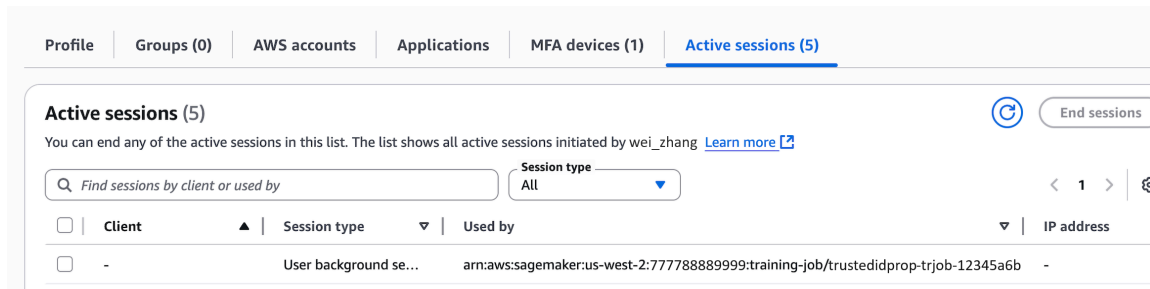
Langkah 6: Kirim pekerjaan SageMaker pelatihan dan lihat detail sesi latar belakang pengguna

Di SageMaker Studio, luncurkan notebook Jupyter baru dan kirimkan pekerjaan pelatihan. Saat pekerjaan sedang berjalan, selesaikan langkah-langkah berikut untuk melihat informasi sesi dan untuk memverifikasi bahwa konteks sesi latar belakang pengguna aktif.

1. Buka konsol Pusat Identitas IAM.
2. Pilih Pengguna.
3. Pada halaman Pengguna, pilih nama 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 untuk pengguna ini.

- Untuk mencari sesi berdasarkan Nama Sumber Daya Amazon (ARN) dari pekerjaan yang menggunakan sesi, dalam daftar Jenis sesi, pilih Sesi latar belakang pengguna, lalu masukkan ARN pekerjaan di kotak pencarian.

Berikut ini adalah contoh bagaimana pekerjaan pelatihan yang menggunakan sesi latar belakang pengguna muncul di tab Sesi aktif untuk pengguna.



Langkah 7: Lihat CloudTrail log untuk memverifikasi propagasi identitas tepercaya di CloudTrail

Ketika propagasi identitas tepercaya diaktifkan, tindakan muncul di log CloudTrail peristiwa di bawah `onBehalfOf` elemen. Ini `userId` mencerminkan ID pengguna Pusat Identitas IAM yang memulai pekerjaan pelatihan. A CloudTrail cara berikut menangkap proses propagasi identitas tepercaya.

```

      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AR0A123456789EXAMPLE:SageMaker",
        "arn": "arn:aws:sts::111122223333:assumed-role/SageMaker-
ExecutionRole-20250728T125817/SageMaker",
        "accountId": "111122223333",
        "accessKeyId": "ASIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AR0A123456789EXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/service-role/SageMaker-
ExecutionRole-20250728T125817",
            "accountId": "111122223333",
            "userName": "SageMaker-ExecutionRole-20250728T125817"
          },
          "attributes": {
            "creationDate": "2025-07-29T17:17:10Z",
            "mfaAuthenticated": "false"
          }
        }
      }

```

```
    },  
    "onBehalfOf": {  
        "userId": "2801d3e0-f0e1-707f-54e8-f558b19f0a10",  
        "identityStoreArn": "arn:aws:identitystore::777788889999:identitystore/  
d-1234567890"  
    }  
},
```

Pertimbangan runtime

Jika administrator menetapkan tugas pelatihan atau pemrosesan yang berjalan `MaxRuntimeInSeconds` lama yang lebih rendah dari durasi sesi latar belakang pengguna, SageMaker Studio menjalankan tugas untuk durasi sesi latar belakang pengguna minimum `MaxRuntimeInSeconds` atau durasi sesi latar belakang pengguna.

Untuk informasi selengkap `MaxRuntimeInSeconds` nya, lihat panduan untuk `CreateTrainingJob` [StoppingCondition](#) parameter di Referensi SageMaker API Amazon.

Layanan otorisasi

Dalam semua kasus penggunaan [analitik dan data lakehouse](#), Anda dapat mencapai kontrol akses yang halus menggunakan:

- AWS Lake Formation - untuk bimbingan, lihat [Penyiapan AWS Lake Formation dengan Pusat Identitas IAM](#).
- Amazon S3 Access Grants - untuk panduan, lihat [Menyiapkan Hibah Akses Amazon S3 dengan Pusat Identitas IAM](#).

Penyiapan AWS Lake Formation dengan Pusat Identitas IAM

[AWS Lake Formation](#) adalah layanan terkelola yang menyederhanakan pembuatan dan pengelolaan danau data pada AWS. Ini mengotomatiskan pengumpulan data, katalog, dan keamanan, menyediakan repositori terpusat untuk menyimpan dan menganalisis beragam jenis data. Lake Formation menawarkan kontrol akses yang halus dan terintegrasi dengan berbagai layanan AWS analitik, memungkinkan organisasi untuk secara efisien mengatur, mengamankan, dan memperoleh wawasan dari danau data mereka.

Ikuti langkah-langkah berikut untuk mengaktifkan Lake Formation untuk memberikan izin data berdasarkan identitas pengguna menggunakan Pusat Identitas IAM dan propagasi identitas tepercaya.

Prasyarat

Sebelum Anda dapat memulai dengan tutorial ini, Anda harus menyiapkan yang berikut:

- [Aktifkan Pusat](#) Identitas IAM. [Instance organisasi](#) direkomendasikan. Untuk informasi selengkapnya, lihat [Prasyarat dan pertimbangan](#).

Langkah-langkah untuk mengatur propagasi identitas tepercaya

1. Integrasikan Pusat Identitas IAM dengan AWS Lake Formation mengikuti panduan dalam Menghubungkan For [masi Danau dengan Pusat Identitas IAM](#).

Important

Jika Anda tidak memiliki AWS Glue Data Catalog tabel, Anda harus membuatnya agar dapat digunakan untuk memberikan akses AWS Lake Formation ke pengguna dan grup Pusat Identitas IAM. Lihat [Membuat objek di AWS Glue Data Catalog](#) untuk informasi selengkapnya.

2. Daftarkan lokasi danau data.

[Daftarkan lokasi S3](#) tempat data tabel Glue disimpan. Dengan melakukan ini, Lake Formation akan menyediakan akses sementara ke lokasi S3 yang diperlukan saat tabel ditanyakan, menghilangkan kebutuhan untuk menyertakan izin S3 dalam peran layanan (misalnya peran layanan Athena yang dikonfigurasi pada). WorkGroup

- a. Arahkan ke lokasi danau data di bawah bagian Administrasi di panel navigasi di AWS Lake Formation konsol. Pilih Daftar lokasi.

Ini akan memungkinkan Lake Formation menyediakan kredensial IAM sementara dengan izin yang diperlukan untuk mengakses lokasi data S3.

- b. Masukkan jalur S3 dari lokasi data AWS Glue tabel di bidang jalur Amazon S3.
- c. Di bagian peran IAM, jangan pilih peran terkait layanan jika Anda ingin menggunakannya dengan propagasi identitas tepercaya. Buat peran terpisah dengan izin berikut.

Untuk menggunakan kebijakan ini, ganti kebijakan *italicized placeholder text* dalam contoh dengan informasi Anda sendiri. Untuk petunjuk tambahan, lihat [Membuat kebijakan](#) atau [Mengedit kebijakan](#). Kebijakan izin harus memberikan akses ke lokasi S3 yang ditentukan di jalur:

- i. Kebijakan izin:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LakeFormationDataAccessPermissionsForS3",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::Your-S3-Bucket/*"
      ]
    }
  ]
}
```

```

        "Sid":
        "LakeFormationDataAccessPermissionsForS3ListBucket",
        "Effect": "Allow",
        "Action": [
            "s3:ListBucket"
        ],
        "Resource": [
            "arn:aws:s3:::Your-S3-Bucket"
        ]
    },
    {
        "Sid": "LakeFormationDataAccessServiceRolePolicy",
        "Effect": "Allow",
        "Action": [
            "s3:ListAllMyBuckets"
        ],
        "Resource": [
            "arn:aws:s3:::*"
        ]
    }
]
}

```

- ii. Hubungan kepercayaan: Ini harus mencakup `sts:SectContext`, yang diperlukan untuk propagasi identitas tepercaya.

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "Service": "lakeformation.amazonaws.com"
            },
            "Action": [
                "sts:AssumeRole",
                "sts:SetContext"
            ]
        }
    ]
}

```

```
}
```

Note

Peran IAM yang dibuat oleh wizard adalah peran terkait layanan dan tidak termasuk `sts:SetContext`

- d. Setelah membuat peran IAM, pilih Daftar lokasi.

Propagasi identitas tepercaya dengan Lake Formation di seberang Akun AWS

AWS Lake Formation mendukung penggunaan [AWS Resource Access Manager \(RAM\)](#) untuk berbagi tabel Akun AWS dan bekerja dengan propagasi identitas tepercaya ketika akun pemberi dan akun penerima hibah berada di tempat yang sama, di yang sama Wilayah AWS AWS Organizations, dan berbagi instance organisasi yang sama dari Pusat Identitas IAM. Lihat berbagi [Cross-account data di Formasi Danau](#) untuk informasi lebih lanjut.

Menyiapkan Hibah Akses Amazon S3 dengan Pusat Identitas IAM

[Amazon S3 Access Grants](#) memberikan fleksibilitas untuk memberikan kontrol akses halus berbasis identitas ke lokasi S3. Anda dapat menggunakan Amazon S3 Access Grants untuk memberikan akses bucket Amazon S3 langsung ke pengguna dan grup perusahaan Anda. Ikuti langkah-langkah berikut untuk mengaktifkan S3 Access Grants dengan IAM Identity Center dan mencapai propagasi identitas tepercaya.

Prasyarat

Sebelum Anda dapat memulai dengan tutorial ini, Anda harus menyiapkan yang berikut:

- [Aktifkan Pusat](#) Identitas IAM. [Instance organisasi](#) direkomendasikan. Untuk informasi selengkapnya, lihat [Prasyarat dan pertimbangan](#).

Mengkonfigurasi S3 Access Grants untuk propagasi identitas tepercaya melalui Pusat Identitas IAM

Jika Anda sudah memiliki Amazon S3 Hibah Akses contoh dengan lokasi terdaftar, ikuti langkah-langkah ini:

1. [Kaitkan instance](#) Pusat Identitas IAM Anda.

2. [Buat hibah.](#)

Jika Anda belum membuat Amazon S3 Hibah Akses Namun, ikuti langkah-langkah ini:

1. [Buat Access Grants instance S3](#) - Anda dapat membuat satu Access Grants instance S3 per Wilayah AWS. Saat Anda membuat Access Grants instance S3, pastikan untuk mencentang kotak ☐ Add IAM Identity Center instance dan berikan ARN instance Pusat Identitas IAM Anda. Pilih Selanjutnya.

Gambar berikut menunjukkan halaman Buat Access Grants instance S3 di Access Grants konsol Amazon S3:

2. Daftarkan lokasi - Setelah Anda [membuat Access Grants instance Amazon S3](#) Wilayah AWS di akun Anda, Anda men [daftarkan lokasi S3](#) di instance tersebut. Access Grants Lokasi S3 memetakan wilayah S3 default (S3://), bucket, atau awalan ke peran IAM. S3 Access Grants mengasumsikan peran Amazon S3 ini untuk menjual kredensial sementara kepada penerima hibah yang mengakses lokasi tertentu. Anda harus terlebih dahulu mendaftarkan setidaknya satu lokasi di Access Grants instans S3 Anda sebelum Anda dapat membuat hibah akses.

Untuk cakupan Lokasi, tentukan s3://, yang mencakup semua bucket Anda di Wilayah tersebut. Ini adalah ruang lingkup lokasi yang disarankan untuk sebagian besar kasus penggunaan. Jika Anda memiliki kasus penggunaan manajemen akses lanjutan, Anda dapat mengatur ruang lingkup lokasi ke bucket s3://*bucket* atau awalan tertentu di dalam buckets3://*bucket/prefix-with-path*. Untuk informasi selengkapnya, lihat [Mendaftarkan lokasi](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

 Note

Pastikan lokasi S3 dari AWS Glue tabel yang ingin Anda berikan akses disertakan dalam jalur ini.

Prosedur ini mengharuskan Anda untuk mengkonfigurasi peran IAM untuk lokasi. Peran ini harus mencakup izin untuk mengakses ruang lingkup lokasi. Anda dapat menggunakan wizard konsol S3 untuk membuat peran. Anda harus menentukan ARN Access Grants instans S3 Anda dalam kebijakan untuk peran IAM ini. Nilai default ARN Access Grants instance S3 Anda adalah `arn:aws:s3:Your-Region:Your-AWS-Account-ID:access-grants/default`.

Contoh kebijakan izin berikut memberikan izin Amazon S3 ke peran IAM yang Anda buat. Dan contoh kebijakan kepercayaan yang mengikutinya memungkinkan prinsi Access Grants pal layanan S3 untuk mengambil peran IAM.

a. Kebijakan izin

Untuk menggunakan kebijakan ini, ganti kebijakan *italicized placeholder text* dalam contoh dengan informasi Anda sendiri. Untuk petunjuk tambahan, lihat [Membuat kebijakan](#) atau [Mengedit kebijakan](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ObjectLevelReadPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectVersionAcl",
        "s3:ListMultipartUploadParts"
      ],
      "Resource": [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

```

    ],
    "Condition": {
      "StringEquals": {
        "aws:ResourceAccount": "111122223333"
      },
      "ArnEquals": {
        "s3:AccessGrantsInstanceArn": [
          "arn:aws:s3:::access-grants/instance-id"
        ]
      }
    }
  },
  {
    "Sid": "ObjectLevelWritePermissions",
    "Effect": "Allow",
    "Action": [
      "s3:PutObject",
      "s3:PutObjectAcl",
      "s3:PutObjectVersionAcl",
      "s3:DeleteObject",
      "s3:DeleteObjectVersion",
      "s3:AbortMultipartUpload"
    ],
    "Resource": [
      "arn:aws:s3:::*"
    ],
    "Condition": {
      "StringEquals": {
        "aws:ResourceAccount": "111122223333"
      },
      "ArnEquals": {
        "s3:AccessGrantsInstanceArn": [
          "arn:aws:s3:::access-grants/instance-id"
        ]
      }
    }
  },
  {
    "Sid": "BucketLevelReadPermissions",
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket"
    ],
    "Resource": [

```

```

        "arn:aws:s3:::*"
    ],
    "Condition": {
        "StringEquals": {
            "aws:ResourceAccount": "111122223333"
        },
        "ArnEquals": {
            "s3:AccessGrantsInstanceArn": [
                "arn:aws:s3:::access-grants/instance-id"
            ]
        }
    }
},
{
    "Sid": "OptionalKMSPermissionsForSSEEncryption",
    "Effect": "Allow",
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": [
        "*"
    ]
}
]
}

```

b. Kebijakan kepercayaan

Dalam kebijakan kepercayaan peran IAM, berikan akses utama layanan S3 Access Grants (`access-grants.s3.amazonaws.com`) ke peran IAM yang Anda buat. Untuk melakukannya, Anda dapat membuat file JSON yang berisi pernyataan berikut ini. Untuk menambahkan kebijakan kepercayaan ke akun Anda, lihat [Membuat peran menggunakan kebijakan kepercayaan khusus](#).

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1234567891011",

```

```

        "Effect": "Allow",
        "Action": [
            "sts:AssumeRole",
            "sts:SetSourceIdentity"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "111122223333",
                "aws:SourceArn": "Your-Custom-Access-Grants-Location-
ARN"
            }
        },
        {
            "Sid": "Stmt1234567891012",
            "Effect": "Allow",
            "Action": "sts:SetContext",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333",
                    "aws:SourceArn": "Your-Custom-Access-Grants-Location-
ARN"
                },
                "ForAllValues:ArnEquals": {
                    "sts:RequestContextProviders":
                        "arn:aws:iam::aws:contextProvider/IdentityCenter"
                }
            }
        }
    ]
}

```

Buat Hibah Akses Amazon S3

Jika Anda memiliki Access Grants instans Amazon S3 dengan lokasi terdaftar dan Anda telah mengaitkan instance Pusat Identitas IAM dengan itu, Anda dapat [membuat hibah](#). Di halaman Create Grant console S3, lengkapi yang berikut ini:

Buat hibah

1. Pilih lokasi yang dibuat pada langkah sebelumnya. Anda dapat mengurangi ruang lingkup hibah dengan menambahkan sub-awalan. Sub-awalan dapat berupa bucket/prefix, atau objek dalam bucket. Untuk informasi selengkapnya, lihat [Subprefix](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.
2. Di bawah Izin dan akses, pilih Baca dan atau Tulis tergantung kebutuhan Anda.
3. Di tipe Granter, pilih Identitas Direktori dari Pusat Identitas IAM.
4. Berikan ID Pengguna atau Grup Pusat Identitas IAM. Anda dapat menemukan ID pengguna dan grup di konsol Pusat Identitas IAM di bawah bagian [Pengguna](#) dan Grup. Pilih Selanjutnya.
5. Pada halaman Tinjau dan Selesai, tinjau pengaturan untuk S3 Access Grant lalu pilih Buat Hibah.

Gambar berikut menunjukkan halaman Buat Hibah di Access Grants konsol Amazon S3:

The screenshot shows the 'Create Grant' page in the AWS S3 Access Grants console. The page is divided into several sections:

- Grant scope:** This section allows you to define the scope of the grant. It includes fields for 'Location' (set to 's3://') and 'Subprefix - optional' (set to 'bucket-name/prefix/'). There are buttons for 'Browse locations' and 'Register location'. A note states: 'The grant scope is a combination of the location and the subprefix. Choose a registered location or register a new location. To narrow the scope, specify a subprefix. If you use the default "s3://" location, you must specify a subprefix.'
- Permissions and access:** This section allows you to define the permissions for the grant. It includes a checkbox for 'The grant scope is an object' and a section for 'Permissions' with checkboxes for 'Read' and 'Write'.
- Grantee type:** This section allows you to select the type of grantee. It includes radio buttons for 'Directory identity from IAM Identity Center' (selected), 'IAM principal', and 'User'.
- Directory identity type:** This section allows you to select the type of directory identity. It includes radio buttons for 'User' and 'Group' (selected).
- IAM Identity Center group ID:** This section allows you to enter the group ID. It includes a text input field and a link to 'IAM Identity Center console'.

Menyiapkan aplikasi OAuth 2.0 Anda sendiri

Penyebaran 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 pengguna 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 tersebut dapat meneruskan identitas pengguna dalam permintaan untuk mengakses data masuk Layanan AWS.

 Important

Untuk mengakses aplikasi yang Layanan AWS 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 Layanan AWS (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](#)
- [Tentukan aplikasi tepercaya](#)
- [Menggunakan aplikasi dengan penerbit token tepercaya](#)

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 Pusat Identitas IAM. Gunakan prosedur berikut untuk menambahkan aplikasi Anda ke Pusat Identitas IAM.

Topik

- [Langkah 1: Pilih jenis aplikasi](#)
- [Langkah 2: Tentukan detail aplikasi](#)
- [Langkah 3: Tentukan pengaturan otentikasi](#)
- [Langkah 4: Tentukan kredensial aplikasi](#)
- [Langkah 5: Tinjau dan konfigurasi](#)

Langkah 1: Pilih jenis aplikasi

1. Buka konsol [Pusat Identi](#) tas IAM.
2. Pilih Aplikasi.
3. Pilih tab Customer managed.
4. Pilih Tambah aplikasi.
5. Pada halaman Pilih jenis aplikasi, di bawah preferensi Setup, 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 penugasan pengguna dan grup, pilih salah satu opsi berikut:
 - Memerlukan penugasan — 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 disetel ke Terlihat.
 - Tidak memerlukan penugasan — Izinkan semua pengguna dan grup IAM Identity Center resmi 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 disetel ke Tidak terlihat.
3. Di bawah portal AWS akses, masukkan URL tempat pengguna dapat mengakses aplikasi dan tentukan apakah ubin aplikasi akan terlihat atau tidak terlihat di portal AWS akses. Jika Anda memilih Tidak terlihat, bahkan pengguna yang ditugaskan 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 [Sumber daya penandaan 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 yang dikelola pelanggan yang mendukung OAuth 2.0 ke Pusat Identitas IAM, Anda harus menentukan penerbit token terpercaya. Penerbit token terpercaya 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 terpercaya, lakukan salah satu dari hal berikut:

- Untuk menggunakan penerbit token terpercaya yang ada:

Pilih kotak centang di samping nama penerbit token terpercaya yang ingin Anda gunakan.

- Untuk menambahkan penerbit token terpercaya baru:

1. Pilih Buat penerbit token terpercaya.

2. Tab browser baru terbuka. Ikuti langkah 5 hingga 8 inci [Cara menambahkan penerbit token terpercaya ke konsol Pusat Identitas IAM](#).

3. Setelah Anda menyelesaikan langkah-langkah ini, kembali ke jendela browser yang Anda gunakan untuk pengaturan aplikasi Anda dan pilih penerbit token terpercaya yang baru saja Anda tambahkan.

4. Dalam daftar penerbit token terpercaya, pilih kotak centang di sebelah nama penerbit token terpercaya yang baru saja Anda tambahkan.

Setelah Anda memilih penerbit token terpercaya, bagian Konfigurasi penerbit token terpercaya yang dipilih akan muncul.

2. Di bawah Konfigurasi penerbit token terpercaya yang dipilih, masukkan klaim Aud. Klaim mengidentifikasi audiens (penerima) yang dituju untuk token yang dihasilkan oleh penerbit token terpercaya. Untuk informasi selengkapnya, lihat [Klaim Aud](#).
3. Untuk mencegah pengguna Anda harus melakukan autentikasi ulang saat mereka menggunakan aplikasi ini, pilih Aktifkan pemberian token penyegaran. Ketika 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 kredensial aplikasi](#).

Langkah 4: Tentukan kredensial aplikasi

Selesaikan langkah-langkah dalam prosedur ini untuk menentukan kredensial yang digunakan aplikasi Anda untuk melakukan tindakan pertukaran token dengan aplikasi tepercaya. Kredensial ini digunakan dalam kebijakan berbasis sumber daya. Kebijakan 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 melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah.

Kebijakan ini memerlukan tindakan [CreateTokenWithIAM](#) API. Untuk informasi selengkapnya tentang kebijakan ini, dan contoh yang dapat Anda sesuaikan sesuai kebutuhan untuk lingkungan Anda, lihat [Resource-based contoh kebijakan untuk Pusat Identitas IAM](#).

1. Pada halaman Tentukan kredensial aplikasi, lakukan salah satu hal berikut:
 - Untuk menentukan satu atau beberapa 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 [Cross-account akses 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 non-AWS kredensial):
 1. Pilih Edit kebijakan aplikasi.
 2. Ubah kebijakan Anda dengan mengetik atau menempelkan teks di kotak teks JSON.

3. Selesaikan peringatan keamanan, kesalahan, atau peringatan umum yang dihasilkan selama validasi kebijakan. Untuk informasi selengkapnya, lihat [Memvalidasi kebijakan IAM](#) di Panduan AWS Identity and Access Management Pengguna.
2. Pilih Berikutnya dan lanjutkan ke halaman berikutnya [Langkah 5: Tinjau dan konfigurasi](#).

Langkah 5: Tinjau dan konfigurasi

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 Tambahkan aplikasi.
3. Aplikasi yang Anda tambahkan muncul di daftar aplikasi yang dikelola pelanggan.
4. Setelah menyiapkan aplikasi yang dikelola pelanggan di Pusat Identitas IAM, Anda harus menentukan satu atau lebih Layanan AWS, 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 penyebaran identitas. Tentukan AWS layanan yang memiliki data yang perlu diakses oleh pengguna aplikasi yang dikelola pelanggan Anda. Saat pengguna masuk ke aplikasi yang dikelola pelanggan, aplikasi tersebut akan meneruskan identitas pengguna Anda ke aplikasi tepercaya.

Gunakan prosedur berikut untuk memilih layanan, lalu tentukan aplikasi individual untuk dipercaya untuk layanan tersebut.

1. Buka konsol [Pusat Identitas IAM](#).
2. Pilih Aplikasi.
3. Pilih tab Customer managed.
4. Dalam daftar aplikasi yang dikelola pelanggan, pilih aplikasi OAuth 2.0 yang ingin Anda mulai meminta 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 penyebaran 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 Konfigurasi akses, di bawah Metode konfigurasi, lakukan salah satu dari hal berikut:
 - Pilih akses per aplikasi — Pilih opsi ini untuk mengonfigurasi tingkat akses yang berbeda untuk setiap aplikasi. Pilih aplikasi yang ingin Anda konfigurasi tingkat akses, lalu pilih Edit akses. Di Tingkat akses yang akan 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 berdasarkan per aplikasi.
10. Pilih Berikutnya.
11. Pada halaman Tinjau konfigurasi, 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 Percaya.

Menggunakan aplikasi dengan penerbit token tepercaya

Penerbit token tepercaya memungkinkan Anda menggunakan propagasi identitas tepercaya dengan aplikasi yang mengotentikasi di luar. AWS Dengan penerbit token tepercaya, Anda dapat mengotorisasi aplikasi ini untuk membuat permintaan atas nama pengguna mereka untuk mengakses aplikasi yang AWS dikelola.

Topik berikut menjelaskan cara kerja penerbit token tepercaya dan memberikan panduan penyiapan.

Topik

- [Ikhtisar penerbit token tepercaya](#)

- [Prasyarat dan pertimbangan untuk penerbit token terpercaya](#)
- [Rincian klaim JTI](#)
- [Pengaturan konfigurasi penerbit token terpercaya](#)
- [Menyiapkan penerbit token terpercaya](#)
- [Identity-enhanced Sesi peran IAM](#)

Ikhtisar penerbit token terpercaya

Propagasi identitas terpercaya menyediakan mekanisme yang memungkinkan aplikasi yang melakukan otentikasi di luar AWS untuk membuat permintaan atas nama pengguna mereka dengan menggunakan penerbit token terpercaya. Penerbit token terpercaya adalah server otorisasi OAuth 2.0 yang membuat token yang ditandatangani. Token ini mengotorisasi aplikasi yang memulai permintaan (meminta aplikasi) untuk akses ke Layanan AWS(menerima aplikasi). Aplikasi yang meminta memulai permintaan akses atas nama pengguna yang diautentikasi oleh penerbit token terpercaya. Pengguna dikenal oleh penerbit token terpercaya dan Pusat Identitas IAM.

Layanan AWS yang menerima permintaan mengelola otorisasi halus ke sumber daya mereka berdasarkan pengguna dan keanggotaan grup seperti yang diwakili dalam direktori Pusat Identitas. Layanan AWS tidak dapat menggunakan token dari penerbit token eksternal secara langsung.

Untuk mengatasi hal ini, Pusat Identitas IAM menyediakan cara bagi aplikasi yang meminta, atau AWS driver yang digunakan aplikasi yang meminta, untuk menukar token yang dikeluarkan oleh penerbit token terpercaya dengan token yang dihasilkan oleh Pusat Identitas IAM. Token yang dihasilkan oleh Pusat Identitas IAM mengacu pada pengguna Pusat Identitas IAM yang sesuai. Aplikasi yang meminta, atau pengemudi, 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 seperti yang diwakili di Pusat Identitas IAM.

Important

Memilih server otorisasi OAuth 2.0 untuk ditambahkan sebagai penerbit token terpercaya adalah keputusan keamanan yang memerlukan pertimbangan cermat. Hanya pilih penerbit token terpercaya 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 IAM Identity Center dengan token yang dibuat IAM Identity Center.

Prasyarat dan pertimbangan untuk penerbit token tepercaya

Sebelum 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 adalah penyedia identitas yang Anda gunakan sebagai sumber identitas untuk Pusat Identitas IAM, tidak harus demikian. Untuk informasi tentang cara mengatur penerbit token tepercaya, lihat dokumentasi untuk penyedia identitas yang relevan.

Note

Anda dapat mengonfigurasi hingga 10 penerbit token tepercaya untuk digunakan dengan Pusat Identitas IAM, selama Anda memetakan identitas setiap pengguna di penerbit token tepercaya ke pengguna terkait di Pusat Identitas IAM.

- 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 menerbitkan 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 Layanan AWS yang akan diakses setelah token ditukar dengan token dari Pusat Identitas IAM. Untuk informasi selengkapnya, lihat [Klaim Aud](#).

- [Waktu Kedalu](#) warsa (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 Pusat Identitas IAM.

 Note

Menggunakan kunci penandatanganan khusus untuk JWT dari tidak Microsoft Entra ID didukung. Untuk menggunakan token dari penerbit token Microsoft Entra ID tepercaya, Anda tidak dapat menggunakan kunci penandatanganan khusus.

- Klaim opsional

Pusat Identitas IAM 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, bila ada, mencegah token yang memiliki JTI yang sama digunakan kembali untuk pertukaran token. Untuk informasi selengkapnya tentang klaim JTI, lihat [Rincian klaim JTI](#).

- Konfigurasi Pusat Identitas IAM 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 hal berikut:

- Sinkronisasi pengguna ke Pusat Identitas IAM dengan menggunakan protokol System for Cross-domain Identity Management (SCIM) 2.0.
- Buat pengguna langsung di Pusat Identitas IAM.

Rincian klaim JTI

Jika Pusat Identitas IAM menerima permintaan untuk menukar token yang telah ditukar IAM Identity Center, permintaan gagal. Untuk mendeteksi dan mencegah penggunaan kembali token untuk pertukaran token, Anda dapat menyertakan klaim JTI. Pusat Identitas IAM melindungi dari 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 mungkin 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 IAM Identity Center API. Untuk informasi tentang mengonfigurasi aplikasi yang dikelola pelanggan untuk mendapatkan dan menukar token yang benar, lihat dokumentasi untuk aplikasi.

Pengaturan konfigurasi penerbit token tepercaya

Bagian berikut menjelaskan pengaturan yang diperlukan untuk menyiapkan dan menggunakan penerbit token tepercaya.

Topik

- [URL titik akhir penemuan OIDC \(URL penerbit\)](#)
- [Pemetaan atribut](#)
- [Klaim Aud](#)

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 Pusat Identitas IAM, 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 Pusat Identitas IAM tidak memvalidasi URL ini, jika URL tidak dibentuk dengan benar, penyiapan penerbit token tepercaya akan gagal tanpa pemberitahuan. URL titik akhir penemuan OIDC harus dapat dijangkau melalui port 80 dan 443 saja.

Pusat Identitas IAM menggunakan URL ini untuk mendapatkan informasi tambahan tentang penerbit token terpercaya. Misalnya, Pusat Identitas IAM menggunakan URL ini untuk mendapatkan informasi yang diperlukan untuk memverifikasi token yang dihasilkan oleh penerbit token terpercaya. Saat menambahkan penerbit token terpercaya 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 terpercaya kepada satu pengguna di Pusat Identitas IAM. Anda harus menentukan pemetaan atribut saat menambahkan penerbit token terpercaya ke Pusat Identitas IAM. Pemetaan atribut ini digunakan dalam klaim dalam token yang dihasilkan oleh penerbit token terpercaya. Nilai dalam klaim digunakan untuk mencari Pusat Identitas IAM. Pencarian menggunakan atribut yang ditentukan untuk mengambil satu pengguna di Pusat Identitas IAM, 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 Pusat Identitas IAM berikut: nama pengguna, email, dan ID eksternal. Nilai 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 diautentikasi melalui penyedia identitas yang tidak terfederasi ke Pusat Identitas IAM, penyedia identitas tersebut harus diatur sebagai penerbit token terpercaya. Aplikasi yang menerima permintaan akses (aplikasi penerima) harus menukar token yang dihasilkan oleh penerbit token terpercaya dengan token yang dihasilkan oleh IAM Identity Center.

Untuk informasi tentang cara mendapatkan nilai klaim aud untuk aplikasi penerima karena terdaftar di penerbit token terpercaya, lihat dokumentasi untuk penerbit token terpercaya Anda atau hubungi administrator penerbit token terpercaya untuk mendapatkan bantuan.

Menyiapkan penerbit token terpercaya

Untuk mengaktifkan propagasi identitas terpercaya untuk aplikasi yang mengotentikasi secara eksternal ke Pusat Identitas IAM, satu atau lebih administrator harus menyiapkan penerbit token terpercaya. Penerbit token terpercaya 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 (an Layanan AWS).

Topik

- [Mengkoordinasikan peran dan tanggung jawab administratif](#)
- [Tugas untuk menyiapkan penerbit token tepercaya](#)
- [Cara menambahkan penerbit token tepercaya ke konsol Pusat Identitas IAM](#)
- [Cara melihat atau mengedit setelan penerbit token tepercaya di konsol Pusat Identitas IAM](#)
- [Proses pengaturan 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, diperlukan koordinasi yang erat. 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	Koordinasi dengan
Administrator Pusat Identitas IAM	Menambahkan IdP eksternal sebagai penerbit token tepercaya ke konsol Pusat Identitas IAM. Membantu mengatur pemetaan atribut yang benar antara Pusat Identitas IAM dan IdP eksternal.	Administrator IdP eksternal (penerbit token tepercaya) AWS administrator layanan

Peran	Melakukan tugas-tugas ini	Koordinasi dengan
	Memberi tahu administrator AWS layanan saat penerbit token tepercaya ditambahkan ke konsol Pusat Identitas IAM.	
Administrator IdP eksternal (penerbit token tepercaya)	<p>Mengkonfigurasi IdP eksternal untuk mengeluarkan token.</p> <p>Membantu mengatur pemetaan atribut yang benar antara Pusat Identitas IAM dan IdP eksternal.</p> <p>Memberikan nama audiens (klaim Aud) kepada administrator AWS layanan.</p>	<p>Administrator Pusat Identitas IAM</p> <p>AWS administrator layanan</p>
AWS administrator layanan	<p>Memeriksa konsol AWS layanan untuk penerbit token tepercaya . Penerbit token tepercaya akan terlihat di konsol AWS layanan setelah administrator Pusat Identitas IAM menambakkannya ke konsol Pusat Identitas IAM.</p> <p>Mengkonfigurasi AWS layanan untuk menggunakan penerbit token tepercaya.</p>	<p>Administrator Pusat Identitas IAM</p> <p>Administrator IdP eksternal (penerbit token tepercaya)</p>

Tugas untuk menyiapkan penerbit token tepercaya

Untuk mengatur penerbit token tepercaya, administrator Pusat Identitas IAM, administrator IdP (penerbit token tepercaya) eksternal, 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 terpercaya.

1. Tambahkan penerbit token terpercaya ke Pusat Identitas IAM — Administrator Pusat Identitas IAM [menambahkan penerbit token terpercaya dengan menggunakan konsol](#) atau API Pusat Identitas IAM. https://docs.aws.amazon.com/singlesignon/latest/APIReference/API_Operations.html Konfigurasi ini memerlukan penentuan yang berikut:
 - Nama untuk penerbit token terpercaya.
 - URL titik akhir penemuan OIDC (di konsol Pusat Identitas IAM, URL ini disebut URL penerbit). Titik akhir penemuan harus dapat dijangkau melalui port 80 dan 443 saja.
 - Pemetaan atribut untuk pencarian pengguna. Pemetaan atribut ini digunakan dalam klaim dalam token yang dihasilkan oleh penerbit token terpercaya. Nilai dalam klaim digunakan untuk mencari Pusat Identitas IAM. Pencarian menggunakan atribut yang ditentukan untuk mengambil satu pengguna di Pusat Identitas IAM.
2. Hubungkan AWS layanan ke Pusat Identitas IAM — Administrator AWS layanan harus menghubungkan aplikasi ke Pusat Identitas IAM dengan menggunakan konsol untuk aplikasi atau API aplikasi.

Setelah penerbit token terpercaya ditambahkan ke konsol Pusat Identitas IAM, token ini juga terlihat di konsol AWS layanan dan tersedia untuk AWS dipilih administrator layanan.

3. Konfigurasi penggunaan pertukaran token — Di konsol AWS layanan, administrator layanan mengonfigurasi AWS layanan untuk menerima token yang dikeluarkan oleh penerbit token terpercaya. Token ini ditukar dengan token yang dihasilkan oleh IAM Identity Center. Ini mengharuskan menentukan nama penerbit token terpercaya dari Langkah 1, dan nilai klaim Aud yang sesuai dengan AWS layanan.

Penerbit token terpercaya menempatkan nilai klaim Aud di token yang dikeluarkan untuk menunjukkan bahwa token dimaksudkan untuk digunakan oleh AWS layanan. Untuk mendapatkan nilai ini, hubungi administrator untuk penerbit token terpercaya.

Cara menambahkan penerbit token tepercaya ke konsol Pusat Identitas IAM

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 Pusat Identitas IAM dan di konsol aplikasi.
6. Di bawah Atribut peta, lakukan hal berikut:
 - Untuk atribut penyedia identitas, pilih atribut dari daftar untuk dipetakan ke atribut di penyimpanan identitas Pusat Identitas IAM.
 - Untuk atribut Pusat Identitas IAM, 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 [Sumber daya penandaan AWS IAM Identity Center](#).

8. Pilih Buat penerbit token tepercaya.

9. Setelah Anda selesai membuat penerbit token terpercaya, hubungi administrator aplikasi untuk memberi tahu mereka nama penerbit token terpercaya, sehingga mereka dapat mengonfirmasi bahwa penerbit token terpercaya terlihat di konsol yang berlaku.
10. Administrator aplikasi harus memilih penerbit token terpercaya ini di konsol yang berlaku untuk mengaktifkan akses pengguna ke aplikasi dari aplikasi yang dikonfigurasi untuk propagasi identitas terpercaya.

Cara melihat atau mengedit setelan penerbit token terpercaya di konsol Pusat Identitas IAM

Setelah menambahkan penerbit token terpercaya ke konsol Pusat Identitas IAM, Anda dapat melihat dan mengedit pengaturan yang relevan.

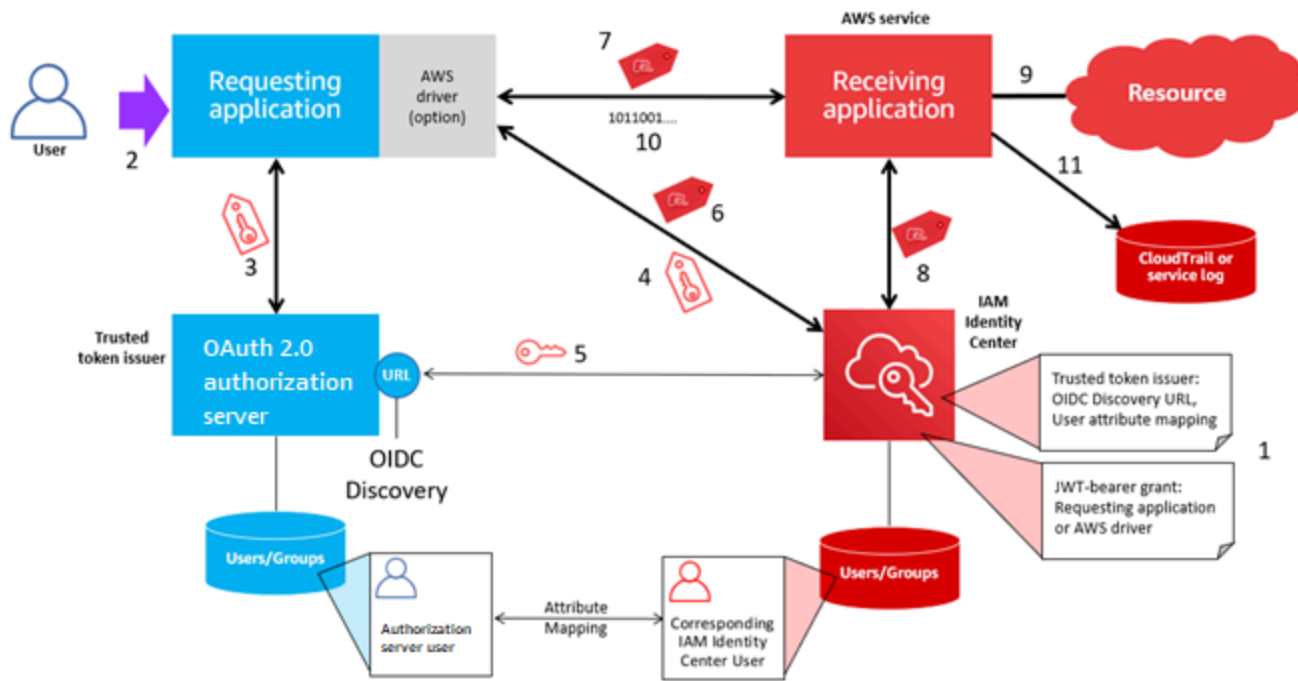
Jika Anda berencana untuk mengedit setelan penerbit token terpercaya, perlu diingat bahwa hal itu dapat menyebabkan pengguna kehilangan akses ke aplikasi apa pun yang dikonfigurasi untuk menggunakan penerbit token terpercaya. Untuk menghindari gangguan akses pengguna, sebaiknya Anda berkoordinasi dengan administrator untuk aplikasi apa pun yang dikonfigurasi untuk menggunakan penerbit token terpercaya sebelum Anda mengedit setelan.

Untuk melihat atau mengedit setelan penerbit token terpercaya 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 terpercaya, pilih penerbit token terpercaya yang ingin Anda lihat atau edit.
5. Pilih Tindakan, dan kemudian pilih Edit.
6. Pada halaman Edit penerbit token terpercaya, lihat atau edit pengaturan sesuai kebutuhan. Anda dapat mengedit nama penerbit token terpercaya, pemetaan atribut, dan tag.
7. Pilih Simpan perubahan.
8. Di kotak dialog Edit penerbit token terpercaya, Anda akan diminta untuk mengonfirmasi bahwa Anda ingin membuat perubahan. Pilih Konfirmasi.

Proses pengaturan dan alur permintaan untuk aplikasi yang menggunakan penerbit token terpercaya

Bagian ini menjelaskan proses penyiapan dan alur permintaan untuk aplikasi yang menggunakan penerbit token terpercaya untuk propagasi identitas terpercaya. Diagram berikut memberikan gambaran umum tentang proses ini.



Langkah-langkah berikut memberikan informasi tambahan tentang proses ini.

1. Siapkan Pusat Identitas IAM dan aplikasi terkel AWS ola penerima untuk menggunakan penerbit token terpercaya. Untuk informasi, lihat [Tugas untuk menyiapkan penerbit token terpercaya](#).
2. Alur permintaan dimulai ketika pengguna membuka aplikasi yang meminta.
3. Aplikasi yang meminta meminta token dari penerbit token terpercaya untuk memulai permintaan ke aplikasi terkel AWS ola penerima. Jika pengguna belum diautentikasi, proses ini memicu aliran otentikasi. Token berisi informasi berikut:
 - Subjek (Sub) pengguna.
 - Atribut yang digunakan Pusat Identitas IAM untuk mencari pengguna terkait di Pusat Identitas IAM.
 - Klaim audiens (Aud) yang berisi nilai yang dikaitkan penerbit token terpercaya dengan aplikasi terkel AWS ola penerima. Jika ada klaim lain, klaim tersebut tidak digunakan oleh Pusat Identitas IAM.

4. Aplikasi yang meminta, atau AWS driver yang menggunakannya, meneruskan token ke Pusat Identitas IAM dan meminta agar token ditukar dengan token yang dihasilkan oleh Pusat Identitas IAM. Jika Anda menggunakan AWS driver, Anda mungkin perlu mengkonfigurasi driver untuk kasus penggunaan ini. Untuk informasi selengkapnya, lihat dokumentasi untuk aplikasi terkel AWS ola yang relevan.
5. Pusat Identitas IAM menggunakan titik akhir OIDC Discovery untuk mendapatkan kunci publik yang dapat digunakan untuk memverifikasi keaslian token. IAM Identity Center kemudian melakukan hal berikut:
 - Memverifikasi token.
 - Menelusuri direktori Identity Center. Untuk melakukan ini, Pusat Identitas IAM menggunakan atribut yang dipetakan yang ditentukan dalam token.
 - Memverifikasi bahwa pengguna diberi wewenang untuk mengakses aplikasi penerima. Jika aplikasi AWS terkelola dikonfigurasi untuk memerlukan penugasan kepada pengguna dan grup, pengguna harus memiliki penugasan langsung atau berbasis grup ke aplikasi; jika tidak, permintaan ditolak. Jika aplikasi ter AWS kelola dikonfigurasi untuk tidak memerlukan penugasan pengguna dan grup, pemrosesan berlanjut.

 Note

AWS layanan memiliki konfigurasi pengaturan default yang menentukan apakah penugasan diperlukan untuk pengguna dan grup. Sebaiknya jangan memodifikasi setelan M memerlukan penugasan untuk aplikasi ini jika Anda berencana menggunakannya dengan propagasi identitas tepercaya. Bahkan jika Anda telah mengonfigurasi izin berbutir halus yang memungkinkan akses pengguna ke sumber daya aplikasi tertentu, memodifikasi setelan M memerlukan penugasan dapat mengakibatkan perilaku tak terduga, termasuk akses pengguna yang terganggu ke sumber daya ini.

- Memverifikasi bahwa aplikasi yang meminta dikonfigurasi untuk menggunakan cakupan yang valid untuk aplikasi terkel AWS ola penerima.
6. Jika langkah verifikasi sebelumnya berhasil, Pusat Identitas IAM membuat token baru. Token baru adalah token buram (terenkripsi) yang mencakup identitas pengguna terkait di Pusat Identitas IAM, audiens (Aud) dari aplikasi terkel AWS ola penerima, dan cakupan yang dapat digunakan aplikasi yang meminta saat membuat permintaan ke aplikasi terkel AWS ola penerima.

7. Aplikasi yang meminta, atau driver yang menggunakannya, memulai permintaan sumber daya ke aplikasi penerima dan meneruskan token yang dihasilkan IAM Identity Center ke aplikasi penerima.
8. Aplikasi penerima melakukan panggilan ke Pusat Identitas IAM untuk mendapatkan identitas pengguna dan cakupan yang dikodekan dalam token. Mungkin juga membuat permintaan untuk mendapatkan atribut pengguna atau keanggotaan grup pengguna dari direktori Identity Center.
9. Aplikasi penerima menggunakan konfigurasi otorisasi untuk menentukan apakah pengguna berwenang untuk mengakses sumber daya aplikasi yang diminta.
10. Jika pengguna diberi wewenang untuk mengakses sumber daya aplikasi yang diminta, aplikasi penerima menanggapi permintaan tersebut.
11. Identitas pengguna, tindakan yang dilakukan atas nama mereka, dan peristiwa lainnya dicatat dalam log dan CloudTrail peristiwa aplikasi penerima. Cara spesifik di mana informasi ini dicatat bervariasi berdasarkan aplikasi.

Identity-enhanced Sesi peran IAM

[AWS Security Token Service](#) (STS) memungkinkan aplikasi untuk mendapatkan sesi peran IAM yang ditingkatkan identitas. Identity-enhanced sesi peran memiliki konteks identitas tambahan yang membawa pengenalan pengguna ke Layanan AWS yang dipanggilnya. Layanan AWS dapat mencari keanggotaan grup dan atribut pengguna di Pusat Identitas IAM dan menggunakannya untuk mengotorisasi akses pengguna ke sumber daya.

AWS aplikasi memperoleh sesi peran yang ditingkatkan identitas dengan membuat permintaan ke tindakan AWS STS [AssumeRole](#) API dan meneruskan pernyataan konteks dengan pengenalan pengguna (`userId`) dalam `ProvidedContexts` parameter permintaan ke `AssumeRole`. Pernyataan konteks diperoleh dari `idToken` klaim yang diterima sebagai tanggapan atas permintaan SSO OIDC ke [CreateTokenWithIAM](#). Ketika AWS aplikasi menggunakan sesi peran yang ditingkatkan identitas untuk mengakses sumber daya, CloudTrail mencatat sesi `userId` awal, dan tindakan yang diambil. Untuk informasi selengkapnya, lihat [Identity-enhanced Pencatatan sesi peran IAM](#).

Topik

- [Jenis sesi peran IAM yang ditingkatkan identitas](#)
- [Identity-enhanced Pencatatan sesi peran IAM](#)

Jenis sesi peran IAM yang ditingkatkan identitas

AWS STS dapat membuat dua jenis sesi peran IAM yang ditingkatkan identitas, tergantung pada pernyataan konteks yang diberikan untuk permintaan. `AssumeRole` Aplikasi yang telah memperoleh token Id dari Pusat Identitas IAM dapat menambahkan `sts:identity_context` (disarankan) atau `sts:audit_context` (Didukung untuk kompatibilitas mundur) ke sesi peran IAM. Sesi peran IAM yang ditingkatkan identitas hanya dapat memiliki satu dari pernyataan konteks ini, bukan keduanya.

Identity-enhanced Sesi peran IAM dibuat dengan `sts:identity_context`

Ketika sesi peran yang ditingkatkan identitas berisi `sts:identity_context` panggilan Layanan AWS menentukan apakah otorisasi sumber daya didasarkan pada pengguna yang diwakili dalam sesi peran, atau jika didasarkan pada peran. Layanan AWS yang mendukung otorisasi berbasis pengguna memberi administrator aplikasi kontrol untuk menetapkan akses ke pengguna atau grup yang menjadi anggotanya pengguna.

Layanan AWS yang tidak mendukung otorisasi berbasis pengguna mengabaikan.

`sts:identity_context` CloudTrail mencatat `userId` pengguna IAM Identity Center dengan semua tindakan yang diambil oleh peran tersebut. Untuk informasi selengkapnya, lihat [Identity-enhanced Pencatatan sesi peran IAM](#).

Untuk mendapatkan jenis sesi peran yang ditingkatkan identitas ini dari AWS STS, aplikasi memberikan nilai `sts:identity_context` bidang dalam [AssumeRole](#) permintaan menggunakan parameter `ProvidedContexts` permintaan. Gunakan `arn:aws:iam::aws:contextProvider/IdentityCenter` sebagai nilai untuk `ProviderArn`.

Untuk informasi selengkapnya tentang bagaimana otorisasi berperilaku, lihat dokumentasi untuk penerima Layanan AWS.

Identity-enhanced Sesi peran IAM dibuat dengan `sts:audit_context`

Di masa lalu `sts:audit_context`, digunakan untuk memungkinkan Layanan AWS untuk mencatat identitas pengguna tanpa menggunakannya untuk membuat keputusan otorisasi. Layanan AWS sekarang dapat menggunakan konteks tunggal - `sts:identity_context` - untuk mencapai ini serta untuk membuat keputusan otorisasi. Sebaiknya gunakan `sts:identity_context` di semua penerapan baru propagasi identitas tepercaya.

Identity-enhanced Pencatatan sesi peran IAM

Ketika permintaan dibuat untuk Layanan AWS menggunakan sesi peran IAM yang ditingkatkan identitas, Pusat Identitas IAM pengguna masuk ke `userId` CloudTrail dalam elemen. `OnBehalfOf`

Cara di mana acara masuk CloudTrail bervariasi berdasarkan Layanan AWS. Tidak semua Layanan AWS mencatat onBehalfOf elemen.

Berikut ini adalah contoh bagaimana permintaan yang dibuat untuk Layanan AWS menggunakan sesi peran yang ditingkatkan identitas masuk. CloudTrail

```
"userIdentity": {
  "type": "AssumedRole",
  "principalId": "AROEXAMPLE:MyRole",
  "arn": "arn:aws:sts::111111111111:assumed-role/MyRole/MySession",
  "accountId": "111111111111",
  "accessKeyId": "ASIAEXAMPLE",
  "sessionContext": {
    "sessionIssuer": {
      "type": "Role",
      "principalId": "AROEXAMPLE",
      "arn": "arn:aws:iam::111111111111:role/MyRole",
      "accountId": "111111111111",
      "userName": "MyRole"
    },
    "attributes": {
      "creationDate": "2023-12-12T13:55:22Z",
      "mfaAuthenticated": "false"
    }
  },
  "onBehalfOf": {
    "userId": "11111111-1111-1111-1111-111111111111",
    "identityStoreArn": "arn:aws:identitystore::111111111111:identitystore/d-1111111111"
  }
}
```

Putar sertifikat Pusat Identitas IAM

Pusat Identitas IAM menggunakan sertifikat untuk mengatur hubungan kepercayaan SAML antara Pusat Identitas IAM dan penyedia layanan aplikasi Anda. Saat Anda menambahkan aplikasi di Pusat Identitas IAM, sertifikat Pusat Identitas IAM secara otomatis dibuat untuk digunakan dengan aplikasi tersebut selama proses penyiapan. Secara default, sertifikat Pusat Identitas IAM 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 pada sertifikat mendekati. Proses penggantian sertifikat yang lebih lama dengan yang lebih baru disebut sebagai rotasi sertifikat.

Pertimbangan sebelum memutar sertifikat

Sebelum memulai proses rotasi sertifikat di Pusat Identitas IAM, pertimbangkan hal berikut:

- Proses rotasi sertifikasi mengharuskan Anda membangun kembali kepercayaan antara Pusat Identitas IAM dan penyedia layanan. Untuk membangun kembali kepercayaan, gunakan prosedur yang disediakan di [Memutar sertifikat Pusat Identitas IAM](#).
- Memperbarui sertifikat dengan penyedia layanan dapat menyebabkan gangguan layanan sementara bagi pengguna Anda sampai kepercayaan berhasil dibangun kembali. Rencanakan operasi ini dengan hati-hati selama jam sibuk jika memungkinkan.

Memutar sertifikat Pusat Identitas IAM

Memutar sertifikat Pusat Identitas IAM adalah proses multi-langkah yang melibatkan hal-hal berikut:

- Menghasilkan sertifikat baru
- Menambahkan sertifikat baru ke situs web penyedia layanan
- Menyetel sertifikat baru menjadi aktif
- Menghapus sertifikat 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 buat dapat dikonfigurasi untuk menggunakan properti berikut:

- Periode validitas — Menentukan waktu yang dialokasikan (dalam bulan) sebelum sertifikat Pusat Identitas IAM 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 https://en.wikipedia.org/wiki/Key_size kunci.

- **Algoritma** — Menentukan algoritma yang digunakan IAM Identity Center saat menandatangani SAM assertion/response L. Anda dapat mengatur nilai ini ke salah satu SHA-1 atau SHA-256. AWS merekomendasikan penggunaan SHA-256 jika memungkinkan, kecuali penyedia layanan Anda mengharuskannya SHA-1. Untuk informasi umum tentang cara kerja algoritma kriptografi, lihat [Public-key krypto](#) grafi.

1. Buka konsol [Pusat Identi](#) tas 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 Kel ola 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 Buat sertifikat baru.
6. Dalam kotak dialog Hasilkan sertifikat Pusat Identitas IAM baru, tentukan nilai yang sesuai untuk Masa berlaku, Algoritma, dan ukuran K unci. Kemudian pilih Generate.

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 instruksi, 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 untuknya. Pusat Identitas IAM akan menggunakan sertifikasi yang ditetapkan sebagai aktif untuk menandatangani semua pernyataan SAML.

1. Buka konsol [Pusat Identi](#) tas 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 Kel ola sertifikat.
5. Pada halaman sertifikat Pusat Identitas IAM, pilih sertifikat yang ingin Anda atur menjadi aktif, pilih Tind akan, lalu pilih Tet apkan sebagai aktif.
6. Dalam dialog Setel sertifikat yang dipilih sebagai aktif, konfirmasi bahwa Anda memahami bahwa menyetel sertifikat ke aktif mungkin mengharuskan Anda untuk membangun kembali kepercayaan, lalu pilih Jadikan aktif.

Langkah 4: Hapus sertifikat lama

Gunakan prosedur berikut untuk menyelesaikan proses rotasi sertifikat untuk aplikasi Anda. Anda hanya dapat menghapus sertifikat yang dalam keadaan Tidak aktif.

1. Buka konsol [Pusat Identi](#) tas 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 Kel ola sertifikat.
5. Pada halaman sertifikat Pusat Identitas IAM, pilih sertifikat yang ingin Anda hapus. Pilih Tind akan lalu pilih H apus.
6. Di kotak dialog H apus sertifikat, pilih H apus.

Indikator status kedaluwarsa sertifikat

Di konsol Pusat Identitas IAM, halaman Aplikasi menampilkan ikon indikator status di properti setiap aplikasi. Ikon-ikon ini ditampilkan di kolom Kedaluwarsa di sebelah 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 90 hari lagi.

Untuk memeriksa status sertifikat

1. Buka konsol [Pusat Identitas](#) IAM.
2. Pilih Aplikasi.
3. Dalam daftar aplikasi, tinjau status sertifikat dalam daftar seperti yang ditunjukkan pada kolom Kedaluwarsa.

Memahami properti aplikasi di konsol Pusat Identitas IAM

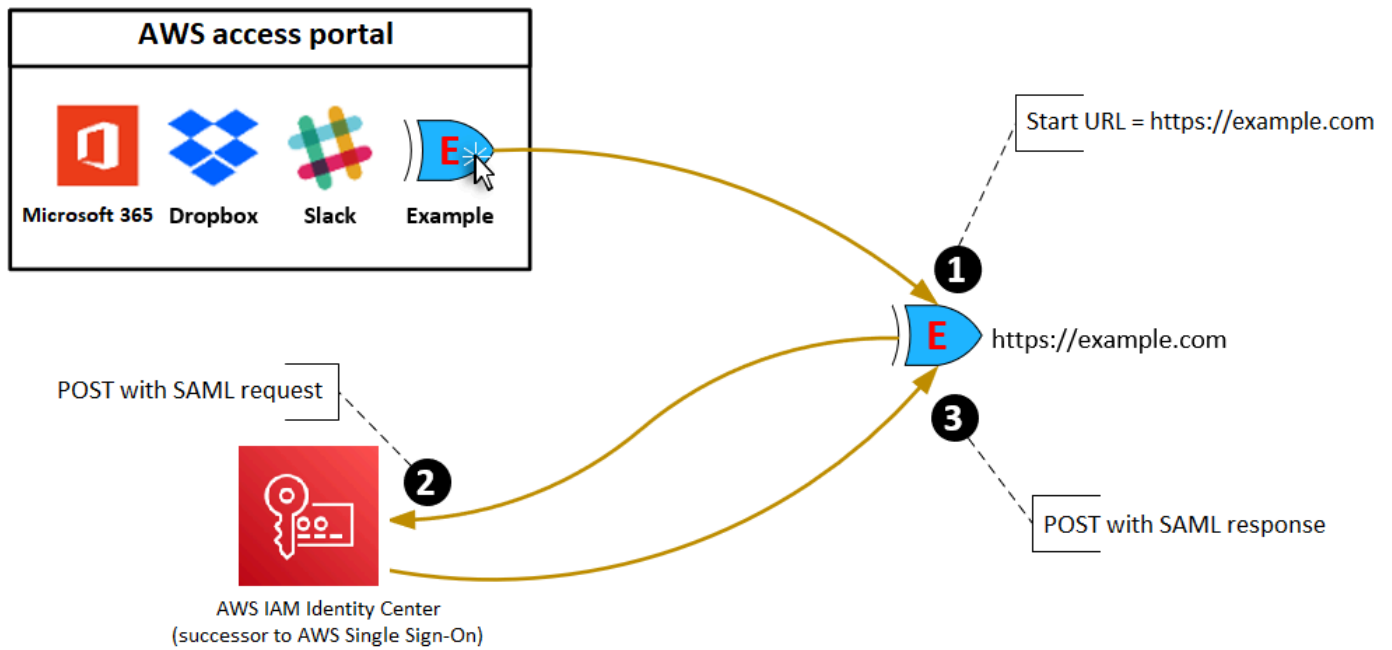
Di Pusat Identitas IAM Anda dapat menyesuaikan pengalaman pengguna dengan mengonfigurasi URL mulai aplikasi, status relai, dan durasi sesi.

URL mulai aplikasi

Anda menggunakan URL awal aplikasi untuk memulai proses federasi dengan aplikasi Anda. Penggunaan tipikal adalah untuk aplikasi yang hanya mendukung pengikatan yang diprakarsai oleh penyedia layanan (SP).

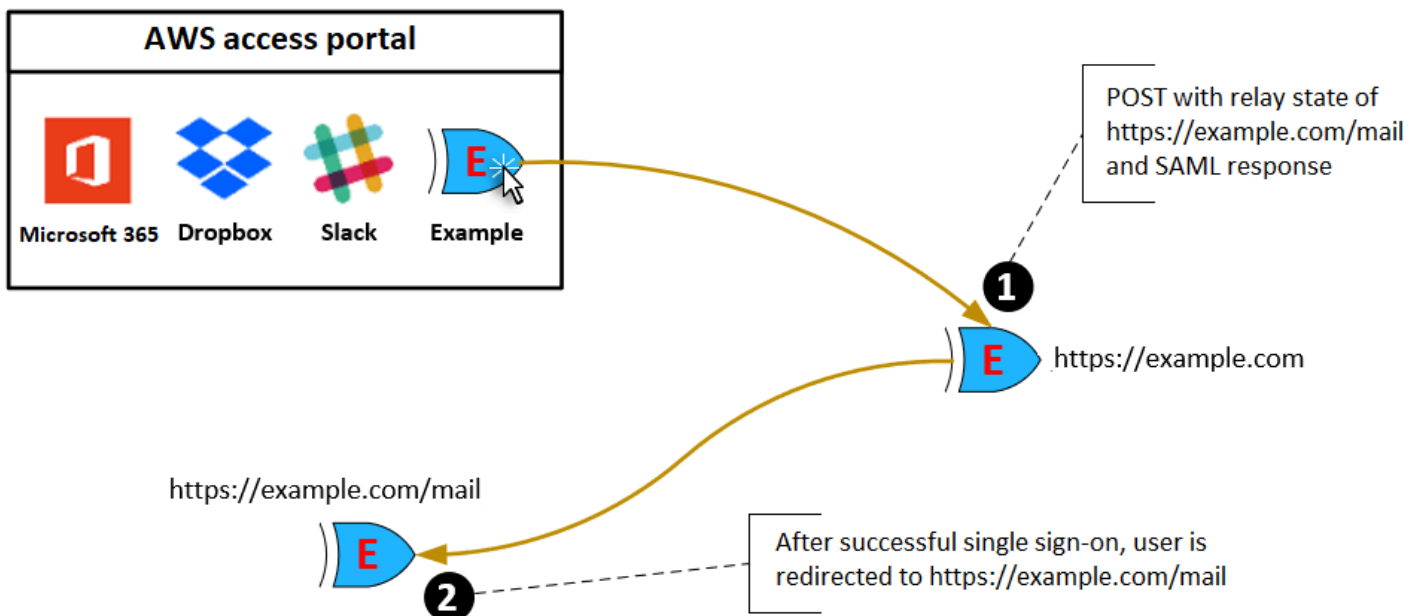
Langkah-langkah dan diagram berikut menggambarkan alur kerja otentikasi URL mulai aplikasi saat pengguna memilih aplikasi di portal AWS akses:

1. Browser pengguna mengalihkan permintaan otentikasi menggunakan nilai untuk URL awal aplikasi (dalam hal ini `https://example.com`).
2. Aplikasi mengirimkan HTML POST dengan a `SAMLRequest` ke Pusat Identitas IAM.
3. IAM Identity Center kemudian mengirim HTML POST dengan `SAMLResponse` kembali ke aplikasi.



Status relai

Selama proses otentikasi federasi, status relai mengalihkan pengguna dalam aplikasi. Untuk SAML 2.0, nilai ini diteruskan, tidak dimodifikasi, ke aplikasi. Setelah properti aplikasi dikonfigurasi, IAM Identity Center mengirimkan nilai status relai bersama dengan respons SAML ke aplikasi.



Durasi sesi

Durasi sesi adalah lamanya waktu di mana sesi pengguna aplikasi valid. Untuk SAML 2.0, ini digunakan untuk mengatur `SessionNotOnOrAfter` tanggal elemen pernyataan SAML. `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. Hal 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 mengkonfigurasi nilai. Ini dapat terjadi ketika aplikasi hanya mendukung panjang sesi tertentu.

Untuk informasi selengkapnya tentang bagaimana durasi sesi digunakan, lihat dokumentasi aplikasi spesifik Anda.

Menetapkan akses pengguna ke aplikasi di konsol Pusat Identitas IAM

Anda dapat menetapkan pengguna akses masuk tunggal ke aplikasi SAML 2.0 di katalog aplikasi atau ke aplikasi SAML 2.0 kustom.

Pertimbangan untuk tugas kelompok:

- Tetapkan akses langsung ke grup. Untuk membantu menyederhanakan administrasi izin akses, sebaiknya Anda menetapkan akses langsung ke grup daripada pengguna individual. 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, Pusat Identitas IAM 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 yang menjadi anggotanya pengguna.

Untuk menetapkan akses pengguna atau grup ke aplikasi

 Important

Untuk AWS aplikasi terkelola, Anda harus menambahkan pengguna langsung dari dalam konsol aplikasi yang relevan atau melalui API.

1. Buka konsol [Pusat Identi](#) tas IAM.

 Note

Jika Anda mengelola pengguna di AWS Managed Microsoft AD, pastikan konsol Pusat Identitas IAM menggunakan Wilayah AWS ayah 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 akses.
4. Pada halaman detail aplikasi, di bagian Pengguna yang ditugaskan, pilih Tetapkan pengguna.
5. Di kotak dialog Tetapkan pengguna, masukkan nama tampilan pengguna atau nama grup. Anda dapat menentukan beberapa pengguna atau grup dengan memilih akun yang berlaku saat mereka muncul di hasil penelusuran.
6. Pilih Tetapkan pengguna.

Hapus akses pengguna ke aplikasi SAML 2.0

Gunakan prosedur ini untuk menghapus akses pengguna ke aplikasi SAML 2.0 di katalog aplikasi atau aplikasi SAML 2.0 kustom. Untuk informasi selengkapnya tentang sesi dan durasi otentikasi, lihat [Memahami sesi otentikasi di Pusat Identitas IAM](#).

Untuk menghapus akses pengguna ke aplikasi

1. Buka konsol [Pusat Identi](#) tas IAM.

2. Pilih Aplikasi.
3. Dalam daftar aplikasi, pilih aplikasi yang ingin Anda hapus 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. Di kotak dialog Hapus akses, verifikasi nama pengguna atau grup. Kemudian pilih Hapus akses.

Memetakan atribut dalam aplikasi Anda ke atribut Pusat Identitas IAM

Beberapa penyedia layanan memerlukan pernyataan SAML 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 Pusat Identitas IAM.

Untuk memetakan atribut aplikasi ke atribut di Pusat Identitas IAM

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 lalu 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 Pusat Identitas IAM. Untuk melihat daftar atribut pengguna yang diizinkan di Pusat Identitas IAM, lihat tabel di [Pemetaan atribut antara Pusat Identitas IAM dan direktori Penyedia Identitas Eksternal](#).
8. Di kolom ketiga tabel, pilih format yang sesuai untuk atribut dari menu.
9. Pilih Simpan perubahan.

Konfigurasi akses ke Akun AWS

Instans organisasi dari Pusat Identitas IAM terintegrasi dengan AWS Organizations. Ini memungkinkan Anda untuk mengelola izin secara terpusat di beberapa Akun AWS tanpa mengonfigurasi akses satu per satu ke setiap akun.

Tabel berikut membandingkan opsi manajemen akses akun yang harus Anda pertimbangkan:

	Peran IAM dengan manajer akses akun	Kumpulan izin Pusat Identitas IAM	Peran IAM dengan federasi IAM langsung
Terbaik untuk	Tenaga kerja pengguna dan grup dengan peran IAM khusus yang bervariasi di seluruh akun. Pembuatan dan penyediaan peran terdesentralisasi dengan penetapan peran terpusat kepada pengguna.	Akses tenaga kerja dasar yang beragam seperti read-only dan admin. Pembuatan dan penyediaan peran terpusat.	Beban kerja
Lingkup	Beberapa akun dalam suatu AWS organisasi	Beberapa akun dalam suatu AWS organisasi	Per akun
Penyediaan peran IAM	<ul style="list-style-type: none"> Infrastruktur sebagai kode (IaC) Penyediaan manual melalui konsol AWS IAM 	Disediakan secara otomatis	<ul style="list-style-type: none"> Infrastruktur sebagai kode (IaC) Penyediaan manual melalui konsol AWS IAM atau konsol IdP eksternal
Role-to-identity pemetaan berada di	Manajer akses akun	Pusat Identitas IAM	IdP Eksternal

	Peran IAM dengan manajer akses akun	Kumpulan izin Pusat Identitas IAM	Peran IAM dengan federasi IAM langsung
Pengalaman pengguna akhir	Pengguna mengakses Akun AWS melalui URL portal akses akun. Memerlukan otentikasi Pusat Identitas IAM.	Pengguna mengakses Akun AWS melalui URL portal AWS akses.	Pengguna mengakses Akun AWS melalui aplikasi SAML khusus akun (ikon) di portal IdP mereka.
AWS CLI pengalaman pengguna	Pengguna masuk AWS dan mengakses Akun AWS dengan peran tertentu di browser web. Pengguna mengeksekusi login pada baris perintah untuk mengambil kredensial sesi peran IAM dari browser. Selama sesi peran IAM, pengguna dapat bekerja dengan AWS CLI tanpa melakukan autentikasi ulang.	Pengguna mengonfigurasi profil termasuk akun yang diinginkan dan pasangan peran dengan mengetikkan konfigurasi sso. Jenis pengguna aws sso login untuk memulai sesi baru menggunakan profil. Jika tidak ada sesi Pusat Identitas IAM yang aktif, pengguna melakukan otentikasi di browser. Lihat Panduan AWS IAM Identity Center Pengguna untuk detail selengkapnya.	Integrasi kustom menggunakan penyedia kredensial AWS SDK

Akun AWS tipe

Ada dua jenis Akun AWS di AWS Organizations:

- Akun manajemen - Akun AWS Yang digunakan untuk membuat organisasi.
- Akun anggota - Sisa dari Akun AWS akun 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 di delegasikan untuk Pusat Identitas IAM. Pengguna di akun ini dapat melakukan sebagian besar tugas administratif 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)	✔Iya	✔Ya	✔Ya
Menambahkan, mengedit, atau menghapus pengguna atau grup	✘Tidak	✔Ya*	✔Iya
Mengaktifkan atau menonaktifkan akses pengguna	✘Tidak	✔Iya	✔Ya
Mengaktifkan, menonaktifkan, atau mengelola atribut masuk	✘Tidak	✔Iya	✔Ya
Mengubah atau mengelola sumber identitas	✘Tidak	✔Iya	✔Ya
Membuat, mengedit, atau menghapus	✘Tidak	✔Iya	✔Ya

Tugas administrasi Pusat Identitas IAM	Akun Anggota	Akun administrator yang didelegasikan	Akun manajemen
aplikasi yang dikelola pelanggan			
Membuat, mengedit, atau menghapus aplikasi ter AWS kelola	✔Iya	✔Ya	✔Ya
Konfigurasi MFA	✘Tidak	✔Iya	✔Ya
Kelola kumpulan izin yang tidak disediakan di akun manajemen	✘Tidak	✔Iya	✔Ya
Mengelola kumpulan izin yang disediakan di akun manajemen	✘Tidak	✘Tidak	✔Iya
Aktifkan Pusat Identitas IAM	✘Tidak	✘Tidak	✔Iya
Hapus konfigurasi Pusat Identitas IAM	✘Tidak	✘Tidak	✔Iya
Mengaktifkan atau menonaktifkan akses pengguna di akun manajemen	✘Tidak	✘Tidak	✔Iya
Mendaftarkan atau membatalkan pendaftaran akun anggota sebagai administrator yang didelegasikan	✘Tidak	✘Tidak	✔Iya

*Lihat praktik terbaik untuk administrasi yang didelegasikan mengenai penugasan pengguna dan grup ke akun manajemen.

Menugaskan Akun AWS akses

Anda dapat menggunakan kumpulan izin untuk menyederhanakan cara Anda menetapkan pengguna dan grup dalam akses organisasi Anda Akun AWS. Kumpulan izin disimpan di Pusat Identitas IAM dan menentukan tingkat akses yang dimiliki pengguna dan grup ke. Akun AWS Anda dapat membuat satu kumpulan izin dan menetapkan ke beberapa di Akun AWS dalam organisasi Anda. Anda juga dapat menetapkan beberapa set izin untuk pengguna yang sama.

Anda juga dapat menggunakan manajer akses [akun](#) — fitur IAM — untuk menetapkan peran IAM yang ada kepada pengguna dan grup Pusat Identitas IAM di akun organisasi Anda. Anda dapat menggunakan manajer akses akun sendiri, atau bersama dengan kumpulan izin. Manajer akses akun memberi Anda akses ke set fitur peran IAM lengkap, termasuk kebijakan kepercayaan khusus, tag peran untuk ABAC, dan jalur peran yang dapat dikonfigurasi.

Untuk informasi selengkapnya tentang kumpulan izin, lihat [Membuat, mengelola, dan menghapus set izin](#).

Note

Anda juga dapat menetapkan akses masuk tunggal pengguna ke aplikasi. Untuk informasi, lihat [Konfigurasi akses ke aplikasi](#).

End-user pengalaman

Portal AWS akses menyediakan pengguna Pusat Identitas IAM akses masuk tunggal ke semua aplikasi yang ditugaskan Akun AWS melalui portal web. Portal AWS akses berbeda dari [Konsol Manajemen AWS](#), yang merupakan kumpulan konsol layanan untuk mengelola AWS sumber daya.

Saat Anda membuat kumpulan izin, nama yang Anda tentukan untuk kumpulan izin 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 Konsol Manajemen AWS atau mengambil kredensial sementara untuk mengakses AWS layanan secara terprogram.

Untuk membuka Konsol Manajemen AWS atau mengambil kredensial 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. Menggunakan kredensial direktori mereka, mereka masuk ke portal AWS akses.
3. Setelah otentikasi, pada halaman portal AWS akses, mereka memilih tab Akun Akun AWS untuk menampilkan daftar yang mereka akses.
4. Pengguna kemudian memilih Akun AWS yang ingin mereka gunakan.
5. Di bawah nama Akun AWS, kumpulan izin apa pun yang ditugaskan pengguna akan muncul sebagai peran yang tersedia. Misalnya, jika Anda menetapkan pengguna `john_stiles` ke kumpulan `PowerUser` pulan izin, peran akan ditampilkan di portal AWS akses sebagai `PowerUser/john_stiles`. Pengguna yang diberi beberapa kumpulan izin memilih peran mana yang akan digunakan. Pengguna dapat memilih peran mereka untuk mengakses Konsol Manajemen AWS.
6. Selain peran, pengguna portal AWS akses dapat mengambil kredensial sementara untuk baris perintah atau akses terprogram dengan memilih tombol `Akses`.

Untuk panduan langkah demi langkah yang dapat Anda berikan kepada pengguna tenaga kerja Anda, lihat [Menyiapkan dan menggunakan AWS portal akses](#) dan [Mendapatkan kredensial pengguna Pusat Identitas IAM untuk AWS CLI atau AWS SDK](#).

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 mendelegasikan dan menegakkan pengguna mana yang memiliki akses masuk tunggal ke tertentu Akun AWS di organisasi Anda. AWS Organizations Anda perlu menetapkan satu atau lebih pengguna dengan akses ke akun, untuk menggunakan peran ini. Untuk informasi selengkapnya, lihat [Memahami peran terkait layanan di Pusat Identitas IAM](#) dan [Menggunakan peran terkait layanan untuk Pusat Identitas IAM](#).

Membatasi akses ke penyimpanan identitas dari akun anggota

Untuk layanan penyimpanan identitas yang digunakan oleh Pusat Identitas IAM, pengguna yang memiliki akses ke akun anggota dapat menggunakan tindakan API yang memerlukan izin Baca. Akun anggota memiliki akses ke tindakan Baca pada direktori sso dan ruang nama identitystore. Untuk informasi selengkapnya, lihat [Tindakan, sumber daya, dan kunci kondisi untuk AWS IAM Identity Center direktori](#) dan [Tindakan, sumber daya, dan kunci kondisi untuk Penyimpanan Identitas](#) di Referensi Otorisasi Layanan.

Untuk mencegah pengguna di akun anggota menggunakan operasi API di penyimpanan 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 penyimpanan identitas.

