



Panduan Pengguna

AWS Resource Access Manager



AWS Resource Access Manager: Panduan Pengguna

Copyright © 2024 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 menghina atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan properti dari masing-masing pemilik, yang mungkin berafiliasi, terkait dengan, atau disponsori oleh Amazon, atau tidak.

Table of Contents

| | |
|---|----|
| Apa itu AWS RAM? | 1 |
| Ikhtisar video | 1 |
| Manfaat dari AWS RAM | 2 |
| Bagaimana dengan akses lintas akun dengan kebijakan berbasis sumber daya? | 2 |
| Cara kerja berbagi sumber daya | 3 |
| Berbagi sumber daya Anda | 3 |
| Menggunakan sumber daya bersama | 5 |
| Mengakses AWS RAM | 5 |
| Harga untuk AWS RAM | 6 |
| Kepatuhan dan standar internasional | 6 |
| PCI DSS | 6 |
| FedRAMP | 6 |
| SOC dan ISO | 7 |
| Mulai | 8 |
| Istilah dan konsep | 8 |
| Berbagi sumber daya | 8 |
| Berbagi akun | 9 |
| Mengonsumsi prinsipal | 10 |
| Kebijakan berbasis sumber daya | 12 |
| Izin terkelola | 16 |
| Versi izin terkelola | 17 |
| Berbagi sumber daya Anda | 18 |
| Aktifkan berbagi sumber daya dalam AWS Organizations | 18 |
| Buat berbagi sumber daya | 20 |
| Menggunakan sumber daya bersama | 29 |
| Menanggapi undangan berbagi sumber daya | 30 |
| Menggunakan sumber daya yang dibagikan dengan Anda | 32 |
| Bekerja dengan sumber bersama | 33 |
| Sumber daya regional dan global | 33 |
| Apa perbedaan antara sumber daya Regional dan global? | 34 |
| Pembagian sumber daya dan Wilayah mereka | 35 |
| Sumber daya yang dimiliki oleh Anda | 37 |
| Melihat pembagian sumber daya yang Anda buat | 37 |
| Membuat berbagi sumber daya | 40 |

| | |
|--|-----|
| Memperbarui pembagian sumber daya | 49 |
| Melihat sumber daya bersama | 56 |
| Melihat kepala sekolah yang Anda bagikan | 58 |
| Cara menghapus berbagi sumber sumber sumber sumber sumber sumber sumber sumber sumber sumber | 60 |
| Sumber daya yang dibagikan dengan Anda | 62 |
| Menerima dan menolak undangan | 62 |
| Melihat berbagi sumber daya yang dibagikan dengan Anda | 66 |
| Melihat sumber daya yang dibagikan dengan Anda | 68 |
| Lihat kepala sekolah berbagi dengan Anda | 70 |
| Meninggalkan berbagi sumber daya | 71 |
| ID Availability Zone | 74 |
| Sumber daya yang dapat dibagikan | 78 |
| AWS App Mesh | 80 |
| AWS AppSync GraphQL API | 80 |
| Amazon Aurora | 81 |
| AWS Private Certificate Authority | 82 |
| Amazon DataZone | 83 |
| AWS CodeBuild | 84 |
| Amazon EC2 | 86 |
| EC2 Image Builder | 91 |
| Amazon FSx for OpenZFS | 95 |
| AWS Glue | 96 |
| AWS License Manager | 100 |
| AWS Marketplace | 101 |
| AWS Migration Hub Refactor Spaces | 101 |
| AWS Network Firewall | 103 |
| AWS Outposts | 104 |
| Amazon S3 di Outposts | 107 |
| Penjelajah Sumber Daya AWS | 108 |
| AWS Resource Groups | 109 |
| Amazon Route 53 | 110 |
| Pengendali Pemulihan Aplikasi Amazon Route 53 | 114 |
| Amazon Simple Storage Service | 116 |
| Amazon SageMaker | 116 |
| AWS Service Catalog AppRegistry | 124 |

| | |
|---|-----|
| AWS Systems Manager Incident Manager | 126 |
| AWS Systems Manager Toko Parameter | 127 |
| Amazon VPC | 129 |
| Kisi VPC Amazon | 139 |
| AWS Awan WAN | 141 |
| Mengelola izin diAWS RAM | 143 |
| Melihat izin yang dikelola | 144 |
| Membuat dan menggunakan izin terkelola pelanggan | 149 |
| Membuat izin terkelola pelanggan | 150 |
| Membuat versi baru izin terkelola pelanggan | 151 |
| Pilih versi yang berbeda untuk menjadi default untuk izin yang dikelola pelanggan | 153 |
| Menghapus versi izin terkelola pelanggan | 155 |
| Menghapus izin terkelola pelanggan | 156 |
| Memperbarui versi izin terkelola | 157 |
| Pertimbangan izin yang dikelola pelanggan | 159 |
| Cara kerja izin terkelola | 160 |
| Jenis izin terkelola | 161 |
| Keamanan | 164 |
| Perlindungan data | 165 |
| Identity and access management | 166 |
| Cara kerja AWS RAM dengan IAM | 166 |
| AWSKebijakan yang dikelola | 169 |
| Menggunakan Peran Tertaut Layanan | 174 |
| Kebijakan contoh IAM | 176 |
| Contoh SCP | 178 |
| Nonaktifkan berbagi dengan Organizations | 182 |
| Pencatatan dan pemantauan | 183 |
| Pemantauan menggunakan CloudWatch Acara | 184 |
| Mencatat log panggilan API AWS RAM dengan AWS CloudTrail | 186 |
| Ketahanan | 188 |
| Keamanan infrastruktur | 188 |
| Memecahkan masalah | 190 |
| Kesalahan: ID Akun tidak ada | 190 |
| Skenario | 190 |
| Penyebab | 190 |
| Solusi | 190 |

| | |
|---|------|
| Kesalahan: Akses Ditolak Pengecualian | 191 |
| Skenario | 191 |
| Penyebab | 191 |
| Solusi | 191 |
| Kesalahan: Pengecualian Sumber Daya Tidak Diketahui | 193 |
| Skenario | 193 |
| Penyebab | 193 |
| Solusi | 194 |
| Kesalahan: Berbagi di luar organisasi tidak diizinkan | 194 |
| Skenario | 194 |
| Kemungkinan penyebab dan solusi | 195 |
| Kesalahan: Tidak dapat melihat sumber daya bersama | 196 |
| Skenario | 196 |
| Kemungkinan penyebab dan solusi | 196 |
| Kesalahan: Batasi Pengecualian Terlampaui | 198 |
| Skenario | 198 |
| Penyebab | 198 |
| Solusi | 198 |
| Tidak ada undangan yang diterima | 199 |
| Skenario | 199 |
| Penyebab | 199 |
| Tidak dapat berbagi VPC | 199 |
| Skenario | 199 |
| Penyebab | 199 |
| Kuota layanan | 201 |
| Menggunakan AWS SDKs | 204 |
| Riwayat dokumen | 205 |
| | CCXV |

Apakah AWS Resource Access Manager itu?

AWS Resource Access Manager(AWS RAM) membantu Anda membagikan sumber daya dengan aman di seluruh Akun AWS, dalam organisasi atau unit organisasi (OU), dan dengan peran dan pengguna AWS Identity and Access Management (IAM) untuk jenis sumber daya yang didukung. Jika Anda memiliki beberapa Akun AWS, Anda dapat membuat sumber daya sekali dan gunakan AWS RAM untuk membuat sumber daya itu dapat digunakan oleh akun lain tersebut. Jika akun Anda dikelola oleh AWS Organizations, Anda dapat berbagi sumber daya dengan semua akun lain di organisasi atau hanya akun yang terkandung oleh satu atau lebih unit organisasi tertentu (oU). Anda juga dapat berbagi dengan ID akun tertentu Akun AWS, terlepas dari apakah akun tersebut merupakan bagian dari organisasi. [Beberapa jenis sumber daya yang didukung](#) juga memungkinkan Anda membagikannya dengan peran dan pengguna IAM tertentu.

Daftar Isi

- [Ikhtisar video](#)
- [Manfaat dari AWS RAM](#)
- [Cara kerja berbagi sumber daya](#)
- [Mengakses AWS RAM](#)
- [Harga untuk AWS RAM](#)
- [Kepatuhan dan standar internasional](#)

Ikhtisar video

Video berikut memberikan pengantar singkat AWS RAM dan menjelaskan cara membuat pembagian sumber daya. Untuk informasi selengkapnya, lihat [???](#).

Video berikut menunjukkan cara menerapkan izin AWS terkelola ke AWS sumber daya Anda. Untuk informasi selengkapnya, lihat [???](#).

Video ini menunjukkan cara menulis dan mengasosiasikan izin terkelola pelanggan mengikuti praktik terbaik dengan hak istimewa yang paling tidak. Untuk informasi lebih lanjut, lihat [???](#).

Manfaat dari AWS RAM

Mengapa menggunakan AWS RAM? Ini menawarkan manfaat berikut:

- Mengurangi biaya operasional Anda — Buat sumber daya satu kali, lalu gunakan AWS RAM untuk membagikan sumber daya tersebut dengan akun lain. Ini menghilangkan kebutuhan untuk menyediakan sumber daya duplikat di setiap akun, yang mengurangi overhead operasional. Dalam akun yang memiliki sumber daya, AWS RAM menyederhanakan pemberian akses ke setiap peran dan pengguna di akun tersebut tanpa harus menggunakan kebijakan izin berbasis identitas.
- Memberikan keamanan dan konsistensi — Sederhanakan manajemen keamanan untuk sumber daya bersama Anda dengan menggunakan satu set kebijakan dan izin. Jika Anda ingin membuat sumber daya duplikat di semua akun terpisah, Anda akan memiliki tugas untuk menerapkan kebijakan dan izin yang identik, dan kemudian harus menjaganya tetap identik di semua akun tersebut. Sebaliknya, semua pengguna berbagi AWS RAM sumber daya dikelola oleh satu set kebijakan dan izin. AWS RAM menawarkan pengalaman konsisten untuk berbagi berbagai jenis AWS sumber daya.
- Menyediakan visibilitas dan kemampuan audit — Lihat detail penggunaan untuk sumber daya bersama Anda melalui integrasi AWS RAM dengan Amazon CloudWatch dan AWS CloudTrail. AWS RAM memberikan visibilitas komprehensif ke sumber daya dan akun bersama.

Bagaimana dengan akses lintas akun dengan kebijakan berbasis sumber daya?

Anda dapat membagikan beberapa jenis AWS sumber daya dengan yang lain Akun AWS dengan melampirkan [kebijakan berbasis sumber daya](#) yang mengidentifikasi prinsipal AWS Identity and Access Management (IAM) (peran IAM dan pengguna) di luar Akun AWS. Namun, berbagi sumber daya dengan melampirkan kebijakan tidak memanfaatkan manfaat tambahan yang AWS RAM diberikan. Dengan menggunakan AWS RAM Anda mendapatkan fitur-fitur berikut:

- Anda dapat berbagi dengan [organisasi atau unit organisasi \(OU\)](#) tanpa harus menghitung setiap Akun AWS ID.
- Pengguna dapat melihat sumber daya yang dibagikan langsung dengan mereka di Layanan AWS konsol asal dan operasi API seolah-olah sumber daya tersebut langsung ada di akun pengguna. Misalnya, jika Anda menggunakan AWS RAM subnet Amazon VPC dengan akun lain, pengguna di akun tersebut dapat melihat subnet di konsol Amazon VPC dan dalam hasil operasi Amazon VPC API yang dilakukan di akun tersebut. Sumber daya yang dibagikan dengan melampirkan kebijakan

berbasis sumber daya tidak terlihat seperti ini; sebagai gantinya, Anda harus menemukan dan secara eksplisit merujuk ke sumber daya dengan Amazon Resource Name (ARN).

- Pemilik sumber daya dapat melihat prinsipal mana yang memiliki akses ke setiap sumber daya individu yang telah mereka bagikan.
- Jika Anda berbagi sumber daya dengan akun yang bukan bagian dari organisasi AWS RAM, maka lakukan proses undangan. Penerima harus menerima undangan sebelum kepala sekolah tersebut dapat mengakses sumber daya bersama. [Setelah mengaktifkan kemampuan untuk berbagi dalam organisasi](#), berbagi dengan akun di organisasi tidak memerlukan undangan.

Jika Anda memiliki sumber daya yang telah Anda bagikan menggunakan kebijakan izin berbasis sumber daya, Anda dapat mempromosikan sumber daya tersebut ke sumber daya yang AWS RAM dikelola sepenuhnya dengan melakukan salah satu hal berikut:

- Gunakan Operasi API [PromoteResourceShareCreatedFromPolicy](#).
- Gunakan setara operasi API, yang merupakan [promote-resource-share-created-from-policy](#) perintah AWS Command Line Interface (AWS CLI).

Cara kerja berbagi sumber daya

Ketika Anda berbagi sumber daya di akun kepemilikan dengan yang lain Akun AWS, akun konsumsi, Anda memberikan akses kepada prinsipal dalam akun konsumsi ke sumber daya bersama.

Kebijakan dan izin apa pun yang berlaku untuk peran dan pengguna di akun konsumsi juga berlaku untuk sumber daya bersama. Sumber daya dalam berbagi terlihat seperti sumber daya asli yang Akun AWS Anda bagikan.


Anda dapat berbagi sumber daya global dan Regional. Untuk informasi selengkapnya, lihat [Berbagi sumber daya Regional dibandingkan dengan sumber daya global](#).

Berbagi sumber daya Anda

Dengan, AWS RAM Anda dapat berbagi sumber daya yang Anda miliki dengan membuat [berbagi sumber daya](#). Untuk membuat pembagian sumber daya, Anda menentukan hal berikut:

- Wilayah AWS Di mana Anda ingin membuat pembagian sumber daya. Di konsol, Anda memilih dari menu dropdown Region di sudut kanan atas konsol. Dalam AWS CLI, Anda menggunakan `--region` parameter.

- Pembagian sumber daya hanya dapat berisi sumber daya Regional yang Wilayah AWS sama dengan pangsa sumber daya.
- Pembagian sumber daya dapat berisi sumber daya global hanya jika pangsa sumber daya berada di Wilayah asal yang ditunjuk untuk sumber daya global, AS Timur (Virginia Utara), us-east-1.
- Nama untuk pembagian sumber daya.
- Daftar sumber daya yang ingin Anda berikan akses sebagai bagian dari pembagian sumber daya ini.
- Prinsipal tempat Anda memberikan akses ke pembagian sumber daya. Kepala sekolah dapat individu Akun AWS, akun dalam organisasi atau unit organisasi (OU) di AWS Organizations, atau individu AWS Identity and Access Management (IAM) peran atau pengguna.

 Note

Tidak semua jenis sumber daya dapat dibagikan dengan peran dan pengguna. Untuk informasi tentang sumber daya yang dapat Anda bagikan dengan prinsipal ini, lihat [Sumber daya yang dapat dibagikan AWS](#).

- [Izin terkelola](#) untuk dikaitkan dengan setiap jenis sumber daya yang Anda sertakan dalam pembagian sumber daya. Izin yang dikelola menentukan apa yang dapat dilakukan prinsipal di akun lain dengan sumber daya dalam pembagian sumber daya.

Perilaku izin tergantung jenis:

- Jika prinsipal berada di akun yang berbeda dari akun yang memiliki sumber daya, maka izin yang dilampirkan pada pangsa sumber daya adalah izin maksimum yang tersedia untuk diberikan kepada peran dan pengguna di akun tersebut. Administrator akun tersebut kemudian harus memberikan peran individu dan pengguna akses ke sumber daya bersama dengan kebijakan berbasis identitas IAM. Izin yang diberikan dalam kebijakan tersebut tidak dapat melebihi yang ditentukan dalam izin yang dilampirkan pada pembagian sumber daya.

Akun kepemilikan sumber daya mempertahankan kepemilikan penuh atas sumber daya yang dibagikannya.

Menggunakan sumber daya bersama

Ketika pemilik sumber daya membagikannya dengan akun Anda, Anda dapat mengakses sumber daya bersama seperti yang Anda lakukan jika akun Anda memilikinya. Anda dapat mengakses sumber daya dengan menggunakan konsol, AWS CLI perintah, dan operasi API layanan yang relevan. Operasi API yang diizinkan dilakukan oleh prinsipal di akun Anda bervariasi tergantung pada jenis sumber daya dan ditentukan oleh AWS RAM izin yang dilampirkan ke pembagian sumber daya. Semua kebijakan IAM dan kebijakan kontrol layanan yang dikonfigurasi di akun Anda juga terus berlaku, yang memungkinkan Anda memanfaatkan investasi yang ada dalam kontrol keamanan dan tata kelola.

Saat mengakses sumber daya bersama menggunakan layanan sumber daya tersebut, Anda memiliki kemampuan dan batasan yang sama dengan sumber daya Akun AWS yang dimiliki.

- Jika sumber daya Regional, maka Anda dapat mengaksesnya dari hanya Wilayah AWS di mana ia ada di akun kepemilikan.
- Jika sumber daya bersifat global, maka Anda dapat mengaksesnya dari apa pun Wilayah AWS yang didukung oleh konsol layanan dan alat sumber daya. Anda dapat melihat dan mengelola pangsa sumber daya dan sumber daya globalnya di AWS RAM konsol dan alat hanya di Wilayah rumah yang ditunjuk, AS Timur (Virginia N.), us-east-1.

Mengakses AWS RAM

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

Konsol AWS RAM

AWS RAM menyediakan antarmuka pengguna berbasis web, AWS RAM konsol. Jika Anda telah mendaftar untuk Akun AWS, Anda dapat mengakses AWS RAM konsol dengan masuk ke [AWS Management Console](#) dan memilih AWS RAM dari halaman beranda konsol.

Anda juga dapat menavigasi di browser Anda langsung ke [AWS RAM konsol](#). Jika Anda belum masuk, maka Anda diminta untuk melakukannya sebelum konsol muncul.

AWS CLI dan Alat untuk Windows PowerShell

The AWS CLI dan AWS Tools for PowerShell menyediakan akses langsung ke operasi API AWS RAM publik. AWS mendukung alat-alat ini pada Windows, macOS, dan Linux. [Untuk informasi lebih lanjut tentang memulai, atau Panduan AWS Tools for Windows PowerShell Pengguna. AWS](#)

[Command Line Interface](#) Untuk informasi lebih lanjut tentang perintah AWS RAM, lihat [Referensi AWS CLI Perintah](#) atau [Referensi AWS Tools for Windows PowerShell Cmdlet](#).

AWS SDK

AWS menyediakan perintah API untuk serangkaian bahasa pemrograman yang luas. Untuk informasi lebih lanjut tentang memulai, lihat [Panduan Referensi AWS SDK dan Alat](#).

API Kueri

Jika Anda tidak menggunakan salah satu bahasa pemrograman yang didukung, maka AWS RAM HTTPS Query API memberi Anda akses terprogram ke AWS RAM dan AWS. Dengan AWS RAM API, Anda dapat mengeluarkan permintaan HTTPS langsung ke layanan. Saat Anda menggunakan AWS RAM API, Anda harus menyertakan kode untuk menandatangani permintaan secara digital menggunakan kredensial Anda. Untuk informasi lebih lanjut, lihat [Referensi API AWS RAM](#).

Harga untuk AWS RAM

Tidak ada biaya tambahan untuk menggunakan AWS RAM atau untuk membuat berbagi sumber daya dan berbagi sumber daya Anda di seluruh akun. Biaya penggunaan sumber daya bervariasi tergantung pada jenis sumber daya. Untuk informasi lebih lanjut tentang cara AWS menagih, lihat dokumentasi untuk layanan memiliki sumber daya.

Kepatuhan dan standar internasional

PCI DSS

AWS RAM mendukung pemrosesan, penyimpanan, dan transmisi data kartu kredit oleh merchant atau penyedia layanan, dan telah divalidasi sebagai sesuai dengan Standar Keamanan Data (DSS) Industri Kartu Pembayaran (PCI).

Untuk informasi lebih lanjut tentang PCI DSS, termasuk cara meminta salinan AWS PCI Compliance Package, lihat [PCI DSS Level 1](#).

FedRAMP

AWS RAM diberi wewenang sebagai FedRAMP Moderate Wilayah AWS: US East (N. Virginia), US East (Ohio), US West (Oregon), dan US West (Oregon), dan US West (Oregon), US West (Oregon), dan US West (Oregon), dan US West (Oregon), dan US West (Oregon), dan US West (Oregon).

AWS RAM diberi wewenang sebagai FedRAMP High sebagai berikut Wilayah AWS: AWS GovCloud (AS-Barat) dan AWS GovCloud (AS-timur).

Program Manajemen Risiko dan Otorisasi Federal (FedRAMP) adalah program di seluruh pemerintah AS yang memberikan pendekatan standar untuk penilaian keamanan, otorisasi, dan pemantauan berkelanjutan untuk produk dan layanan cloud.

Untuk informasi lebih lanjut tentang kepatuhan FedRAMP, lihat [FedRAMP](#).

SOC dan ISO

AWS RAM dapat digunakan untuk beban kerja yang tunduk pada kepatuhan Service Organization Control (SOC) dan Standar Organisasi Internasional untuk Standardisasi (ISO) ISO 9001, ISO 27001, ISO 27017, ISO 27018, dan ISO 27701. Pelanggan di bidang keuangan, perawatan kesehatan, dan sektor teregulasi lainnya dapat memperoleh wawasan tentang proses dan kontrol keamanan yang melindungi data pelanggan yang dapat ditemukan dalam laporan SOC, serta sertifikat AWS ISO dan CSA STAR di [AWS Artifact](#).

Untuk informasi lebih lanjut tentang kepatuhan SOC, lihat [SOC](#).

Untuk informasi selengkapnya tentang kepatuhan ISO, lihat [ISO 9001](#), [ISO 27001](#), [ISO 27017](#), [ISO 27018](#), dan [ISO 27701](#).

Memulai dengan AWS RAM

dengan AWS Resource Access Manager, Anda dapat berbagi sumber daya dengan individu lain Akun AWS. Jika akun Anda dikelola oleh AWS Organizations, Anda juga dapat berbagi sumber daya dengan akun lain di organisasi Anda. Anda juga dapat menggunakan sumber daya yang dibagikan dengan Anda oleh orang lain Akun AWS.