```
{
  "Sid": "ExplicitlyBlockIdentityStoreAccess",
  "Effect": "Deny",
  "Action": ["identitystore:*", "sso-directory:*"],
  "Resource": "*"
}
```

Note

Untuk memastikan aplikasi ter AWS kelola berfungsi dengan baik dengan Pusat Identitas IAM Anda, Anda harus menghindari menerapkan SCP ini ke Akun AWS tempat Anda menerapkan aplikasi tersebut. Juga, jika Anda menggunakan administrasi yang didelegasikan, Anda harus menghindari menerapkan SCP ini ke akun administrasi yang didelegasikan. Untuk informasi selengkapnya, lihat [Praktik terbaik](#).

Untuk informasi selengkapnya, lihat [Kebijakan Kontrol Layanan \(SCP\)](#) di Panduan Pengguna AWS Organizations .

Administrator yang didelegasikan

Administrasi yang didelegasikan menyediakan cara mudah bagi pengguna yang ditugaskan di akun anggota terdaftar untuk melakukan sebagian besar tugas administratif Pusat Identitas IAM. Saat Anda mengaktifkan Pusat Identitas IAM, instance Pusat Identitas IAM Anda dibuat di akun

manajemen secara AWS Organizations default. Ini awalnya dirancang dengan cara ini sehingga Pusat Identitas IAM dapat menyediakan, membatalkan penyediaan, dan memperbarui peran di semua akun anggota organisasi Anda. Meskipun instance Pusat Identitas IAM Anda harus selalu berada di akun manajemen, Anda dapat memilih untuk mendelegasikan administrasi Pusat Identitas IAM ke akun anggota di 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 akun anggota organisasi Anda

Untuk informasi selengkapnya tentang cara kerja IAM Identity Center AWS Organizations, lihat [Konfigurasi akses ke Akun AWS](#). Untuk informasi tambahan dan untuk meninjau contoh skenario perusahaan yang menunjukkan cara mengonfigurasi administrasi yang didelegasikan, lihat [Memulai dengan administrasi yang didelegasikan IAM Identity Center](#) di Blog AWS Keamanan.

Topik

- [Praktik terbaik](#)
- [Prasyarat](#)
- [Daftarkan akun anggota](#)
- [Menghapus 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 terendah, kami sangat menyarankan Anda membatasi akses ke akun manajemen untuk sesedikit mungkin orang. Fitur administrator yang didelegasikan dimaksudkan untuk meminimalkan jumlah orang yang

memerlukan akses ke akun manajemen. Anda juga dapat mempertimbangkan untuk menggunakan akses [yang ditingg](#)ikan sementara untuk memberikan akses ini hanya bila diperlukan.

- Kumpulan izin khusus untuk akun manajemen — Gunakan kumpulan izin khusus untuk akun manajemen. Untuk alasan keamanan, kumpulan izin yang digunakan untuk akses ke akun manajemen hanya dapat dimodifikasi oleh administrator Pusat Identitas IAM dari akun manajemen. Administrator yang didelegasikan tidak dapat mengubah kumpulan izin yang disediakan di akun manajemen.
- Tetapkan pengguna saja (bukan grup) ke kumpulan izin di akun manajemen — Karena akun manajemen memiliki hak istimewa khusus, Anda harus berhati-hati saat menetapkan akses ke akun ini di konsol atau AWS Command Line Interface (CLI). Jika Anda menetapkan grup ke kumpulan izin dengan akses ke akun manajemen, siapa pun yang memiliki izin untuk mengubah keanggotaan dalam grup tersebut dapat add/remove menggunakan grup to/from tersebut, dan dengan demikian memengaruhi siapa yang memiliki akses ke akun manajemen. Ini adalah admin grup apa pun yang memiliki kontrol atas sumber identitas Anda, termasuk administrator penyedia identitas (IdP), administrator Layanan Domain Direktori Aktif (AD DS) Microsoft, atau administrator Pusat Identitas IAM. Oleh karena itu, Anda harus menetapkan pengguna secara langsung ke kumpulan izin yang memberikan akses di akun manajemen, dan menghindari grup. Jika Anda menggunakan grup untuk mengelola akses ke akun manajemen, pastikan bahwa kontrol yang tepat ada di IdP untuk membatasi siapa yang memiliki kemampuan untuk memodifikasi grup tersebut, dan memastikan bahwa perubahan pada grup tersebut (atau perubahan kredensial untuk pengguna di akun manajemen) dicatat dan ditinjau seperlunya.
- Pertimbangkan lokasi Direktori Aktif Anda — Jika Anda berencana menggunakan Active Directory sebagai sumber identitas Pusat Identitas IAM, cari direktori di akun anggota tempat Anda mengaktifkan fitur administrator yang didelegasikan IAM Identity Center. Jika Anda memutuskan untuk mengubah sumber identitas Pusat Identitas IAM dari sumber lain ke Active Directory, atau mengubahnya dari Active Directory ke sumber lain, direktori harus berada di akun anggota administrator yang didelegasikan IAM Identity Center. Jika Anda ingin Direktori Aktif Anda berada di akun manajemen, Anda harus melakukan pengaturan di akun manajemen karena administrator yang didelegasikan tidak akan memiliki izin yang diperlukan untuk menyelesaikannya.

Batasi tindakan penyimpanan identitas Pusat Identitas IAM di akun administrasi yang didelegasikan dengan sumber identitas eksternal

Jika Anda menggunakan sumber identitas eksternal seperti IdP atau Directory Service, Anda harus menerapkan kebijakan yang membatasi tindakan penyimpanan identitas yang dapat diambil oleh admin Pusat Identitas IAM dari dalam akun administrasi yang didelegasikan. Operasi menulis dan

menghapus harus dipertimbangkan dengan cermat. Umumnya, sumber identitas eksternal adalah sumber kebenaran bagi pengguna dan atribut mereka, dan untuk keanggotaan grup. Jika Anda memodifikasi ini menggunakan API penyimpanan identitas atau konsol, perubahan Anda akan diganti selama siklus sinkronisasi normal. Yang terbaik adalah menyerahkan operasi ini ke kendali eksklusif sumber kebenaran identitas Anda. Ini juga mencegah administrator Pusat Identitas IAM memodifikasi keanggotaan grup untuk memberikan akses ke kumpulan izin atau aplikasi yang ditetapkan grup, daripada menyerahkan kontrol keanggotaan grup kepada admin IdP Anda. Anda juga harus menjaga siapa yang dapat membuat token pembawa SCIM dari akun administrasi yang didelegasikan, karena ini dapat memungkinkan admin akun anggota untuk memodifikasi grup dan pengguna melalui klien SCIM.

Mungkin ada kalanya operasi tulis atau hapus sesuai dari akun admin yang didelegasikan. Misalnya, Anda dapat membuat grup tanpa menambahkan anggota, lalu membuat tugas ke kumpulan izin tanpa harus menunggu admin IdP membuat grup. Tidak ada yang akan memiliki akses ke tugas itu sampai admin IdP menyediakan grup dan proses sinkronisasi IdP menetapkan anggota grup. Mungkin juga tepat untuk menghapus pengguna atau grup untuk mencegah masuk atau otorisasi selama waktu ketika Anda tidak dapat menunggu proses sinkronisasi IdP untuk menghapus akses oleh pengguna atau grup. Namun, penyalahgunaan izin ini dapat mengganggu pengguna. Anda harus menggunakan prinsip hak istimewa terkecil saat menetapkan izin penyimpanan identitas. Anda dapat mengontrol tindakan penyimpanan identitas mana yang diizinkan oleh admin akun administrasi yang didelegasikan menggunakan kebijakan kontrol layanan (SCP).

Contoh SCP di bawah ini mencegah penugasan pengguna ke grup melalui Identity Store API dan Konsol Manajemen AWS, yang direkomendasikan ketika sumber identitas Anda eksternal. Ini tidak mempengaruhi sinkronisasi pengguna dari Directory Service atau dari IdP eksternal (melalui SCIM).

Note

Ada kemungkinan bahwa, meskipun Anda menggunakan sumber identitas eksternal, organisasi Anda bergantung, sepenuhnya atau sebagian, pada API Identity Store untuk penyediaan pengguna dan grup. Oleh karena itu, sebelum mengaktifkan SCP ini, Anda harus mengonfirmasi bahwa proses penyediaan pengguna Anda tidak menggunakan operasi API Identity Store ini. Juga, lihat bagian berikutnya untuk informasi tentang cara membatasi pengelolaan keanggotaan grup untuk grup tertentu.

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

```

"Statement": [
  { "Effect": "Deny",
    "Action": ["identitystore:CreateGroupMembership"],
    "Resource": [ "*" ] }
]
}

```

Jika Anda ingin mencegah penambahan pengguna hanya ke grup yang memberikan akses ke akun manajemen, Anda dapat mereferensikan grup tertentu menggunakan grup ARN dalam format berikut: `arn:${Partition}:identitystore:::group/${GroupId}`. Jenis sumber daya ini dan jenis sumber daya lainnya yang tersedia di Identity Store didokumentasikan dalam [tipe Resource yang ditentukan oleh AWS Identity Store](#) di Referensi Otorisasi Layanan. Anda juga dapat mempertimbangkan untuk menyertakan API Identity Store tambahan di SCP. Untuk informasi selengkapnya, lihat [Tindakan](#) di Referensi API Identity Store.

Dengan menambahkan pernyataan kebijakan berikut ke SCP Anda, Anda dapat mencegah pembuatan token pembawa SCIM oleh admin yang didelegasikan. Anda dapat menerapkan ini untuk kedua sumber identitas eksternal.

Note

Jika admin yang didelegasikan perlu mengatur penyediaan pengguna dengan SCIM, atau melakukan rotasi token pembawa SCIM secara berkala, Anda harus mengizinkan sementara akses ke API ini agar admin yang didelegasikan menyelesaikan tugas-tugas tersebut.

```

{ "Effect": "Deny",
  "Action": ["sso-directory:CreateBearerToken"],
  "Resource": [ "*" ]
}

```

Batasi tindakan penyimpanan identitas Pusat Identitas IAM di akun administrasi yang didelegasikan untuk pengguna yang dikelola secara lokal

Jika Anda membuat pengguna dan grup secara langsung di Pusat Identitas IAM, bukan menggunakan IdP eksternal atau Directory Service, Anda harus mengambil tindakan pencegahan untuk siapa yang dapat membuat pengguna, mengatur ulang kata sandi, dan mengontrol keanggotaan grup. Tindakan ini memberi administrator kekuatan besar untuk siapa yang dapat

masuk dan siapa yang dapat memperoleh akses melalui keanggotaan dalam grup. Kebijakan ini paling baik diterapkan sebagai kebijakan in-line dalam kumpulan izin yang Anda gunakan untuk administrator Pusat Identitas IAM Anda, bukan sebagai SCP. Contoh kebijakan inline berikut memiliki dua tujuan. Pertama, mencegah penambahan pengguna ke grup tertentu. Anda dapat menggunakan ini untuk mencegah admin yang didelegasikan menambahkan pengguna ke grup yang memberikan akses ke akun manajemen. Kedua, mencegah penerbitan token pembawa SCIM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    { "Effect": "Deny",
      "Action": ["identitystore:CreateGroupMembership"],
      "Resource": [ arn:${Partition}:identitystore:::group/${GroupId1},
                    arn:${Partition}:identitystore:::group/${GroupId2}
                  ]
    },
    { "Effect": "Deny",
      "Action": ["sso-directory:CreateBearerToken"],
      "Resource": [ "*" ] }
  ]
}
```

Pisahkan manajemen konfigurasi Pusat Identitas IAM dari manajemen PermissionSet

Pisahkan tugas administratif termasuk modifikasi sumber identitas eksternal, manajemen token SCIM, konfigurasi batas waktu sesi dari tugas untuk membuat, memodifikasi, dan menetapkan kumpulan izin dengan membuat kumpulan izin admin yang berbeda dari akun manajemen Anda.

Batas penerbitan token pembawa SCIM

Token pembawa SCIM memungkinkan sumber identitas eksternal untuk menyediakan pengguna, grup, dan keanggotaan grup melalui protokol SCIM ketika sumber identitas Pusat Identitas IAM Anda adalah IdP eksternal seperti Okta atau ID Entra. Anda dapat mengatur SCP berikut untuk mencegah pembuatan token pembawa SCIM oleh administrator yang didelegasikan. Jika administrator yang didelegasikan perlu mengatur penyediaan pengguna dengan SCIM, atau melakukan rotasi token pembawa SCIM secara berkala, Anda harus mengizinkan sementara akses ke API ini untuk memungkinkan administrator yang didelegasikan menyelesaikan tugas-tugas tersebut.

```
{ "Effect": "Deny",  
  "Action": ["sso-directory:CreateBearerToken"],  
  "Resource": [ "*" ]  
}
```

Gunakan tag set izin dan daftar akun untuk mendelegasikan administrasi akun tertentu

Anda dapat membuat kumpulan izin yang Anda tetapkan ke administrator Pusat Identitas IAM untuk mendelegasikan siapa yang dapat membuat kumpulan izin, dan siapa yang dapat menetapkan kumpulan izin mana di akun mana. Hal ini dilakukan dengan menandai kumpulan izin dan menggunakan kondisi kebijakan dalam kumpulan izin yang Anda tetapkan ke administrator. Misalnya, Anda dapat membuat kumpulan izin yang memungkinkan pengguna membuat kumpulan izin asalkan diberi tag dengan cara tertentu. Anda juga dapat membuat kebijakan yang memungkinkan administrator untuk menetapkan kumpulan izin yang memiliki tag tertentu di akun tertentu. Ini dapat membantu Anda mendelegasikan manajemen atas akun tanpa memberikan administrator hak istimewa untuk mengubah akses dan hak istimewa mereka atas akun administrasi yang didelegasikan. Misalnya, dengan memberi tag pada kumpulan izin yang Anda gunakan hanya di akun administrasi yang didelegasikan, Anda dapat menentukan kebijakan yang hanya memberi orang tertentu izin untuk mengubah kumpulan izin dan penugasan yang memengaruhi akun administrasi yang didelegasikan. Anda juga dapat memberikan izin kepada orang lain untuk mengelola daftar akun di luar akun administrasi yang didelegasikan. Untuk mempelajari selengkapnya, lihat [Mendelegasikan manajemen kumpulan izin dan penetapan akun AWS IAM Identity Center](#) di Blog AWS Keamanan.

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 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, akun tersebut disebut sebagai akun administrator yang di delegasikan. Untuk mempelajari lebih lanjut tentang tugas yang dapat dilakukan oleh akun administrator yang didelegasikan, lihat [Akun AWS tipe](#).

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 kredensial 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 kumpulan 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 Konsol Manajemen AWS menggunakan kredensial akun manajemen Anda AWS Organizations. Kredensial akun manajemen diperlukan untuk menjalankan [RegisterDelegatedAdministrator](#) API.
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 Daftar administrator yang didelegasikan, pilih Akun AWS yang ingin Anda daftarkan, lalu pilih Daftar akun.

Menghapus pendaftaran akun anggota

Anda hanya dapat membatalkan pendaftaran akun anggota saat masuk dengan kredensial 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 bagi semua pengguna admin untuk mengelola Pusat Identitas IAM dari akun tersebut. 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 penugasan 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 AWS akses.

Untuk membatalkan pendaftaran akun anggota

1. Masuk ke Konsol Manajemen AWS menggunakan kredensial akun manajemen Anda AWS Organizations. Kredensial akun manajemen diperlukan untuk menjalankan [DeregisterDelegatedAdministrator](#) API.
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 Batalkan pendaftaran akun.
5. Di kotak dialog Batalkan pendaftaran akun, tinjau implikasi keamanan, lalu masukkan nama akun anggota untuk mengonfirmasi bahwa Anda memahami.
6. Pilih Batalkan pendaftaran akun.

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 Pusat Identitas IAM.

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 sementara yang ditinggikan untuk Akun AWS

Semua akses ke Akun AWS melibatkan beberapa tingkat hak istimewa. Operasi sensitif, seperti mengubah konfigurasi untuk lingkungan produksi, memerlukan perlakuan khusus karena ruang lingkup dan dampak potensial. Akses peningkatan sementara (juga dikenal sebagai akses just-in-time) adalah cara untuk meminta, menyetujui, dan melacak penggunaan izin untuk melakukan tugas tertentu selama waktu tertentu. Akses peningkatan sementara melengkapi bentuk kontrol akses lainnya, seperti set izin dan otentikasi multi-faktor.

Note

Untuk memastikan kelangsungan bisnis, kami sarankan [Anda mengatur akses darurat ke Konsol Manajemen AWS](#).

Untuk memenuhi berbagai kebutuhan pelanggan, AWS IAM Identity Center terintegrasi dengan solusi dari mitra Kompetensi AWS Keamanan. AWS memvalidasi bahwa solusi ini menangani serangkaian persyaratan akses sementara yang ditinggikan secara umum. Kami menyarankan Anda meninjau setiap solusi mitra dengan hati-hati sehingga Anda dapat memilih salah satu yang paling sesuai dengan kebutuhan dan preferensi unik Anda, termasuk bisnis Anda, arsitektur lingkungan cloud Anda, dan anggaran Anda.

Solusi yang divalidasi termasuk Platform [Manajemen Akses Apono](#), [CyberArk Akses Cloud Aman](#), Per [mintaan Akses Okta](#), dan [Tenable](#) (sebelumnya Ermetic).

Mitra dapat menominasikan solusi menggunakan aplikasi Kompetensi AWS Keamanan di Pusat Mitra. Untuk informasi selengkapnya, lihat Mit [AWS ra Kompetensi Keamanan](#).

Note

Jika Anda menggunakan Layanan Amazon Elastic Kubernetes berbasis sumber daya atau AWS Key Management Service, lihat [Referensi kumpulan izin di kebijakan sumber daya, peta konfigurasi Cluster Amazon EKS, dan kebijakan AWS KMS utama](#) sebelum Anda memilih solusi tepat waktu.

Akses masuk tunggal ke Akun AWS

Anda dapat menetapkan izin pengguna di direktori yang terhubung 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 administrator database izin luas ke Amazon RDS di akun pengembangan tetapi membatasi izin mereka di akun produksi. Pusat Identitas IAM mengonfigurasi Akun AWS semua izin pengguna yang diperlukan secara otomatis.

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 memiliki [IAMFullAccess](#) kebijakan atau izin yang setara sebelum Anda dapat mengaturnya. Pembatasan keamanan tambahan ini tidak diperlukan untuk akun anggota mana pun di AWS organisasi Anda.

Topik

- [Menetapkan akses pengguna atau grup ke Akun AWS](#)
- [Menghapus akses pengguna dan grup ke Akun AWS](#)
- [Cabut akses pengguna](#)
- [Mendelegasikan siapa yang dapat menetapkan akses masuk tunggal ke pengguna dan grup di akun manajemen](#)

Menetapkan akses pengguna atau grup ke Akun AWS

Gunakan prosedur berikut untuk menetapkan akses masuk tunggal ke pengguna dan grup di direktori yang terhubung dan gunakan kumpulan izin untuk menentukan tingkat akses mereka.

Untuk memeriksa akses pengguna dan grup yang ada, lihat [Melihat dan mengubah kumpulan izin](#).

Note

Untuk menyederhanakan administrasi izin akses, kami menyarankan Anda menetapkan akses langsung ke grup daripada pengguna individual. Dengan grup, Anda dapat memberikan atau menolak izin ke grup pengguna daripada harus menerapkan izin tersebut ke setiap individu. Jika pengguna pindah ke organisasi yang berbeda, 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 Identi](#) tas IAM.

Note

Pastikan konsol Pusat Identitas IAM menggunakan Wilayah tempat AWS Managed Microsoft AD direktori Anda berada sebelum Anda pindah ke langkah berikutnya.

2. Di panel navigasi, di bawah Multi-account izin, pilih Akun AWS.
3. Pada Akun AWS halaman, daftar tampilan pohon organisasi Anda ditampilkan. Pilih kotak centang di sebelah yang Akun AWS ingin Anda tetapkan akses. Jika Anda menyiapkan akses administratif untuk Pusat Identitas IAM, pilih kotak centang di sebelah akun manajemen.

 Note

Anda dapat memilih hingga 10 Akun AWS sekaligus per kumpulan izin saat 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 pengguna, grup, dan kumpulan 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 memberikan 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 diberikan 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 kumpulan izin, pada halaman Tetapkan kumpulan izin ke *AWS-account-name* "", lakukan hal berikut:
 1. Pilih satu atau lebih kumpulan izin. Jika diperlukan, Anda dapat membuat dan memilih kumpulan izin baru.
 - Untuk memilih satu atau beberapa kumpulan izin yang ada, di bawah Kumpulan izin, pilih kumpulan izin yang ingin Anda terapkan ke pengguna dan grup yang Anda pilih pada langkah sebelumnya.
 - Untuk membuat satu atau lebih kumpulan izin baru, pilih Buat kumpulan izin, dan ikuti langkah-langkah di [Membuat kumpulan izin](#). Setelah Anda membuat kumpulan izin yang ingin Anda terapkan, di konsol Pusat Identitas IAM, kembali ke Akun AWS dan ikuti instruksi hingga Anda mencapai Langkah 2: Pilih kumpulan izin. Ketika Anda mencapai langkah ini, pilih kumpulan izin baru yang Anda buat, dan lanjutkan ke langkah berikutnya dalam prosedur ini.

2. Setelah Anda mengonfirmasi bahwa kumpulan izin yang benar dipilih, pilih Berikutnya.
7. Untuk Langkah 3: Tinjau dan Kirim, pada halaman Tinjau dan kirim tugas ke **AWS-account-name**, lakukan hal berikut:
 1. Tinjau pengguna, grup, dan kumpulan izin yang dipilih.
 2. Setelah Anda mengonfirmasi bahwa pengguna, grup, dan kumpulan izin yang benar dipilih, pilih Kirim.

Pertimbangan-pertimbangan

- Proses penugasan pengguna dan grup mungkin membutuhkan waktu beberapa menit untuk diselesaikan. Biarkan halaman ini terbuka sampai proses berhasil selesai.

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 memiliki [IAMFullAccess](#) kebijakan atau izin yang setara sebelum Anda dapat mengaturnya. Pembatasan keamanan tambahan ini tidak diperlukan untuk akun anggota mana pun di AWS organisasi Anda.

8. Jika salah satu dari berikut ini berlaku, ikuti langkah-langkah [Meminta pengguna untuk MFA](#) untuk mengaktifkan MFA untuk Pusat Identitas IAM:
 - Anda menggunakan direktori Identity Center 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 MFA dengan AWS Directory Service

Note

Jika Anda menggunakan penyedia identitas eksternal, perhatikan bahwa IdP eksternal, bukan Pusat Identitas IAM, mengelola setelan MFA. MFA di Pusat Identitas IAM tidak didukung untuk digunakan oleh eksternal. IdPs

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

Atau, Anda dapat menggunakan [AWS CloudFormation](#) untuk membuat dan menetapkan kumpulan izin dan menetapkan pengguna ke kumpulan izin tersebut. Pengguna kemudian dapat [masuk ke portal AWS akses](#) atau menggunakan [perintah](#) AWS Command Line Interface (AWS CLI).

Note

Topik ini mencakup penetapan akses menggunakan kumpulan izin. Untuk menetapkan peran IAM yang ada kepada pengguna dan grup Pusat Identitas IAM — dengan set fitur peran IAM lengkap — lihat manajer akses [akun](#) di Panduan Pengguna IAM.

Menghapus akses pengguna dan grup ke Akun AWS

Gunakan prosedur ini untuk menghapus akses masuk tunggal Akun AWS untuk satu atau lebih pengguna dan grup di direktori terhubung Anda. Atau, Anda dapat menggunakan [delete-](#) AWS CLI account-.

Note

Bila Anda perlu menghentikan penyediaan pengguna atau grup Pusat Identitas IAM, Anda harus terlebih [dahulu menghapus penetapan kumpulan izin](#) dari pengguna dan grup sebelum menghapus pengguna dan grup.

Untuk menghapus akses pengguna dan grup ke Akun AWS

1. Buka konsol [Pusat Identitas](#) IAM.
2. Di panel navigasi, di bawah Multi-account izin, pilih Akun AWS.
3. Pada Akun AWS halaman, daftar tampilan pohon organisasi Anda muncul. Pilih nama Akun AWS yang berisi pengguna dan grup yang ingin Anda hapus akses masuk tunggal.
4. Pada halaman Ikhtisar untuk Akun AWS, di bawah Pengguna dan grup yang ditugaskan, pilih nama satu atau lebih pengguna atau grup, lalu pilih Hapus akses.
5. Di kotak dialog Hapus akses, konfirmasi bahwa nama pengguna atau grup sudah benar, lalu pilih Hapus akses.

Cabut akses pengguna

Berikut ini adalah prosedur umum untuk mencabut sesi set izin aktif untuk pengguna Pusat Identitas IAM. Prosedur ini mengasumsikan bahwa Anda ingin menghapus semua akses untuk pengguna yang telah mengkompromikan kredensial atau untuk aktor jahat yang ada di sistem. Prasyaratnya adalah mengikuti panduan di [Bersiaplah untuk mencabut sesi peran IAM aktif yang dibuat oleh kumpulan izin](#). Kami berasumsi bahwa kebijakan tolak semua hadir dalam kebijakan kontrol layanan (SCP).

Note

AWS merekomendasikan Anda membangun otomatisasi untuk menangani semua langkah kecuali operasi konsol saja.

1. Dapatkan ID pengguna dari orang yang aksesnya harus Anda cabut. Anda dapat menggunakan API penyimpanan identitas untuk menemukan pengguna berdasarkan nama pengguna mereka.
2. Perbarui kebijakan Tolak untuk menambahkan ID pengguna dari langkah 1 dalam kebijakan kontrol layanan (SCP) Anda. Setelah menyelesaikan langkah ini, pengguna target kehilangan akses dan tidak dapat mengambil tindakan dengan peran apa pun yang dipengaruhi kebijakan.
3. Hapus semua penetapan kumpulan izin untuk pengguna. Jika akses ditetapkan melalui keanggotaan grup, hapus pengguna dari semua grup dan semua penetapan kumpulan izin langsung. Langkah ini mencegah pengguna mengambil peran IAM tambahan. Jika pengguna memiliki sesi portal AWS akses aktif dan Anda menonaktifkan pengguna, mereka dapat terus mengambil peran baru sampai Anda menghapus akses mereka.
4. Hapus semua penetapan peran IAM untuk pengguna di pengelola akses akun. Jika akses ditetapkan melalui keanggotaan grup, hapus pengguna dari semua grup dan semua penetapan peran IAM langsung. Langkah ini mencegah pengguna mengambil peran IAM tambahan yang dikelola di manajer akses akun. Jika pengguna memiliki sesi portal akses AWS akun aktif dan Anda menonaktifkan pengguna, mereka dapat terus mengambil peran baru sampai Anda menghapus akses mereka.
5. Jika Anda menggunakan penyedia identitas (IdP) atau Microsoft Active Directory sebagai sumber identitas, nonaktifkan pengguna di sumber identitas. Menonaktifkan pengguna mencegah pembuatan sesi portal AWS akses tambahan. Gunakan dokumentasi IdP atau Microsoft Active Directory API untuk mempelajari cara mengotomatiskan langkah ini. Jika Anda menggunakan

direktori Pusat Identitas IAM sebagai sumber identitas, jangan nonaktifkan akses pengguna. Anda akan menonaktifkan akses pengguna di langkah 7.

6. Di konsol Pusat Identitas IAM, temukan pengguna dan hapus sesi aktif mereka.
 - a. Pilih Pengguna.
 - b. Pilih pengguna yang sesi aktifnya ingin Anda hapus.
 - c. Pada halaman detail pengguna, pilih tab Sesi aktif.
 - d. Pilih kotak centang di samping sesi yang ingin Anda hapus dan pilih Hapus sesi.

Setelah menghapus sesi pengguna, pengguna akan segera kehilangan akses ke portal AWS akses. Pelajari tentang durasi [sesi](#).

7. Di konsol Pusat Identitas IAM, nonaktifkan akses pengguna.
 - a. Pilih Pengguna.
 - b. Pilih pengguna yang aksesnya ingin Anda nonaktifkan.
 - c. Pada halaman detail pengguna, perluas Informasi umum dan pilih tombol Nonaktifkan akses pengguna untuk mencegah login lebih lanjut dari pengguna.
8. Biarkan kebijakan Tolak berlaku setidaknya selama 12 jam. Jika tidak, pengguna dengan sesi peran IAM aktif akan memulihkan tindakan dengan peran IAM. Jika Anda menunggu 12 jam, sesi aktif akan berakhir dan pengguna tidak akan dapat mengakses peran IAM lagi.

 Important

Jika Anda menonaktifkan akses pengguna sebelum menghentikan sesi pengguna (Anda menyelesaikan langkah 7 tanpa menyelesaikan langkah 6), Anda tidak dapat lagi menghentikan sesi pengguna melalui konsol Pusat Identitas IAM. Jika Anda secara tidak sengaja menonaktifkan akses pengguna sebelum menghentikan sesi pengguna, Anda dapat mengaktifkan kembali pengguna, menghentikan sesi mereka, dan kemudian menonaktifkan akses mereka lagi.

Anda sekarang dapat mengubah kredensial pengguna jika kata sandi mereka dikompromikan dan [memulihkan tugas mereka](#).

Mendelegasikan 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 satu Pengguna root akun AWS atau pengguna yang memiliki kebijakan AWSSSOMasterAccountAdministrator dan terkel IAMFullAccess AWS ola yang dilampirkan, yang dapat menetapkan akses masuk tunggal ke akun manajemen. IAMFullAccessKebijakan AWSSSOMasterAccountAdministrator dan mengelola akses masuk tunggal ke akun manajemen dalam AWS Organizations organisasi.

Atau, Anda dapat menggunakan AWS CLI untuk membuat, melampirkan kebijakan ke, dan menetapkan kumpulan izin. Berikut ini mencantumkan perintah untuk setiap langkah:

- Untuk membuat kumpulan izin: [create-permission-set](#)
- Untuk melampirkan AWS Managed Policy ke kumpulan izin: lampirkan-managed-policy-to-permission [-set](#)
- Untuk melampirkan kebijakan yang dikelola pelanggan ke kumpulan izin: lampirkan-customer-managed-policy-to-permission [-set](#)
- Untuk menetapkan kumpulan izin ke prinsipal: [create-account-](#)

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 [Membuat kumpulan izin](#) untuk membuat kumpulan izin, lalu lakukan hal berikut:
 1. Pada halaman Buat kumpulan izin baru, pilih kotak centang Buat kumpulan izin khusus, lalu pilih Berikutnya: Detail.
 2. Pada halaman Buat kumpulan izin baru, tentukan nama untuk kumpulan izin kustom dan secara opsional, deskripsi. Jika diperlukan, ubah durasi sesi dan tentukan URL status relai.

 Note

Untuk URL status relay, Anda harus menentukan URL yang ada di Konsol Manajemen AWS. Contoh:

`https://console.aws.amazon.com/ec2/`

Untuk informasi selengkapnya, lihat [Atur status relai untuk akses cepat ke Konsol Manajemen AWS](#).

3. Di bawah Kebijakan apa yang ingin Anda sertakan dalam kumpulan izin Anda? , pilih kotak centang Lamp AWS irkan kebijakan terkelola.
 4. Dalam daftar kebijakan IAM, pilih AWSS SOMasterAccountAdministrator dan kebijakan terkel IAMFullAccess AWS ola. Kebijakan ini memberikan izin kepada pengguna dan grup mana pun yang diberi akses ke kumpulan izin ini di masa mendatang.
 5. Pilih Berikutnya: Tanda.
 6. Di bawah Tambah tag (opsional), tentukan nilai untuk K unci dan Nilai (opsional), lalu pilih Berikutnya: Review. Untuk informasi selengkapnya tentang tag, lihat [Sumber daya penandaan AWS IAM Identity Center](#).
 7. Tinjau pilihan yang Anda buat, lalu pilih Buat.
3. Ikuti langkah-langkah [Menetapkan akses pengguna atau grup ke Akun AWS](#) untuk menetapkan pengguna dan grup yang sesuai ke kumpulan izin yang baru saja Anda buat.
 4. Komunikasikan hal berikut kepada pengguna yang ditugaskan: 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.

Kelola Akun AWS dengan set izin

Kumpulan izin adalah template yang Anda buat dan pelihara yang mendefinisikan kumpulan dari satu atau beberapa kebijakan https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html IAM. Kumpulan izin menyederhanakan penetapan Akun AWS akses untuk pengguna dan grup di organisasi Anda. Misalnya, Anda dapat membuat kumpulan izin Admin Database yang mencakup kebijakan untuk mengelola layanan AWS RDS, DynamoDB, dan Aurora, dan menggunakan kumpulan izin tunggal tersebut untuk memberikan akses ke daftar target Akun AWS dalam [AWS Organisasi](#) untuk administrator database Anda.

 Note

Instans organisasi Anda harus mengaktifkan izin multi-akun agar kumpulan izin berfungsi. Secara default, saat Anda membuat instance organisasi, izin multi-akun diaktifkan. Jika sebelumnya tidak diaktifkan, gunakan tab Manajemen pada halaman Pengaturan untuk mengaktifkan izin multi-akun sehingga Anda dapat membuat kumpulan izin. Anda juga dapat menggunakan [UpdateInstance](#) API untuk mengaktifkan izin multi-akun.

Pusat Identitas IAM menetapkan akses ke pengguna atau grup dalam satu atau lebih Akun AWS dengan kumpulan izin. Saat Anda menetapkan kumpulan izin, Pusat Identitas IAM membuat peran IAM Identity Center-controlled IAM yang sesuai di setiap akun, dan melampirkan kebijakan yang ditentukan dalam kumpulan izin ke peran tersebut. Pusat Identitas IAM mengelola peran, dan mengizinkan pengguna resmi yang telah Anda tetapkan untuk mengambil peran tersebut, dengan menggunakan Portal Pengguna Pusat Identitas IAM atau AWS CLI. Saat Anda memodifikasi kumpulan izin, Pusat Identitas IAM memastikan bahwa kebijakan dan peran IAM yang sesuai diperbarui sesuai.

Anda dapat menambahkan kebijakan [AWS terkelola](#), kebijakan [yang dikelola pelanggan](#), [kebijakan sebaris](#), dan kebijakan terkel [AWS ola untuk fungsi pekerjaan](#) ke kumpulan izin Anda. Anda juga dapat menetapkan kebijakan AWS terkelola atau kebijakan yang dikelola pelanggan sebagai batas [izin](#).

Untuk membuat kumpulan izin, lihat [Membuat, mengelola, dan menghapus set izin](#).

Jika manajemen akses Anda memerlukan kemampuan di luar apa yang ditawarkan kumpulan izin — seperti kebijakan kepercayaan khusus, tag peran, atau jalur peran yang dapat dikonfigurasi — Anda dapat menggunakan manajer akses [akun](#) di IAM. Manajer akses akun memungkinkan Anda menetapkan peran IAM yang ada untuk pengguna dan grup Pusat Identitas IAM. Anda dapat menggunakannya secara independen atau bersama-sama dengan kumpulan izin untuk mendapatkan akses ke set fitur peran IAM lengkap.

Membuat kumpulan izin yang menerapkan izin hak istimewa terkecil

Untuk mengikuti praktik terbaik menerapkan izin hak istimewa terkecil, setelah Anda membuat kumpulan izin administratif, Anda membuat kumpulan izin yang lebih ketat dan menetapkan ke satu atau lebih pengguna. Kumpulan 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 terkel AWS ola. Setelah mempelajari izin mana yang digunakan, 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 untuk 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 Anda membuat pengguna administratif di Pusat Identitas IAM, Anda dapat membuat kumpulan izin baru yang memberikan `PowerUserAccess` izin, lalu menetapkan kumpulan izin tersebut kepada diri Anda sendiri. Tidak seperti kumpulan izin administratif, yang menggunakan `AdministratorAccess` izin, kum `PowerUserAccess` pulan izin tidak mengizinkan pengelolaan pengguna dan grup IAM. Saat Anda masuk ke portal AWS akses untuk mengakses AWS akun Anda, Anda dapat memilih `PowerUserAccess` daripada `AdministratorAccess` melakukan tugas pengembangan di akun.

Perhatikan sejumlah pertimbangan berikut:

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

Dengan kumpulan izin yang telah ditentukan sebelumnya, yang menggunakan izin yang telah [ditentukan sebelumnya](#), Anda memilih AWS satu kebijakan 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 ter [AWS kelola untuk fungsi pekerjaan](#).

- Anda dapat mengonfigurasi durasi sesi untuk kumpulan izin untuk mengontrol lamanya waktu pengguna masuk ke Akun AWS.

Ketika pengguna bergabung ke dalam Akun AWS dan menggunakan Konsol AWS Manajemen atau Antarmuka Baris Per AWSintah (AWS CLI), Pusat Identitas IAM menggunakan pengaturan durasi sesi pada set izin untuk mengontrol durasi sesi. Secara default, nilai untuk durasi sesi, yang menentukan lamanya waktu pengguna dapat masuk ke 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 untuk Akun AWS](#).

- Anda juga dapat mengonfigurasi durasi sesi portal AWS akses untuk mengontrol lamanya waktu pengguna tenaga kerja masuk ke portal.

Secara default, nilai untuk Durasi sesi maksimum, yang menentukan lamanya waktu pengguna tenaga kerja dapat masuk ke portal AWS akses sebelum mereka harus melakukan autentikasi ulang, adalah delapan jam. Anda dapat menentukan nilai maksimum 90 hari. Untuk informasi selengkapnya, lihat [Mengkonfigurasi durasi sesi di Pusat Identitas IAM](#).

- Saat Anda masuk ke portal AWS akses, pilih peran yang memberikan izin hak istimewa terkecil.

Setiap kumpulan izin yang Anda buat dan tetapkan untuk pengguna Anda muncul sebagai peran yang tersedia di portal AWS akses. Saat Anda masuk ke portal sebagai pengguna tersebut, pilih peran yang sesuai dengan kumpulan 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 kumpulan izin yang ada atau baru untuk pengguna tersebut.

Untuk informasi, lihat, [Menetapkan akses pengguna atau grup ke Akun AWS](#).

Topik

- [Izin yang telah ditentukan sebelumnya untuk AWS kebijakan terkelola](#)
- [Izin khusus untuk AWS kebijakan yang dikelola dan dikelola pelanggan](#)
- [Membuat, mengelola, dan menghapus set izin](#)
- [Konfigurasi properti kumpulan izin](#)

Izin yang telah ditentukan sebelumnya untuk AWS kebijakan terkelola

Anda dapat membuat kumpulan izin yang telah ditentukan sebelumnya dengan kebijakan AWS terkelola.

Saat membuat kumpulan izin dengan izin yang telah ditentukan sebelumnya, Anda memilih satu kebijakan dari daftar kebijakan ter AWS kelola. Dalam kebijakan yang tersedia, Anda dapat memilih dari Kebijakan izin umum dan kebijakan fungsi pekerjaan.

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 pekerjaan

Pilih dari daftar kebijakan AWS terkelola yang memungkinkan untuk mengakses sumber daya di 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 [AWS kebijakan terkelola untuk fungsi pekerjaan](#) di panduan AWS Identity and Access Management pengguna.

Untuk petunjuk tentang cara membuat kumpulan izin, lihat [Membuat, mengelola, dan menghapus set izin](#).

Izin khusus untuk AWS kebijakan yang dikelola dan dikelola pelanggan

Anda dapat membuat kumpulan izin dengan izin khusus, menggabungkan kebijakan terkel AWS dan kebijakan yang dikelola pelanggan yang Anda miliki di AWS Identity and Access Management (IAM) bersama dengan kebijakan sebaris. Anda juga dapat menyertakan batas izin, menetapkan izin maksimum yang dapat diberikan kebijakan lain kepada pengguna kumpulan izin Anda.

Untuk petunjuk tentang cara membuat kumpulan izin, lihat [Membuat, mengelola, dan menghapus set izin](#).

Jenis kebijakan yang dapat Anda lampirkan ke kumpulan izin

Topik

- [Kebijakan inline](#)
- [AWS kebijakan terkelola](#)
- [Kebijakan yang dikelola pelanggan](#)
- [Batas izin](#)

Kebijakan inline

Anda dapat melampirkan kebijakan sebaris ke kumpulan izin. Kebijakan sebaris adalah blok teks yang diformat sebagai kebijakan IAM yang Anda tambahkan langsung ke kumpulan izin Anda. Anda dapat menempelkan kebijakan, atau membuat kebijakan baru dengan alat pembuatan kebijakan di konsol Pusat Identitas IAM saat Anda membuat kumpulan izin baru. Anda juga dapat membuat kebijakan IAM dengan [AWS Policy Generator](#).

Saat Anda menerapkan kumpulan izin dengan kebijakan sebaris, Pusat Identitas IAM membuat kebijakan IAM di Akun AWS tempat Anda menetapkan kumpulan izin. Pusat Identitas IAM membuat kebijakan saat Anda menetapkan kumpulan izin ke akun. Kebijakan tersebut kemudian dilampirkan ke peran IAM di Akun AWS yang diasumsikan pengguna Anda.

Saat Anda membuat kebijakan sebaris dan menetapkan kumpulan izin, Pusat Identitas IAM mengonfigurasi kebijakan di Akun AWS untuk Anda. Saat membuat kumpulan izin dengan [Kebijakan yang dikelola pelanggan](#), Anda harus membuat kebijakan di Akun AWS diri Anda sendiri sebelum menetapkan kumpulan izin.

AWS kebijakan terkelola

Anda dapat melampirkan kebijakan AWS terkelola ke kumpulan izin Anda. AWS kebijakan yang dikelola adalah kebijakan IAM yang diper AWS tahanan. Sebaliknya, apakah [Kebijakan yang dikelola pelanggan](#) kebijakan IAM di akun Anda yang Anda buat dan pertahankan. AWS kebijakan terkelola menangani kasus penggunaan hak istimewa paling sedikit yang umum di Akun AWS. Anda dapat menetapkan kebijakan AWS terkelola sebagai izin untuk peran yang dibuat Pusat Identitas IAM, atau sebagai batas https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html izin.

AWS memeli [AWS hara kebijakan terkelola untuk fungsi pekerjaan](#) yang menetapkan izin akses khusus pekerjaan ke sumber daya Anda AWS . Anda dapat menambahkan satu kebijakan fungsi pekerjaan saat memilih untuk menggunakan izin yang telah ditentukan sebelumnya dengan kumpulan izin Anda. Saat memilih Iz in khusus, Anda dapat menambahkan lebih dari satu kebijakan fungsi pekerjaan.

Anda Akun AWS juga berisi sejumlah besar kebijakan I AWS AM terkelola untuk spesifik Layanan AWS dan kombinasi Layanan AWS. Saat membuat kumpulan izin dengan izin khusus, Anda dapat memilih dari banyak kebijakan terkel AWS ola tambahan untuk ditetapkan ke kumpulan izin Anda.

AWS mengisi setiap Akun AWS dengan kebijakan terkel AWS ola. Untuk menerapkan kumpulan izin dengan AWS kebijakan terkelola, Anda tidak perlu membuat kebijakan terlebih dahulu di Akun AWS. Saat membuat kumpulan izin dengan [Kebijakan yang dikelola pelanggan](#), Anda harus membuat kebijakan di Akun AWS diri Anda sendiri sebelum menetapkan kumpulan izin.

Untuk informasi selengkapnya tentang AWS kebijakan terkelola, [AWS lihat kebijakan ter](#) kelola di Panduan Pengguna IAM.

Kebijakan yang dikelola pelanggan

Anda dapat melampirkan kebijakan yang dikelola pelanggan ke kumpulan izin Anda. Kebijakan yang dikelola pelanggan adalah kebijakan IAM di akun Anda yang Anda buat dan pelihara. Sebaliknya, apakah [AWS kebijakan terkelola](#) kebijakan IAM di akun Anda yang diper AWS tahankan. Anda dapat menetapkan kebijakan yang dikelola pelanggan sebagai izin untuk peran yang dibuat Pusat Identitas IAM, atau sebagai batas https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_boundaries.html izin.

Saat membuat kumpulan izin dengan kebijakan yang dikelola pelanggan, Anda harus membuat kebijakan IAM dengan nama dan jalur yang sama di setiap Akun AWS tempat IAM Identity Center menetapkan kumpulan izin Anda. Jika Anda menentukan jalur khusus, pastikan untuk menentukan jalur yang sama di masing-masing jalur Akun AWS. Untuk informasi selengkapnya, lihat [Nama dan jalur yang mudah diingat](#) dalam Panduan Pengguna IAM. Pusat Identitas IAM melampirkan kebijakan IAM ke peran IAM yang dibuat di Anda. Akun AWS Sebagai praktik terbaik, terapkan izin yang sama ke kebijakan di setiap akun tempat Anda menetapkan kumpulan izin. Untuk informasi selengkapnya, lihat [Menggunakan kebijakan IAM dalam kumpulan izin](#).

Note

Saat kebijakan yang dikelola pelanggan dilampirkan ke kumpulan izin, nama kebijakan tidak peka huruf besar/kecil.

Untuk informasi selengkapnya, lihat [Kebijakan yang dikelola pelanggan](#) di Panduan Pengguna IAM.

Batas izin

Anda dapat melampirkan batas izin ke kumpulan izin Anda. Batas izin adalah AWS kebijakan IAM yang dikelola atau dikelola pelanggan yang menetapkan izin maksimum yang dapat diberikan kebijakan berbasis identitas kepada prinsipal IAM. Saat Anda menerapkan batas izin, Anda, [Kebijakan inline](#)[Kebijakan yang dikelola pelanggan](#), dan [AWS kebijakan terkelola](#) tidak dapat memberikan izin apa pun yang melebihi izin yang diberikan batas izin Anda. Batas izin tidak memberikan izin apa pun, melainkan membuatnya sehingga IAM mengabaikan semua izin di luar batas.

Saat membuat kumpulan izin dengan kebijakan yang dikelola pelanggan sebagai batas izin, Anda harus membuat kebijakan IAM dengan nama yang sama di setiap Akun AWS tempat IAM Identity Center menetapkan kumpulan izin Anda. Pusat Identitas IAM melampirkan kebijakan IAM sebagai batas izin ke peran IAM yang dibuat di Anda. Akun AWS

Untuk informasi lebih lanjut, lihat [Batas izin untuk entitas IAM](#) dalam Panduan Pengguna IAM.

Membuat, mengelola, dan menghapus set izin

Kumpulan izin menentukan tingkat akses yang dimiliki pengguna dan grup ke Akun AWS. Kumpulan izin disimpan di Pusat Identitas IAM dan dapat disediakan untuk satu atau lebih. Akun AWS Anda dapat menetapkan lebih dari satu set izin untuk pengguna. Untuk informasi selengkapnya tentang kumpulan izin dan cara penggunaannya di Pusat Identitas IAM, lihat [Kelola Akun AWS dengan set izin](#).

Note

Anda dapat mencari dan mengurutkan kumpulan izin berdasarkan nama di konsol Pusat Identitas IAM.

Ingatlah pertimbangan berikut saat membuat kumpulan izin:

- Contoh organisasi

Untuk menggunakan kumpulan izin, Anda harus menggunakan instance Organisasi dari Pusat Identitas IAM. Untuk informasi selengkapnya, lihat [Instans organisasi dan akun dari Pusat Identitas IAM](#).

- Mulai dengan kumpulan izin yang telah ditentukan

Dengan kumpulan izin yang telah ditentukan sebelumnya, yang menggunakan izin yang telah [ditentukan sebelumnya](#), Anda memilih AWS satu kebijakan 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 ter [AWS kelola untuk fungsi pekerjaan](#). Setelah mengumpulkan data penggunaan, Anda dapat menyempurnakan kumpulan izin agar lebih ketat.

- Batasi durasi sesi manajemen untuk periode kerja yang wajar

Saat pengguna bergabung ke dalam Akun AWS dan menggunakan AWS Command Line Interface (AWS CLI), Pusat Identitas IAM menggunakan pengaturan durasi sesi pada kumpulan izin untuk mengontrol durasi sesi. Konsol Manajemen AWS Ketika sesi pengguna mencapai durasi sesi, mereka akan keluar dari konsol dan diminta untuk masuk lagi. Sebagai praktik terbaik keamanan, sebaiknya Anda tidak mengatur durasi sesi lebih lama dari yang diperlukan untuk melakukan peran. Secara default, nilai untuk durasi sesi adalah satu jam. Anda dapat menentukan nilai maksimum 12 jam. Untuk informasi selengkapnya, lihat [Tetapkan durasi sesi untuk Akun AWS](#).

- Batasi durasi sesi portal pengguna tenaga kerja

Pengguna tenaga kerja menggunakan sesi portal untuk memilih peran dan mengakses aplikasi. Secara default, nilai untuk Durasi sesi maksimum, yang menentukan lamanya waktu pengguna tenaga kerja dapat masuk ke portal AWS akses sebelum mereka harus melakukan autentikasi ulang, adalah delapan jam. Anda dapat menentukan nilai maksimum 90 hari. Untuk informasi selengkapnya, lihat [Mengkonfigurasi durasi sesi di Pusat Identitas IAM](#).

- Gunakan peran yang memberikan izin hak istimewa terkecil

Setiap kumpulan izin yang Anda buat dan tetapkan untuk pengguna Anda muncul sebagai peran yang tersedia di portal AWS akses. Saat Anda masuk ke portal sebagai pengguna tersebut, pilih peran yang sesuai dengan kumpulan izin paling ketat yang dapat Anda gunakan untuk melakukan tugas di akun, bukan AdministratorAccess. Uji kumpulan izin Anda untuk memverifikasi bahwa mereka menyediakan akses yang diperlukan sebelum mengirim undangan pengguna.

Note

Anda juga dapat menggunakan [AWS CloudFormation](#) untuk membuat dan menetapkan kumpulan izin dan menetapkan pengguna ke kumpulan izin tersebut.

Topik

- [Membuat kumpulan izin](#)
- [Melihat dan mengubah kumpulan izin](#)
- [Delegasikan administrasi kumpulan izin](#)
- [Menggunakan kebijakan IAM dalam kumpulan izin](#)
- [Menghapus kumpulan izin di Pusat Identitas IAM](#)
- [Menghapus kumpulan izin di Pusat Identitas IAM](#)

Membuat kumpulan izin

Gunakan prosedur ini untuk membuat kumpulan izin yang telah ditentukan sebelumnya yang menggunakan kebijakan terkel AWS ola tunggal, atau kumpulan izin khusus yang menggunakan hingga 10 kebijakan ter AWS kelola atau yang dikelola pelanggan dan kebijakan sebaris. Anda dapat meminta penyesuaian untuk jumlah maksimum 10 kebijakan di konsol Kuota [Layanan](#) untuk IAM. Anda dapat membuat kumpulan izin di konsol Pusat Identitas IAM.

Note

Untuk menggunakan kumpulan izin, Anda harus menggunakan instance Organisasi dari Pusat Identitas IAM. Untuk informasi selengkapnya, lihat [Instans organisasi dan akun dari Pusat Identitas IAM](#).

Untuk membuat kumpulan izin

1. Buka konsol [Pusat Identi](#) tas IAM.
2. Di bawah Multi-account izin, pilih Kumpulan izin.
3. Pilih Buat kumpulan izin.
4. Pada halaman Pilih jenis kumpulan izin, di bawah Jenis kumpulan izin, pilih jenis kumpulan izin.
5. Pilih satu atau beberapa kebijakan yang ingin Anda gunakan untuk kumpulan izin, berdasarkan jenis kumpulan izin:
 - Kumpulan izin yang telah ditentukan
 1. Di bawah Kebijakan untuk kumpulan izin yang telah ditentukan sebelumnya, pilih salah satu kebijakan fungsi Pekerjaan IAM atau Kebijakan izin umum dalam daftar, lalu

pilih Berikutnya. Untuk informasi selengkapnya, lihat [AWS kebijakan terkelola untuk fungsi pekerjaan AWS dan kebijakan terkelola](#) di Panduan AWS Identity and Access Management Pengguna.

2. Buka Langkah 6 untuk menyelesaikan halaman Detail Set Perizinan Tentukan.

- Kumpulan izin khusus

1. Pilih Berikutnya.

2. Pada halaman Tentukan kebijakan dan batas izin, pilih jenis kebijakan IAM yang ingin Anda terapkan ke kumpulan izin baru Anda. Secara default, Anda dapat menambahkan kombinasi hingga 10 kebijakan terkelola dan kebijakan yang AWS dikelola Pelanggan ke kumpulan izin Anda. Kuota ini ditetapkan oleh IAM. Untuk meningkatkannya, minta peningkatan kebijakan terkelola kuota IAM yang dilampirkan ke peran IAM di konsol Kuota Layanan di setiap Akun AWS tempat Anda ingin menetapkan kumpulan izin.

- Perluas AWS kebijakan 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 ke pengguna di kumpulan izin.

- b. Jika Anda ingin menambahkan jenis kebijakan lain, pilih wadahnya dan buat pilihan Anda. Pilih Berikutnya ketika Anda telah memilih semua kebijakan yang ingin Anda terapkan. Buka Langkah 6 untuk menyelesaikan halaman Detail Set Perizinan Tentukan.

- 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 Anda tambahkan ke kumpulan izin. Di setiap akun tempat Anda ingin menetapkan kumpulan 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 buat pilihan Anda. Pilih Berikutnya ketika Anda telah memilih semua kebijakan yang ingin Anda terapkan. Buka Langkah 6 untuk menyelesaikan halaman Detail Set Perizinan Tentukan.

- Perluas Kebijakan sebaris untuk menambahkan teks JSON-formatted kebijakan kustom. Kebijakan sebaris tidak sesuai dengan sumber daya IAM yang ada. Untuk membuat kebijakan sebaris, masukkan bahasa kebijakan khusus dalam formulir yang disediakan. Pusat Identitas IAM menambahkan kebijakan ke sumber daya IAM yang dibuat di akun anggota Anda. Untuk informasi selengkapnya, lihat [Kebijakan inline](#).
 - a. Tambahkan tindakan dan sumber daya yang Anda inginkan dalam editor interaktif ke kebijakan sebaris Anda. Pernyataan tambahan dapat ditambahkan dengan Tambahkan pernyataan baru.
 - b. Jika Anda ingin menambahkan jenis kebijakan lain, pilih wadahnya dan buat pilihan Anda. Pilih Berikutnya ketika Anda telah memilih semua kebijakan yang ingin Anda terapkan. Buka Langkah 6 untuk menyelesaikan halaman Detail Set Perizinan Tentukan.
- Perluas batas izin untuk menambahkan kebijakan IAM yang AWS dikelola atau dikelola pelanggan sebagai izin maksimum yang dapat ditetapkan oleh kebijakan lain dalam kumpulan izin. Untuk informasi selengkapnya, lihat [Batas izin](#).
 - a. Pilih Gunakan batas izin untuk mengontrol izin maksimum.
 - b. Pilih AWS kebijakan terkelola untuk menetapkan kebijakan dari IAM yang dibuat dan AWS dipelihara sebagai batas izin Anda. Pilih 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 buat pilihan Anda. Pilih Berikutnya ketika Anda telah memilih semua kebijakan yang ingin Anda terapkan. Buka Langkah 6 untuk menyelesaikan halaman Detail Set Perizinan Tentukan.

6. Pada halaman Tentukan detail kumpulan izin, lakukan hal berikut:

1. Di bawah Nama kumpulan izin, ketikkan nama untuk mengidentifikasi kumpulan izin ini di Pusat Identitas IAM. Nama yang Anda tentukan untuk kumpulan izin ini muncul di portal AWS akses sebagai peran yang tersedia. Pengguna masuk ke portal AWS akses, pilih Akun AWS, lalu pilih peran.

 Note

Nama kumpulan izin harus unik dalam instans Pusat Identitas IAM Anda.

2. (Opsional) Anda juga dapat mengetikkan 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 masuk sebelum konsol mengeluarkan mereka dari sesi mereka. Untuk informasi selengkapnya, lihat [Tetapkan durasi sesi untuk Akun AWS](#).
4. (Opsional) Tentukan nilai untuk status Relay. Nilai ini digunakan dalam proses federasi untuk mengarahkan pengguna di dalam akun. Untuk informasi selengkapnya, lihat [Atur status relay untuk akses cepat ke Konsol Manajemen AWS](#).

 Note

URL status relay harus berada di dalam Konsol Manajemen AWS. Contoh:

`https://console.aws.amazon.com/ec2/`

5. Perluas Tag (opsional), pilih Tambah tag, lalu tentukan nilai untuk K unci dan Nilai (opsional).

Untuk informasi tentang tanda, lihat [Sumber daya penandaan 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 kumpulan izin, kumpulan izin tidak disediakan (digunakan di mana pun Akun AWS). Untuk menyediakan kumpulan izin di sebuah Akun AWS, Anda harus menetapkan akses Pusat Identitas IAM ke pengguna dan grup di akun, lalu menerapkan kumpulan izin ke pengguna dan grup tersebut. Untuk informasi selengkapnya, lihat [Menetapkan akses pengguna atau grup ke Akun AWS](#).

Melihat dan mengubah kumpulan izin

Anda dapat menggunakan kumpulan izin untuk memberikan akses kepada pengguna Akun AWS. Anda dapat melihat dan mengubah kumpulan izin dengan AWS IAM Identity Center konsol. Anda dapat mencari dan mengurutkan kumpulan izin berdasarkan nama di konsol Pusat Identitas IAM. Untuk informasi selengkapnya tentang kumpulan izin dan cara penggunaannya di Pusat Identitas IAM, lihat [the section called “Kumpulan izin”](#).

Kumpulan izin tidak diperlukan untuk mengelola akses pengguna ke aplikasi.

 Note

Untuk menggunakan kumpulan izin, Anda harus menggunakan instance Organisasi dari Pusat Identitas IAM. Untuk informasi selengkapnya, lihat [Instans organisasi dan akun dari Pusat Identitas IAM](#).

Melihat penugasan kumpulan izin

Gunakan prosedur ini untuk melihat setelan izin yang diterapkan di AWS IAM Identity Center konsol.

All Akun AWS where a permission set is provisioned

Untuk melihat semua tugas untuk kumpulan izin, gunakan prosedur berikut:

1. Masuk ke Konsol Manajemen AWS dan buka AWS IAM Identity Center konsol di <https://console.aws.amazon.com/singlesignon/>.
2. Di bawah Multi-account izin, pilih Kumpulan izin.
3. Pada halaman Kumpulan izin, pilih kumpulan izin yang ingin Anda lihat.
4. Setelah berada di halaman kumpulan izin yang dipilih, di bawah tab Akun, Anda dapat melihat akun tempat kumpulan izin digunakan. Anda dapat memilih akun untuk melihat bagaimana kumpulan izin disediakan dalam akun. Anda dapat [menghapus](#), mengedit, dan melampirkan kebijakan ke kumpulan izin.

All permission sets for an Akun AWS

Untuk melihat semua tugas untuk kumpulan izin, gunakan prosedur berikut:

1. Masuk ke Konsol Manajemen AWS dan buka AWS IAM Identity Center konsol di <https://console.aws.amazon.com/singlesignon/>.
2. Di bawah Multi-account izin, pilih Akun AWS. Pilih akun yang ingin Anda lihat kumpulan izin yang disediakan.
3. Setelah berada di Akun AWS halaman yang dipilih, di bawah tab Kumpulan izin, Anda dapat melihat kumpulan izin berbeda yang ditetapkan untuk yang dipilih Akun AWS. Anda dapat memilih hyperlink kumpulan izin untuk mempelajari lebih lanjut tentang kumpulan izin.

All applied permission sets to users and groups

Untuk melihat semua kumpulan izin yang ditetapkan untuk pengguna atau grup, gunakan prosedur berikut:

1. Masuk ke Konsol Manajemen AWS dan buka AWS IAM Identity Center konsol di <https://console.aws.amazon.com/singlesignon/>.
2. Pilih Pengguna atau Grup di bawah Dasbor untuk melihat pengguna atau grup Pusat Identitas IAM.
 - a. Setelah berada di halaman Pengguna, pilih pengguna yang ingin Anda lihat kumpulan izin yang diterapkan. Selanjutnya, pilih Akun AWS tab dan di Akun AWS bawah bagian akses AWS akun. Anda akan dapat melihat kumpulan izin yang diterapkan dan Akun AWS untuk pengguna yang dipilih.
 - b. Setelah berada di halaman Grup, pilih grup yang ingin Anda lihat kumpulan izin yang diterapkan. Selanjutnya, pilih Akun AWS tab dan di Akun AWS bawah bagian Akun AWS akses. Anda akan dapat melihat kumpulan izin yang diterapkan dan Akun AWS untuk grup yang dipilih.

Mengubah kumpulan izin

Gunakan prosedur ini untuk mengubah kumpulan [izin](#) dengan konsol Pusat Identitas IAM. Anda dapat menambahkan atau menghapus kumpulan izin dari pengguna atau grup.

1. Masuk ke Konsol Manajemen AWS dan buka AWS IAM Identity Center konsol di <https://console.aws.amazon.com/singlesignon/>.
2. Di bawah Multi-account izin, pilih Akun AWS.
3. Pada Akun AWS halaman, daftar tampilan pohon organisasi Anda muncul. Pilih nama Akun AWS dari mana Anda ingin mengubah kumpulan izin.
4. Pada halaman Ikhtisar Akun AWS, di bawah Pengguna dan Grup yang Ditugaskan, pilih nama pengguna atau nama grup dari kumpulan izin yang ingin Anda ubah. Kemudian pilih U bah kumpulan izin.
5. Buat perubahan yang diinginkan pada kumpulan izin dan kemudian pilih S impan perubahan.
6. Arahkan ke tab Kumpulan izin dan pilih kumpulan izin yang baru saja diubah dan pilih Per barui.
7. Pada halaman Per barui izin, pilih Per barui.

Delegasikan administrasi kumpulan izin

Pusat Identitas IAM memungkinkan Anda mendelegasikan pengelolaan kumpulan izin dan penugasan di akun dengan membuat kebijakan [IAM](#) yang mereferensikan Nama Sumber [Daya Amazon \(ARN\) sumber daya Pusat Identi](#) tas IAM. Misalnya, Anda dapat membuat kebijakan yang memungkinkan administrator yang berbeda untuk mengelola penugasan di akun tertentu untuk kumpulan izin dengan tag tertentu.

Note

Untuk menggunakan kumpulan izin, Anda harus menggunakan instance Organisasi dari Pusat Identitas IAM. Untuk informasi selengkapnya, lihat [Instans organisasi dan akun dari Pusat Identitas IAM](#).

Anda dapat menggunakan salah satu metode berikut untuk membuat jenis kebijakan ini.

- (Disarankan) Buat [kumpulan izin](#) di Pusat Identitas IAM, masing-masing dengan kebijakan yang berbeda, dan tetapkan kumpulan izin ke pengguna atau grup yang berbeda. Ini memungkinkan Anda mengelola izin administratif untuk pengguna yang masuk menggunakan sumber [identitas Pusat Identi](#) tas IAM pilihan Anda.
- 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 kumpulan izin Pusat Identitas IAM dan jenis sumber daya akun.

Jenis Sumber Daya	ARN	Tombol Konteks
PermissionSet	arn:\${Partition}:sso::permissionSet	aws:ResourceTag/\${TagKey}

Jenis Sumber Daya	ARN	Tombol Konteks
	<code>/\${InstanceId}/\${PermissionSetId}</code>	
Akun	<code>arn:\${Partition}:sso:::account/\${AccountId}</code>	Tidak Berlaku

Menggunakan kebijakan IAM dalam kumpulan izin

Di [Membuat kumpulan izin](#), Anda mempelajari cara menambahkan kebijakan, termasuk kebijakan yang dikelola pelanggan dan batas izin, ke kumpulan izin. Saat Anda menambahkan kebijakan dan izin yang dikelola pelanggan ke kumpulan 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 kumpulan izin, dan mencocokkannya dengan spesifikasi nama dan jalur kumpulan izin Anda. Saat Anda menetapkan kumpulan izin ke organisasi Akun AWS Anda, Pusat Identitas IAM membuat peran [AWS Identity and Access Management \(IAM\)](#) dan melampirkan kebijakan [IAM Anda](#) ke peran tersebut.

Pertimbangan-pertimbangan

- Untuk menggunakan kumpulan izin, Anda harus menggunakan instance Organisasi dari Pusat Identitas IAM. Untuk informasi selengkapnya, lihat [Instans organisasi dan akun dari Pusat Identitas IAM](#).
- Sebelum menetapkan kumpulan izin dengan kebijakan IAM, Anda harus menyiapkan akun anggota Anda. Nama kebijakan IAM di akun anggota Anda harus sesuai dengan nama kebijakan di akun manajemen Anda. Pusat Identitas IAM gagal menetapkan kumpulan izin jika kebijakan tidak ada di akun anggota Anda.

Note

Saat kebijakan yang dikelola pelanggan dilampirkan ke kumpulan izin, nama kebijakan tidak peka huruf besar/kecil.

- Izin yang diberikan kebijakan tidak harus sama persis antar akun.

Menetapkan kebijakan IAM ke kumpulan izin

1. Buat kebijakan IAM di setiap Akun AWS tempat Anda ingin menetapkan kumpulan izin.
2. Tetapkan izin ke kebijakan IAM. Anda dapat menetapkan izin yang berbeda di akun yang berbeda. Untuk pengalaman yang konsisten, konfigurasi dan pertahankan izin yang identik di setiap kebijakan. Anda dapat menggunakan sumber daya otomatisasi seperti AWS CloudFormation StackSets untuk membuat salinan kebijakan IAM dengan nama dan izin yang sama di setiap akun anggota. Untuk informasi selengkap CloudFormation StackSets nya, lihat [Bekerja dengan AWS CloudFormation StackSets](#) di Panduan AWS CloudFormation Pengguna.
3. Buat kumpulan izin di akun manajemen Anda dan tambahkan kebijakan IAM Anda di bawah Kebijakan yang dikelola pelanggan atau batas Izin. Untuk detail selengkapnya tentang cara membuat kumpulan izin, Lihat [Membuat kumpulan izin](#).
4. Tambahkan kebijakan sebaris, kebijakan AWS terkelola, atau kebijakan IAM tambahan yang telah Anda siapkan.
5. Buat dan tetapkan kumpulan izin Anda.

Menghapus kumpulan izin di Pusat Identitas IAM

Anda dapat menghapus kumpulan izin dari pengguna dan grup Pusat Identitas IAM di konsol Pusat Identitas IAM. Anda juga dapat menghapus kumpulan izin dari Akun AWS. Untuk informasi selengkapnya tentang kumpulan izin dan cara penggunaannya di Pusat Identitas IAM, lihat [Kelola Akun AWS dengan set izin](#).

Note

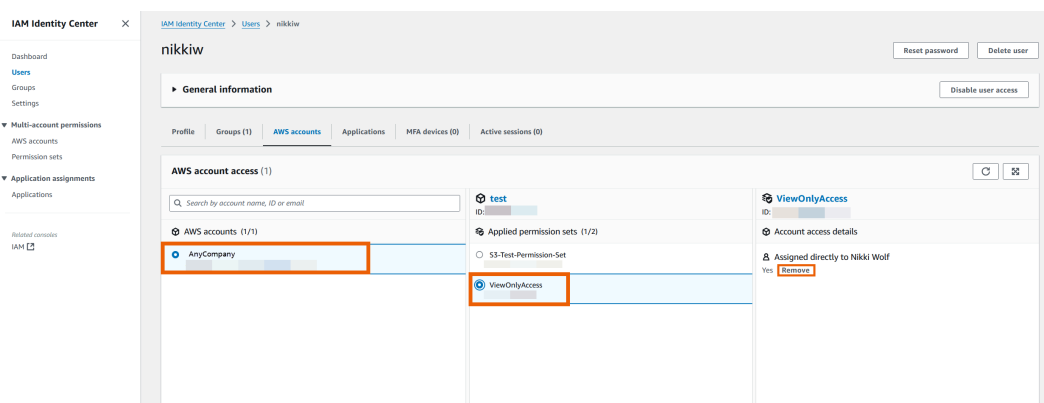
Untuk menggunakan kumpulan izin, Anda harus menggunakan instance Organisasi dari Pusat Identitas IAM. Untuk informasi selengkapnya, lihat [Instans organisasi dan akun dari Pusat Identitas IAM](#).

Remove permission set from a user

Menghapus kumpulan izin dari pengguna

Gunakan prosedur ini untuk menghapus kumpulan izin dari pengguna dengan konsol Pusat Identitas IAM.

1. Masuk ke Konsol Manajemen AWS dan buka AWS IAM Identity Center konsol di <https://console.aws.amazon.com/singlesignon/>.
2. Di bawah Pusat Identitas IAM, pilih Pengguna.
3. Pilih nama pengguna pengguna yang ingin Anda hapus kumpulan izin.
4. Pada halaman detail pengguna, pilih Akun AWS tab. Di bawah Akun AWS akses, pilih Anda Akun AWS.
5. Di panel kanan, izin yang diterapkan untuk pengguna yang dipilih muncul. Pilih kumpulan izin yang ingin Anda hapus. Di bawah Detail Akses Akun, pilih Hapus.
6. Sebuah kotak dialog muncul menanyakan apakah Anda ingin menghapus kumpulan izin ini. Pilih Hapus.

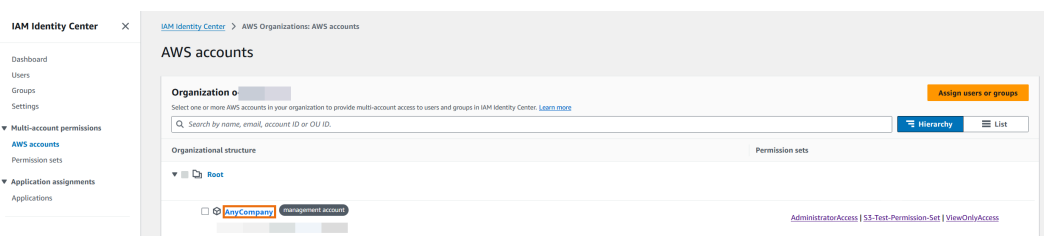


Remove permission set from a group

Menghapus kumpulan izin dari grup

Gunakan prosedur ini untuk menghapus kumpulan izin dari grup dengan konsol Pusat Identitas IAM.

1. Masuk ke Konsol Manajemen AWS dan buka AWS IAM Identity Center konsol di <https://console.aws.amazon.com/singlesignon/>.
2. Di bawah Multi-account izin, pilih Akun AWS. Pilih tautan ke akun manajemen Anda.



3. Di bawah tab Pengguna dan grup yang ditugaskan, pilih grup tempat Anda ingin menghapus kumpulan izin, lalu pilih U bah kumpulan izin.
4. Pada halaman U bah kumpulan izin, kosongkan kumpulan izin yang ingin Anda hapus, lalu pilih S impan perubahan.

Remove permission set from an Akun AWS

Gunakan prosedur ini untuk menghapus kumpulan izin dari Akun AWS konsol IAM Identity Center.

1. Masuk ke Konsol Manajemen AWS dan buka AWS IAM Identity Center konsol di <https://console.aws.amazon.com/singlesignon/>.
2. Di bawah Multi-account izin, pilih Akun AWS. Pilih nama Akun AWS dari mana Anda ingin menghapus kumpulan izin.
3. Pada halaman Ikhtisar Akun AWS, pilih tab Kumpulan izin. Pilih kumpulan izin yang ingin Anda hapus. Kemudian pilih H apus.
4. Di kotak dialog Hapus kumpulan izin, konfirmasikan bahwa kumpulan izin yang benar dipilih, ketik **Delete** untuk mengonfirmasi penghapusan, lalu pilih Hapus akses.

Menghapus kumpulan izin di Pusat Identitas IAM

Sebelum Anda dapat menghapus kumpulan izin dari Pusat Identitas IAM, Anda harus mengh [ap](#) usnya dari semua Akun AWS yang menggunakan kumpulan izin. Untuk memeriksa akses pengguna dan grup yang ada, lihat [Melihat dan mengubah kumpulan izin](#).

Pertimbangan-pertimbangan

- Untuk menggunakan kumpulan izin, Anda harus menggunakan instance Organisasi dari Pusat Identitas IAM. Untuk informasi selengkapnya, lihat [Instans organisasi dan akun dari Pusat Identitas IAM](#).
- Jika Anda ingin mencabut sesi kumpulan izin aktif, lihat [the section called “Akhir sesi aktif untuk pengguna tenaga kerja”](#).
- Anda harus menghapus kumpulan izin dan penetapan aplikasi dari pengguna atau grup yang ingin Anda hapus sebelum menghapusnya. Jika tidak, Anda akan memiliki kumpulan izin dan aplikasi yang tidak ditetapkan dan tidak digunakan di Pusat Identitas IAM.

Gunakan prosedur berikut untuk menghapus satu atau lebih kumpulan izin sehingga tidak dapat lagi digunakan oleh siapa pun Akun AWS di organisasi.

⚠ Important

Semua pengguna dan grup yang telah ditetapkan kumpulan izin ini, terlepas dari Akun AWS apa yang menggunakannya, tidak akan dapat lagi masuk. Untuk memeriksa akses pengguna dan grup yang ada, lihat [Melihat dan mengubah kumpulan izin](#).

Untuk menghapus kumpulan izin dari Akun AWS

1. Buka konsol [Pusat Identi](#) tas IAM.
2. Di bawah Multi-account izin, pilih Kumpulan izin.
3. Pilih kumpulan izin yang ingin Anda hapus, lalu pilih Hapus.
4. Di kotak dialog Hapus kumpulan izin, ketik nama kumpulan izin untuk mengonfirmasi penghapusan, lalu pilih Hapus. Nama domain tidak peka huruf besar/kecil.

Konfigurasikan properti kumpulan izin

Di Pusat Identitas IAM, administrator dapat menyelesaikan tugas konfigurasi dan manajemen berikut untuk mengontrol akses pengguna dan durasi sesi.

Tugas	Pelajari selengkapnya
Administrator dapat mengatur durasi maksimum untuk sesi pengguna saat mengakses AWS sumber daya melalui Pusat Identitas IAM.	Tetapkan durasi sesi untuk Akun AWS
Administrator dapat menyesuaikan halaman arahan yang dilihat pengguna setelah berhasil mengotentikasi melalui Pusat Identitas IAM.	Atur status relai untuk akses cepat ke Konsol Manajemen AWS
Pastikan pengguna tidak lagi memiliki akses ke AWS sumber daya saat izin mereka dicabut.	Menggunakan kebijakan Tolak untuk mencabut izin pengguna aktif

Tetapkan durasi sesi untuk Akun AWS

Untuk setiap kumpulan [izin](#), Anda dapat menentukan durasi sesi untuk mengontrol lamanya waktu pengguna dapat masuk ke Akun AWS. Ketika durasi yang ditentukan berlalu, AWS tandatangani pengguna keluar dari sesi.

Saat Anda membuat kumpulan izin baru, durasi sesi diatur ke 1 jam (dalam detik) secara default. Durasi sesi minimum adalah 1 jam, dan dapat diatur hingga maksimum 12 jam. Pusat Identitas IAM secara otomatis membuat peran IAM di setiap akun yang ditetapkan untuk setiap kumpulan izin, dan mengonfigurasi peran ini dengan durasi sesi maksimum 12 jam.

Saat pengguna bergabung ke Akun AWS konsol mereka atau saat AWS Command Line Interface (AWS CLI) digunakan, Pusat Identitas IAM menggunakan pengaturan durasi sesi pada set izin untuk mengontrol durasi sesi. Secara default, peran IAM yang dihasilkan oleh Pusat Identitas IAM untuk kumpulan 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 terbaik keamanan, sebaiknya Anda tidak mengatur durasi sesi lebih lama dari yang diperlukan untuk melakukan peran.

Setelah membuat kumpulan izin, Anda dapat memperbaruinya untuk menerapkan durasi sesi baru. Gunakan prosedur berikut untuk mengubah durasi sesi untuk kumpulan izin.

Untuk mengatur durasi sesi

1. Buka konsol [Pusat Identitas IAM](#).
2. Di bawah Multi-account izin, pilih Kumpulan izin.
3. Pilih nama kumpulan izin yang ingin Anda ubah durasi sesi.
4. Pada halaman detail untuk kumpulan izin, di sebelah kanan judul bagian Pengaturan umum, pilih Edit.
5. Pada halaman Edit pengaturan kumpulan izin umum, pilih nilai baru untuk Durasi sesi.
6. Jika kumpulan izin disediakan di salah satu Akun AWS, nama-nama akun muncul di bawah Akun AWS untuk penyediaan ulang secara otomatis. Setelah nilai durasi sesi untuk kumpulan izin diperbarui, semua Akun AWS yang menggunakan kumpulan izin disediakan ulang. Ini berarti

bahwa nilai baru untuk pengaturan ini diterapkan ke semua Akun AWS yang menggunakan kumpulan izin.

7. Pilih Simpan perubahan.
8. Di bagian atas Akun AWS halaman, pemberitahuan muncul.
 - Jika kumpulan izin disediakan dalam satu atau lebih Akun AWS, notifikasi mengonfirmasi bahwa kumpulan izin Akun AWS berhasil disediakan ulang, dan kumpulan izin yang diperbarui diterapkan ke akun.
 - Jika kumpulan izin tidak disediakan dalam sebuah Akun AWS, notifikasi mengonfirmasi bahwa pengaturan untuk kumpulan izin telah diperbarui.

Atur status relai untuk akses cepat ke Konsol Manajemen AWS

Secara default, saat pengguna masuk ke portal AWS akses, memilih akun, dan kemudian memilih peran yang dibuat dari AWS kumpulan izin yang ditetapkan, Pusat Identitas IAM mengalihkan browser pengguna ke. Konsol Manajemen AWS Anda dapat mengubah perilaku ini dengan menyetel status relai ke URL konsol yang berbeda.

Mengatur status relai memungkinkan Anda memberi pengguna akses cepat ke konsol yang paling sesuai untuk peran mereka. Misalnya, Anda dapat mengatur 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, Pusat Identitas IAM 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 tertentu Wilayah AWS, sertakan spesifikasi Wilayah sebagai bagian dari URL. Misalnya, untuk mengarahkan pengguna ke konsol Amazon EC2 di Wilayah AS Timur (Ohio) (us-east-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-west-2) dan Anda ingin mengarahkan pengguna ke Wilayah tersebut, tentukan. **<https://us-west-2.console.aws.amazon.com/>**

Konfigurasi status relai

Gunakan prosedur berikut untuk mengonfigurasi URL status relai untuk kumpulan izin.

1. Buka konsol [Pusat Identi](#) tas IAM.
2. Di bawah Multi-account izin, pilih Kumpulan izin.
3. Pilih nama kumpulan izin yang ingin Anda atur URL status relai baru.
4. Pada halaman detail untuk kumpulan izin, di sebelah kanan judul bagian Pengaturan umum, pilih Edit.
5. Pada halaman Edit pengaturan kumpulan izin umum, di bawah Status Relay, ketik URL konsol untuk salah satu AWS layanan. Contoh:

`https://console.aws.amazon.com/ec2/`

Note

URL status relay harus berada di dalam Konsol Manajemen AWS.

6. Jika kumpulan izin disediakan di salah satu Akun AWS, nama-nama akun muncul di bawah Akun AWS untuk penyediaan ulang secara otomatis. Setelah URL status relai untuk kumpulan izin diperbarui, semua Akun AWS yang menggunakan kumpulan izin disediakan ulang. Ini berarti bahwa nilai baru untuk pengaturan ini diterapkan ke semua Akun AWS yang menggunakan kumpulan izin.
7. Pilih Simpan perubahan.
8. Di bagian atas halaman AWS Organisasi, pemberitahuan muncul.
 - Jika kumpulan izin disediakan dalam satu atau lebih Akun AWS, notifikasi mengonfirmasi bahwa kumpulan izin Akun AWS berhasil disediakan ulang, dan kumpulan izin yang diperbarui diterapkan ke akun.
 - Jika kumpulan izin tidak disediakan dalam sebuah Akun AWS, notifikasi mengonfirmasi bahwa pengaturan untuk kumpulan izin telah diperbarui.

Note

Anda dapat mengotomatiskan proses ini dengan menggunakan AWS API, AWS SDK, atau AWS Command Line Interface(AWS CLI). Untuk informasi selengkapnya, lihat:

- Tindakan `CreatePermissionSet` akan `UpdatePermissionSet` atau di Referensi API Pusat Identitas [IAM](#)
- Per `create-permission-set` `update-permission-set` intah atau di [sso-admin](#) bagian Referensi AWS CLI Perintah.

Menggunakan kebijakan Tolak untuk mencabut izin pengguna aktif

Anda mungkin perlu mencabut akses pengguna Pusat Identitas IAM Akun AWS saat pengguna secara aktif menggunakan kumpulan izin. Anda dapat menghapus kemampuan mereka untuk menggunakan sesi peran IAM aktif mereka dengan menerapkan kebijakan Tolak untuk pengguna yang tidak ditentukan sebelumnya, lalu bila diperlukan, Anda dapat memperbarui kebijakan Tolak untuk menentukan pengguna yang aksesnya ingin Anda blokir. Topik ini menjelaskan cara membuat kebijakan Tolak dan pertimbangan tentang cara menerapkan kebijakan tersebut.

Bersiaplah untuk mencabut sesi peran IAM aktif yang dibuat oleh kumpulan izin

Anda dapat mencegah pengguna mengambil tindakan dengan peran IAM yang mereka gunakan secara aktif dengan menerapkan kebijakan tolak semua untuk pengguna tertentu melalui penggunaan Kebijakan Kontrol Layanan. Anda juga dapat mencegah pengguna menggunakan kumpulan izin apa pun sampai Anda mengubah kata sandinya, yang menghapus aktor jahat yang secara aktif menyalahgunakan kredentif yang dicuri. Jika Anda perlu menolak akses secara luas dan mencegah pengguna memasukkan kembali kumpulan izin atau mengakses kumpulan izin lainnya, Anda juga dapat menghapus semua akses pengguna, menghentikan sesi portal AWS akses aktif, dan menonaktifkan login pengguna. Lihat [the section called “Akhir sesi aktif untuk pengguna tenaga kerja”](#) untuk mempelajari cara menggunakan kebijakan Tolak bersama dengan tindakan tambahan untuk pencabutan akses yang lebih luas.

Kebijakan tolak

Anda dapat menggunakan kebijakan Tolak dengan kondisi yang cocok dengan pengguna `UserId` dari penyimpanan identitas Pusat Identitas IAM untuk mencegah tindakan lebih lanjut oleh peran IAM yang digunakan pengguna secara aktif. Menggunakan kebijakan ini menghindari dampak pada pengguna lain yang mungkin menggunakan kumpulan izin yang sama saat Anda menerapkan kebijakan Tolak. Kebijakan ini menggunakan ID pengguna placeholder, *Add user ID here*, untuk `"identitystore:userId"` itu Anda akan memperbarui dengan ID pengguna yang ingin Anda cabut aksesnya.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "*"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "identitystore:userId": "Add user ID here"
        }
      }
    }
  ]
}
```

Meskipun Anda dapat menggunakan kunci kondisi lain seperti `aws:userId`, `identitystore:userId` pasti karena itu adalah nilai unik global yang dikaitkan dengan satu orang. Penggunaan `aws:userId` dalam kondisi dapat dipengaruhi oleh bagaimana atribut pengguna disinkronkan dari sumber identitas Anda dan dapat berubah jika nama pengguna atau alamat email pengguna berubah.

Dari konsol Pusat Identitas IAM, Anda dapat menemukan pengguna `identitystore:userId` dengan menavigasi ke Pengguna, mencari pengguna berdasarkan nama, memperluas bagian Informasi Umum dan menyalin ID Pengguna. Juga nyaman untuk menghentikan sesi portal AWS akses pengguna dan menonaktifkan akses masuk mereka di bagian yang sama saat mencari ID Pengguna. Anda dapat mengotomatiskan proses untuk membuat kebijakan Tolak dengan mendapatkan ID Pengguna pengguna melalui kueri API penyimpanan identitas.

Menyebarkan kebijakan penolakan

Anda dapat menggunakan ID pengguna placeholder yang tidak valid, seperti *Add user ID here*, untuk menerapkan kebijakan Tolak terlebih dahulu menggunakan Kebijakan Kontrol Layanan (SCP) yang Anda lampirkan ke Akun AWS pengguna yang mungkin memiliki akses. Ini adalah pendekatan yang direkomendasikan untuk kemudahan dan kecepatan dampaknya. Saat mencabut akses

pengguna dengan kebijakan Tolak, Anda akan mengedit kebijakan untuk mengganti ID pengguna placeholder dengan ID pengguna orang yang aksesnya ingin Anda cabut. Ini mencegah pengguna mengambil tindakan apa pun dengan izin yang ditetapkan di setiap akun yang Anda lampirkan SCP. Ini memblokir tindakan pengguna bahkan jika mereka menggunakan sesi portal AWS akses aktif mereka untuk menavigasi ke akun yang berbeda dan mengambil peran yang berbeda. Dengan akses pengguna diblokir sepenuhnya oleh SCP, Anda kemudian dapat menonaktifkan kemampuan mereka untuk masuk, mencabut tugas mereka, dan menghentikan sesi portal AWS akses mereka jika diperlukan.

Sebagai alternatif untuk menggunakan SCP, Anda juga dapat menyertakan kebijakan Tolak dalam kebijakan sebaris dari kumpulan izin dan dalam kebijakan yang dikelola pelanggan yang digunakan oleh kumpulan izin yang dapat diakses pengguna.

Jika Anda harus mencabut akses untuk lebih dari satu orang, Anda dapat menggunakan daftar nilai di blok kondisi, seperti:

```
"Condition": {
  "StringEquals": {
    "identitystore:userId": [" user1 userId", "user2 userId"...]
  }
}
```

Important

Apa pun metode yang Anda gunakan, Anda harus mengambil tindakan korektif lainnya dan menyimpan ID pengguna dalam kebijakan setidaknya selama 12 jam. Setelah waktu itu, peran apa pun yang diasumsikan pengguna kedaluwarsa dan Anda kemudian dapat menghapus ID pengguna mereka dari kebijakan Tolak.

Mereferensikan kumpulan izin dalam kebijakan sumber daya, peta konfigurasi Cluster Amazon EKS, dan AWS KMS kebijakan utama

Saat Anda menetapkan kumpulan izin ke AWS akun, Pusat Identitas IAM membuat peran dengan nama yang dimulai dengan `AWSReservedSSO_`.

Nama lengkap dan Nama Sumber Daya Amazon (ARN) untuk peran menggunakan format berikut:

Nama	ARN
AWSReservedSSO_ <i>permission-set-name_unique-suffix</i>	arn:aws:iam:: <i>aws-account-ID</i> :role/aws-reserved/sso.amazonaws.com/ <i>aws-region</i> /AWSReservedSSO_ <i>permission-set-name_unique-suffix</i>

Jika sumber identitas Anda di Pusat Identitas IAM di-host di us-east-1, tidak ada *aws-region* di ARN. Nama lengkap dan ARN untuk peran menggunakan format berikut:

Nama	ARN
AWSReservedSSO_ <i>permission-set-name_unique-suffix</i>	arn:aws:iam:: <i>aws-account-ID</i> :role/aws-reserved/sso.amazonaws.com/AWSReservedSSO_ <i>permission-set-name_unique-suffix</i>

Misalnya, jika Anda membuat kumpulan izin yang memberikan akses AWS akun ke administrator database, peran yang sesuai dibuat dengan nama berikut dan ARN:

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 penugasan ke kumpulan izin ini di AWS akun, peran terkait yang dibuat oleh Pusat Identitas IAM juga dihapus. Jika Anda membuat penugasan baru ke kumpulan izin yang sama nanti, Pusat Identitas IAM membuat peran baru untuk kumpulan 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 akan menyebabkan kebijakan apa pun yang mereferensikan nama asli dan ARN menjadi usang, yang mengganggu akses bagi individu yang menggunakan kumpulan izin yang sesuai. Misalnya, perubahan dalam ARN untuk peran akan mengganggu akses bagi pengguna kumpulan izin jika ARN asli direferensikan dalam konfigurasi berikut:

- Dalam `aws-auth ConfigMap` file untuk cluster Amazon Elastic Kubernetes Service (Amazon EKS) saat Anda menggunakan `aws-auth ConfigMap` untuk akses cluster.
- Dalam kebijakan berbasis sumber daya untuk kunci AWS Key Management Service (AWS KMS). Kebijakan ini juga disebut sebagai kebijakan utama.

Note

Kami menyarankan Anda menggunakan entri akses [Amazon EKS](#) untuk mengelola akses ke cluster Amazon EKS Anda. Ini memungkinkan Anda menggunakan izin IAM untuk mengelola prinsipal yang memiliki akses ke cluster Amazon EKS. Dengan menggunakan entri akses Amazon EKS, Anda dapat menggunakan prinsip IAM dengan izin Amazon EKS untuk mendapatkan kembali akses ke cluster tanpa menghubungi Dukungan.

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 AWS KMS jika ARN berubah. 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 dengan izin untuk memperbarui kebijakan `aws-auth ConfigMap` atau kebijakan AWS KMS utama, hubungi Dukungan untuk mendapatkan kembali akses ke sumber daya tersebut.

Rekomendasi untuk menghindari gangguan akses

Untuk menghindari gangguan akses karena perubahan dalam ARN untuk peran yang sesuai dengan kumpulan izin, kami sarankan Anda melakukan hal berikut.

- Pertahankan setidaknya satu penetapan kumpulan izin.

Pertahankan penugasan ini di AWS akun yang berisi peran yang Anda rujuk di `aws-auth ConfigMap` untuk Amazon EKS, kebijakan utama di AWS KMS, atau kebijakan berbasis sumber daya untuk lainnya. Layanan AWS

Misalnya, jika Anda membuat kumpulan `EKSAccess` izin dan mereferensikan peran yang sesuai ARN dari AWS akun `111122223333`, maka tetapkan grup administratif secara permanen ke set izin di akun tersebut. Karena penugasan bersifat permanen, Pusat Identitas IAM tidak akan menghapus peran yang sesuai, yang menghilangkan risiko penggantian nama. Grup administratif akan selalu memiliki akses tanpa risiko eskalasi hak istimewa.

- Untuk cluster Amazon EKS yang menggunakan **aws-auth ConfigMap** dan AWS KMS: Sertakan peran yang dibuat di IAM.

Jika Anda mereferensikan ARN peran `aws-auth ConfigMap` untuk kumpulan izin di cluster Amazon EKS atau dalam kebijakan utama untuk AWS KMS kunci, sebaiknya Anda juga menyertakan setidaknya satu peran yang Anda buat di IAM. Peran harus memungkinkan Anda mengakses cluster Amazon EKS atau mengelola kebijakan AWS KMS utama. Kumpulan izin harus dapat mengambil peran ini. Dengan begitu, jika peran ARN untuk kumpulan izin berubah, Anda dapat memperbarui referensi ke ARN dalam kebijakan `aws-auth ConfigMap` atau AWS KMS kunci. Bagian selanjutnya memberikan contoh bagaimana Anda dapat membuat kebijakan kepercayaan untuk peran yang dibuat di IAM. Peran hanya dapat diasumsikan oleh `kum AdministratorAccess` pulan izin.

Contoh kebijakan kepercayaan khusus

Berikut ini adalah contoh kebijakan kepercayaan khusus yang menyediakan kumpulan `AdministratorAccess` izin dengan akses ke peran yang dibuat di IAM. Elemen kunci dari kebijakan ini meliputi:

- Elemen Utama dari kebijakan kepercayaan ini menentukan prinsi AWS `pal` akun. Dalam kebijakan ini, kepala sekolah di AWS akun `111122223333` dengan `sts:AssumeRole` izin dapat mengambil peran yang dibuat di IAM.

- Kebijakan kepercayaan ini menetapkan persyaratan tambahan untuk kepala sekolah yang dapat mengambil peran yang dibuat di IAM. Condition element Dalam kebijakan ini, izin yang disetel dengan peran berikut ARN dapat mengambil peran tersebut.

```
arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/  
AWSReservedSSO_AdministratorAccess_*
```

Note

ConditionElement menyer ArnLike takan operator kondisi dan menggunakan wildcard di akhir peran set izin ARN, bukan akhiran unik. Ini berarti bahwa kebijakan mengizinkan kumpulan izin untuk mengambil peran yang dibuat di IAM meskipun peran ARN untuk kumpulan izin berubah.

JSON

```
{  
  "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 tersebut akan memberi Anda akses darurat ke cluster Amazon EKS Anda AWS KMS keys, atau AWS sumber daya lain jika kumpulan izin atau semua penugasan ke kumpulan izin dihapus dan dibuat ulang secara tidak sengaja.

Attribute-based kontrol akses

Attribute-based kontrol akses (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut. Anda dapat menggunakan Pusat Identitas IAM untuk mengelola akses ke AWS sumber daya di beberapa sumber daya Akun AWS menggunakan atribut pengguna yang berasal dari sumber identitas Pusat Identitas IAM mana pun. Di AWS, atribut ini disebut tag. Menggunakan atribut pengguna sebagai tag AWS membantu Anda menyederhanakan proses pembuatan izin berbutir halus AWS dan memastikan bahwa tenaga kerja Anda hanya mendapatkan akses ke AWS sumber daya dengan tag yang cocok.

Misalnya, Anda dapat menetapkan pengembang Bob dan Sally, yang berasal dari dua tim berbeda, ke kumpulan izin yang sama di Pusat Identitas IAM (atau peran IAM yang sama di manajer akses akun) lalu pilih atribut nama tim untuk kontrol akses. Saat Bob dan Sally masuk ke mereka Akun AWS, Pusat Identitas IAM 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 pembaruan izin apa pun AWS.

Pendekatan ini juga membantu mengurangi jumlah izin berbeda yang perlu Anda buat dan kelola di Pusat Identitas IAM karena pengguna yang terkait dengan kumpulan izin yang sama (atau di manajer akses akun karena pengguna yang terkait dengan peran IAM yang sama) sekarang dapat memiliki izin unik berdasarkan atributnya. Anda dapat menggunakan atribut pengguna ini dalam kumpulan izin Pusat Identitas IAM (atau peran IAM saat menggunakan penetapan peran manajer akses akun) dan kebijakan berbasis sumber daya untuk menerapkan ABAC ke AWS sumber daya dan menyederhanakan pengelolaan izin dalam skala besar.

Manfaat

Berikut ini adalah manfaat tambahan menggunakan ABAC di Pusat Identitas IAM.

- ABAC memerlukan kumpulan izin yang lebih sedikit — Karena Anda tidak perlu membuat kebijakan yang berbeda untuk fungsi pekerjaan yang berbeda, Anda membuat lebih sedikit kumpulan izin (atau peran IAM saat menggunakan manajer akses akun). 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 diberi tag dengan tepat 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 di 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 mengkonfigurasi 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 [CreateInstanceAccessControlAttributeConfiguration](#) di Panduan Referensi API Pusat Identitas IAM.

Topik

- [Daftar Periksa: Mengkonfigurasi ABAC di AWS menggunakan Pusat Identitas IAM](#)
- [Atribut untuk kontrol akses](#)

Daftar Periksa: Mengkonfigurasi ABAC di AWS menggunakan Pusat Identitas IAM

Daftar periksa ini mencakup tugas konfigurasi yang diperlukan untuk mempersiapkan AWS sumber daya Anda dan untuk mengatur Pusat Identitas IAM untuk akses ABAC. Selesaikan tugas dalam daftar periksa ini secara berurutan. Ketika tautan referensi membawa Anda ke topik, kembali 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 Pusat Identitas IAM, Anda harus terlebih dahulu menambahkan tag ke semua AWS sumber daya yang ingin Anda terapkan untuk ABAC.	<ul style="list-style-type: none"> • Menandai sumber daya AWS

Langka	Tugas	Referensi
2	Tinjau cara mengonfigurasi sumber identitas Anda di Pusat Identitas IAM dengan identitas dan atribut pengguna terkait di penyimpanan identitas Anda. Pusat Identitas IAM memungkinkan Anda menggunakan atribut pengguna dari sumber identitas Pusat Identitas IAM yang didukung untuk ABAC di AWS	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • Memulai
	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • Memilih atribut saat menggunakan penyedia identitas eksternal sebagai sumber identitas Anda
	<ul style="list-style-type: none"> • Jika Anda memilih agar IdP mengirim atribut, konfigurasi IdP Anda untuk mengirimkan atribut dalam pernyataan SAML. Lihat <code>Optional</code> bagian dalam tutorial untuk IdP spesifik Anda. 	<ul style="list-style-type: none"> • Tutorial sumber identitas Pusat Identitas IAM
	<ul style="list-style-type: none"> • Jika Anda menggunakan IdP sebagai sumber identitas dan memilih untuk memilih atribut di Pusat Identitas IAM, selidiki cara mengonfigurasi SCIM sehingga nilai atribut berasal dari IdP Anda. Jika Anda tidak dapat menggunakan SCIM dengan IdP Anda, tambahkan pengguna dan atributnya menggunakan halaman Pengguna konsol Pusat Identitas IAM. 	<ul style="list-style-type: none"> • Menyediakan pengguna dan grup dari penyedia identitas eksternal menggunakan SCIM • Atribut penyedia identitas eksternal yang didukung

Langka	Tugas	Referensi
	<ul style="list-style-type: none"> Jika Anda menggunakan Active Directory atau Pusat Identitas IAM sebagai sumber identitas, atau Anda menggunakan IdP dan memilih untuk memilih atribut di Pusat Identitas IAM, tinjau atribut yang tersedia yang dapat Anda konfigurasi. Kemudian segera lanjutkan ke langkah 4 untuk mulai mengonfigurasi atribut ABAC Anda menggunakan konsol IAM Identity Center. 	<ul style="list-style-type: none"> Memilih atribut saat menggunakan Pusat Identitas IAM sebagai sumber identitas Anda Memilih atribut saat menggunakan AWS Managed Microsoft AD sebagai sumber identitas Anda Pemetaan default antara IAM Identity Center dan Microsoft AD
4	<p>Pilih atribut yang akan digunakan untuk ABAC menggunakan halaman Atribut untuk kontrol akses di konsol Pusat Identitas IAM. Dari halaman ini Anda dapat memilih atribut untuk kontrol akses dari sumber identitas yang Anda konfigurasi pada langkah 2. Setelah identitas Anda dan atributnya berada di Pusat Identitas IAM, Anda harus membuat pasangan kunci-nilai (pemetaan) yang akan diteruskan ke Anda Akun AWS untuk digunakan dalam keputusan kontrol akses.</p>	<ul style="list-style-type: none"> Mengaktifkan dan mengonfigurasi atribut untuk kontrol akses
5	<p>Buat kebijakan izin khusus dalam kumpulan izin Anda (atau peran IAM saat menggunakan pengelola akses akun) dan gunakan atribut kontrol akses untuk membuat aturan ABAC sehingga pengguna hanya dapat mengakses sumber daya dengan tag yang cocok. Atribut pengguna yang Anda konfigurasi pada langkah 4 digunakan sebagai tag AWS untuk keputusan kontrol akses. Anda dapat merujuk ke atribut kontrol akses dalam kebijakan izin menggunakan <code>aws:PrincipalTag/key</code> kondisi tersebut.</p>	<ul style="list-style-type: none"> Buat kebijakan izin untuk ABAC di Pusat Identitas IAM

Langka	Tugas	Referensi
6	Di berbagai Akun AWS, tetapkan pengguna ke kumpulan izin yang Anda buat di langkah 5. Melakukan hal itu memastikan bahwa ketika mereka bergabung ke akun mereka dan mengakses AWS sumber daya, mereka hanya mendapatkan akses berdasarkan tag yang cocok.	<ul style="list-style-type: none"> • Menetapkan akses pengguna atau grup 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 Anda gunakan 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). Di kumpulan izin Pusat Identitas IAM (atau peran IAM saat menggunakan manajer akses akun), Anda kemudian menulis kebijakan yang memberikan akses kepada pengguna hanya jika atribut Departemen cocok dengan tag departemen yang Anda tetapkan ke bucket S3 Anda. Pusat Identitas IAM meneruskan atribut departemen pengguna ke akun yang diakses. Atribut tersebut kemudian digunakan untuk menentukan akses berdasarkan kebijakan. Saat Pusat Identitas IAM meneruskan atribut ini ke akun, atribut tersebut dikirim sebagai tag sesi yang dapat Anda rujuk menggunakan kunci `aws:PrincipalTag/tag-key` kondisi di semua jenis kebijakan AWS IAM yang relevan. Untuk informasi lebih lanjut tentang ABAC, lihat [Attribute-based kontrol akses](#).

Memulai

Cara Anda mulai 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 kumpulan izin (atau kebijakan peran IAM saat menggunakan

pengelola akses akun). Kebijakan ini harus memberikan identitas pengguna akses ke AWS sumber daya.

Memilih atribut saat menggunakan Pusat Identitas IAM sebagai sumber identitas Anda

Saat Anda mengonfigurasi Pusat Identitas IAM sebagai sumber identitas, pertama-tama Anda menambahkan pengguna dan mengonfigurasi atribut mereka. Selanjutnya, navigasikan ke halaman **Atribut** untuk kontrol akses dan pilih atribut yang ingin Anda gunakan dalam kebijakan. Terakhir, navigasikan ke Akun AWS halaman untuk membuat atau mengedit kumpulan izin untuk menggunakan atribut untuk ABAC.

Memilih atribut saat menggunakan AWS Managed Microsoft AD sebagai sumber identitas Anda

Saat mengonfigurasi Pusat Identitas IAM AWS Managed Microsoft AD sebagai sumber identitas Anda, pertama-tama Anda memetakan serangkaian atribut dari Active Directory ke atribut pengguna di Pusat Identitas IAM. Selanjutnya, arahkan ke halaman **Atribut** untuk kontrol akses. Kemudian pilih atribut mana yang akan digunakan dalam konfigurasi ABAC berdasarkan kumpulan atribut SSO yang ada yang dipetakan dari Active Directory. Terakhir, penulis aturan ABAC menggunakan atribut kontrol akses dalam kumpulan izin (atau peran IAM saat menggunakan manajer akses akun) untuk memberikan identitas pengguna akses 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 antara IAM Identity Center dan Microsoft AD](#)

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.

- Konfigurasikan pemetaan atribut di konsol Pusat Identitas IAM. Anda dapat memetakan atribut dari direktori Pusat Identitas IAM ke tag sesi pada halaman **Atribut** untuk kontrol akses di konsol Pusat Identitas IAM. Nilai atribut yang Anda pilih di sini bersumber dari direktori Identity Center dan menggantikan nilai untuk atribut yang cocok yang berasal dari IdP melalui pernyataan SAML. Tergantung pada apakah Anda menggunakan SCIM, pertimbangkan hal berikut:
 - Jika menggunakan SCIM, IdP secara otomatis menyinkronkan nilai atribut ke Pusat Identitas IAM. Anda kemudian dapat memilih atribut yang disinkronkan ini pada halaman **Atribut** untuk kontrol akses untuk menggunakannya sebagai tag sesi.
 - Jika Anda tidak menggunakan SCIM, Anda harus menambahkan pengguna secara manual dan mengatur atribut mereka seperti jika Anda menggunakan Pusat Identitas IAM sebagai sumber

identitas. Selanjutnya, navigasikan ke halaman Atribut untuk kontrol akses dan pilih atribut yang ingin Anda gunakan dalam kebijakan.

- Berikan atribut dari IdP Anda melalui pernyataan SAML. Anda dapat mengonfigurasi IdP untuk mengirim atribut sebagai tag sesi melalui pernyataan SAML. Untuk melakukan ini, konfigurasi IdP Anda untuk mengirim pernyataan SAML dengan nama atribut yang disetel ke `https://aws.amazon.com/SAML/Attributes/AccessControl:TagKey`, ganti `TagKey` dengan kunci tag sesi yang ingin Anda isi. Pusat Identitas IAM meneruskan nama atribut dan nilai dari IdP untuk evaluasi kebijakan.

Tidak perlu mengonfigurasi pemetaan atribut ABAC pada halaman Atribut untuk kontrol akses untuk atribut yang Anda berikan melalui pernyataan SAML dari IdP eksternal Anda. Namun, jika Anda mengonfigurasi pemetaan ABAC untuk atribut yang sama pada halaman Atribut untuk kontrol akses, pemetaan dari direktori Identity Center diutamakan dan menggantikan nilai yang dikirim oleh IdP Anda dalam pernyataan SAML.

Note

Atribut dalam pernyataan SAML 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 eksternal IdPs Anda, atribut ini akan selalu diteruskan ketika pengguna bergabung ke dalam Akun AWS. Untuk informasi tentang cara mengonfigurasi atribut pengguna untuk kontrol akses di IdP Anda untuk dikirim melalui pernyataan SAML, lihat [Tutorial sumber identitas Pusat Identitas IAM](#) untuk IdP Anda.

Untuk daftar lengkap atribut yang didukung untuk atribut pengguna di Pusat Identitas IAM ke atribut pengguna di eksternal Anda IdPs, lihat [Atribut penyedia identitas eksternal yang didukung](#).

Untuk memulai dengan ABAC di Pusat Identitas IAM, lihat topik berikut.

Topik

- [Mengaktifkan dan mengonfigurasi atribut untuk kontrol akses](#)
- [Buat kebijakan izin untuk ABAC di Pusat Identitas IAM](#)

Mengaktifkan dan mengonfigurasi atribut untuk kontrol akses

Untuk menggunakan kontrol akses berbasis atribut (ABAC), Anda harus mengaktifkannya terlebih dahulu di halaman Pengaturan konsol Pusat Identitas IAM atau API Pusat Identitas [IAM](#). Terlepas dari sumber identitasnya, Anda selalu dapat mengonfigurasi atribut pengguna dari Identity Store untuk digunakan di ABAC. Di konsol, Anda dapat melakukan ini dengan menavigasi ke tab Atribut untuk kontrol akses di halaman Pengaturan. Jika Anda menggunakan penyedia identitas eksternal (IdP) sebagai sumber identitas, Anda juga memiliki opsi untuk menerima atribut dari IdP eksternal dalam pernyataan SAML. Dalam hal ini, Anda perlu mengkonfigurasi IdP eksternal untuk mengirim atribut yang diinginkan. Jika atribut dari pernyataan SAML juga didefinisikan sebagai atribut ABAC di Pusat Identitas IAM, Pusat Identitas IAM akan mengirimkan nilai dari Penyimpanan Identitasnya sebagai tag https://docs.aws.amazon.com/IAM/latest/UserGuide/id_session-tags.html sesi saat masuk ke Akun AWS.

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 SAML dari IdP eksternal Anda, atribut tersebut langsung dikirim ke Akun AWS ketika pengguna bergabung. Atribut tidak akan tersedia di Pusat Identitas IAM untuk pemetaan.

Topik

- [Aktifkan atribut untuk kontrol akses](#)
- [Pilih atribut Anda untuk kontrol akses](#)
- [Nonaktifkan atribut untuk kontrol akses](#)

Aktifkan atribut untuk kontrol akses

Gunakan prosedur berikut untuk mengaktifkan fitur kontrol atribut untuk akses (ABAC) menggunakan konsol Pusat Identitas IAM.

Note

Jika Anda memiliki kumpulan izin yang sudah ada dan berencana untuk mengaktifkan ABAC di instans Pusat Identitas IAM Anda, pembatasan keamanan tambahan mengharuskan Anda

terlebih dahulu memiliki kebijakan tersebut: `iam:UpdateAssumeRolePolicy`. Pembatasan keamanan tambahan ini tidak diperlukan jika Anda tidak memiliki kumpulan izin yang dibuat di akun Anda.

Jika instans Pusat Identitas IAM dibuat sebelum Desember 2020 dan Anda berencana untuk mengaktifkan ABAC di dalamnya, Anda harus memiliki `iam:UpdateAssumeRolePolicy` kebijakan yang terkait dengan peran administratif Pusat Identitas IAM, terlepas dari apakah Anda memiliki kumpulan 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 informasi Atribut untuk kontrol akses, lalu pilih Aktifkan. Lanjutkan ke prosedur berikutnya untuk mengkonfigurasinya.

Pilih atribut Anda untuk kontrol akses

Gunakan prosedur berikut untuk mengatur atribut untuk konfigurasi ABAC Anda.

 Note

Prosedur ini hanya berlaku jika Anda ingin memetakan atribut dari direktori Pusat Identitas IAM untuk digunakan sebagai tag sesi. Jika Anda meneruskan atribut dari penyedia identitas eksternal (IdP) melalui pernyataan SAML, Anda tidak perlu mengonfigurasi pemetaan atribut di sini. Untuk informasi selengkapnya, lihat [Memilih atribut saat menggunakan penyedia identitas eksternal sebagai sumber identitas Anda](#). Nilai yang ditetapkan dalam pemetaan dari direktori Identity Center mengganti nilai yang ditetapkan dalam pernyataan SAML.

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 Tambah atribut dan masukkan detail Kunci dan Nilai. Di sinilah Anda akan memetakan atribut yang berasal dari sumber identitas Anda ke atribut yang diteruskan IAM Identity Center sebagai tag sesi.

Key ⓘ	Value (optional) ⓘ	Remove
Department	<code>\${path:enterprise.department}</code>	✕
CostCenter	<code>\${path:enterprise.costCenter}</code>	✕
Add new key	Add new value	

Kunci mewakili nama yang Anda berikan pada atribut untuk digunakan dalam kebijakan. Ini bisa berupa nama sewenang-wenang, tetapi Anda perlu menentukan nama yang tepat dalam kebijakan yang Anda buat untuk kontrol akses. Misalnya, katakanlah Anda menggunakan Okta (IdP eksternal) sebagai sumber identitas Anda dan perlu meneruskan data pusat biaya organisasi Anda sebagai tag sesi. Di Key, Anda akan memasukkan nama yang sama CostCenter seperti nama kunci Anda. Penting untuk dicatat bahwa nama mana pun yang Anda pilih di sini, nama itu juga harus diberi nama yang persis sama di nama Anda [aws: PrincipalTag kunci kondisi](#) (yaitu, "ec2:ResourceTag/CostCenter": "\${aws:PrincipalTag/CostCenter}").

Note

Gunakan atribut nilai tunggal untuk kunci Anda, misalnya, **Manager**. Pusat Identitas IAM 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 di [Pemetaan atribut antara Pusat Identitas IAM dan direktori Penyedia Identitas Eksternal](#). 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 adalah `${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 SAML.

5. Pilih Simpan perubahan.

Sekarang setelah Anda mengonfigurasi pemetaan atribut kontrol akses Anda, Anda perlu menyelesaikan proses konfigurasi ABAC. Untuk melakukan ini, buat aturan ABAC Anda dan tambahkan aturan tersebut ke kebijakan berbasis and/or sumber daya kumpulan izin Anda. Ini diperlukan agar Anda dapat memberikan identitas pengguna akses ke AWS sumber daya. Untuk informasi selengkapnya, lihat [Buat kebijakan izin untuk ABAC di Pusat Identitas IAM](#).

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 Kelola atribut.
4. Pada halaman Kelola atribut untuk kontrol akses, pilih Non aktifkan.
5. Di jendela dialog Non aktifkan atribut untuk kontrol akses, tinjau informasi dan ketika siap masukkan **DISABLE**, lalu pilih Konfirmasi.

 Important

Langkah ini menghapus semua atribut dan menghentikan penggunaan atribut untuk kontrol akses saat menyatukan ke Akun AWS terlepas dari apakah ada atribut yang ada dalam pernyataan SAML dari penyedia sumber identitas eksternal.

Buat kebijakan izin untuk ABAC di Pusat Identitas IAM

Anda dapat membuat kebijakan izin yang menentukan siapa yang dapat mengakses AWS sumber daya 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.

aws:PrincipalTag kunci kondisi

Anda dapat menggunakan atribut kontrol akses dalam kumpulan izin (atau peran IAM saat menggunakan manajer akses akun) menggunakan kunci `aws:PrincipalTag` kondisi untuk

membuat aturan kontrol akses. Misalnya, dalam kebijakan berikut, Anda dapat menandai semua sumber daya di organisasi Anda dengan pusat biaya masing-masing. Anda juga dapat menggunakan kumpulan izin tunggal (atau peran IAM saat menggunakan manajer akses akun) 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 dalam AWS sesi ketika pengembang berfederasi. 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.

JSON

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

Saat pengguna bergabung ke Akun AWS melalui Pusat Identitas IAM, atribut kontrol akses yang dikonfigurasi diteruskan sebagai tag sesi. Anda dapat mereferensikan tag sesi ini di kebijakan menggunakan kunci `aws:PrincipalTag/tag-key` kondisi. Kunci kondisi ini didukung di semua jenis kebijakan AWS IAM yang relevan di mana Anda dapat menggunakan kondisi, termasuk kebijakan berbasis identitas, kebijakan berbasis sumber daya, batas izin, kebijakan kontrol layanan (SCP), dan kebijakan titik akhir VPC. Ini memungkinkan Anda membuat keputusan kontrol akses yang halus berdasarkan atribut pengguna di seluruh AWS lingkungan Anda.

Untuk informasi selengkapnya, lihat [aws:PrincipalTag](#) dan [EC2: Memulai atau menghentikan instans berdasarkan pencocokan tag prinsip 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](#).

Memahami peran terkait layanan di Pusat Identitas IAM

[Service-linked peran](#) adalah izin IAM yang telah ditentukan sebelumnya yang memungkinkan Pusat Identitas IAM mendelegasikan dan menegakkan pengguna mana yang memiliki akses masuk tunggal ke tertentu Akun AWS di organisasi Anda. AWS Organizations Layanan memungkinkan fungsionalitas ini dengan menyediakan peran terkait layanan di setiap bagian dalam organisasinya Akun AWS. Layanan ini kemudian memungkinkan AWS layanan lain seperti Pusat Identitas IAM 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 membuat peran terkait layanan di semua akun dalam organisasi di. AWS Organizations Pusat Identitas IAM juga membuat peran terkait layanan yang sama di setiap akun yang kemudian ditambahkan ke organisasi Anda. Peran ini memungkinkan Pusat Identitas IAM mengakses sumber daya setiap akun atas nama Anda. Untuk informasi selengkapnya, lihat [Konfigurasi akses ke Akun AWS](#).

Service-linked peran yang dibuat di masing-masing Akun AWS diberi nama `AWSServiceRoleForSSO`. Untuk informasi selengkapnya, lihat [Menggunakan peran terkait layanan untuk Pusat Identitas IAM](#).

 Catatan

- Jika Anda masuk ke akun AWS Organizations manajemen, akun tersebut menggunakan peran Anda yang saat ini masuk dan bukan peran terkait layanan. Ini mencegah eskalasi hak istimewa.
- Ketika Pusat Identitas IAM melakukan operasi IAM apa pun di akun AWS Organizations manajemen, semua operasi dilakukan menggunakan kredensial prinsipal IAM. Ini memungkinkan log in CloudTrail untuk memberikan visibilitas siapa yang membuat semua perubahan hak istimewa di akun manajemen.

Menyiapkan dan menggunakan AWS portal akses

Portal AWS akses menghubungkan tenaga kerja Anda ke Akun AWS dan aplikasi cloud melalui Pusat Identitas IAM. Administrator mengonfigurasi portal dan mengelola akses pengguna, sementara pengguna akhir masuk sekali untuk mengakses semua sumber daya resmi mereka dengan mulus.

Portal AWS akses menyediakan akses masuk tunggal ke:

- Akun AWS dalam organisasi Anda.
- AWS aplikasi yang dikelola seperti Amazon Quick dan Kiro.
- Aplikasi cloud seperti Office 365, Concur, Salesforce, dan lainnya.

Saat pengguna masuk ke portal, mereka menemukan aplikasi Akun AWS dan aplikasi yang diizinkan untuk diakses tanpa masuk tambahan.

Portal AWS akses juga menyediakan akses ke aplikasi akses AWS akun — di mana pengguna dapat melihat dan mengakses peran IAM yang ditugaskan kepada mereka melalui manajer [akses](#) akun.

Memulai dengan AWS portal akses

Untuk administrator:

Anda memerlukan akses administratif ke instans [organisasi](#) atau instance [???](#) akun Pusat Identitas IAM untuk mengonfigurasi portal AWS akses dan mengelola akses pengguna.

1. Secara opsional menyesuaikan URL portal AWS akses.
2. Tetapkan akses pengguna ke Akun AWS dan aplikasi. Sumber AWS daya yang ditugaskan ditampilkan di portal.

Untuk pengguna akhir:

Administrator Anda harus telah menyelesaikan pen AWS yiapan portal akses dan memberi Anda URL portal dan kredentif masuk Anda.

1. Dapatkan URL portal Anda dari administrator Anda (biasanya `https://your-company.awsapps.com/start`).

2. Masuk menggunakan kredensial yang disediakan oleh administrator Anda.
3. Akses sumber daya Anda di portal Anda.

Konfigurasi AWS portal akses

Sebagai administrator, Anda dapat menyesuaikan portal AWS akses untuk memenuhi kebutuhan organisasi Anda dan memastikan pengguna dapat dengan mudah mengakses sumber daya resmi mereka.

Apa yang dapat Anda konfigurasi

AWS aktivasi portal akses: Siapkan akses pengguna awal ke portal AWS akses, termasuk aktivasi kredensial pengguna dan proses masuk pertama kali.

URL portal AWS akses kustom (opsional): Personalisasi URL portal AWS akses organisasi Anda dari format default (`d-xxxxxxxxxx.awsapps.com/start`) ke subdomain yang lebih mudah dikenali (`your-company.awsapps.com/start`).

Sebelum Anda mulai

Pastikan Anda memiliki akses administratif ke Pusat Identitas IAM, verifikasi bahwa Pusat Identitas IAM diatur sebagai instans [organisasi](#) atau instance [akun](#), dan rencanakan nama subdomain kustom Anda (ini adalah konfigurasi satu kali yang tidak dapat diubah nanti).

Setelah dikonfigurasi, pengguna dapat mengakses portal AWS akses menggunakan URL khusus dan mengikuti proses aktivasi yang telah Anda tetapkan untuk organisasi Anda.

Topik

- [Mengaktifkan AWS portal akses untuk pengguna IAM Identity Center pertama kali](#)
- [Menyesuaikan AWS URL portal akses](#)
- [Konfirmasikan pengguna dapat masuk ke AWS portal akses](#)

Mengaktifkan AWS portal akses untuk pengguna IAM Identity Center pertama kali

Jika ini adalah pertama kalinya Anda mencoba masuk ke portal AWS akses, periksa email Anda untuk petunjuk tentang cara mengaktifkan kredensial pengguna Anda.