Jika Anda tidak mengaktifkan berbagi di dalam AWS Organizations, Anda tidak dapat berbagi sumber daya dengan organisasi Anda atau dengan unit organisasi (OU) di organisasi Anda. Namun, Anda masih dapat berbagi sumber daya dengan individu Akun AWS di organisasi Anda. Untuk [jenis sumber daya yang didukung](#), Anda juga dapat berbagi sumber daya dengan individu AWS Identity and Access Management (IAM) peran atau pengguna di organisasi Anda. Dalam hal ini, prinsipal ini diperlakukan seolah-olah mereka adalah akun eksternal, bukan sebagai bagian dari organisasi Anda. Mereka menerima undangan untuk bergabung dengan pembagian sumber daya dan mereka harus menerima undangan untuk bergabung dengan pembagian sumber daya dan mereka harus menerima undangan untuk bergabung dengan pembagian sumber daya dan mereka harus menerima undangan untuk bergabung dengan pembagian sumber daya dan mereka harus menerima undangan

Konten

- [Syarat dan konsep untuk AWS RAM](#)
- [Berbagi AWS sumber daya Anda](#)
- [Menggunakan AWS sumber daya bersama](#)

Syarat dan konsep untuk AWS RAM

Konsep-konsep berikut membantu menjelaskan bagaimana Anda dapat menggunakan AWS Resource Access Manager (AWS RAM) untuk berbagi sumber daya Anda.

Berbagi sumber daya

Anda berbagi sumber daya menggunakan AWS RAM dengan membuat berbagi sumber daya. Pembagian sumber daya memiliki tiga elemen berikut:

- Daftar satu atau lebih AWS sumber daya untuk dibagikan.
- Daftar satu atau lebih [utama](#) kepada siapa akses ke sumber daya diberikan.

- SEBUAH [izin terkelola](#) untuk setiap jenis sumber daya yang Anda sertakan di bagian. Setiap izin terkelola berlaku untuk semua sumber daya jenis itu dalam pembagian sumber daya tersebut.

Setelah Anda menggunakan AWS RAM untuk membuat pembagian sumber daya, prinsipal yang ditentukan dalam pembagian sumber daya dapat diberikan akses ke sumber daya berbagi.

- Jika Anda menghidupkan AWS RAM berbagi dengan AWS Organizations, dan prinsipal Anda yang Anda bagikan berada di organisasi yang sama dengan akun berbagi, prinsipal tersebut dapat menerima akses segera setelah administrator akun mereka memberi mereka izin untuk menggunakan sumber daya menggunakan AWS Identity and Access Management (IAM) kebijakan izin.
- Jika Anda tidak menghidupkan AWS RAM berbagi dengan Organizations, Anda masih dapat berbagi sumber daya dengan individu Akun AWS yang ada di organisasi Anda. Administrator di akun konsumsi menerima undangan untuk bergabung dengan pembagian sumber daya, dan mereka harus menerima undangan sebelum kepala sekolah yang ditentukan dalam pembagian sumber daya dapat mengakses sumber daya bersama.
- Anda juga dapat berbagi dengan akun di luar organisasi Anda, jika jenis sumber daya mendukungnya. Administrator di akun konsumsi menerima undangan untuk bergabung dengan pembagian sumber daya, dan mereka harus menerima undangan sebelum kepala sekolah yang ditentukan dalam pembagian sumber daya dapat mengakses sumber daya bersama. Untuk informasi tentang jenis sumber daya yang mendukung jenis berbagi ini, lihat [Sumber daya yang dapat dibagikan AWS](#) dan melihat [Dapat berbagi dengan akun di luar organisasinya](#) kolom.

Berbagi akun

The berbagi akun berisi sumber daya yang dibagikan dan di mana AWS RAM administrator membuat AWS berbagi sumber daya dengan menggunakan AWS RAM.

Sebuah AWS RAM administrator adalah prinsipal IAM yang memiliki izin untuk membuat dan mengonfigurasi pembagian sumber daya di Akun AWS. Karena AWS RAM bekerja dengan melampirkan kebijakan berbasis sumber daya ke sumber daya dalam pembagian sumber, AWS RAM administrator juga harus memiliki izin untuk memanggil `PutResourcePolicy` operasi di Layanan AWS untuk setiap jenis sumber daya yang termasuk dalam sumber daya.

Mengonsumsi prinsipal

The akun konsumsi adalah akun AWS yang mana sumber daya dibagikan. Pembagian sumber daya dapat menentukan seluruh akun sebagai prinsipal, atau untuk beberapa jenis sumber daya, peran individu, atau pengguna dalam akun. Untuk informasi tentang jenis sumber daya yang mendukung jenis berbagi ini, lihat [Sumber daya yang dapat dibagikan AWS](#) dan melihat [Dapat berbagi dengan peran & pengguna IAM](#) kolom.

AWS RAM juga mendukung prinsip layanan sebagai konsumen pembagian sumber daya. Untuk informasi tentang jenis sumber daya yang mendukung jenis berbagi ini, lihat [Sumber daya yang dapat dibagikan AWS](#) dan melihat [Dapat berbagi dengan kepala sekolah layanan](#) kolom.

Prinsipal dalam akun konsumsi hanya dapat melakukan tindakan yang diizinkan oleh kedua-duanya dari izin berikut:

- Izin terkelola yang dilampirkan ke pembagian sumber daya. Ini menentukan maksimum perizinan yang dapat diberikan ke kepala sekolah di akun konsumsi.
- Kebijakan berbasis identitas IAM yang dilampirkan pada peran individu atau pengguna oleh administrator IAM di akun konsumsi. Kebijakan tersebut harus memberikan `Allow` akses ke tindakan tertentu dan ke [Amazon Resource Name \(ARN\) Amazon](#) sumber daya di akun berbagi.

AWS RAM mendukung tipe utama IAM berikut sebagai konsumen pembagian sumber daya:

- Lain Akun AWS— Pembagian sumber daya membuat sumber daya yang disertakan dalam akun berbagi tersedia untuk akun konsumsi.
- Peran IAM individu atau pengguna di akun lain— Beberapa jenis sumber daya mendukung berbagi langsung dengan peran IAM individu atau pengguna. Tentukan jenis utama ini dengan ARN.
 - Peran IAM—`arn:aws:iam::123456789012:role/rolename`
 - Pengguna IAM—`arn:aws:iam::123456789012:user/username`
- Prinsipal layanan— Bagikan sumber daya dengan AWS layanan untuk memberikan akses layanan ke pembagian sumber daya. Pembagian utama layanan memungkinkan AWS layanan untuk mengambil tindakan atas nama Anda untuk meringankan beban operasional.

Untuk berbagi dengan kepala layanan, pilih untuk mengizinkan berbagi dengan siapa pun, dan kemudian, di bawah Pilih jenis utama, pilih Prinsipal layanan dari daftar dropdown. Tentukan nama kepala layanan dalam format berikut:

- `service-id.amazonaws.com`

Untuk mengurangi risiko wakil yang bingung, kebijakan sumber daya menunjukkan ID akun pemilik sumber daya diaws : SourceAccountkunci kondisi.

- Akun dalam suatu organisasi— Jika akun berbagi dikelola olehAWS Organizations, maka pembagian sumber daya dapat menentukan ID organisasi untuk dibagikan dengan semua akun di organisasi. Pembagian sumber daya dapat menentukan ID unit organisasi (OU) untuk dibagikan dengan semua akun di OU tersebut. Akun berbagi hanya dapat dibagikan dengan organisasinya sendiri atau ID OU dalam organisasinya sendiri. Tentukan akun dalam suatu organisasi oleh ARN organisasi atau OU.
- Semua akun dalam suatu organisasiBerikut ini adalah contoh ARN dari sebuah organisasi diAWS Organizations:

```
arn:aws:organizations::123456789012:organization/o-<orgid>
```

- Semua akun di unit organisasi— Berikut ini adalah contoh ARN dari ID OU:

```
arn:aws:organizations::123456789012:organization/o-<orgid>/ou-<rootid>-<ouid>
```

Important

Ketika Anda berbagi dengan organisasi atau OU, dan cakupan itu mencakup akun yang memiliki pembagian sumber daya, semua kepala sekolah di akun berbagi secara otomatis mendapatkan akses ke sumber daya dalam pembagian. Akses yang diberikan ditentukan oleh izin terkelola yang terkait dengan pembagian. Hal ini dikarenakan kebijakan sumber daya yangAWS RAMmelekat pada setiap sumber daya dalam penggunaan berbagi"Principal": "*". Untuk informasi selengkapnya, lihat [Implikasi penggunaan"Principal": "*"dalam kebijakan berbasis sumber daya](#).

Prinsipal di akun konsumsi lainnya tidak segera mendapatkan akses ke sumber daya saham. Administrator akun lain harus terlebih dahulu melampirkan kebijakan izin berbasis identitas ke kepala sekolah yang sesuai. Kebijakan tersebut harus memberikanAllowakses ke ARN sumber daya individu dalam pembagian sumber daya. Izin dalam kebijakan tersebut tidak dapat melebihi yang ditentukan dalam izin terkelola yang terkait dengan pembagian sumber daya.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen teks yang menerapkan bahasa kebijakan IAM. Tidak seperti kebijakan berbasis identitas yang Anda lampirkan ke prinsipal, seperti peran IAM atau pengguna, Anda lampirkan kebijakan berbasis sumber daya ke sumber daya. AWS RAM kebijakan berbasis sumber daya penulis atas nama Anda berdasarkan informasi yang Anda berikan untuk pembagian sumber daya Anda. Anda harus menentukan **Principalelemen** kebijakan yang menentukan siapa yang dapat mengakses sumber daya. Untuk informasi selengkapnya, lihat [Kebijakan berbasis identitas dan kebijakan berbasis sumber daya](#) di Panduan Pengguna IAM.

Kebijakan berbasis sumber daya yang dihasilkan oleh AWS RAM dievaluasi bersama dengan semua jenis kebijakan IAM lainnya. Ini termasuk kebijakan berbasis identitas IAM yang dilampirkan pada prinsipal yang mencoba mengakses sumber daya, dan kebijakan kontrol layanan (SCP) untuk AWS Organizations yang mungkin berlaku untuk Akun AWS. Kebijakan berbasis sumber daya yang dihasilkan oleh AWS RAM berpartisipasi dalam logika evaluasi kebijakan yang sama seperti semua kebijakan IAM lainnya. Untuk detail lengkap evaluasi kebijakan dan cara menentukan izin yang dihasilkan, lihat [Logika evaluasi kebijakan](#) di Panduan Pengguna IAM.

AWS RAM memberikan pengalaman berbagi sumber daya yang sederhana dan aman dengan menyediakan easy-to-use kebijakan berbasis sumber daya.

Untuk tipe sumber daya yang mendukung kebijakan berbasis sumber daya, AWS RAM secara otomatis membangun dan mengelola kebijakan berbasis sumber daya untuk Anda. Untuk sumber daya tertentu, AWS RAM membangun kebijakan berbasis sumber daya dengan menggabungkan informasi dari semua pembagian sumber daya yang mencakup sumber daya tersebut. Misalnya, pertimbangkan Amazon SageMaker pipeline yang Anda bagikan dengan menggunakan AWS RAM dan termasuk dalam dua pembagian sumber daya yang berbeda. Anda dapat menggunakan satu pembagian sumber daya untuk menyediakan akses hanya-baca ke seluruh organisasi Anda. Anda kemudian dapat menggunakan pembagian sumber daya lainnya hanya untuk memberikan SageMaker izin eksekusi untuk satu akun. AWS RAM secara otomatis menggabungkan dua set izin yang berbeda ke dalam kebijakan sumber daya tunggal dengan beberapa pernyataan. Ini kemudian melampirkan kebijakan berbasis sumber daya ke sumber daya pipa. Anda dapat melihat kebijakan sumber daya dasar ini dengan memanggil [GetResourcePolicy](#) operasi. Layanan AWS kemudian gunakan kebijakan berbasis sumber daya tersebut untuk memberi wewenang kepada prinsipal mana pun yang mencoba melakukan tindakan pada sumber daya bersama.

Meskipun Anda dapat membuat kebijakan berbasis sumber daya secara manual dan melampirkannya ke sumber daya Anda dengan menelepon `PutResourcePolicy`, kami sarankan Anda menggunakan AWS RAM karena memberikan keuntungan sebagai berikut:

- Dapat ditemukan untuk konsumen saham— Jika Anda berbagi sumber daya dengan menggunakan AWS RAM, pengguna dapat melihat semua sumber daya yang dibagikan dengan mereka secara langsung di konsol layanan yang memiliki sumber daya dan operasi API seolah-olah sumber daya tersebut langsung ada di akun pengguna. Misalnya, jika Anda berbagi AWS CodeBuild proyek dengan akun lain, pengguna di akun konsumsi dapat melihat proyek di CodeBuild konsol dan dalam hasil CodeBuild Operasi API dilakukan. Sumber daya yang dibagikan dengan langsung ke kebijakan berbasis sumber daya tidak terlihat seperti ini. Sebaliknya, Anda harus menemukan dan secara eksplisit merujuk ke sumber daya oleh ARN-nya.
- Pengelolaan untuk pemilik saham— Jika Anda berbagi sumber daya dengan menggunakan AWS RAM, pemilik sumber daya di akun berbagi dapat secara terpusat melihat akun lain mana yang memiliki akses ke sumber daya mereka. Jika Anda berbagi sumber daya menggunakan kebijakan berbasis sumber daya, Anda dapat melihat akun pengguna hanya dengan memeriksa kebijakan untuk sumber daya individual di konsol layanan atau API yang relevan.
- Efisiensi— Jika Anda berbagi sumber daya dengan menggunakan AWS RAM, Anda dapat berbagi banyak sumber daya dan mengelolanya sebagai satu unit. Sumber daya yang dibagikan hanya dengan menggunakan kebijakan berbasis sumber daya memerlukan kebijakan individual yang dilampirkan ke setiap sumber daya yang Anda bagikan.
- Kesederhanaan— Dengan AWS RAM, Anda tidak perlu memahami bahasa kebijakan IAM berbasis JSON. AWS RAM memberi ready-to-use AWS izin terkelola yang dapat Anda pilih untuk dilampirkan ke pembagian sumber daya Anda.

Dengan menggunakan AWS RAM, Anda bahkan dapat membagikan beberapa jenis sumber daya yang belum mendukung kebijakan berbasis sumber daya. Untuk jenis sumber daya seperti itu, AWS RAM secara otomatis menghasilkan kebijakan berbasis sumber daya sebagai representasi dari izin aktual. Pengguna dapat melihat representasi ini dengan memanggil [GetResourcePolicy](#). Ini termasuk jenis sumber daya berikut:

- Amazon Aurora - kluster DB
- Amazon EC2 — reservasi kapasitas dan host khusus
- AWS License Manager- Konfigurasi lisensi
- AWS Outposts— Tabel rute gateway lokal, pos terdepan, dan situs

- Amazon Route 53 - Aturan penerusan
- Amazon Virtual Private Cloud — Alamat IPv4 milik pelanggan, daftar awalan, subnet, target cermin lalu lintas, gateway transit, dan domain multicast gateway transit

Contoh dari AWS RAM kebijakan berbasis sumber daya yang dihasilkan

Jika Anda berbagi sumber daya gambar EC2 Image Builder dengan seorang individu akun, AWS RAM menghasilkan kebijakan yang terlihat seperti contoh berikut dan melampirkannya ke sumber daya gambar apa pun yang disertakan dalam pembagian sumber daya.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:root"},
      "Action": [
        "imagebuilder:GetImage",
        "imagebuilder:ListImages",
      ],
      "Resource": "arn:aws:imagebuilder:us-east-1:123456789012:image/testimage/1.0.0/44"
    }
  ]
}
```

Jika Anda berbagi sumber daya gambar EC2 Image Builder dengan Peran IAM atau pengguna dalam yang berbeda Akun AWS, AWS RAM menghasilkan kebijakan yang terlihat seperti contoh berikut dan melampirkannya ke sumber daya gambar apa pun yang disertakan dalam pembagian sumber daya.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/MySampleRole"
      },
      "Action": [
        "imagebuilder:GetImage",
      ]
    }
  ]
}
```

```

        "imagebuilder:ListImages",
    ],
    "Resource": "arn:aws:imagebuilder:us-east-1:123456789012:image/
testimage/1.0.0/44"
    }
]
}

```

Jika Anda berbagi sumber daya gambar EC2 Image Builder dengan semua akun di organisasi atau dengan akun OU, AWS RAM menghasilkan kebijakan yang terlihat seperti contoh berikut dan melampirkannya ke sumber daya gambar apa pun yang disertakan dalam pembagian sumber daya.

Note

Kebijakan ini menggunakan "Principal": "*" dan kemudian menggunakan "Condition" elemen untuk membatasi izin ke identitas yang cocok dengan yang ditentukan PrincipalOrgID. Untuk informasi selengkapnya, lihat [Implikasi penggunaan "Principal": "*" dalam kebijakan berbasis sumber daya](#).

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "imagebuilder:GetImage",
        "imagebuilder:ListImages",
      ],
      "Resource": "arn:aws:imagebuilder:us-east-1:123456789012:image/
testimage/1.0.0/44"
      "Condition": {
        "StringEquals": {
          "aws:PrincipalOrgID": "o-123456789"
        }
      }
    }
  ]
}

```

Implikasi penggunaan "Principal": "*" dalam kebijakan berbasis sumber daya

Saat Anda memasukkan "Principal": "*" dalam kebijakan berbasis sumber daya, kebijakan memberikan akses ke semua prinsipal IAM di akun yang berisi sumber daya, tunduk pada batasan apa pun yang diberlakukan oleh `Condition` elemen, jika ada. Eksplisit `Deny` pernyataan dalam kebijakan apa pun yang berlaku untuk prinsipal panggilan mengesampingkan izin yang diberikan oleh kebijakan ini. Namun, sebuah implisit `Deny` (yang berarti kurangnya eksplisit `Allow`) dalam setiap kebijakan identitas yang berlaku, kebijakan batas izin, atau kebijakan sesitidak menghasilkan `Deny` kepada kepala sekolah yang diberikan akses ke suatu tindakan oleh kebijakan berbasis sumber daya tersebut.

Jika perilaku ini tidak diinginkan untuk skenario Anda, maka Anda dapat membatasi perilaku ini dengan menambahkan eksplisit `Deny` pernyataan terhadap kebijakan identitas, batas izin, atau kebijakan sesi yang memengaruhi peran dan pengguna yang relevan.

Izin terkelola

Izin terkelola menentukan tindakan apa yang dapat dilakukan oleh prinsipal dalam kondisi apa pada jenis sumber daya yang didukung dalam pembagian sumber daya. Saat membuat pembagian sumber daya, Anda harus menentukan izin terkelola mana yang akan digunakan untuk setiap jenis sumber daya yang disertakan dalam pembagian sumber daya. Izin terkelola mencantumkan kumpulan `actions` dan kondisi bahwa kepala sekolah dapat melakukan dengan sumber daya yang dibagikan menggunakan AWS RAM.

Anda hanya dapat melampirkan satu perizinan untuk setiap jenis sumber daya dalam pembagian sumber. Anda tidak dapat membuat pembagian sumber daya di mana beberapa sumber daya dari jenis tertentu menggunakan satu izin terkelola dan sumber daya lain dari jenis yang sama menggunakan izin terkelola yang berbeda. Untuk melakukan itu, Anda perlu membuat dua pembagian sumber daya yang berbeda dan membagi sumber daya di antara mereka, memberikan setiap set izin terkelola yang berbeda. Ada dua jenis izin terkelola:

AWS izin terkelola

AWS izin terkelola dibuat dan dikelola oleh AWS dan memberikan izin untuk skenario pelanggan umum. AWS RAM mendefinisikan setidaknya satu AWS izin terkelola untuk setiap jenis sumber daya yang didukung. Beberapa jenis sumber daya mendukung lebih dari satu AWS izin terkelola, dengan satu izin terkelola yang ditetapkan sebagai AWS default. The [default AWS izin terkelola](#) dikaitkan kecuali Anda menentukan sebaliknya.

Izin yang dikelola pelanggan

Izin terkelola pelanggan adalah izin terkelola yang Anda buat dan pertahankan dengan menentukan secara tepat tindakan mana yang dapat dilakukan dalam kondisi mana dengan sumber daya yang dibagikan menggunakan AWS RAM. Misalnya, Anda ingin membatasi akses baca untuk kumpulan Amazon VPC IP Address Manager (IPAM), yang membantu Anda mengelola alamat IP Anda dalam skala besar. Anda dapat membuat izin terkelola pelanggan bagi pengembang Anda untuk menetapkan alamat IP, tetapi tidak melihat rentang alamat IP yang ditetapkan akun pengembang lain. Anda dapat mengikuti praktik terbaik dengan hak istimewa paling sedikit, hanya memberikan izin yang diperlukan untuk melakukan tugas pada sumber daya bersama.

Anda menentukan izin Anda sendiri untuk jenis sumber daya dalam berbagi sumber daya dengan opsi untuk menambahkan kondisi seperti [Kunci Konteks Global](#) dan [kunci khusus layanan](#) untuk menentukan kondisi di mana kepala sekolah memiliki akses ke sumber daya. Izin ini dapat digunakan dalam satu atau lebih AWS RAMsaham. Izin yang dikelola pelanggan adalah wilayah tertentu.

AWS RAM mengambil izin terkelola sebagai masukan untuk membuat [kebijakan berbasis sumber daya](#) untuk sumber daya yang Anda bagikan.

Versi izin terkelola

Setiap perubahan pada izin terkelola direpresentasikan sebagai versi baru dari izin terkelola tersebut. Versi baru adalah default untuk semua pembagian sumber daya baru. Setiap izin terkelola selalu memiliki satu versi yang ditetapkan sebagai versi default. Ketika Anda atau AWS membuat versi izin terkelola baru, Anda harus secara eksplisit memperbarui izin terkelola untuk setiap pembagian sumber daya yang ada. Anda dapat mengevaluasi perubahan sebelum menerapkannya ke bagian sumber daya Anda di langkah ini. Semua pembagian sumber daya baru akan secara otomatis menggunakan versi baru dari izin terkelola untuk jenis sumber daya yang sesuai.

AWS versi izin terkelola

AWS menangani semua perubahan AWS izin terkelola. Perubahan tersebut mengatasi fungsionalitas baru atau menghapus kekurangan yang ditemukan. Anda hanya dapat menerapkan versi izin terkelola default ke pembagian sumber daya Anda.

Versi izin yang dikelola pelanggan

Anda menangani semua perubahan pada izin terkelola pelanggan. Anda dapat membuat versi default baru, menetapkan versi yang lebih lama sebagai default, atau menghapus versi yang tidak lagi terkait dengan pembagian sumber daya apa pun. Setiap perizinan yang dikelola pelanggan dapat memiliki hingga lima versi.

Saat membuat atau memperbarui pembagian sumber daya, Anda hanya dapat melampirkan versi default dari izin terkelola yang ditentukan. Untuk informasi selengkapnya, lihat [Memperbarui izin AWS terkelola ke versi yang lebih baru](#).

Berbagi AWS sumber daya Anda

Untuk berbagi sumber daya yang Anda miliki dengan menggunakan AWS RAM, lakukan hal berikut:

- [Aktifkan berbagi sumber daya dalam AWS Organizations](#) (opsional)
- [Buat berbagi sumber daya](#)

Catatan

- Berbagi sumber daya dengan prinsipal di luar Akun AWS yang memiliki sumber daya tidak mengubah izin atau kuota yang berlaku untuk sumber daya dalam akun yang membuatnya.
- AWS RAM adalah layanan regional. Prinsipal yang Anda bagikan dapat mengakses pembagian sumber daya hanya Wilayah AWS di mana mereka dibuat.
- Beberapa sumber daya memiliki pertimbangan dan prasyarat khusus untuk berbagi. Untuk informasi selengkapnya, lihat [Sumber daya yang dapat dibagikan AWS](#).

Aktifkan berbagi sumber daya dalam AWS Organizations

Ketika akun Anda dikelola oleh AWS Organizations, Anda dapat memanfaatkannya untuk berbagi sumber daya dengan lebih mudah. Dengan atau tanpa Organizations, pengguna dapat berbagi dengan akun individu. Namun, jika akun Anda berada dalam suatu organisasi, maka Anda dapat berbagi dengan akun individual, atau dengan semua akun di organisasi atau di OU tanpa harus menghitung setiap akun.

Untuk berbagi sumber daya dalam organisasi, Anda harus terlebih dahulu menggunakan AWS RAM konsol atau AWS Command Line Interface (AWS CLI) untuk mengaktifkan berbagi dengan AWS Organizations. Ketika Anda berbagi sumber daya di organisasi Anda, AWS RAM tidak mengirim undangan ke kepala sekolah. Prinsipal di organisasi Anda mendapatkan akses ke sumber daya bersama tanpa bertukar undangan.

Saat Anda mengaktifkan berbagi sumber daya dalam organisasi Anda, AWS RAM buat peran terkait layanan yang disebut **AWSServiceRoleForResourceAccessManager**. Peran ini hanya dapat diasumsikan oleh AWS RAM layanan, dan memberikan AWS RAM izin untuk mengambil informasi tentang organisasi yang menjadi anggotanya, dengan menggunakan kebijakan yang AWS dikelola. `AWSResourceAccessManagerServiceRolePolicy`

Jika Anda tidak perlu lagi berbagi sumber daya dengan seluruh organisasi atau OU, Anda dapat menonaktifkan berbagi sumber daya. Untuk informasi selengkapnya, lihat [Menonaktifkan berbagi sumber daya dengan AWS Organizations](#).

Izin minimum

Untuk menjalankan prosedur di bawah ini, Anda harus masuk sebagai kepala sekolah di akun manajemen organisasi yang memiliki izin berikut:

- `ram:EnableSharingWithAwsOrganization`
- `iam:CreateServiceLinkedRole`
- `organizations:enableAWSServiceAccess`
- `organizations:DescribeOrganization`

Persyaratan

- Anda dapat melakukan langkah-langkah ini hanya saat masuk sebagai prinsipal di akun manajemen organisasi.
- Organisasi harus mengaktifkan semua fitur. Untuk informasi selengkapnya, lihat [Mengaktifkan semua fitur di organisasi Anda](#) di Panduan AWS Organizations Pengguna.

Important

Anda harus mengaktifkan berbagi AWS Organizations dengan menggunakan AWS RAM konsol atau AWS CLI perintah [enable-sharing-with-aws-organization](#). Ini memastikan bahwa peran `AWSServiceRoleForResourceAccessManager` terkait layanan dibuat.

Jika Anda mengaktifkan akses tepercaya AWS Organizations dengan menggunakan AWS Organizations konsol atau [enable-aws-service-access](#) AWS CLI perintah, peran `AWSServiceRoleForResourceAccessManager` terkait layanan tidak dibuat, dan Anda tidak dapat berbagi sumber daya dalam organisasi Anda.

Console

Untuk mengaktifkan berbagi sumber daya dalam organisasi Anda

1. Buka halaman [Pengaturan](#) di AWS RAM konsol.
2. Pilih Aktifkan berbagi dengan AWS Organizations, lalu pilih Simpan pengaturan.

AWS CLI

Untuk mengaktifkan berbagi sumber daya dalam organisasi Anda

Gunakan perintah [enable-sharing-with-aws-organization](#).

Perintah ini dapat digunakan di mana saja Wilayah AWS, dan memungkinkan berbagi dengan AWS Organizations di semua Wilayah yang AWS RAM didukung.

```
$ aws ram enable-sharing-with-aws-organization
{
  "returnValue": true
}
```

Buat berbagi sumber daya

Untuk berbagi sumber daya yang Anda miliki, buat pembagian sumber daya. Berikut adalah gambaran umum prosesnya:

1. Tambahkan sumber daya yang ingin Anda bagikan.
2. Untuk setiap jenis sumber daya yang Anda sertakan dalam share, tentukan [izin terkelola](#) yang akan digunakan untuk jenis sumber daya tersebut.
 - Anda dapat memilih dari salah satu izin AWS terkelola yang tersedia, izin terkelola pelanggan yang sudah ada, atau membuat izin terkelola pelanggan baru.
 - AWS izin terkelola dibuat oleh AWS untuk mencakup kasus penggunaan standar.

- Izin terkelola pelanggan memungkinkan Anda menyesuaikan izin terkelola Anda sendiri untuk memenuhi kebutuhan keamanan dan bisnis Anda.

Note

Jika izin terkelola yang dipilih memiliki beberapa versi, maka AWS RAM secara otomatis melampirkan versi default. Anda hanya dapat melampirkan versi yang ditetapkan sebagai default.

3. Tentukan prinsip yang ingin Anda akses ke sumber daya.

Pertimbangan-pertimbangan

- Jika nanti Anda perlu menghapus AWS sumber daya yang Anda sertakan dalam berbagi, sebaiknya Anda menghapus sumber daya dari pembagian sumber daya apa pun yang menyertakannya, atau menghapus pembagian sumber daya.
- Jenis sumber daya yang dapat Anda sertakan dalam pembagian sumber daya tercantum di [Sumber daya yang dapat dibagikan AWS](#).
- Anda dapat berbagi sumber daya hanya jika Anda [memilikinya](#). Anda tidak dapat berbagi sumber daya yang dibagikan dengan Anda.
- AWS RAM adalah layanan regional. Saat Anda berbagi sumber daya dengan prinsipal di tempat lain Akun AWS, prinsipal tersebut harus mengakses setiap sumber daya dari sumber daya yang sama Wilayah AWS dengan yang dibuat. Untuk sumber daya global yang didukung, Anda dapat mengakses sumber daya tersebut dari sumber daya apa pun Wilayah AWS yang didukung oleh konsol layanan dan alat sumber daya tersebut. Anda dapat melihat pembagian sumber daya tersebut dan sumber daya globalnya di AWS RAM konsol dan alat hanya di Wilayah asal yang ditunjuk, AS Timur (Virginia N.), us-east-1. Untuk informasi selengkapnya tentang AWS RAM dan sumber daya global, lihat [Berbagi sumber daya Regional dibandingkan dengan sumber daya global](#).
- Jika akun yang Anda bagikan adalah bagian dari organisasi AWS Organizations dan berbagi dalam organisasi Anda diaktifkan, semua prinsipal di organisasi yang Anda bagikan secara otomatis diberikan akses ke pembagian sumber daya tanpa menggunakan undangan. Seorang kepala sekolah di akun dengan siapa Anda berbagi di luar konteks organisasi menerima undangan untuk bergabung dengan pembagian sumber daya dan diberikan akses ke sumber daya bersama hanya setelah mereka menerima undangan.
- Jika Anda berbagi dengan kepala layanan, Anda tidak dapat mengaitkan prinsip lain dengan pembagian sumber daya.

- Jika berbagi antara akun atau kepala sekolah yang merupakan bagian dari organisasi, maka setiap perubahan keanggotaan organisasi secara dinamis memengaruhi akses ke pembagian sumber daya.
- Jika Anda menambahkan Akun AWS ke organisasi atau OU yang memiliki akses ke pembagian sumber daya, maka akun anggota baru tersebut secara otomatis mendapatkan akses ke pembagian sumber daya. Administrator akun yang Anda bagikan kemudian dapat memberikan kepala sekolah individu di akun tersebut akses ke sumber daya di bagian tersebut.
- Jika Anda menghapus akun dari organisasi atau OU yang memiliki akses ke pembagian sumber daya, maka setiap prinsipal di akun tersebut secara otomatis kehilangan akses ke sumber daya yang diakses melalui pembagian sumber daya tersebut.
- Jika Anda berbagi langsung dengan akun anggota atau dengan peran IAM atau pengguna di akun anggota dan kemudian menghapus akun tersebut dari organisasi, maka setiap prinsipal di akun tersebut kehilangan akses ke sumber daya yang diakses melalui pembagian sumber daya tersebut.

Important

Ketika Anda berbagi dengan organisasi atau OU, dan cakupan itu mencakup akun yang memiliki pembagian sumber daya, semua kepala sekolah di akun berbagi secara otomatis mendapatkan akses ke sumber daya dalam pembagian. Akses yang diberikan ditentukan oleh izin terkelola yang terkait dengan pembagian. Ini karena kebijakan berbasis sumber daya yang AWS RAM melekat pada setiap sumber daya dalam penggunaan berbagi.

"Principal": "*" Untuk informasi selengkapnya, lihat [Implikasi penggunaan "Principal": "*" dalam kebijakan berbasis sumber daya](#).

Prinsipal di akun konsumsi lainnya tidak segera mendapatkan akses ke sumber daya saham. Administrator akun lain harus terlebih dahulu melampirkan kebijakan izin berbasis identitas ke kepala sekolah yang sesuai. Kebijakan tersebut harus memberikan Allow akses ke ARN sumber daya individu dalam pembagian sumber daya. Izin dalam kebijakan tersebut tidak dapat melebihi yang ditentukan dalam izin terkelola yang terkait dengan pembagian sumber daya.

- Anda hanya dapat menambahkan organisasi yang menjadi anggota akun Anda, dan OU dari organisasi tersebut ke pembagian sumber daya Anda. Anda tidak dapat menambahkan OU atau organisasi dari luar organisasi Anda sendiri ke pembagian sumber daya sebagai prinsipal. Namun, Anda dapat menambahkan individu Akun AWS atau, untuk layanan yang didukung, peran IAM dan pengguna dari luar organisasi Anda sebagai prinsipal untuk berbagi sumber daya.

Note

Tidak semua jenis sumber daya dapat dibagikan dengan peran dan pengguna IAM. Untuk informasi tentang sumber daya yang dapat Anda bagikan dengan prinsipal ini, lihat [Sumber daya yang dapat dibagikan AWS](#)

- Untuk jenis sumber daya berikut, Anda memiliki waktu tujuh hari untuk menerima undangan untuk bergabung dengan berbagi untuk jenis sumber daya berikut. Jika Anda tidak menerima undangan sebelum kedaluwarsa, undangan secara otomatis ditolak.

Important

Untuk jenis sumber daya bersama yang tidak ada dalam daftar berikut, Anda memiliki waktu 12 jam untuk menerima undangan untuk bergabung dengan pembagian sumber daya. Setelah 12 jam, undangan kedaluwarsa dan prinsipal pengguna akhir dalam pembagian sumber daya dipisahkan. Undangan tidak dapat lagi diterima oleh pengguna akhir.

- Amazon Aurora - kluster DB
- Amazon EC2 — reservasi kapasitas dan host khusus
- AWS License Manager- Konfigurasi lisensi
- AWS Outposts— Tabel rute gateway lokal, pos terdepan, dan situs
- Amazon Route 53 - Aturan penerusan
- Amazon VPC - Alamat IPv4 milik pelanggan, daftar awalan, subnet, target cermin lalu lintas, gateway transit, domain multicast gateway transit

Console

Untuk membuat pembagian sumber daya

1. Buka [konsol AWS RAM](#).
2. Karena pembagian AWS RAM sumber daya ada secara spesifik Wilayah AWS, pilih yang sesuai Wilayah AWS dari daftar tarik-turun di sudut kanan atas konsol. Untuk melihat pembagian sumber daya yang berisi sumber daya global, Anda harus mengatur Wilayah

AWS ke US East (Virginia N.), (us-east-1). Untuk informasi selengkapnya tentang berbagi sumber daya global, lihat [Berbagi sumber daya Regional dibandingkan dengan sumber daya global](#). Jika Anda ingin memasukkan sumber daya global dalam pembagian sumber daya, maka Anda harus memilih Wilayah asal yang ditunjuk, AS Timur (Virginia N.), us-east-1.

3. Jika Anda baru AWS RAM, pilih Buat berbagi sumber daya dari halaman beranda. Jika tidak, pilih Buat berbagi sumber daya dari halaman [Dibagikan oleh saya: Berbagi sumber daya](#).
4. Pada Langkah 1: Tentukan detail berbagi sumber daya, lakukan hal berikut:
 - a. Untuk Nama, masukkan nama deskriptif untuk berbagi sumber daya.
 - b. Di bawah Sumber Daya, pilih sumber daya untuk ditambahkan ke pembagian sumber daya sebagai berikut:
 - Untuk Pilih jenis sumber daya, pilih jenis sumber daya yang akan dibagikan. Ini menyaring daftar sumber daya yang dapat dibagikan hanya ke sumber daya dari jenis yang dipilih.
 - Dalam daftar sumber daya yang dihasilkan, pilih kotak centang di sebelah sumber daya individual yang ingin Anda bagikan. Sumber daya yang dipilih bergerak di bawah Sumber daya yang dipilih.

Jika Anda berbagi sumber daya yang terkait dengan zona ketersediaan tertentu, maka menggunakan ID Zona Ketersediaan (ID AZ) membantu Anda menentukan lokasi relatif sumber daya ini di seluruh akun. Untuk informasi selengkapnya, lihat [ID Availability Zone untuk AWS sumber daya Anda](#).
 - c. (Opsional) Untuk [melampirkan tag](#) ke berbagi sumber daya, di bawah Tag, masukkan kunci tag dan nilai. Tambahkan yang lain dengan memilih Tambahkan tag baru. Ulangi langkah ini sesuai kebutuhan. Tag ini hanya berlaku untuk pembagian sumber daya itu sendiri, bukan untuk sumber daya dalam pembagian sumber daya.
5. Pilih Selanjutnya.
6. Pada Langkah 2: Kaitkan izin terkelola dengan setiap jenis sumber daya, Anda dapat memilih untuk mengaitkan izin terkelola yang dibuat AWS dengan jenis sumber daya, memilih izin terkelola pelanggan yang ada, atau Anda dapat membuat izin terkelola pelanggan Anda sendiri untuk jenis sumber daya yang didukung. Untuk informasi selengkapnya, lihat [Jenis izin terkelola](#).

Pilih Buat izin terkelola pelanggan untuk membuat izin terkelola pelanggan yang memenuhi persyaratan kasus penggunaan berbagi Anda. Untuk informasi selengkapnya,

lihat [Membuat izin terkelola pelanggan](#). Setelah menyelesaikan proses, pilih



dan kemudian Anda dapat memilih izin terkelola pelanggan baru Anda dari daftar tarik-turun izin terkelola.

Note

Jika izin terkelola yang dipilih memiliki beberapa versi, maka AWS RAM secara otomatis melampirkan versi default. Anda hanya dapat melampirkan versi yang ditetapkan sebagai default.

Untuk menampilkan tindakan yang diizinkan izin terkelola, perluas Lihat templat kebijakan untuk izin terkelola ini.

7. Pilih Selanjutnya.
8. Pada Langkah 3: Berikan akses ke kepala sekolah, lakukan hal berikut:
 - a. Secara default, Izinkan berbagi dengan siapa pun dipilih, yang berarti, untuk jenis sumber daya yang mendukungnya, Anda dapat berbagi sumber daya dengan Akun AWS yang berada di luar organisasi Anda. Ini tidak memengaruhi jenis sumber daya yang hanya dapat dibagikan dalam organisasi, seperti subnet Amazon VPC. Anda juga dapat membagikan beberapa [jenis sumber daya yang didukung](#) dengan peran dan pengguna IAM.

Untuk membatasi berbagi sumber daya hanya untuk akun dan kepala sekolah di organisasi Anda, pilih Izinkan berbagi hanya dalam organisasi Anda.

- b. Untuk Kepala Sekolah, lakukan hal berikut:
 - Untuk menambahkan organisasi, unit organisasi (OU), atau Akun AWS yang merupakan bagian dari organisasi, aktifkan Menampilkan struktur organisasi. Ini menampilkan tampilan pohon organisasi Anda. Kemudian, pilih kotak centang di sebelah setiap prinsipal yang ingin Anda tambahkan.

Important

Ketika Anda berbagi dengan organisasi atau OU, dan cakupan itu mencakup akun yang memiliki pembagian sumber daya, semua kepala sekolah di

akun berbagi secara otomatis mendapatkan akses ke sumber daya dalam pembagian. Akses yang diberikan ditentukan oleh izin terkelola yang terkait dengan pembagian. Ini karena kebijakan berbasis sumber daya yang AWS RAM melekat pada setiap sumber daya dalam penggunaan berbagi. "Principal": "*" Untuk informasi selengkapnya, lihat [Implikasi penggunaan "Principal": "*" dalam kebijakan berbasis sumber daya](#). Prinsipal di akun konsumsi lainnya tidak segera mendapatkan akses ke sumber daya saham. Administrator akun lain harus terlebih dahulu melampirkan kebijakan izin berbasis identitas ke kepala sekolah yang sesuai. Kebijakan tersebut harus memberikan Allow akses ke ARN sumber daya individu dalam pembagian sumber daya. Izin dalam kebijakan tersebut tidak dapat melebihi yang ditentukan dalam izin terkelola yang terkait dengan pembagian sumber daya.

- Jika Anda memilih organisasi (ID dimulai dengan o-), maka prinsipal Akun AWS di semua organisasi dapat mengakses pembagian sumber daya.
- Jika Anda memilih OU (ID dimulai dengan ou-), maka prinsipal Akun AWS di semua OU itu dan OU anaknya dapat mengakses pembagian sumber daya.
- Jika Anda memilih individu Akun AWS, maka hanya kepala sekolah di akun itu yang dapat mengakses pembagian sumber daya.

Note

Sakelar struktur organisasi tampilan hanya muncul jika berbagi dengan AWS Organizations diaktifkan dan Anda masuk ke akun manajemen untuk organisasi.

Anda tidak dapat menggunakan metode ini untuk menentukan Akun AWS di luar organisasi Anda, atau peran IAM atau pengguna. Sebagai gantinya, Anda harus menonaktifkan Menampilkan struktur organisasi dan menggunakan daftar drop-down dan kotak teks untuk memasukkan ID atau ARN.

- Untuk menentukan prinsipal berdasarkan ID atau ARN, termasuk kepala sekolah yang berada di luar organisasi, maka untuk setiap prinsipal, pilih jenis utama. Selanjutnya, masukkan ID (untuk Akun AWS, organisasi, atau OU) atau ARN (untuk peran IAM

atau pengguna), lalu pilih Tambah. Jenis utama yang tersedia dan format ID dan ARN adalah sebagai berikut:

- Akun AWS— Untuk menambahkan Akun AWS, masukkan ID akun 12 digit. Misalnya:

```
123456789012
```

- Organisasi — Untuk menambahkan semua yang Akun AWS ada di organisasi Anda, masukkan ID organisasi. Misalnya:

```
o-abcd1234
```

- Unit organisasi (OU) - Untuk menambahkan OU, masukkan ID OU. Misalnya:


```
ou-abcd-1234efgh
```

- Peran IAM — Untuk menambahkan peran IAM, masukkan ARN peran tersebut. Gunakan sintaks berikut:

```
arn:partition:iam::account:role/role-name
```

Misalnya:

```
arn:aws:iam::123456789012:role/MyS3AccessRole
```

 Note

Untuk mendapatkan ARN unik untuk peran IAM, [lihat daftar peran di konsol IAM](#), gunakan perintah [get-role](#) AWS CLI atau tindakan API. [GetRole](#)

- Pengguna IAM — Untuk menambahkan pengguna IAM, masukkan ARN pengguna. Gunakan sintaks berikut:

```
arn:partition:iam::account:user/user-name
```

Misalnya:

```
arn:aws:iam::123456789012:user/bob
```

Note

Untuk mendapatkan ARN unik untuk pengguna IAM, [lihat daftar pengguna di konsol IAM](#), gunakan `get-user` AWS CLI perintah, atau tindakan API. [GetUser](#)

- Prinsipal layanan — Untuk menambahkan prinsipal layanan, pilih Prinsipal layanan dari dropdown tipe utama Pilih. Masukkan nama kepala AWS layanan. Gunakan sintaks berikut:

- `service-id.amazonaws.com`

Misalnya:

`pca-connector-ad.amazonaws.com`

- c. Untuk Prinsipal yang dipilih, verifikasi bahwa prinsipal yang Anda tentukan muncul dalam daftar.

9. Pilih Selanjutnya.

10. Pada Langkah 4: Tinjau dan buat, tinjau detail konfigurasi untuk berbagi sumber daya Anda. Untuk mengubah konfigurasi untuk langkah apa pun, pilih tautan yang sesuai dengan langkah yang ingin Anda kembalikan dan buat perubahan yang diperlukan.
11. Setelah Anda selesai meninjau pembagian sumber daya, pilih Buat berbagi sumber daya.

Diperlukan beberapa menit untuk menyelesaikan sumber daya dan asosiasi utama. Izinkan proses ini selesai sebelum Anda mencoba menggunakan pembagian sumber daya.

12. Anda dapat menambahkan dan menghapus sumber daya dan prinsipal atau menerapkan tag khusus ke pembagian sumber daya Anda kapan saja. Anda dapat mengubah izin terkelola untuk jenis sumber daya yang disertakan dalam pembagian sumber daya, untuk jenis yang mendukung lebih dari izin terkelola default. Anda dapat menghapus pembagian sumber daya ketika Anda tidak lagi ingin berbagi sumber daya. Untuk informasi selengkapnya, lihat [Bagikan AWS sumber daya yang dimiliki oleh Anda](#).

AWS CLI

Untuk membuat pembagian sumber daya

Gunakan perintah [create-resource-share](#). Perintah berikut membuat pembagian sumber daya yang dibagikan dengan semua yang Akun AWS ada di organisasi. Share berisi konfigurasi AWS License Manager lisensi, dan memberikan izin terkelola default untuk jenis sumber daya tersebut.

Note

Jika Anda ingin menggunakan izin terkelola pelanggan dengan jenis sumber daya dalam pembagian sumber daya ini, Anda dapat menggunakan izin terkelola pelanggan yang sudah ada atau membuat izin terkelola pelanggan baru. Catat ARN untuk izin yang dikelola pelanggan, dan kemudian buat pembagian sumber daya. Untuk informasi selengkapnya, lihat [Membuat izin terkelola pelanggan](#).