Untuk mengaktifkan kredentif pengguna Anda

1. Bergantung pada email yang Anda terima dari perusahaan Anda, pilih salah satu metode berikut untuk mengaktifkan kredensial pengguna Anda sehingga Anda dapat mulai menggunakan portal AWS akses.
 - a. Jika Anda menerima email dengan subjek Undangan untuk bergabung dengan Pusat Identitas AWS IAM, 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 dikirim email dari dukungan TI perusahaan atau administrator TI, ikuti instruksi yang mereka berikan untuk mengaktifkan kredentif pengguna Anda.
2. Setelah Anda mengaktifkan kredentif pengguna dengan memberikan kata sandi baru, portal AWS akses akan membuat Anda masuk secara otomatis. Jika ini tidak terjadi, Anda dapat secara manual masuk ke portal AWS akses dengan menggunakan petunjuk yang disediakan di [Masuk ke AWS portal akses](#).

Menyesuaikan AWS URL portal 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 cari bagian Ringkasan Pengaturan.
3. Pilih tombol Konfigurasi di bawah URL portal AWS akses Anda.

 Note

Jika tombol Ku stomisasi tidak ditampilkan, itu berarti portal AWS akses telah disesuaikan. Menyesuaikan URL portal AWS akses adalah operasi satu kali yang tidak dapat dibalik.

4. Masukkan nama subdomain yang Anda inginkan dan pilih S impan.

Anda sekarang dapat masuk ke Kon AWS sol melalui portal AWS akses Anda dengan URL khusus Anda.

Konfirmasikan pengguna dapat masuk ke AWS portal akses

Langkah-langkah berikut adalah untuk administrator Pusat Identitas IAM untuk mengonfirmasi bahwa pengguna Pusat Identitas IAM dapat masuk ke portal AWS akses dan mengakses. Akun AWS

Masuk ke AWS portal akses

1. Lakukan salah satu dari hal berikut untuk masuk ke Konsol Manajemen AWS.
 - Baru untuk AWS (pengguna root) - Masuk sebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.
 - Sudah menggunakan AWS (kredenSIAL IAM) - Masuk dengan kredenSIAL IAM Anda dan pilih peran admin.
2. Buka konsol [Pusat Identi](#) tas 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 kredensial pengguna Active Directory atau IdP.
 - Jika Anda menggunakan direktori Pusat Identitas default sebagai sumber identitas Anda, masuk dengan menggunakan nama pengguna yang Anda tentukan saat membuat pengguna dan kata sandi baru yang Anda tentukan untuk pengguna tersebut.

6. Di tab Akun, cari Akun AWS dan perluas.
7. Peran yang tersedia untuk Anda ditampilkan. Misalnya, jika Anda diberi kumpulan AdministratorAccess izin dan kumpulan izin Pen agihan, peran tersebut ditampilkan di portal AWS akses. Pilih nama peran IAM yang ingin Anda gunakan untuk sesi.
8. Jika Anda diarahkan ke Konsol AWS Manajemen, Anda berhasil menyelesaikan pengaturan akses ke Akun AWS.

Note

Jika Anda tidak melihat Akun AWS daftar apa pun, kemungkinan pengguna belum ditugaskan ke kumpulan izin untuk akun tersebut. Untuk petunjuk tentang menetapkan pengguna ke kumpulan izin, lihat [Menetapkan akses pengguna atau grup ke Akun AWS](#).

Sekarang setelah Anda mengonfirmasi bahwa Anda dapat masuk menggunakan kredensial Pusat Identitas IAM, beralih ke browser yang Anda gunakan untuk masuk Konsol Manajemen AWS dan keluar dari pengguna root atau kredensial pengguna IAM Anda.

Important

Kami sangat menyarankan Anda menggunakan kredentif pengguna administratif Pusat Identitas IAM saat masuk ke portal AWS akses untuk melakukan tugas administratif alih-alih menggunakan kredentif pengguna IAM atau 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 kumpulan izin hanya melalui Pusat Identitas IAM.

Gunakan AWS portal akses

Anda dapat meluncurkan beberapa aplikasi dengan memilih tab aplikasi Akun AWS atau di portal. Kehadiran ikon aplikasi di portal AWS akses Anda berarti bahwa administrator dari perusahaan Anda telah memberi Anda akses ke Akun AWS aplikasi tersebut. Ini juga berarti bahwa Anda dapat mengakses semua akun atau aplikasi ini dari portal AWS akses tanpa petunjuk masuk tambahan.

Cara menggunakan AWS portal akses

Untuk menggunakan portal AWS akses:

1. Dapatkan URL portal Anda dari administrator Anda (biasanya terlihat seperti `https://your-company.awsapps.com/start`).
2. Masuk menggunakan kredensial yang disediakan oleh administrator Anda.
3. Pilih akun dan aplikasi di portal Anda yang ingin Anda akses.

Administrator mengontrol apa yang Anda lihat di portal berdasarkan peran dan izin Anda. 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

- [Masuk ke AWS portal akses](#)
- [Mengatur ulang AWS akses kata sandi pengguna portal](#)
- [Mendapatkan kredensial pengguna Pusat Identitas IAM untuk AWS CLI atau AWS SDK](#)
- [Membuat tautan pintasan ke Konsol Manajemen AWS tujuan](#)
- [Mendaftarkan perangkat Anda untuk MFA](#)
- [Melihat dan mengakhiri sesi aktif Anda](#)

Masuk ke AWS portal akses

Portal AWS akses menyediakan pengguna Pusat Identitas IAM akses masuk tunggal ke semua aplikasi yang ditugaskan Akun AWS melalui portal web. Berikut ini menguraikan cara masuk ke portal AWS akses, kiat untuk masuk, dan cara keluar dari portal AWS akses.

Prasyarat

Pusat Identitas IAM harus diaktifkan untuk menggunakan portal AWS akses. Untuk informasi selengkapnya, lihat [Aktifkan Pusat Identitas IAM](#).

 Note

Setelah Anda masuk, durasi default untuk sesi portal AWS akses Anda adalah 8 jam. Ketahuilah bahwa administrator dapat [mengubah dur](#)asi sesi ini.

Masuk ke AWS portal akses

Untuk masuk ke AWS portal akses

1. Di jendela browser Anda, tempelkan URL masuk yang diberikan kepada Anda dan pilih Enter. URL terlihat seperti `d-xxxxxxxxxx.awsapps.com/start` atau `your_subdomain.awsapps.com/start`. Kami menyarankan Anda menandai tautan ini ke portal sekarang sehingga Anda dapat dengan cepat mengaksesnya nanti.
2. Masuk menggunakan kredensial masuk perusahaan standar Anda.

 Note

Jika administrator Anda mengirimkan Anda kata sandi satu kali (OTP) email dan ini adalah pertama kalinya Anda masuk, masukkan kata sandi itu. Setelah Anda masuk, Anda harus membuat kata sandi baru untuk masuk di masa mendatang.

Jika Anda diminta memasukkan kode Verifikasi, periksa email Anda, lalu salin dan tempel kode tersebut ke halaman masuk.

 Note

Kode verifikasi biasanya dikirim melalui email, tetapi metode pengiriman dapat bervariasi. Periksa dengan administrator Anda untuk detailnya.

3. Setelah masuk, Anda dapat mengakses aplikasi apa pun Akun AWS yang ditampilkan di portal.

Perangkat tepercaya

Saat Anda memilih opsi Ini adalah perangkat tepercaya dari halaman masuk, Pusat Identitas IAM menganggap semua login di masa mendatang dari perangkat tersebut sebagai resmi. Ini berarti bahwa Pusat Identitas IAM tidak akan menampilkan 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 diberi alamat IP yang tidak dikenal.

Kiat masuk untuk AWS portal akses

Berikut adalah beberapa tips untuk membantu Anda mengelola pengalaman portal AWS akses Anda.

- Kadang-kadang, Anda mungkin perlu keluar dan masuk kembali ke portal AWS akses. Ini mungkin diperlukan untuk mengakses aplikasi baru yang baru saja ditugaskan administrator kepada Anda. Namun, ini tidak diperlukan, 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 selesai menggunakan aplikasi, Anda dapat menutup aplikasi atau keluar dari portal AWS akses. Menutup aplikasi 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 kredensial Anda dari sesi browser.
- Setelah Anda masuk ke portal AWS akses, Anda dapat beralih ke peran. Mengalihkan peran sementara mengesampingkan izin pengguna asli Anda dan sebagai gantinya memberi Anda izin yang ditetapkan untuk peran tersebut. Untuk informasi selengkapnya, lihat [Ber alih ke peran \(konsol\)](#).

Keluar dari AWS portal akses

Saat Anda keluar dari portal, kredensial Anda sepenuhnya dihapus dari sesi browser. Untuk informasi selengkapnya, [lihat Keluar dari portal AWS akses](#) di AWS Sign-In panduan.

Untuk keluar dari AWS portal 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.

Mengatur ulang AWS akses kata sandi pengguna portal

Portal AWS akses menyediakan [pengguna Pusat Identitas](#) IAM akses masuk tunggal ke semua AWS akun yang ditugaskan dan aplikasi cloud melalui portal web. Portal AWS akses berbeda dari [Konsol Manajemen AWS](#), yang merupakan kumpulan konsol layanan untuk mengelola AWS sumber daya.

Gunakan prosedur ini untuk mengatur ulang kata sandi pengguna Pusat Identitas IAM Anda untuk portal AWS akses. Pelajari lebih [lanjut tentang Jenis Pengguna](#) di Panduan AWS Sign-In Pengguna.

Pertimbangan-pertimbangan

Fungsi reset kata sandi untuk portal AWS akses hanya tersedia untuk pengguna instans Identity Center yang menggunakan direktori Identity Center atau [AWS Managed Microsoft AD](#) sebagai sumber identitasnya. Jika pengguna Anda terhubung ke penyedia identitas eksternal atau Konektor [AD](#), pengaturan ulang kata sandi pengguna harus dilakukan dari penyedia identitas eksternal atau terhubungActive Directory.

- Jika sumber identitas Anda adalah direktori Pusat Identitas IAM, lihat [Persyaratan kata sandi saat mengelola identitas di Pusat Identitas IAM](#).
- Jika sumber identitas Anda adalah AWS Managed Microsoft AD, lihat Persyaratan [kata sandi saat mengatur ulang kata sandi di AWS Managed Microsoft AD](#).

Untuk mengatur ulang kata sandi Anda ke AWS portal 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 menerima email undangan untuk bergabung dengan Pusat Identitas AWS tas IAM yang menyertakan URL masuk tertentu ke portal akses. AWS Atau, administrator Anda mungkin telah langsung memberi Anda kata sandi satu kali dan URL portal AWS akses. Jika Anda tidak dapat menemukan informasi ini, mintalah administrator Anda untuk mengirimkannya kepada Anda.

Untuk informasi selengkapnya tentang masuk ke portal AWS akses, lihat [Masuk AWS ke portal 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 reset kata sandi telah dikirim. Pilih Lanjutkan.
5. Anda akan menerima email dari `no-reply@signin.aws` dengan subjek Reset kata sandi yang diminta. Di email Anda, pilih Reset 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` dengan baris subjek Kata sandi diperbarui.

Note

Administrator dapat mengatur ulang kata sandi Anda dengan mengirimkan 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, lihat [Setel ulang kata sandi pengguna Pusat Identitas IAM untuk pengguna akhir](#).

Mendapatkan kredensial pengguna Pusat Identitas IAM untuk AWS CLI atau AWS SDK

Anda dapat mengakses AWS layanan secara terprogram dengan menggunakan Perangkat Pengembangan AWS Command Line Interface AWS Perangkat Lunak (SDK) dengan kredentif pengguna dari Pusat Identitas IAM. Topik ini menjelaskan cara mendapatkan kredensial sementara untuk pengguna di Pusat Identitas IAM.

Portal AWS akses memberi pengguna Pusat Identitas IAM 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 kredensial sementara. Anda kemudian dapat menggunakan kredensial, juga disebut sebagai kredentif pengguna Pusat Identitas IAM, di AWS CLI AWS SDK atau untuk mengakses sumber daya dalam 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. Untuk informasi tentang AWS SDK, lihat Panduan Refer [AWS ensi SDK dan Alat](#).

Note

Pengguna di Pusat Identitas IAM berbeda dari pengguna [IAM](#). Pengguna IAM diberikan kredensial jangka panjang ke AWS sumber daya. Pengguna di Pusat Identitas IAM diberikan kredensial sementara. Sebaiknya gunakan kredensial sementara sebagai praktik terbaik keamanan untuk mengakses kredensial Anda Akun AWS karena kredensial ini dibuat setiap kali Anda masuk.

Prasyarat

Untuk mendapatkan kredensial sementara untuk pengguna Pusat Identitas IAM Anda, Anda memerlukan yang berikut:

- 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 dengan IAM Identity Center](#)
- Akses pengguna ke Akun AWS — Untuk memberikan izin kepada pengguna Pusat Identitas IAM untuk mengambil kredensial sementara mereka, Anda atau administrator harus menetapkan pengguna Pusat Identitas IAM ke kumpulan [izin](#). Kumpulan izin disimpan di Pusat Identitas IAM dan menentukan tingkat akses yang dimiliki pengguna Pusat Identitas IAM ke Akun AWS. Jika administrator Anda membuat pengguna Pusat Identitas IAM untuk Anda, minta mereka untuk menambahkan akses ini untuk Anda. Untuk informasi selengkapnya, lihat [Menetapkan akses pengguna atau grup ke Akun AWS](#).
- AWS CLI diinstal - Untuk menggunakan kredensial sementara, Anda harus menginstal AWS CLI. Untuk petunjuk, lihat Meng [instal atau memperbarui versi terbaru AWS CLI](#) di Panduan AWS CLI Pengguna.

Pertimbangan-pertimbangan

Sebelum Anda menyelesaikan langkah-langkah untuk mendapatkan kredensial 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 kumpulan izin, Pusat Identitas IAM membuat peran IAM yang sesuai dari kumpulan izin. Peran IAM yang dibuat oleh kumpulan izin berbeda dari peran IAM yang dibuat dengan AWS Identity and Access Management cara berikut:
 - Pusat Identitas IAM memiliki dan mengamankan peran yang dibuat oleh kumpulan izin. Hanya IAM Identity Center yang dapat memodifikasi peran ini.
 - Hanya pengguna di Pusat Identitas IAM yang dapat mengambil peran yang sesuai dengan kumpulan izin yang ditetapkan. Anda tidak dapat menetapkan akses kumpulan 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 kredensial sementara untuk peran yang Anda buat di IAM, lihat [Menggunakan kredensial keamanan sementara dengan AWS CLI](#) di Panduan AWS Identity and Access Management Pengguna.

- Anda dapat mengatur durasi sesi untuk kumpulan izin — Setelah Anda masuk ke portal AWS akses, kumpulan izin yang ditugaskan pengguna Pusat Identitas IAM Anda akan muncul sebagai peran yang tersedia. Pusat Identitas IAM membuat sesi terpisah untuk peran ini. Sesi ini bisa dari satu hingga 12 jam, tergantung durasi sesi yang dikonfigurasi untuk kumpulan izin. Durasi sesi default adalah satu jam. Untuk informasi selengkapnya, lihat [Tetapkan durasi sesi untuk Akun AWS](#).

Mendapatkan dan menyegarkan kredensi sementara

Anda bisa mendapatkan dan menyegarkan kredensi sementara untuk pengguna Pusat Identitas IAM secara otomatis atau manual.

Topik

- [Penyegaran kredensi otomatis \(disarankan\)](#)
- [Penyegaran kredensi manual](#)

Penyegaran kredensi otomatis (disarankan)

Penyegaran kredensi 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 ditugaskan untuk setiap peran Akun AWS.

Untuk mengakses peran yang dibuat untuk pengguna Pusat Identitas IAM 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 kredensial sementara dan menyegarkan kredensial secara otomatis.

Untuk informasi selengkapnya, lihat Meng [onfigurasi profil Anda dengan `aws configure sso wizard`](#) di Panduan AWS Command Line Interface Pengguna.

Untuk mendapatkan kredentif sementara yang secara otomatis menyegarkan

1. Masuk ke portal AWS akses dengan menggunakan URL masuk tertentu yang disediakan oleh administrator Anda. Jika Anda membuat pengguna Pusat Identitas IAM, ki AWS rim undangan email yang menyertakan URL masuk Anda. Untuk informasi selengkapnya, [lihat Masuk AWS ke portal akses](#) di Panduan AWS Sign-In Pengguna.
2. Di tab Akun, 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 AWS daftar apa pun, kemungkinan Anda belum ditugaskan ke kumpulan izin untuk akun tersebut. Dalam hal ini, hubungi administrator Anda dan minta mereka untuk menambahkan akses ini untuk Anda. Untuk informasi selengkapnya, lihat [Menetapkan akses pengguna atau grup ke Akun AWS](#).

3. Di bawah nama akun, kumpulan izin yang ditugaskan pengguna Pusat Identitas IAM Anda muncul sebagai peran yang tersedia. Misalnya, jika pengguna Pusat Identitas IAM Anda ditugaskan ke `PowerUserAccess` kumpulan izin untuk akun, peran tersebut muncul di portal AWS akses sebagai `PowerUserAccess`.
4. Bergantung pada pilihan Anda di samping nama peran, pilih tombol Ak ses atau pilih Baris perintah atau akses terprogram.

5. Di kotak dialog Dapatkan kredensial, pilih macOS dan Linux, Windows, atau PowerShell, tergantung pada sistem operasi tempat Anda menginstallnya AWS CLI.
6. Di bawah kredensial Pusat Identitas AWS IAM (Direkomendasikan), SSO Start URL dan Anda SSO Region akan ditampilkan. Nilai-nilai ini diperlukan untuk mengonfigurasi profil yang diaktifkan Pusat Identitas IAM dan sso-session ke profil Anda AWS CLI. Untuk menyelesaikan konfigurasi ini, ikuti petunjuk di [Konfigurasi profil Anda dengan aws configure sso wizard](#) di Panduan AWS Command Line Interface Pengguna.

Lanjutkan menggunakan yang AWS CLI diperlukan untuk Anda Akun AWS sampai kredensialnya kedaluwarsa.

Penyegaran kredensi manual

Anda dapat menggunakan metode penyegaran kredensial manual untuk mendapatkan kredensial sementara untuk peran yang terkait dengan kumpulan izin tertentu dalam suatu peran tertentu Akun AWS. Untuk melakukannya, Anda menyalin dan menempelkan perintah yang diperlukan untuk kredensial sementara. Dengan metode ini, Anda harus menyegarkan kredensial sementara secara manual.

Anda dapat menjalankan AWS CLI perintah hingga kredensial sementara Anda kedaluwarsa.

Untuk mendapatkan kredensial yang Anda refresh secara manual

1. Masuk ke portal AWS akses dengan menggunakan URL masuk tertentu yang disediakan oleh administrator Anda. Jika Anda membuat pengguna Pusat Identitas IAM, ki AWS rim undangan email yang menyertakan URL masuk Anda. Untuk informasi selengkapnya, [lihat Masuk AWS ke portal akses](#) di Panduan AWS Sign-In Pengguna.
2. Di tab Akun, cari Akun AWS dari mana Anda ingin mengambil kredensial akses dan perluas untuk menampilkan nama peran IAM (misalnya Administrator). Bergantung pada pilihan Anda di samping nama peran IAM, pilih tombol Akses atau pilih Baris perintah atau akses terprogram.

Note

Jika Anda tidak melihat Akun AWS daftar apa pun, kemungkinan Anda belum ditugaskan ke kumpulan izin untuk akun tersebut. Dalam hal ini, hubungi administrator Anda dan minta mereka untuk menambahkan akses ini untuk Anda. Untuk informasi selengkapnya, lihat [Menetapkan akses pengguna atau grup ke Akun AWS](#).

3. Di kotak dialog Dapatkan kredensial, pilih macOS dan Linux , Windows PowerShell, atau, tergantung pada sistem operasi tempat Anda menginstal AWS CLI.
4. Pilih salah satu opsi berikut:
 - Opsi 1: Tetapkan variabel AWS lingkungan

Pilih opsi ini untuk mengganti semua pengaturan kredensial, termasuk pengaturan apa pun dalam `credentials` file dan `config` file. Untuk informasi selengkapnya, lihat Variabel [lingkungan untuk mengonfigurasi AWS CLI](#) di 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 kredensial Anda

Pilih opsi ini untuk menjalankan perintah dengan kumpulan kredensial 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 kredensial ini, tentukan `--profile` opsi dalam AWS CLI perintah Anda. Ini mempengaruhi semua lingkungan yang menggunakan file kredensial 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 lebih lanjut, lihat [Alat untuk Membangun di AWS](#).

Untuk menggunakan opsi ini, salin nilai ke clipboard Anda, tempelkan nilai ke dalam kode Anda, dan tetapkan ke variabel yang sesuai untuk SDK Anda. Untuk informasi selengkapnya, lihat dokumentasi untuk API SDK spesifik Anda.

Membuat tautan pintasan ke Konsol Manajemen AWS tujuan

Tautan pintasan yang dibuat di portal AWS akses membawa pengguna Pusat Identitas IAM ke tujuan tertentu di Konsol Manajemen AWS, dengan kumpulan izin tertentu, dan di tempat tertentu Akun AWS.

Tautan pintasan menghemat waktu untuk Anda dan kolaborator Anda. Alih-alih menavigasi ke URL tujuan yang diinginkan di Konsol Manajemen AWS (misalnya, halaman instance bucket Amazon S3) melalui beberapa halaman, termasuk portal AWS akses, Anda dapat menggunakan tautan pintasan untuk mencapai tujuan yang sama secara otomatis.

Opsi tujuan tautan pintasan

Tautan pintasan memiliki tiga opsi tujuan, tercantum di sini berdasarkan prioritas:

- (Opsional) URL tujuan apa pun yang Konsol Manajemen AWS ditentukan dalam tautan pintasan. Misalnya, halaman instance bucket Amazon S3.
- (Opsional) URL status Administrator-configured relai untuk set izin yang dimaksud. Untuk informasi selengkapnya tentang pengaturan status relai, lihat [Atur status relai untuk akses cepat ke Konsol Manajemen AWS](#).
- Konsol Manajemen AWS rumah. Tujuan default jika Anda tidak menentukan satu.

Note

Navigasi otomatis ke tujuan hanya berhasil jika Anda diautentikasi dengan Pusat Identitas IAM dan memiliki set izin yang diperlukan ditetapkan untuk AWS akun dan URL tujuan.

Portal AWS akses menyertakan tombol **Buat pintasan** yang membantu Anda membuat tautan pintasan yang dapat dibagikan. Jika Anda berencana untuk menentukan URL tujuan (opsi pertama dalam daftar sebelumnya), Anda dapat menyalin URL ke clipboard untuk membagikannya.

Buat tautan pintasan di AWS portal akses

1. Saat masuk ke portal AWS akses, pilih tab **Akun** dan kemudian pilih tombol **Buat pintasan**.
2. Di kotak dialog:
 - a. Pilih Akun AWS menggunakan ID akun atau nama akun. Saat Anda mengetik, menu drop-down menampilkan ID akun yang cocok dan nama yang dapat Anda akses. Anda hanya dapat memilih akun yang dapat Anda akses.
 - b. Secara opsional pilih peran IAM dari daftar drop-down. Ini adalah kumpulan izin yang ditetapkan untuk Anda untuk akun yang dipilih. Jika Anda mengabaikan memilih peran, pengguna akan diminta untuk memilih satu yang ditugaskan kepada mereka untuk akun yang dipilih saat menggunakan tautan pintasan.

 Note

Anda tidak dapat memberikan akses baru dengan tautan pintasan. Tautan pintasan hanya berfungsi dengan kumpulan izin yang sudah ditetapkan untuk pengguna. Jika pengguna tidak memiliki kumpulan izin yang diperlukan yang ditetapkan untuk akun dan URL tujuan, mereka ditolak aksesnya.

- c. Secara opsional masukkan URL tujuan portal AWS akses. Jika Anda menghilangkan memasukkan URL, tujuan secara otomatis ditentukan saat menggunakan tautan pintasan, berdasarkan opsi tujuan tautan pintasan yang disebutkan sebelumnya.
- d. Tautan pintasan Anda dihasilkan di bagian bawah kotak dialog, berdasarkan masukan Anda. Pilih tombol Salin URL. Anda sekarang dapat membuat bookmark dengan tautan pintasan yang disalin atau membagikannya dengan kolaborator Anda yang memiliki akses ke akun yang sama dengan kumpulan izin yang sama atau kumpulan izin lain yang memadai.

Membangun aman Konsol Manajemen AWS tautan pintasan dengan pengkodean URL

Semua nilai parameter URL, termasuk ID akun, nama kumpulan izin, dan URL tujuan, harus URL-encoded.

Tautan pintasan memperluas URL portal AWS akses dengan jalur berikut:

/#/console?

account_id=[*account_ID*]&role_name=[*permission_set_name*]&destination=[*destination*]

URL lengkap di AWS partisi klasik mengikuti pola ini:

Titik akhir IPv4:

https://[*your_subdomain*].awsapps.com/start/#/console?

account_id=[*account_ID*]&role_name=[*permission_set_name*]&destination=[*destination*]

Dual-stack titik akhir

https://[*identity_center_instance_id*].portal.[*region*].app.aws/#/console?

account_id=[*account_ID*]&role_name=[*permission_set_name*]&destination=[*destination*]

Berikut adalah contoh tautan pintasan yang menandatangani pengguna ke akun 123456789012 dengan kum S3FullAccess pulan izin, dan membawanya ke halaman beranda konsol S3:

- Titik akhir IPv4: `https://example.awsapps.com/start/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.aws.amazon.com%2Fs3%2Fhome`
- Dual-stack titik akhir: `https://ssoins-1234567890abcdef.portal.us-east-1.app.aws/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.aws.amazon.com%2Fs3%2Fhome`
- (AWS GovCloud (US) Region) Titik akhir IPv4: `https://start.us-gov-west-1.us-gov-home.awsapps.com/directory/example/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.amazonaws-us-gov.com%2Fs3%2Fhome`
- (AWS GovCloud (US) Region) Dual-stack titik akhir: `https://ssoins-1234567890abcdef.portal.us-gov-west-1.app.aws/#/console?account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.amazonaws-us-gov.com%2Fs3%2Fhome`

Mendaftarkan perangkat Anda untuk MFA

Untuk pengguna di direktori Identity Center, gunakan prosedur berikut dalam portal AWS akses untuk mendaftarkan perangkat baru Anda untuk otentikasi multi-faktor (MFA).

Important

MFA di Pusat Identitas IAM saat ini tidak didukung untuk penyedia identitas [eksternal](#).

Sebelum Anda mulai

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](#).

Daftarkan perangkat Anda

Untuk mendaftarkan perangkat Anda untuk digunakan dengan MFA

1. Masuk ke portal AWS akses Anda. Untuk informasi selengkapnya, lihat [Masuk ke AWS portal akses](#).
2. Di dekat kanan atas halaman, pilih perangkat MFA.
3. Pada halaman perangkat Multi-factor otentikasi (MFA), pilih Daftarkan perangkat.

Note

Jika opsi Daftar perangkat MFA berwarna abu-abu, hubungi administrator Anda untuk bantuan mendaftarkan perangkat Anda.

4. Pada halaman Daftar perangkat MFA, pilih salah satu jenis perangkat MFA berikut, dan ikuti petunjuknya:
 - Aplikasi otentikator
 1. Pada halaman Siapkan aplikasi otentikator, 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 otentikator 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 otentikator:
 - i. Pilih Tampilkan kode QR, lalu gunakan aplikasi untuk memindai kode QR. Misalnya, Anda dapat memilih ikon kamera atau memilih opsi yang mirip dengan Pindai kode. 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 Pusat Identitas IAM, sebaiknya simpan 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 tersebut terjadi, Anda dapat dengan cepat mengonfigurasi ulang aplikasi untuk menggunakan konfigurasi MFA yang sama.

3. Pada halaman **Siapkan aplikasi otentikator**, 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 dengan AWS.

- **Kunci keamanan atau otentikator Built-in**

1. Pada halaman **Daftarkan kunci keamanan pengguna Anda**, ikuti petunjuk yang disediakan oleh browser atau platform Anda.

 Note

Pengalaman 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 **Ubah nama**, masukkan nama baru, lalu pilih **Simpan**.

Melihat dan mengakhiri sesi aktif Anda

Anda dapat menggunakan portal AWS akses untuk melihat daftar sesi aktif Anda, dan jika diperlukan, akhiri satu sesi atau lebih.

Akhiri sesi aktif menggunakan AWS portal akses

1. Masuk ke portal AWS akses Anda. Untuk informasi selengkapnya, lihat [Masuk ke AWS portal akses](#).
2. Di dekat kanan atas halaman, pilih Keamanan.
3. Pada halaman Keamanan, angka dalam tanda kurung di sebelah Sesi aktif menunjukkan berapa banyak sesi aktif yang Anda miliki. Pilih kotak centang di samping setiap sesi yang ingin Anda akhiri, lalu pilih Akhiri sesi.

Tip

Untuk sesi latar belakang pengguna, Anda dapat mencari sesi berdasarkan Nama Sumber Daya Amazon (ARN) dari pekerjaan yang menggunakan sesi tersebut. Dalam daftar Jenis sesi, pilih Sesi latar belakang pengguna, lalu masukkan ARN pekerjaan di kotak pencarian.

Anda hanya dapat mengakhiri sesi aktif yang dimuat. Jika Anda memiliki banyak sesi, pilih Muat sesi yang lebih aktif untuk menampilkan sesi tambahan.

4. Pilih kotak centang di samping setiap sesi yang ingin Anda akhiri, lalu pilih Akhiri sesi.
5. Kotak dialog muncul yang mengonfirmasi bahwa Anda mengakhiri sesi aktif. Tinjau informasi, dan jika Anda ingin melanjutkan, ketik `confirm`, lalu pilih Akhiri sesi.
6. Anda dikembalikan ke daftar sesi aktif Anda. Pesan pemberitahuan hijau muncul untuk menunjukkan bahwa sesi yang dipilih berhasil diakhiri.

Menggunakan Pusat Identitas IAM di beberapa Wilayah AWS

Topik ini menjelaskan cara menggunakan AWS IAM Identity Center di beberapa Wilayah AWS. Pelajari cara mereplikasi instans Anda ke Wilayah tambahan, mengelola akses dan sesi tenaga kerja, menerapkan aplikasi, dan memelihara akses akun selama gangguan layanan.

Saat Anda mengaktifkan instance organisasi dari Pusat Identitas IAM, Anda memilih satu Wilayah AWS (Wilayah utama). Anda dapat mereplikasi instance ini ke tambahan Wilayah AWS selama pembuatan instance atau setelahnya, jika memenuhi prasyarat tertentu. Pusat Identitas IAM secara otomatis mereplikasi identitas tenaga kerja, kumpulan izin, penugasan pengguna dan grup, sesi, dan metadata lainnya dari Wilayah utama ke Wilayah tambahan yang dipilih.

Manfaat dukungan Multi-wilayah

Mereplikasi Pusat Identitas IAM ke tambahan Wilayah AWS memberikan dua manfaat utama:

- Peningkatan ketahanan Akun AWS akses — Tenaga kerja Anda dapat mengakses Akun AWS mereka meskipun instans Pusat Identitas IAM mengalami gangguan layanan di Wilayah utamanya. Ini berlaku untuk akses dengan izin yang disediakan sebelum gangguan.
- Fleksibilitas yang ditingkatkan dalam memilih Wilayah AWS penerapan untuk aplikasi terkelola — Anda AWS dapat menerapkan aplikasi terkelola di Wilayah pilihan Anda untuk memenuhi persyaratan residensi data aplikasi dan meningkatkan kinerja melalui kedekatan dengan pengguna. Aplikasi yang digunakan di Wilayah tambahan mengakses identitas tenaga kerja yang direplikasi secara lokal untuk kinerja dan keandalan yang optimal.

Prasyarat dan pertimbangan

Sebelum mereplikasi instance Pusat Identitas IAM, pastikan persyaratan berikut terpenuhi:

- Jenis instans - Instans Pusat Identitas IAM Anda harus berupa instance [???](#) organisasi. Multi-Region dukungan tidak tersedia dalam contoh [akun](#).
- Sumber identitas - Instans Pusat Identitas IAM Anda harus terhubung ke penyedia identitas eksternal (IdP), seperti [Okta](#), atau menggunakan direktori Pusat [Identitas](#) sebagai sumber identitas. Multi-Region dukungan tidak tersedia untuk instans yang menggunakan [Active Directory](#) sebagai sumber identitas.

- AWS Wilayah - Multi-Region dukungan tersedia di Wilayah [komersial yang diaktifkan secara default](#) di wilayah Anda Akun AWS. Opt-in Wilayah saat ini tidak didukung.
- Jenis kunci KMS untuk enkripsi saat diam - Instans Pusat Identitas IAM Anda harus dikonfigurasi dengan kunci KMS yang dikelola [pelanggan multi-wilayah](#). Kunci KMS harus berada di AWS akun yang sama dengan Pusat Identitas IAM. Untuk informasi selengkapnya, lihat [Menerapkan kunci KMS yang dikelola pelanggan di AWS IAM Identity Center](#).
- AWS kompatibilitas aplikasi terkelola - Kunjungi tabel aplikasi [the section called “Aplikasi yang dapat Anda gunakan dengan IAM Identity Center”](#) untuk mengonfirmasi dua persyaratan aplikasi berikut:
 - Semua aplikasi terkel AWS yang digunakan oleh organisasi Anda harus mendukung Pusat Identitas IAM yang dikonfigurasi dengan kunci KMS yang dikelola pelanggan.
 - Aplikasi AWS terkelola yang ingin Anda terapkan di Wilayah tambahan harus mendukung jenis penerapan ini.
- Kompatibilitas IdP eksternal (hanya penyedia identitas eksternal) - Jika Anda menggunakan penyedia identitas eksternal, IdP harus mendukung beberapa URL layanan konsumen (ACS) assertion untuk sepenuhnya memanfaatkan dukungan Multi-wilayah. Ini adalah fitur SAML yang didukung oleh IdPs seperti Okta, Microsoft Entra ID, PingFederate, PingOne, dan JumpCloud.

Jika Anda menggunakan IdP yang tidak mendukung beberapa URL ACS, misalnya, sebaiknya Google Workspace Anda bekerja sama dengan vendor IdP Anda untuk mengaktifkan fitur ini. Prasyarat ini tidak berlaku saat menggunakan direktori Identity Center sebagai sumber identitas. Untuk opsi yang tersedia tanpa beberapa URL ACS, lihat [the section called “Penggunaan AWS aplikasi yang dikelola tanpa beberapa URL ACS”](#) dan [the section called “Akun AWS akses ketahanan tanpa beberapa URL ACS”](#).

Memilih Wilayah Tambahan

Saat memilih Wilayah tambahan di antara Wilayah komersial yang diaktifkan secara default, pertimbangkan faktor-faktor berikut:

- Persyaratan kepatuhan — Jika Anda perlu menjalankan aplikasi AWS terkelola yang mengakses kumpulan data terbatas pada Wilayah tertentu untuk alasan kepatuhan, pilih Wilayah tempat kumpulan data berada.
- Optimalisasi kinerja — Jika residensi data bukan faktor, pilih Wilayah yang paling dekat dengan pengguna aplikasi Anda untuk mengoptimalkan pengalaman mereka.

- Dukungan aplikasi — Verifikasi bahwa AWS aplikasi yang Anda butuhkan tersedia di Wilayah yang Anda pilih.
- Akun AWS ketahanan akses — Untuk kelangsungan akses ke Akun AWS s, pilih Wilayah yang secara geografis jauh dari Wilayah utama instans Pusat Identitas IAM Anda.

 Note

IAM Identity Center memiliki kuota pada jumlah Wilayah AWS. Untuk informasi selengkapnya, lihat [the section called “Kuota tambahan”](#).

Mereplikasi Pusat Identitas IAM ke Wilayah tambahan

Jika lingkungan Anda memenuhi [prasyarat](#), seperti mengonfigurasi Pusat Identitas IAM dengan kunci KMS yang dikelola pelanggan multi-wilayah, selesaikan langkah-langkah berikut untuk mereplikasi instance Pusat Identitas IAM Anda ke Wilayah tambahan. Wilayah utama Anda terus beroperasi secara normal selama dan setelah langkah-langkah ini.

 Note

Jika Anda membuat instance organisasi baru, Anda dapat mengaktifkan Multi-wilayah selama pembuatan instance. Untuk informasi selengkapnya, lihat [Aktifkan Pusat Identitas IAM](#).

Langkah 1: Buat kunci replika di Wilayah tambahan

Sebelum mereplikasi Pusat Identitas IAM ke Wilayah, Anda harus terlebih dahulu membuat kunci replika kunci KMS yang dikelola pelanggan di Wilayah tersebut dan mengonfigurasi kunci replika dengan izin yang diperlukan untuk operasi Pusat Identitas IAM. Untuk petunjuk tentang membuat kunci replika multi-wilayah, lihat [Membuat kunci replika multi-wilayah](#).

Pendekatan yang disarankan untuk izin kunci KMS adalah menyalin kebijakan kunci dari kunci utama, yang memberikan izin yang sama yang telah ditetapkan untuk Pusat Identitas IAM di Wilayah utama. Atau, Anda dapat menentukan kebijakan Region-specific utama, meskipun pendekatan ini meningkatkan kompleksitas pengelolaan izin di seluruh Wilayah dan mungkin memerlukan koordinasi tambahan saat memperbarui kebijakan di masa mendatang.

 Note

AWS KMS tidak menyinkronkan kebijakan kunci KMS Anda di seluruh Wilayah kunci KMS Multi-wilayah Anda. Agar kebijakan kunci KMS tetap sinkron di seluruh Wilayah kunci KMS, Anda harus menerapkan perubahan di setiap Wilayah secara individual.

Langkah 2: Tambahkan Wilayah di Pusat Identitas IAM

Menambahkan Wilayah di Pusat Identitas IAM memicu replikasi otomatis data Pusat Identitas IAM ke Wilayah tersebut. Replikasi tidak sinkron dengan konsistensi akhirnya. Tab berikut memberikan instruksi untuk melakukan ini di Konsol Manajemen AWS dan AWS CLI.

Console

Untuk menambahkan Wilayah

1. Buka konsol [Pusat Identi](#) tas IAM.
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Pilih tab Manajemen.
4. Di bagian Regions for IAM Identity Center, pilih Tam bah Wilayah.
5. Di bagian Wilayah AWS tersedia untuk replikasi, pilih pilihan Anda Wilayah AWS. Jika Region tidak muncul dalam daftar, maka tidak tersedia untuk replikasi karena kunci KMS belum direplikasi di sana. Untuk informasi selengkapnya, lihat [the section called “Menerapkan kunci KMS yang dikelola pelanggan”](#).
6. Pilih Tam bah Wilayah.
7. Di bagian Regions for IAM Identity Center, pantau status Wilayah. Gunakan tombol Refresh (panah melingkar) untuk memeriksa status Wilayah terbaru sesuai kebutuhan. Setelah replikasi selesai, lanjutkan ke Langkah 2.

AWS CLI

Untuk menambahkan Wilayah

```
aws sso-admin add-region \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --region-name eu-west-1
```


Untuk memeriksa status Wilayah saat ini

```
aws sso-admin describe-region \
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \
  --region-name eu-west-1
```

Ketika status Wilayah AKTIF, Anda dapat melanjutkan ke Langkah 2.

Durasi replikasi awal ke Wilayah tambahan tergantung pada jumlah data dalam instance Pusat Identitas IAM Anda. Perubahan inkremental berikutnya direplikasi dalam hitungan detik dalam banyak kasus.

Langkah 3 (hanya penyedia identitas eksternal): Perbarui pengaturan IdP eksternal

Langkah ini hanya berlaku jika Anda menggunakan penyedia identitas eksternal (IdP). Jika Anda menggunakan direktori Identity Center sebagai sumber identitas Anda, lewati ke Langkah 4.

Ikuti tutorial untuk IdP eksternal Anda [Tutorial sumber identitas](#) untuk langkah-langkah berikut:

Langkah 3.a: Tambahkan URL Assertion Consumer Service (ACS) ke IdP eksternal Anda

Langkah ini memungkinkan masuk langsung ke setiap Wilayah tambahan dan diperlukan untuk mengaktifkan masuk ke aplikasi terkelola yang digunakan di Wilayah tersebut dan untuk akses ke Akun AWS s melalui Wilayah tersebut. AWS Untuk mempelajari di mana menemukan URL ACS, lihat [Titik akhir ACS di primer dan tambahan Wilayah AWS](#).

Langkah 3.b (Opsional): Jadikan Portal akses AWS tersedia di portal IdP eksternal

Jadi Portal akses AWS kan di Wilayah tambahan tersedia sebagai aplikasi bookmark di portal IdP eksternal. Aplikasi bookmark hanya berisi tautan (URL) ke tujuan yang diinginkan dan mirip dengan bookmark browser. Anda dapat menemukan Portal akses AWS URL di konsol dengan memilih Lihat semua Portal akses AWS URL di bagian Wilayah untuk Pusat Identitas IAM. Untuk informasi selengkapnya, lihat [the section called “AWS akses titik akhir portal di primer dan tambahan Wilayah AWS”](#).

Pusat Identitas IAM mendukung IdP-initiated SAML SSO di setiap Wilayah tambahan, tetapi eksternal IdPs biasanya mendukung ini hanya dengan satu URL ACS. Untuk kontinuitas, kami sarankan agar URL ACS Wilayah utama tetap digunakan untuk IdP-initiated SAML SSO dan mengandalkan aplikasi bookmark dan bookmark browser untuk akses ke Wilayah tambahan.

Langkah 4: Konfirmasikan daftar izin firewall dan gateway

Tinjau daftar izin domain Anda di firewall atau gateway, dan perbarui berdasarkan daftar izin yang terdokumentasi. [???](#)

Langkah 5: Berikan informasi kepada pengguna

Berikan pengguna Anda informasi tentang pengaturan baru, termasuk Portal akses AWS URL di Wilayah tambahan dan cara menggunakan Wilayah tambahan. Tinjau bagian berikut untuk detail yang relevan:

- [the section called “Akses tenaga kerja melalui Wilayah tambahan”](#)
- [the section called “Failover ke Wilayah tambahan untuk akses Akun AWS ”](#)
- [the section called “Menyebarkan dan mengelola aplikasi di berbagai aplikasi Wilayah AWS”](#)

Wilayah berubah setelah menambahkan Wilayah pertama

Anda dapat menambah dan menghapus Wilayah tambahan. Wilayah utama tidak dapat dihapus selain dengan menghapus seluruh instance Pusat Identitas IAM. Untuk informasi selengkapnya tentang menghapus Wilayah, lihat [the section called “Menghapus Wilayah dari Pusat Identitas IAM”](#).

Anda tidak dapat mempromosikan Wilayah tambahan menjadi wilayah utama atau menurunkan Wilayah utama menjadi tambahan.

Data apa yang direplikasi?

Pusat Identitas IAM mereplikasi data berikut:

Data	Sumber dan target replikasi
Identitas tenaga kerja (pengguna, grup, keanggotaan grup)	Dari Wilayah utama ke Wilayah tambahan
Kumpulan izin dan penugasan nya ke pengguna dan grup	Dari Wilayah utama ke Wilayah tambahan

Data	Sumber dan target replikasi
Konfigurasi (seperti pengaturan SAML IdP eksternal)	Dari Wilayah utama ke Wilayah tambahan
Metadata aplikasi dan penugasan aplikasi untuk pengguna dan grup	Dari Wilayah Pusat Identitas IAM yang terhubung aplikasi ke Wilayah lain yang diaktifkan
Penerbit token tepercaya	Dari Wilayah utama ke Wilayah tambahan
Sesi	Dari Wilayah asal sesi ke Wilayah lain yang diaktifkan

Note

Pusat Identitas IAM tidak mereplikasi data yang disimpan dalam aplikasi ter AWS kelola. Selain itu, itu tidak mengubah jejak regional dari penerapan aplikasi. Misalnya, jika instance Pusat Identitas IAM Anda berada di AS Timur (Virginia Utara), dan Amazon Redshift digunakan di Wilayah yang sama, mereplikasi Pusat Identitas IAM ke AS Barat (Oregon) tidak memengaruhi Wilayah penyebaran Amazon Redshift dan data yang disimpannya.

Pertimbangan:

- Pengidentifikasi sumber daya global di seluruh Wilayah yang diaktifkan - Pengguna, grup, kumpulan izin, dan sumber daya lainnya memiliki pengenalan yang sama di seluruh Wilayah yang diaktifkan.
- Replikasi tidak memengaruhi peran IAM yang disediakan - Peran IAM yang ada yang disediakan dari penetapan kumpulan izin digunakan selama masuk akun dari Wilayah mana pun yang diaktifkan.

Akses tenaga kerja melalui Wilayah tambahan

Bagian ini menjelaskan bagaimana tenaga kerja Anda dapat mengakses Portal akses AWS, Akun AWS s, dan aplikasi ketika Anda telah mengaktifkan Pusat Identitas IAM di beberapa Wilayah.

Portal akses AWS Di Wilayah tambahan menampilkan Akun AWS s dan aplikasi yang dapat diakses oleh tenaga kerja Anda dengan cara yang sama seperti di Wilayah utama. Tenaga kerja Anda dapat masuk ke Portal akses AWS dalam Wilayah tambahan melalui tautan langsung ke titik akhir portal regional (misalnya, <https://ssoins-111111h2222j33pp.eu-west-1.portal.amazonaws.com>). Jika Anda menggunakan penyedia identitas eksternal, tenaga kerja Anda juga dapat masuk melalui aplikasi [bookmark yang](#) Anda atur di IdP eksternal.

Anda dapat menggunakan Portal akses AWS titik akhir di Wilayah tambahan untuk mengotorisasi akses ke API sebagai pengguna Pusat Identitas IAM. AWS CLI Fungsi ini bekerja dengan cara yang sama seperti di Wilayah utama. Namun, otorisasi CLI tidak direplikasi di seluruh Wilayah yang diaktifkan. Oleh karena itu, Anda harus mengotorisasi CLI di setiap Wilayah secara individual.

Sesi pengguna di beberapa Wilayah AWS

Pusat Identitas IAM mereplikasi sesi pengguna dari Wilayah asal ke Wilayah lain yang diaktifkan. Pencabutan sesi dan keluar di satu Wilayah juga direplikasi ke Wilayah lainnya.

Pencabutan sesi oleh administrator Pusat Identitas IAM

Administrator Pusat Identitas IAM dapat mencabut sesi pengguna di Wilayah tambahan. Saat sesi direplikasi di seluruh Wilayah, dalam kondisi normal cukup untuk mencabut sesi di satu Wilayah dan membiarkan Pusat Identitas IAM mereplikasi perubahan ke Wilayah lain yang diaktifkan. Jika Wilayah utama Pusat Identitas IAM mengalami gangguan, administrator dapat melakukan operasi ini di Wilayah tambahan.

Portal akses AWS titik akhir di primer dan tambahan Wilayah AWS

Jika Anda perlu mencari URL portal AWS akses untuk Wilayah yang diaktifkan, ikuti langkah-langkah berikut:

1. Buka konsol [Pusat Identi](#) tas IAM.
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Pilih tab Manajemen.
4. Di bagian Wilayah untuk Pusat Identitas IAM, pilih Lihat semua URL portal AWS akses.

Tabel berikut menentukan Portal akses AWS titik akhir di seluruh Wilayah utama dan tambahan dari instance Pusat Identitas IAM.

Portal akses AWS titik akhir	Region primer	Regional tambahan	Pola dan contoh URL
IPv4 klasik hanya 1	Ya	Tidak	<p>Pola: <code>https://[Identity Store ID].awsapps.com/start</code></p> <p>Contoh: <code>https://d-12345678.awsapps.com/start</code></p>
Custom-alias IPv4 hanya 1	Ya (opsional)	Tidak	<p>Pola: <code>https://[custom alias].awsapps.com/start</code></p> <p>Contoh: <code>https://mycompany.awsapps.com/start</code></p>
Alternatif IPv4 hanya 2	Ya	Ya	<p>Pola: <code>https://[Identity Center instance ID].[Region].portal.amazonaws.com</code></p> <p>Contoh: <code>https://ssoins-111111h2222j33pp.eu-west-1.portal.amazonaws.com</code></p>
Dual-stack ²	Ya	Ya	<p>Pola: <code>https://[Identity Center instance ID].portal.[Region].app.aws</code></p> <p>Contoh: <code>https://ssoins-111111h2222j33pp.portal.eu-west-1.app.aws</code></p>

¹ Di Wilayah tambahan, alias khusus tidak didukung, dan domain `awsapps.com` induk tidak tersedia.

² Titik akhir portal IPv4 alternatif dan dual-stack portal tidak memiliki trailing di URL/start.

Titik akhir Assertion Consumer Service (ACS) di primer dan tambahan Wilayah AWS

Note

Bagian ini hanya berlaku untuk instans yang menggunakan penyedia identitas eksternal (IdP). Jika Anda menggunakan direktori Identity Center sebagai sumber identitas Anda, konfigurasi URL ACS tidak diperlukan.

Jika Anda perlu mencari URL ACS atau mengunduhnya sebagai bagian dari metadata SAML, ikuti langkah-langkah berikut:

1. Buka konsol [Pusat Identi](#) tas IAM.
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Pilih tab Sumber identitas.
4. Di menu tarik - turun Tindakan, pilih Kelola otentikasi.
5. Bagian metadata penyedia layanan menampilkan URL Portal akses AWS dan ACS untuk setiap Wilayah yang diaktifkan. IPv4-only dan URL dual-stack ditampilkan pada tab terpisah. Jika IdP Anda mendukung pengunggahan file metadata SAML, Anda dapat memilih Unduh file metadata untuk mengunduh file metadata SAML dengan semua URL ACS. Jika IdP Anda tidak mendukung pengunggahan file metadata, atau Anda lebih suka menambahkan URL ACS satu per satu, Anda dapat menyalin URL individual dari tabel di konsol, atau pilih Lihat URL ACS lalu Salin semua URL. Pertahankan URL ACS yang sudah dikonfigurasi untuk Wilayah utama untuk memastikan bahwa sistem masuk tunggal SAML yang diprakarsai penyedia layanan dari Wilayah utama tetap berfungsi.

Tabel berikut menentukan titik akhir SAML Assertion Consumer Service (ACS) di seluruh Wilayah utama dan tambahan dari instance Pusat Identitas IAM:

Titik akhir ACS	Region primer	Regional tambahan	Pola dan contoh URL
Hanya IPv4	Ya	Ya	Pola: <code>https://[Region].signin.aws/platform/saml/acs/[Tenant ID]</code>

Titik akhir ACS	Region primer	Regional tambahan	Pola dan contoh URL
			Contoh: <code>https://us-west-2.signin.aws/platform/saml/acs/1111111111111111-aaee-ffff-dddd-111111111111</code>
Hanya IPv4 alternatif*	Ya	Tidak	Pola: <code>https://[Region].signin.aws.amazon.com/platform/saml/acs/[Tenant ID]</code> Contoh: <code>https://us-west-2.signin.aws.amazon.com/platform/saml/acs/1111111111111111-aaee-ffff-dddd-111111111111</code>
Dual-stack	Ya	Ya	Pola: <code>https://[Region].sso.signin.aws/platform/saml/acs/[Tenant ID]</code> Contoh: <code>https://us-west-2.sso.signin.aws/platform/saml/acs/1111111111111111-aaee-ffff-dddd-111111111111</code>

* Untuk instance yang diaktifkan sebelum Februari 2026, pertahankan titik akhir ini karena proses masuk tunggal SAML yang diprakarsai penyedia layanan ke Wilayah utama mengharuskannya. Pusat Identitas IAM tidak menggunakan titik akhir ini untuk instans yang diaktifkan pada Februari 2026 atau yang lebih baru.

Penggunaan AWS aplikasi yang dikelola tanpa beberapa URL ACS

Note

Bagian ini hanya berlaku untuk instans yang menggunakan penyedia identitas eksternal (IdP). Jika Anda menggunakan direktori Pusat Identitas sebagai sumber identitas Anda, batasan ini tidak berlaku.

Beberapa penyedia identitas eksternal (IdPs) tidak mendukung beberapa URL layanan konsumen (ACS) asertion di aplikasi Pusat Identitas IAM mereka. Beberapa URL ACS adalah fitur SAML yang diperlukan untuk masuk langsung ke Wilayah tertentu di Pusat Identitas IAM Multi-wilayah.

Misalnya, jika Anda meluncurkan aplikasi terkel AWS ola melalui tautan aplikasi, sistem akan memicu masuk melalui Wilayah Pusat Identitas IAM yang terhubung dengan aplikasi. Namun, jika URL ACS untuk Wilayah tersebut tidak dikonfigurasi di IdP eksternal, login gagal.

Untuk mengatasi masalah ini, bekerjasama dengan vendor IdP Anda untuk mengaktifkan dukungan untuk beberapa URL ACS. Sementara itu, Anda masih dapat menggunakan aplikasi ter AWS kelola di Wilayah tambahan. Pertama, masuk ke Wilayah yang URL ACS-nya dikonfigurasi di IdP eksternal (Wilayah utama secara default). Setelah Anda memiliki sesi aktif di Pusat Identitas IAM, Anda dapat meluncurkan aplikasi dari portal AWS akses di Wilayah yang diaktifkan, atau melalui tautan aplikasi.

Failover ke Wilayah tambahan untuk Akun AWS akses

Topik Akun AWS akses melalui Pusat Identitas IAM dibahas secara ekstensif di [Akun AWS akses](#). Bagian ini memberikan detail tambahan yang relevan untuk mempertahankan Akun AWS akses Wilayah AWS di beberapa wilayah jika terjadi gangguan layanan di Wilayah utama.

Jika instance Pusat Identitas IAM Anda mengalami gangguan di Wilayah utama (misalnya, portal AWS akses di Wilayah utama tidak tersedia), tenaga kerja Anda dapat beralih ke Wilayah tambahan untuk terus mengakses Akun AWS s dan aplikasi yang tidak terpengaruh. Untuk informasi selengkapnya, lihat [the section called “Akses tenaga kerja melalui Wilayah tambahan”](#).

Sebaiknya Anda mengkomunikasikan Portal akses AWS titik akhir di Wilayah tambahan kepada tenaga kerja Anda segera setelah Anda menyelesaikan penyiapan di [the section called “Mereplikasi Pusat Identitas IAM ke Wilayah tambahan”](#). Jika Anda menggunakan penyedia identitas eksternal,

komunikasikan juga pengaturan IdP (seperti aplikasi bookmark untuk Wilayah tambahan). Ini akan memungkinkan mereka untuk siap untuk failover ke Wilayah tambahan jika diperlukan.

Demikian pula, kami menyarankan agar AWS CLI pengguna membuat [AWS CLI profil](#) untuk Wilayah tambahan untuk setiap profil yang mereka miliki untuk Wilayah utama. Kemudian, mereka dapat beralih ke profil itu jika ada gangguan layanan di Wilayah utama.

Note

Kontinuitas akses ke Akun AWS s bergantung pada izin seperti penetapan kumpulan izin dan keanggotaan grup yang disediakan dan direplikasi sebelum gangguan layanan. Jika Anda menggunakan penyedia identitas eksternal, kontinuitas juga tergantung pada kesehatan IdP eksternal Anda. Sebaiknya organisasi Anda juga menyiapkan akses [AWS break-glass](#) untuk mempertahankan AWS akses ke sekelompok kecil pengguna istimewa ketika sumber identitas mengalami gangguan layanan. [Akses darurat](#) adalah opsi serupa yang membutuhkan IdP eksternal.

Akun AWS akses ketahanan tanpa beberapa URL ACS

Note

Bagian ini hanya berlaku untuk instans yang menggunakan penyedia identitas eksternal (IdP). Jika Anda menggunakan direktori Pusat Identitas sebagai sumber identitas Anda, batasan ini tidak berlaku.

Beberapa penyedia identitas eksternal (IdPs) tidak mendukung beberapa URL layanan konsumen (ACS) asertion di aplikasi Pusat Identitas IAM mereka. Beberapa URL ACS adalah fitur SAML yang diperlukan untuk masuk langsung ke Wilayah tertentu di Pusat Identitas IAM Multi-wilayah.

Untuk memungkinkan pengguna mengakses Akun AWS melalui beberapa Wilayah Pusat Identitas IAM, Anda harus mengonfigurasi URL ACS regional masing-masing di IdP eksternal. Namun, jika IdP eksternal hanya mendukung satu URL ACS dalam aplikasi Pusat Identitas IAM mereka, pengguna dapat langsung masuk ke satu Wilayah Pusat Identitas IAM.

Untuk mengatasi masalah ini, bekerjasama dengan vendor IdP Anda untuk mengaktifkan dukungan untuk beberapa URL ACS. Sementara itu, Anda dapat menggunakan Wilayah tambahan sebagai cadangan untuk akses ke Akun AWS.

Jika gangguan layanan Pusat Identitas IAM terjadi di Wilayah utama, Anda harus memperbarui URL ACS di IdP eksternal dengan URL ACS Wilayah tambahan. Setelah pembaruan ini, pengguna Anda dapat mengakses portal AWS akses di Wilayah tambahan menggunakan aplikasi Pusat Identitas IAM yang ada di portal IdP eksternal, atau melalui tautan langsung yang Anda bagikan dengan mereka.

Sebaiknya Anda menguji pengaturan ini secara berkala untuk memastikan bahwa pengaturan ini berfungsi saat diperlukan dan mengkomunikasikan proses failover ini ke organisasi Anda.

Note

Saat Anda menggunakan Wilayah tambahan untuk akses Akun AWS dalam pengaturan ini, pengguna Anda mungkin tidak dapat mengakses aplikasi ter AWS kelola yang terhubung ke Wilayah utama. Oleh karena itu, kami merekomendasikan ini hanya sebagai tindakan sementara untuk mempertahankan akses ke Akun AWS.

Menyebarkan dan mengelola aplikasi di berbagai aplikasi AWS Wilayah

Topik akses aplikasi melalui Pusat Identitas IAM dibahas secara ekstensif di [Akses aplikasi](#). Bagian ini memberikan detail tambahan yang relevan dengan penerapan dan pengelolaan aplikasi di beberapa aplikasi Wilayah AWS.

Menyebarkan dan mengelola AWS aplikasi yang dikelola di beberapa Wilayah AWS

Dengan instance Pusat Identitas IAM wilayah tunggal, Anda dapat menerapkan aplikasi terkel AWS di Wilayah yang sama dengan instans Anda. Beberapa aplikasi seperti Amazon Q Business mendukung koneksi lintas wilayah ke Pusat Identitas IAM, yang memungkinkan penyebarannya di luar Wilayah Pusat Identitas IAM jika aplikasi yang diinginkan tersedia di sana. Namun, panggilan lintas wilayah dapat menyebabkan kinerja aplikasi lebih lambat, dan sebagian besar AWS aplikasi terkelola tidak mendukung jenis koneksi ini.

Instans Pusat Identitas IAM Multi-wilayah memungkinkan Anda menyebarkan aplikasi ter AWS kelola di Wilayah mana pun yang diaktifkan dengan koneksi ke Pusat Identitas IAM di Wilayah yang sama (“Region-local koneksi”). Penerapan di Wilayah utama didukung oleh semua aplikasi terkel AWS ola terintegrasi. Untuk mengonfirmasi aplikasi AWS terkelola mana yang mendukung penerapan

di Wilayah tambahan Pusat Identitas IAM, lihat tabel aplikasi di [the section called “Aplikasi yang dapat Anda gunakan dengan IAM Identity Center”](#). Bagaimanapun, aplikasi yang AWS dikelola harus tersedia di Wilayah tempat Anda ingin menerapkannya.

Dengan Region-local koneksi ke Pusat Identitas IAM, aplikasi terkel AWS ola mengakses identitas tenaga kerja di Wilayah yang sama untuk kinerja dan keandalan yang optimal. Sebaiknya pilih Region-local koneksi saat menerapkan aplikasi terkel AWS ola setiap kali [prasyarat ter](#)enuhi.

Untuk menyebarkan AWS aplikasi terkelola di Wilayah tambahan Pusat Identitas IAM, mulai penerapan di Wilayah tersebut melalui konsol aplikasi atau API dengan cara yang sama seperti yang Anda gunakan di Wilayah utama.

Pertimbangan:

- Jika Anda belum mereplikasi Pusat Identitas IAM ke Wilayah tersebut, sebaiknya lakukan ini terlebih dahulu agar penerapan aplikasi dapat segera selesai.
- AWS Aplikasi yang dikelola akan, dalam banyak kasus, secara otomatis membuat Region-local koneksi jika Anda telah mereplikasi Pusat Identitas IAM ke Wilayah.
- Jika aplikasi AWS terkelola menawarkan koneksi lintas wilayah ke Pusat Identitas IAM, sebaiknya pilih sam Region-local bungan asalkan [prasyarat ter](#)enuhi.
- Jika aplikasi tidak mendukung penerapan di Wilayah tambahan, Anda dapat menyebarkannya di Wilayah utama asalkan aplikasi tersedia di sana.

Important

Jika instance Pusat Identitas IAM Anda multi-regional, semua aplikasi terkel AWS ola yang digunakan oleh organisasi Anda harus mendukung Pusat Identitas IAM yang dikonfigurasi dengan kunci KMS yang dikelola pelanggan terlepas dari Wilayah penerapan aplikasi. Konfirmasikan ini [the section called “Aplikasi yang dapat Anda gunakan dengan IAM Identity Center”](#) sebelum menerapkan aplikasi dan sebelum mengonfigurasi kunci KMS yang dikelola pelanggan di Pusat Identitas IAM Anda.

Wilayah manajemen aplikasi

Setelah Anda menyebarkan aplikasi AWS terkelola di Wilayah tambahan Pusat Identitas IAM menggunakan Region-local koneksi, Anda mengelola aplikasi dan penugasannya ke pengguna

dan grup di Wilayah yang sama. Pusat Identitas IAM mereplikasi metadata aplikasi termasuk penugasan ke pengguna dan grup ke Wilayah lain yang diaktifkan sehingga tenaga kerja Anda dapat meluncurkan aplikasi dari Wilayah mana pun yang diaktifkan.

Jika aplikasi AWS terkelola menggunakan koneksi lintas wilayah ke Pusat Identitas IAM, Anda dapat mengelola detail aplikasi seperti nama dan deskripsi, serta penugasan aplikasi ke pengguna dan grup melalui konsol Pusat Identitas IAM dan API di Wilayah yang terhubung. Terlepas dari jenis koneksi, Anda dapat mengelola aplikasi melalui konsolnya di Wilayah penyebarannya.

Propagasi identitas tepercaya

Anda dapat menggunakan propagasi identitas tepercaya dengan aplikasi ter AWS kelola yang mendukungnya di Wilayah mana pun yang diaktifkan dari instans Pusat Identitas IAM Anda.

Semua aplikasi yang menyebarkan konteks identitas satu sama lain harus berada di Wilayah yang sama.

Ketergantungan aplikasi pada Wilayah Pusat Identitas IAM yang terhubung

Setiap aplikasi AWS terkelola terhubung ke Wilayah Pusat Identitas IAM tertentu selama penerapan. Aplikasi kemudian bergantung pada Wilayah tersebut untuk masuk pengguna, bahkan jika Pusat Identitas IAM Anda diaktifkan di beberapa Wilayah. Jika Pusat Identitas IAM Anda mengalami gangguan di Wilayah tersebut, pengguna mungkin tidak dapat mengakses aplikasi terkel AWS ola yang terhubung ke Wilayah.

Menyebarkan dan mengelola aplikasi yang dikelola pelanggan di berbagai aplikasi Wilayah AWS

Pusat Identitas IAM mendukung aplikasi yang dikelola pelanggan SAML dan OAuth2. [Anda dapat memilih untuk membuatnya di Wilayah yang diaktifkan dari instance Pusat Identitas IAM Anda.](#) Setelah Anda membuatnya, Anda mengelola aplikasi dan penugasannya ke pengguna dan grup di Wilayah yang sama.

Menghapus Wilayah dari Pusat Identitas IAM

Untuk menghapus Wilayah tambahan dari instance Pusat Identitas IAM Anda, ikuti langkah-langkah berikut:

Langkah 1: Perbarui konfigurasi IdP eksternal (jika ada)

Jika Anda menggunakan penyedia identitas eksternal, Anda dapat memilih untuk menghapus URL ACS untuk Wilayah ini dari IdP eksternal Anda atau menyimpannya jika Anda ingin menambahkan Wilayah ini lagi nanti. Kami menyarankan Anda menghapus atau menyembunyikan aplikasi bookmark yang mungkin telah Anda buat untuk Portal akses AWS di Wilayah ini. Jika Anda menggunakan direktori Identity Center sebagai sumber identitas Anda, lanjutkan ke Langkah 2.