```
$ aws ram create-resource-share \
  --region us-east-1 \
  --name MyLicenseConfigShare \
  --permission-arns arn:aws:ram::aws:permission/
AWSRAMDefaultPermissionLicenseConfiguration \
  --resource-arns arn:aws:license-manager:us-east-1:123456789012:license-
configuration:lic-abc123 \
  --principals arn:aws:organizations::123456789012:organization/o-1234abcd
{
  "resourceShare": {
    "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/12345678-abcd-09876543",
    "name": "MyLicenseConfigShare",
    "owningAccountId": "123456789012",
    "allowExternalPrincipals": true,
    "status": "ACTIVE",
    "creationTime": "2021-09-14T20:42:40.266000-07:00",
    "lastUpdatedTime": "2021-09-14T20:42:40.266000-07:00"
  }
}
```

Menggunakan AWS sumber daya bersama

Untuk mulai menggunakan sumber daya yang dibagikan dengan akun Anda menggunakan AWS Resource Access Manager, selesaikan tugas berikut.

Tugas

- [Menanggapi undangan berbagi sumber daya](#)
- [Menggunakan sumber daya yang dibagikan dengan Anda](#)

Menanggapi undangan berbagi sumber daya

Jika Anda menerima undangan untuk bergabung dengan berbagi sumber daya, Anda harus menerimanya untuk mendapatkan akses ke sumber daya bersama.

Undangan tidak digunakan dalam skenario berikut:

- Jika Anda adalah bagian dari sebuah organisasi diAWS Organizations dan berbagi dalam organisasi Anda diaktifkan, maka prinsipal di organisasi secara otomatis mendapatkan akses ke sumber bersama tanpa undangan.
- Jika Anda berbagi dengan Akun AWS yang memiliki sumber daya, maka prinsipal di akun itu secara otomatis mendapatkan akses ke sumber daya bersama tanpa undangan.

Console

Untuk menanggapi undangan

1. Buka halaman [Shared with me: Resource shares](#) diAWS RAM konsol.

Note

Sebuah saham sumber daya terlihat hanyaWilayah AWS di mana ia dibuat. Jika berbagi sumber daya yang diharapkan tidak muncul di konsol, Anda mungkin perlu beralih ke yang berbedaWilayah AWS menggunakan kontrol drop-down di sudut kanan atas.

2. Tinjau daftar saham sumber daya yang telah Anda berikan akses.

Kolom Status menunjukkan status partisipasi Anda saat ini untuk berbagi sumber daya. PendingStatus menunjukkan bahwa Anda telah ditambahkan ke pembagian sumber daya, tetapi Anda belum menerima atau menolak undangan tersebut.

3. Untuk menanggapi undangan berbagi sumber daya, pilih ID berbagi sumber daya dan pilih Terima berbagi sumber daya untuk menerima undangan, atau Tolak berbagi sumber daya

untuk menolak undangan. Jika Anda menolak undangan, Anda tidak mendapatkan akses ke sumber daya. Jika Anda menerima undangan, Anda mendapatkan akses ke sumber daya.

AWS CLI

Untuk memulai, dapatkan daftar undangan berbagi sumber daya yang tersedia untuk Anda. Contoh perintah berikut dijalankan di `us-west-2` Wilayah, dan menunjukkan satu share sumber daya tersedia di `PENDING` negara bagian.

```
$ aws ram get-resource-share-invitations
{
  "resourceShareInvitations": [
    {
      "resourceShareInvitationArn": "arn:aws:ram:us-
west-2:111122223333:resource-share-invitation/1234abcd-ef12-9876-5432-aaaaaa111111",
      "resourceShareName": "MyNewResourceShare",
      "resourceShareArn": "arn:aws:ram:us-west-2:111122223333:resource-
share/1234abcd-ef12-9876-5432-bbbbbb222222",
      "senderAccountId": "111122223333",
      "receiverAccountId": "444455556666",
      "invitationTimestamp": "2021-09-15T15:00:32.568000-07:00",
      "status": "PENDING"
    }
  ]
}
```

Anda dapat menggunakan Amazon Resource Name (ARN) dari undangan dari perintah sebelumnya sebagai parameter di perintah berikutnya untuk menerima undangan itu.

```
$ aws ram accept-resource-share-invitation \
  --resource-share-invitation-arn arn:aws:ram:us-west-2:111122223333:resource-
share-invitation/1234abcd-ef12-9876-5432-aaaaaa111111
{
  "resourceShareInvitation": {
    "resourceShareInvitationArn": "arn:aws:ram:us-west-2:111122223333:resource-
share-invitation/1234abcd-ef12-9876-5432-aaaaaa111111",
    "resourceShareName": "MyNewResourceShare",
    "resourceShareArn": "arn:aws:ram:us-west-2:111122223333:resource-
share/1234abcd-ef12-9876-5432-bbbbbb222222",
    "senderAccountId": "111122223333",
    "receiverAccountId": "444455556666",
    "invitationTimestamp": "2021-09-15T15:14:12.580000-07:00",
```

```
    "status": "ACCEPTED"  
  }  
}
```

Output menunjukkan bahwa status telah berubah menjadi ACCEPTED. Sumber daya yang termasuk dalam pembagian sumber daya sekarang tersedia untuk prinsipal di akun penerima.

Menggunakan sumber daya yang dibagikan dengan Anda

Setelah menerima undangan untuk bergabung dengan berbagi sumber daya, Anda dapat melakukan tindakan spesifik pada sumber daya bersama. Tindakan ini bervariasi menurut jenis sumber daya. Untuk informasi selengkapnya, lihat [Sumber daya yang dapat dibagikan AWS](#). Sumber daya tersedia langsung di setiap konsol layanan sumber daya dan operasi API/CLI. Jika sumber daya bersifat regional, maka Anda harus menggunakan yang benar Wilayah AWS di konsol layanan atau perintah API/CLI. Jika sumber daya global, maka Anda harus menggunakan wilayah rumah yang ditunjuk, AS Timur (Virginia N.), us-east-1 Untuk melihat sumber daya di AWS RAM, Anda harus membuka AWS RAM konsol untuk berbagi sumber daya Wilayah AWS yang dibuat di.

Bekerja dengan AWS sumber daya bersama

Anda dapat menggunakan AWS Resource Access Manager (AWS RAM) untuk berbagi AWS sumber daya yang Anda miliki dan mengakses AWS sumber daya yang dibagikan dengan Anda.

Daftar Isi

- [Berbagi sumber daya Regional dibandingkan dengan sumber daya global](#)
 - [Apa perbedaan antara sumber daya Regional dan global?](#)
 - [Pembagian sumber daya dan Wilayah mereka](#)
- [Bagikan AWS sumber daya yang dimiliki oleh Anda](#)
 - [Melihat pembagian sumber daya yang Anda buat AWS RAM](#)
 - [Membuat pembagian sumber daya di AWS RAM](#)
 - [Memperbarui pangsa sumber daya AWS RAM](#)
 - [Melihat sumber daya bersama Anda di AWS RAM](#)
 - [Melihat prinsip-prinsip yang Anda bagikan sumber daya AWS RAM](#)
 - [Menghapus pangsa sumber daya di AWS RAM](#)
- [Akses AWS sumber daya yang dibagikan dengan Anda](#)
 - [Menerima dan menolak undangan berbagi sumber daya](#)
 - [Melihat berbagi sumber daya yang dibagikan dengan Anda](#)
 - [Melihat sumber daya yang dibagikan dengan Anda](#)
 - [Lihat kepala sekolah berbagi dengan Anda](#)
 - [Meninggalkan berbagi sumber daya](#)
 - [Prasyarat untuk meninggalkan pembagian sumber daya](#)
 - [Cara meninggalkan pembagian sumber daya](#)
- [ID Availability Zone untuk AWS sumber daya Anda](#)

Berbagi sumber daya Regional dibandingkan dengan sumber daya global

Topik ini membahas perbedaan cara AWS Resource Access Manager (AWS RAM) bekerja dengan [sumber daya Regional dan global](#).

Sumber daya bersifat Regional atau global. Anda dapat menggunakan bidang keempat di [Amazon Resource Name \(ARN\)](#) untuk mengidentifikasi apakah sumber daya bersifat Regional atau global. Sumber daya regional menunjukkan Wilayah AWS. Jika kosong, maka sumber daya bersifat global.

Apa perbedaan antara sumber daya Regional dan global?

Sumber daya regional

Sebagian besar sumber daya yang dapat Anda bagikan AWS RAM adalah Regional. Anda membuat mereka dalam tertentu Wilayah AWS, dan kemudian mereka ada di Wilayah itu. Untuk melihat atau berinteraksi dengan sumber daya tersebut, Anda harus mengarahkan operasi Anda ke Wilayah tersebut. Misalnya, untuk membuat instans Amazon Elastic Compute Cloud (Amazon EC2) dengan AWS Management Console, Anda [memilih](#) instans Wilayah AWS yang ingin Anda buat. Jika Anda menggunakan AWS Command Line Interface (AWS CLI) untuk membuat instance, maka Anda menyertakan `--region` parameter. AWSSDK masing-masing memiliki mekanisme yang setara untuk menentukan Wilayah yang digunakan operasi.

Ada beberapa alasan untuk menggunakan sumber daya Regional. Salah satu alasan yang baik adalah untuk memastikan bahwa sumber daya, dan titik akhir layanan yang Anda gunakan untuk mengaksesnya, sedekat mungkin dengan pelanggan. Ini meningkatkan kinerja dengan meminimalkan latensi. Alasan lain adalah untuk memberikan batas isolasi. Ini memungkinkan Anda membuat salinan sumber daya independen di beberapa Wilayah untuk mendistribusikan beban dan meningkatkan skalabilitas. Pada saat yang sama, ia mengisolasi sumber daya satu sama lain untuk meningkatkan ketersediaan.

Jika Anda menentukan yang berbeda Wilayah AWS di konsol atau AWS CLI perintah, maka Anda tidak dapat lagi melihat atau berinteraksi dengan sumber daya yang dapat Anda lihat di Wilayah sebelumnya.

Saat Anda melihat [Amazon Resource Name \(ARN\)](#) untuk sumber daya Regional, Wilayah yang berisi sumber daya ditentukan sebagai bidang keempat di ARN. Misalnya, instans Amazon EC2 adalah sumber daya Regional. Sumber daya tersebut memiliki ARN yang terlihat mirip dengan contoh berikut untuk VPC yang ada di `us-east-1` Wilayah.

```
arn:aws:ec2:us-east-1:123456789012:instance/i-0a6f30921424d3eee
```

Sumber daya global

Beberapa AWS layanan mendukung sumber daya yang dapat Anda akses secara global, artinya Anda dapat menggunakan sumber daya dari mana saja. Anda tidak menentukan Wilayah AWS di

konsol layanan global. Untuk mengakses sumber daya global, Anda tidak menentukan `--region` parameter saat menggunakan operasi layanan AWS CLI dan AWS SDK.

Sumber daya global mendukung kasus di mana sangat penting bahwa hanya satu instance dari sumber daya tertentu yang dapat ada pada satu waktu. Dalam skenario seperti itu, replikasi atau sinkronisasi antara salinan di Wilayah yang berbeda tidak memadai. Harus mengakses titik akhir global tunggal, dengan kemungkinan peningkatan latensi, dianggap dapat diterima untuk memastikan bahwa setiap perubahan secara instan terlihat oleh konsumen sumber daya. Misalnya, saat Anda membuat jaringan inti AWS Cloud WAN sebagai sumber daya global, jaringan ini konsisten untuk semua pengguna. Ini muncul sebagai jaringan global tunggal yang berdekatan di semua Wilayah.

[Amazon Resource Name \(ARN\)](#) untuk sumber daya global tidak menyertakan Wilayah. Bidang keempat ARN tersebut kosong, seperti contoh ARN berikut untuk jaringan inti Cloud WAN.

```
arn:aws:networkmanager::123456789012:core-network/core-network-0514d38fa6f796cea
```

Pembagian sumber daya dan Wilayah mereka

AWS RAM adalah layanan Regional, dan bagian sumber daya adalah Regional. Oleh karena itu, pangsa sumber daya dapat berisi sumber daya yang Wilayah AWS sama dengan pangsa sumber daya, dan sumber daya global yang didukung. Wilayah tempat Anda membuat pangsa sumber daya adalah Wilayah asal pangsa sumber daya.

Important

Saat ini, Anda dapat membuat saham sumber daya dengan sumber daya global hanya di rumah yang ditunjuk Wilayah AS Timur (Virginia) Wilayah, `us-east-1`. Meskipun Anda dapat membuat pangsa sumber daya hanya di Wilayah rumah tunggal tersebut, sumber daya global yang dibagikan akan muncul sebagai sumber daya global standar saat dilihat di konsol layanan tersebut atau operasi CLI dan SDK. Pembatasan ke Wilayah asal hanya berlaku untuk pangsa sumber daya, bukan sumber daya yang dikandungnya.

Untuk berbagi sumber daya Regional yang Anda buat di `us-west-2` Wilayah, Anda harus mengkonfigurasi AWS RAM konsol untuk menggunakan `us-west-2` dan membuat berbagi sumber daya di sana. Anda tidak dapat membuat pangsa sumber daya yang mencakup sumber

daya Regional dari yang berbeda Wilayah AWS. Ini berarti bahwa untuk berbagi sumber daya dari keduanya `us-west-2` dan `eu-north-1`, Anda harus membuat dua saham sumber daya yang berbeda. Anda tidak dapat menggabungkan sumber daya dari dua Wilayah yang berbeda menjadi satu bagian sumber daya.

Untuk berbagi sumber daya global di AWS RAM konsol, Anda harus mengkonfigurasi AWS RAM konsol untuk menggunakan Wilayah rumah yang ditunjuk, AS Timur (Virginia N.). `us-east-1` Kemudian, buat pangsa sumber daya di Wilayah rumah yang ditunjuk. Anda dapat mencampur sumber daya global dalam pembagian sumber daya hanya dengan sumber daya dari `us-east-1` Wilayah.

Meskipun sumber daya global dapat dilihat dalam pangsa AWS RAM sumber daya hanya di Wilayah asal yang ditunjuk, sumber daya global masih menjadi sumber daya global setelah Anda membagikannya. Anda dapat mengaksesnya di bagian yang dibagikan Akun AWS dari Wilayah mana pun tempat Anda dapat mengaksesnya di aslinya Akun AWS.

Pertimbangan-pertimbangan

- Untuk membuat berbagi sumber daya di AWS RAM konsol, Anda harus menggunakan Wilayah yang berisi sumber daya yang ingin Anda bagikan. Jika Anda ingin menyertakan sumber daya global, maka Anda harus menggunakan Wilayah rumah yang ditunjuk untuk membuat bagian. Misalnya, untuk berbagi jaringan inti AWS Cloud WAN, Anda harus membuat pangsa sumber daya di `us-east-1` Wilayah.
- Untuk melihat atau memodifikasi pangsa sumber daya di AWS RAM konsol, Anda harus menggunakan Wilayah yang berisi pangsa sumber daya. Demikian pula, operasi AWS RAM AWS CLI dan SDK memungkinkan Anda berinteraksi dengan hanya berbagi sumber daya yang ada di Wilayah yang Anda tentukan dalam operasi Anda. Untuk melihat atau memodifikasi saham sumber daya yang mengandung sumber daya global, Anda harus menggunakan Wilayah asal yang ditunjuk, AS Timur (Virginia Utara), `us-east-1`
- Untuk melihat sumber daya Regional di AWS RAM konsol untuk memasukkannya ke dalam pangsa sumber daya, Anda harus menggunakan Wilayah yang berisi sumber daya Regional.
- Untuk melihat sumber daya global di AWS RAM konsol untuk memasukkannya ke dalam pangsa sumber daya, Anda harus menggunakan Wilayah asal yang ditunjuk, AS Timur (Virginia Utara), `us-east-1`
- Anda dapat membuat pangsa sumber daya dengan sumber daya Regional dan global hanya di Wilayah asal yang ditunjuk, AS Timur (Virginia Utara), `us-east-1`

Bagikan AWS sumber daya yang dimiliki oleh Anda

Anda dapat menggunakan AWS Resource Access Manager (AWS RAM) untuk berbagi sumber daya yang Anda tentukan dengan prinsipal yang Anda tentukan. Bagian ini menjelaskan bagaimana Anda dapat membuat berbagi sumber daya baru, memodifikasi saham sumber daya yang ada, dan menghapus berbagi sumber daya yang tidak lagi Anda butuhkan.

Topik

- [Melihat pembagian sumber daya yang Anda buat AWS RAM](#)
- [Membuat pembagian sumber daya di AWS RAM](#)
- [Memperbarui pangsa sumber daya AWS RAM](#)
- [Melihat sumber daya bersama Anda di AWS RAM](#)
- [Melihat prinsip-prinsip yang Anda bagikan sumber daya AWS RAM](#)
- [Menghapus pangsa sumber daya di AWS RAM](#)

Melihat pembagian sumber daya yang Anda buat AWS RAM

Anda dapat melihat daftar pembagian sumber daya yang Anda buat. Anda dapat melihat sumber daya yang Anda bagikan dan kepala sekolah dengan siapa mereka dibagikan.

Console

Melihat Anda dapat melihat Anda dapat melihat Anda

1. Buka halaman [Shared by me: Resource shares](#) di AWS RAM konsol.
2. Karena pembagian AWS RAM sumber daya ada secara spesifik Wilayah AWS, pilih yang sesuai Wilayah AWS dari daftar dropdown di sudut kanan atas konsol. Untuk melihat pembagian sumber daya yang berisi sumber daya global, Anda harus mengatur Wilayah AWS ke US East (N. Virginia), (us-east-1). Untuk informasi selengkapnya tentang pembagian sumber daya global, lihat [Berbagi sumber daya Regional dibandingkan dengan sumber daya global](#).
3. Jika salah satu izin terkelola yang digunakan oleh pembagian sumber daya dalam hasil memiliki versi baru dari izin terkelola yang ditetapkan sebagai default, maka halaman tersebut menampilkan spanduk untuk memberi tahu Anda. Anda dapat memilih untuk memperbarui semua versi izin terkelola sekaligus dengan memilih Tinjau dan memperbarui semua di bagian atas halaman.

Atau, untuk berbagi sumber daya individual dengan satu atau beberapa versi baru izin terkelola, kolom Status menampilkan Pembaruan yang tersedia. Memilih tautan tersebut memulai proses meninjau versi izin terkelola yang diperbarui dan memungkinkan Anda menetapkannya sebagai versi untuk jenis sumber daya yang relevan dalam satu sumber daya tersebut.

4. (Opsional) Terapkan filter untuk menemukan saham sumber daya tertentu. Anda dapat menerapkan beberapa filter untuk mempersempit pencarian Anda. Anda dapat mengetikkan kata kunci, seperti bagian dari nama berbagi sumber daya untuk hanya mencantumkan saham sumber daya yang menyertakan teks tersebut dalam nama. Pilih kotak teks untuk melihat daftar dropdown bidang atribut yang disarankan. Setelah Anda memilih salah satu, Anda dapat memilih dari daftar nilai yang tersedia untuk bidang itu. Anda dapat menambahkan atribut atau kata kunci lain sampai Anda menemukan sumber daya yang Anda inginkan.
5. Pilih nama pembagian sumber daya yang akan ditinjau. Konsol menampilkan informasi berikut tentang pangsa sumber daya:
 - Ringkasan — Mencantumkan nama berbagi sumber daya, ID, pemilik, Amazon Resource Name (ARN), tanggal pembuatan, apakah itu mengizinkan berbagi dengan akun eksternal, dan statusnya saat ini.
 - Izin Terkelola - Mencantumkan izin terkelola yang dilampirkan ke pangsa sumber daya ini. Paling banyak dapat ada satu izin terkelola per jenis sumber daya yang disertakan dalam pembagian sumber daya. Setiap izin terkelola menampilkan versi izin terkelola yang terkait dengan pembagian sumber daya. Jika bukan versi default, maka konsol menampilkan tautan Pembaruan ke versi default. Jika Anda memilih tautan itu, maka Anda diberi kesempatan untuk memperbarui berbagi sumber daya untuk menggunakan versi default.
 - Sumber daya bersama - Mencantumkan sumber daya individual yang disertakan dalam pangsa sumber daya. Pilih ID sumber daya untuk membuka tab browser baru untuk melihat sumber daya di konsol layanan aslinya.
 - Kepala sekolah bersama - Daftar kepala sekolah dengan siapa sumber daya dibagikan.
 - Tags - Mencantumkan pasangan nilai kunci tag yang dilampirkan ke pangsa sumber daya itu sendiri; ini bukan tag yang dilampirkan ke sumber daya individual yang disertakan dalam pangsa sumber daya.

AWS CLI

Melihat Anda dapat melihat Anda dapat melihat Anda

Anda dapat menggunakan [get-resource-shares](#) perintah dengan parameter yang `--resource-owner` diatur `SELF` untuk menampilkan rincian saham sumber daya yang dibuat di Akun AWS.

Contoh berikut menunjukkan saham sumber daya yang dibagi dalam current Wilayah AWS (`us-east-1`) untuk panggilan Akun AWS. Untuk mendapatkan saham sumber daya yang dibuat di Wilayah yang berbeda, gunakan `--region <region-code>` parameter. Untuk menyertakan pembagian sumber daya yang berisi sumber daya global, Anda harus menentukan Wilayah US East (N. Virginia) `us-east-1`.

```
$ aws ram get-resource-shares \
  --resource-owner SELF
{
  "resourceShares": [
    {
      "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/2ebe77d7-4156-4a93-87a4-228568d04425",
      "name": "MySubnetShare",
      "owningAccountId": "123456789012",
      "allowExternalPrincipals": true,
      "status": "ACTIVE",
      "creationTime": "2021-09-10T15:38:54.449000-07:00",
      "lastUpdatedTime": "2021-09-10T15:38:54.449000-07:00",
      "featureSet": "STANDARD"
    },
    {
      "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/818d71dd-7512-4f71-99c6-2ae57aa010bc",
      "name": "MyLicenseConfigShare",
      "owningAccountId": "123456789012",
      "allowExternalPrincipals": true,
      "status": "ACTIVE",
      "creationTime": "2021-09-14T20:42:40.266000-07:00",
      "lastUpdatedTime": "2021-09-14T20:42:40.266000-07:00",
      "featureSet": "STANDARD"
    }
  ]
}
```

Membuat pembagian sumber daya di AWS RAM

Untuk berbagi sumber daya yang Anda miliki, buat pembagian sumber daya. Berikut adalah gambaran umum prosesnya:

1. Tambahkan sumber daya yang ingin Anda bagikan.
2. Untuk setiap jenis sumber daya yang Anda sertakan dalam share, tentukan [izin terkelola](#) yang akan digunakan untuk jenis sumber daya tersebut.
 - Anda dapat memilih dari salah satu izin AWS terkelola yang tersedia, izin terkelola pelanggan yang sudah ada, atau membuat izin terkelola pelanggan baru.
 - AWS izin terkelola dibuat oleh AWS untuk mencakup kasus penggunaan standar.
 - Izin terkelola pelanggan memungkinkan Anda menyesuaikan izin terkelola Anda sendiri untuk memenuhi kebutuhan keamanan dan bisnis Anda.

Note

Jika izin terkelola yang dipilih memiliki beberapa versi, maka AWS RAM secara otomatis melampirkan versi default. Anda hanya dapat melampirkan versi yang ditetapkan sebagai default.

3. Tentukan prinsip yang ingin Anda akses ke sumber daya.

Pertimbangan-pertimbangan

- Jika nanti Anda perlu menghapus AWS sumber daya yang Anda sertakan dalam berbagi, sebaiknya Anda menghapus sumber daya dari pembagian sumber daya apa pun yang menyertakannya, atau menghapus pembagian sumber daya.
- Jenis sumber daya yang dapat Anda sertakan dalam pembagian sumber daya tercantum di [Sumber daya yang dapat dibagikan AWS](#).
- Anda dapat berbagi sumber daya hanya jika Anda [memilikinya](#). Anda tidak dapat berbagi sumber daya yang dibagikan dengan Anda.
- AWS RAM adalah layanan regional. Saat Anda berbagi sumber daya dengan prinsipal di tempat lain Akun AWS, prinsipal tersebut harus mengakses setiap sumber daya dari sumber daya yang sama Wilayah AWS dengan yang dibuat. Untuk sumber daya global yang didukung, Anda dapat mengakses sumber daya tersebut dari sumber daya apa pun Wilayah AWS yang didukung oleh konsol layanan dan alat sumber daya tersebut. Anda dapat melihat pembagian sumber daya

tersebut dan sumber daya globalnya di AWS RAM konsol dan alat hanya di Wilayah asal yang ditunjuk, AS Timur (Virginia N.),us-east-1. Untuk informasi selengkapnya tentang AWS RAM dan sumber daya global, lihat [Berbagi sumber daya Regional dibandingkan dengan sumber daya global](#).

- Jika akun yang Anda bagikan adalah bagian dari organisasi AWS Organizations dan berbagi dalam organisasi Anda diaktifkan, semua prinsipal di organisasi yang Anda bagikan secara otomatis diberikan akses ke pembagian sumber daya tanpa menggunakan undangan. Seorang kepala sekolah dalam akun dengan siapa Anda berbagi di luar konteks organisasi menerima undangan untuk bergabung dengan pembagian sumber daya dan diberikan akses ke sumber daya bersama hanya setelah mereka menerima undangan.
- Jika Anda berbagi dengan kepala layanan, Anda tidak dapat mengaitkan prinsip lain dengan pembagian sumber daya.
- Jika berbagi antara akun atau kepala sekolah yang merupakan bagian dari organisasi, maka setiap perubahan keanggotaan organisasi secara dinamis memengaruhi akses ke pembagian sumber daya.
 - Jika Anda menambahkan Akun AWS ke organisasi atau OU yang memiliki akses ke pembagian sumber daya, maka akun anggota baru tersebut secara otomatis mendapatkan akses ke pembagian sumber daya. Administrator akun yang Anda bagikan kemudian dapat memberikan kepala sekolah individu di akun tersebut akses ke sumber daya di bagian tersebut.
 - Jika Anda menghapus akun dari organisasi atau OU yang memiliki akses ke pembagian sumber daya, maka setiap prinsipal di akun tersebut secara otomatis kehilangan akses ke sumber daya yang diakses melalui pembagian sumber daya tersebut.
 - Jika Anda berbagi langsung dengan akun anggota atau dengan peran IAM atau pengguna di akun anggota dan kemudian menghapus akun tersebut dari organisasi, maka setiap prinsipal di akun tersebut kehilangan akses ke sumber daya yang diakses melalui pembagian sumber daya tersebut.

Important

Ketika Anda berbagi dengan organisasi atau OU, dan cakupan itu mencakup akun yang memiliki pembagian sumber daya, semua kepala sekolah di akun berbagi secara otomatis mendapatkan akses ke sumber daya dalam pembagian. Akses yang diberikan ditentukan oleh izin terkelola yang terkait dengan pembagian. Ini karena kebijakan berbasis sumber daya yang AWS RAM melekat pada setiap sumber daya dalam penggunaan berbagi.

"Principal": "*" Untuk informasi selengkapnya, lihat [Implikasi penggunaan "Principal": "*" dalam kebijakan berbasis sumber daya](#).

Prinsipal di akun konsumsi lainnya tidak segera mendapatkan akses ke sumber daya saham. Administrator akun lain harus terlebih dahulu melampirkan kebijakan izin berbasis identitas ke kepala sekolah yang sesuai. Kebijakan tersebut harus memberikan Allow akses ke ARN sumber daya individu dalam pembagian sumber daya. Izin dalam kebijakan tersebut tidak dapat melebihi yang ditentukan dalam izin terkelola yang terkait dengan pembagian sumber daya.

- Anda hanya dapat menambahkan organisasi yang menjadi anggota akun Anda, dan OU dari organisasi tersebut ke pembagian sumber daya Anda. Anda tidak dapat menambahkan OU atau organisasi dari luar organisasi Anda sendiri ke pembagian sumber daya sebagai prinsipal. Namun, Anda dapat menambahkan individu Akun AWS atau, untuk layanan yang didukung, peran IAM dan pengguna dari luar organisasi Anda sebagai prinsipal untuk berbagi sumber daya.

Note

Tidak semua jenis sumber daya dapat dibagikan dengan peran dan pengguna IAM. Untuk informasi tentang sumber daya yang dapat Anda bagikan dengan prinsipal ini, lihat [Sumber daya yang dapat dibagikan AWS](#)

- Untuk jenis sumber daya berikut, Anda memiliki waktu tujuh hari untuk menerima undangan bergabung dengan share untuk jenis sumber daya berikut. Jika Anda tidak menerima undangan sebelum kedaluwarsa, undangan secara otomatis ditolak.

Important

Untuk jenis sumber daya bersama yang tidak ada dalam daftar berikut, Anda memiliki waktu 12 jam untuk menerima undangan untuk bergabung dengan pembagian sumber daya. Setelah 12 jam, undangan kedaluwarsa dan prinsipal pengguna akhir dalam pembagian sumber daya dipisahkan. Undangan tidak dapat lagi diterima oleh pengguna akhir.

- Amazon Aurora - kluster DB
- Amazon EC2 — reservasi kapasitas dan host khusus
- AWS License Manager- Konfigurasi lisensi
- AWS Outposts— Tabel rute gateway lokal, pos terdepan, dan situs
- Amazon Route 53 - Aturan penerusan

- Amazon VPC - Alamat IPv4 milik pelanggan, daftar awalan, subnet, target cermin lalu lintas, gateway transit, domain multicast gateway transit

Console

Untuk membuat pembagian sumber daya

1. Buka [konsol AWS RAM](#).
2. Karena pembagian AWS RAM sumber daya ada secara spesifik Wilayah AWS, pilih yang sesuai Wilayah AWS dari daftar tarik-turun di sudut kanan atas konsol. Untuk melihat pembagian sumber daya yang berisi sumber daya global, Anda harus mengatur Wilayah AWS ke US East (Virginia N.), (us-east-1). Untuk informasi selengkapnya tentang berbagi sumber daya global, lihat [Berbagi sumber daya Regional dibandingkan dengan sumber daya global](#). Jika Anda ingin memasukkan sumber daya global dalam pembagian sumber daya, maka Anda harus memilih Wilayah asal yang ditunjuk, AS Timur (Virginia N.), us-east-1.
3. Jika Anda baru AWS RAM, pilih Buat berbagi sumber daya dari halaman beranda. Jika tidak, pilih Buat berbagi sumber daya dari halaman [Dibagikan oleh saya: Berbagi sumber daya](#).
4. Pada Langkah 1: Tentukan detail berbagi sumber daya, lakukan hal berikut:
 - a. Untuk Nama, masukkan nama deskriptif untuk berbagi sumber daya.
 - b. Di bawah Sumber Daya, pilih sumber daya untuk ditambahkan ke pembagian sumber daya sebagai berikut:
 - Untuk Pilih jenis sumber daya, pilih jenis sumber daya yang akan dibagikan. Ini menyaring daftar sumber daya yang dapat dibagikan hanya ke sumber daya dari jenis yang dipilih.
 - Dalam daftar sumber daya yang dihasilkan, pilih kotak centang di sebelah sumber daya individual yang ingin Anda bagikan. Sumber daya yang dipilih bergerak di bawah Sumber daya yang dipilih.

Jika Anda berbagi sumber daya yang terkait dengan zona ketersediaan tertentu, maka menggunakan ID Zona Ketersediaan (ID AZ) membantu Anda menentukan lokasi relatif sumber daya ini di seluruh akun. Untuk informasi selengkapnya, lihat [ID Availability Zone untuk AWS sumber daya Anda](#).
 - c. (Opsional) Untuk [melampirkan tag](#) ke berbagi sumber daya, di bawah Tag, masukkan kunci tag dan nilai. Tambahkan yang lain dengan memilih Tambahkan tag baru. Ulangi

langkah ini sesuai kebutuhan. Tag ini hanya berlaku untuk pembagian sumber daya itu sendiri, bukan untuk sumber daya dalam pembagian sumber daya.

5. Pilih Selanjutnya.
6. Pada Langkah 2: Kaitkan izin terkelola dengan setiap jenis sumber daya, Anda dapat memilih untuk mengaitkan izin terkelola yang dibuat AWS dengan jenis sumber daya, memilih izin terkelola pelanggan yang ada, atau Anda dapat membuat izin terkelola pelanggan Anda sendiri untuk jenis sumber daya yang didukung. Untuk informasi selengkapnya, lihat [Jenis izin terkelola](#).

Pilih Buat izin terkelola pelanggan untuk membuat izin terkelola pelanggan yang memenuhi persyaratan kasus penggunaan berbagi Anda. Untuk informasi selengkapnya, lihat [Membuat izin terkelola pelanggan](#). Setelah menyelesaikan proses, pilih



dan kemudian Anda dapat memilih izin terkelola pelanggan baru Anda dari daftar tarik-turun izin terkelola.

Note

Jika izin terkelola yang dipilih memiliki beberapa versi, maka AWS RAM secara otomatis melampirkan versi default. Anda hanya dapat melampirkan versi yang ditetapkan sebagai default.


Untuk menampilkan tindakan yang diizinkan izin terkelola, perluas Lihat templat kebijakan untuk izin terkelola ini.

7. Pilih Selanjutnya.
8. Pada Langkah 3: Berikan akses ke kepala sekolah, lakukan hal berikut:
 - a. Secara default, Izinkan berbagi dengan siapa pun dipilih, yang berarti, untuk jenis sumber daya yang mendukungnya, Anda dapat berbagi sumber daya dengan Akun AWS yang berada di luar organisasi Anda. Ini tidak memengaruhi jenis sumber daya yang hanya dapat dibagikan dalam organisasi, seperti subnet Amazon VPC. Anda juga dapat membagikan beberapa [jenis sumber daya yang didukung](#) dengan peran dan pengguna IAM.

Untuk membatasi berbagi sumber daya hanya untuk akun dan kepala sekolah di organisasi Anda, pilih Izinkan berbagi hanya dalam organisasi Anda.

b. Untuk Kepala Sekolah, lakukan hal berikut:

- Untuk menambahkan organisasi, unit organisasi (OU), atau Akun AWS yang merupakan bagian dari organisasi, aktifkan Menampilkan struktur organisasi. Ini menampilkan tampilan pohon organisasi Anda. Kemudian, pilih kotak centang di sebelah setiap prinsipal yang ingin Anda tambahkan.

 Important

Ketika Anda berbagi dengan organisasi atau OU, dan cakupan itu mencakup akun yang memiliki pembagian sumber daya, semua kepala sekolah di akun berbagi secara otomatis mendapatkan akses ke sumber daya dalam pembagian. Akses yang diberikan ditentukan oleh izin terkelola yang terkait dengan pembagian. Ini karena kebijakan berbasis sumber daya yang AWS RAM melekat pada setiap sumber daya dalam penggunaan berbagi. "Principal": "*" Untuk informasi selengkapnya, lihat [Implikasi penggunaan "Principal": "*" dalam kebijakan berbasis sumber daya](#).

Prinsipal di akun konsumsi lainnya tidak segera mendapatkan akses ke sumber daya saham. Administrator akun lain harus terlebih dahulu melampirkan kebijakan izin berbasis identitas ke kepala sekolah yang sesuai. Kebijakan tersebut harus memberikan Allow akses ke ARN sumber daya individu dalam pembagian sumber daya. Izin dalam kebijakan tersebut tidak dapat melebihi yang ditentukan dalam izin terkelola yang terkait dengan pembagian sumber daya.

- Jika Anda memilih organisasi (ID dimulai dengan o-), maka prinsipal Akun AWS di semua organisasi dapat mengakses pembagian sumber daya.
- Jika Anda memilih OU (ID dimulai dengan ou-), maka prinsipal Akun AWS di semua OU itu dan OU anaknya dapat mengakses pembagian sumber daya.
- Jika Anda memilih individu Akun AWS, maka hanya kepala sekolah di akun itu yang dapat mengakses pembagian sumber daya.

Note

Sakelar struktur organisasi tampilan hanya muncul jika berbagi dengan AWS Organizations diaktifkan dan Anda masuk ke akun manajemen untuk organisasi.

Anda tidak dapat menggunakan metode ini untuk menentukan Akun AWS di luar organisasi Anda, atau peran IAM atau pengguna. Sebagai gantinya, Anda harus menonaktifkan Menampilkan struktur organisasi dan menggunakan daftar drop-down dan kotak teks untuk memasukkan ID atau ARN.

- Untuk menentukan prinsipal berdasarkan ID atau ARN, termasuk kepala sekolah yang berada di luar organisasi, maka untuk setiap prinsipal, pilih jenis utama. Selanjutnya, masukkan ID (untuk Akun AWS, organisasi, atau OU) atau ARN (untuk peran IAM atau pengguna), lalu pilih Tambah. Jenis utama yang tersedia dan format ID dan ARN adalah sebagai berikut:

- Akun AWS— Untuk menambahkan Akun AWS, masukkan ID akun 12 digit.
Misalnya:

123456789012

- Organisasi — Untuk menambahkan semua yang Akun AWS ada di organisasi Anda, masukkan ID organisasi. Misalnya:

o-abcd1234

- Unit organisasi (OU) - Untuk menambahkan OU, masukkan ID OU. Misalnya:

ou-abcd-1234efgh

- Peran IAM — Untuk menambahkan peran IAM, masukkan ARN peran tersebut. Gunakan sintaks berikut:

arn:*partition*:iam::*account*:role/*role-name*

Misalnya:

arn:aws:iam::123456789012:role/MyS3AccessRole

Note

Untuk mendapatkan ARN unik untuk peran IAM, [lihat daftar peran di konsol IAM](#), gunakan perintah [get-role](#) AWS CLI atau tindakan API. [GetRole](#)

- Pengguna IAM — Untuk menambahkan pengguna IAM, masukkan ARN pengguna. Gunakan sintaks berikut:

```
arn:partition:iam::account:user/user-name
```

Misalnya:

```
arn:aws:iam::123456789012:user/bob
```

Note

Untuk mendapatkan ARN unik untuk pengguna IAM, [lihat daftar pengguna di konsol IAM](#), gunakan [get-user](#) AWS CLI perintah, atau tindakan API. [GetUser](#)

- Prinsipal layanan — Untuk menambahkan prinsipal layanan, pilih Prinsipal layanan dari dropdown tipe utama Pilih. Masukkan nama kepala AWS layanan. Gunakan sintaks berikut:

- *service-id*.amazonaws.com

Misalnya:

```
pca-connector-ad.amazonaws.com
```

- c. Untuk Prinsipal yang dipilih, verifikasi bahwa prinsipal yang Anda tentukan muncul dalam daftar.

9. Pilih Selanjutnya.

10. Pada Langkah 4: Tinjau dan buat, tinjau detail konfigurasi untuk berbagi sumber daya Anda. Untuk mengubah konfigurasi untuk langkah apa pun, pilih tautan yang sesuai dengan langkah yang ingin Anda kembalikan dan buat perubahan yang diperlukan.

11. Setelah Anda selesai meninjau pembagian sumber daya, pilih Buat berbagi sumber daya.

Diperlukan beberapa menit untuk menyelesaikan sumber daya dan asosiasi utama. Izinkan proses ini selesai sebelum Anda mencoba menggunakan pembagian sumber daya.

12. Anda dapat menambahkan dan menghapus sumber daya dan prinsipal atau menerapkan tag khusus ke pembagian sumber daya Anda kapan saja. Anda dapat mengubah izin terkelola untuk jenis sumber daya yang disertakan dalam pembagian sumber daya, untuk jenis yang mendukung lebih dari izin terkelola default. Anda dapat menghapus pembagian sumber daya ketika Anda tidak lagi ingin berbagi sumber daya. Untuk informasi selengkapnya, lihat [BagikanAWS sumber daya yang dimiliki oleh Anda](#).

AWS CLI

Untuk membuat pembagian sumber daya

Gunakan perintah [create-resource-share](#). Perintah berikut membuat pembagian sumber daya yang dibagikan dengan semua yang Akun AWS ada di organisasi. Berbagi berisi konfigurasi AWS License Manager lisensi, dan memberikan izin terkelola default untuk jenis sumber daya tersebut.

Note

Jika Anda ingin menggunakan izin terkelola pelanggan dengan jenis sumber daya dalam pembagian sumber daya ini, Anda dapat menggunakan izin terkelola pelanggan yang sudah ada atau membuat izin terkelola pelanggan baru. Catat ARN untuk izin yang dikelola pelanggan, dan kemudian buat pembagian sumber daya. Untuk informasi selengkapnya, lihat [Membuat izin terkelola pelanggan](#).

```
$ aws ram create-resource-share \
  --region us-east-1 \
  --name MyLicenseConfigShare \
  --permission-arns arn:aws:ram::aws:permission/
AWSRAMDefaultPermissionLicenseConfiguration \
  --resource-arns arn:aws:license-manager:us-east-1:123456789012:license-
configuration:lic-abc123 \
  --principals arn:aws:organizations::123456789012:organization/o-1234abcd
{
  "resourceShare": {
    "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/12345678-abcd-09876543",
```