Langkah 2: Hapus Wilayah

Console

Untuk menghapus Wilayah

1. Buka konsol [Pusat Identitas IAM](#).
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Pilih tab Manajemen.
4. Di bagian Regions for IAM Identity Center, pilih Wilayah tambahan yang ingin Anda hapus.
5. Pilih Hapus.
6. Sebelum mengonfirmasi penghapusan dengan memilih Hapus Wilayah, perhatikan peringatan tentang potensi hilangnya akses ke aplikasi yang dibuat di Wilayah Pusat Identitas IAM ini. Jika Anda tidak yakin apakah Anda memiliki aplikasi tersebut, pilih Aplikasi di panel navigasi dan konfirmasi Wilayah yang terhubung di kolom Di buat dari untuk setiap aplikasi yang AWS dikelola dan yang dikelola pelanggan.

Note

Anda dapat terus dikenakan biaya untuk penerapan aplikasi terkelola AWS yang masih terhubung ke Wilayah yang dihapus meskipun Anda kehilangan akses ke aplikasi ini. Untuk mencegah hal ini, Anda perlu menghapus penerapan AWS aplikasi terkelola ini melalui konsol aplikasi atau API sebelum menghapus Wilayah di Pusat Identitas IAM. Jika Anda telah menghapus Wilayah Pusat Identitas IAM, Anda dapat memulihkan akses ke aplikasi dengan menambahkan Wilayah kembali.

7. Di bagian Regions for IAM Identity Center, pantau status Wilayah. Gunakan tombol Refresh (panah melingkar) untuk melihat status Wilayah terbaru sesuai kebutuhan. Setelah Wilayah dihapus, Wilayah tidak lagi muncul di daftar Wilayah.

AWS CLI

Untuk menghapus Wilayah

```
aws sso-admin remove-region \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --region-name eu-west-1
```

Untuk memeriksa status Wilayah saat ini

```
aws sso-admin describe-region \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --region-name eu-west-1
```

Saat Wilayah dihapus, lanjutkan ke Langkah 3.

Langkah 3: Hapus kunci replika

Anda dapat memilih untuk menghapus kunci replika dari Wilayah ini untuk menghindari biaya penyimpanan KMS. Untuk informasi selengkapnya, lihat [Menghapus AWS KMS kunci](#).

Important

Pastikan untuk menghapus hanya kunci replika di Wilayah tertentu ini. Wilayah Pusat Identitas IAM lainnya terus bergantung pada kunci KMS di Wilayah lain yang diaktifkan untuk operasi normal.

API layanan Pusat Identitas IAM didukung dalam tambahan AWS Wilayah

API	Fungsionalitas di Wilayah tambahan
API Pusat Identitas	Didukung: <ul style="list-style-type: none">• read/write Operasi manajemen aplikasi• Operasi baca instans

API	Fungsionalitas di Wilayah tambahan
	Tidak didukung: <ul style="list-style-type: none"> • Operasi penulisan apa pun selain terkait aplikasi • Kumpulan izin dan operasi pembacaan penugasan akun
API Toko Identitas	Operasi baca
API OIDC	Semua operasi didukung
Akses Portal API	Semua operasi didukung
API SCIM	Tidak ada operasi yang didukung

AWS CloudTrail peristiwa Pusat Identitas IAM di Wilayah primer dan tambahan

Di AWS CloudTrail dalamnya, Anda dapat mengaudit tindakan yang dilakukan pengguna dan administrator Pusat Identitas IAM di semua instans Pusat Identi Wilayah AWS tas IAM yang diaktifkan. Per AWS CloudTrailistiwa dipancarkan dan dicatat di Wilayah tempat tindakan berlangsung. Untuk informasi selengkapnya, lihat [the section called “Pencatatan dan Pemantauan”](#).

Ketersediaan kasus penggunaan Pusat Identitas IAM di Wilayah primer dan tambahan

Fitur	Ketersediaan wilayah
Direktori tenaga kerja dengan portal pengguna	
Akses pengguna ke Portal akses AWS termasuk login portal dan sesi global (satu kali masuk untuk semua Wilayah)	Semua Wilayah yang diaktifkan
Tampilan semua akun yang ditugaskan	Semua Wilayah yang diaktifkan

Fitur	Ketersediaan wilayah
Tampilan semua aplikasi yang ditetapkan (terlepas dari di mana aplikasi dibuat)	Semua Wilayah yang diaktifkan
Baca akses ke pengguna, grup, dan keanggotaan di Kon AWS sol atau melalui API Identity Store	Semua Wilayah yang diaktifkan
Cabut sesi pengguna	Semua Wilayah yang diaktifkan
Sinkronisasi otomatis pengguna dan grup dari sumber identitas eksternal (seperti IdP eksternal melalui SCIM API atau Identity Store API). Baris ini hanya berlaku untuk penyedia identitas eksternal.	Hanya Wilayah Utama
Konfigurasi penyedia identitas otomatis dengan SCIM	Hanya Wilayah Utama
Konfigurasi SAML SSO dengan IdP eksternal	Hanya Wilayah Utama - baca akses melalui konsol di semua Wilayah yang diaktifkan
Create/update/delete operasi pada pengguna, grup, dan keanggotaan grup melalui konsol atau API Identity Store.	Hanya wilayah utama. Saat menggunakan direktori Identity Center, operasi ini tersedia melalui konsol Pusat Identitas IAM dan Identity Store API di Wilayah utama. Saat menggunakan IdP eksternal dengan penyedia SCIM, operasi tulis diblokir di konsol (kecuali akses disable/enable pengguna dan hapus pengguna). Wilayah Tambahan: akses baca-saja.
Operasi bidang data pengguna (reset kata sandi, manajemen perangkat MFA) melalui Portal akses AWS (hanya direktori Identity Center)	Semua Wilayah yang diaktifkan (hanya berlaku saat menggunakan direktori Identity Center sebagai sumber identitas)
Multi-account akses	

Fitur	Ketersediaan wilayah
Akses akun yang ditetapkan melalui tautan Portal akses AWS, AWS CLI, dan pintasan	Semua Wilayah yang diaktifkan
Mengelola kumpulan izin multi-akun dan penugasan nya di konsol dan API (termasuk akses peningkatan sementara)	Hanya Wilayah Utama
Akses ke aplikasi dan AWS layanan	
Menyebar aplikasi terkelola melalui konsol aplikasi dan API	Semua Wilayah yang diaktifkan — tergantung pada ketersediaan regional aplikasi dan dukungan untuk penerapan di Wilayah tambahan
Buat aplikasi yang dikelola pelanggan melalui konsol Identity Center dan API	Semua Wilayah yang diaktifkan
Mengelola metadata aplikasi dan penugasan di konsol dan API	Wilayah Pusat Identitas IAM yang terhubung dengan aplikasi
Luncurkan aplikasi dari Portal akses AWS atau langsung melalui tautan aplikasi atau bookmark	Semua Wilayah yang diaktifkan
Instans SSO ke Amazon EC2	Semua Wilayah yang diaktifkan
Propagasi identitas tepercaya	
Buat penerbit token tepercaya	Hanya Wilayah Utama
Propagasi identitas tepercaya dengan aplikasi AWS terkelola	Semua Wilayah yang diaktifkan - Aplikasi yang menyebarkan konteks identitas satu sama lain harus berada di Wilayah yang sama
Fitur administratif lainnya	

Fitur	Ketersediaan wilayah
Semua fitur administratif lainnya seperti Manajemen wilayah, manajemen kunci KMS, manajemen instans, dan manajemen sesi (kecuali pencabutan sesi)	Hanya Wilayah Utama - akses baca tersedia di semua Wilayah yang diaktifkan untuk beberapa data (penugasan kumpulan izin dikecualikan)

Desain ketahanan dan perilaku Regional

Layanan IAM Identity Center dikelola sepenuhnya dan menggunakan layanan yang sangat tersedia dan tahan lama AWS, seperti Amazon S3 dan Amazon EC2. Untuk memastikan ketersediaan jika terjadi gangguan Availability Zone, IAM Identity Center beroperasi di beberapa Availability Zone. Anda dapat mereplikasi instans Pusat Identitas IAM Anda ke Wilayah tambahan untuk mempertahankan akses akun dengan izin yang sudah disediakan jika terjadi gangguan Regional. Untuk informasi selengkapnya, lihat [Menggunakan Pusat Identitas IAM di beberapa Wilayah AWS](#).

Anda mengaktifkan Pusat Identitas IAM di akun AWS Organizations manajemen Anda. Ini diperlukan untuk Pusat Identitas IAM untuk menyediakan, menghentikan 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, disebut sebagai “Wilayah utama”. Jika Anda ingin menerapkan ke spesifik Wilayah AWS, ubah pilihan Wilayah sebelum mengaktifkan Pusat Identitas IAM karena Wilayah utama tidak dapat diubah setelah Pusat Identitas IAM diaktifkan.

IAM Identity Center mendukung sebagian besar fungsi administratif hanya dari Wilayah utama. Ini termasuk koneksi ke penyedia identitas eksternal, sinkronisasi pengguna dan grup, dan pembuatan dan penetapan set izin ke pengguna dan grup. Sebaliknya, pengelolaan aplikasi dan tugasnya harus dilakukan di Wilayah Pusat Identitas IAM tempat aplikasi dibuat.

Note

Bahkan jika Pusat Identitas IAM Anda direplikasi ke Wilayah tambahan, kami sarankan Anda mengatur akses [AWS break-glass](#). Ini membantu Anda mempertahankan AWS akses untuk sekelompok kecil pengguna istimewa selama acara seperti gangguan layanan di iDP eksternal. [Akses darurat](#) adalah opsi lain yang menggunakan identitas dari iDP eksternal alih-alih pengguna IAM; Namun, itu tidak melindungi terhadap gangguan pada iDP eksternal.

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 AI, bagaimanapun, harus diinstal di Wilayah instans Pusat Identitas IAM Anda agar pengguna dapat mengautentikasi dan menetapkan akses ke aplikasi ini. Untuk informasi tentang kendala Regional saat menggunakan aplikasi dengan IAM Identity Center, lihat dokumentasi untuk aplikasi dan. [the](#)

[section called “Menyebarkan dan AWS mengelola aplikasi terkelola di berbagai aplikasi Wilayah AWS”](#)

Anda juga dapat menggunakan IAM Identity Center untuk mengautentikasi dan mengotorisasi akses ke aplikasi yang dikelola SAML-based pelanggan 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 mereka tidak mendukung akses AWS akun dan karena mereka membuat titik kontrol kedua yang terisolasi yang tidak terhubung ke instans organisasi Anda.

Dirancang untuk ketersediaan

Tabel berikut memberikan ketersediaan yang dirancang untuk dicapai oleh IAM Identity Center dalam satu AWS Wilayah. Nilai-nilai ini tidak mewakili Perjanjian Tingkat Layanan atau jaminan, melainkan memberikan wawasan tentang tujuan desain. Persentase ketersediaan merujuk akses ke data atau fungsi, dan bukan referensi ke daya tahan (misalnya, retensi data jangka panjang).

Komponen layanan	Tujuan desain ketersediaan
Bidang data (termasuk masuk)	99.95%
Bidang kontrol	99.90%

Mengatur akses darurat ke Konsol Manajemen AWS

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 Konsol Manajemen AWS

AWS memungkinkan 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 Konsol Manajemen AWS melalui, dengan menggunakan kredensial 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. [Jika Anda memilih untuk tidak bergantung pada IDP eksternal, pertimbangkan untuk mengatur AWS akses break-glass](#)

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.

Topik

- [Ringkasan konfigurasi akses darurat](#)
- [Bagaimana merancang peran operasi penting Anda](#)
- [Cara merencanakan model akses Anda](#)
- [Bagaimana merancang peran darurat, akun, dan pemetaan grup](#)
- [Cara membuat konfigurasi akses darurat Anda](#)
- [Tugas persiapan darurat](#)
- [Proses failover darurat](#)
- [Kembali ke operasi normal](#)
- [One-time pengaturan aplikasi federasi IAM langsung di Okta](#)
- [One-time pengaturan aplikasi federasi IAM langsung dengan ADFS](#)

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](#). Akun ini akan menjadi akun operasi darurat Anda.

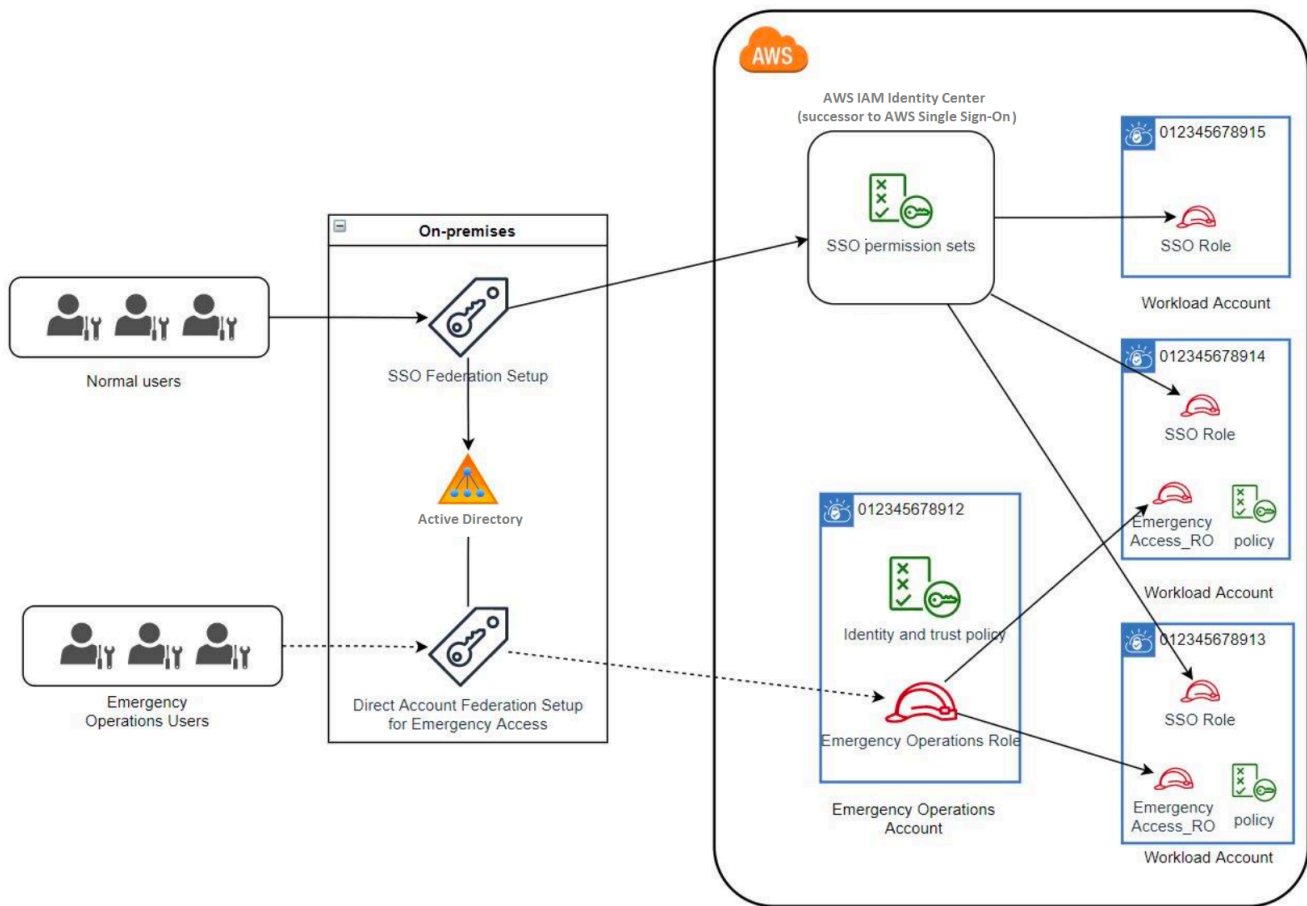
2. Hubungkan IDP Anda ke akun operasi darurat dengan menggunakan federasi berbasis [SAMP 2.0](#).
3. Di akun operasi darurat, [buat peran untuk federasi penyedia identitas pihak ketiga](#). Selain itu, buat peran operasi darurat di setiap akun beban kerja Anda, dengan izin yang diperlukan.
4. [Delegasikan 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. Konsol Manajemen AWS

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 ke Konsol Manajemen AWS, 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

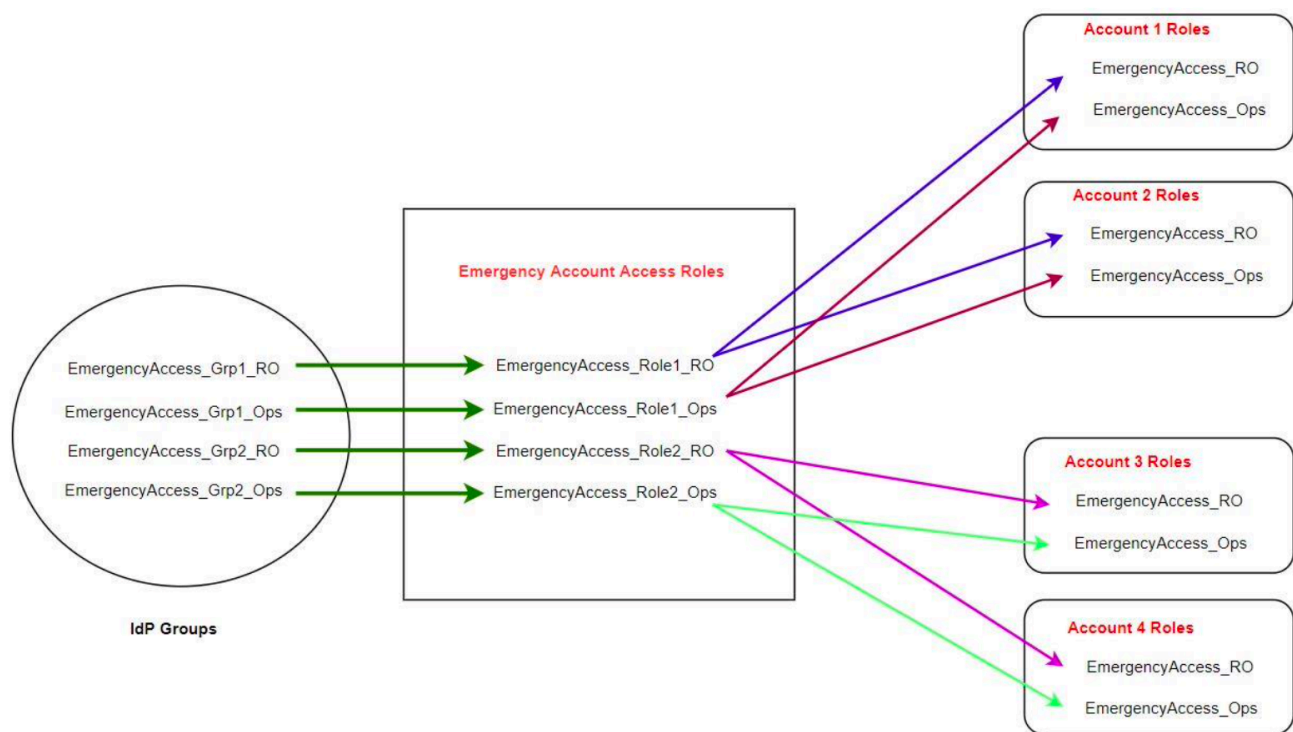
Sebelum Anda mengonfigurasi akses darurat, buat rencana bagaimana model akses akan bekerja. Gunakan proses berikut untuk membuat rencana ini.

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 individu juga memiliki kebijakan izin untuk peran yang dapat dilakukan di akun. Kebijakan izin dapat berupa kebijakan [AWS terkelola atau kebijakan](#) yang [dikelola pelanggan](#).

Akun	Peran untuk membuat	Kebijakan kepercayaan	Kebijakan izin
Akun 1	Emergency Access_RO	Emergency Access_Role1_RO	arn:aws:iam::aws:policy/ReadOnlyAccess
Akun 1	Emergency Access_Ops	Emergency Access_Role1_Ops	arn:aws:iam::aws:policy/job-function/SystemAdministrator
Akun 2	Emergency Access_RO	Emergency Access_Role2_RO	arn:aws:iam::aws:policy/ReadOnlyAccess
Akun 2	Emergency Access_Ops	Emergency Access_Role2_Ops	arn:aws:iam::aws:policy/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. Jika Anda menggunakan Okta atau eksternal lainnya IdPs sebagai sumber identitas Anda, lihat [One-time pengaturan aplikasi federasi IAM langsung di Okta](#). Jika Anda menggunakan Active Directory sebagai sumber identitas Anda, lihat [One-time pengaturan aplikasi federasi IAM langsung dengan ADFS](#).
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.

One-time pengaturan 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 Mengonfigurasi SAMP 2.0 untuk Federasi AWS Akun](#). Untuk menangani skenario kegagalan regional, saat Anda mengonfigurasi titik akhir masuk, kami menyarankan Anda mengaktifkan titik akhir non-regional dan beberapa titik akhir regional untuk semua Wilayah tempat Anda beroperasi untuk meningkatkan ketahanan federasi. Saat mengonfigurasi URL ACS untuk akses darurat ini, kami sarankan Anda menggunakan titik akhir regional Wilayah yang berbeda dari yang digunakan Pusat Identitas IAM Anda. Lihat [Sign-in titik akhir](#) dalam Referensi AWS Umum untuk daftar titik akhir regional.

5. Pada tab Sign-On Opsi, pilih SAMP 2.0 dan masukkan pengaturan Filter Grup dan Pola Nilai Peran. Nama grup untuk direktori pengguna tergantung pada filter yang Anda konfigurasi.

Group Filter	<code>^aws\#\S+\#(?{{role}})[w\-.]+\#(?{{accountid}}\d+)\$</code>
Role Value Pattern	<code>arn:aws:iam::{{accountid}}:saml-provider/Okta,arn:aws:iam::{{accountid}}:role/{{role}}</code>

Pada gambar di atas, `role` variabelnya adalah untuk peran operasi darurat di akun akses darurat Anda. Misalnya, jika Anda membuat `EmergencyAccess_Role1_R0` peran (seperti yang dijelaskan dalam tabel pemetaan) di Akun AWS 123456789012, dan jika pengaturan filter grup Anda dikonfigurasi seperti yang ditunjukkan pada gambar di atas, nama grup Anda seharusnya `aws#EmergencyAccess_Role1_R0#123456789012`.

6. Di direktori Anda (misalnya, direktori Anda di Active Directory), buat grup akses darurat dan tentukan nama untuk direktori (misalnya, `aws#EmergencyAccess_Role1_R0#123456789012`). Tetapkan pengguna Anda ke grup ini dengan menggunakan mekanisme penyediaan yang ada.
7. Di akun akses darurat, [konfigurasi 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_R0` peran. Untuk ilustrasi, lihat akun darurat pada diagram di bawah [Bagaimana merancang peran darurat, akun, dan pemetaan grup](#). Ganti contoh penyedia SAMP ARN dengan yang benar yang telah Anda buat di akun akses darurat. Ganti titik akhir regional dalam contoh dengan wilayah pilihan Anda.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::123456789012:saml-provider/[SAML PROVIDER NAME]"
      },
      "Action": [
```

```

        "sts:AssumeRoleWithSAML",
        "sts:TagSession"
    ],
    "Condition": {
        "StringEquals": {
            "SAML:aud": [
                "https://signin.aws.amazon.com/saml",
                "https://us-west-2.signin.aws.amazon.com/saml",
                "https://us-west-1.signin.aws.amazon.com/saml",
                "https://us-east-2.signin.aws.amazon.com/saml"
            ]
        }
    }
},
{
    "Effect": "Allow",
    "Principal": {
        "Federated": "arn:aws:iam::123456789012:saml-provider/Okta"
    },
    "Action": "sts:SetSourceIdentity"
}
]
}

```

8. Berikut ini adalah pernyataan contoh untuk kebijakan izin yang dilampirkan ke EmergencyAccess_Role1_R0 peran. Untuk ilustrasi, lihat akun darurat pada diagram di bawah [Bagaimana merancang peran darurat, akun, dan pemetaan grup](#).

JSON

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": [
                "arn:aws:iam::111122223333:role/EmergencyAccess_R0",
                "arn:aws:iam::444455556666:role/EmergencyAccess_R0"
            ]
        }
    ]
}

```

```
]
}
```

9. Pada akun beban kerja, konfigurasi kebijakan kepercayaan khusus. Berikut ini adalah contoh pernyataan untuk kebijakan kepercayaan yang melekat pada EmergencyAccess_R0 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](#)

JSON

```
{
  "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.

One-time pengaturan aplikasi federasi IAM langsung dengan ADFS

Panduan ini menjelaskan proses penyiapan satu kali untuk mengonfigurasi federasi IAM langsung dengan mengaktifkan ADFS akses darurat Akun AWS ketika Pusat Identitas IAM tidak tersedia.

Prasyarat

Jika Anda berencana untuk mengonfigurasi ADFS dengan Microsoft AD yang AWS Dikelola, sebaiknya Anda [mengonfigurasi Multi-Region replikasi](#) terlebih dahulu dan melanjutkan dengan langkah-langkah berikut di Wilayah tambahan dan bukan di Wilayah utama untuk ketahanan.

Rencanakan konvensi penamaan grup Active Directory Anda

Buat grup AD menggunakan pola penamaan tertentu yang memungkinkan pencocokan otomatis antara nama grup dan peran AWS IAM.

Format penamaan grup: AWS-<AccountNumber>-<RoleName>

Untuk ilustrasi, lihat akun darurat pada diagram di bawah [Bagaimana merancang peran darurat, akun, dan pemetaan grup](#). Ketika pengguna ditugaskan ke grup ini, mereka diberikan akses ke EmergencyAccess_Role1_R0 peran dalam akun123456789012. Jika pengguna dikaitkan dengan beberapa grup, mereka melihat daftar peran yang tersedia Akun AWS dan dapat memilih peran mana yang akan diambil.

AWS konfigurasi

Pengaturan lengkap mencakup konfigurasi dalam akun akses darurat dan akun beban kerja. Untuk ilustrasi pengaturan keseluruhan, lihat [Bagaimana merancang peran darurat, akun, dan pemetaan grup](#).

1. [Buat penyedia identitas SAMP](#)
2. [Buat peran akses darurat](#)
3. [Konfigurasi peran akun beban kerja](#)

Buat penyedia identitas SAMP

Di akun akses darurat, buat penyedia identitas SAMP di IAM dengan mengikuti langkah-langkah di [Buat penyedia identitas SAMP di IAM](#). Unduh metadata yang diperlukan dari server AndaADFS:

```
https://<yourADFSserverFQDN>/FederationMetadata/2007-06/  
FederationMetadata.xml
```

Buat peran akses darurat

[Buat peran akses darurat](#) di akun darurat menggunakan SAMP 2.0 Federation sebagai tipe entitas tepercaya. Pilih penyedia SAMP 2.0 yang Anda buat di langkah sebelumnya.

Pertimbangan:

- Sertakan semua Wilayah tempat Anda beroperasi — pilih setiap Wilayah di mana Anda memiliki beban kerja aktif untuk memastikan federasi tetap tersedia selama gangguan Regional.
- Konfigurasi setidaknya satu titik akhir Regional tambahan, bahkan jika Anda beroperasi di satu Wilayah — misalnya, jika Anda hanya beroperasi di us-east-1, tambahkan us-west-2 sebagai titik akhir sekunder. Anda dapat gagal melewati IDP Anda ke titik akhir masuk us-west-2 SAMP dan tetap mengakses us-east-1 sumber daya Anda, bahkan tanpa beban kerja apa pun. us-west-2
- Aktifkan titik akhir non-regional dan titik akhir regional — Meskipun titik akhir non-regional (<https://signin.aws.amazon.com/saml>) sangat tersedia, titik akhir () di-host dalam satu titik Wilayah AWSus-east-1, sementara titik akhir regional (<https://<region>.signin.aws.amazon.com/saml>) meningkatkan ketahanan dengan mengurangi ketergantungan pada satu titik akhir global.

Konfigurasi kebijakan kepercayaan

Lihat [One-time pengaturan aplikasi federasi IAM langsung di Okta](#) contoh kebijakan kepercayaan dengan beberapa titik akhir regional masuk. Ganti contoh titik akhir regional dan ARN penyedia SAMP dengan milik Anda.

Konfigurasi kebijakan izin

Lihat [One-time pengaturan aplikasi federasi IAM langsung di Okta](#) contoh kebijakan izin yang Anda lampirkan ke peran akses darurat.

Konfigurasi peran akun beban kerja

Untuk peran akun beban kerja, konfigurasi kebijakan kepercayaan khusus yang memungkinkan peran akses darurat di akun akses darurat untuk mengasumsikan peran tersebut. Lihat [One-time pengaturan aplikasi federasi IAM langsung di Okta](#) contoh kebijakan kepercayaan, di mana akun 123456789012 adalah akun akses darurat.

Konfigurasi Direktori Aktif

Langkah-langkah berikut menjelaskan cara mengkonfigurasi Active Directory dan ADFS untuk akses darurat.

1. [Buat grup](#)

2. [Buat pesta yang mengandalkan](#)

3. [Buat aturan klaim](#)

Buat grup

Buat grup darurat di Active Directory sesuai dengan konvensi penamaan yang dijelaskan sebelumnya (misalnya, AWS-123456789012-EmergencyAccess_Role1_R0). Tetapkan pengguna ke grup ini melalui mekanisme penyediaan yang ada.

Buat pesta yang mengandalkan

ADFSfederasi membutuhkan konfigurasi partai yang mengandalkan. Pihak yang mengandalkan adalah AWS Security Token Service (AWS STS), yang mengalihdayakan otentikasi ADFS sebagai penyedia identitas.

1. Di konsol ADFS Manajemen, gunakan menu Tindakan dan pilih Tambahkan Kepercayaan Pihak yang Mengandalkan. Pilih Klaim sadar saat menambahkan pihak yang mengandalkan.
2. Untuk metadata federasi, masukkan URL Metadata dari info metadata penyedia identitas di konsol IAM. Contoh:

```
https://signin.aws.amazon.com/static/saml/SAMLSPXXXXXX/saml-metadata.xml
```

3. Tetapkan nama tampilan untuk pihak yang mengandalkan (misalnya, Akses AWS Akun) dan kemudian pilih Berikutnya.
4. Pilih siapa yang ingin Anda aktifkan untuk mengakses AWS. Anda dapat memilih grup tertentu dan menentukan persyaratan seperti MFA.
5. Pilih Tutup pada halaman Selesai untuk menyelesaikan Add Relying Party Trust Wizard. AWS sekarang dikonfigurasi sebagai pihak yang mengandalkan.

Buat aturan klaim

ADFSmenggunakan Bahasa Aturan Klaim untuk menerbitkan dan mengubah klaim antara penyedia klaim dan pihak yang mengandalkan. Anda perlu membuat empat aturan klaim:NameId,RoleSessionName, Dapatkan Grup Iklan, dan Peran untuk AWS Akses.

Right-click pada pihak yang mengandalkan dan kemudian pilih Edit Kebijakan Penerbitan Klaim. Pilih Tambahkan Aturan untuk menambahkan aturan.

1. NameId

- a. Pilih Transform an Incoming Claim dan kemudian pilih Next.
- b. Gunakan pengaturan berikut:
 - Nama aturan klaim: NameId
 - Jenis klaim masuk: Windows Account Name
 - Jenis klaim keluar: Name ID
 - Format ID nama keluar: Persistent Identifier
 - Lewati semua nilai klaim: diperiksa
- c. Pilih OK.

2. RoleSessionName

- a. Pilih Tambahkan aturan.
- b. Dalam daftar templat aturan Klaim, pilih Kirim Atribut LDAP sebagai Klaim.
- c. Gunakan pengaturan berikut:
 - Nama aturan klaim: RoleSessionName
 - Toko atribut: Active Directory
 - Atribut LDAP: E-Mail-Addresses
 - Jenis Klaim Keluar: <https://aws.amazon.com/SAML/Attributes/RoleSessionName>
- d. Pilih OK.

3. Dapatkan Grup AD

- a. Pilih Tambahkan aturan.
- b. Dalam daftar templat aturan Klaim, pilih Kirim Klaim Menggunakan Aturan Kustom, lalu pilih Berikutnya.
- c. Untuk Nama Aturan Klaim, masukkan Get AD Groups, lalu di Aturan khusus, masukkan yang berikut ini:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
=> add(store = "Active Directory", types = ("http://temp/variable"), query =
";tokenGroups;{0}", param = c.Value);
```

Aturan kustom ini menggunakan skrip dalam bahasa aturan klaim yang mengambil semua grup yang menjadi anggota pengguna yang diautentikasi dan menempatkannya ke dalam klaim sementara bernama. `http://temp/variable`

 Note

Pastikan tidak ada spasi tambahan untuk menghindari hasil yang tidak terduga.

4. Atribut Peran

- a. Pilih Tambahkan aturan.
- b. Dalam daftar templat aturan Klaim, pilih Kirim Klaim Menggunakan Aturan Kustom, lalu pilih Berikutnya.
- c. Untuk Nama Aturan Klaim, masukkan `Roles`, lalu di Aturan khusus, masukkan yang berikut ini:

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([\d]{12})"]
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
  RegexReplace(c.Value, "AWS-([\d]{12})-", "arn:aws:iam::$1:saml-provider/
  <ADFS>,arn:aws:iam::$1:role/"));
```

Aturan khusus ini menggunakan ekspresi reguler untuk mengubah setiap keanggotaan grup formulir `AWS-<Account Number>-<Role Name>` menjadi ARN peran IAM dan ARN penyedia federasi IAM formulir ARN yang diharapkan. AWS

 Note

Dalam contoh bahasa aturan di atas, ADFS mewakili nama logis yang diberikan kepada penyedia identitas SAMP dalam pengaturan penyedia AWS identitas. Ubah ini berdasarkan nama logis yang Anda pilih di konsol IAM untuk penyedia identitas Anda.

Uji konfigurasi

Uji apakah solusinya bekerja dengan mengautentikasi di `https://<yourADFSserverFQDN>/adfs/ls/IdpInitiatedSignOn.aspx`. Pilih nama pihak yang mengandalkan yang Anda buat dari daftar dropdown situs.

Perbarui titik akhir pernyataan SAMP default di ADFS

Important

Saat mengonfigurasi kepercayaan pihak yang mengandalkan ADFS, titik akhir Pernyataan SAMP default yang bukan `https://signin.aws.amazon.com/` merupakan titik akhir global dan berada di `us-east-1`. Kami menyarankan Anda mengubah titik akhir default ke titik akhir regional yang berbeda dari tempat Pusat Identitas IAM Anda dikonfigurasi untuk ketahanan. Misalnya, jika Pusat Identitas IAM Anda diterapkan `us-east-1` dan Anda juga beroperasi `us-west-2`, ubah titik akhir konsumen Pernyataan SAMP default menjadi `https://us-west-2.signin.aws.amazon.com/saml`.

1. Pilih Properti pada kepercayaan pihak yang mengandalkan dan buka tab Pemantauan. Kosongkan kotak centang Secara Otomatis Perbarui pihak yang mengandalkan.
2. Buka tab Endpoints, pilih titik akhir login pilihan Anda, dan pilih Edit.
3. Pilih kotak centang Setel URL tepercaya sebagai default. Pilih OK dan Terapkan agar pengaturan diterapkan.

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 AWS antara Anda. [Model tanggung jawab bersama](#) menggambarkan 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. Third-party auditor secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari program [AWS kepatuhan](#). Untuk mempelajari tentang program kepatuhan yang berlaku untuk 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 Pusat Identitas IAM. 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 Pusat Identitas IAM](#)
- [Konsol Pusat Identitas IAM dan otorisasi API](#)
- [AWS STS kunci konteks kondisi untuk Pusat Identitas IAM](#)
- [Pencatatan dan pemantauan di Pusat Identitas IAM](#)
- [Validasi kepatuhan untuk Pusat Identitas IAM](#)
- [Ketahanan di Pusat Identitas IAM](#)
- [Keamanan infrastruktur di Pusat Identitas IAM](#)

Manajemen identitas dan akses untuk Pusat Identitas IAM

Akses ke Pusat Identitas IAM memerlukan kredensial yang AWS dapat digunakan untuk mengotentikasi permintaan Anda. Kredensial tersebut harus memiliki izin untuk mengakses AWS sumber daya, seperti aplikasi ter AWS kelola.

Otentikasi AWS ke portal 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 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 ke mereka 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 tugas sehari-hari dari konsol Pusat Identitas IAM.

- [Autentikasi](#)
- [Kontrol akses](#)

Autentikasi

Pelajari cara mengakses AWS menggunakan identitas <https://docs.aws.amazon.com/IAM/latest/UserGuide/id.html> IAM.

Kontrol akses

Anda dapat memiliki kredentif yang valid untuk mengotentikasi 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 ke Pusat Identitas IAM.

Note

Jika instance Pusat Identitas IAM dikonfigurasi dengan kunci KMS yang dikelola pelanggan, administrator Pusat Identitas IAM Anda dan aktor lain yang memerlukan akses ke kunci KMS

akan memerlukan izin tambahan. Lihat [Menerapkan kunci KMS yang dikelola pelanggan di AWS IAM Identity Center](#).

Bagian berikut menjelaskan cara mengelola izin untuk Pusat Identitas IAM. Anda sebaiknya membaca gambaran umum terlebih dahulu.

- [Ikhtisar pengelolaan izin akses ke sumber daya Pusat Identitas IAM Anda](#)
- [Identity-based contoh kebijakan untuk Pusat Identitas IAM](#)
- [Resource-based contoh kebijakan untuk Pusat Identitas IAM](#)
- [Menggunakan peran terkait layanan untuk Pusat Identitas IAM](#)

Ikhtisar pengelolaan 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-prinsip](#)
- [Menentukan kondisi dalam kebijakan](#)

Sumber daya dan operasi Pusat Identitas IAM

Di Pusat Identitas IAM, sumber daya utama adalah instance aplikasi, profil, dan kumpulan izin.

Memahami kepemilikan sumber daya

Pemilik sumber daya adalah Akun AWS yang membuat sumber daya. Artinya, pemilik sumber daya adalah entitas Akun AWS utama (akun, pengguna, atau peran IAM) yang mengotentikasi permintaan yang membuat sumber daya. Contoh berikut menggambarkan cara kerjanya:

- Jika membuat Pengguna root akun AWS sumber daya Pusat Identitas IAM, seperti instance aplikasi atau kumpulan izin, Anda Akun AWS adalah pemilik sumber daya tersebut.
- Jika Anda membuat pengguna di AWS akun Anda dan memberikan izin kepada 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 Pusat Identitas IAM. 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

- [Identity-based kebijakan \(kebijakan IAM\)](#)
- [Resource-based kebijakan](#)

Identity-based kebijakan (kebijakan IAM)

Anda dapat menambahkan izin ke identitas IAM. Misalnya, Anda dapat melakukan hal berikut:

- Melampirkan kebijakan izin ke pengguna atau grup di Anda Akun AWS — Administrator akun dapat menggunakan kebijakan izin yang terkait dengan pengguna tertentu untuk memberikan izin kepada 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 kumpulan izin. Perhatikan bahwa karakter wildcard (*) pada `Resource` elemen menunjukkan bahwa tindakan diizinkan untuk semua sumber daya Pusat Identitas IAM yang dimiliki oleh akun.

JSON

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

Untuk informasi selengkapnya tentang menggunakan kebijakan berbasis identitas dengan Pusat Identitas IAM, lihat [Identity-based contoh kebijakan untuk Pusat Identitas IAM](#). Untuk informasi lebih lanjut tentang pengguna, kelompok, peran, dan izin, lihat [Identitas \(Pengguna, Grup, dan Peran\)](#) dalam Panduan Pengguna IAM.

Resource-based kebijakan

Layanan lain, seperti Amazon S3, juga mendukung kebijakan izin berbasis sumber daya. Misalnya, Anda dapat melampirkan kebijakan ke bucket S3 untuk mengelola izin akses ke bucket tersebut. Pusat Identitas IAM tidak mendukung kebijakan berbasis sumber daya.

Menentukan elemen kebijakan: tindakan, efek, sumber daya, dan prinsip-prinsip

Untuk setiap sumber daya Pusat Identitas IAM (lihat [Sumber daya dan operasi Pusat Identitas IAM](#)), layanan mendefinisikan serangkaian operasi API. Untuk memberikan izin untuk operasi API ini, Pusat Identitas IAM 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 `DescribePermissionsPolicies` operasi Pusat Identitas IAM.
- **Efek** – Anda menentukan efek ketika pengguna meminta tindakan tertentu—efek ini dapat berupa pemberian izin atau penolakan. Jika Anda tidak secara jelas memberikan akses (mengizinkan) ke sumber daya, maka akses akan ditolak secara implisit. Anda juga dapat secara eksplisit menolak akses ke sumber daya, yang mungkin Anda lakukan untuk memastikan bahwa pengguna tidak dapat 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). Pusat Identitas IAM tidak mendukung kebijakan berbasis sumber daya.

Untuk mempelajari selengkapnya tentang sintaks dan deskripsi kebijakan IAM, lihat referensi kebijakan [AWS IAM](#) di Panduan Pengguna IAM.

Menentukan kondisi dalam kebijakan

Saat Anda memberikan izin, Anda dapat menggunakan bahasa kebijakan akses untuk menentukan kondisi yang diperlukan agar kebijakan mulai berlaku. Misalnya, Anda mungkin ingin kebijakan diterapkan hanya setelah tanggal tertentu. Untuk informasi selengkapnya tentang menentukan kondisi dalam bahasa kebijakan, lihat [Kondisi](#) dalam Panduan Pengguna IAM.

Untuk menyatakan kondisi, Anda menggunakan kunci kondisi standar. Tidak ada kunci kondisi khusus untuk Pusat Identitas IAM. Namun, ada kunci AWS kondisi yang dapat Anda gunakan sebagaimana mestinya. Untuk daftar AWS kunci lengkap, lihat Kunci kondisi global yang [tersedia](#) di Panduan Pengguna IAM.

Identity-based contoh kebijakan untuk Pusat Identitas IAM

Topik ini memberikan contoh kebijakan IAM yang dapat Anda buat untuk memberikan izin kepada pengguna dan peran untuk mengelola Pusat Identitas IAM.

Important

Sebaiknya 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 pengelolaan izin akses ke sumber daya Pusat Identitas IAM Anda](#).

Bagian dalam topik ini membahas 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. Kebijakan contoh ini adalah kebijakan berbasis identitas, yang tidak menentukan elemen Principal. Ini karena dengan kebijakan berbasis identitas, Anda tidak menentukan kepala sekolah yang mendapatkan izin. Sebagai gantinya, 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 tersebut. Anda dapat membuat kebijakan berbasis identitas di IAM dan melampirkannya ke pengguna, grup, peran. and/or Anda juga dapat menerapkan kebijakan ini ke pengguna Pusat Identitas IAM saat membuat kumpulan izin di Pusat Identitas IAM.

Note

Gunakan contoh ini saat Anda membuat kebijakan untuk lingkungan Anda dan pastikan untuk menguji kasus uji positif (“akses diberikan”) dan negatif (“akses ditolak”) sebelum Anda 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 Akun AWS di Pusat Identitas IAM](#)
- [Contoh 3: Izinkan pengguna mengelola aplikasi di Pusat Identitas IAM](#)
- [Contoh 4: Izinkan pengguna mengelola pengguna dan grup di direktori Pusat Identitas Anda](#)

Contoh 1: Izinkan pengguna untuk melihat Pusat Identitas IAM

Kebijakan izin berikut memberikan izin baca-saja kepada pengguna sehingga pengguna dapat melihat semua pengaturan dan informasi direktori yang dikonfigurasi di Pusat Identitas IAM.

Note

Kebijakan ini disediakan untuk tujuan contoh saja. Di lingkungan produksi, sebaiknya gunakan kebijakan terkel ViewOnlyAccess AWS ola untuk Pusat Identitas IAM.

JSON

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

```

{
  "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:ListDelegatedAdministrators",
    "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 Akun AWS di Pusat Identitas IAM

Kebijakan izin berikut memberikan izin untuk mengizinkan pengguna membuat, mengelola, dan menerapkan kumpulan izin untuk Anda Akun AWS.

JSON

```

{
  "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": "AccessToSSOProvisionedRoles" bagian "Sid": "IAMListPermissions", dan 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 mengelola aplikasi di Pusat Identitas IAM

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:AssociateProfileOperasi` yang digunakan dalam contoh kebijakan berikut diperlukan untuk pengelolaan penugasan pengguna dan grup ke aplikasi. Hal ini juga memungkinkan pengguna untuk menetapkan pengguna dan grup Akun AWS dengan menggunakan kumpulan izin yang ada. Jika pengguna harus mengelola Akun AWS akses dalam Pusat Identitas IAM, dan memerlukan izin yang diperlukan untuk mengelola kumpulan izin, lihat [Contoh 2: Izinkan pengguna untuk mengelola izin Akun AWS di Pusat 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 bebas kesalahan untuk kasus ini.

JSON

```
{
  "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 Anda

Kebijakan izin berikut memberikan izin untuk mengizinkan pengguna membuat, melihat, memodifikasi, dan menghapus pengguna dan grup di Pusat Identitas IAM.

Dalam beberapa kasus, modifikasi langsung ke pengguna dan grup di Pusat Identitas IAM dibatasi. Misalnya, ketika Active Directory, atau penyedia identitas eksternal dengan Penyediaan Otomatis diaktifkan, dipilih sebagai sumber identitas.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sso-directory:ListGroupForUser",
        "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.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sso:DescribeAccountAssignmentCreationStatus",
        "sso:DescribeAccountAssignmentDeletionStatus",
        "sso:DescribePermissionSet",
        "sso:DescribePermissionSetProvisioningStatus",
        "sso:DescribeRegisteredRegions",
        "sso:GetApplicationInstance",
        "sso:GetApplicationTemplate",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetManagedApplicationInstance",
        "sso:GetMfaDeviceManagementForDirectory",
        "sso:GetPermissionSet",
        "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": "*"
}
]
}

```

Resource-based contoh kebijakan untuk Pusat Identitas IAM

Setiap aplikasi yang bekerja dengan IAM Identity Center dan menggunakan [OAuth 2.0](#) memerlukan kebijakan berbasis sumber daya. Aplikasi dapat dikelola atau AWS dikelola pelanggan. Kebijakan berbasis sumber daya yang diperlukan, yang disebut kebijakan aplikasi (atau [ActorPolicy](#) dalam API), mendefinisikan prinsipal [IAM mana yang diizinkan untuk memanggil](#) tindakan API metode otentikasi IAM seperti. [CreateTokenWithIAM](#) Metode otentikasi IAM memungkinkan prinsipal IAM, seperti peran IAM atau layanan, untuk mengotentikasi ke AWS layanan OIDC Pusat Identitas IAM dengan menyajikan kredensial IAM untuk meminta atau mengelola token akses di `/token? aws_i` `am=t` titik akhir.

Kebijakan aplikasi mengatur operasi untuk menerbitkan token (`CreateTokenWithIAM`). Kebijakan ini juga mengatur tindakan khusus izin yang hanya digunakan oleh aplikasi terkel AWS untuk memvalidasi token (`IntrospectTokenWithIAM`) dan mencabut token (`RevokeTokenWithIAM`). Untuk aplikasi yang dikelola pelanggan, Anda mengonfigurasi kebijakan ini dengan menentukan prinsipal IAM mana yang diizinkan untuk memanggil `CreateTokenWithIAM`. Ketika kepala sekolah resmi memanggil tindakan API ini, kepala sekolah menerima token akses dan penyegaran untuk aplikasi.

Jika Anda menggunakan konsol Pusat Identitas IAM untuk menyiapkan aplikasi yang dikelola pelanggan untuk propagasi identitas, lihat [Langkah 4 di Menyiapkan aplikasi OAuth 2.0 yang dikelola pelanggan](#) untuk informasi tentang cara mengonfigurasi kebijakan aplikasi. Untuk contoh kebijakan, lihat [Contoh kebijakan: Izinkan peran IAM untuk membuat token akses dan menyegarkan](#) nanti dalam topik ini.

Persyaratan kebijakan

Kebijakan harus memenuhi persyaratan berikut:

- Kebijakan harus menyertakan `Version` elemen yang ditetapkan ke "2012-10-17".
- Kebijakan harus mencakup setidaknya satu `Statement` elemen.
- Setiap kebijakan `Statement` harus mencakup elemen-elemen berikut: `Effect`, `Principal`, `Action`, dan `Resource`.

Elemen kebijakan

Kebijakan harus mencakup elemen-elemen berikut:

Versi

Menentukan versi dokumen kebijakan. Atur versi ke 2012-10-17 (versi terbaru).

Pernyataan

Berisi `PolicyStatements`. Kebijakan harus berisi setidaknya satu `Statement`.

Setiap kebijakan `Statement` terdiri dari elemen-elemen berikut.

Efek

(Diperlukan) Menentukan apakah akan mengizinkan atau menolak izin dalam pernyataan kebijakan. Nilai-nilai yang valid adalah `Allow` atau `Deny`.

Principal

(Diperlukan) [Prinsip](#) adalah identitas yang mendapatkan izin yang ditentukan dalam pernyataan kebijakan. Anda dapat menentukan peran IAM atau prinsipal AWS layanan.

Tindakan

(Diperlukan) Operasi API layanan IDC Pusat Identitas IAM untuk mengizinkan atau menolak. Tindakan yang valid meliputi:

- `sso-oauth:CreateTokenWithIAM`: Tindakan ini, yang sesuai dengan operasi [CreateTokenWithIAM](#) API, memberikan izin untuk membuat dan mengembalikan akses dan menyegarkan token untuk aplikasi klien resmi yang diautentikasi menggunakan entitas IAM apa pun, seperti peran AWS layanan atau pengguna. Token ini mungkin berisi cakupan yang ditentukan yang menentukan izin seperti `read:profile` atau `write:data`.
- `sso-oauth:IntrospectTokenWithIAM` [hanya izin]: Memberikan izin untuk memvalidasi dan mengambil informasi tentang token akses OAuth 2.0 aktif dan token penyegaran, termasuk cakupan dan izin terkait. Izin ini hanya digunakan oleh aplikasi ter AWS kelola dan tidak didokumentasikan dalam Referensi API IDC Pusat Identitas IAM.
- `RevokeTokenWithIAM` [hanya izin]: Memberikan izin untuk mencabut token akses OAuth 2.0 dan menyegarkan token, membatalkannya sebelum kedaluwarsa normalnya. Izin ini hanya digunakan oleh aplikasi ter AWS kelola dan tidak didokumentasikan dalam Referensi API IDC Pusat Identitas IAM.

Sumber daya

(Diperlukan) Dalam kebijakan ini, nilai `Resource` elemen adalah `"*"`, yang berarti "aplikasi ini."

Untuk informasi selengkapnya tentang sintaks AWS kebijakan, lihat Refer [AWS ensi Kebijakan IAM](#) di Panduan Pengguna IAM.

Contoh kebijakan: Izinkan peran IAM untuk membuat token akses dan menyegarkan

Kebijakan izin berikut memberikan izin kepada `ExampleAppClientRole`, peran IAM yang diasumsikan oleh beban kerja, untuk membuat dan mengembalikan akses dan menyegarkan token.

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