```
    "name": "MyLicenseConfigShare",
    "owningAccountId": "123456789012",
    "allowExternalPrincipals": true,
    "status": "ACTIVE",
    "creationTime": "2021-09-14T20:42:40.266000-07:00",
    "lastUpdatedTime": "2021-09-14T20:42:40.266000-07:00"
  }
}
```

Memperbarui pangsa sumber dayaAWS RAM

Anda dapat memperbarui pembagian sumber dayaAWS RAM kapan saja dengan cara berikut:

- Anda dapat menambahkan prinsipal, sumber daya, atau tag ke pangsa sumber daya yang Anda buat.
- Untuk jenis sumber daya yang mendukung lebih dari izinAWS terkelola default, Anda dapat memilih izin terkelola mana yang berlaku untuk sumber daya dari setiap jenis.
- Bila izin terkelola yang dilampirkan ke berbagi sumber daya memiliki versi default baru, Anda dapat memperbarui izin terkelola untuk menggunakan versi baru.
- Anda dapat mencabut akses ke sumber daya bersama dengan menghapus prinsipal atau sumber daya dari berbagi sumber daya. Jika Anda mencabut akses, prinsipal tidak lagi memiliki akses ke sumber daya bersama.

Note

Prinsipal dengan siapa Anda berbagi sumber daya dapat meninggalkan pangsa sumber daya Anda jika berbagi kosong atau hanya berisi jenis sumber daya yang mendukung meninggalkan berbagi sumber daya. Jika berbagi sumber daya berisi jenis sumber daya yang tidak mendukung meninggalkan, pesan muncul untuk menginformasikan prinsip-prinsip bahwa mereka harus menghubungi pemilik berbagi. Dalam hal ini, Anda, sebagai pemilik pangsa sumber daya, harus menghapus prinsipal dari pangsa sumber daya Anda. Untuk daftar jenis sumber daya yang tidak mendukung tindakan ini, lihat [Prasyarat untuk meninggalkan pembagian sumber daya](#).

Console

Untuk memperbarui berbagi sumber daya

1. Arahkan ke halaman [Shared by me: Resource shares](#) di AWS RAM konsol.
2. Karena pembagian AWS RAM sumber daya ada secara spesifik Wilayah AWS, pilih yang sesuai Wilayah AWS dari daftar tarik-turun di sudut kanan atas konsol. Untuk melihat pembagian sumber daya yang mengandung sumber daya global, Anda harus mengatur Wilayah AWS ke US East (N. Virginia), (us-east-1). Untuk informasi selengkapnya tentang berbagi sumber daya global, lihat [Berbagi sumber daya Regional dibandingkan dengan sumber daya global](#).
3. Pilih berbagi sumber daya dan kemudian pilih Ubah.
4. Pada Langkah 1: Tentukan rincian berbagi sumber daya, tinjau rincian berbagi sumber daya, dan jika diperlukan, perbarui salah satu dari berikut ini:
 - a. (Opsional) Untuk mengubah nama berbagi sumber daya, edit Nama.
 - b. (Opsional) Untuk menambahkan sumber daya ke sumber daya berbagi, di bawah Sumber daya, pilih jenis sumber daya dan kemudian pilih kotak centang di sebelah sumber daya untuk menambahkannya ke berbagi sumber daya. Sumber daya global hanya akan muncul jika Anda mengatur Wilayah ke US East (N. Virginia), (us-east-1) dalam US East (N. Virginia us-east-1), (us-east-1) dalam AWS Management Console.
 - c. (Opsional) Untuk menghapus sumber daya dari berbagi sumber daya, cari sumber daya di bawah Sumber daya yang dipilih, lalu pilih X di samping ID sumber daya.
 - d. (Opsional) Untuk menambahkan tanda ke pembagian sumber daya, dalam tanda, masukkan tanda dan nilai dalam kotak teks kosong. Untuk menambahkan lebih dari satu kunci tanda dan pasangan nilai, pilih Tambahkan tanda baru. Anda dapat menambahkan hingga 50 tanda.
 - e. Untuk menghapus tag dari pangsa sumber daya, di bawah Tag, cari tag dan pilih Hapus di sebelahnya.
5. Pilih Selanjutnya.
6. (Opsional) Pada Langkah 2: Mengaitkan izin terkelola dengan setiap jenis sumber daya, Anda dapat memilih untuk mengaitkan izin terkelola yang dibuat AWS dengan jenis sumber daya, memilih izin terkelola pelanggan yang ada, atau Anda dapat membuat izin terkelola pelanggan sendiri. Untuk informasi selengkapnya, lihat [Jenis izin terkelola](#).


Anda juga dapat memilih Buat izin terkelola pelanggan untuk membuat izin terkelola pelanggan yang memenuhi persyaratan kasus penggunaan berbagi Anda. Untuk informasi selengkapnya, lihat [Membuat izin terkelola pelanggan](#). Setelah menyelesaikan proses,

pilih 

lalu Anda dapat memilih izin terkelola pelanggan baru dari daftar tarik-turun Izin terkelola.

Untuk menampilkan tindakan yang diizinkan oleh izin terkelola, luaskan Lihat templat kebijakan untuk izin terkelola ini.

7. Jika versi izin terkelola yang saat ini ditetapkan ke sumber daya bukan versi default saat ini, maka Anda dapat memperbarui ke versi default dengan memilih Pembaruan ke versi default.

 Note

Sampai Anda menyimpan perubahan Anda ke berbagi sumber daya setelah langkah terakhir, Anda dapat membatalkan pembaruan versi dengan memilih Kembalikan ke versi sebelumnya. Namun, untuk izin AWS terkelola, setelah Anda menyimpan pangsa sumber daya, perubahan bersifat final dan Anda tidak dapat lagi kembali ke versi sebelumnya.

8. Pilih Selanjutnya.
9. Pada Langkah 3: Pilih prinsipal yang diizinkan untuk mengakses, meninjau prinsip-prinsip yang dipilih, dan jika diperlukan, perbarui salah satu dari berikut ini:
 - a. (Opsional) Untuk mengubah apakah pembagian diaktifkan dengan prinsipal di dalam atau di luar organisasi Anda, pilih salah satu opsi berikut:
 - Untuk berbagi sumber daya dengan Akun AWS atau peran IAM individu atau pengguna yang berada di luar organisasi Anda, pilih Izinkan berbagi dengan prinsipal eksternal.
 - Untuk membatasi berbagi sumber daya hanya pada prinsipal di organisasi Anda AWS Organizations, pilih Izinkan berbagi dengan prinsipal di organisasi Anda saja.
 - b. Untuk Kepala Sekolah, lakukan hal berikut:
 - (Opsional) Untuk menambahkan organisasi, unit organisasi (OU), atau anggota Akun AWS di dalam organisasi Anda, aktifkan Tampilkan struktur organisasi untuk menampilkan tampilan pohon organisasi Anda. Kemudian pilih kotak centang di samping setiap pokok yang ingin Anda tambahkan.

⚠ Important

Ketika Anda berbagi dengan organisasi atau OU, dan ruang lingkup tersebut mencakup akun yang memiliki pangsa sumber daya, semua prinsipal di akun berbagi secara otomatis mendapatkan akses ke sumber daya dalam berbagi. Akses yang diberikan ditentukan oleh izin terkelola yang terkait dengan berbagi. Ini karena kebijakan berbasis sumber daya yang AWS RAM melekat pada setiap sumber daya dalam penggunaan saham "Principal": "*". Untuk informasi selengkapnya, lihat [Implikasi penggunaan "Principal": "*" dalam kebijakan berbasis sumber daya](#).

Prinsipal di akun konsumsi lainnya tidak segera mendapatkan akses ke sumber daya saham. Administrator akun lain harus terlebih dahulu melampirkan kebijakan izin berbasis identitas ke prinsipal yang sesuai. Kebijakan tersebut harus memberikan Allow akses ke ARN sumber daya individu dalam pangsa sumber daya. Izin dalam kebijakan tersebut tidak dapat melebihi yang ditentukan dalam izin terkelola yang terkait dengan berbagi sumber daya.

ℹ Note

Toggle struktur organisasi Tampilan hanya muncul jika berbagi dengan AWS Organizations diaktifkan dan Anda masuk sebagai kepala sekolah di akun manajemen organisasi.

Anda tidak dapat menggunakan metode ini untuk menentukan Akun AWS di luar organisasi Anda, atau peran IAM atau pengguna. Sebagai gantinya, Anda harus menambahkan prinsipal ini dengan memasukkan pengenalan mereka, yang ditampilkan di kotak teks di bawah sakelar struktur organisasi Tampilan. Lihat bullet.

- (Opsional) Untuk menambahkan prinsipal dengan pengenalnya, pilih jenis pokok dari daftar dropdown, lalu masukkan ID atau ARN untuk prinsipal. Terakhir, pilih Tambah.

Jika Anda memilih individu Akun AWS, maka hanya akun itu yang dapat mengakses pangsa sumber daya. Anda dapat memilih salah satu opsi berikut.

- LainAkun AWS (selain pemilik sumber daya) - Membuat sumber daya tersedia untuk akun lain. Administrator akun tersebut harus menyelesaikan proses dengan memberikan akses ke sumber daya bersama menggunakan kebijakan izin berbasis identitas untuk peran individu dan pengguna. Izin tersebut tidak dapat melebihi yang ditentukan dalam izin terkelola yang dilampirkan pada pangsa sumber daya.
- IniAkun AWS (pemilik sumber daya) — Semua peran dan pengguna di akun pemilik sumber daya secara otomatis menerima akses yang ditentukan oleh izin terkelola yang dilampirkan ke pangsa sumber daya.
- Penambahan segera muncul di daftar prinsip-prinsip yang dipilih.

Anda kemudian dapat menambahkan akun tambahan, OU, atau organisasi Anda dengan mengulangi langkah ini.

- (Opsional) Untuk menghapus kepala sekolah, cari di bawah Prinsipal yang dipilih, centang kotak, lalu pilih Batalkan pilihan.

10. Pilih Selanjutnya.

11. Pada Langkah 4: Tinjau dan perbarui, tinjau detail konfigurasi untuk berbagi sumber daya Anda.

12. Untuk mengubah konfigurasi untuk langkah apa pun, pilih tautan yang sesuai dengan langkah yang ingin Anda kembalikan, lalu buat perubahan yang diperlukan.

Jika ada izin terkelola yang masih menggunakan versi selain default, Anda memiliki kesempatan lain untuk mengatasinya dengan memilih Perbarui ke versi default.

13. Pilih Perbarui berbagi sumber daya setelah Anda selesai membuat perubahan.

AWS CLI

Untuk memperbarui berbagi sumber daya

Anda dapat menggunakan AWS CLI perintah berikut untuk memodifikasi pembagian sumber daya:

- Untuk mengganti nama pangsa sumber daya, atau mengubah apakah prinsipal eksternal diizinkan, gunakan perintah [update-resource-share](#). Contoh berikut mengganti nama share sumber daya yang ditentukan dan menetapkan untuk memungkinkan hanya prinsipal dari organisasinya. Anda harus menggunakan endpoint layanan untuk Wilayah AWS yang berisi berbagi sumber daya.

```
$ aws ram update-resource-share \
```

```

--region us-east-1 \
--resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE \
--name "my-renamed-resource-share" \
--no-allow-external-principals
{
  "resourceShare": {
    "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
    "name": "my-renamed-resource-share",
    "owningAccountId": "123456789012",
    "allowExternalPrincipals": false,
    "status": "ACTIVE",
    "creationTime": 1565295733.282,
    "lastUpdatedTime": 1565303080.023
  }
}

```

- Untuk menambahkan sumber daya ke berbagi sumber daya, gunakan perintah [associate-resource-share](#). Contoh berikut menambahkan subnet ke share sumber daya yang ditentukan.

```

$ aws ram associate-resource-share \
--region us-east-1 \
--resource-arns arn:aws:ec2:us-east-1:123456789012:subnet/
subnet-0250c25a1f4e15235 \
--resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE
{
  "resourceShareAssociations": [
    "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
    "associatedEntity": "arn:aws:ec2:us-east-1:123456789012:subnet/
subnet-0250c25a1f4e15235",
    "associationType": "RESOURCE",
    "status": "ASSOCIATING",
    "external": false
  ]
}

```

- Untuk menambah atau mengganti izin terkelola untuk jenis sumber daya dalam berbagi sumber daya, gunakan perintah [list-permissions](#) dan [associate-resource-share-permission](#). Anda hanya dapat menetapkan satu izin terkelola per jenis sumber daya dalam pembagian sumber daya.

Jika Anda mencoba menambahkan izin terkelola ke jenis sumber daya yang sudah memiliki izin terkelola, Anda harus menyertakan `--replace` opsi atau perintah gagal dengan kesalahan.

Contoh perintah berikut mencantumkan ARN untuk izin terkelola yang tersedia untuk subnet Amazon Elastic Compute Cloud (Amazon EC2), dan kemudian menggunakan salah satu ARN tersebut untuk menggantikan izin AWS terkelola yang saat ini ditetapkan untuk jenis sumber daya tersebut dalam berbagi sumber daya yang ditentukan.

```
$ aws ram list-permissions \
  --resource-type ec2:Subnet
{
  "permissions": [
    {
      "arn": "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionSubnet",
      "version": "1",
      "defaultVersion": true,
      "name": "AWSRAMDefaultPermissionSubnet",
      "resourceType": "ec2:Subnet",
      "creationTime": "2020-02-27T11:38:26.727000-08:00",
      "lastUpdatedTime": "2020-02-27T11:38:26.727000-08:00"
    }
  ]
}
$ aws ram associate-resource-share-permission \
  --region us-east-1 \
  --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-share/
f1d72a60-da19-4765-b4f9-e27b658b15b8 \
  --permission-arn arn:aws:ram::aws:permission/AWSRAMDefaultPermissionSubnet
{
  "returnValue": true
}
```

- Untuk menghapus sumber daya dari berbagi sumber daya, gunakan perintah [disassociate-resource-share](#). Contoh berikut menghapus subnet Amazon EC2 dengan ARN yang ditentukan dari pangsa sumber daya yang ditentukan.

```
$ aws ram disassociate-resource-share \
  --region us-east-1 \
  --resource-arns arn:aws:ec2:us-east-1:123456789012:subnet/
subnet-0250c25a1f4e15235 \
  --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE
```

```
{
  "resourceShareAssociations": [
    {
      "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
      "associatedEntity": "arn:aws:ec2:us-east-1:ubnet/
subnet-0250c25a1f4e15235",
      "associationType": "RESOURCE",
      "status": "DISASSOCIATING",
      "external": false
    }
  ]
}
```

- Untuk memodifikasi tag yang dilampirkan ke berbagi sumber daya, gunakan perintah [tag-resource](#) dan [untag-resource](#). Contoh berikut menambahkan tagproject=lima ke share sumber daya yang ditentukan.

```
$ aws ram tag-resource \
  --region us-east-1 \
  --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-share/
f1d72a60-da19-4765-b4f9-e27b658b15b8 \
  --tags key=project,value=lima
```

Contoh berikut menghapus tag dengan kunciproject dari share sumber daya yang ditentukan.

```
$ aws ram untag-resource \
  --region us-east-1 \
  --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-share/
f1d72a60-da19-4765-b4f9-e27b658b15b8 \
  --tag-keys=project
```

Perintah tanda tidak akan menghasilkan keluaran saat berhasil.

Melihat sumber daya bersama Anda diAWS RAM

Anda dapat melihat daftar sumber daya individual yang telah Anda bagikan, di semua saham sumber daya. Daftar ini membantu Anda menentukan sumber daya yang saat ini Anda bagikan, jumlah pembagian sumber daya yang disertakan, dan jumlah prinsipal yang memiliki akses ke mereka.

Console

Untuk melihat sumber daya yang saat ini Anda bagikan

1. Buka halaman [Shared by me: Shared resources](#) di AWS RAM konsol.
2. Karena AWS RAM sumber daya ada secara spesifik Wilayah AWS, pilih yang sesuai Wilayah AWS dari daftar dropdown di sudut kanan atas konsol. Untuk melihat sumber daya yang berisi sumber daya global, Anda harus mengatur Wilayah AWS ke US East (N. Virginia), (`us-east-1`). Untuk informasi selengkapnya tentang berbagi sumber daya global, lihat [Berbagi sumber daya Regional dibandingkan dengan sumber daya global](#).
3. Untuk setiap sumber daya bersama, informasi berikut tersedia:
 - ID Sumber Daya — ID dari sumber daya. Pilih ID sumber daya untuk membuka tab browser baru untuk melihat sumber daya di konsol layanan aslinya.
 - Tipe sumber daya - Tipe sumber daya.
 - Tanggal berbagi terakhir - Tanggal terakhir dibagikan sumber daya.
 - Saham sumber daya - Jumlah saham sumber daya yang menyertakan sumber daya. Untuk melihat daftar saham sumber daya, pilih nomornya.
 - Kepala Sekolah — Jumlah kepala sekolah yang dapat mengakses sumber daya. Pilih nilai untuk melihat prinsipal.

AWS CLI

Untuk melihat sumber daya yang saat ini Anda bagikan

Anda dapat menggunakan perintah [list-resources](#) dengan parameter yang `--resource-owner` disetel `SELF` untuk menampilkan detail sumber daya yang saat ini Anda bagikan.

Contoh berikut menunjukkan sumber daya yang disertakan dalam saham sumber daya di Wilayah AWS (`us-east-1`) untuk panggilan Akun AWS. Untuk mendapatkan sumber daya yang Anda bagikan di Wilayah yang berbeda, gunakan `--region <region-code>` parameter.

```
$ aws ram list-resources \
  --region us-east-1 \
  --resource-owner SELF
{
  "resources": [
    {
```

```
    "arn": "arn:aws:license-manager:us-east-1:123456789012:license-configuration:lic-ecbd5574fd92cb0d312baea260e4cece",
    "type": "license-manager:LicenseConfiguration",
    "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-share/818d71dd-7512-4f71-99c6-2ae57aa010bc",
    "creationTime": "2021-09-14T20:42:40.266000-07:00",
    "lastUpdatedTime": "2021-09-14T20:42:41.081000-07:00"
  },
  {
    "arn": "arn:aws:license-manager:us-east-1:123456789012:license-configuration:lic-ecbd5574fd92cb0d312baea260e4cece",
    "type": "license-manager:LicenseConfiguration",
    "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-share/a477f3b2-4001-4dcb-bd54-7c8d23b4f07d",
    "creationTime": "2021-07-22T11:48:11.104000-07:00",
    "lastUpdatedTime": "2021-07-22T11:48:11.971000-07:00"
  }
]
```

Melihat prinsip-prinsip yang Anda bagikan sumber daya AWS RAM

Anda dapat melihat prinsip-prinsip yang Anda bagikan sumber daya dengan, di semua saham sumber daya. Melihat daftar prinsipal ini membantu Anda menentukan siapa yang memiliki akses ke sumber daya bersama Anda.

Console

Untuk melihat prinsip-prinsip tempat Anda berbagi sumber daya

1. Arahkan ke halaman [Shared by me: Prinsipal](#) di AWS RAM konsol.
2. Karena AWS RAM sumber daya saham ada secara spesifik Wilayah AWS, pilih yang sesuai Wilayah AWS dari daftar dropdown di sudut kanan atas konsol. Untuk melihat saham sumber daya yang berisi sumber daya global, Anda harus mengatur Wilayah AWS ke US East (N. Virginia), (`us-east-1`). Untuk informasi selengkapnya tentang berbagi sumber daya global, lihat [Berbagi sumber daya Regional dibandingkan dengan sumber daya global](#).
3. Terapkan filter untuk menemukan prinsipal tertentu. Anda dapat menerapkan beberapa filter untuk mempersempit pencarian Anda. Pilih kotak teks untuk melihat daftar dropdown bidang atribut yang disarankan. Setelah Anda memilih salah satu, Anda dapat memilih dari daftar

nilai yang tersedia untuk bidang itu. Anda dapat menambahkan atribut atau kata kunci lain sampai Anda menemukan sumber daya yang Anda inginkan.

4. Untuk setiap kepala sekolah dalam daftar, konsol menampilkan informasi berikut:
 - ID Utama - ID kepala sekolah. Pilih ID untuk membuka tab browser baru untuk melihat prinsipal di konsol aslinya.
 - Saham sumber daya - Jumlah saham sumber daya yang Anda bagikan dengan pokok yang ditentukan. Pilih nomor untuk melihat daftar saham sumber daya.
 - Sumber Daya - Jumlah sumber daya yang Anda bagikan dengan kepala sekolah. Pilih nomor untuk melihat daftar sumber daya bersama.

AWS CLI

Untuk melihat prinsip-prinsip tempat Anda berbagi sumber daya

Anda dapat menggunakan perintah [list-principals](#) untuk mendapatkan daftar prinsipal yang Anda referensikan dalam pembagian sumber daya yang Anda buat saat ini Wilayah AWS untuk akun panggilan.

Contoh berikut mencantumkan prinsipal yang memiliki akses ke saham yang dibuat di Wilayah default untuk akun panggilan. Dalam contoh ini, prinsipal adalah organisasi akun panggilan dan terpisah Akun AWS, sebagai bagian dari dua saham sumber daya yang berbeda. Anda harus menggunakan endpoint layanan untuk Wilayah AWS yang berisi berbagi sumber daya.

```
$ aws ram list-principals \
  --region us-east-1 \
  --resource-owner SELF
{
  "principals": [
    {
      "id": "arn:aws:organizations::123456789012:organization/o-a1b2c3dr",
      "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-share/a477f3b2-4001-4dcb-bd54-7c8d23b4f07d",
      "creationTime": "2021-09-14T20:40:58.532000-07:00",
      "lastUpdatedTime": "2021-09-14T20:40:59.610000-07:00",
      "external": false
    },
    {
      "id": "111111111111",
```

```

    "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/6405fa7c-0786-4e15-8c9f-8aec02802f18",
    "creationTime": "2021-09-15T15:00:31.601000-07:00",
    "lastUpdatedTime": "2021-09-15T15:14:13.618000-07:00",
    "external": true
  }
]
}

```

Menghapus pangsa sumber daya diAWS RAM

Anda dapat menghapus berbagi sumber daya. Saat Anda menghapus pangsa sumber daya, semua prinsipal yang terkait dengan berbagi sumber daya kehilangan akses ke sumber daya bersama. Menghapus berbagi sumber daya tidak akan menghapus sumber daya bersama.

Untuk menghapus sumber AWS daya

Jika Anda perlu menghapus AWS sumber daya yang disertakan dalam berbagi sumber daya, AWS sarankan Anda terlebih dahulu memastikan bahwa Anda menghapus sumber daya dari setiap bagian sumber daya yang menyertakannya, atau menghapus pangsa sumber daya.

Pangsa sumber daya yang dihapus tetap terlihat diAWS RAM konsol untuk waktu yang singkat setelah penghapusan, tetapi statusnya berubah menjadi Deleted.

Console

Cara menghapus berbagi sumber daya

1. Buka halaman [Shared by me: Resource shares](#) diAWS RAM konsol.
2. KarenaAWS RAM sumber daya di sudut kanan atas konsol. Wilayah AWS Untuk melihat sumber daya yang berisi sumber daya yang berisi sumber daya yang berisi sumber daya, (us-east-1). Untuk informasi selengkapnya tentang berbagi


```
        "owningAccountId": "123456789012",
        "allowExternalPrincipals": true,
        "status": "ACTIVE",
        "creationTime": "2021-09-10T15:38:54.449000-07:00",
        "lastUpdatedTime": "2021-09-10T15:38:54.449000-07:00",
        "featureSet": "STANDARD"
    }
]
}
$ aws ram delete-resource-share \
  --region us-east-1 \
  --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/2ebe77d7-4156-4a93-87a4-228568d04425
{
  "returnValue": true
}
```

Akses AWS sumber daya yang dibagikan dengan Anda

Dengan AWS Resource Access Manager (AWS RAM), Anda dapat melihat pembagian sumber daya yang telah ditambahkan, sumber daya bersama yang dapat Anda akses, dan sumber daya Akun AWS yang telah dibagikan dengan Anda. Anda juga dapat meninggalkan pembagian sumber daya ketika Anda tidak lagi memerlukan akses ke sumber daya bersama.

Konten

- [Menerima dan menolak undangan berbagi sumber daya](#)
- [Melihat berbagi sumber daya yang dibagikan dengan Anda](#)
- [Melihat sumber daya yang dibagikan dengan Anda](#)
- [Lihat kepala sekolah berbagi dengan Anda](#)
- [Meninggalkan berbagi sumber daya](#)

Menerima dan menolak undangan berbagi sumber daya

Untuk mengakses sumber daya bersama, pemilik pembagian sumber daya harus menambahkan Anda sebagai prinsipal. Pemilik dapat menambahkan salah satu dari berikut ini sebagai prinsipal ke pembagian sumber daya.

- Organisasi di mana akun Anda menjadi anggota

- Unit organisasi (OU) yang berisi akun Anda
- Akun pribadi Anda
- Untuk jenis sumber daya yang didukung, peran atau pengguna IAM spesifik Anda


Jika Anda ditambahkan ke pembagian sumber daya melalui anggota organisasi AWS Organizations, dan berbagi dalam organisasi diaktifkan, maka Anda secara otomatis mendapatkan akses ke sumber daya bersama tanpa harus menerima undangan. Akun AWS Prinsipal layanan juga mendapatkan akses otomatis ke sumber daya bersama tanpa menerima undangan. Jika akun di mana Anda menerima akses kemudian dihapus dari organisasi, maka setiap prinsipal di akun itu secara otomatis kehilangan akses ke sumber daya yang diakses melalui pembagian sumber daya tersebut.

Jika Anda ditambahkan ke pembagian sumber daya oleh salah satu dari berikut ini, Anda menerima undangan untuk bergabung dengan pembagian sumber daya:

- Akun di luar organisasi Anda di AWS Organizations
- Akun di dalam organisasi Anda saat berbagi dengan tidak AWS Organizations diaktifkan

Jika Anda menerima undangan untuk bergabung dengan pembagian sumber daya, Anda harus menerimanya untuk mengakses sumber daya bersama. Jika Anda menolak undangan, Anda tidak dapat mengakses sumber daya bersama.

Untuk jenis sumber daya berikut, Anda memiliki waktu tujuh hari untuk menerima undangan bergabung dengan share untuk jenis sumber daya berikut. Jika Anda tidak menerima undangan sebelum kedaluwarsa, undangan secara otomatis ditolak.

 Important

Untuk jenis sumber daya bersama yang tidak ada dalam daftar berikut, Anda memiliki waktu 12 jam untuk menerima undangan untuk bergabung dengan pembagian sumber daya. Setelah 12 jam, undangan kedaluwarsa dan prinsipal pengguna akhir dalam pembagian sumber daya dipisahkan. Undangan tidak dapat lagi diterima oleh pengguna akhir.

- Amazon Aurora - kluster DB
- Amazon EC2 — reservasi kapasitas dan host khusus
- AWS License Manager - Konfigurasi lisensi

- AWS Outposts — Tabel rute gateway lokal, pos terdepan, dan situs
- Amazon Route 53 - Aturan penerusan
- Amazon VPC - Alamat IPv4 milik pelanggan, daftar awalan, subnet, target cermin lalu lintas, gateway transit, domain multicast gateway transit

Console

Untuk menanggapi undangan untuk berbagi sumber daya

1. Arahkan ke halaman [Berbagi dengan saya: Berbagi sumber daya](#) di AWS RAM konsol.
2. Karena pembagian AWS RAM sumber daya ada secara spesifik Wilayah AWS, pilih yang sesuai Wilayah AWS dari daftar tarik-turun di sudut kanan atas konsol. Untuk melihat pembagian sumber daya yang berisi sumber daya global, Anda harus mengatur Wilayah AWS ke US East (Virginia N.), (`us-east-1`). Untuk informasi selengkapnya tentang berbagi sumber daya global, lihat [Berbagi sumber daya Regional dibandingkan dengan sumber daya global](#).
3. Tinjau daftar pembagian sumber daya yang telah Anda tambahkan.

Kolom Status menunjukkan status partisipasi Anda saat ini untuk pembagian sumber daya. Pending Status menunjukkan bahwa Anda telah ditambahkan ke pembagian sumber daya, tetapi Anda belum menerima atau menolak undangan.

4. Untuk menanggapi undangan berbagi sumber daya, pilih ID berbagi sumber daya dan pilih Terima pembagian sumber daya untuk menerima undangan, atau Tolak pembagian sumber daya untuk menolak undangan. Jika Anda menolak undangan, Anda tidak mendapatkan akses ke sumber daya. Jika Anda menerima undangan, Anda mendapatkan akses ke sumber daya.

AWS CLI

Untuk menanggapi undangan untuk berbagi sumber daya

Anda dapat menggunakan perintah berikut untuk menerima atau menolak undangan untuk berbagi sumber daya:

- [get-resource-share-invitations](#)
- [accept-resource-share-invitation](#)
- [reject-resource-share-invitation](#)

1. Contoh berikut dimulai dengan menggunakan [get-resource-share-invitations](#) perintah untuk mengambil daftar semua undangan yang tersedia untuk pengguna. Akun AWS CLI queryParameter memungkinkan Anda membatasi output hanya untuk undangan tersebut dengan disetel ke. status PENDING Contoh ini menunjukkan satu undangan dari akun 111111111111 saat ini PENDING untuk akun saat ini dalam yang ditentukan. 123456789012 Wilayah AWS

```
$ aws ram get-resource-share-invitations \
  --region us-east-1 \
  --query 'resourceShareInvitations[?status==`PENDING`]'
{
  "resourceShareInvitations": [
    {
      "resourceShareInvitationArn": "arn:aws:ram:us-
east-1:111111111111:resource-share-invitation/3b3bc051-
fbf6-4336-8377-06c559dfee49",
      "resourceShareName": "Test TrngAcct Resource Share",
      "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/c4506c70-df75-4e6c-ac30-42ca03295a37",
      "senderAccountId": "111111111111",
      "receiverAccountId": "123456789012",
      "invitationTimestamp": "2021-09-21T08:56:24.977000-07:00",
      "status": "PENDING"
    }
  ]
}
```

2. Setelah Anda menemukan undangan yang ingin Anda terima, catat resourceShareInvitationArn di output yang akan digunakan dalam perintah berikutnya untuk menerima undangan.

```
$ aws ram accept-resource-share-invitation \
  --region us-east-1 \
  --resource-share-invitation-arn arn:aws:ram:us-east-1:111111111111:resource-
share-invitation/3b3bc051-fbf6-4336-8377-06c559dfee49
{
  "resourceShareInvitation": {
    "resourceShareInvitationArn": "arn:aws:ram:us-
east-1:111111111111:resource-share-invitation/3b3bc051-
fbf6-4336-8377-06c559dfee49",
    "resourceShareName": "Test TrngAcct Resource Share",
```

```

    "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-share/
c4506c70-df75-4e6c-ac30-42ca03295a37",
    "senderAccountId": "111111111111",
    "receiverAccountId": "123456789012",
    "invitationTimestamp": "2021-09-21T09:18:24.545000-07:00",
    "status": "ACCEPTED"
  }
}

```

Jika berhasil, perhatikan bahwa respons menunjukkan bahwa status telah berubah dari PENDING keACCEPTED.

Jika Anda ingin menolak undangan, jalankan [reject-resource-share-invitation](#) perintah, dengan parameter yang sama.

```

$ aws ram reject-resource-share-invitation \
  --region us-east-1 \
  --resource-share-invitation-arn arn:aws:ram:us-east-1:111111111111:resource-
share-invitation/3b3bc051-fbf6-4336-8377-06c559dfec49
{
  "resourceShareInvitation": {
    "resourceShareInvitationArn": "arn:aws:ram:us-east-1:111111111111:resource-
share-invitation/3b3bc051-fbf6-4336-8377-06c559dfec49",
    "resourceShareName": "Test TrngAcct Resource Share",
    "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-share/
c4506c70-df75-4e6c-ac30-42ca03295a37",
    "senderAccountId": "111111111111",
    "receiverAccountId": "123456789012",
    "invitationTimestamp": "2021-09-21T09:18:24.545000-07:00",
    "status": "REJECTED"
  }
}

```

Melihat berbagi sumber daya yang dibagikan dengan Anda

Anda dapat melihat saham sumber daya yang Anda miliki akses. Anda dapat melihat prinsipal mana yang berbagi sumber daya dengan Anda dan sumber daya mana yang mereka bagikan.

Console

Untuk melihat saham sumber daya

1. Arahkan ke halaman [Shared with me: Resource shares](#) di AWS RAM konsol.
2. Karena pembagian AWS RAM sumber daya tersedia secara spesifik Wilayah AWS, pilih yang sesuai Wilayah AWS dari daftar dropdown di sudut kanan atas konsol. Untuk melihat pembagian sumber daya yang berisi sumber daya global, Anda harus mengatur Wilayah AWS ke US East (N. Virginia), (us-east-1). Untuk informasi selengkapnya tentang pembagian sumber daya global, lihat [Berbagi sumber daya Regional dibandingkan dengan sumber daya global](#).
3. (Opsional) Terapkan filter untuk menemukan saham sumber daya tertentu. Anda dapat menerapkan beberapa filter untuk mempersempit pencarian Anda. Anda dapat mengetikkan kata kunci, seperti bagian dari nama berbagi sumber daya untuk hanya mencantumkan saham sumber daya yang menyertakan teks tersebut dalam nama. Pilih kotak teks untuk melihat daftar dropdown bidang atribut yang disarankan. Setelah Anda memilih salah satu, Anda dapat memilih dari daftar nilai yang tersedia untuk bidang itu. Anda dapat menambahkan atribut atau kata kunci lain sampai Anda menemukan sumber daya yang Anda inginkan.
4. AWS RAM Konsol menampilkan informasi berikut:
 - Nama — Nama pembagian sumber daya.
 - ID - ID berbagi sumber daya. Pilih ID untuk melihat halaman detail pembagian sumber daya.
 - Pemilik - ID Akun AWS yang membuat pangsa sumber daya.
 - Status — Status pembagian sumber daya saat ini. Nilai yang mungkin termasuk:
 - Active- Pangsa sumber daya aktif dan tersedia untuk digunakan.
 - Deleted— Pembagian sumber daya akan dihapus dan tidak lagi tersedia untuk digunakan.
 - Pending- Undangan untuk menerima bagian sumber daya sedang menunggu tanggapan.

AWS CLI

Untuk melihat saham sumber daya

Gunakan [get-resource-shares](#) perintah dengan `--resource-owner` parameter yang diatur ke `OTHER-ACCOUNTS`.

Contoh berikut menunjukkan daftar saham sumber daya yang dibagikan dalam yang ditentukan Wilayah AWS dengan akun panggilan oleh orang lain Akun AWS.

```
$ aws ram get-resource-shares \
  --region us-east-1 \
  --resource-owner OTHER-ACCOUNTS
{
  "resourceShares": [
    {
      "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
      "name": "Prod Env Shared Licenses",
      "owningAccountId": "111111111111",
      "allowExternalPrincipals": true,
      "status": "ACTIVE",
      "creationTime": "2021-09-21T08:50:41.308000-07:00",
      "lastUpdatedTime": "2021-09-21T08:50:41.308000-07:00",
      "featureSet": "STANDARD"
    },
    {
      "resourceShareArn": "arn:aws:ram:us-east-1:222222222222:resource-share/
c4506c70-df75-4e6c-ac30-42ca03295a37",
      "name": "Prod Env Shared Subnets",
      "owningAccountId": "222222222222",
      "allowExternalPrincipals": true,
      "status": "ACTIVE",
      "creationTime": "2021-09-21T08:56:24.737000-07:00",
      "lastUpdatedTime": "2021-09-21T08:56:24.737000-07:00",
      "featureSet": "STANDARD"
    }
  ]
}
```

Melihat sumber daya yang dibagikan dengan Anda

Anda dapat melihat sumber daya bersama yang dapat Anda akses. Anda dapat melihat prinsipal mana yang berbagi sumber daya dengan Anda dan saham sumber daya mana yang menyertakan sumber daya.

Console

Melihat sumber daya yang dibagikan dengan Anda

1. Arahkan ke halaman [Shared with me: Shared resources](#) di AWS RAM konsol.
2. Karena AWS RAM sumber daya akan tersedia secara spesifik Wilayah AWS, pilih yang sesuai Wilayah AWS dari daftar tarik-turun di sudut kanan atas konsol. Sumber daya akan tersedia di sudut kanan atas konsol. Untuk melihat sumber daya yang berisi daya global, Anda harus mengatur Wilayah AWS ke US East (N. Virginia), (`us-east-1`). Untuk informasi lebih lanjut tentang berbagi daya global, lihat [Berbagi sumber daya Regional dibandingkan dengan sumber daya global](#).
3. Terapkan filter untuk menemukan sumber daya bersama tertentu. Anda dapat menerapkan beberapa filter untuk mempersempit pencarian Anda.
4. Informasi berikut tersedia di tab Jaringan:
 - ID Sumber Daya — ID dari sumber daya. Pilih ID sumber daya untuk melihatnya di konsol layanannya.
 - Tipe daya — Tipe daya yang akan dibagikan.
 - Tanggal berbagi terakhir - Tanggal di mana sumber daya dibagikan dengan Anda.
 - Saham sumber daya - Jumlah saham sumber daya di mana sumber daya disertakan. Pilih nilai untuk melihat saham sumber daya.
 - ID pemilik daya — ID dari kepala daya yang memiliki daya yang dibagikan.

AWS CLI

Melihat sumber daya yang dibagikan dengan Anda

Anda dapat menggunakan perintah [list-resources](#) untuk melihat sumber daya yang dibagikan dengan Anda.

Perintah contoh berikut menampilkan rincian tentang sumber daya yang dapat diakses melalui share sumber daya di ditentukan Wilayah AWS dari yang lain Akun AWS.

```
$ aws ram list-resources \
  --region us-east-1 \
  --resource-owner OTHER-ACCOUNTS
```

```
{
  "resources": [
    {
      "arn": "arn:aws:license-manager:us-east-1:111111111111:license-configuration:lic-36be0485f5ae379cc74cf8e9242ab143",
      "type": "license-manager:LicenseConfiguration",
      "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-share/8b831ba0-63df-4608-be3c-19096b1ee16e",
      "status": "AVAILABLE",
      "creationTime": "2021-09-21T08:50:41.308000-07:00",
      "lastUpdatedTime": "2021-09-21T08:50:42.517000-07:00"
    }
  ]
}
```

Lihat kepala sekolah berbagi dengan Anda

Anda dapat melihat daftar semua prinsipal yang berbagi sumber daya dengan Anda. Anda dapat melihat sumber daya dan sumber daya yang dibagikan dengan Anda.

Console

Untuk melihat prinsip-prinsip yang berbagi sumber daya dengan Anda

1. Buka konsol AWS RAM di <https://console.aws.amazon.com/ram>.
2. Karena AWS RAM sumber daya tersedia secara spesifik Wilayah AWS, pilih yang sesuai Wilayah AWS dari daftar tarik-turun di sudut kanan atas konsol. Untuk melihat saham sumber daya yang berisi sumber daya global, Anda harus mengatur Wilayah AWS ke US East (N. Virginia), (`us-east-1`). Untuk informasi selengkapnya tentang berbagi sumber daya global, lihat [Berbagi sumber daya Regional dibandingkan dengan sumber daya global](#).
3. Di panel navigasi, pilih Dibagikan dengan saya, Kepala Sekolah.
4. (Opsional) Anda dapat menerapkan filter untuk menemukan prinsipal tertentu. Anda dapat menerapkan beberapa filter untuk mempersempit pencarian Anda.
5. Konsol menampilkan informasi berikut:
 - ID Utama - ID kepala sekolah yang berbagi dengan Anda.
 - Saham sumber daya - Jumlah saham sumber daya yang ditambahkan oleh prinsipal kepada Anda. Pilih nomor untuk melihat daftar saham sumber daya.

- Sumber daya - Jumlah sumber daya yang dibagikan oleh kepala sekolah dengan Anda. Pilih nilai untuk melihat daftar sumber daya.

AWS CLI

Untuk melihat prinsip-prinsip yang berbagi sumber daya dengan Anda

Anda dapat menggunakan perintah [list-principals](#) untuk mengambil daftar prinsipal yang berbagi sumber daya dengan AndaAkun AWS.

Contoh perintah berikut menampilkan rincian tentangAkun AWS yang berbagi berbagi sumber daya dengan akun yang digunakan untuk memanggil operasi dalam ditentukanWilayah AWS.

```
$ aws ram list-principals \
  --region us-east-1 \
  --resource-owner OTHER-ACCOUNTS
{
  "principals": [
    {
      "id": "111111111111",
      "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
      "creationTime": "2021-09-21T08:50:41.308000-07:00",
      "lastUpdatedTime": "2021-09-21T09:06:25.545000-07:00",
      "external": true
    }
  ]
}
```

Meninggalkan berbagi sumber daya

Jika Anda tidak lagi memerlukan akses ke sumber daya yang dibagikan dengan Anda, Anda dapat meninggalkan pembagian sumber daya kapan saja. Saat Anda meninggalkan pembagian sumber daya, Anda kehilangan akses ke sumber daya bersama.

Prasyarat untuk meninggalkan pembagian sumber daya

- Anda dapat meninggalkan pembagian sumber daya hanya jika dibagikan dengan Anda sebagai individu Akun AWS dan bukan dalam konteks organisasi. Anda tidak dapat meninggalkan

pembagian sumber daya jika ditambahkan ke Akun AWS dalamnya oleh bagian dalam organisasi Anda dan berbagi dengan AWS Organizations diaktifkan. Akses ke pembagian sumber daya dalam suatu organisasi bersifat otomatis.

- Untuk meninggalkan pembagian sumber daya, verifikasi bahwa pembagian sumber daya kosong atau hanya berisi jenis sumber daya yang mendukung meninggalkan berbagi.

Berikut ini adalah satu-satunya jenis sumber daya yang mendukung meninggalkan berbagi sumber daya.

| Layanan | Tipe sumber daya |
|---------------------|--|
| Amazon Aurora | <code>rds:Cluster</code> |
| Amazon EC2 | <code>ec2:CapacityReservation</code> <code>ec2:DedicatedHost</code> |
| AWS License Manager | <code>license-manager:LicenseConfiguration</code> |
| AWS Outposts | <code>ec2:LocalGatewayRouteTable</code> <code>outposts:Outpost</code> <code>outposts:Site</code> |
| Amazon Route 53 | <code>route53resolver:ResolverRule</code> |
| Amazon VPC | <code>ec2:CoipPool</code> <code>ec2:PrefixList</code> <code>ec2:Subnet</code> <code>ec2:TrafficMirrorTarget</code> <code>ec2:TransitGateway</code> <code>ec2:TransitGatewayMulticastDomain</code> |

Cara meninggalkan pembagian sumber daya

Console

Untuk meninggalkan pembagian sumber daya

1. Arahkan ke halaman [Berbagi dengan saya: Berbagi sumber daya](#) di AWS RAM konsol.
2. Karena pembagian AWS RAM sumber daya ada secara spesifik Wilayah AWS, pilih yang sesuai Wilayah AWS dari daftar tarik-turun di sudut kanan atas konsol. Untuk melihat pembagian sumber daya yang berisi sumber daya global, Anda harus mengatur Wilayah AWS ke US East (Virginia N.), (`us-east-1`). Untuk informasi selengkapnya tentang berbagi sumber daya global, lihat [Berbagi sumber daya Regional dibandingkan dengan sumber daya global](#).
3. Pilih pembagian sumber daya yang ingin Anda tinggalkan.
4. Pilih Tinggalkan berbagi sumber daya, dan di kotak dialog konfirmasi, pilih Tinggalkan.

AWS CLI

Untuk meninggalkan pembagian sumber daya

Anda dapat menggunakan [disassociate-resource-share](#) perintah untuk meninggalkan pembagian sumber daya.

Contoh perintah berikut menyebabkan Akun AWS yang memanggil perintah kehilangan akses ke sumber daya yang dibagikan oleh pembagian sumber daya yang ditentukan oleh ARN. Anda harus mengarahkan permintaan ke titik akhir layanan di Wilayah AWS yang berisi pembagian sumber daya yang ingin Anda tinggalkan.

1. Pertama, ambil daftar pembagian sumber daya untuk mengambil ARN dari pembagian sumber daya yang ingin Anda tinggalkan.

```
$ aws ram get-resource-shares \
  --region us-east-1 \
  --resource-owner OTHER-ACCOUNTS
{
  "resourceShares": [
    {
      "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
```

```

        "name": "Prod Environment Shared Licenses",
        "owningAccountId": "111111111111",
        "allowExternalPrincipals": true,
        "status": "ACTIVE",
        "creationTime": "2021-09-21T08:50:41.308000-07:00",
        "lastUpdatedTime": "2021-09-21T08:50:41.308000-07:00",
        "featureSet": "STANDARD"
    }
]
}

```

2. Kemudian, Anda dapat menjalankan perintah untuk meninggalkan pembagian sumber daya itu. Perhatikan bahwa Anda juga harus menentukan ID akun Anda, 123456789012, sebagai kepala sekolah untuk memisahkan dari pembagian sumber daya yang ditentukan, yang dibagikan oleh akun 111111111111.

```

$ aws ram disassociate-resource-share \
  --region us-east-1 \
  --resource-share-arn arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e \
  --principals 123456789012
    {
      "resourceShareAssociations": [
        {
          "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
          "associatedEntity": "123456789012",
          "associationType": "PRINCIPAL",
          "status": "DISASSOCIATING",
          "external": false
        }
      ]
    }
}

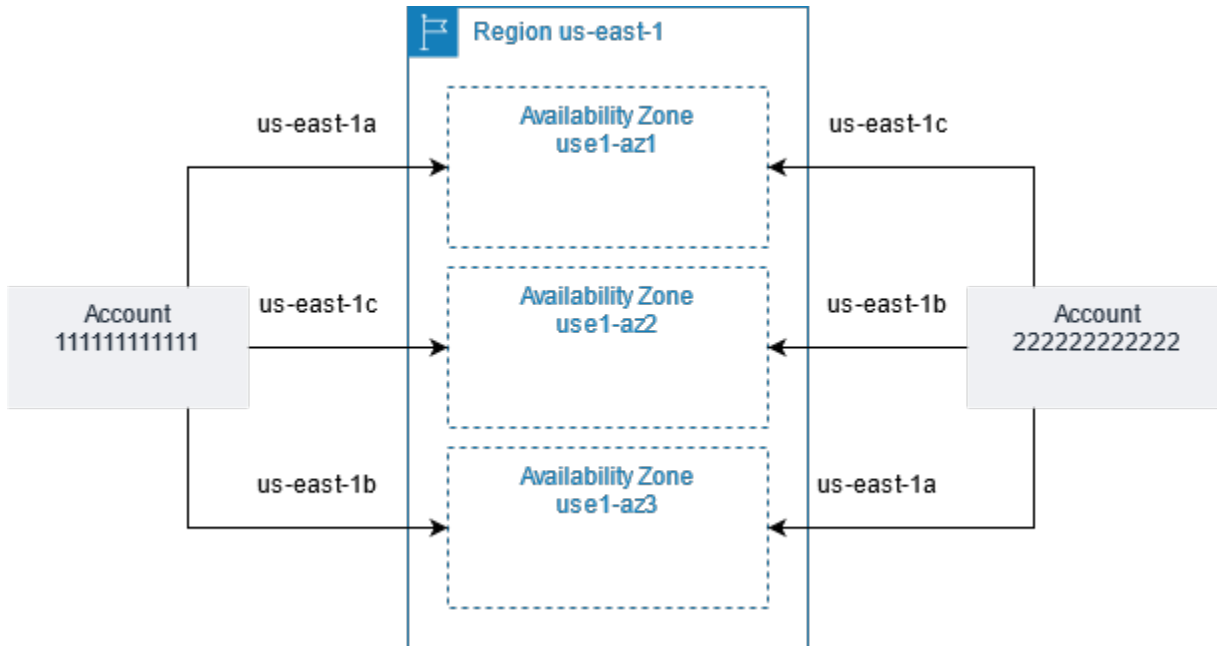
```

ID Availability Zone untuk AWS sumber daya Anda

AWS memetakan Availability Zone fisik secara acak ke nama Availability Zone untuk masing-masing Akun AWS. Pendekatan ini membantu mendistribusikan sumber daya di seluruh Availability Zone di Wilayah AWS, alih-alih sumber daya yang mungkin terkonsentrasi di Availability Zone “a” untuk setiap Wilayah. Akibatnya, Availability Zone us-east-1a untuk AWS akun Anda mungkin

tidak mewakili lokasi fisik yang sama dengan AWS akun yang berbeda. `us-east-1a` Untuk informasi selengkapnya, lihat [Wilayah dan Availability Zone](#) di Panduan Pengguna Amazon EC2.

Ilustrasi berikut menunjukkan bagaimana ID AZ sama untuk setiap akun meskipun nama Availability Zone dapat memetakan secara berbeda untuk setiap akun.



Untuk beberapa sumber daya, Anda harus mengidentifikasi tidak hanya Wilayah AWS, tetapi juga Availability Zone. Misalnya, subnet Amazon VPC. Dalam satu akun, pemetaan Availability Zone ke nama tertentu tidak penting. Tetapi, ketika Anda menggunakan AWS RAM untuk berbagi sumber daya seperti itu dengan yang lain Akun AWS, pemetaan itu penting. Pemetaan acak ini mempersulit kemampuan akun mengakses sumber daya bersama untuk mengetahui Availability Zone mana yang akan direferensikan. Untuk membantu hal ini, sumber daya tersebut juga memungkinkan Anda mengidentifikasi lokasi sebenarnya dari sumber daya Anda relatif terhadap akun Anda dengan menggunakan ID AZ. ID AZ adalah pengenal unik dan konsisten untuk Availability Zone di semua Akun AWS. Misalnya, `use1-az1` adalah ID AZ untuk Availability Zone di `us-east-1` Wilayah dan mewakili lokasi fisik yang sama di setiap AWS akun.

Anda dapat menggunakan ID AZ untuk menentukan lokasi sumber daya di satu akun relatif terhadap sumber daya di akun lain. Misalnya, jika Anda membagikan subnet di Availability Zone dengan ID AZ `use1-az2` dengan akun lain, subnet ini tersedia untuk akun tersebut di Availability Zone yang juga memiliki ID AZ yang juga `use1-az2`. ID AZ untuk setiap subnet ditampilkan di konsol Amazon VPC, dan dapat ditanya menggunakan AWS CLI.

Console

Untuk melihat ID AZ untuk Availability Zone di akun Anda

1. Arahkan ke halaman [AWS RAM konsol](#) di AWS RAM konsol.
2. Anda dapat melihat ID AZ untuk arusnya di Wilayah AWS bawah ID AZ Anda.

AWS CLI

Untuk melihat ID AZ untuk Availability Zone di akun Anda

Perintah contoh berikut menunjukkan ID AZ untuk Availability Zone di Wilayah us-west-2 dan bagaimana mereka dipetakan untuk panggilan Akun AWS.