```
    "Sid": "AllowRoleToCreateTokens",
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::111122223333:role/ExampleAppClientRole"
    },
    "Action": "sso-oauth:CreateTokenWithIAM",
    "Resource": "*"
  }
]
```

AWS kebijakan terkelola untuk Pusat Identitas IAM

Untuk [membuat kebijakan](#) yang dikelola pelanggan IAM yang memberi tim Anda hanya izin yang mereka butuhkan membutuhkan waktu dan keahlian. Untuk memulai dengan cepat, Anda dapat menggunakan kebijakan ter AWS kelola. 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 ter AWS kelola. 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 ter AWS kelola, sehingga pembaruan kebijakan tidak akan merusak izin yang ada.

Selain itu, AWS mendukung kebijakan terkelola untuk fungsi pekerjaan yang mencakup beberapa layanan. Misalnya, kebijakan terkel ReadOnlyAccess AWS menyediakan akses baca-saja ke semua AWS layanan dan sumber daya. Saat layanan meluncurkan fitur baru, AWS menambahkan izin baca-saja 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 untuk membuat daftar dan menghapus sesi pengguna tersedia di bawah namespace `identitystore-auth` baru. Izin tambahan apa pun untuk tindakan di namespace ini akan diperbarui di halaman ini. Saat membuat kebijakan IAM kustom Anda, hindari menggunakan `*` after `identitystore-auth` karena ini berlaku untuk semua tindakan yang ada di namespace saat ini atau di masa mendatang.

AWS kebijakan yang dikelola: AWSSSOMasterAccountAdministrator

AWSSSOMasterAccountAdministratorKebijakan ini memberikan tindakan administratif yang diperlukan kepada kepala sekolah. Kebijakan ini ditujukan untuk kepala sekolah yang melakukan peran pekerjaan sebagai AWS IAM Identity Center administrator. Seiring waktu daftar tindakan yang disediakan akan diperbarui agar sesuai dengan fungsionalitas Pusat Identitas IAM yang ada dan tindakan yang diperlukan sebagai administrator.

Anda dapat melampirkan kebijakan AWSSSOMasterAccountAdministrator ke identitas IAM Anda. Saat melampirkan AWSSSOMasterAccountAdministrator kebijakan ke identitas, Anda memberikan AWS IAM Identity Center izin administratif. Kepala sekolah dengan kebijakan ini dapat mengakses Pusat Identitas IAM dalam akun AWS Organizations manajemen dan semua akun anggota. Prinsip ini dapat sepenuhnya mengelola semua operasi Pusat Identitas IAM, termasuk kemampuan untuk membuat instance Pusat Identitas IAM, pengguna, kumpulan izin, dan penugasan. Kepala sekolah juga dapat membuat instance penugasan tersebut di seluruh akun anggota AWS organisasi dan membuat koneksi antara direktori terkelola dan AWS Directory Service Pusat Identitas IAM. Saat fitur administratif baru dirilis, administrator akun akan diberikan izin ini secara otomatis.

Kebijakan ini juga mencakup AWS Key Management Service izin yang diperlukan untuk instans Pusat Identitas IAM yang menggunakan kunci yang dikelola pelanggan untuk enkripsi.

Pengelompokan izin

Kebijakan ini dikelompokkan ke dalam pernyataan berdasarkan kumpulan izin yang diberikan.

- AWSSSOMasterAccountAdministrator- Mengizinkan Pusat Identitas IAM untuk [meneruskan peran layanan yang](#) AWSServiceRoleforSSO diberi nama ke Pusat Identitas IAM sehingga nantinya dapat mengambil peran dan melakukan tindakan atas nama mereka. Ini diperlukan ketika orang atau aplikasi mencoba mengaktifkan Pusat Identitas IAM. Untuk informasi selengkapnya, lihat [Konfigurasi akses ke Akun AWS](#).
- AWSSSOMemberAccountAdministrator- Mengizinkan Pusat Identitas IAM untuk melakukan tindakan administrator akun di lingkungan multi-akun AWS . Untuk informasi selengkapnya, lihat [AWS kebijakan yang dikelola: AWSSSOMemberAccountAdministrator](#).
- AWSSSOManageDelegatedAdministrator- Mengizinkan Pusat Identitas IAM untuk mendaftarkan dan membatalkan pendaftaran administrator yang didelegasikan untuk organisasi Anda.

- `AllowKMSKeyUseViaService` dan `AllowKMSKeyDiscovery` — Mengizinkan AWS Key Management Service operasi untuk kunci yang dikelola pelanggan yang digunakan oleh instans Pusat Identitas IAM.

Untuk melihat izin kebijakan ini, lihat [AWSSSOMasterAccountAdministrator](#) di Referensi Kebijakan AWS Terkelola.

Informasi tambahan tentang kebijakan ini

Saat Pusat Identitas IAM diaktifkan untuk pertama kalinya, layanan Pusat Identitas IAM membuat peran terkait [layanan](#) 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`.

AWS kebijakan yang dikelola: `AWSSSOMemberAccountAdministrator`

`AWSSSOMemberAccountAdministrator` Kebijakan ini memberikan tindakan administratif yang diperlukan kepada kepala sekolah. Kebijakan ini ditujukan untuk kepala sekolah yang menjalankan peran sebagai administrator Pusat Identitas IAM. Seiring waktu daftar tindakan yang disediakan akan diperbarui agar sesuai dengan fungsionalitas Pusat Identitas IAM yang ada dan tindakan yang diperlukan sebagai administrator.

Anda dapat melampirkan kebijakan `AWSSSOMemberAccountAdministrator` ke identitas IAM Anda. Saat melampirkan `AWSSSOMemberAccountAdministrator` kebijakan ke identitas, Anda memberikan AWS IAM Identity Center izin administratif. Kepala sekolah dengan kebijakan ini dapat mengakses Pusat Identitas IAM dalam akun AWS Organizations manajemen dan semua akun anggota. Prinsip ini dapat sepenuhnya mengelola semua operasi Pusat Identitas IAM, termasuk kemampuan untuk membuat pengguna, kumpulan izin, dan penugasan. Kepala sekolah juga dapat membuat instance penugasan tersebut di seluruh akun anggota AWS organisasi dan membuat koneksi antara direktori terkelola dan AWS Directory Service Pusat Identitas IAM. Saat fitur administratif baru dirilis, administrator akun diberikan izin ini secara otomatis.

Kebijakan ini juga mencakup AWS Key Management Service izin yang diperlukan untuk instans Pusat Identitas IAM yang menggunakan kunci yang dikelola pelanggan untuk enkripsi.

Untuk melihat izin kebijakan ini, lihat [AWSSSOMemberAccountAdministrator](#) di Referensi Kebijakan AWS Terkelola.

Informasi tambahan tentang kebijakan ini

Administrator Pusat Identitas IAM mengelola pengguna, grup, dan kata sandi di penyimpanan direktori Pusat Identitas mereka (direktori sso). Peran admin akun mencakup izin untuk tindakan berikut:

- "sso:*"
- "sso-directory:*"

Administrator Pusat Identitas IAM memerlukan izin terbatas untuk Directory Service tindakan berikut untuk melakukan tugas harian.

- "ds:DescribeTrusts"
- "ds:UnauthorizeApplication"
- "ds:DescribeDirectories"
- "ds:AuthorizeApplication"
- "ds>CreateAlias"

Izin ini memungkinkan administrator Pusat Identitas IAM untuk mengidentifikasi direktori yang ada dan mengelola aplikasi sehingga mereka dapat dikonfigurasi untuk digunakan dengan Pusat Identitas IAM. Untuk informasi selengkapnya tentang masing-masing tindakan ini, lihat izin [Directory Service API: Referensi tindakan, sumber daya, dan kondisi](#).

Pusat Identitas IAM menggunakan kebijakan IAM untuk memberikan izin kepada pengguna Pusat Identitas IAM. Administrator Pusat Identitas IAM membuat kumpulan izin dan melampirkan kebijakan ke mereka. Administrator Pusat Identitas IAM harus memiliki izin untuk membuat daftar kebijakan yang ada sehingga mereka dapat memilih kebijakan mana yang akan digunakan dengan kumpulan izin yang mereka buat atau perbarui. Untuk menetapkan izin aman dan fungsional, administrator Pusat Identitas IAM harus memiliki izin untuk menjalankan validasi kebijakan Penganalisis Akses IAM.

- "iam:ListPolicies"
- "access-analyzer:ValidatePolicy"

Administrator Pusat Identitas IAM 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 Pusat Identitas IAM kemampuan untuk bekerja dengan sumber daya organisasi (akun) untuk tugas-tugas administratif Pusat Identitas IAM dasar seperti berikut:

- Mengidentifikasi akun manajemen milik organisasi
- Mengidentifikasi akun anggota milik organisasi
- Meng AWS aktifkan akses layanan untuk akun
- Menyiapkan dan mengelola administrator yang didelegasikan

Untuk informasi selengkapnya tentang menggunakan administrator yang didelegasikan dengan Pusat Identitas IAM, lihat [Administrator yang didelegasikan](#). Untuk informasi selengkapnya tentang bagaimana izin ini digunakan dengan AWS Organizations, lihat [Menggunakan AWS Organizations dengan AWS layanan lain](#).

AWS kebijakan yang dikelola: AWSSSODirectoryAdministrator

Anda dapat melampirkan kebijakan AWSSSODirectoryAdministrator ke identitas IAM Anda.

Kebijakan ini memberikan izin administratif atas pengguna dan grup Pusat Identitas IAM. Kepala sekolah dengan kebijakan ini terlampir dapat melakukan pembaruan apa pun untuk pengguna dan grup Pusat Identitas IAM. Kebijakan ini juga mencakup AWS Key Management Service izin yang

diperlukan untuk instans Pusat Identitas IAM yang menggunakan kunci yang dikelola pelanggan untuk enkripsi.

Kebijakan ini mencakup izin berikut:

- Direktori Pusat Identitas IAM - Akses administratif penuh ke operasi direktori Pusat Identitas IAM.
- Identity Store - Akses administratif penuh ke operasi penyimpanan identitas dan otentikasi.
- Pusat Identitas IAM - Izin untuk membuat daftar asosiasi direktori.
- AWS Key Management Service- Izin untuk mendekripsi, menjelaskan kunci, dan menghasilkan kunci data untuk kunci yang dikelola pelanggan yang digunakan oleh instans Pusat Identitas IAM.

Untuk melihat izin kebijakan ini, lihat [AWSSSODirectoryAdministrator](#) di Referensi Kebijakan AWS Terkelola.

AWS kebijakan yang dikelola: AWSSSOREadOnly

Anda dapat melampirkan kebijakan AWSSSOREadOnly ke identitas IAM Anda.

Kebijakan ini memberikan izin baca-saja yang memungkinkan pengguna melihat informasi di Pusat Identitas IAM. Prinsipal dengan kebijakan ini tidak dapat melihat pengguna atau grup Pusat Identitas IAM secara langsung. Kepala sekolah dengan kebijakan ini terlampir tidak dapat melakukan pembaruan apa pun di Pusat Identitas IAM. Misalnya, kepala sekolah dengan izin ini dapat melihat pengaturan Pusat Identitas IAM, tetapi tidak dapat mengubah nilai setelan apa pun.

Kebijakan ini juga mencakup AWS Key Management Service izin yang diperlukan untuk instans Pusat Identitas IAM yang menggunakan kunci yang dikelola pelanggan untuk enkripsi.

Untuk melihat izin kebijakan ini, lihat [AWSSSOREadOnly](#) di Referensi Kebijakan AWS Terkelola.

AWS kebijakan yang dikelola: AWSSSODirectoryReadOnly

Anda dapat melampirkan kebijakan AWSSSODirectoryReadOnly ke identitas IAM Anda.

Kebijakan ini memberikan izin baca-saja yang memungkinkan pengguna melihat pengguna dan grup di Pusat Identitas IAM. Prinsipal dengan kebijakan ini terlampir tidak dapat melihat penugasan Pusat Identitas IAM, kumpulan izin, aplikasi, atau setelan. Kepala sekolah dengan kebijakan ini terlampir tidak dapat melakukan pembaruan apa pun di Pusat Identitas IAM. Misalnya, kepala sekolah dengan izin ini dapat melihat pengguna Pusat Identitas IAM, tetapi mereka tidak dapat mengubah atribut pengguna atau menetapkan perangkat MFA.

Kebijakan ini juga mencakup AWS Key Management Service izin yang diperlukan untuk instans Pusat Identitas IAM yang menggunakan kunci yang dikelola pelanggan untuk enkripsi.

Untuk melihat izin kebijakan ini, lihat [AWSSSODirectoryReadOnly](#) di Referensi Kebijakan AWS Terkelola.

AWS kebijakan yang dikelola: AWSIdentitySyncFullAccess

Anda dapat melampirkan kebijakan `AWSIdentitySyncFullAccess` ke identitas IAM Anda.

Prinsipal dengan kebijakan ini dilampirkan 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.

Rincian izin

Untuk melihat izin kebijakan ini, lihat [AWSIdentitySyncFullAccess](#) di Referensi Kebijakan AWS Terkelola.

AWS kebijakan yang dikelola: AWSIdentitySyncReadOnlyAccess

Anda dapat melampirkan kebijakan `AWSIdentitySyncReadOnlyAccess` ke identitas IAM Anda.

Kebijakan ini memberikan izin baca-saja 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, kepala sekolah dengan izin ini dapat melihat pengaturan sinkronisasi identitas, tetapi tidak dapat mengubah nilai profil atau filter apa pun.

Untuk melihat izin kebijakan ini, lihat [AWSIdentitySyncReadOnlyAccess](#) di Referensi Kebijakan AWS Terkelola.

AWS kebijakan yang dikelola: AWSSSOServiceRolePolicy

Anda tidak dapat melampirkan `AWSSSOServiceRolePolicy` kebijakan ke identitas IAM Anda.

Kebijakan ini dilampirkan ke peran terkait layanan yang memungkinkan Pusat Identitas IAM mendelegasikan dan menegakkan pengguna mana yang memiliki akses masuk tunggal ke dalam tertentu. Akun AWS AWS Organizations Saat Anda mengaktifkan IAM, peran terkait layanan dibuat di semua bagian dalam organisasi Anda. Akun AWS Pusat Identitas IAM juga membuat peran

terkait layanan yang sama di setiap akun yang kemudian ditambahkan ke organisasi Anda. Peran ini memungkinkan Pusat Identitas IAM mengakses sumber daya setiap akun atas nama Anda. Service-linked peran yang dibuat di masing-masing Akun AWS diberi nama `AWSServiceRoleForSSO`. Untuk informasi selengkapnya, lihat [Menggunakan peran terkait layanan untuk Pusat Identitas IAM](#).

AWS kebijakan yang dikelola: `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`.

Untuk melihat izin kebijakan ini, lihat [AWSIAMIdentityCenterAllowListForIdentityContext](#) di Referensi Kebijakan AWS Terkelola.

AWS kebijakan yang dikelola: `AWSIdentityCenterExternalManagementPolicy`

Anda dapat melampirkan kebijakan `AWSIdentityCenterExternalManagementPolicy` ke identitas IAM Anda.

Kebijakan ini menyediakan akses untuk mengelola pengguna Pusat Identitas IAM dari penyedia eksternal.

Untuk melihat izin kebijakan ini, lihat [AWSIdentityCenterExternalManagementPolicy](#) di Referensi Kebijakan AWS Terkelola.

IAM Identity Center memperbarui ke AWS kebijakan terkelola

Tabel berikut menjelaskan pembaruan kebijakan terkel AWS ola 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.

Ubah	Deskripsi	Date
AWSIdentityCenterExternalManagementPolicy	Kebijakan terkelola yang diperbarui untuk mengubah	Desember 5, 2025

Ubah	Deskripsi	Date
	ARN untuk penyewa penyewa penyewaan.	
AWSIdentityCenterExternalManagementPolicy	Kebijakan ini menyediakan akses untuk mengelola pengguna Pusat Identitas IAM dari penyedia eksternal.	November 21, 2025
AWSSSOMasterAccountAdministrator , AWSSSOMemberAccountAdministrator , AWSSSOReadOnly , AWSSSODirectoryAdministrator , AWSSSODirectoryReadOnly	Kebijakan terkelola yang diperbarui untuk menyertakan AWS KMS izin yang diperlukan untuk instans Pusat Identitas IAM yang menggunakan kunci yang dikelola pelanggan untuk enkripsi.	17. September 2025
AWSSSOServiceRolePolicy	Kebijakan ini sekarang menyertakan izin untuk meneleponidentity-sync:DeleteSyncProfile .	Februari 11, 2025
AWSIAMIdentityCenterAllowListForIdentityContext	Kebijakan ini sekarang mencakup qapps:ListQAppSessionData dan qapps:ExportQAppSessionData tindakan untuk mendukung sesi konsol yang ditingkatkan identitas untuk aplikasi terkel AWS ola yang mendukung sesi ini.	Oktober 2, 2024

Ubah	Deskripsi	Date
<u>AWSSSOMasterAccountAdministrator</u>	Pusat Identitas IAM menambahkan tindakan baru untuk memberikan DeleteSyncProfile izin agar Anda dapat menggunakan kebijakan ini untuk menghapus profil sinkronisasi. Ini adalah tindakan yang terkait dengan DeleteInstance API.	September 26, 2024
<u>AWSIAMIdentityCenterAllowListForIdentityContext</u>	Kebijakan ini sekarang menyertakan s3:ListCallerAccessGrants tindakan untuk mendukung sesi konsol yang ditingkatkan identitas untuk aplikasi terkelola AWS yang mendukung sesi ini.	4 September 2024
<u>AWSIAMIdentityCenterAllowListForIdentityContext</u>	Kebijakan ini sekarang mencakup aoss:APIAccessAll , es:ESHttpHead , es:ESHttpPost , es:ESHttpGet es:ESHttpPatch es:ESHttpDelete , dan es:ESHttpPut tindakan untuk mendukung sesi konsol yang ditingkatkan identitas untuk aplikasi terkelola AWS yang mendukung sesi ini.	Juli 12, 2024

Ubah	Deskripsi	Date
AWSIAMIdentityCenterAllowListForIdentityContext	Kebijakan ini sekarang mencakup <code>qapps:PredictQApp</code> , <code>qapps:ImportDocument</code> , <code>qapps:AssociateLibraryItemReview</code> , <code>qapps:DissociateLibraryItemReview</code> , <code>qapps:GetQAppSession</code> , <code>qapps:UpdateQAppSession</code> , <code>qapps:GetQAppSessionMetadata</code> , <code>qapps:UpdateQAppSessionMetadata</code> , dan <code>qapps:TagResource</code> tindakan untuk mendukung sesi konsol yang ditingkatkan identitas untuk aplikasi terkelola yang mendukung sesi ini.	27 Juni 2024

Ubah	Deskripsi	Date
AWSIAMIdentityCenterAllowListForIdentityContext	Kebijakan ini sekarang mencakup elasticmapreduce:AddJobFlowSteps ,,, elasticmapreduce:DescribeCluster elasticmapreduce:CancelSteps elasticmapreduce:DescribeStep , dan elasticmapreduce:ListSteps tindakan untuk mendukung propagasi identitas tepercaya di Amazon EMR.	17 Mei 2024

Ubah	Deskripsi	Date
<u>AWSIAMIdentityCenterAllowListForIdentityContext</u>	Kebijakan ini sekarang mencakup <code>qapps:CreateQApp</code> , <code>qapps:PredictProblemStatementFromConversation</code> , <code>qapps:PredictQAppFromProblemStatement</code> , <code>qapps:CopyQApp</code> , <code>qapps:GetQApp</code> , <code>qapps:ListQApps</code> , <code>qapps:UpdateQApp</code> , <code>qapps>DeleteQApp</code> , <code>qapps:AssociateQAppWithUser</code> , <code>qapps:DisassociateQAppFromUser</code> , <code>qapps:ImportDocumentToQAppSession</code> , <code>qapps:CreateLibraryItem</code> , <code>qapps:GetLibraryItem</code> , <code>qapps:UpdateLibraryItem</code> , <code>qapps:CreateLibraryItemReview</code> , <code>qapps:ListLibraryItems</code> , <code>qapps:CreateSubscriptionToken</code> , <code>qapps:StartQAppSession</code> , dan <code>qapps:StopQAppSession</code> tindakan untuk mendukung sesi konsol yang	April 30, 2024

Ubah	Deskripsi	Date
	ditingkatkan identitas untuk aplikasi terkel AWS ola yang mendukung sesi ini.	
<u>AWSSSOMasterAccountAdministrator</u>	Kebijakan ini sekarang mencakup <code>signin:CreateTrustedIdentityPropagationApplicationForConsole</code> dan <code>signin:ListTrustedIdentityPropagationApplicationsForConsole</code> tindakan untuk mendukung sesi konsol yang ditingkatkan identitas untuk aplikasi terkel AWS ola yang mendukung sesi ini.	April 26, 2024
<u>AWSSSOMemberAccountAdministrator</u>	Kebijakan ini sekarang mencakup <code>signin:CreateTrustedIdentityPropagationApplicationForConsole</code> dan <code>signin:ListTrustedIdentityPropagationApplicationsForConsole</code> tindakan untuk mendukung sesi konsol yang ditingkatkan identitas untuk aplikasi terkel AWS ola yang mendukung sesi ini.	April 26, 2024

Ubah	Deskripsi	Date
AWSSSOReadOnly	Kebijakan ini sekarang mencakup <code>signin:ListTrustedIdentityPropagationsForConsole</code> tindakan untuk mendukung sesi konsol yang ditingkatkan identitas untuk aplikasi terkel AWS ola yang mendukung sesi ini.	April 26, 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Kebijakan ini sekarang mencakup <code>qbusiness:PutFeedback</code> tindakan untuk mendukung sesi konsol yang ditingkatkan identitas untuk aplikasi terkel AWS ola yang mendukung sesi ini.	April 26, 2024

Ubah	Deskripsi	Date
AWSIAMIdentityCenterAllowListForIdentityContext	Kebijakan ini sekarang mencakup <code>q:StartConversation</code> , <code>q:SendMessage</code> , <code>q:ListConversations</code> , <code>q:GetConversation</code> , <code>q:StartTroubleshootingAnalysis</code> , <code>q:GetTroubleshootingResults</code> , <code>q:StartTroubleshootingResolutionExplanation</code> , dan <code>q:UpdateTroubleshootingCommandResult</code> tindakan untuk mendukung sesi konsol yang ditingkatkan identitas untuk aplikasi terkel AWS ola yang mendukung sesi ini.	April 24, 2024
AWSIAMIdentityCenterAllowListForIdentityContext	Kebijakan ini sekarang mencakup <code>sts:SetContext</code> tindakan untuk mendukung sesi konsol yang ditingkatkan identitas untuk aplikasi terkel AWS ola yang mendukung sesi ini.	April 19, 2024

Ubah	Deskripsi	Date
<u>AWSIAMIdentityCenterAllowListForIdentityContext</u>	Kebijakan ini sekarang mencakup <code>qbusiness:Chat</code> , <code>qbusiness:ChatSync</code> , <code>qbusiness:ListConversations</code> , <code>qbusiness:ListMessages</code> , dan <code>qbusiness:DeleteConversation</code> tindakan untuk mendukung sesi konsol yang ditingkatkan identitas untuk aplikasi terkelola AWS yang mendukung sesi ini.	April 11, 2024
<u>AWSIAMIdentityCenterAllowListForIdentityContext</u>	Kebijakan ini sekarang mencakup <code>s3:GetDataAccess</code> tindakan <code>s3:GetAccessGrants</code> dan <code>InstanceForPrefix</code> dan.	26 November 2023
<u>AWSIAMIdentityCenterAllowListForIdentityContext</u>	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
<u>AWSSSODirectoryReadOnly</u>	Kebijakan ini sekarang menyertakan namespace baru <code>identitystore-auth</code> dengan izin baru untuk memungkinkan pengguna membuat daftar dan mendapatkan sesi.	21 Februari 2023

Ubah	Deskripsi	Date
AWSSSOServiceRolePolicy	Kebijakan ini sekarang memungkinkan UpdateSAMLProvider tindakan diambil pada akun manajemen .	20 Oktober 2022
AWSSSOMasterAccountAdministrator	Kebijakan ini sekarang menyertakan namespace baru <code>identitystore-auth</code> dengan izin baru untuk mengizinkan admin membuat daftar dan menghapus sesi untuk pengguna.	20 Oktober 2022
AWSSSOMemberAccountAdministrator	Kebijakan ini sekarang menyertakan namespace baru <code>identitystore-auth</code> dengan izin baru untuk mengizinkan admin membuat daftar dan menghapus sesi untuk pengguna.	20 Oktober 2022
AWSSSODirectoryAdministrator	Kebijakan ini sekarang menyertakan namespace baru <code>identitystore-auth</code> dengan izin baru untuk mengizinkan admin membuat daftar dan menghapus sesi untuk pengguna.	20 Oktober 2022

Ubah	Deskripsi	Date
<u>AWSSSOMasterAccountAdministrator</u>	Kebijakan ini sekarang menyertakan izin baru untuk menelepon <u>ListDelegatedAdministrators</u> on AWS Organizations. Kebijakan ini juga sekarang menyertakan subset izin AWSSSOManageDelegatedAdministrator yang mencakup izin untuk memanggil <u>RegisterDelegatedAdministrator</u> dan <u>DeregisterDelegatedAdministrator</u> .	Agustus 16, 2022
<u>AWSSSOMemberAccountAdministrator</u>	Kebijakan ini sekarang menyertakan izin baru untuk menelepon <u>ListDelegatedAdministrators</u> on AWS Organizations. Kebijakan ini juga sekarang menyertakan subset izin AWSSSOManageDelegatedAdministrator yang mencakup izin untuk memanggil <u>RegisterDelegatedAdministrator</u> dan <u>DeregisterDelegatedAdministrator</u> .	Agustus 16, 2022

Ubah	Deskripsi	Date
AWSSSOReadOnly	Kebijakan ini sekarang menyertakan izin baru untuk menelepon ListDelegatedAdministrators on AWS Organizations.	Agustus 11, 2022
AWSSSOServiceRolePolicy	Kebijakan ini sekarang menyertakan izin baru untuk menelepon DeleteRolePermissionsBoundary dan PutRolePermissionsBoundary .	14 Juli 2022
AWSSSOServiceRolePolicy	Kebijakan ini sekarang menyertakan izin baru yang mengizinkan panggilan ListAWSServiceAccessForOrganization and ListDelegatedAdministrators masuk AWS Organizations.	Mei 11, 2022
AWSSSOMasterAccountAdministrator AWSSSOMemberAccountAdministrator AWSSSOReadOnly	Tambahkan izin Penganalisis Akses IAM yang memungkinkan kepala sekolah menggunakan pemeriksaan kebijakan untuk validasi.	28 April 2022

Ubah	Deskripsi	Date
AWSSSOMasterAccountAdministrator	<p>Kebijakan ini sekarang mengizinkan semua tindakan layanan IAM Identity Center Identity Store.</p> <p>Untuk informasi tentang tindakan yang tersedia di layanan IAM Identity Center Identity Store, lihat Referensi API Identity Center Identity Store IAM.</p>	29 Maret 2022
AWSSSOMemberAccountAdministrator	Kebijakan ini sekarang mengizinkan semua tindakan layanan IAM Identity Center Identity Store.	29 Maret 2022
AWSSSODirectoryAdministrator	Kebijakan ini sekarang mengizinkan semua tindakan layanan IAM Identity Center Identity Store.	29 Maret 2022
AWSSSODirectoryReadOnly	Kebijakan ini sekarang memberikan akses ke tindakan pembacaan layanan IAM Identity Center Identity Store IAM. 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

Ubah	Deskripsi	Date
AWSIdentitySyncReadOnlyAccess	Kebijakan ini memberikan izin baca-saja yang memungkinkan kepala sekolah untuk melihat setelah sinkronisasi identitas.	3 Maret 2022
AWSSSOReadOnly	Kebijakan ini memberikan izin baca-saja yang memungkinkan kepala sekolah untuk melihat setelah konfigurasi Pusat Identitas IAM.	4 Agustus 2021
Pusat Identitas IAM mulai melacak perubahan	Pusat Identitas IAM mulai melacak perubahan untuk kebijakan ter AWS kelola.	4 Agustus 2021

Menggunakan peran terkait layanan untuk Pusat Identitas IAM

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 sebelumnya oleh Pusat Identitas IAM dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda. Untuk informasi selengkapnya, lihat [Memahami peran terkait layanan di Pusat Identitas IAM](#).

Peran terkait layanan membuat pengaturan Pusat Identitas IAM 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, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat [AWS Layanan yang Bekerja dengan IAM](#) dan cari layanan yang memiliki Ya di kolom Peran Service-Linked . Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Service-linked izin peran untuk Pusat Identitas IAM

Pusat Identitas IAM menggunakan peran terkait layanan yang dinamai `AWSServiceRoleForSSO` untuk memberikan izin Pusat Identitas IAM untuk mengelola AWS sumber daya, termasuk peran IAM, kebijakan, dan IdP SAML atas nama Anda.

Per `AWSServiceRoleForSSO` an terkait layanan mempercayai layanan berikut untuk mengambil peran:

- Pusat Identitas IAM (awalan layanan: `sso`)

Kebijakan izin `AWSSSOServiceRolePolicy` peran yang ditautkan layanan memungkinkan Pusat Identitas IAM untuk menyelesaikan peran berikut pada 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 `AWSSSOServiceRolePolicy` peran terkait layanan memungkinkan Pusat Identitas IAM untuk menyelesaikan hal berikut pada penyedia SAML dengan awalan nama sebagai `"AWSSSO_"`:

- `iam:CreateSAMLProvider`
- `iam:GetSAMLProvider`
- `iam:UpdateSAMLProvider`
- `iam>DeleteSAMLProvider`

Kebijakan AWSSSOServiceRolePolicy izin peran terkait layanan memungkinkan Pusat Identitas IAM menyelesaikan hal berikut pada semua organisasi:

- `organizations:DescribeAccount`
- `organizations:DescribeOrganization`
- `organizations:ListAccounts`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:ListDelegatedAdministrators`

Kebijakan AWSSSOServiceRolePolicy izin peran terkait layanan memungkinkan Pusat Identitas IAM menyelesaikan hal berikut pada semua peran IAM (*):

- `iam:listRoles`

Kebijakan izin peran AWSSSOServiceRolePolicy terkait layanan memungkinkan Pusat Identitas IAM untuk menyelesaikan hal berikut di “arn:aws:iam: *: -service- .amazonaws. role/aws role/sso com/ AWSServiceRoleForSSO”:

- `iam:GetServiceLinkedRoleDeletionStatus`
- `iam>DeleteServiceLinkedRole`

Kebijakan izin peran AWSSSOServiceRolePolicy terkait layanan memungkinkan Pusat Identitas IAM menyelesaikan hal berikut pada “arn:aws:identity-sync: *: *:profile/*”:

- `identity-sync>DeleteSyncProfile`

Untuk informasi selengkapnya tentang pembaruan kebijakan AWSSSOServiceRolePolicy izin peran terkait layanan, lihat. [IAM Identity Center memperbarui ke AWS kebijakan terkelola](#)

JSON

```
{
  "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": [
      "*"
    ]
  },
  {
    "Sid": "AllowDeleteSyncProfile",
    "Effect": "Allow",
    "Action": [
      "identity-sync:DeleteSyncProfile"
    ],
    "Resource": [
      "arn:aws:identity-sync:*:*:profile/*"
    ]
  }
]
}

```

Anda harus mengonfigurasi izin agar entitas IAM (seperti pengguna, grup, atau peran) dapat membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat izin [Service-linked peran](#) di Panduan Pengguna IAM.

Membuat peran terkait layanan untuk Pusat Identitas IAM

Anda tidak perlu membuat peran terkait layanan secara manual. Setelah diaktifkan, Pusat Identitas IAM membuat peran terkait layanan di semua akun dalam organisasi di Organisasi. AWS Pusat Identitas IAM juga membuat peran terkait layanan yang sama di setiap akun yang kemudian ditambahkan ke organisasi Anda. Peran ini memungkinkan Pusat Identitas IAM mengakses sumber daya setiap akun atas nama Anda.

Catatan

- Jika Anda masuk ke akun AWS Organizations manajemen, akun tersebut menggunakan peran Anda yang saat ini masuk dan bukan peran terkait layanan. Ini mencegah eskalasi hak istimewa.

- Ketika Pusat Identitas IAM melakukan operasi IAM apa pun di akun AWS Organizations manajemen, semua operasi dilakukan menggunakan kredensial 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 Pusat Identitas IAM sebelum 7 Desember 2017, ketika layanan tersebut mulai mendukung peran terkait layanan, maka Pusat Identitas IAM membuat peran tersebut `AWSServiceRoleForSSO` 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 Pusat Identitas IAM

Pusat Identitas IAM tidak mengizinkan Anda mengedit peran terkait `AWSServiceRoleForSSO` layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin merujuk peran tersebut. Namun, Anda dapat mengedit penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat [Mengedit peran terkait layanan](#) dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk Pusat Identitas IAM

Anda tidak perlu menghapus `AWSServiceRoleForSSO` peran secara manual. Ketika sebuah Akun AWS dihapus dari AWS organisasi, Pusat Identitas IAM 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, 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. [Menghapus akses pengguna dan grup ke Akun AWS](#) untuk semua pengguna dan grup yang memiliki akses ke Akun AWS.
2. [Menghapus kumpulan izin di Pusat Identitas IAM](#) yang telah Anda kaitkan dengan Akun AWS.

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, CLI IAM, atau API CLI untuk menghapus peran tertaut layanan `AWSServiceRoleForSSO`. Untuk informasi selengkapnya, lihat [Menghapus Service-Linked Per](#) an di Panduan Pengguna IAM.

Konsol Pusat Identitas IAM 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 instance Pusat Identitas IAM yang 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 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 penyangkalan eksplisit atas 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 yang 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
UpdateApplicationInstanceDisplayData UpdateApplicationInstanceStatus UpdateManagedApplicationInstanceStatus	UpdateApplication

Tindakan API setelah Oktober 2020

Instans Pusat Identitas IAM yang dibuat sebelum 15 Oktober 2020 menghormati tindakan API lama dan baru selama tidak ada penolakan eksplisit atas 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
DetachManagedPolicy	DeletePermissionsPolicy	DetachManagedPolicyFromPermissionSet
DisassociateProfile	DisassociateProfile	DeleteAccountAssignment
GetApplicationInstanceForAWSAccount	GetApplicationInstance	ListAccountAssignments
GetAWSAccountProfileStatus	GetProfile	ListPermissionSetsProvisionedToAccount
GetPermissionSet	GetPermissionSet	DescribePermissionSet

Operation name	API actions used before October 15, 2020	API actions used after October 15, 2020
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
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, dan metadata tentang permintaan itu sendiri. Service-specific kunci kondisi didefinisikan untuk digunakan dengan AWS layanan individual.

IAM Identity Center menyertakan penyedia AWS STS konteks yang memungkinkan aplikasi terkel AWS ola dan aplikasi pihak ketiga untuk menambahkan nilai untuk kunci kondisi yang ditentukan oleh Pusat Identitas IAM. Kunci-kunci ini disertakan dalam peran https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html IAM. Nilai-nilai kunci ditetapkan ketika aplikasi meneruskan token ke AWS STS. Aplikasi memperoleh token yang diteruskan dengan AWS STS salah satu cara berikut:

- Selama otentikasi dengan Pusat Identitas IAM.
- Setelah pertukaran token dengan penerbit token [tepercaya](#) untuk propagasi identitas tepercaya. Dalam hal ini, aplikasi memperoleh token dari penerbit token tepercaya dan menukar token tersebut dengan token dari Pusat Identitas IAM.

Kunci ini biasanya digunakan oleh aplikasi yang terintegrasi dengan propagasi identitas tepercaya. Dalam beberapa kasus, ketika nilai kunci ada, 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 Pusat Identitas IAM mana yang menggunakan peran tersebut. Contohnya mirip dengan menggunakan `SourceId`. Namun `SourceId`, tidak seperti, nilai untuk `UserId` mewakili pengguna tertentu yang diverifikasi dari penyimpanan 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](#)
- [toko identitas: IdentityStoreArn](#)
- [pusat identitas: ApplicationArn](#)
- [pusat identitas: CredentialId](#)
- [pusat identitas: InstanceArn](#)

toko identitas: UserId

Kunci konteks ini adalah `UserId` milik pengguna Pusat Identitas IAM yang menjadi subjek pernyataan konteks yang dikeluarkan oleh Pusat Identitas IAM. Pernyataan konteks diteruskan ke

AWS STS. Anda dapat menggunakan kunci ini untuk membandingkan pengguna Pusat Identitas IAM atas nama siapa permintaan dibuat dengan pengidentifikasi untuk pengguna yang Anda tentukan dalam kebijakan. `UserId`

- Ketersediaan — Kunci ini disertakan dalam konteks permintaan setelah pernyataan konteks yang dikeluarkan oleh Pusat Identitas IAM ditetapkan, 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 — Single-valued

toko identitas: `IdentityStoreArn`

Kunci konteks ini adalah ARN dari penyimpanan identitas yang dilampirkan ke instance Pusat Identitas IAM yang mengeluarkan pernyataan konteks. Ini juga merupakan toko identitas tempat Anda dapat mencari `identitystore:UserID`. Anda dapat menggunakan kunci ini dalam kebijakan untuk menentukan apakah `identitystore:UserID` berasal dari penyimpanan identitas ARN yang diharapkan.

- Ketersediaan — Kunci ini disertakan dalam konteks permintaan setelah pernyataan konteks yang dikeluarkan oleh Pusat Identitas IAM ditetapkan, 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 — Single-valued

pusat identitas: `ApplicationArn`

Kunci konteks ini adalah ARN dari aplikasi tempat 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 Pusat Identitas IAM.
- Tipe data — [Arn](#), [String](#)
- Jenis nilai — Single-valued

pusat identitas: CredentialId

Kunci konteks ini adalah ID acak untuk kredensial peran yang ditingkatkan 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 Pusat Identitas IAM.
- Tipe data — [String](#)
- Jenis nilai — Single-valued

pusat identitas: InstanceArn

Kunci konteks ini adalah ARN dari instance Pusat Identitas IAM yang mengeluarkan pernyataan konteks untuk `identitystore:UserID` Anda dapat menggunakan kunci ini untuk menentukan apakah pernyataan konteks `identitystore:UserID` dan berasal dari ARN instance Pusat Identitas IAM yang diharapkan.

- Ketersediaan — Kunci ini disertakan dalam konteks permintaan operasi AWS STS AssumeRole API. Konteks permintaan mencakup pernyataan konteks yang dikeluarkan oleh Pusat Identitas IAM.
- Tipe data — [Arn](#), [String](#)
- Jenis nilai — Single-valued

Pencatatan dan pemantauan di Pusat Identitas IAM

Praktik terbaik adalah memantau organisasi Anda untuk memastikan bahwa perubahan dicatat. Pemantauan membantu Anda memastikan bahwa Anda dapat menyelidiki perubahan yang tidak terduga dan mengembalikan perubahan yang tidak diinginkan. IAM Identity Center saat ini mendukung dua AWS layanan yang membantu Anda memantau organisasi Anda dan aktivitas yang terjadi di dalamnya: AWS CloudTrail dan Amazon EventBridge.

Topik

- [Mencatat panggilan API Pusat Identitas IAM dengan AWS CloudTrail](#)
- [Pencatatan panggilan SCIM API IAM Identity Center dengan AWS CloudTrail](#)

- [Hubungkan komponen aplikasi dengan Amazon EventBridge](#)
- [Pencatatan 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 Pusat Identitas IAM. CloudTrail menangkap panggilan API untuk Pusat Identitas IAM 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 terus menerus ke bucket Amazon S3, termasuk acara untuk Pusat Identitas IAM. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol di 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 itu dibuat, dan detail tambahan.

Untuk mempelajari selengkap CloudTrail nya, lihat Panduan [AWS CloudTrail Pengguna](#).

Tabel berikut merangkum CloudTrail peristiwa Pusat Identitas IAM, sumber CloudTrail peristiwa, dan API yang cocok. Lihat referensi API Pusat Identitas [IAM](#) untuk mempelajari lebih lanjut tentang API.

Note

Ada grup CloudTrail acara tambahan, yang disebut Sign-in, yang dipan AWS carkan untuk masuk AWS sebagai pengguna Pusat Identitas IAM. Peristiwa ini tidak memiliki API publik yang cocok, dan karenanya tidak tercantum dalam referensi API.

CloudTrail acara	API Publik	Deskripsi	CloudTrail sumber acara
Pusat Identitas IAM	Pusat Identitas IAM	API Pusat Identitas IAM memungkinkan pengelolaan kumpulan izin, aplikasi, penerbit token tepercaya,	sso.amazonaws.com

CloudTrail acara	API Publik	Deskripsi	CloudTrail sumber acara
		penugasan akun dan aplikasi, instans Pusat Identitas IAM, dan tag.	
Toko Identitas	Toko Identitas	Identity Store API memungkinkan pengelolaan siklus hidup pengguna dan grup tenaga kerja Anda, serta keanggotaan grup pengguna. Juga, mereka mendukung pengelolaan perangkat MFA pengguna.	sso-directory.amazonaws.com, identitystore.amazonaws.com
OID C	OID C	API OIDC mendukung propagasi identitas tepercaya, dan masuk ke AWS CLI dan toolkit IDE sebagai pengguna Pusat Identitas IAM yang sudah diautentikasi.	sso.amazonaws.com, sso-oauth.amazonaws.com
AWS portal akses	AWS portal akses	API portal AWS akses mendukung operasi portal AWS akses dan pengguna mendapatkan kredensial akun melalui AWS CLI.	sso.amazonaws.com

CloudTrail acara	API Publik	Deskripsi	CloudTrail sumber acara
SCIM	SCIM	API SCIM mendukung penyediaan pengguna, grup, dan keanggotaan grup melalui protokol SCIM. Untuk informasi selengkapnya, lihat Pencatatan panggilan SCIM API IAM Identity Center dengan AWS CloudTrail .	identitystore-scim.amazonaws.com
AWS Sign-In	Tidak ada API publik	AWS memancarkan Sign-in CloudTrail peristiwa untuk otentikasi pengguna dan aliran federasi ke Pusat Identitas IAM.	signin.amazonaws.com

Topik

- [CloudTrail kasus penggunaan untuk Pusat Identitas IAM](#)
- [Informasi Pusat Identitas IAM di CloudTrail](#)

CloudTrail kasus penggunaan untuk Pusat Identitas IAM

Per CloudTrail peristiwa yang dipancarkan Pusat Identitas IAM dapat berharga untuk berbagai kasus penggunaan. Organisasi dapat menggunakan log peristiwa ini untuk memantau dan mengaudit akses dan aktivitas pengguna dalam AWS lingkungan mereka. Ini dapat membantu kasus penggunaan kepatuhan, karena log menangkap detail tentang siapa yang mengakses sumber daya apa dan kapan. Anda juga dapat menggunakan CloudTrail data untuk investigasi insiden, memungkinkan tim menganalisis tindakan pengguna dan melacak perilaku yang mencurigakan. Selain itu, riwayat acara

dapat mendukung upaya pemecahan masalah, memberikan visibilitas ke dalam perubahan yang dilakukan pada izin pengguna dan konfigurasi dari waktu ke waktu.

Bagian berikut menjelaskan kasus penggunaan dasar yang menginformasikan alur kerja Anda seperti audit, investigasi insiden, dan pemecahan masalah.

Mengidentifikasi pengguna di peristiwa yang diprakarsai pengguna CloudTrail Pusat Identitas IAM

Pusat Identitas IAM memancarkan dua CloudTrail bidang yang memungkinkan Anda mengidentifikasi pengguna Pusat Identitas IAM di balik CloudTrail peristiwa, seperti masuk ke Pusat Identitas IAM atau AWS CLI, dan menggunakan portal AWS akses, termasuk mengelola perangkat MFA:

- `userId`— Pengidentifikasi pengguna yang unik dan tidak dapat diubah dari Identity Store dari instance Pusat Identitas IAM.
- `identityStoreArn`— Nama Sumber Daya Amazon (ARN) dari Identity Store yang berisi pengguna.

`identityStoreArn` dan `userId` ang dan ditampilkan dalam `onBehalfOf` elemen bersarang di dalam `userIdentity` elemen seperti yang ditunjukkan dalam contoh log CloudTrail peristiwa berikut. Log peristiwa ini menunjukkan dua bidang ini pada acara di mana `userIdentity` isnya adalah `"IdentityCenterUser"`. Anda juga dapat menemukan bidang ini pada acara untuk pengguna Pusat Identitas IAM yang diautentikasi di mana `userIdentity` isnya adalah `"Unknown"`. Alur kerja Anda harus menerima kedua nilai tipe.

```
"userIdentity":{
  "type":"IdentityCenterUser",
  "accountId":"111122223333",
  "onBehalfOf": {
    "userId": "544894e8-80c1-707f-60e3-3ba6510dfac1",
    "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
  },
  "credentialId" : "90e292de-5eb8-446e-9602-90f7c45044f7"
}
```

Tip

Kami menyarankan Anda menggunakan `userId` dan `identityStoreArn` untuk mengidentifikasi pengguna di balik CloudTrail peristiwa Pusat Identitas IAM.

`principalId` `username` dan di bawah `userIdentity` elemen tidak lagi tersedia. Jika alur kerja Anda, seperti audit atau respons insiden, bergantung pada memiliki akses ke `username`, Anda memiliki dua opsi:

- Ambil nama pengguna dari direktori Pusat Identitas IAM seperti yang dijelaskan di [Nama pengguna dalam acara masuk CloudTrail](#).
- Dapatkan `Username` yang dipancarkan Pusat Identitas IAM di bawah `additionalEventData` elemen di Sign-in. Opsi ini tidak memerlukan akses ke direktori Pusat Identitas IAM. Untuk informasi selengkapnya, lihat [Nama pengguna dalam acara masuk CloudTrail](#).

Untuk mengambil detail pengguna, termasuk `username` bidang, Anda menanyakan Identity Store dengan ID pengguna dan ID Penyimpanan Identitas sebagai parameter. Anda dapat melakukan tindakan ini melalui permintaan [DescribeUser](#) API atau melalui CLI. Berikut ini adalah contoh perintah CLI. Anda dapat menghilangkan `region` parameter jika instance Pusat Identitas IAM Anda berada di Wilayah default CLI.

```
aws identitystore describe-user \
--identity-store-id d-1234567890 \
--user-id 544894e8-80c1-707f-60e3-3ba6510dfac1 \
--region your-region-id
```

Untuk menentukan nilai Identity Store ID untuk perintah CLI pada contoh sebelumnya, Anda dapat mengekstrak ID Penyimpanan Identitas dari `identityStoreArn` nilai. Dalam contoh `ARNarn:aws:identitystore::111122223333:identitystore/d-1234567890`, Identity Store ID adalah `d-1234567890`. Atau, Anda dapat menemukan Identity Store ID dengan menavigasi ke tab Identity Store di bagian Pengaturan konsol Pusat Identitas IAM.

Jika Anda mengotomatiskan pencarian pengguna di direktori Pusat Identitas IAM, sebaiknya Anda memperkirakan frekuensi pencarian pengguna, dan mempertimbangkan batas throttle Pusat Identitas [IAM di Identity Store API](#). Caching atribut pengguna yang diambil dapat membantu Anda tetap berada dalam batas throttle.

Menghubungkan peristiwa pengguna dalam sesi pengguna yang sama

`Bid` [AuthWorkflowID](#) yang dipancarkan dalam peristiwa masuk memungkinkan pelacakan semua CloudTrail peristiwa yang terkait dengan urutan masuk sebelum dimulainya sesi pengguna Pusat Identitas IAM.

Untuk tindakan pengguna di dalam portal AWS akses, `credentialId` nilainya diatur ke ID sesi pengguna Pusat Identitas IAM yang digunakan untuk meminta tindakan. Anda dapat menggunakan nilai ini untuk mengidentifikasi CloudTrail peristiwa yang dimulai dalam sesi pengguna Pusat Identitas IAM yang diautentikasi yang sama di portal AWS akses.

Note

Anda tidak dapat menggunakannya `credentialId` untuk menghubungkan peristiwa masuk dengan peristiwa berikutnya, seperti penggunaan portal AWS akses. Nilai `credentialId` bidang yang dipancarkan dalam acara masuk memiliki penggunaan internal, dan kami sarankan Anda tidak mengandalkannya. Nilai `credentialId` bidang yang dipancarkan untuk peristiwa portal [AWS akses yang](#) dipanggil dengan OIDC sama dengan ID token akses.

Mengidentifikasi detail sesi latar belakang pengguna di peristiwa yang diprakarsai pengguna CloudTrail Pusat Identitas IAM

A CloudTrail cara berikut menangkap proses pertukaran token OAuth 2.0, di mana token akses yang ada (`theSubjectToken`) yang mewakili sesi interaktif pengguna ditukar dengan token penyegaran (`theRequestedTokenType`). Token penyegaran memungkinkan setiap pengguna yang memulai pekerjaan yang berjalan lama untuk terus berjalan dengan izin pengguna, bahkan setelah pengguna keluar.

Untuk sesi latar belakang [pengguna Pusat Identitas IAM](#), CloudTrail acara menyertakan elemen tambahan yang dipanggil `resource` dalam `requestParameters` elemen. `resourceParameter` berisi Nama Sumber Daya Amazon (ARN) dari pekerjaan yang berjalan di latar belakang. Elemen ini hanya ada dalam catatan CloudTrail peristiwa dan tidak disertakan dalam tanggapan IAM Identity Center [CreateTokenWithIAM](#) API atau SDK.

```
{
  "clientId": "EXAMPLE-CLIENT-ID",
  "grantType": "urn:ietf:params:oauth:grant-type:token-exchange",
  "code": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "redirectUri": "https://example.com/callback",
  "assertion": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "subjectToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "subjectTokenType": "urn:ietf:params:oauth:token-type:access_token",
  "requestedTokenType": "urn:ietf:params:oauth:token-type:refresh_token",
  "resource": "arn:aws:sagemaker:us-west-2:123456789012:training-job/my-job"
```

```
}
```

Menghubungkan pengguna antara Pusat Identitas IAM dan direktori eksternal

Pusat Identitas IAM menyediakan dua atribut pengguna yang dapat Anda gunakan untuk menghubungkan pengguna di direktorinya dengan pengguna yang sama di direktori eksternal (misalnya, Microsoft Active Directory dan Okta Universal Directory).

- `externalId`— Pengidentifikasi eksternal pengguna Pusat Identitas IAM. Kami sarankan Anda memetakan pengidentifikasi ini ke pengenalan pengguna yang tidak dapat diubah di direktori eksternal. Perhatikan bahwa Pusat Identitas IAM tidak memancarkan nilai ini di CloudTrail.
- `username`— Nilai yang disediakan pelanggan yang biasanya digunakan pengguna untuk masuk. Nilai dapat berubah (misalnya, dengan pembaruan SCIM). Perhatikan bahwa ketika sumber identitas adalah Directory Service, nama pengguna yang dipancarkan Pusat Identitas IAM CloudTrail cocok dengan nama pengguna yang Anda masukkan untuk otentikasi. Nama pengguna tidak harus sama persis dengan nama pengguna di direktori Pusat Identitas IAM.

Jika Anda memiliki akses ke CloudTrail acara tetapi tidak ke direktori Pusat Identitas IAM, Anda dapat menggunakan nama pengguna yang dipancarkan di bawah `additionalEventData` elemen saat masuk. Untuk detail selengkapnya tentang nama pengguna di `additionalEventData`, lihat [Nama pengguna dalam acara masuk CloudTrail](#).

Pemetaan dua atribut pengguna ini ke atribut pengguna yang sesuai dalam direktori eksternal didefinisikan di Pusat Identitas IAM ketika sumber identitas adalah Directory Service. Untuk informasi, lihat [Pemetaan atribut antara Pusat Identitas IAM dan direktori Penyedia Identitas Eksternal](#). Ekster IdPs nal yang menyediakan pengguna dengan SCIM memiliki pemetaan mereka sendiri. Bahkan jika Anda menggunakan direktori Pusat Identitas IAM sebagai sumber identitas, Anda dapat menggunakan `externalId` atribut untuk mereferensikan silang prinsip-prinsip keamanan ke direktori eksternal Anda.

Bagian berikut menjelaskan bagaimana Anda dapat mencari pengguna Pusat Identitas IAM berdasarkan pengguna `username` dan `externalId`.

Melihat pengguna Pusat Identitas IAM berdasarkan nama pengguna dan `ExternalID`

Anda dapat mengambil atribut pengguna dari direktori Pusat Identitas IAM untuk nama pengguna yang dikenal dengan terlebih dahulu meminta yang sesuai `userId` menggunakan permintaan [GetUserId](#) API, lalu mengeluarkan permintaan [DescribeUser](#) API, seperti yang ditunjukkan pada contoh sebelumnya. Contoh berikut menunjukkan bagaimana Anda dapat mengambil `userId` dari

Identity Store untuk nama pengguna tertentu. Anda dapat menghilangkan `region` parameter jika instance Pusat Identitas IAM Anda berada di Wilayah default dengan CLI.

```
aws identitystore get-user-id \
  --identity-store d-9876543210 \
  --alternate-identifier '{
    "UniqueAttribute": {
      "AttributePath": "username",
      "AttributeValue": "anyuser@example.com"
    }
  }' \
  --region your-region-id
```

Demikian pula, Anda dapat menggunakan mekanisme yang sama ketika Anda mengetahuinya `externalId`. Perbarui jalur atribut dalam contoh sebelumnya dengan `externalId` nilai, dan nilai atribut dengan spesifik `externalId` yang Anda cari.

Melihat Secure Identifier (SID) pengguna di Microsoft Active Directory (AD) dan `ExternalId`

Dalam kasus tertentu, Pusat Identitas IAM memancarkan SID pengguna di `principalId` bidang CloudTrail peristiwa, seperti yang dipancarkan portal AWS akses dan API OIDC. Kasus-kasus ini sedang dihapus. Sebaiknya alur kerja Anda menggunakan atribut AD `objectguid` saat Anda memerlukan pengenalan pengguna unik dari AD. Anda dapat menemukan nilai ini di `externalId` atribut di direktori Pusat Identitas IAM. Namun, jika alur kerja Anda memerlukan penggunaan SID, ambil nilai dari AD karena tidak tersedia melalui API Pusat Identitas IAM.

[Menghubungkan peristiwa pengguna dalam sesi pengguna yang sama](#) menjelaskan bagaimana Anda dapat menggunakan `username` bidang `externalId` dan untuk menghubungkan pengguna Pusat Identitas IAM dengan pengguna yang cocok di direktori eksternal. Secara default, Pusat Identitas IAM memetakan `externalId` ke `objectguid` atribut di AD, dan pemetaan ini diperbaiki. Pusat Identitas IAM memungkinkan administrator fleksibilitas untuk memetakan `username` secara berbeda dari pemetaan defaultnya `userprincipalname` di AD.

Anda dapat melihat pemetaan ini di konsol Pusat Identitas IAM. Arahkan ke tab Sumber Identitas Pengaturan, dan pilih Kelola sinkronisasi di menu Tindakan. Di bagian Kelola Sinkronisasi, pilih tombol Lihat pemetaan atribut.

Meskipun Anda dapat menggunakan pengidentifikasi pengguna AD unik apa pun yang tersedia di Pusat Identitas IAM untuk mencari pengguna di AD, sebaiknya gunakan dalam kueri Anda karena `objectguid` ini adalah pengidentifikasi yang tidak dapat diubah. Contoh berikut menunjukkan

cara menanyakan Microsoft AD dengan Powershell untuk mengambil pengguna menggunakan objectguid nilai 16809ecc-7225-4c20-ad98-30094aefdbca pengguna. Tanggapan yang berhasil untuk kueri ini mencakup SID pengguna.

```
Install-WindowsFeature -Name RSAT-AD-PowerShell

Get-ADUser `
  -Filter {objectGUID -eq [GUID]::Parse("16809ecc-7225-4c20-ad98-30094aefdbca")} `
  -Properties *
```

Informasi Pusat Identitas IAM di CloudTrail

CloudTrail diaktifkan pada Anda Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi di Pusat Identitas IAM, aktivitas tersebut dicatat dalam suatu CloudTrail acara bersama dengan peristiwa AWS layanan lainnya di riwayat acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di Akun AWS. Untuk informasi selengkapnya, lihat [Melihat acara dengan CloudTrail riwayat acara](#).

Note

Untuk informasi selengkapnya tentang bagaimana identifikasi pengguna dan pelacakan tindakan pengguna dalam CloudTrail peristiwa berkembang, lihat [Perubahan penting pada CloudTrail peristiwa untuk Pusat Identitas IAM](#) di Blog AWS Keamanan.

Untuk catatan acara yang berkelanjutan di Anda Akun AWS, termasuk acara untuk Pusat Identitas IAM, buat jejak. Jejak CloudTrail memungkinkan pengiriman file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol tersebut, jejak diterapkan ke semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di AWS partisi dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan bertindak berdasarkan data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat topik berikut di Panduan Pengguna AWS CloudTrail :

- [Ikhtisar untuk membuat jejak](#)
- [CloudTrail layanan dan integrasi yang didukung](#)
- [Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail](#)
- [Mener CloudTrail ima file log dari beberapa Wilayah](#) dan [M CloudTrail enerima file log dari beberapa akun](#)

Saat CloudTrail logging diaktifkan di Anda Akun AWS, panggilan API yang dilakukan ke tindakan Pusat Identitas IAM dilacak dalam file log. Catatan Pusat Identitas IAM 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 acara untuk API Pusat Identitas IAM yang didukung

Bagian berikut memberikan informasi tentang CloudTrail peristiwa yang terkait dengan API berikut yang didukung IAM Identity Center:

- [API Pusat Identitas IAM](#)
- [API Toko Identitas](#)
- [API OIDC](#)
- [AWS akses portal API](#)
- [API SCIM](#)

CloudTrail peristiwa operasi API Pusat Identitas IAM

Daftar berikut berisi CloudTrail peristiwa yang dipancarkan oleh operasi Pusat Identitas IAM publik dengan sumber `sso.amazonaws.com` peristiwa. Untuk informasi selengkapnya tentang operasi API Pusat Identitas IAM publik, lihat Referensi API Pusat Identitas [IAM](#).

Anda mungkin menemukan peristiwa tambahan CloudTrail untuk operasi API konsol IAM Identity Center yang bergantung pada konsol. Untuk informasi selengkapnya tentang API konsol ini, lihat Referensi [Otorisasi Layanan](#).

- [AttachCustomerManagedPolicyReferenceToPermissionSet](#)
- [AttachManagedPolicyToPermissionSet](#)
- [CreateAccountAssignment](#)
- [CreateApplication](#)
- [CreateApplicationAssignment](#)
-

[CreateInstance](#)

- [CreateInstanceAccessControlAttributeConfiguration](#)
- [CreatePermissionSet](#)
- [CreateTrustedTokenIssuer](#)
- [DeleteAccountAssignment](#)
- [DeleteApplication](#)
- [DeleteApplicationAccessScope](#)
- [DeleteApplicationAssignment](#)
- [DeleteApplicationAuthenticationMethod](#)
- [DeleteApplicationGrant](#)
- [DeleteInlinePolicyFromPermissionSet](#)
- [DeleteInstance](#)
- [DeleteInstanceAccessControlAttributeConfiguration](#)
- [DeletePermissionsBoundaryFromPermissionSet](#)
- [DeletePermissionSet](#)
- [DeleteTrustedTokenIssuer](#)
- [DescribeAccountAssignmentCreationStatus](#)
- [DescribeAccountAssignmentDeletionStatus](#)

- [DescribeApplication](#)
- [DescribeApplicationAssignment](#)
- [DescribeApplicationProvider](#)
- [DescribeInstance](#)
- [DescribeInstanceAccessControlAttributeConfiguration](#)
- [DescribePermissionSet](#)
- [DescribePermissionSetProvisioningStatus](#)
- [DescribeTrustedTokenIssuer](#)
- [DetachCustomerManagedPolicyReferenceFromPermissionSet](#)
- [DetachManagedPolicyFromPermissionSet](#)
- [GetApplicationAccessScope](#)
- [GetApplicationAssignmentConfiguration](#)
- [GetApplicationAuthenticationMethod](#)
- [GetApplicationGrant](#)
- [GetInlinePolicyForPermissionSet](#)
-

[GetPermissionsBoundaryForPermissionSet](#)

-

[ListAccountAssignmentCreationStatus](#)

-

[ListAccountAssignmentDeletionStatus](#)

-

[ListAccountAssignments](#)

-

[ListAccountAssignmentsForPrincipal](#)

-

[ListAccountsForProvisionedPermissionSet](#)

-

[ListApplicationAccessScopes](#)

-

[ListApplicationAssignments](#)

-

[ListApplicationAssignmentsForPrincipal](#)

-

[ListApplicationAuthenticationMethods](#)

-

[ListApplicationGrants](#)

-

[ListApplicationProviders](#)

-

[ListApplications](#)

-

[ListCustomerManagedPolicyReferencesInPermissionSet](#)

-

[ListInstances](#)

-

[ListManagedPoliciesInPermissionSet](#)

•

[ListPermissionSetProvisioningStatus](#)

•

[ListPermissionSets](#)

•

[ListPermissionSetsProvisionedToAccount](#)

•

[ListTagsForResource](#)

•

[ListTrustedTokenIssuers](#)

•

[ProvisionPermissionSet](#)

•

[PutApplicationAccessScope](#)

•

[PutApplicationAssignmentConfiguration](#)

•

[PutApplicationAuthenticationMethod](#)

•

[PutApplicationGrant](#)

•

[PutInlinePolicyToPermissionSet](#)

•

[PutPermissionsBoundaryToPermissionSet](#)

•

[TagResource](#)

•

[UntagResource](#)

•

[UpdateApplication](#)

-

[UpdateInstance](#)

-

[UpdateInstanceAccessControlAttributeConfiguration](#)

-

[UpdatePermissionSet](#)

-

[UpdateTrustedTokenIssuer](#)

CloudTrail peristiwa operasi API Identity Store

Daftar berikut berisi CloudTrail peristiwa yang dipancarkan oleh operasi Identity Store publik dengan sumber `identitystore.amazonaws.com` peristiwa. Untuk informasi selengkapnya tentang operasi API Identity Store publik, lihat Referensi API [Identity Store](#).

Anda mungkin menemukan peristiwa tambahan CloudTrail untuk operasi API konsol Identity Store dengan sumber `sso-directory.amazonaws.com` peristiwa. API ini mendukung konsol dan portal AWS akses. Jika Anda perlu mendeteksi terjadinya operasi tertentu, seperti menambahkan anggota ke grup, sebaiknya pertimbangkan operasi API publik dan konsol. Untuk informasi selengkapnya tentang API konsol ini, lihat Referensi [Otorisasi Layanan](#).

- [CreateGroup](#)
- [CreateGroupMembership](#)
- [CreateUser](#)
- [DeleteGroup](#)
- [DeleteGroupMembership](#)
- [DeleteUser](#)
- [DescribeGroup](#)
- [DescribeGroupMembership](#)
- [DescribeUser](#)
- [GetGroupId](#)
- [GetGroupMembershipId](#)
- [GetUserId](#)

- [IsMemberInGroups](#)
- [ListGroupMemberships](#)
- [ListGroupMembershipsForMember](#)
- [ListGroups](#)
- [ListUsers](#)
- [UpdateGroup](#)
- [UpdateUser](#)

CloudTrail peristiwa operasi API OIDC

Daftar berikut berisi CloudTrail peristiwa yang dipancarkan oleh operasi OIDC publik. Untuk informasi selengkapnya tentang operasi API OIDC publik, lihat Referensi API [OIDC](#).

- [CreateToken](#)(sumber acarasso.amazonaws.com)
- [CreateTokenWithIAM](#)(sumber acarasso-oauth.amazonaws.com)

CloudTrail peristiwa dari AWS akses operasi API portal

Daftar berikut berisi CloudTrail peristiwa yang dipancarkan oleh operasi API portal AWS akses dengan sumber sso.amazonaws.com peristiwa. Operasi API yang dicatat tidak tersedia di API publik mendukung operasi portal AWS akses. Menggunakan AWS CLI dapat menyebabkan emisi CloudTrail peristiwa dari operasi API portal AWS akses publik dan yang tidak tersedia di API publik. Untuk informasi selengkapnya tentang operasi API portal AWS akses publik, lihat Referensi API portal [AWS akses](#).

- [Authenticate](#)(Tidak tersedia di API publik. Menyediakan login ke portal AWS akses.)
- [Federate](#)(Tidak tersedia di API publik. Menyediakan federasi ke dalam aplikasi.)
- [ListAccountRoles](#)
- [ListAccounts](#)
- [ListApplications](#)(Tidak tersedia di API publik. Menyediakan sumber daya yang ditugaskan pengguna untuk ditampilkan di portal AWS akses.)
- [ListProfilesForApplication](#)(Tidak tersedia di API publik. Menyediakan metadata aplikasi untuk ditampilkan di portal AWS akses.)
- [GetRoleCredentials](#)
- [Logout](#)

CloudTrail peristiwa operasi SCIM API

Untuk informasi tentang operasi SCIM API publik, lihat Refer [ensi API portal](#) AWS akses.

Informasi identitas dalam acara Pusat CloudTrail Identitas IAM

Setiap entri peristiwa atau log berisi informasi tentang entitas yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut ini:

- Apakah permintaan dibuat dengan pengguna root atau kredentif pengguna AWS Identity and Access Management (IAM).
- Apakah permintaan tersebut dibuat dengan kredensial keamanan sementara untuk satu peran atau pengguna gabungan.
- Apakah permintaan itu dibuat oleh AWS layanan lain.
- Apakah permintaan dibuat oleh pengguna Pusat Identitas IAM. Jika demikian, `identityStoreArn` bidang `userId` dan tersedia di CloudTrail acara untuk mengidentifikasi pengguna Pusat Identitas IAM yang memulai permintaan. Untuk informasi selengkapnya, lihat [Mengidentifikasi pengguna di peristiwa yang diprakarsai pengguna CloudTrail Pusat Identitas IAM](#).

Untuk informasi selengkapnya, lihat [Elemen userIdentity CloudTrail](#).

Note

Saat ini, Pusat Identitas IAM tidak memancarkan CloudTrail peristiwa untuk login pengguna ke aplikasi AWS web terkelola (misalnya, Amazon SageMaker AI Studio) dengan API [OIDC](#). Aplikasi web ini adalah bagian dari kumpulan yang lebih luas [the section called “AWS aplikasi yang dikelola”](#), yang juga mencakup aplikasi non-web seperti Amazon Athena SQL dan Amazon S3 Access Grants.

Memahami CloudTrail acara untuk Pusat Identitas IAM

Trail adalah konfigurasi yang memungkinkan pengiriman acara ke bucket Amazon S3 yang Anda tentukan. Peristiwa mewakili permintaan tunggal dari sumber apa pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail peristiwa bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi mereka tidak muncul dalam urutan tertentu. Pelajari tentang [isi CloudTrail catatan](#) di Panduan CloudTrail Pengguna.

Contoh ini menunjukkan entri CloudTrail log yang menangkap `DescribePermissionsPolicies` tindakan yang dilakukan oleh pengguna IAM (samadams) yang berinteraksi dengan Pusat Identitas IAM:

```
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJAIENLMexample",
        "arn": "arn:aws:iam::08966example:user/samadams",
        "accountId": "111122223333",
        "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": "111122223333"
    }
  ]
}
```

Contoh ini menunjukkan entri CloudTrail log yang menangkap `ListApplications` tindakan yang dilakukan oleh pengguna Pusat Identitas IAM dalam portal AWS akses:

```
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IdentityCenterUser",
        "accountId": "111122223333",
        "onBehalfOf": {
          "userId": "94d00cd8-e9e6-4810-b177-b08e84775435",
          "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
        },
        "credentialId": "cdee2490-82ed-43b3-96ee-b75fbf0b97a5"
      },
      "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": "111122223333"
    }
  ]
}
```

Contoh ini menunjukkan entri CloudTrail log yang menangkap CreateToken tindakan yang dilakukan oleh pengguna Pusat Identitas IAM yang mengotentikasi dengan layanan OIDC Pusat Identitas IAM:

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "accountId": "111122223333",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84775435",
```

```

    "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
  },
  "credentialId" : "cdee2490-82ed-43b3-96ee-b75fbf0b97a5"
},
"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": "111122223333",
    "type": "IdentityStoreId",
    "ARN": "d-1234567890"
  }
],
"eventType": "AwsApiCall",
"recipientAccountId": "111122223333"
}

```

Memahami acara masuk ke Pusat Identitas IAM

AWS CloudTrail mencatat peristiwa masuk yang berhasil dan tidak berhasil untuk semua sumber identitas Pusat Identitas IAM. Identitas yang bersumber dari Pusat Identitas IAM dan Active Directory (Konektor AD dan AWS Managed Microsoft AD) menyertakan peristiwa masuk

tambahan yang ditangkap setiap kali pengguna diminta untuk menyelesaikan tantangan atau faktor kredensial tertentu, selain status permintaan verifikasi kredensial tertentu. Hanya setelah pengguna menyelesaikan semua tantangan kredensial yang diperlukan, pengguna akan masuk, yang akan mengakibatkan `UserAuthentication` peristiwa dicatat.

Tabel berikut menangkap setiap nama CloudTrail acara masuk Pusat Identitas IAM, tujuan, dan penerapannya ke sumber identitas yang berbeda.

Nama peristiwa	Tujuan acara	Penerapan sumber identitas
<code>CredentialChallenge</code>	Digunakan untuk memberi tahu bahwa Pusat Identitas IAM telah meminta pengguna untuk menyelesaikan tantangan kredensial tertentu dan menentukan <code>CredentialType</code> yang diperlukan (Misalnya, <code>PASSWORD</code> atau <code>TOTP</code>).	Pengguna Pusat Identitas IAM asli, Konektor AD, dan AWS Managed Microsoft AD
<code>CredentialVerification</code>	Digunakan untuk memberi tahu bahwa pengguna telah mencoba menyelesaikan <code>CredentialChallenge</code> permintaan tertentu dan menentukan apakah kredensial itu berhasil atau gagal.	Pengguna Pusat Identitas IAM asli, Konektor AD, dan AWS Managed Microsoft AD
<code>UserAuthentication</code>	Digunakan untuk memberi tahu bahwa semua persyaratan otentikasi yang ditantang pengguna telah berhasil diselesaikan dan bahwa pengguna berhasil masuk. Pengguna yang gagal menyelesaikan tantangan kredensial yang diperlukan akan mengakibatkan tidak ada	Semua sumber identitas

Nama peristiwa	Tujuan acara	Penerapan sumber identitas
	<i>UserAuthentication</i> peristiwa yang dicatat.	

Tabel berikut menangkap bidang data peristiwa berguna tambahan yang terkandung dalam CloudTrail acara masuk tertentu.

Bidang	Tujuan acara	Sign-in penerapan acara	Contoh nilai
AuthWorkflowID	Digunakan untuk menghubungkan semua peristiwa yang dipancarkan di seluruh urutan masuk. Untuk setiap login pengguna, beberapa peristiwa dapat dipancarkan oleh Pusat Identitas IAM.	CredentialChallenge, CredentialVerification, UserAuthentication	"AuthWorkflowID": "9de74b32-8362-4a01-a524-de21df59fd83"
CredentialType	Digunakan untuk menentukan kredensi atau faktor yang ditantang. UserAuthentication peristiwa akan mencakup semua CredentialType nilai yang berhasil diverifikasi di seluruh urutan masuk pengguna.	CredentialChallenge, CredentialVerification, UserAuthentication	CredentialType": "KATA SANDI" atau "": CredentialType "KATA SANDI, TOTP" (nilai yang mungkin termasuk: KATA SANDI, TOTP, WEBAUTHN, EXTERNAL_IDP, RESYNC_TOTP, EMAIL_OTP)

Bidang	Tujuan acara	Sign-in penerapan acara	Contoh nilai
DeviceEnrollmentRequired	Digunakan untuk menentukan bahwa pengguna diminta untuk mendaftar perangkat MFA saat masuk, dan bahwa pengguna berhasil menyelesaikan permintaan itu.	UserAuthentication	"DeviceEnrollmentRequired": "benar"
LoginTo	Digunakan untuk menentukan lokasi pengalihan setelah urutan masuk yang berhasil.	UserAuthentication	"LoginTo": "https://mydirectory.awsapps.com/start/....."

CloudTrail peristiwa dalam alur masuk Pusat Identitas IAM

Diagram berikut menjelaskan alur masuk dan CloudTrail peristiwa yang dipan Sign-in carkan.

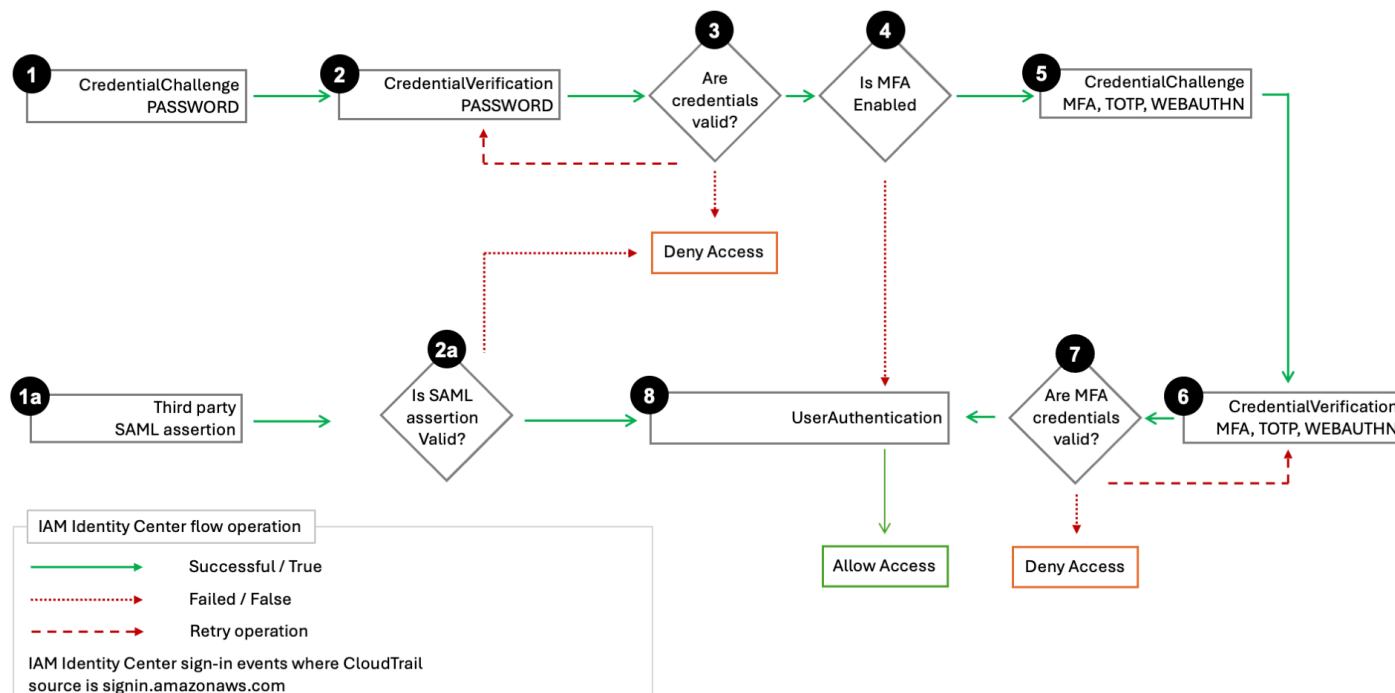


Diagram menunjukkan alur masuk kata sandi dan aliran masuk federasi.

Alur login kata sandi, yang terdiri dari langkah 1—8, menunjukkan langkah-langkah selama proses login nama pengguna dan kata sandi. Pusat Identitas IAM disetel `userIdentity.additionalEventData.CredentialType` ke "PASSWORD", dan Pusat Identitas IAM melewati siklus tantangan-respons kredensial, mencoba lagi sesuai kebutuhan.

Jumlah langkah tergantung pada jenis [login dan keberadaan otentikasi multi-faktor \(MFA\)](#). Proses awal menghasilkan tiga atau lima CloudTrail peristiwa dengan `UserAuthentication` mengakhiri urutan untuk otentikasi yang berhasil. Upaya otentikasi kata sandi yang gagal mengakibatkan kejadian tambahan karena IAM Identity Center menerbitkan ulang `CredentialChallenge` untuk otentikasi reguler atau, jika diaktifkan, MFA.

Alur masuk kata sandi juga mencakup skenario di mana pengguna Pusat Identitas IAM yang baru dibuat dengan panggilan `CreateUser` API masuk dengan kata sandi satu kali (OTP). Jenis kredensial dalam skenario ini adalah "EMAIL_OTP".

Alur masuk federasi, yang terdiri dari langkah 1a, 2a, dan 8, menunjukkan langkah-langkah utama selama proses otentikasi federasi di mana pernyataan [SAML disediakan oleh penyedia identitas, divalidasi oleh Pusat Identitas IAM](#), dan jika berhasil, hasilnya. `UserAuthentication` Pusat

Identitas IAM tidak memanggil urutan otentikasi MFA internal pada langkah 3 — 7 karena penyedia identitas federasi eksternal bertanggung jawab atas semua otentikasi kredensi pengguna.

Nama pengguna dalam acara masuk CloudTrail

Pusat Identitas IAM memancarkan `UserName` bidang di bawah `additionalEventData` elemen sekali per berhasil masuk pengguna Pusat Identitas IAM. Daftar berikut menjelaskan dua peristiwa masuk dalam lingkup, dan kondisi di mana peristiwa ini terjadi. Hanya satu kondisi yang benar saat pengguna masuk.

- `CredentialChallenge`
 - `CredentialTypeKapan "PASSWORD"` — berlaku untuk otentikasi kata sandi dengan Directory Service atau Direktori Pusat Identitas IAM.
 - `CredentialTypeKapan "EMAIL_OTP"` — hanya berlaku Direktori Pusat Identitas IAM saat pengguna yang dibuat dengan panggilan `CreateUser` API mencoba masuk untuk pertama kalinya, dan pengguna menerima kata sandi satu kali untuk masuk dengan kata sandi itu sekali.
- `UserAuthentication`
 - `CredentialTypeKapan "EXTERNAL_IDP"` — berlaku untuk otentikasi dengan IdP eksternal.

Nilai `UserName` untuk otentikasi yang berhasil adalah sebagai berikut:

- Ketika sumber identitas adalah IdP eksternal, nilainya sama dengan `nameID` nilai dalam pernyataan SAML yang masuk. Nilai ini sama dengan `UserName` bidang di Direktori Pusat Identitas IAM.
- Ketika sumber identitas adalah Direktori Pusat Identitas IAM, nilai yang dipancarkan sama dengan `UserName` bidang di direktori ini.
- Ketika sumber identitas adalah Directory Service, nilai yang dipancarkan sama dengan nama pengguna yang dimasukkan pengguna selama otentikasi. Misalnya, pengguna yang memiliki nama pengguna `anyuser@company.com`, dapat mengotentikasi dengan `anyuser`, `anyuser@company.com`, atau `company.com/anyuser`, dan dalam setiap kasus nilai yang dimasukkan dipancarkan CloudTrail masing-masing.

Penyembunyian keamanan dari upaya nama pengguna yang salah

Bid `UserName` yang berisi string `HIDDEN_DUE_TO_SECURITY_REASONS` ketika peristiwa yang direkam adalah kegagalan masuk konsol yang disebabkan oleh input nama pengguna yang salah.

CloudTrail tidak merekam konten dalam kasus ini karena teks dapat berisi informasi sensitif, seperti yang dijelaskan dalam contoh berikut:

- Pengguna secara tidak sengaja mengetik kata sandi di bidang nama pengguna.
- Pengguna secara tidak sengaja mengetikkan nama akun email pribadi, pengenal masuk bank, atau ID pribadi lainnya.

 Tip

Kami menyarankan Anda menggunakan `userId` dan `identityStoreArn` untuk mengidentifikasi pengguna di balik CloudTrail peristiwa Pusat Identitas IAM. Jika Anda perlu menggunakan `userName` bidang tersebut, Anda dapat menggunakan `additionalEventData` elemen di `userName` bawah yang dipancarkan sekali per proses masuk yang berhasil.

Untuk informasi tambahan tentang bagaimana Anda dapat menggunakan `UserName` bidang ini, lihat [Menghubungkan peristiwa pengguna dalam sesi pengguna yang sama](#).

Contoh peristiwa untuk skenario masuk ke Pusat Identitas IAM

Contoh berikut menggambarkan urutan CloudTrail peristiwa khas yang dihasilkan selama berbagai sken AWS ario masuk. Contoh-contoh ini berfungsi sebagai pola referensi untuk membantu Anda menafsirkan log otentikasi, mengidentifikasi masalah keamanan, dan memverifikasi bahwa kebijakan otentikasi Anda berfungsi dengan benar.

Topik

- [Masuk berhasil saat melakukan autentikasi hanya dengan kata sandi](#)
- [Masuk berhasil saat melakukan otentikasi dengan penyedia identitas eksternal](#)
- [Masuk berhasil saat mengotentikasi dengan kata sandi dan aplikasi autentikasi kata sandi satu kali \(TOTP\) berbasis waktu](#)
- [Masuk yang berhasil saat mengotentikasi dengan kata sandi dan pendaftaran MFA paksa diperlukan](#)
- [Gagal masuk karena otentikasi kata sandi yang salah](#)

Masuk berhasil saat melakukan autentikasi hanya dengan kata sandi

Urutan peristiwa berikut menangkap contoh login hanya kata sandi yang berhasil.

CredentialChallenge (Kata Sandi)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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",
    "UserName": "bobsmith@example.com",
    "CredentialType": "PASSWORD"
  },
  "requestID": "5be44ffb-6946-4f47-acaf-1adebd4afead",
  "eventID": "27ea7725-c1fd-4355-bdba-d0e628e0e604",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "eventCategory": "Management",
  "serviceEventDetails": {
    "CredentialChallenge": "Success"
  }
}
```

```
}
```

Berhasil CredentialVerification (Kata Sandi)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYSBsh1Ic50BAA6ftz73M6LsflWDLf0xvi02K3wet946lC30f_iWdilx-zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7Tqzi0LiBLBUSx-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"
  }
}
```

```
}
```

Masuk berhasil saat melakukan otentikasi dengan penyedia identitas eksternal

Urutan peristiwa berikut menangkap contoh proses masuk yang berhasil saat diautentikasi melalui protokol SAML menggunakan penyedia identitas eksternal.

Berhasil UserAuthentication (Penyedia Identitas Eksternal)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYSBshIic50BAA6ftz73M6LsfLWdlf0xvi02K3wet946lC30f_iWdilx-zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7Tqzi0LiBLBUSX-east-1",
    "CredentialType": "EXTERNAL_IDP",
    "UserName": "bobsmith@example.com"
  },
  "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"
    }
  }
}

```

Masuk berhasil saat mengotentikasi dengan kata sandi dan aplikasi autentikasi kata sandi satu kali (TOTP) berbasis waktu

Urutan peristiwa berikut menangkap contoh di mana otentikasi multi-faktor diperlukan selama masuk dan pengguna berhasil masuk menggunakan kata sandi dan aplikasi otentikator TOTP.

CredentialChallenge (Kata Sandi)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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",
    "UserName": "bobsmith@example.com"
  },
  "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"
  }
}

```

Berhasil CredentialVerification (Kata Sandi)

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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":"IdentityCenterUser",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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"
    }
  }
}

```

Berhasil CredentialVerification (TOTP)

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "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\u003d11F1r1mCVJ-4Y5UY6RI10UCXvRePCHd6195xvYg1rwo1Pj7B-7UGIG1YUUVe31Nkzd7ihxKn6DMdnFf00108qc3RFSx-pjBXXKG_jUcvBk_UILdGytV4o1u97h42B-TA_6uwdmJiw1dcCz_Rv44d_BS0PkulW-5LVJy1oeP1H0FPPMeheyuk5Uy48d5of9-c\u0026wdc_csrf_token"
  }
}

```

```
\u003dNMLui44guoVnxRd0qu2tYJIdyyFPX6SDRNTspIScfMM0AgFbho1nvvCaxPTghHbgHCRIXdfffFtzH0sL1ow419Bobn
\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 mengotentikasi dengan kata sandi dan pendaftaran MFA paksa diperlukan

Urutan peristiwa berikut menunjukkan autentikasi kata sandi yang berhasil di mana pengguna diminta untuk mendaftar dan berhasil menyelesaikan otentikasi multi-faktor (MFA) sebelum menyelesaikan proses masuk mereka.

CredentialChallenge (Kata Sandi)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IdentityCenterUser",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    }
  },
  "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
},
"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",
        "UserName": "bobsmith@example.com"
    },
    "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"
    }
}

```

Berhasil CredentialVerification (Kata Sandi)

```

{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IdentityCenterUser",
        "arn": "",
        "accountId": "111122223333",
        "accessKeyId": "",
        "onBehalfOf": {
            "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
            "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
        },
        "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
    },
    "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 (Kata Sandi + Pendaftaran MFA Diperlukan)

```

{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IdentityCenterUser",
        "arn": "",
        "accountId": "111122223333",
        "accessKeyId": "",
        "onBehalfOf": {
            "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
            "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
        },
        "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
    },
    "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_maUsZ7ABETjeQhyWfvIHyz52rgR28sYAKN1oEk2G07czrwzXvE9HL1N2K9De8LyBEV83SFeDQfrWpkwXf
FJyJqkoGrt_w6rm_MpAn0uyrVq8udY_EgU3fh0L3QWvWiQuYnDPMYPmmy_qkZgR9rz__BI
\u0026wdc_csrf_token
\u003dJih9U62o5LQDtYLNqCK8a6xj0gJg5BRWq2tbl75y8vAmwZhAqrggrgbxXat2M646UZGp93krw7WYQdHIgi50YI9QSc
\u003dd-9067230c03\u0026region\u003ddus-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 karena otentikasi kata sandi yang salah

Urutan peristiwa berikut menunjukkan upaya otentikasi di mana pengguna berhasil memasukkan nama pengguna mereka tetapi gagal dalam langkah verifikasi kata sandi, yang mengakibatkan tidak berhasil masuk.

CredentialChallenge (Kata Sandi)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"Unknown",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
  },

```



```

"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",
  "UserName":"bobsmith@example.com"
},
"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",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":""
  },
  "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"
  }
}
```

Pencatatan panggilan SCIM API IAM Identity Center dengan AWS CloudTrail

[IAM Identity Center SCIM](#) terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau. Layanan AWS CloudTrail menangkap panggilan API untuk SCIM sebagai peristiwa. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. Untuk mempelajari selengkapnya CloudTrail, lihat Panduan [AWS CloudTrail Pengguna](#).

Note

CloudTrail diaktifkan pada Anda Akun AWS saat Anda membuat akun. Namun, Anda mungkin perlu memutar token akses Anda untuk melihat peristiwa dari SCIM, jika token Anda dibuat sebelum September 2024.

Untuk informasi selengkapnya, lihat [Putar token akses](#).

SCIM mendukung logging untuk operasi berikut sebagai peristiwa di: CloudTrail

- [CreateGroup](#)
- [CreateUser](#)

- [DeleteGroup](#)
- [DeleteUser](#)
- [GetGroup](#)
- [GetSchema](#)
- [GetUser](#)
- [ListGroups](#)
- [ListResourceTypes](#)
- [ListSchemas](#)
- [ListUsers](#)
- [PatchGroup](#)
- [PatchUser](#)
- [PutUser](#)
- [ServiceProviderConfig](#)

Contoh CloudTrail acara

Contoh berikut menunjukkan log CloudTrail peristiwa khas yang dihasilkan selama operasi SCIM dengan IAM Identity Center. Contoh-contoh ini menunjukkan struktur dan konten peristiwa untuk operasi yang berhasil dan skenario kesalahan umum, membantu Anda memahami cara menafsirkan CloudTrail log saat memecahkan masalah penyediaan SCIM.

CreateUser Operasi yang berhasil

A CloudTrail cara ini menunjukkan CreateUser operasi yang berhasil dilakukan melalui SCIM API. Acara menangkap parameter permintaan (dengan informasi sensitif tertutup) dan elemen respons, termasuk ID pengguna yang baru dibuat. Jenis peristiwa ini dihasilkan ketika penyedia identitas berhasil menyediakan pengguna baru ke Pusat Identitas IAM menggunakan protokol SCIM.

```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "WebIdentityUser",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
```

```

"eventName": "CreateUser",
"awsRegion": "us-east-1",
"sourceIPAddress": "xx.xxx.xxx.xxx",
"userAgent": "Go-http-client/2.0",
"requestParameters": {
  "httpBody": {
    "displayName": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "schemas" : [
      "urn:ietf:params:scim:schemas:core:2.0:User"
    ],
    "name": {
      "familyName": "HIDDEN_DUE_TO_SECURITY_REASONS",
      "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "active": true,
    "userName": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "tenantId": "xxxx"
},
"responseElements": {
  "meta" : {
    "created" : "Oct 10, 2024, 1:23:45 PM",
    "lastModified" : "Oct 10, 2024, 1:23:45 PM",
    "resourceType" : "User"
  },
  "displayName" : "HIDDEN_DUE_TO_SECURITY_REASONS",
  "schemas" : [
    "urn:ietf:params:scim:schemas:core:2.0:User"
  ],
  "name": {
    "familyName": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "active": true,
  "id" : "c4488478-a0e1-700e-3d75-96c6bb641596",
  "userName": "HIDDEN_DUE_TO_SECURITY_REASONS"
},
"requestID": "xxxx",
"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",

```

```

"tlsDetails": {
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}

```

PatchGroup Operasi gagal: Atribut jalur yang diperlukan hilang

Per CloudTrailistiwa ini menunjukkan PatchGroup operasi gagal yang mengaki ValidationException batkan pesan kesalahan "Missing path in PATCH request". Kesalahan terjadi karena PATCH operasi memerlukan atribut jalur untuk menentukan atribut grup mana yang akan dimodifikasi, tetapi atribut ini hilang dari permintaan.

```

{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "PatchGroup",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ValidationException",
  "errorMessage": "Missing path in PATCH request",
  "requestParameters": {
    "httpBody": {
      "operations": [
        {
          "op": "REMOVE",
          "value": "HIDDEN_DUE_TO_SECURITY_REASONS"
        }
      ],
      "schemas": [
        "HIDDEN_DUE_TO_SECURITY_REASONS"
      ]
    },
    "tenantId": "xxxx",
    "id": "xxxx"
  },
  "responseElements": null,

```

```

"requestID": "xxxx",
"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}

```

CreateGroup Operasi gagal: Nama grup sudah ada

Per CloudTrailistiwa ini menunjukkan CreateGroup operasi gagal yang mengaki ConflictException batkan pesan kesalahan "Duplicate GroupDisplayName". Kesalahan ini terjadi saat mencoba membuat grup dengan nama tampilan yang sudah ada di Pusat Identitas IAM. Penyedia identitas harus menggunakan nama grup unik atau memperbarui grup yang ada alih-alih membuat yang baru.

```

{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "CreateGroup",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ConflictException",
  "errorMessage": "Duplicate GroupDisplayName",
  "requestParameters": {
    "httpBody": {
      "displayName": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "tenantId": "xxxx"
  },
  "responseElements": null,
  "requestID": "xxxx",

```

```

"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}

```

PatchUser Operasi gagal: Beberapa alamat email tidak didukung

Per CloudTrailistiwa ini menunjukkan PatchUser operasi gagal yang mengaki ValidationException batkan pesan kesalahan "List attribute emails exceeds allowed limit of 1". Kesalahan ini terjadi saat mencoba menetapkan beberapa alamat email ke pengguna, karena Pusat Identitas IAM hanya mendukung satu alamat email per pengguna. Penyedia identitas harus mengonfigurasi pemetaan SCIM untuk mengirim hanya satu alamat email untuk setiap pengguna.

```

{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "PatchUser",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ValidationException",
  "errorMessage": "List attribute emails exceeds allowed limit of 1",
  "requestParameters": {
    "httpBody": {
      "operations": [
        {
          "op": "REPLACE",
          "path": "emails",
          "value": "HIDDEN_DUE_TO_SECURITY_REASONS"
        }
      ]
    }
  }
}

```

```

    ],
    "schemas": [
        "HIDDEN_DUE_TO_SECURITY_REASONS"
    ]
  },
  "tenantId": "xxxx",
  "id": "xxxx"
},
"responseElements": null,
"requestID": "xxxx",
"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}

```

Kesalahan validasi SCIM API umum di Pusat Identitas IAM

Pesan kesalahan validasi berikut biasanya muncul di CloudTrail acara saat menggunakan SCIM API dengan IAM Identity Center. Kesalahan validasi ini biasanya terjadi selama operasi penyediaan pengguna dan grup.

Untuk panduan terperinci tentang menyelesaikan kesalahan ini dan mengonfigurasi penyediaan SCIM dengan benar, lihat artikel ini [AWS re:Post](#).

- Email atribut daftar melebihi batas yang diizinkan 1
- Daftar alamat atribut yang diizinkan batas 1
- 1 kesalahan validasi terdeteksi: Nilai di `*name.FamilyName*` gagal memenuhi batasan: Anggota harus memenuhi pola ekspresi reguler: `[\\ p {L}\\ p {M}\\ p {S}\\ p {N}\\ p {N}\\ p {P}\\ t\\ n\\ r] +`
- 2 kesalahan validasi terdeteksi: Nilai di `'Name.FamilyName'` gagal memenuhi batasan: Anggota harus memiliki panjang lebih besar dari atau sama dengan 1; Nilai di `'Name.FamilyName'` gagal memenuhi batasan: Anggota harus memenuhi pola ekspresi reguler: `[\\ p {L}\\ p {M}\\ p {S}\\ p {N}\\ p {P}\\ t\\ n\\ r] +`
- 2 kesalahan validasi terdeteksi: Nilai di `'urn:ietf:params:scim:schemas:extension:enterprise:2.0:User.manager.value'` gagal memenuhi batasan: Anggota harus memiliki panjang lebih besar

dari atau sama dengan 1; Nilai di 'urn:ietf:params:scim:schemas:extension:enterprise:2.0:' gagal memenuhi batasan: Anggota harus memenuhi pola ekspresi reguler: `[\\ p {L}\\ p {M}\\ p {S}\\ p {N}\\ p {P}\\ t\\ n\\ r] +User.manager.value`,

- JSON tidak valid dari RequestBody
- Format Filter Tidak Valid

Hubungkan komponen aplikasi dengan Amazon EventBridge

Anda dapat mengintegrasikan Pusat Identitas IAM dengan [Amazon EventBridge](#) untuk meningkatkan peristiwa yang memulai pemberitahuan administratif atau memanggil alur kerja otomatis sebagai respons terhadap tindakan Pusat Identitas IAM tertentu yang direkam dalam acara. CloudTrail

Misalnya, Anda dapat mengonfigurasi [EventBridge aturan](#) untuk mendeteksi ketika pengguna menghapus aplikasi atau ketika Pusat Identitas IAM membuat grup baru. Tergantung pada kasus penggunaan Anda, Anda dapat merutekan peristiwa ini ke topik Amazon SNS untuk memberi tahu administrator atau memanggil otomatisasi tambahan menggunakan AWS Lambda, Fungsi [Langkah](#), atau layanan lainnya [EventBridge-supported](#) .

Pencatatan kesalahan sinkronisasi AD yang dapat dikonfigurasi

Anda dapat mengaktifkan logging pada konfigurasi sinkronisasi Active Directory (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 yang dapat dikonfigurasi dan mengambil tindakan jika berlaku. Anda dapat mengirim log ke grup CloudWatch log Amazon Logs, 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 yang dijual, lihat Meng [aktifkan logging dari Layanan AWS](#).

Note

Anda dikenakan biaya untuk logging. Untuk informasi selengkapnya, [lihat Log Dijual](#) di [halaman](#) CloudWatch Harga Amazon.

Untuk mengaktifkan log kesalahan sinkronisasi AD yang dapat dikonfigurasi

1. Masuk ke konsol [Pusat Identi](#) tas 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 bucket tujuan.
 - c. Pilih Ke Firehose. Kemudian pilih atau masukkan aliran pengiriman tujuan.
5. Pilih Kirim.

Untuk menonaktifkan log kesalahan sinkronisasi AD yang dapat dikonfigurasi

1. Masuk ke konsol [Pusat Identi](#) tas 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 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 terperinci tentang kesalahan yang terjadi.

sync_source

Sumber sinkronisasi adalah tempat entitas disinkronkan. Untuk Pusat Identitas IAM, ini adalah Direktori Aktif (AD) yang dikelola oleh Directory Service. Sumber sinkronisasi berisi domain dan ARN dari direktori yang terpengaruh.

sync_target

Target sinkronisasi adalah tujuan tempat entitas disimpan. Untuk Pusat Identitas IAM, ini adalah Toko Identitas. Target sinkronisasi berisi ARN Identity Store yang terpengaruh.

source_entity_id

Pengidentifikasi unik untuk entitas yang menyebabkan kesalahan. Untuk Pusat Identitas IAM, ini adalah SID entitas.

source_entity_type

Jenis entitas yang menyebabkan kesalahan. Nilai dapat berupa USER atau GROUP.

eventTimestamp

Stempel waktu ketika kesalahan terjadi.

Contoh log kesalahan 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

Third-party auditor menilai keamanan dan kepatuhan Layanan AWS seperti AWS IAM Identity Center sebagai bagian dari beberapa program AWS kepatuhan.

Pengalaman AWS pendaftaran baru kami tidak dirancang untuk beban kerja yang diatur. Jika Anda menggunakan pengalaman AWS pendaftaran baru kami, tetapi ingin menggunakannya AWS untuk beban kerja yang diatur, Anda dapat [mendaftar untuk AWS \(lanjutan\)](#) atau [mengaktifkan fitur lanjutan](#) untuk lingkungan Anda AWS .

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat [Layanan AWS di Lingkup berdasarkan Program Kepatuhan](#) dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program Kep [AWS atuhan Program Jaminan](#) .

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. Untuk informasi selengkapnya tentang tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS, lihat Dokumentasi [AWS Keamanan](#).

Standar kepatuhan yang didukung

Pusat Identitas IAM 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 Health Insurance Portability and Accountability Act (HIPAA) untuk memasukkan Pusat Identitas IAM sebagai layanan yang memenuhi syarat [HIPAA](#).

AWS menawarkan [HIPAA-focused whitepaper](#) untuk pelanggan yang ingin mempelajari lebih lanjut tentang bagaimana mereka dapat menggunakannya 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 sesuai telah diterapkan dan menentukan model tanggung jawab yang sesuai untuk memenuhi persyaratan Manual Keamanan Informasi Pemerintah Australia (ISM) yang diproduksi oleh Pusat Keamanan Cyber Australia (ACSC). Untuk informasi selengkapnya, lihat Sumber [Daya IRAP](#).



IAM Identity Center memiliki Sertifikat Kepatuhan untuk Standar Keamanan Data (DSS) Industri Kartu Pembayaran (PCI) versi 3.2 pada Penyedia Layanan Level 1.

Pelanggan yang menggunakan AWS produk dan layanan untuk menyimpan, memproses, atau mengirimkan data pemegang kartu dapat menggunakan sumber identitas berikut di Pusat Identitas IAM untuk mengelola sertifikasi kepatuhan PCI DSS mereka sendiri:

- Active Directory
- Penyedia identitas eksternal

Sumber identitas Pusat Identitas IAM saat ini tidak sesuai dengan PCI DSS.

Untuk informasi selengkapnya tentang PCI DSS, termasuk cara meminta salinan Paket Kepatuhan AWS PCI, lihat [PCI DSS level 1](#).



Laporan Kontrol Sistem & Organisasi (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 Artefak](#)
- AWS SOC 2: Laporan Keamanan, Ketersediaan, & Kerahasiaan - [Unduh dengan AWS Artefak](#)
- [AWS SOC 3: Laporan Keamanan, Ketersediaan, & Kerahasiaan](#)

Pusat Identitas IAM berada dalam ruang lingkup untuk laporan AWS SOC 1, SOC 2, dan SOC 3. Untuk informasi selengkapnya, lihat Kepatuhan [SOC](#).

Ketahanan di Pusat Identitas IAM

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Zona Ketersediaan. AWS Wilayah menyediakan beberapa Zona Ketersediaan 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 secara otomatis melakukan failover di antara Zona Ketersediaan tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur biasa yang terdiri dari satu atau beberapa pusat data.

Untuk informasi selengkapnya tentang AWS Wilayah dan Zona Ketersediaan, 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 keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat [AWS Keamanan Cloud](#). Untuk merancang AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infra [struktur](#) di Security Pillar AWS Well-Architected Framework.

Anda menggunakan panggilan API yang di AWS publikasikan untuk mengakses Pusat Identitas IAM melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Suite Cipher dengan kerahasiaan maju sempurna (PFS) seperti DHE (Ephemeral) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Perlindungan data di Pusat Identitas IAM

Model Tanggung Jawab Berbagi sama berlaku untuk perlindungan data di Pusat Identitas AWS dan IAM. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas konfigurasi keamanan dan tugas manajemen untuk AWS layanan yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, silakan lihat [Pertanyaan Umum Privasi Data](#). Untuk informasi tentang perlindungan data di Eropa, lihat [AWS postingan blog Model Tanggung Jawab Bersama dan GDPR](#) AWS di Blog Keamanan .

Kami menyarankan Anda mengamankan data Anda dengan cara berikut:

- Gunakan otentikasi multi-faktor (MFA) dengan IAM Identity Center.
- Gunakan TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang menggunakan CloudTrail jalur untuk menangkap AWS aktivitas, lihat [Bekerja dengan CloudTrail jejak](#) di Panduan AWS CloudTrail Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default dalam AWS layanan.

Kami sangat menyarankan agar Anda tidak pernah memasukkan informasi rahasia atau sensitif, seperti alamat email pelanggan Anda, ke dalam tag atau bidang teks bentuk bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan AWS IAM Identity Center, atau AWS layanan lain menggunakan konsol, API AWS CLI, atau AWS SDK. Setiap data yang Anda masukkan ke dalam tag atau bidang teks bentuk bebas yang digunakan untuk nama dapat digunakan untuk log diagnostik.

Enkripsi saat bergerak

IAM Identity Center melindungi data dalam perjalanan, saat melakukan perjalanan ke dan dari layanan, dengan secara otomatis mengenkripsi semua data antar-jaringan menggunakan protokol enkripsi Transport Layer Security (TLS) 1.2 atau TLS 1.3. Permintaan HTTPS langsung yang diautentikasi dengan IAM dan dikirim ke IAM Identity Center API, Identity Store API, atau API OIDC, ditandatangani menggunakan Algoritma Versi 4 Tanda [AWS Tangan](#) untuk membuat koneksi yang aman.

Privasi data

Dengan IAM Identity Center, Anda mempertahankan kendali atas data organisasi Anda. Identitas pengguna dan grup Anda yang disimpan di Pusat Identitas IAM dibagikan dengan AWS layanan lain seperti aplikasi terkel [AWS ola](#) hanya jika Anda mengaktifkannya dengan Pusat Identitas IAM, dan jika diperlukan oleh layanan tersebut.

Untuk informasi tambahan, lihat FAQ Privasi [AWS Data](#).

Retensi data

Pusat Identitas IAM menyimpan data Anda seperti identitas pengguna dan grup, dan metadata, hingga Anda menghapusnya dari layanan. Saat Anda menghapus instance Pusat Identitas IAM, data yang dikandungnya juga dihapus.

Enkripsi saat diam

IAM Identity Center menyediakan enkripsi untuk melindungi data pelanggan saat diam menggunakan jenis kunci berikut:

- Kunci milik AWS (tipe kunci default) - Pusat Identitas IAM menggunakan kunci ini secara default untuk mengenkripsi data Anda secara otomatis. Anda tidak dapat melihat, mengelola, mengaudit penggunaannya, atau menggunakan kunci AWS yang dimiliki untuk tujuan lain. IAM Identity Center menangani manajemen kunci sepenuhnya untuk menjaga keamanan data Anda, tanpa Anda harus mengambil tindakan apa pun. Untuk informasi selengkapnya, lihat kunci yang [AWS dimiliki](#) di Panduan [AWS Key Management Service Pengembang](#).
- Kunci yang dikelola pelanggan — Dalam instance organisasi Pusat Identitas IAM, Anda dapat memilih kunci yang dikelola pelanggan simetris untuk enkripsi pada sisa data identitas tenaga kerja Anda seperti atribut pengguna dan grup. Anda membuat, memiliki, dan mengelola kunci enkripsi ini. Karena Anda memiliki kontrol penuh atas lapisan enkripsi ini, Anda dapat melakukan tugas-tugas seperti:
 - Menetapkan dan memelihara kebijakan utama untuk membatasi akses ke kunci hanya untuk kepala sekolah IAM yang membutuhkan akses, seperti Pusat Identitas IAM dan [AWS aplikasi yang dikelola](#) dalam hal yang sama AWS Organizations dan administratornya.
 - Menetapkan dan memelihara kebijakan IAM untuk akses ke kunci termasuk akses lintas akun
 - Mengaktifkan dan menonaktifkan kebijakan utama
 - Memutar materi kriptografi kunci

- Mengaudit akses ke data Anda yang membutuhkan akses kunci
- Menambahkan tanda
- Membuat alias kunci
- Kunci penjadwalan untuk penghapusan

Untuk mempelajari cara menerapkan kunci KMS yang dikelola pelanggan di Pusat Identitas IAM, lihat [Menerapkan kunci KMS yang dikelola pelanggan di AWS IAM Identity Center](#) Untuk informasi selengkapnya tentang kunci yang dikelola [pelanggan, lihat kunci yang dikelola pelanggan](#) di Panduan AWS Key Management Service Pengembang.

 Note

IAM Identity Center secara otomatis mengaktifkan enkripsi saat diam menggunakan kunci KMS yang AWS dimiliki untuk melindungi data pelanggan tanpa biaya. Namun, AWS KMS biaya berlaku saat menggunakan kunci yang dikelola pelanggan. Untuk informasi selengkapnya tentang harga, lihat [AWS Key Management Service harga](#).

Pertimbangan untuk menerapkan kunci yang dikelola pelanggan:

- Kunci khusus: Sebaiknya buat kunci KMS khusus yang dikelola pelanggan baru untuk setiap instans Pusat Identitas IAM daripada menggunakan kembali kunci yang sudah ada. Pendekatan ini memberikan pemisahan tugas yang lebih jelas, menyederhanakan manajemen kontrol akses, dan membuat audit keamanan lebih mudah. Memiliki kunci khusus juga mengurangi risiko dengan membatasi dampak perubahan kunci pada satu instance Pusat Identitas IAM.
- Penggunaan Pusat Identitas IAM di beberapa instans Wilayah AWS: Jika Anda berencana untuk mereplikasi instans Pusat Identitas IAM ke instans tambahan Wilayah AWS, Anda harus menggunakan kunci KMS yang dikelola pelanggan untuk enkripsi saat diam. Jenis kunci KMS yang AWS dimiliki default tidak didukung di Pusat Identitas IAM multi-regional. Untuk informasi selengkapnya, lihat [Menggunakan Pusat Identitas IAM di beberapa Wilayah AWS](#).

 Note

Pusat Identitas IAM menggunakan enkripsi [amplop](#) dalam enkripsi data identitas tenaga kerja Anda. Kunci KMS Anda memainkan peran kunci pembungkus yang mengenkripsi kunci data yang sebenarnya digunakan untuk mengenkripsi data.

Untuk informasi selengkapnya tentang AWS KMS, lihat [Apa itu Layanan Manajemen K AWS unci?](#)

Konteks enkripsi Pusat Identitas IAM

Konteks [enkripsi](#) adalah kumpulan opsional pasangan kunci-nilai non-rahasia yang berisi informasi kontekstual tambahan tentang data. AWS KMS menggunakan konteks enkripsi sebagai data terautentikasi tambahan untuk mendukung enkripsi yang diautentikasi. Saat Anda menyertakan konteks enkripsi dalam permintaan untuk mengenkripsi data, AWS KMS mengikat konteks enkripsi ke data terenkripsi. Untuk mendekripsi data, Anda menyertakan konteks enkripsi yang sama dalam permintaan. Lihat Panduan Peng [AWS KMS embang](#) untuk informasi selengkapnya tentang konteks enkripsi.

Pusat Identitas IAM menggunakan kunci konteks enkripsi dari berikut ini: `aws:sso:instance-arn`, `aws:identitystore:identitystore-arn`, dan `tenant-key-id`. Misalnya, konteks enkripsi berikut dapat muncul dalam operasi AWS KMS API yang dipanggil oleh [IAM Identity Center API](#).

```
"encryptionContext": {
  "tenant-key-id": "ssoins-1234567890abcdef",
  "aws:sso:instance-arn": "arn:aws:sso::instance/ssoins-1234567890abcdef"
}
```

Konteks enkripsi berikut dapat muncul dalam operasi AWS KMS API yang dipanggil oleh [Identity Store API](#).

```
"encryptionContext": {
  "tenant-key-id": "12345678-1234-1234-1234-123456789012",
  "aws:identitystore:identitystore-arn":
    "arn:aws:identitystore::123456789012:identitystore/d-1234567890"
}
```

Menggunakan konteks enkripsi untuk mengontrol akses ke kunci yang dikelola pelanggan Anda

Anda dapat menggunakan konteks enkripsi dalam kebijakan kunci dan kebijakan IAM sebagai kondisi untuk mengontrol akses ke kunci yang dikelola pelanggan simetris Anda. Beberapa templat kebijakan utama di dalamnya menyer [Pernyataan kebijakan utama KMS lanjutan](#) takan kondisi tersebut untuk memastikan kunci hanya digunakan dengan instance Pusat Identitas IAM tertentu.

Memantau kunci enkripsi Anda untuk Pusat Identitas IAM

Saat menggunakan kunci KMS yang dikelola pelanggan dengan instans Pusat Identitas IAM, Anda dapat menggunakan [AWS CloudTrail](#) atau [Amazon CloudWatch Logs](#) untuk melacak permintaan yang dikirim IAM Identity Center. AWS KMS Operasi API KMS yang dipanggil Pusat Identitas IAM terdaftar di dalamnya. [Langkah 2: Siapkan pernyataan kebijakan utama KMS](#) CloudTrail peristiwa untuk operasi API ini berisi konteks enkripsi, yang memungkinkan Anda memantau operasi AWS KMS API yang dipanggil oleh instance Pusat Identitas IAM Anda untuk mengakses data yang dienkripsi oleh kunci yang dikelola pelanggan Anda.

Contoh konteks enkripsi CloudTrail jika terjadi operasi AWS KMS API:

```
{
  "requestParameters": {
    "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
    "encryptionContext": {
      "aws:sso:instance-arn": "arn:aws:sso:::instance/ssoins-xxxxxxxxxxxxxxxxxx",
      "tenant-key-id": "ssoins-xxxxxxxxxxxxxxxxxx"
    }
  }
}
```

AWS penyimpanan aplikasi terkelola, enkripsi, dan penghapusan atribut identitas Pusat Identitas IAM

Beberapa AWS aplikasi terkelola yang digunakan untuk Anda gunakan AWS IAM Identity Center, seperti AWS Systems Manager dan Amazon CodeCatalyst, menyimpan atribut pengguna dan grup tertentu dari Pusat Identitas IAM di penyimpanan data mereka sendiri. Enkripsi diam dengan kunci KMS yang dikelola pelanggan di Pusat Identitas IAM tidak meluas ke pengguna Pusat Identitas IAM dan atribut grup yang disimpan dalam AWS aplikasi terkelola. AWS aplikasi yang dikelola mendukung metode enkripsi yang berbeda untuk data yang mereka simpan. Terakhir, saat Anda menghapus atribut pengguna dan grup dalam Pusat Identitas IAM, aplikasi terkel AWS ini dapat terus menyimpan informasi ini setelah penghapusan di Pusat Identitas IAM. Lihat panduan pengguna aplikasi terkel AWS Anda untuk enkripsi dan keamanan data yang disimpan dalam aplikasi.

Menerapkan kunci KMS yang dikelola pelanggan di AWS IAM Identity Center

Kunci yang dikelola pelanggan adalah AWS kunci Layanan Manajemen Kunci yang Anda buat, miliki, dan kelola. Untuk menerapkan kunci KMS yang dikelola pelanggan untuk enkripsi saat diam di Pusat Identi AWS tas IAM, ikuti langkah-langkah berikut:

Important

Beberapa aplikasi AWS terkelola tidak dapat digunakan dengan Pusat Identi AWS tas IAM yang dikonfigurasi dengan kunci KMS yang dikelola pelanggan. Lihat [AWS aplikasi terkelola yang dapat Anda gunakan dengan IAM Identity Center](#).

1. [Langkah 1: Identifikasi kasus penggunaan untuk organisasi Anda](#)- Untuk menentukan izin yang benar untuk penggunaan kunci KMS, Anda perlu mengidentifikasi kasus penggunaan yang relevan di seluruh organisasi Anda. Izin kunci KMS terdiri dari pernyataan kebijakan kunci KMS dan kebijakan berbasis identitas yang bekerja sama untuk memungkinkan prinsipal IAM yang sesuai menggunakan kunci KMS untuk kasus penggunaan spesifik mereka.
2. [Langkah 2: Siapkan pernyataan kebijakan utama KMS](#)- Pilih templat pernyataan kebijakan kunci KMS terkait berdasarkan kasus penggunaan yang diidentifikasi pada Langkah 1, dan isi pengidentifikasi yang diperlukan dan nama utama IAM. Mulailah dengan pernyataan kebijakan kunci KMS dasar, dan jika kebijakan keamanan Anda mengharuskannya, sempurnakan pernyataan kebijakan utama KMS lanjutan.
3. [Langkah 3: Buat kunci KMS yang dikelola pelanggan](#)- Buat kunci KMS di AWS KMS yang memenuhi persyaratan Pusat Identitas IAM, dan tambahkan pernyataan kebijakan kunci KMS yang disiapkan pada Langkah 2 ke kebijakan kunci KMS.
4. [Langkah 4: Konfigurasikan kebijakan IAM untuk penggunaan kunci KMS lintas akun](#)- Pilih templat pernyataan kebijakan IAM terkait berdasarkan kasus penggunaan yang diidentifikasi pada Langkah 1, dan persiapkan untuk digunakan dengan mengisi kunci ARN. Kemudian, izinkan prinsipal IAM untuk setiap kasus penggunaan tertentu untuk menggunakan kunci KMS di seluruh akun dengan menambahkan pernyataan kebijakan IAM yang telah disiapkan ke kebijakan IAM kepala sekolah.
5. [Langkah 5: Konfigurasikan kunci KMS di Pusat Identitas IAM](#)- Aktifkan kunci KMS yang dikelola pelanggan di instance Pusat Identitas IAM Anda untuk menggunakannya untuk enkripsi saat diam.

Langkah 1: Identifikasi kasus penggunaan untuk organisasi Anda

Sebelum membuat dan mengonfigurasi kunci KMS yang dikelola pelanggan Anda, identifikasi kasus penggunaan Anda dan siapkan izin kunci KMS yang diperlukan. Lihat Panduan Pengembang [AWS KMS](#) untuk informasi selengkapnya tentang kebijakan kunci KMS.

Prinsipal IAM yang memanggil API layanan Pusat Identitas IAM memerlukan izin. Misalnya, administrator yang didelegasikan dapat diberi wewenang untuk menggunakan API ini melalui kebijakan kumpulan izin. Ketika Pusat Identitas IAM dikonfigurasi dengan kunci yang dikelola pelanggan, prinsipal IAM juga harus memiliki izin untuk menggunakan API KMS melalui API layanan Pusat Identitas IAM. Anda menentukan izin API KMS ini di dua tempat: kebijakan kunci KMS dan kebijakan IAM yang terkait dengan prinsipal IAM.

Izin kunci KMS terdiri dari:

1. Pernyataan kebijakan kunci KMS yang Anda tentukan pada kunci KMS selama pembuatannya di [Langkah 3: Buat kunci KMS yang dikelola pelanggan](#)
2. Pernyataan kebijakan IAM untuk prinsipal IAM yang Anda tentukan [Langkah 4: Konfigurasi kebijakan IAM untuk penggunaan kunci KMS lintas akun](#) setelah membuat kunci KMS.

Tabel berikut menentukan kasus penggunaan yang relevan dan prinsip-prinsip IAM yang memerlukan izin untuk menggunakan kunci KMS Anda.

Kasus penggunaan	Prinsipal IAM yang membutuhkan izin untuk menggunakan kunci KMS	Required/Optional
Penggunaan Pusat Identi AWS tas IAM	<ul style="list-style-type: none"> • Administrator Pusat Identi AWS tas IAM • Layanan Pusat Identitas IAM dan layanan Identity Store terkait 	Diperlukan
Penggunaan aplikasi ter AWS kelola dengan IAM Identity Center	<ul style="list-style-type: none"> • Administrator aplikasi AWS terkelola • AWS aplikasi yang dikelola • Peran layanan yang diasum AWS sikan oleh aplikasi terkelola untuk 	Opsional

Kasus penggunaan	Prinsipal IAM yang membutuhkan izin untuk menggunakan kunci KMS	Required/ Optional
	memanggil API layanan Pusat Identitas IAM	
Penggunaan AWS Control Tower pada instance Pusat Identi AWS tas IAM yang diaktifkan	<ul style="list-style-type: none"> AWS Control Tower administrator 	Opsional
Instans SSO ke Amazon EC2 dengan Pusat Identitas AWS IAM	<ul style="list-style-type: none"> Prinsipal IAM yang diberi wewenang untuk melakukan SSO ke instans Amazon EC2 	Opsional
Kasus penggunaan lain yang melakukan panggilan ke API layanan Pusat Identitas IAM dengan prinsipal IAM, seperti aplikasi yang dikelola pelanggan, alur kerja penyediaan set izin, atau fungsi AWS Lambda	<ul style="list-style-type: none"> Prinsip IAM yang digunakan oleh alur kerja ini untuk memanggil API layanan Pusat Identitas IAM 	Opsional

Note

Beberapa prinsipal IAM yang tercantum dalam tabel memerlukan izin API AWS KMS. Namun, untuk melindungi data pengguna dan grup Anda di Pusat Identitas IAM, hanya layanan IAM Identity Center dan Identity Store yang langsung memanggil API AWS KMS.

Langkah 2: Siapkan pernyataan kebijakan utama KMS

Mulailah dengan [Kebijakan kunci KMS dasar](#) dan sesuaikan untuk organisasi Anda. Jika Anda memerlukan kebijakan yang lebih spesifik berdasarkan persyaratan keamanan Anda, Anda dapat mengubah pernyataan kebijakan menggunakan contoh di [Pernyataan kebijakan utama KMS lanjutan](#). Untuk panduan tentang keputusan ini, lihat [Pertimbangan untuk memilih pernyataan kebijakan utama KMS dasar vs. lanjutan](#).

1. Salin kebijakan dasar ke editor dan masukkan pengidentifikasi yang diperlukan dan nama utama IAM dalam pernyataan kebijakan kunci KMS. Untuk bantuan menemukan nilai dari pengidentifikasi yang direferensikan, lihat [Di mana menemukan pengidentifikasi yang diperlukan](#).
2. Jika persyaratan keamanan Anda membutuhkannya, perbaiki pernyataan kebijakan menggunakan contoh di [Pernyataan kebijakan utama KMS lanjutan](#).

Important

Berhati-hatilah saat memodifikasi kebijakan kunci KMS untuk kunci yang sudah digunakan oleh Pusat Identitas IAM. Meskipun IAM Identity Center memvalidasi izin enkripsi dan dekripsi saat Anda mengkonfigurasi kunci KMS pada awalnya, IAM tidak dapat memverifikasi perubahan kebijakan berikutnya. Menghapus izin yang diperlukan secara tidak sengaja dapat mengganggu operasi normal Pusat Identitas IAM Anda. Untuk panduan memecahkan masalah kesalahan umum terkait kunci yang dikelola pelanggan di Pusat Identitas IAM, lihat [Memecahkan masalah kunci yang dikelola pelanggan di AWS IAM Identity Center](#)

Note

IAM Identity Center dan Identity Store terkait memerlukan izin tingkat layanan untuk menggunakan kunci KMS yang dikelola pelanggan Anda. Persyaratan ini meluas ke aplikasi AWS terkelola yang memanggil API layanan Pusat Identitas IAM menggunakan kredensial layanan. Untuk kasus penggunaan lain di mana API layanan Pusat Identitas IAM dipanggil dengan sesi akses [maju](#), hanya prinsipal IAM yang memulai (seperti administrator) yang memerlukan izin kunci KMS. Khususnya, pengguna akhir yang menggunakan portal AWS akses AWS dan aplikasi terkelola tidak memerlukan izin kunci KMS langsung, karena mereka diberikan melalui layanan masing-masing.

Langkah 3: Buat kunci KMS yang dikelola pelanggan

Anda dapat membuat kunci yang dikelola pelanggan menggunakan Konsol AWS Manajemen atau API AWS KMS. Saat membuat kunci, tambahkan pernyataan kebijakan kunci KMS yang Anda siapkan di Langkah 2 ke dalam kebijakan kunci KMS. Untuk petunjuk terperinci, termasuk panduan tentang kebijakan kunci KMS default, lihat Panduan [Pengembang Layanan Manajemen K AWS unci](#).

Kunci harus memenuhi persyaratan berikut:

- Kunci KMS harus berada di Wilayah yang sama AWS dengan instance Pusat Identitas IAM
- Anda dapat memilih kunci Multi-wilayah atau Satu wilayah. Namun, jika Anda berencana untuk menggunakan Pusat Identitas IAM dalam beberapa, Wilayah AWS Anda harus membuat kunci KMS multi-wilayah. Anda tidak dapat mengonversi kunci KMS satu wilayah ke kunci Multi-wilayah, jadi sebaiknya mulai dengan kunci KMS multi-wilayah kecuali Anda memiliki persyaratan khusus untuk menggunakan kunci KMS wilayah tunggal.
- Kunci KMS harus berupa kunci simetris yang dikonfigurasi untuk penggunaan “mengkripsi dan mendekripsi”
- Kunci KMS harus berada di akun AWS Organizations manajemen yang sama dengan instance organisasi Pusat Identitas IAM

Note

Jika Anda berencana untuk mereplikasi kunci KMS ini ke Wilayah tempat Anda ingin mereplikasi Pusat Identitas IAM Anda, sebaiknya selesaikan penyiapan terlebih dahulu di bagian ini, lalu ikuti panduan di [the section called “Mereplikasi Pusat Identitas IAM ke Wilayah tambahan”](#)

Langkah 4: Konfigurasikan kebijakan IAM untuk penggunaan kunci KMS lintas akun

Setiap prinsipal IAM yang menggunakan API layanan Pusat Identitas IAM dari AWS akun lain, seperti administrator yang didelegasikan IAM Identity Center, juga memerlukan pernyataan kebijakan IAM yang memungkinkan penggunaan kunci KMS melalui API ini.

Untuk setiap kasus penggunaan yang diidentifikasi pada langkah 1:

1. Temukan templat pernyataan kebijakan IAM terkait di kunci KMS dasar dan pernyataan kebijakan IAM.
2. Salin template ke editor dan isi kunci ARN, yang sekarang tersedia setelah pembuatan kunci KMS di langkah 3. Untuk bantuan menemukan nilai ARN kunci, lihat [Di mana menemukan pengidentifikasi yang diperlukan](#).
3. Di bagian Konsol Manajemen AWS, cari kebijakan IAM dari prinsipal IAM yang terkait dengan kasus penggunaan. Lokasi kebijakan ini bervariasi tergantung pada kasus penggunaan dan bagaimana akses diberikan.
 - Untuk akses yang diberikan langsung di IAM, Anda dapat menemukan prinsipal IAM, seperti peran IAM di konsol IAM.

- Untuk akses yang diberikan melalui Pusat Identitas IAM, Anda dapat menemukan set izin terkait di konsol Pusat Identitas IAM.
4. Tambahkan pernyataan kebijakan IAM khusus kasus penggunaan ke peran IAM dan simpan perubahan.

 Note

Kebijakan IAM yang dijelaskan di sini adalah kebijakan berbasis identitas. Meskipun kebijakan tersebut dapat dilampirkan ke pengguna, grup, dan peran IAM, kami merekomendasikan penggunaan peran IAM jika memungkinkan. Lihat panduan pengguna IAM untuk informasi selengkapnya tentang peran IAM versus pengguna IAM.

Konfigurasi tambahan di beberapa AWS aplikasi yang dikelola

Beberapa AWS aplikasi terkelola mengharuskan Anda mengonfigurasi peran layanan untuk mengizinkan aplikasi menggunakan API layanan Pusat Identitas IAM. Jika organisasi Anda menggunakan aplikasi AWS terkelola dengan Pusat Identitas IAM, selesaikan langkah-langkah berikut untuk setiap aplikasi yang digunakan:

1. Lihat panduan pengguna aplikasi untuk mengonfirmasi apakah izin telah diperbarui untuk menyertakan izin terkait kunci KMS untuk penggunaan aplikasi dengan Pusat Identitas IAM.
2. Jika demikian, perbarui izin seperti yang diinstruksikan dalam panduan pengguna aplikasi untuk menghindari gangguan pada operasi aplikasi.

 Note

Jika Anda tidak yakin apakah aplikasi AWS terkelola menggunakan izin ini, sebaiknya periksa panduan pengguna semua aplikasi terkel AWS yang digunakan. Anda hanya perlu melakukan konfigurasi ini sekali untuk setiap aplikasi yang memerlukan konfigurasi.

Langkah 5: Konfigurasi kunci KMS di Pusat Identitas IAM

 Important

Sebelum melanjutkan dengan langkah ini:

- Pastikan aplikasi terkel AWS ola Anda kompatibel dengan kunci KMS yang dikelola pelanggan. Untuk daftar aplikasi yang kompatibel, lihat aplikasi ter [AWS kelola yang dapat Anda gunakan dengan Pusat](#) Identitas IAM. Jika Anda memiliki aplikasi yang tidak kompatibel, jangan lanjutkan.
- Konfigurasi izin yang diperlukan untuk penggunaan kunci KMS. Tanpa izin yang tepat, langkah ini mungkin gagal atau mengganggu administrasi Pusat Identitas IAM, penggunaan aplikasi ter AWS kelola, dan kasus penggunaan lainnya yang memerlukan izin kunci KMS. Untuk informasi selengkapnya, lihat [Langkah 1: Identifikasi kasus penggunaan untuk organisasi Anda](#).
- Pastikan izin untuk aplikasi ter AWS kelola dan aplikasi yang dikelola pelanggan yang memanggil API layanan Pusat Identitas IAM dengan peran IAM juga memungkinkan penggunaan kunci KMS melalui API layanan Pusat Identitas IAM. Beberapa AWS aplikasi terkelola mengharuskan Anda mengonfigurasi izin, seperti peran layanan, untuk penggunaan API ini. Lihat Panduan Pengguna untuk setiap aplikasi terkelola AWS yang digunakan untuk mengonfirmasi apakah Anda perlu menambahkan izin kunci KMS tertentu.

Tentukan kunci KMS saat mengaktifkan instance organisasi baru dari Pusat Identitas IAM

 Note

Jika Wilayah AWS diaktifkan secara default, Anda dapat mengonfigurasi kunci yang dikelola pelanggan sebagai bagian dari pembuatan instance. Untuk informasi selengkapnya, lihat [Aktifkan Pusat Identitas IAM](#).

Saat mengaktifkan instance organisasi baru dari Pusat Identitas IAM di Wilayah di mana opsi konfigurasi instans tidak tersedia, Anda dapat menentukan kunci KMS yang dikelola pelanggan selama penyiapan. Ini memastikan instance menggunakan kunci Anda untuk enkripsi saat diam sejak awal. Sebelum Anda mulai, lihat [Pertimbangan untuk kunci KMS yang dikelola pelanggan dan kebijakan kunci KMS lanjutan](#).

1. Pada halaman Aktifkan Pusat Identitas IAM, perluas bagian Enkripsi saat istirahat.
2. Pilih Kelola Enkripsi.
3. Pilih kunci yang dikelola pelanggan.
4. Untuk kunci KMS, lakukan salah satu hal berikut:

- a. Pilih Pilih dari kunci KMS Anda dan pilih kunci yang Anda buat dari daftar dropdown.
 - b. Pilih Masukkan kunci KMS ARN dan masukkan ARN lengkap kunci Anda.
5. Pilih Simpan.
 6. Pilih Aktif kan untuk menyelesaikan penyiapan.

Untuk informasi selengkapnya, lihat Meng [aktifkan Pusat](#) Identitas IAM.

Mengubah konfigurasi kunci untuk instance organisasi yang ada dari Pusat Identitas IAM

Anda dapat mengubah kunci KMS yang dikelola pelanggan ke kunci lain atau beralih ke kunci yang AWS dimiliki kapan saja.

Console

Untuk mengubah konfigurasi kunci KMS Anda

1. Buka konsol Pusat Identitas IAM di <https://console.aws.amazon.com/singlesignon/>.
2. Pada panel navigasi, silakan pilih Pengaturan.
3. Pilih tab Pengaturan tambahan.
4. Pilih Kel ola enkripsi.
5. Pilih salah satu cara berikut:
 - a. Kunci yang dikelola pelanggan - Pilih kunci yang dikelola pelanggan yang berbeda dari dropdown atau masukkan kunci baru ARN.
 - b. AWS kunci yang dimiliki - Beralih ke opsi enkripsi default.
6. Pilih Simpan.

AWS CLI

Untuk mengubah instance organisasi yang ada dari Pusat Identitas IAM untuk menggunakan kunci yang dikelola pelanggan KMS

```
aws sso-admin update-instance \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --encryption-configuration \  
    KeyType=CUSTOMER_MANAGED_KEY,KmsKeyArn=arn:aws:kms:us-  
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab
```

Untuk mengubah instance organisasi yang ada dari Pusat Identitas IAM untuk menggunakan kunci yang AWS dimiliki

```
aws sso-admin update-instance \  
  --instance-arn arn:aws:sso:::instance/ssoins-1234567890abcdef \  
  --encryption-configuration KeyType=AWS_OWNED_KMS_KEY
```

Pertimbangan utama yang dikelola pelanggan

- Memperbarui kunci KMS yang dikonfigurasi untuk operasi Pusat Identitas IAM tidak berpengaruh pada sesi pengguna aktif di Pusat Identitas IAM Anda. Anda dapat terus menggunakan portal AWS akses, konsol Pusat Identitas IAM, dan API layanan Pusat Identitas IAM selama proses ini.
- Saat beralih ke kunci KMS baru, Pusat Identitas IAM memvalidasi bahwa ia dapat menggunakan kunci dengan sukses untuk enkripsi dan dekripsi. Jika Anda membuat kesalahan selama penyiapan kebijakan kunci atau kebijakan IAM, konsol akan menampilkan pesan kesalahan penjelasan, dan kunci KMS sebelumnya akan tetap digunakan.
- Rotasi kunci KMS tahunan default akan berlangsung secara otomatis. Anda dapat merujuk ke Panduan Peng [AWS KMS embang](#) untuk informasi tentang topik seperti rotasi [kunci](#), [pemantauan AWS KMS kunci](#), dan pengen [dalian akses ke penghapusan kunci](#).

Important

Jika kunci KMS yang dikelola pelanggan yang digunakan oleh instance Pusat Identitas IAM dihapus, dinonaktifkan, atau tidak dapat diakses karena kebijakan kunci KMS yang salah, pengguna tenaga kerja Anda dan administrator Pusat Identitas IAM tidak akan dapat menggunakan Pusat Identitas IAM. Hilangnya akses dapat bersifat sementara (kebijakan kunci dapat diperbaiki) atau permanen (kunci yang dihapus tidak dapat dipulihkan) tergantung pada keadaan. Sebaiknya [batasi akses](#) ke operasi penting, seperti menghapus atau menonaktifkan kunci KMS. Selain itu, kami menyarankan agar organisasi Anda menyiapkan prosedur [AWS akses pecahan kaca](#) untuk memastikan pengguna istimewa Anda dapat mengakses jika AWS Pusat Identitas IAM tidak dapat diakses.

Di mana menemukan pengidentifikasi yang diperlukan

Saat mengonfigurasi izin untuk kunci KMS yang dikelola pelanggan, Anda memerlukan pengidentifikasi AWS sumber daya tertentu untuk melengkapi kebijakan kunci dan templat pernyataan kebijakan IAM. Masukkan pengidentifikasi yang diperlukan (misalnya, ID organisasi) dan nama utama IAM dalam pernyataan kebijakan kunci KMS.

Di bawah ini adalah panduan untuk menemukan pengidentifikasi ini di Konsol AWS Manajemen.

Pusat Identitas IAM Nama Sumber Daya Amazon (ARN) dan Toko Identitas ARN

Instans Pusat Identitas IAM adalah AWS sumber daya dengan ARN uniknya sendiri seperti `arn:aws:sso::: -1234567890abcdef. instance/sso:ins` ARN mengikuti pola yang didokumentasikan di bagian tipe sumber daya Pusat Identitas IAM dari Referensi Otorisasi Layanan.

Setiap instance Pusat Identitas IAM memiliki Identity Store terkait yang menyimpan identitas pengguna dan grup. Identity Store memiliki pengenal unik yang disebut Identity Store ID (misalnya, `d-123456789a`). ARN mengikuti pola yang didokumentasikan di bagian Jenis sumber daya Identity Store dari Referensi [Otorisasi Layanan](#).

Anda dapat menemukan nilai ARN dan Identity Store ID di halaman Pengaturan Pusat Identitas IAM Anda. ID penyimpanan identitas ada di tab Sumber Identitas.

AWS Organizations ID

Jika Anda ingin menentukan ID organisasi (misalnya, `o-exampleorg1`) di kebijakan utama Anda, Anda dapat menemukan nilainya di halaman Pengaturan Pusat Identitas IAM dan konsol Organisasi. ARN mengikuti pola yang didokumentasikan di bagian Jenis sumber daya Organisasi dari Referensi Otorisasi Layanan.

Kunci KMS ARN

Anda dapat menemukan ARN dari kunci KMS di AWS KMS konsol. Pilih kunci yang dikelola pelanggan di sebelah kiri, klik tombol yang ARN-nya ingin Anda cari, dan Anda akan melihatnya di bagian Konfigurasi Umum. ARN mengikuti pola yang didokumentasikan di bagian AWS KMS tipe sumber daya Referensi Otorisasi Layanan.

Lihat Panduan Peng AWS Key Management Service embang untuk informasi selengkapnya tentang Kebijakan Utama dalam AWS KMS dan pemecahan masalah AWS KMS izin. Untuk informasi selengkapnya tentang kebijakan IAM dan representasi JSON mereka, lihat Panduan Pengguna IAM.

Kebijakan kunci KMS dasar

Kebijakan kunci KMS berikut mencakup skenario penerapan yang paling umum: instans Pusat Identitas IAM dengan administrator yang didelegasikan dan aplikasi terkel AWS ola, termasuk AWS Control Tower, SSO ke instans Amazon EC2, dan alur kerja khusus. Gunakan kebijakan ini sebagai titik awal saat membuat kunci KMS yang dikelola pelanggan untuk Pusat Identitas IAM. Jika Anda memerlukan kontrol akses yang lebih terperinci, seperti membatasi kunci ke instans atau aplikasi Pusat Identitas IAM tertentu, lihat [Pernyataan kebijakan utama KMS lanjutan](#). Harap dicatat jika menggunakan kunci Multi-wilayah, kebijakan yang sama harus digunakan di semua replika untuk membantu memastikan otorisasi yang konsisten.

Untuk menggunakan kebijakan ini, ganti nilai placeholder berikut dengan nilai milik Anda:

- **111122223333**— ID AWS akun instans Pusat Identitas IAM Anda (akun AWS Organizations manajemen).
- **444455556666**— ID AWS akun administrasi yang didelegasikan Anda. Jika Anda tidak menggunakan administrasi yang didelegasikan, hapus prinsip ini.

Karena Pusat Identitas AWS IAM mengharuskan kunci KMS berada di Akun yang sama AWS dengan layanan, pernyataan berikut menggunakan `${aws:ResourceAccount}` variabel `${aws:ResourceOrgID}` dan alih-alih nilai literal. Anda dapat mengganti variabel-variabel ini dengan ID AWS Organisasi dan ID AWS Akun jika Anda lebih suka melakukannya.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowIdentityCenterAdminAccounts",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:root",
          "arn:aws:iam::444455556666:root"
        ]
      },
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Sid": "AllowIdentityCenterAndIdentityStoreToDescribeKey",
```

```

    "Effect": "Allow",
    "Principal": {
      "Service": [
        "identitystore.amazonaws.com",
        "sso.amazonaws.com"
      ]
    },
    "Action": "kms:DescribeKey",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "${aws:ResourceAccount}"
      }
    }
  },
  {
    "Sid": "AllowIdentityCenterAndIdentityStoreToUseKey",
    "Effect": "Allow",
    "Principal": {
      "Service": [
        "identitystore.amazonaws.com",
        "sso.amazonaws.com"
      ]
    },
    "Action": [
      "kms:Decrypt",
      "kms:ReEncryptTo",
      "kms:ReEncryptFrom",
      "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "${aws:ResourceAccount}"
      },
      "ForAnyValue:StringEquals": {
        "kms:EncryptionContextKeys": [
          "aws:sso:instance-arn",
          "aws:identitystore:identitystore-arn"
        ]
      }
    }
  }
},
{

```



```

    "Sid": "AllowOrgPrincipalsViaIdentityCenterAndIdentityStore",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:PrincipalOrgID": "${aws:ResourceOrgID}"
      },
      "StringLike": {
        "kms:ViaService": [
          "sso.*.amazonaws.com",
          "identitystore.*.amazonaws.com"
        ]
      },
      "ForAnyValue:StringEquals": {
        "kms:EncryptionContextKeys": [
          "aws:sso:instance-arn",
          "aws:identitystore:identitystore-arn"
        ]
      }
    }
  },
  {
    "Sid": "AllowManagedApps",
    "Effect": "Allow",
    "Principal": "*",
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "Bool": {
        "aws:PrincipalIsAWSService": "true"
      },
      "StringEquals": {
        "aws:SourceOrgID": "${aws:ResourceOrgID}"
      },
      "StringLike": {
        "kms:ViaService": [
          "identitystore.*.amazonaws.com",
          "sso.*.amazonaws.com"
        ]
      },
      "ForAnyValue:StringEquals": {
        "kms:EncryptionContextKeys": [

```

```

        "aws:sso:instance-arn",
        "aws:identitystore:identitystore-arn"
    ]
}
}
}
]
}

```

Kebijakan ini berisi lima pernyataan. Tabel berikut menjelaskan apa yang dilakukan setiap pernyataan.

Pernyataan	Tujuan
<code>AllowIdentityCenterAdminAccounts</code>	Memberikan izin kunci KMS penuh ke akun manajemen Pusat Identitas IAM dan akun administrasi yang didelegasikan. Ini termasuk tindakan manajemen kunci seperti memodifikasi kebijakan kunci dan penjadwalan penghapusan kunci. Administrator di akun ini dapat mengelola dan menggunakan kunci jika mereka memiliki izin yang diperlukan dalam kebijakan berbasis identitas mereka.
<code>AllowIdentityCenterAndIdentityStoreToDescribeKey</code>	Mengizinkan prinsipal layanan Pusat Identitas IAM dan Identity Store untuk mengambil metadata kunci. Ini diperlukan untuk operasi layanan yang memvalidasi kunci tanpa melakukan enkripsi atau dekripsi. <code>aws:SourceAccount</code> Kondisi ini membantu memastikan hanya instance Pusat Identitas IAM yang dapat menggunakan kunci KMS Anda.
<code>AllowIdentityCenterAndIdentityStoreToUseKey</code>	Mengizinkan prinsipal layanan Pusat Identitas IAM dan Identity Store menggunakan kunci untuk operasi enkripsi seperti mengenkripsi, mendekripsi, dan mengenkripsi ulang data. <code>aws:SourceAccount</code> Kondisi ini membantu memastikan hanya instance Pusat Identitas IAM yang dapat menggunakan kunci KMS Anda.
<code>AllowOrgPrincipalsViaIdentityCenterAndIdentityStore</code>	Mengizinkan prinsipal IAM di AWS Organisasi Anda untuk mendekripsi data melalui layanan Pusat Identitas IAM dan Penyimpanan Identitas. Ini mencakup administrator aplikasi

Pernyataan	Tujuan
	yang berinteraksi dengan Center-integrated AWS layanan Identitas IAM menggunakan Forward Access Sessions (FAS).
AllowManagedApps	Memungkinkan AWS aplikasi terkelola untuk mendekripsi data yang dilindungi oleh kunci KMS Anda melalui Pusat Identitas IAM dan Penyimpanan Identitas.

Gunakan pernyataan kebijakan IAM berikut [Langkah 4: Konfigurasi kebijakan IAM untuk penggunaan kunci KMS lintas akun](#) untuk mengizinkan administrator yang didelegasikan menggunakan kunci KMS melalui API layanan Pusat Identitas IAM. Ganti kunci contoh ARN dengan kunci KMS ARN Anda yang sebenarnya. Wilayah wildcard dalam contoh mengakomodasi semua replika kunci KMS multi-wilayah.

Untuk kasus penggunaan lintas akun selain administrasi Pusat Identitas IAM, seperti SSO ke instans Amazon EC2 atau administrasi aplikasi terkel AWS, cukup `AllowCrossAccountKMSKeyUse` upkan ke `kms:Decrypt` hanya dan menghapus pernyataan tersebut. `AllowListKMSKeyAliases`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCrossAccountKMSKeyUse",
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:DescribeKey"
      ],
      "Resource": [
        "arn:aws:kms:*:111122223333:key/mrk-1234abcd-12ab-34cd-56ef-1234567890ab"
      ]
    },
    {
      "Sid": "AllowListKMSKeyAliases",
      "Effect": "Allow",
      "Action": "kms:ListAliases",
      "Resource": "*"
    }
  ]
}
```

```
]
}
```

Pernyataan kebijakan utama KMS lanjutan

Gunakan pernyataan kebijakan kunci KMS lanjutan untuk menerapkan kontrol akses yang lebih terperinci untuk kunci KMS yang dikelola pelanggan Anda. Kebijakan ini dibangun di atas [Kebijakan kunci KMS dasar](#) dengan menambahkan kondisi konteks enkripsi dan batasan khusus layanan. Sebelum memutuskan apakah akan menggunakan pernyataan kebijakan kunci KMS lanjutan, pastikan untuk meninjau pertimbangan terkait.

Menggunakan konteks enkripsi untuk membatasi akses

Anda dapat membatasi penggunaan kunci KMS ke instance Pusat Identitas IAM tertentu dengan menambahkan kondisi konteks enkripsi ke `AllowManagedApps` pernyataan `AllowOrgPrincipalsViaIdentityCenterAndIdentityStore` dan di dalam. [Kebijakan kunci KMS dasar](#) Tambahkan kondisi berikut dengan instance Identity Center spesifik ARN dan Identity Store ARN Anda. Anda juga dapat menambahkan kondisi konteks enkripsi yang sama ke kebijakan IAM yang dikonfigurasi untuk penggunaan kunci KMS lintas akun.

Pusat Identitas

```
"StringEquals": {
  "kms:EncryptionContext:aws:sso:instance-arn":
  "arn:aws:sso::instance/ssoins-1234567890abcdef"
}
```

Penyimpanan Identitas

```
"StringEquals": {
  "kms:EncryptionContext:aws:identitystore:identitystore-arn":
  "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
}
```

Jika Anda memerlukan bantuan untuk menemukan pengidentifikasi ini, lihat [Di mana menemukan pengidentifikasi yang diperlukan](#).

 Note

Anda dapat menggunakan kunci KMS yang dikelola pelanggan hanya dengan instance organisasi Pusat Identitas IAM. Kunci yang dikelola pelanggan harus berada di akun manajemen AWS organisasi, yang membantu memastikan kunci digunakan dengan satu instance Pusat Identitas IAM. Namun, mekanisme konteks enkripsi memberikan perlindungan teknis independen dari penggunaan instance tunggal. Anda juga dapat menggunakan kunci `aws:SourceArn` kondisi dalam pernyataan kebijakan kunci KMS yang ditujukan untuk prinsipal layanan Identity Center dan Identity Store.

Pertimbangan untuk menerapkan kondisi konteks enkripsi

Sebelum menerapkan kondisi konteks enkripsi, tinjau persyaratan berikut:

- **DescribeKey tindakan.** Konteks enkripsi tidak dapat diterapkan pada tindakan “kms:DescribeKey”, yang dapat digunakan oleh administrator Pusat Identitas IAM. Saat mengonfigurasi kebijakan kunci KMS Anda, kecualikan konteks enkripsi untuk tindakan khusus ini untuk memastikan operasi yang tepat dari instance Pusat Identitas IAM Anda.
- **Pengaturan instans baru.** Jika Anda mengaktifkan instance Pusat Identitas IAM baru dengan kunci KMS yang dikelola pelanggan, lihat [Pertimbangan untuk kunci KMS yang dikelola pelanggan dan kebijakan kunci KMS lanjutan](#)
- **Perubahan sumber identitas.** Saat mengubah sumber identitas Anda ke atau dari Active Directory, konteks enkripsi memerlukan perhatian khusus. Lihat [Pertimbangan untuk mengubah sumber identitas Anda](#).

Templat kebijakan

Pilih dari templat kebijakan lanjutan ini berdasarkan persyaratan keamanan Anda. Seimbangkan kontrol akses granular dengan overhead administratif yang mereka perkenalkan.

Topik yang dibahas di sini:

- [Pernyataan kebijakan KMS untuk penggunaan read-only dari instance Pusat Identitas IAM tertentu.](#) Bagian ini menunjukkan penggunaan konteks enkripsi untuk akses read-only ke IAM Identity Center.
- [Pernyataan kebijakan utama KMS yang disempurnakan untuk penggunaan AWS aplikasi yang dikelola.](#) Bagian ini menunjukkan cara menyempurnakan kebijakan kunci KMS untuk aplikasi AWS

terkelola menggunakan konteks enkripsi dan informasi aplikasi, seperti prinsip layanan aplikasi, ARN aplikasi, dan ID AWS akun.

Pernyataan kebijakan KMS untuk penggunaan read-only dari instance Pusat Identitas IAM tertentu

Kebijakan ini memungkinkan [auditor keamanan](#) dan personel lain yang hanya memerlukan akses baca ke Pusat Identitas IAM untuk menggunakan kunci KMS.

Untuk menggunakan kebijakan ini:

1. Ganti contoh prinsipal IAM administrator read-only dengan prinsipal IAM administrator Anda yang sebenarnya
2. Ganti contoh instance IAM Identity Center instance ARN dengan ARN instans aktual
3. Ganti contoh Identity Store ARN dengan ARN Identity Store Anda yang sebenarnya
4. Jika menggunakan administrasi [yang didelegasikan](#), lihat [Langkah 4: Konfigurasi kebijakan IAM untuk penggunaan kunci KMS lintas akun](#)

Jika Anda memerlukan bantuan untuk menemukan nilai pengidentifikasi ini, lihat [Di mana menemukan pengidentifikasi yang diperlukan](#).

Setelah Anda memperbarui template dengan nilai-nilai Anda, kembalilah [Langkah 2: Siapkan pernyataan kebijakan utama KMS](#) untuk menyiapkan pernyataan kebijakan utama KMS tambahan, sesuai kebutuhan.

Tindakan KMS:Decrypt saja tidak membatasi akses ke operasi read-only. Kebijakan IAM harus menerapkan akses baca-saja pada API layanan Pusat Identitas IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowReadOnlyAccessToIdentityCenterAPI",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyAdminRole"
      },
      "Action": "kms:Decrypt",
    }
  ]
}
```

```

    "Resource": "*",
    "Condition": {
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn":
"arn:aws:sso::instance/ssoins-1234567890abcdef"
      }
    },
    {
      "Sid": "AllowReadOnlyAccessToIdentityStoreAPI",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/MyAdminRole"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn":
"arn:aws:identitystore::111122223333:identitystore/d-1234567890"
        }
      }
    }
  ]
}

```

Pernyataan kebijakan utama KMS yang disempurnakan untuk penggunaan AWS aplikasi yang dikelola

Templat kebijakan ini memberikan kontrol yang lebih terperinci atas aplikasi ter AWS kelola mana yang dapat menggunakan kunci KMS Anda.

Note

Beberapa aplikasi AWS terkelola tidak dapat digunakan dengan Pusat Identitas IAM yang dikonfigurasi dengan kunci KMS yang dikelola pelanggan. Lihat aplikasi [AWS terkelola yang dapat Anda gunakan dengan Pusat](#) Identitas IAM.

Mem [Kebijakan kunci KMS dasar](#) ungkinan aplikasi ter AWS kelola apa pun dari akun mana pun di AWS organisasi yang sama untuk menggunakan kunci KMS. Gunakan kebijakan yang disempurnakan ini untuk membatasi akses dengan:

- Prinsip layanan aplikasi
- ARN instance aplikasi
- AWS ID akun
- Konteks enkripsi untuk instans Pusat Identitas IAM tertentu

 Note

Prinsip layanan adalah pengidentifikasi unik untuk AWS layanan, biasanya diformat sebagai servicename.amazonaws.com (misalnya, elasticmapreduce.amazonaws.com untuk Amazon EMR).

Batasi berdasarkan akun

Templat pernyataan kebijakan kunci KMS ini memungkinkan aplikasi AWS terkelola di AWS akun tertentu untuk menggunakan kunci KMS menggunakan instance Pusat Identitas IAM tertentu.

Untuk menggunakan kebijakan ini:

1. Ganti contoh prinsip layanan dengan prinsip layanan aplikasi Anda yang sebenarnya
2. Ganti contoh ID akun dengan ID akun aktual tempat aplikasi ter AWS kelola Anda digunakan
3. Ganti contoh Identity Store ARN dengan ARN Identity Store Anda yang sebenarnya
4. Ganti contoh contoh IAM Identity Center instance ARN dengan ARN instance aktual Anda

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowServiceInSpecificAccountsToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
```



```

    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": [
          "111122223333",
          "444455556666"
        ]
      },
      "StringLike": {
        "kms:ViaService": "sso.*.amazonaws.com",
        "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/
ssoins-1234567890abcdef"
      },
      "Bool": {
        "aws:PrincipalIsAWSService": "true"
      }
    },
    {
      "Sid": "AllowServiceInSpecificAccountsToUseTheKMSKeyViaIdentityStore",
      "Effect": "Allow",
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": [
            "111122223333",
            "444455556666"
          ]
        },
        "StringLike": {
          "kms:ViaService": "identitystore.*.amazonaws.com",
          "kms:EncryptionContext:aws:identitystore:identitystore-arn":
"arn:aws:identitystore::111122223333:identitystore/d-1234567890"
        },
        "Bool": {
          "aws:PrincipalIsAWSService": "true"
        }
      }
    }
  ]

```

```
}
```

Batasi berdasarkan instance aplikasi

Templat pernyataan kebijakan kunci KMS ini memungkinkan instance aplikasi ter AWS kelola tertentu untuk menggunakan kunci KMS menggunakan instance Pusat Identitas IAM tertentu.

Untuk menggunakan kebijakan ini:

1. Ganti contoh prinsip layanan dengan prinsip layanan aplikasi Anda yang sebenarnya
2. Ganti contoh aplikasi ARN dengan contoh aplikasi ARN Anda yang sebenarnya
3. Ganti contoh Identity Store ARN dengan ARN Identity Store Anda yang sebenarnya
4. Ganti contoh contoh IAM Identity Center instance ARN dengan ARN instance aktual Anda

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSpecificAppInstanceToUseTheKMSKeyViaIdentityCenter",
      "Effect": "Allow",
      "Principal": {
        "Service": "myapp.amazonaws.com"
      },
      "Action": "kms:Decrypt",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceARN": "arn:aws:myapp:us-east-1:111122223333:application/my-
application"
        },
        "StringLike": {
          "kms:ViaService": "sso.*.amazonaws.com",
          "kms:EncryptionContext:aws:sso:instance-arn": "arn:aws:sso:::instance/
ssoins-1234567890abcdef"
        },
        "Bool": {
          "aws:PrincipalIsAWSService": "true"
        }
      }
    }
  ],
  {
```

```

    "Sid": "AllowSpecificAppInstanceToUseTheKMSKeyViaIdentityStore",
    "Effect": "Allow",
    "Principal": {
      "Service": "myapp.amazonaws.com"
    },
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:SourceARN": "arn:aws:myapp:us-east-1:111122223333:application/my-
application"
      },
      "StringLike": {
        "kms:ViaService": "identitystore.*.amazonaws.com",
        "kms:EncryptionContext:aws:identitystore:identitystore-arn":
"arn:aws:identitystore::111122223333:identitystore/d-1234567890"
      },
      "Bool": {
        "aws:PrincipalIsAWSService": "true"
      }
    }
  }
]
}

```

Pertimbangan untuk kunci KMS yang dikelola pelanggan dan kebijakan kunci KMS lanjutan

Saat menerapkan kunci KMS yang dikelola pelanggan dengan Pusat Identitas IAM, pertimbangkan faktor-faktor ini yang memengaruhi penyiapan, keamanan, dan pemeliharaan berkelanjutan konfigurasi enkripsi Anda.

Pertimbangan untuk memilih pernyataan kebijakan utama KMS dasar vs. lanjutan

Saat memutuskan apakah akan membuat izin kunci KMS lebih spesifik menggunakan [Pernyataan kebijakan utama KMS lanjutan](#), pertimbangkan overhead manajemen dan kebutuhan keamanan organisasi Anda. Pernyataan kebijakan yang lebih spesifik memberikan kontrol yang lebih detail atas siapa yang dapat menggunakan kunci dan untuk tujuan apa; namun, pernyataan kebijakan tersebut memerlukan pemeliharaan berkelanjutan seiring dengan berkembangnya konfigurasi Pusat Identitas IAM Anda. Misalnya, jika Anda membatasi penggunaan kunci KMS untuk penerapan aplikasi terkel AWS ola tertentu, Anda harus memperbarui kebijakan kunci setiap kali organisasi Anda ingin menerapkan atau membatalkan penerapan aplikasi. Kebijakan yang kurang ketat mengurangi

beban administrasi tetapi dapat memberikan izin yang lebih luas daripada yang diperlukan untuk persyaratan keamanan Anda.

Pertimbangan untuk mengaktifkan instance Pusat Identitas IAM baru dengan kunci KMS yang dikelola pelanggan

Pertimbangan di sini berlaku jika Anda menggunakan konteks enkripsi seperti yang dijelaskan dalam [Pernyataan kebijakan utama KMS lanjutan](#) untuk membatasi penggunaan kunci KMS ke instance Pusat Identitas IAM tertentu.

Saat mengaktifkan instance Pusat Identitas IAM baru dengan kunci KMS yang dikelola pelanggan, Pusat Identitas IAM dan ARN Penyimpanan Identity tidak tersedia sampai setelah penyiapan. Anda memiliki opsi berikut:

- Gunakan pola ARN generik sementara, lalu ganti dengan ARN penuh setelah instance diaktifkan. Ingatlah untuk beralih antara StringEquals dan StringLike operator sesuai kebutuhan.
 - Untuk Pusat Identitas IAM SPN: “arn: \$ {Partition} :sso: ::instance/*”.
 - Untuk Toko Identitas SPN: “arn: \$ {Partition} :identitystore: :\$ {Akun} :identitystore/*”.
- Gunakan “Purpose:key_configuration” di ARN sementara. Ini hanya berfungsi untuk pengaktifan misalnya dan harus diganti dengan ARN yang sebenarnya agar instance Pusat Identitas IAM Anda berfungsi secara normal. Keuntungan dari pendekatan ini adalah Anda tidak dapat lupa untuk mengganti ini setelah instance diaktifkan.
 - Untuk SPN Pusat Identitas IAM, gunakan: “arn: \$ {Partition} :sso: :::KEY_CONFIGURATION” instance/purpose
 - Untuk Identity Store SPN, gunakan: “arn: \$ {Partition} :identitystore: :\$ {Account} ::KEY_CONFIGURATION” identitystore/purpose

 Important

Jangan terapkan konfigurasi ini ke kunci KMS yang sudah digunakan di instance Pusat Identitas IAM yang ada, karena dapat mengganggu operasi normalnya.

- Menghilangkan kondisi konteks enkripsi dari kebijakan kunci KMS hingga instans diaktifkan.

Sumber daya penandaan AWS IAM Identity Center

Tag adalah label atribut kustom yang Anda tambahkan ke AWS sumber daya agar lebih mudah mengidentifikasi, mengatur, 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 tag ke string kosong, tetapi Anda tidak dapat mengatur nilai tag ke null. Mengabaikan nilai tag sama dengan menggunakan sebuah string kosong.

Tag membantu Anda mengidentifikasi dan mengatur AWS sumber daya Anda. Banyak AWS layanan mendukung penandaan, sehingga Anda dapat menetapkan tag yang sama ke sumber daya dari layanan yang berbeda untuk menunjukkan bahwa sumber daya 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 AWS Panduan 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.

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 Pusat Identitas IAM APIs untuk menambahkan, mengedit, atau menghapus tag untuk set izin.

Bagian berikut memberikan informasi lebih lanjut tentang tag untuk IAM Identity Center.

Topik

- [Batasan tag](#)
- [Mengelola tag dengan menggunakan konsol IAM Identity Center](#)

- [AWS CLI contoh](#)
- [Mengelola tag menggunakan IAM Identity Center API](#)

Batasan tag

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 awalan untuk kunci; itu dicadangkan untuk AWS digunakan

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 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.

AWS CLI contoh

AWS CLI Ini 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

Gunakan tindakan API berikut untuk menetapkan, melihat, dan menghapus tag untuk set izin atau instance Pusat Identitas IAM.

- [TagResource](#)
- [ListTagsForResource](#)
- [UntagResource](#)
- [CreatePermissionSet](#)
- [CreateInstance](#)

Mengintegrasikan AWS CLI dengan IAM Identity Center

AWS Integrasi Command Line Interface (CLI) versi 2 dengan IAM Identity Center menyederhanakan proses masuk. Pengembang AWS CLI dapat masuk langsung ke 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 mengonfigurasi IAM Identity Center untuk menggunakan Active Directory untuk otentikasi, pengembang dapat masuk AWS CLI langsung menggunakan kredensialnya Active Directory.

AWS Integrasi CLI dengan IAM Identity Center menawarkan manfaat berikut:

- Perusahaan dapat memungkinkan pengembang mereka untuk masuk menggunakan kredensial dari IAM Identity Center atau Active Directory dengan menghubungkan IAM Identity Center ke Active Directory mereka menggunakan Directory Service
- Pengembang dapat masuk dari CLI untuk akses yang lebih cepat.
- Pengembang dapat membuat daftar dan beralih 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 mengintegrasikan AWS CLI dengan IAM Identity Center

Untuk menggunakan integrasi AWS CLI dengan IAM Identity Center, unduh, instal, dan konfigurasi AWS Command Line Interface versi 2. Untuk langkah-langkah rinci tentang cara mengunduh dan mengintegrasikan Pusat Identitas IAM AWS CLI dengan IAM, lihat [Mengonfigurasi AWS CLI untuk menggunakan Pusat Identitas IAM](#) di Panduan Pengguna.AWS Command Line Interface

Pertimbangan untuk Akses Konsol Manajemen AWS Pribadi

Jika organisasi Anda menggunakan fitur Akses Konsol Manajemen AWS Pribadi, Anda harus mempertimbangkan bagaimana pengguna Anda akan masuk ke Pusat Identitas IAM.

Kebijakan titik akhir VPC membatasi proses masuk ke konsol manajemen, yang mencegah pengguna Anda masuk ke Akun AWS mereka tidak diizinkan untuk mengaksesnya. Untuk informasi selengkapnya, lihat [Akses Konsol Manajemen AWS Pribadi](#) di Panduan Konsol Manajemen AWS Memulai.

Titik akhir VPC memblokir proses masuk ke Pusat Identitas IAM

Penting untuk dicatat bahwa menggunakan titik akhir VPC akan memblokir proses masuk ke Pusat Identitas IAM. Ini terjadi ketika pengguna sudah masuk ke konsol manajemen melalui titik akhir VPC. Untuk memastikan pengguna Anda dapat terus masuk ke Pusat Identitas IAM, mereka harus menggunakan titik akhir publik untuk AWS login, bukan titik akhir VPC.

Kuota dan batasan di Pusat Identitas IAM

Tabel berikut menjelaskan kuota dalam Pusat Identitas IAM. 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 untuk mengelola Pusat Identitas IAM secara terpusat jika Anda memiliki lebih dari 50.000 pengguna, 10.000 grup, 500 set izin, atau 3.000 aplikasi. Untuk informasi lebih lanjut tentang CLI, lihat [Mengintegrasikan AWS CLI 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 SAML	50.000 karakter	Tidak
Batas ukuran file sertifikat IdP yang diunggah ke Pusat Identitas IAM	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	3500	Ya
Jumlah set izin yang disediakan yang diizinkan per Akun AWS	500	Ya
Jumlah kebijakan sebaris per kumpulan izin	1	Tidak
Jumlah kebijakan yang AWS dikelola dan dikelola pelanggan per kumpulan izin	25 ¹	Tidak
Ukuran maksimum kebijakan sebaris per kumpulan izin	32.768 byte. Ukuran maksimum karakter non-spasi dalam kebijakan sebaris per kumpulan izin adalah 10.240 byte.	Tidak
Jumlah peran IAM (kumpulan izin) Akun AWS yang dapat diperbarui pada satu waktu	1	Tidak

¹ AWS Identity and Access Management (IAM) menetapkan kuota 10 kebijakan terkelola per peran. Untuk memanfaatkan kuota ini, minta peningkatan kebijakan terkelola kuota IAM yang dilampirkan ke peran IAM di konsol Kuota Layanan untuk setiap Akun AWS tempat Anda ingin menerapkan kumpulan izin.

Note

[Kelola Akun AWS dengan set izin](#) disediakan Akun AWS sebagai peran IAM, atau menggunakan peran IAM yang ada di Akun AWS, dan karenanya 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 penyimpanan identitas Pusat Identitas IAM

Sumber daya	Kuota bawaan	Dapat ditingkatkan
Jumlah pengguna yang didukung di Pusat Identitas IAM	200000	Ya
Jumlah grup yang didukung di Pusat Identitas IAM	100000	Ya

Batas throttle Pusat Identitas IAM

Sumber daya	Kuota bawaan
API Pusat Identitas IAM	API Pusat Identitas IAM memiliki batas throttle kolektif 20 transaksi per detik (TPS). Untuk API baca, Anda dapat membuka kasus dukungan untuk meminta kenaikan batas. API CreateAccountAssignment tulis memiliki batas 15 panggilan asinkron yang luar biasa. Batas ini tidak dapat dinaikkan.

Sumber daya	Kuota bawaan
API Penyimpanan Identitas	Identity Store API memiliki batas throttle 20 transaksi per detik (TPS) per API. Batas ini berlaku per instans Identity Store. Anda dapat membuka kasus dukungan untuk meminta kenaikan batas.
SCIM API	<p>SCIM API memiliki batas throttle per API sebesar 25 transaksi per detik (TPS) untuk menulis API dan 40 TPS untuk API baca. Batas ini berlaku per instans Identity Store. Anda dapat membuka kasus dukungan untuk meminta kenaikan batas.</p> <p>Setiap operasi keanggotaan individu di <code>CreateGroup</code> atau <code>PatchGroup</code> panggilan dihitung sebagai transaksi menuju batas pembatasan operasi keanggotaan terpisah per Identity Store.</p>

Jika instance Pusat Identitas IAM Anda diaktifkan dalam beberapa Wilayah AWS, batas throttle berlaku sama untuk setiap Wilayah yang diaktifkan. Misalnya, Anda akan memiliki batas throttle 20 TPS pada API Penyimpanan Identitas di setiap Wilayah yang diaktifkan. Untuk informasi selengkapnya tentang operasi API yang tersedia di Wilayah tambahan, lihat [tabel yang sesuai](#).

Kuota permintaan layanan OIDC

Sumber daya	Nilai default (permintaan per detik)	Dapat ditingkatkan
Minta tarif dari alamat jarak jauh untuk mendaftarkan klien OAuth publik	20	Ya
Berlaku untuk: RegisterClient		

Sumber daya	Nilai default (permintaan per detik)	Dapat ditingkatkan
<p>Minta tarif dari klien publik yang terdaftar dengan layanan OIDC</p> <p>Berlaku untuk: CreateToken, StartDeviceAuthorization</p>	80	Ya
<p>Tarif permintaan dari semua klien publik yang terdaftar dengan instance Pusat Identitas IAM yang sama</p> <p>Berlaku untuk: CreateToken</p>	250	Ya
<p>Minta tarif dari aplikasi Pusat Identitas IAM yang terdaftar dengan instance Pusat Identitas IAM dengan hibah Token Exchange dan Refresh Token.</p> <p>Berlaku untuk: CreateTokenWithIAM</p>	80	Ya
<p>Tingkat pembuatan token dari semua aplikasi Pusat Identitas IAM yang terdaftar dengan instance Pusat Identitas IAM yang sama dengan hibah JWT Bearer</p> <p>Berlaku untuk: CreateTokenWithIAM</p>	10	Hubungi AWS Dukungan

Jika instans Pusat Identitas IAM Anda diaktifkan dalam beberapa Wilayah AWS, tarif permintaan di atas berlaku sama untuk setiap Wilayah yang diaktifkan. Misalnya, jika tingkat permintaan yang diizinkan untuk mendaftarkan klien OAuth publik dari alamat jarak jauh adalah 20 permintaan per detik, throughput ini tersedia di setiap Wilayah yang diaktifkan. Untuk informasi selengkapnya tentang operasi API yang tersedia di Wilayah tambahan, lihat [tabel yang sesuai](#).

Kuota tambahan

Sumber daya	Kuota bawaan	Dapat ditingkatkan
Jumlah total Akun AWS atau aplikasi yang dapat dikonfigurasi* **	7000	Ya
Jumlah total instans Pusat Identitas IAM per akun	1	Tidak
Jumlah total penerbit token terpercaya	10	Tidak
Jumlah total grup yang dapat ditetapkan ke kumpulan izin per Akun AWS, atau ke aplikasi	100	Tidak
Jumlah total yang Wilayah AWS diaktifkan untuk satu instans Pusat Identitas IAM	6	Ya

* Kuota ini berlaku secara terpisah untuk Akun AWS dan untuk aplikasi. Anda dapat mengonfigurasi hingga 7000 akun dan hingga 7000 aplikasi.

** Oper [ProvisionPermissionSet](#) asi API dapat menyediakan kumpulan izin menggunakan opsi ALL_PROVISIONED_ACCOUNTS untuk, paling banyak, 3500 Akun AWS. Jika Anda perlu menyediakan izin yang disetel ke lebih dari 3500 Akun AWS, Anda dapat menggunakan operasi ProvisionPermissionSet API dengan AWS_ACCOUNT opsi, yang menyediakan izin yang

ditetapkan dalam satu Akun AWS. Anda dapat melakukan hingga tiga panggilan bersamaan ke `ProvisionPermissionSet`.

Memecahkan masalah Pusat Identitas IAM

Berikut ini dapat membantu Anda memecahkan beberapa masalah umum yang mungkin Anda temui saat menyiapkan atau menggunakan konsol Pusat Identitas IAM.

Masalah saat membuat instance akun Pusat Identitas IAM

Beberapa batasan mungkin berlaku saat membuat instance akun Pusat Identitas IAM. Jika Anda tidak dapat membuat instance akun melalui konsol Pusat Identitas IAM, atau pengalaman penyiapan aplikasi terkel AWS ola yang didukung, verifikasi kasus penggunaan berikut:

- Periksa yang lain Wilayah AWS Akun AWS di mana Anda mencoba membuat instance akun. Anda terbatas pada satu instance Pusat Identitas IAM per. Akun AWS Untuk mengaktifkan aplikasi, beralih ke Wilayah AWS dengan instance Pusat Identitas IAM atau beralih ke akun tanpa instance Pusat Identitas IAM.
- Jika organisasi Anda mengaktifkan Pusat Identitas IAM sebelum 14 September 2023, administrator Anda mungkin perlu ikut serta dalam pembuatan instans akun. Bekerja sama dengan administrator Anda untuk mengaktifkan pembuatan instance 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, tambahkan akun Anda ke daftar izinkan.

Anda menerima kesalahan saat mencoba melihat daftar aplikasi cloud yang telah dikonfigurasi sebelumnya untuk bekerja dengan Pusat Identitas IAM

Kesalahan berikut ini terjadi ketika Anda memiliki kebijakan yang mengizinkan `sso:ListApplications` tetapi tidak mengizinkan API Pusat Identitas IAM lainnya. Perbarui kebijakan Anda untuk mengatasi kesalahan ini.

`ListApplications` izin mengotorisasi beberapa API:

- `ListApplicationsAPI`.

- API internal yang mirip dengan `ListApplicationProviders` API yang digunakan di konsol Pusat Identitas IAM.

Untuk membantu menyelesaikan duplikasi, API internal sekarang juga mengizinkan penggunaan tindakan. `ListApplicationProviders` Untuk mengizinkan `ListApplications` API publik tetapi menolak API internal, kebijakan Anda harus menyertakan pernyataan yang menolak `ListApplicationProviders` tindakan tersebut:

```
"Statement": [  
  {  
    "Effect": "Deny",  
    "Action": "sso:ListApplicationProviders",  
    "Resource": "*"  
  },  
  {  
    "Effect": "Allow",  
    "Action": "sso: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": "sso:ListApplicationProviders",  
    "Resource": "*"  
  }  
]
```

Saat kebijakan Anda diperbarui, hubungi Dukungan untuk menghapus tindakan proaktif ini.

Masalah mengenai isi pernyataan SAML yang dibuat oleh Pusat Identitas IAM

Pusat Identitas IAM menyediakan pengalaman debug berbasis web untuk pernyataan SAML yang dibuat dan dikirim oleh Pusat Identitas IAM, termasuk atribut dalam pernyataan ini, saat mengakses Akun AWS dan aplikasi SAML dari portal akses. AWS Untuk melihat detail pernyataan SAML yang dihasilkan IAM Identity Center, gunakan langkah-langkah berikut.

1. Masuk ke portal AWS akses.
2. Saat Anda masuk ke portal, tahan tombol Shift, pilih ubin aplikasi, lalu lepaskan tombol Shift.
3. Periksa informasi pada halaman berjudul `Anda sekarang dalam mode administrator`. Untuk menyimpan informasi ini untuk referensi di masa mendatang, pilih `Salin XML`, dan tempel isinya di tempat lain.
4. Pilih `Kirim <application>` untuk 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 Identity Provider (IdP) dikonfigurasi untuk menyediakan pengguna ke Pusat Identitas IAM menggunakan sinkronisasi SCIM, Anda mungkin mengalami kegagalan sinkronisasi selama proses penyediaan pengguna. Ini mungkin menunjukkan bahwa konfigurasi pengguna di IdP Anda tidak kompatibel dengan persyaratan Pusat Identitas IAM. Ketika ini terjadi, API SCIM Pusat Identitas IAM akan mengembalikan pesan kesalahan yang memberikan wawasan tentang akar penyebab masalah. Anda dapat menemukan pesan kesalahan ini di log atau UI IdP Anda. Atau, Anda dapat menemukan informasi lebih rinci tentang kegagalan penyediaan di [AWS CloudTrail log](#).

Untuk informasi selengkapnya tentang implementasi SCIM Pusat Identitas IAM, termasuk spesifikasi parameter dan operasi yang diperlukan, opsional, dan tidak didukung untuk objek pengguna, lihat Panduan Pengembang Implementasi SCIM Pusat Identitas IAM di [Panduan Pengembang SCIM](#)

Berikut ini adalah beberapa alasan umum untuk kesalahan ini:

1. Objek pengguna di IdP tidak memiliki nama pertama (diberikan), nama (keluarga) terakhir, nama and/or tampilan.

Pesan Kesalahan: "2 kesalahan validasi terdeteksi: Nilai '*name.givenName*' gagal memenuhi batasan: Anggota harus memenuhi pola ekspresi reguler: `[\\ p {L}\\ p {M}\\ p {S}\\ p {N}\\ p {P}\\ p {P}\\ t\\ n\\ r] +`; Nilai '*name.givenName*' gagal memenuhi batasan: Anggota harus memiliki panjang lebih besar dari atau sama dengan 1"

- Solusi: Tambahkan nama pertama (diberikan), terakhir (keluarga), dan tampilan untuk objek pengguna. Selain itu, pastikan pemetaan penyediaan SCIM untuk objek pengguna di IdP Anda dikonfigurasi untuk mengirim nilai yang tidak kosong untuk semua atribut ini.

2. Lebih dari satu nilai untuk atribut tunggal dikirim untuk pengguna (juga dikenal sebagai "atribut multi-nilai"). Misalnya, pengguna mungkin memiliki nomor telepon kantor dan nomor 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.

Pesan Kesalahan: "Atribut daftar *emails* melebihi batas yang diizinkan 1"

- Pilihan solusi:
 - i. Perbarui pemetaan penyediaan SCIM Anda untuk objek pengguna di IdP Anda untuk mengirim hanya satu nilai untuk atribut tertentu. 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 satu atau nol nilai yang ditetapkan untuk atribut tersebut untuk pengguna.
 - iii. Jika atribut tidak diperlukan untuk tindakan apa pun di AWS, 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 hanya menggunakan satu atribut untuk pencocokan dengan pengguna di Pusat Identitas IAM. Misalnya, pemetaan username atau userPrincipalName di IdP ke userName atribut di SCIM untuk penyediaan ke Pusat Identitas IAM akan benar dan cukup untuk sebagian besar implementasi.

Duplikat kesalahan pengguna atau grup saat menyediakan pengguna atau grup dengan penyedia identitas eksternal

Jika Anda mengalami masalah sinkronisasi Pusat Identitas IAM saat menyediakan pengguna atau grup di penyedia identitas eksternal (IdP), itu mungkin karena pengguna atau grup IdP eksternal Anda tidak memiliki nilai atribut unik. Anda mungkin menerima pesan kesalahan berikut di IdP eksternal Anda:

Menolak untuk membuat sumber daya duplikat baru

Anda dapat mengalami masalah ini dalam skenario berikut:

- Skenario 1
 - Anda menggunakan atribut non-unik yang disesuaikan di IdP eksternal untuk atribut yang harus unik di Pusat Identitas IAM. Pengguna atau grup IAM Identity Center yang ada gagal melakukan sinkronisasi ke IdP Anda.
- Skenario 2
 - Anda mencoba membuat pengguna yang memiliki atribut duplikat untuk atribut yang harus unik di Pusat Identitas IAM.
 - Misalnya, Anda membuat atau memiliki pengguna Pusat Identitas IAM yang sudah ada dengan atribut berikut:
 - Nama Pengguna: Jane Doe
 - Alamat Email Utama: jane_doe@example.com
 - Kemudian Anda mencoba untuk membuat pengguna lain di IdP eksternal Anda dengan atribut berikut:
 - Nama Pengguna: Richard Doe
 - Alamat Email Utama: jane_doe@example.com

- IdP eksternal mencoba menyinkronkan dan membuat pengguna di Pusat Identitas IAM. Namun, tindakan ini gagal karena kedua pengguna memiliki nilai duplikat untuk alamat email utama yang harus unik.

Nama pengguna, alamat email utama, dan ExternalID harus unik agar pengguna IdP eksternal Anda berhasil menyinkronkan ke Pusat Identitas IAM. Demikian pula, nama grup harus unik agar grup IdP eksternal Anda berhasil disinkronkan ke Pusat Identitas IAM.

Solusinya adalah meninjau atribut sumber identitas Anda dan memastikannya unik.

Pengguna tidak dapat masuk jika 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 Pusat Identitas IAM menggunakan direktori terhubung yang telah diaktifkan dengan MFA dan mode verifikasi telah disetel ke salah satu atau Context-aware. Always-on Dalam skenario ini, pengguna harus masuk dengan nama logon tingkat bawah (DOMAIN\). UserName Untuk informasi selengkapnya, lihat [MFA untuk pengguna direktori 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 dimulai dengan 'awsReservedsso_'. Ini adalah peran yang telah dibuat oleh layanan Pusat Identitas IAM di akun, dan mereka berasal dari menetapkan set izin ke akun. Mencoba memodifikasi peran ini dari dalam konsol IAM akan mengakibatkan kesalahan berikut:

```
'Cannot perform the operation on the protected role 'AWSReservedSSO_RoleName_Here' -  
this role is only modifiable by AWS'
```


Peran-peran ini hanya dapat dimodifikasi dari konsol Administrator Pusat Identitas IAM, yang ada di akun manajemen. AWS Organizations Setelah dimodifikasi, Anda kemudian dapat mendorong perubahan ke AWS akun yang ditugaskan.

Pengguna direktori tidak dapat mengatur ulang kata sandi mereka

Ketika pengguna direktori mengatur ulang kata sandi mereka menggunakan Lupa Kata Sandi? opsi selama masuk ke portal AWS akses, kata sandi baru mereka harus mematuhi kebijakan kata sandi default seperti yang dijelaskan dalam [Persyaratan kata sandi saat mengelola identitas di Pusat Identitas IAM](#).

Jika pengguna memasukkan kata sandi yang mematuhi kebijakan dan kemudian menerima kesalahan `We couldn't update your password`, periksa untuk melihat apakah kegagalan AWS CloudTrail dicatat. 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 cukup panjang, atau mengandung karakter khusus, dan ini dapat menyebabkan karakter dihapus dalam panggilan API, sehingga mengakibatkan kesalahan. Anda mungkin ingin mencoba mengatur 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 kumpulan 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 pengguna, dihapus kemudian dibuat ulang

menggunakan nama pengguna yang sama (untuk pengguna) atau nama (untuk grup) di penyedia identitas, pengenal internal unik baru dibuat untuk pengguna atau grup baru di Pusat Identitas IAM. Namun, Pusat Identitas IAM masih memiliki referensi ke pengenal 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 Akun AWS lama dari tempat aslinya ditetapkan, lalu menetapkan kembali akses ke pengguna atau grup. Ini memperbarui kumpulan 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 tersebut, lalu menambahkan kembali pengguna atau grup.

Anda juga dapat memeriksa apakah mencatat kegagalan dengan mencari CloudTrail log Anda untuk peristiwa sinkronisasi SCIM yang mereferensikan nama pengguna atau grup yang bersangkutan.

AWS CloudTrail

Saya tidak dapat mengonfigurasi aplikasi saya dari katalog aplikasi dengan benar

Jika Anda menambahkan aplikasi dari katalog aplikasi di Pusat Identitas IAM, 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 Pusat Identitas IAM, 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 satu alasan umum adalah ketidakcocokan antara informasi pengguna yang dibawa dalam permintaan SAML, dan informasi untuk pengguna di Pusat Identitas IAM.

Agar pengguna Pusat Identitas IAM berhasil masuk saat menggunakan IdP eksternal sebagai sumber identitas, berikut ini harus benar:

- Format SAML NameID (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 Pusat Identitas IAM dari federasi SAML 2.0 hanya mendukung 1 pernyataan dalam respons SAML antara penyedia identitas dan Pusat Identitas IAM. Itu tidak mendukung pernyataan SAML terenkripsi.
- Pernyataan berikut berlaku jika [Atribut untuk kontrol akses](#) diaktifkan di akun Pusat Identitas IAM Anda:
 - Jumlah atribut yang dipetakan dalam permintaan SAML harus 50 atau kurang.
 - Permintaan SAML tidak boleh berisi atribut multi-nilai.
 - Permintaan SAML tidak boleh berisi beberapa atribut dengan nama yang sama.
 - Atribut tidak boleh berisi XML terstruktur sebagai nilai.
 - Format Nama harus berupa format yang ditentukan SAML, bukan format generik.

Note

Pusat Identitas IAM tidak melakukan pembuatan pengguna atau grup “tepat waktu” untuk pengguna atau grup baru melalui federasi SAML. 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 instance Pusat Identitas IAM Anda. Pastikan kedua nilai ini cocok dengan tepat.

Selain itu, Anda dapat memecahkan masalah kegagalan masuk penyedia identitas eksternal lebih lanjut dengan membuka AWS CloudTrail dan memfilter nama ExternalIdPDDirectoryLogin acara.

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 otentikator platform di browser macOS dan iOS. Jika pengguna mencoba mendaftar WebAuthn ke 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 browser/platform dukungan. Untuk informasi selengkapnya tentang WebAuthn di Pusat Identitas IAM, lihat [FIDO2 autentikator](#).

Grup “Pengguna Domain” Direktori Aktif tidak disinkronkan dengan benar ke Pusat Identitas IAM

Grup Pengguna Domain Direktori Aktif adalah “grup utama” default untuk objek pengguna AD. Grup utama Direktori Aktif dan keanggotaannya tidak dapat dibaca oleh Pusat Identitas IAM. 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 atau Microsoft 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 'Terjadi kesalahan tak terduga' ketika saya mencoba mendaftar atau masuk menggunakan aplikasi otentikator

Time-based Sistem kata sandi satu kali (TOTP), seperti yang digunakan oleh IAM Identity Center dalam kombinasi dengan aplikasi otentikator berbasis kode, bergantung pada sinkronisasi waktu antara klien dan server. Pastikan perangkat tempat aplikasi otentikator Anda diinstal disinkronkan dengan benar ke sumber waktu yang dapat diandalkan, atau atur waktu secara manual di perangkat Anda agar sesuai dengan sumber yang dapat diandalkan, seperti NIST (<https://www.time.gov/>) atau yang setara lainnya local/regional .

Saya mendapatkan kesalahan 'Ini bukan Anda, ini kami' saat mencoba masuk ke Pusat Identitas IAM

Kesalahan ini menunjukkan ada masalah penyiapan dengan instance Pusat Identitas IAM Anda atau penyedia identitas eksternal (IdP) yang digunakan Pusat Identitas IAM sebagai sumber identitasnya. Kami sarankan Anda memverifikasi yang berikut ini:

- Verifikasi pengaturan tanggal dan waktu pada perangkat yang Anda gunakan untuk masuk. Kami menyarankan Anda mengatur tanggal dan waktu untuk diatur secara otomatis. Jika tidak tersedia, sebaiknya sinkronkan tanggal dan waktu Anda ke server Network Time Protocol (NTP) yang dikenal.
- Pastikan sertifikat IdP yang diunggah ke Pusat Identitas IAM sama dengan yang disediakan oleh IdP Anda. Anda dapat memeriksa sertifikat dari konsol Pusat Identitas IAM dengan menavigasi ke Pengaturan. Di tab Sumber Identitas pilih Tindakan dan kemudian pilih Kelola Otentikasi. Jika sertifikat IdP dan IAM Identity Center tidak cocok, impor sertifikat baru ke Pusat Identitas IAM.
- Pastikan format NameID dalam file metadata penyedia identitas Anda adalah sebagai berikut:
 - `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`
- Jika Anda menggunakan Konektor AD AWS Directory Service sebagai penyedia identitas Anda, verifikasi bahwa kredensial untuk akun layanan sudah benar dan belum kedaluwarsa. Lihat [Memperbarui kredensial akun layanan Konektor AD Anda AWS Directory Service](#) untuk informasi selengkapnya.

Pengguna saya tidak menerima email dari Pusat Identitas IAM

Semua email yang dikirim oleh layanan Pusat Identitas IAM akan berasal dari alamat `no-reply@signin.aws` atau `no-reply@login.awsapps.com`. Sistem email Anda harus dikonfigurasi sehingga menerima email dari alamat email pengirim ini dan tidak menanganinya sebagai sampah atau spam.

Kesalahan: Anda tidak dapat delete/modify/remove/assign mengakses kumpulan 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 izin akun manajemen AWS Organizations. Untuk mengatasi masalah ini, masuk sebagai pengguna yang memiliki izin ini dan coba lakukan tugas lagi atau tetapkan tugas ini kepada seseorang yang memiliki izin yang benar. Untuk informasi selengkapnya, lihat [Daftarkan akun anggota](#).

Kesalahan: Token sesi tidak ditemukan atau tidak valid

Kesalahan ini dapat terjadi ketika klien, seperti browser web, AWS Toolkit, atau AWS CLI, mencoba menggunakan sesi yang dicabut atau tidak valid di sisi server. Untuk memperbaiki masalah ini, kembali ke aplikasi klien atau situs web dan coba lagi, termasuk masuk lagi jika diminta. Ini terkadang mengharuskan Anda untuk juga membatalkan permintaan yang tertunda, seperti upaya koneksi yang tertunda dari AWS Toolkit dalam IDE Anda.

Anggota grup dari domain tepercaya tidak disinkronkan ke Pusat Identitas IAM

Jika grup keamanan berhasil menyinkronkan ke Pusat Identitas IAM, tetapi anggotanya dari domain lokal tepercaya tidak muncul di Pusat Identitas IAM, hal ini dapat disebabkan oleh grup yang berada di AWS Managed Microsoft AD dan berisi Prinsip Keamanan Asing (FSP) yang mewakili pengguna dari domain tepercaya.

Coba langkah-langkah berikut untuk memecahkan masalah:

- Sinkronkan grup langsung dari domain tepercaya: Alih-alih menyinkronkan grup dari AWS Managed Microsoft AD yang berisi anggota lintas domain, buat dan sinkronkan grup langsung dari

domain lokal terpercaya. Pendekatan ini berfungsi karena Pusat Identitas IAM dapat mengakses objek pengguna aktual di domain sumber.

- Verifikasi izin akun layanan: Pastikan akun layanan Pusat Identitas IAM memiliki izin yang diperlukan pada objek pengguna di domain terpercaya: ReadProperties dan ListContents izin.

Memecahkan masalah kunci yang dikelola pelanggan di AWS IAM Identity Center

Topik ini menjelaskan kesalahan terkait kunci yang dikelola pelanggan umum yang mungkin Anda temui saat menggunakan AWS IAM Identity Center dan menyediakan langkah-langkah pemecahan masalah untuk mengatasinya.

Akses Ditolak: Masalah Izin Mendekripsi KMS

Kesalahan: “Pengguna xxxxxxxx tidak berwenang untuk melakukan: KMS:mendekripsi pada sumber daya yang terkait dengan ciphertext ini karena tidak ada kebijakan berbasis identitas yang mengizinkan tindakan KMS:Decrypt”

Pengguna atau prinsipal IAM tidak memiliki kms :Decrypt izin yang diperlukan baik dalam kebijakan IAM atau kebijakan kunci KMS mereka.

Pemecahan masalah dengan AWS CloudTrail:

1. Cari kms .amazonaws .com acara di CloudTrail
2. Cari nama acara Decrypt
3. Tinjau errorMessage bidang errorCode dan
4. Periksa userIdentity untuk mengonfirmasi kepala sekolah mana yang mencoba operasi

Untuk mengatasi masalah ini, berikan izin kms :Decrypt akses utama pengguna atau IAM dalam kebijakan IAM dan kebijakan kunci KMS mereka. Untuk informasi selengkapnya, lihat [Menerapkan kunci KMS yang dikelola pelanggan di AWS IAM Identity Center](#).

AWS kegagalan login aplikasi terkelola dengan kunci yang dikelola pelanggan diaktifkan di Pusat Identitas IAM

Jika tidak ada pengguna Pusat Identitas yang dapat masuk ke aplikasi terkel AWS dan Anda mengaktifkan kunci yang dikelola pelanggan di instans Pusat Identitas IAM Anda, verifikasi bahwa

kebijakan kunci KMS memberikan izin aplikasi terkel AWS ola untuk menggunakan kunci yang dikelola pelanggan. Untuk informasi selengkapnya, lihat [Kebijakan kunci KMS dasar](#).

AWS kegagalan penugasan and/or pengguna instalasi aplikasi terkelola dengan kunci yang dikelola pelanggan diaktifkan di Pusat Identitas IAM

Kesalahan: “Pengguna xxxxxxxx tidak berwenang untuk melakukan: KMS:mendekripsi pada sumber daya yang terkait dengan ciphertext ini karena tidak ada kebijakan berbasis identitas yang mengizinkan tindakan KMS:Decrypt”

Pengguna atau prinsipal IAM tidak memiliki kms :Decrypt izin yang diperlukan baik dalam kebijakan IAM atau kebijakan kunci KMS mereka.

Pemecahan masalah dengan CloudTrail:

1. Cari nama acara Decrypt
2. Tinjau errorMessage bidang errorCode dan
3. Periksa userIdentity untuk mengonfirmasi kepala sekolah mana yang mencoba operasi

Untuk mengatasi masalah ini, berikan izin kms :Decrypt akses utama pengguna atau IAM dalam kebijakan IAM dan kebijakan kunci KMS mereka. Untuk informasi selengkapnya, lihat [Menerapkan kunci KMS yang dikelola pelanggan di AWS IAM Identity Center](#).

Masalah Izin KMS: Mengkonfigurasi Kunci yang Dikelola Pelanggan dengan AWS IAM Identity Center

Pengguna atau prinsipal IAM tidak memiliki satu atau beberapa izin KMS yang diperlukan (kms:Decrypt,, kms:Encryptkms:GenerateDataKey,kms:DescribeKey) saat mengaktifkan kunci yang dikelola pelanggan.

Pemecahan masalah dengan CloudTrail:

1. CariDecrypt,Encrypt,GenerateDataKey, atau DescribeKey acara
2. Tinjau errorMessage bidang errorCode dan
3. Periksa userIdentity untuk mengonfirmasi kepala sekolah mana yang mencoba operasi

Untuk mengatasi masalah ini, berikan semua izin KMS yang diperlukan kepada pengguna atau prinsipal IAM dalam kebijakan berbasis identitas atau kebijakan kunci KMS mereka. Untuk informasi selengkapnya, lihat [Menerapkan kunci KMS yang dikelola pelanggan di AWS IAM Identity Center](#).

AWS kegagalan login portal akses dengan kunci yang dikelola pelanggan diaktifkan di Pusat Identitas IAM

Kesalahan: "Kode KESALAHAN: 0001 - akses IdentityCenter layanan diblokir. Hubungi IdentityCenter admin Anda untuk langkah lebih lanjut.

Jika pengguna tidak dapat masuk ke portal AWS akses dan Anda mengaktifkan kunci yang dikelola pelanggan di instans Pusat Identitas IAM Anda, verifikasi bahwa kebijakan kunci KMS memberikan izin yang diperlukan untuk Pusat Identitas dan Penyimpanan Identitas. Untuk informasi selengkapnya, lihat [Kebijakan kunci KMS dasar](#).

Memecahkan masalah pengaturan Multi-wilayah di AWS IAM Identity Center

Topik ini menjelaskan kesalahan umum terkait pengaturan multi-wilayah yang mungkin Anda temui saat menggunakan AWS IAM Identity Center dan menyediakan langkah-langkah pemecahan masalah untuk mengatasinya.

Wilayah tempat saya ingin mereplikasi instance Pusat Identitas IAM saya tidak tersedia di konsol Pusat Identitas IAM

Anda harus terlebih dahulu membuat kunci replika untuk kunci yang dikelola pelanggan di Wilayah tempat Anda ingin mereplikasi instance Pusat Identitas IAM Anda. Setelah kunci replika dibuat, Anda akan melihat Wilayah dalam daftar Wilayah yang tersedia untuk replikasi. Untuk informasi selengkapnya, lihat [the section called "Langkah 1: Buat kunci replika"](#).

AWS kegagalan masuk aplikasi terkelola di Wilayah tambahan

Jika tidak ada pengguna Pusat Identitas IAM yang dapat masuk ke aplikasi AWS terkelola di Wilayah tambahan setelah Anda menambahkan Wilayah di Pusat Identitas IAM, konfirmasi bahwa Anda mengonfigurasi URL Layanan Konsumen Penegasan (ACS) Wilayah tambahan di penyedia identitas eksternal seperti yang dijelaskan dalam [the section called "Langkah 3 \(hanya penyedia](#)

[identitas eksternal\): Perbarui pengaturan IdP eksternal](#)” Juga, konfirmasi pengguna Anda memiliki konektivitas ke Wilayah.

Masalah yang mengaktifkan instance Pusat Identitas IAM Multi-wilayah

Jika Anda memilih `Multi-Region instance` saat mengaktifkan Pusat Identitas IAM, proses penyiapan akan membuat kunci yang dikelola pelanggan, mereplikasinya ke Wilayah tambahan, mengaktifkan instance Anda, dan menambahkan Wilayah tambahan. Jika salah satu langkah ini gagal, Anda mungkin melihat salah satu kesalahan berikut.

Pembuatan kunci gagal

Kunci yang dikelola pelanggan tidak dapat dibuat di akun Anda. Instans Anda tidak diaktifkan.

Jika ini adalah kesalahan izin, verifikasi bahwa peran Anda memiliki `kms:TagResource` izin `kms:CreateKey` dan, lalu pilih `Aktifkan` untuk mencoba lagi.

Replikasi kunci gagal

Kunci yang dikelola pelanggan dibuat di akun Anda, tetapi kunci replika tidak dapat dibuat di Wilayah tambahan. Instans Anda tidak diaktifkan.

Jika ini adalah kesalahan izin, verifikasi bahwa peran Anda memiliki `kms:ReplicateKey` izin.

Pilih `Aktifkan` untuk mencoba lagi. Kunci yang sama digunakan.

Jika Anda kembali nanti, temukan kunci di AWS KMS konsol dengan memfilter `tagCreatedBy: IAM Identity Center`. Salin ID kunci, lalu pilih `Instans kustom` dan pilih kunci itu.

Untuk memulai dari awal, hapus kunci di AWS KMS konsol dan pilih `Multi-Region instance` untuk membuat yang baru.

Pembuatan instance gagal

Kunci yang dikelola pelanggan dibuat dan direplikasi ke Wilayah tambahan, tetapi instans Anda tidak dapat diaktifkan.

Jika ini adalah kesalahan izin, verifikasi bahwa peran Anda memiliki [izin yang diperlukan untuk membuat instance](#) Pusat Identitas IAM.

Pilih **Aktif** kan untuk mencoba lagi. Kunci yang sama digunakan.

Jika Anda kembali nanti, temukan kunci di AWS KMS konsol dengan memfilter `tagCreatedBy: IAM Identity Center`. Salin ID kunci, lalu pilih **Instans kustom** dan pilih kunci itu.

Untuk memulai dari awal, hapus kunci dan replika di AWS KMS konsol dan pilih **Multi-Region instance** untuk membuat yang baru.

 Note

Kesalahan ini juga dapat terjadi saat menggunakan **instance kustom** jika pembuatan **instance** atau replikasi Wilayah gagal. Jika Anda memberikan kunci yang dikelola pelanggan Anda sendiri, langkah pembuatan kunci dan replikasi tidak berlaku.

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: 21 Oktober 2025

Perubahan	Deskripsi	Tanggal
One-click Pembuatan instance multi-wilayah	Saat mengaktifkan instance organisasi baru di Wilayah yang didukung, Anda dapat memilih antara Single-Region, Multi-Region, atau konfigurasi instans kustom. Multi-Region Opsi ini mengaktifkan ketahanan Multi-wilayah dalam satu klik dengan secara otomatis membuat kunci KMS yang dikelola pelanggan dan mereplikasi instance Anda ke Wilayah tambahan.	Agustus 6, 2026
Multi-account izin sekarang opsional untuk instance baru	Saat membuat instance organisasi, Anda sekarang dapat memilih apakah akan mengaktifkan izin multi-akun. Secara default, izin multi-akun diaktifkan. Anda dapat mengaktifkan izin multi-akun nanti dari pengaturan instans atau dengan menggunakan UpdateInstance API.	Agustus 4, 2026

[Multi-Region dukungan diperluas ke direktori Identity Center](#)

Multi-Region dukungan sekarang bekerja dengan direktori Identity Center sebagai sumber identitas , selain penyedia identitas eksternal.

Juli 28, 2026

[Kuota terpisah untuk AWS akun dan aplikasi](#)

AWS IAM Identity Center sekarang memberlakukan kuota terpisah untuk AWS akun dan aplikasi. Sebelumnya, sumber daya ini berbagi kuota gabungan tunggal. Kuota default baru untuk masing-masing adalah 7.000.

Juni 22, 2026

[Aktif AWS kan akses akun untuk aplikasi yang dikelola pelanggan](#)

Anda sekarang dapat mengaktifkan `cak sso:account:access` upan untuk aplikasi yang dikelola pelanggan dengan penerbit token tepercaya, memungkinkan mereka mengakses kredentif AWS akun secara terprogram atas nama pengguna akhir.

Juni 19, 2026

[Diperbarui waktu sesi otentikasi untuk perubahan keanggotaan grup](#)

Memperbarui tabel perilaku sesi keanggotaan grup untuk mencerminkan bahwa perubahan izin dan akses aplikasi sekarang berlaku segera saat membuat sesi baru.

Mei 28, 2026

Kebijakan kunci KMS dasar yang disederhanakan	Menggabungkan pernyataan kebijakan kunci KMS dasar ke dalam satu kebijakan sederhana, yang menyederhanakan konfigurasi kunci KMS yang dikelola pelanggan untuk enkripsi saat diam.	30 April 2026
Multi-Region dukungan	Menambahkan dukungan Multi-wilayah, termasuk replikasi ke Wilayah tambahan, Akun AWS akses dan penggunaan aplikasi ter AWS kelola di Wilayah tambahan.	Februari 2, 2026
Kebijakan ter AWS kelola yang diperbarui	Memperbarui kebijakan <code>AWSIdentityCenterExternalManagementPolicy</code> AWS terkelola untuk mengubah ARN untuk penyewa penyewa.	Desember 5, 2025
Topik kebijakan AWS terkelola baru	Menambahkan detail untuk kebijakan yang <code>AWSIdentityCenterExternalManagementPolicy</code> AWS dikelola.	November 21, 2025
Auto-provisioning panduan audit dan rekonsiliasi	Menambahkan panduan untuk mengaudit dan merekonsiliasi pengguna, grup, dan keanggotaan grup SCIM yang disediakan secara otomatis menggunakan API dan perintah Identity Store. AWS CLI	Oktober 17, 2025

Kuota permintaan layanan OIDC	Menambahkan kuota permintaan layanan OIDC, termasuk batas tarif untuk pendaftaran klien OAuth, pembuatan token, dan operasi OIDC lainnya.	Oktober 13, 2025
Pembaruan untuk kebijakan AWS terkelola	Pusat Identitas IAM telah memperbarui kebijakan terkelola <code>AWSSSOMasterAccountAdministrator</code> , <code>AWSSSOMemberAccountAdministrator</code> , <code>AWSSSODirectoryAdministrator</code> , dan <code>AWSSSODirectoryReadOnly</code> untuk menyertakan AWS KMS izin yang diperlukan untuk instans Pusat Identitas IAM yang menggunakan kunci yang dikelola pelanggan untuk enkripsi.	17. September 2025
Kunci yang dikelola pelanggan untuk enkripsi saat istirahat	Menambahkan dukungan untuk kunci KMS yang dikelola pelanggan untuk mengenkripsi data identitas tenaga kerja saat diam.	17. September 2025
Contoh kebijakan berbasis sumber daya untuk mengizinkan pembuatan token	Menambahkan contoh kebijakan berbasis sumber daya yang memungkinkan pembuatan token untuk aplikasi klien resmi.	September 16, 2025

Dukungan untuk sesi latar belakang pengguna	Menambahkan konten untuk sesi latar belakang pengguna.	Agustus 11, 2025
Identity-enhanced sesi konsol	Terminologi yang diperbarui untuk sesi konsol yang ditingkatkan identitas (sebelumnya dikenal sebagai sesi sadar identitas).	12 Mei 2025
Memulai reorganisasi	Mengatur ulang konten untuk memulai untuk meningkatkan kejelasan dan pengalaman pengguna.	6 Mei 2025
Hentikan Sinkronisasi AD Pusat Identitas IAM	Anda tidak dapat lagi menyediakan pengguna Direktori Aktif dengan IAM Identity Center AD Sync. Sebagai gantinya, Anda dapat menggunakan IAM Identity Center yang dapat dikonfigurasi AD Sync.	17 April 2025
Konten yang diperbarui untuk sesi yang diautentikasi	Perbarui ke durasi sesi Pusat Identitas IAM saat sesi pengguna dihapus.	April 2, 2025
Pembaruan untuk kebijakan AWS terkelola	Izin yang diperbarui untuk kebijakan AWSSS0ServiceRolePolicy AWS terkelola.	Februari 11, 2025
Alur kerja pengaktifan Pusat Identitas IAM ditingkatkan	Alur kerja yang diperbarui untuk mengaktifkan instans organisasi dan instans akun Pusat Identitas IAM.	Februari 11, 2025

Pembaruan untuk pengaktifan Pusat Identitas IAM	Konten dan prosedur yang diperbarui untuk mengaktifkan instans organisasi dan instans akun Pusat Identitas IAM.	Oktober 10, 2024
Pembaruan untuk kebijakan AWS terkelola	Izin yang diperbarui untuk kebijakan AWSIAMIdentityCenterAllowListForIdentityContext AWS terkelola.	Oktober 2, 2024
Pembaruan untuk kebijakan AWS terkelola	Izin yang diperbarui untuk kebijakan AWSSSOMasterAccountAdministrator AWS terkelola.	September 26, 2024
Pembaruan untuk kebijakan AWS terkelola	Izin yang diperbarui untuk kebijakan AWSIAMIdentityCenterAllowListForIdentityContext AWS terkelola.	4 September 2024
Pembaruan untuk “Apa itu Pusat Identitas IAM?” topik	Memperbarui konten yang menjelaskan manfaat dan kemampuan Pusat Identitas IAM.	Agustus 19, 2024
Pembaruan untuk kebijakan AWS terkelola	Izin yang diperbarui untuk kebijakan AWSIAMIdentityCenterAllowListForIdentityContext AWS terkelola.	Juli 12, 2024
Pembaruan untuk kebijakan AWS terkelola	Izin yang diperbarui untuk kebijakan AWSIAMIdentityCenterAllowListForIdentityContext AWS terkelola.	27 Juni 2024

Pembaruan untuk kebijakan AWS terkelola	Izin yang diperbarui untuk kebijakan AWSIAMIdentityCenterAllowListForIdentityContext AWS terkelola.	17 Mei 2024
Pembaruan untuk kebijakan AWS terkelola	Izin yang diperbarui untuk kebijakan AWSIAMIdentityCenterAllowListForIdentityContext AWS terkelola.	April 30, 2024
Pembaruan untuk kebijakan AWS terkelola	Izin yang diperbarui untuk kebijakan AWSSSOMasterAccountAdministrator AWS terkelola.	April 26, 2024
Pembaruan untuk kebijakan AWS terkelola	Izin yang diperbarui untuk kebijakan AWSSSOMemberAccountAdministrator AWS terkelola.	April 26, 2024
Pembaruan untuk kebijakan AWS terkelola	Izin yang diperbarui untuk kebijakan AWSSS0ReadOnly AWS terkelola.	April 26, 2024
Pembaruan untuk kebijakan AWS terkelola	Izin yang diperbarui untuk kebijakan AWSIAMIdentityCenterAllowListForIdentityContext AWS terkelola.	April 26, 2024
Pembaruan untuk kebijakan AWS terkelola	Izin yang diperbarui untuk kebijakan AWSIAMIdentityCenterAllowListForIdentityContext AWS terkelola.	April 24, 2024

Pembaruan untuk kebijakan AWS terkelola	Izin yang diperbarui untuk kebijakan AWSIAMIdentityCenterAllowListForIdentityContext AWS terkelola.	April 19, 2024
Pembaruan untuk kebijakan AWS terkelola	Izin yang diperbarui untuk kebijakan AWSIAMIdentityCenterAllowListForIdentityContext AWS terkelola.	April 11, 2024
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 yang AWSIAMIdentityCenterAllowListForIdentityContext AWS dikelola.	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 menyertakan referensi ke Create, Update, dan Delete API baru di Identity Center API Reference Guide.	31 Agustus 2022

<u>AWS Single Sign-On (AWS SSO) berganti nama menjadi Pusat Identitas AWS dan IAM</u>	AWS memperkenalkan AWS IAM Identity Center. Pusat Identitas IAM memperluas kemampuan AWS Identity and Access Management (IAM) untuk membantu Anda mengelola akun dan akses ke aplikasi secara terpusat bagi pengguna tenaga kerja Anda. Fitur Pusat Identitas IAM mencakup penugasan aplikasi, izin multi-akun, dan portal AWS akses.	26 Juli 2022
<u>Dukungan untuk batas izin dan kebijakan yang dikelola pelanggan dalam kumpulan izin</u>	Menambahkan konten untuk menggunakan kebijakan terkelola dan AWS dikelola pelanggan AWS Identity and Access Management (IAM) dengan kumpulan izin.	14 Juli 2022
<u>Dukungan untuk Wilayah yang diaktifkan AWS secara manual</u>	Menambahkan konten untuk menggunakan Pusat Identitas IAM di Wilayah yang diaktifkan secara manual.	15 Juni 2022
<u>Pembaruan untuk kebijakan AWS terkelola</u>	Izin yang diperbarui untuk kebijakan <code>AWSSSOServeRolePolicy</code> AWS terkelola.	Mei 11, 2022
<u>Dukungan untuk administrasi yang didelegasikan</u>	Menambahkan konten untuk fitur administrasi yang didelegasikan.	Mei 11, 2022

Pembaruan untuk kebijakan AWS terkelola	Izin yang diperbarui untuk AWSSSOMasterAccountAdministrator, AWSSSOMemberAccountAdministrator, dan kebijakan AWSSSOREadOnly AWS yang dikelola.	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 yang AWSSSOMasterAccountAdministrator AWS dikelola.	4 Agustus 2021
Pembaruan untuk kuota	Penyesuaian tabel kuota.	21 Desember 2020
Kebijakan contoh baru	Menambahkan contoh kebijakan yang dikelola pelanggan baru dan pembaruan ke bagian izin yang diperlukan.	21 Desember 2020
Dukungan untuk kontrol akses berbasis atribut (ABAC)	Menambahkan konten untuk fitur ABAC.	24 November 2020
Dukungan untuk pendaftaran paksa MFA	Pembaruan untuk mengharuskan pengguna mendaftarkan perangkat MFA saat masuk.	23 November 2020
Dukungan untuk WebAuthn	Menambahkan konten untuk WebAuthn fitur baru.	20 November 2020

Dukungan untuk Ping Identity	Menambahkan konten untuk diintegrasikan dengan Ping Identity produk sebagai penyedia identitas eksternal yang didukung.	26 Oktober 2020
Dukungan untuk OneLogin	Menambahkan konten untuk diintegrasikan OneLogin sebagai penyedia identitas eksternal yang didukung.	31 Juli 2020
Dukungan untuk Okta	Menambahkan konten untuk diintegrasikan Okta sebagai penyedia identitas eksternal yang didukung.	28 Mei 2020
Dukungan untuk penyedia identitas eksternal	Mengubah referensi dari direktori ke sumber identitas, menambahkan konten untuk mendukung penyedia identitas eksternal.	26 November 2019
Pengaturan MFA baru	Menghapus topik verifikasi dua langkah dan menambahkan 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
Dukungan untuk durasi sesi pada AWS akun	Menambahkan konten tentang cara mengatur durasi sesi untuk AWS akun.	30 Oktober 2018

<u>Opsi baru untuk menggunakan direktori Identity Center</u>	Menambahkan konten untuk memilih direktori Identity Center atau menghubungkan ke direktori yang ada di Active Directory.	17 Oktober 2018
<u>Dukungan untuk status relai dan durasi sesi pada aplikasi</u>	Menambahkan konten tentang status relai dan durasi sesi untuk aplikasi.	10 Oktober 2018
<u>Dukungan tambahan untuk aplikasi baru</u>	Ditambahkan 4me, BambooHR, Bonusly, Citrix ShareFile, ClickTime, Convo, Deputy, Deskpro, Dome9, DruvalnSync, 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
<u>Dukungan untuk akses multi-akun ke akun manajemen</u>	Menambahkan konten tentang cara mendelegasikan akses multi-akun ke pengguna di akun manajemen.	9 Juli 2018
<u>Dukungan untuk aplikasi baru</u>	Ditambahkan DocuSign, Keeper Security, dan SugarCRM ke katalog aplikasi.	16 Maret 2018

[Dapatkan kredentif sementara untuk akses CLI](#)

Menambahkan informasi tentang cara mendapatkan kredenSIAL sementara untuk menjalankan AWS CLI perintah.

22 Februari 2018

[Panduan baru](#)

Ini adalah rilis pertama dari Panduan Pengguna Pusat Identitas IAM.

7 Desember 2017

AWS Glosarium

Untuk AWS terminologi terbaru, lihat [AWS glosarium di Referensi](#).Glosarium AWS

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.