```
$ aws ec2 describe-availability-zones \
  --region us-west-2
{
  "AvailabilityZones": [
    {
      "State": "available",
      "OptInStatus": "opt-in-not-required",
      "Messages": [],
      "RegionName": "us-west-2",
      "ZoneName": "us-west-2a",
      "ZoneId": "usw2-az2",
      "GroupName": "us-west-2",
      "NetworkBorderGroup": "us-west-2",
      "ZoneType": "availability-zone"
    },
    {
      "State": "available",
      "OptInStatus": "opt-in-not-required",
      "Messages": [],
      "RegionName": "us-west-2",
      "ZoneName": "us-west-2b",
      "ZoneId": "usw2-az1",
      "GroupName": "us-west-2",
      "NetworkBorderGroup": "us-west-2",
      "ZoneType": "availability-zone"
    },
    {
      "State": "available",
```






```
    "OptInStatus": "opt-in-not-required",
    "Messages": [],
    "RegionName": "us-west-2",
    "ZoneName": "us-west-2c",
    "ZoneId": "usw2-az3",
    "GroupName": "us-west-2",
    "NetworkBorderGroup": "us-west-2",
    "ZoneType": "availability-zone"
  },
  {
    "State": "available",
    "OptInStatus": "opt-in-not-required",
    "Messages": [],
    "RegionName": "us-west-2",
    "ZoneName": "us-west-2d",
    "ZoneId": "usw2-az4",
    "GroupName": "us-west-2",
    "NetworkBorderGroup": "us-west-2",
    "ZoneType": "availability-zone"
  }
]
}
```

Sumber daya yang dapat dibagikan AWS

Dengan AWS Resource Access Manager (AWS RAM), Anda dapat berbagi sumber daya yang dibuat dan dikelola oleh orang lain Layanan AWS. Anda dapat berbagi sumber daya dengan individu Akun AWS. Anda juga dapat berbagi sumber daya dengan akun di organisasi atau unit organisasi (OU) di AWS Organizations. Beberapa jenis sumber daya yang didukung juga memungkinkan Anda berbagi sumber daya dengan peran individu AWS Identity and Access Management (IAM) dan pengguna.

Bagian berikut mencantumkan jenis sumber daya, dikelompokkan berdasarkan Layanan AWS, yang dapat Anda bagikan dengan menggunakan AWS RAM. Kolom dalam tabel menentukan fitur mana yang didukung oleh setiap jenis sumber daya:

| | | |
|---|---|-------|
| Dapat berbagi dengan pengguna dan peran IAM |  <p>— Anda dapat berbagi sumber daya jenis ini dengan peran individu AWS Identity and Access Management (IAM) dan pengguna, selain akun.</p> | Ya |
| |  <p>- Anda dapat berbagi sumber daya jenis ini hanya dengan akun.</p> | Tidak |
| Dapat berbagi dengan akun di luar organisasinya |  <p>— Anda hanya dapat berbagi sumber daya jenis ini dengan akun individu, di dalam atau di luar organisasinya. Lihat Pertimbangan untuk informasi lebih lanjut.</p> | Ya |

| | | |
|---|--|-----------------|
| |  <p>- Anda dapat berbagi sumber daya jenis ini hanya dengan akun yang merupakan anggota dari organisasi yang sama.</p> | Tidak |
| <p>Dapat menggunakan izin yang dikelola pelanggan</p> | <p>Semua jenis sumber daya yang didukung oleh izin AWS terkelola AWS RAM dukungan, tetapi Ya di kolom ini berarti bahwa izin terkelola pelanggan juga didukung untuk jenis sumber daya ini.</p>  <p>— sumber daya jenis ini mendukung penggunaan izin yang dikelola pelanggan.</p>  <p>- sumber daya jenis ini tidak mendukung penggunaan izin yang dikelola pelanggan.</p> | Ya |
| <p>Dapat berbagi dengan prinsipal layanan</p> |  <p>- Anda dapat berbagi sumber daya jenis ini dengan Layanan AWS.</p>  <p>- Anda tidak dapat berbagi sumber daya jenis ini dengan Layanan AWS.</p> | Ya Tidak |





AWS App Mesh

Anda dapat membagikan AWS App Mesh sumber daya berikut dengan menggunakan AWS RAM.

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|----------------------------|---|---|---|---|---|
| Mesh apppmesh:Mesh | Buat dan kelola mesh secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Sebuah mesh bersama memungkinkan sumber daya yang dibuat oleh berbeda Akun AWS untuk berkomunikasi satu sama lain dalam mesh yang sama. Untuk informasi selengkapnya, lihat Bekerja dengan jerat bersama di Panduan AWS App Mesh Pengguna. |  Y |  Y Dapat berbagi dengan apa saja Akun AWS. |  T |  Tidak |

AWS AppSync GraphQL API

Anda dapat membagikan resource API AWS AppSync GraphQL berikut dengan menggunakan. AWS RAM

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|-------------------------------------|---|--|--|--|--|
| <p>API GraphQL appsync:Apis</p> | <p>Kelola API AWS AppSync GraphQL secara terpusat, dan bagikan dengan Akun AWS orang lain atau organisasi Anda. Ini memungkinkan beberapa akun berbagi AWS AppSync API sebagai bagian dari pembuatan API AWS AppSync Gabungan terpadu yang dapat mengakses data dari beberapa API subskema di berbagai akun di Wilayah yang sama. Untuk informasi selengkapnya, lihat API yang digabungkan di Panduan AWS AppSync Pengembang.</p> | <p> Y</p> | <p> Y Dapat berbagi dengan apa saja Akun AWS.</p> | <p> Y</p> | <p> Tidak</p> |




Amazon Aurora

Anda dapat membagikan sumber daya Amazon Aurora berikut dengan menggunakan AWS RAM

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|----------------------------|--|---|---|---|---|
| Kluster DB rds:Cluster | Buat dan kelola cluster DB secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan beberapa Akun AWS kloning cluster DB bersama yang dikelola secara terpusat. Untuk informasi selengkapnya, lihat Kloning lintas akun dengan AWS RAM dan Amazon Aurora di Panduan Pengguna Amazon Aurora . |  T |  Y Dapat berbagi dengan apa saja Akun AWS. |  T |  Tidak |


AWS Private Certificate Authority

Anda dapat membagikan AWS Private CA sumber daya berikut dengan menggunakan AWS RAM.

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|--|--|---|---|--|---|
| <p>Otoritas sertifikat swasta (CA)</p> <p>acm-pca:CertificateAuthority</p> | <p>Buat dan kelola otoritas sertifikat pribadi (CA) untuk infrastruktur kunci publik internal (PKI) organisasi Anda, dan bagikan CA tersebut dengan orang lain Akun AWS atau organisasi Anda. Hal ini memungkinkan AWS Certificate Manager pengguna di akun lain mengeluarkan sertifikat X.509 yang ditandatangani oleh CA bersama Anda. Untuk informasi selengkapnya, lihat Mengontrol akses ke CA pribadi di Panduan AWS Private Certificate Authority Pengguna.</p> | <p> Ya</p> | <p> Ya</p> <p>Dapat berbagi dengan apa saja Akun AWS.</p> | <p> Tidak</p> | <p> Ya</p> |









Amazon DataZone

Anda dapat membagikan DataZone sumber daya berikut dengan menggunakan AWS RAM.

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|-------------------------------------|--|---|--|---|---|
| DataZone Domain datazone: Domain | Buat dan kelola domain secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan beberapa akun membuat DataZone domain Amazon. Untuk informasi selengkapnya, lihat Apa itu Amazon DataZone di Panduan DataZone Pengguna Amazon. |  Tidak |  Ya Dapat berbagi dengan apa saja Akun AWS. |  Tidak |  Tidak |

AWS CodeBuild





Anda dapat membagikan AWS CodeBuild sumber daya berikut dengan menggunakan AWS RAM.

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|---|---|---|---|---|---|
| <p>Proyek</p> <p><code>codebuild:Project</code></p> | <p>Buat proyek, dan gunakan untuk menjalankan build. Bagikan proyek dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan beberapa Akun AWS dan pengguna melihat informasi tentang proyek dan menganalisis build-nya. Untuk informasi selengkapnya, lihat Bekerja dengan proyek bersama di Panduan Pengguna AWS CodeBuild Pengguna.</p> |  Y |  Y Dapat berbagi dengan apa saja Akun AWS. |  Y |  Tidak |
| <p>Kelompok laporan</p> <p><code>codebuild:ReportGroup</code></p> | <p>Buat grup laporan, dan gunakan untuk membuat laporan saat Anda membangun proyek. Bagikan grup laporan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan</p> |  Y |  Y Dapat berbagi dengan apa saja Akun AWS. |  Y |  Tidak |

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasi | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|----------------------------|--|---|--|--|---|
| | <p>kan beberapa Akun AWS dan pengguna melihat grup laporan dan laporannya, serta hasil kasus uji untuk setiap laporan. Laporan dapat dilihat selama 30 hari setelah dibuat, dan kemudian kedaluwarsa dan tidak lagi tersedia untuk dilihat. Untuk informasi selengkapnya, lihat Bekerja dengan proyek bersama di Panduan AWS CodeBuild Pengguna.</p> | | | | |

Amazon EC2

Anda dapat membagikan sumber daya Amazon EC2 berikut dengan menggunakan AWS RAM

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|---|---|--|--|--|--|
| <p>Reservasi Kapasitas</p> <p>ec2:CapacityReservation</p> | <p>Buat dan kelola reservasi kapasitas secara terpusat, dan bagikan kapasitas cadangan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan beberapa Akun AWS peluncuran instans Amazon EC2 mereka ke dalam kapasitas cadangan yang dikelola secara terpusat. Untuk informasi selengkapnya, lihat Bekerja dengan Reservasi Kapasitas bersama di Panduan Pengguna Amazon EC2.</p> <div style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; margin-top: 20px;"> <p>⚠ Important</p> <p>Jika Anda tidak memenuhi semua prasyarat untuk berbagi reservasi</p> </div> | <p style="text-align: center;"> T</p> | <p style="text-align: center;"> Y</p> <p>Dapat berbagi dengan apa saja Akun AWS.</p> | <p style="text-align: center;"> T</p> | <p style="text-align: center;"> Tidak</p> |

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|----------------------------|---|---|---|--|---|
| | <p>kapasitas, maka operasi berbagi dapat gagal. Jika ini terjadi dan pengguna mencoba meluncurkan instans Amazon EC2 ke dalam reservasi kapasitas tersebut, instans tersebut diluncurkan sebagai instans sesuai permintaan yang dapat menghasilkan biaya lebih tinggi. Kami menyarankan Anda memverifikasi bahwa Anda dapat mengakses reservasi kapasitas</p> | | | | |


| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasi | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|----------------------------|---|---|--|--|---|
| | <p>bersama dengan mencoba melihatnya di konsol Amazon EC2. Anda juga dapat memantau pembagian sumber daya yang gagal sehingga Anda dapat mengambil tindakan korektif sebelum pengguna meluncurkan instance dengan cara yang meningkatkan biaya Anda. Untuk informasi selengkapnya, lihat Contoh: Memberi tahu kegagalan</p> | | | | |

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan lainnya |
|----------------------------------|--|---|---|---|---|
| | pembagian sumber daya. | | | | |
| Host Khusus ec2:DedicatedHost | Alokasikan dan kelola host khusus Amazon EC2 secara terpusat, dan bagikan kapasitas instans host dengan orang Akun AWS lain atau organisasi Anda. Ini memungkinkan beberapa kali Akun AWS meluncurkan instans Amazon EC2 mereka ke host khusus yang dikelola secara terpusat. Untuk informasi selengkapnya, lihat Bekerja dengan Host Khusus bersama di Panduan Pengguna Amazon EC2. |  T |  Y Dapat berbagi dengan apa saja Akun AWS. |  T |  Tidak |

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan lainnya |
|--|--|---|---|---|---|
| Grup penempatan <code>ec2:PlacementGroup</code> | Bagikan grup penempatan yang Anda miliki di seluruh Akun AWS, baik di dalam maupun di luar organisasi Anda. Anda dapat meluncurkan instans Amazon EC2 dari akun mana pun yang Anda bagikan ke grup penempatan bersama. Untuk informasi selengkapnya, lihat Berbagi grup penempatan di Panduan Pengguna Amazon EC2. |  Y |  Y Dapat berbagi dengan apa saja Akun AWS. |  T |  Tidak |





EC2 Image Builder

Anda dapat membagikan sumber daya EC2 Image Builder berikut dengan AWS RAM menggunakan.

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|---|--|--|---|--|--|
| <p>Komponen-komponen <code>imagebuilder:Component</code></p> | <p>Buat dan kelola komponen secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Kelola siapa yang dapat menggunakan komponen build dan pengujian yang telah ditentukan sebelumnya dalam resep gambar mereka. Untuk informasi selengkapnya, lihat Membagikan sumber daya EC2 Image Builder di Panduan Pengguna EC2 Image Builder.</p> | <p> Y</p> | <p> Y Dapat berbagi dengan apa saja Akun AWS.</p> | <p> Y</p> | <p> Tidak</p> |
| <p>tanda terima kontainer <code>imagebuilder:ContainerRecipe</code></p> | <p>Buat dan kelola resep kontainer Anda secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan Anda untuk mengelola siapa</p> | <p> Y</p> | <p> Y Dapat berbagi dengan apa saja</p> | <p> Y</p> | <p> Tidak</p> |





| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasi | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|----------------------------|---|---|--|--|---|
| | <p>yang dapat menggunakan dokumen yang telah ditentukan untuk menduplikasi build gambar kontainer . Untuk informasi selengkapnya, lihat Membagikan sumber daya EC2 Image Builder di Panduan Pengguna EC2 Image Builder.</p> | | Akun AWS. | | |

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasi | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|-----------------------------|--|---|---|---|---|
| Citra imagebuilder:Image | Buat dan kelola gambar emas Anda secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Kelola siapa yang dapat menggunakan gambar yang dibuat dengan EC2 Image Builder di seluruh organisasi Anda. Untuk informasi selengkapnya, lihat Membagikan sumber daya EC2 Image Builder di Panduan Pengguna EC2 Image Builder. |  Y |  Y Dapat berbagi dengan apa saja Akun AWS. |  Y |  Tidak |

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan lainnya |
|--|--|---|---|---|---|
| Tanda terima citra imagebuilder:ImageRecipe | Buat dan kelola resep gambar Anda secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan Anda mengelola siapa yang dapat menggunakan dokumen yang telah ditentukan untuk menduplikasi build AMI. Untuk informasi selengkapnya, lihat Membagikan sumber daya EC2 Image Builder di Panduan Pengguna EC2 Image Builder. |  Y |  Y Dapat berbagi dengan apa saja Akun AWS. |  Y |  Tidak |

Amazon FSx for OpenZFS

Anda dapat membagikan Amazon FSx berikut untuk sumber daya OpenZFS dengan menggunakan AWS RAM





| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|----------------------------|---|---|---|---|---|
| Volume FSx fsx:Volume | Buat dan kelola FSx untuk volume OpenZFS secara terpusat, dan bagikan dengan orang lain atau organisasi Anda. Akun AWS Ini memungkinkan beberapa akun melakukan replikasi data menggunakan OpenZfs snapshot di bawah volume bersama melalui FSx API atau <code>CreateVolume CopySnapshotAndUpdateVolume</code> Untuk informasi selengkapnya, lihat Replikasi data sesuai permintaan di Amazon FSx for OpenZFS User Guide. |  Y |  Y Dapat berbagi dengan apa saja Akun AWS. |  Y |  Tidak |

AWS Glue

Anda dapat membagikan AWS Glue sumber daya berikut dengan menggunakan AWS RAM.





| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|--|---|--|--|--|--|
| <p>Katalog data</p> <p><code>glue:Catalog</code></p> | <p>Kelola katalog data pusat, dan bagikan metadata tentang database dan tabel dengan Akun AWS atau organisasi Anda. Ini memungkinkan pengguna untuk menjalankan kueri pada data di beberapa akun. Untuk informasi selengkapnya, lihat Berbagi Tabel Katalog Data dan Database di Seluruh AWS Akun di Panduan AWS Lake Formation Pengembangan.</p> | <p> T</p> | <p> Y</p> <p>Dapat berbagi dengan apa saja Akun AWS.</p> | <p> T</p> | <p> Tidak</p> |
| <p>Basis Data</p> <p><code>glue:Database</code></p> | <p>Buat dan kelola database katalog data secara terpusat, dan bagikan dengan Akun AWS atau organisasi Anda. Database adalah kumpulan tabel katalog data. Ini memungkinkan pengguna untuk</p> | <p> T</p> | <p> Y</p> <p>Dapat berbagi dengan apa saja Akun AWS.</p> | <p> T</p> | <p> Tidak</p> |

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasi | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|----------------------------|--|---|--|--|---|
| | menjalankan kueri dan mengekstrak, mengubah, dan memuat (ETL) pekerjaan yang dapat bergabung dan menanyakan data di beberapa akun. Untuk informasi selengkapnya, lihat Berbagi Tabel Katalog Data dan Database di Seluruh AWS Akun di Panduan AWS Lake Formation Pengembang. | | | | |

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan lainnya |
|----------------------------------|--|---|---|---|---|
| Tabel <code>glue:Table</code> | <p>Buat dan kelola tabel katalog data secara terpusat, dan bagikan dengan Akun AWS atau organisasi Anda. Tabel katalog data berisi metadata tentang tabel data di Amazon S3, sumber data JDBC, Amazon Redshift, sumber streaming, dan penyimpanan data lainnya. Ini memungkinkan pengguna untuk menjalankan kueri dan pekerjaan ETL yang dapat bergabung dan menanyakan data di beberapa akun. Untuk informasi selengkapnya, lihat Berbagi Tabel Katalog Data dan Database di Seluruh AWS Akun di Panduan AWS Lake Formation Pengembang.</p> |  T |  Y Dapat berbagi dengan apa saja Akun AWS. |  T |  Tidak |





AWS License Manager

Anda dapat membagikan AWS License Manager sumber daya berikut dengan menggunakan AWS RAM.

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasi | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|--|---|---|--|---|---|
| Konfigurasi lisensi <code>license-manager:LicenseConfiguration</code> | Buat dan kelola konfigurasi lisensi secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan Anda menegakkan aturan lisensi yang dikelola secara terpusat yang didasarkan pada ketentuan perjanjian perusahaan Anda di beberapa. Akun AWS Untuk informasi selengkapnya, lihat Konfigurasi lisensi di License Manager di Panduan Pengguna License Manager. |  Tidak |  Ya Dapat berbagi dengan apa saja Akun AWS. |  Tidak |  Tidak |





AWS Marketplace

Anda dapat membagikan AWS Marketplace sumber daya berikut dengan menggunakan AWS RAM.

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|--|--|---|---|---|---|
| Entitas Katalog Marketplace <code>aws-marketplace:Entity</code> | Buat, kelola, dan bagikan entitas di seluruh Akun AWS atau di organisasi Anda di AWS Marketplace. Untuk informasi selengkapnya, lihat Berbagi sumber daya AWS RAM di AWS Marketplace Catalog API Referensi . |  Y |  Y Dapat berbagi dengan apa saja Akun AWS. |  T |  Tidak |

AWS Migration Hub Refactor Spaces

Anda dapat membagikan AWS Migration Hub Refactor Spaces sumber daya berikut dengan menggunakan AWS RAM.

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|--|---|---|---|---|---|
| Lingkungan Ruang Refactor refactor-spaces:Environment | Buat lingkungan Refactor Spaces, dan gunakan untuk memuat aplikasi Refactor Spaces Anda. Bagikan lingkungan dengan akun lain Akun AWS atau semua akun di organisasi Anda. Hal ini memungkinkan beberapa Akun AWS dan pengguna melihat informasi tentang lingkungan dan aplikasi di dalamnya. Untuk informasi selengkapnya, lihat Berbagi lingkungan Ruang Refactor yang digunakan AWS RAM dalam Panduan AWS Migration Hub Refactor Spaces Pengguna. |  Y |  Y Dapat berbagi dengan apa saja Akun AWS. |  Y |  Tidak |

AWS Network Firewall









Anda dapat membagikan AWS Network Firewall sumber daya berikut dengan menggunakan AWS RAM.

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|--|--|---|---|---|---|
| Kebijakan Firewall <code>network-firewall:FirewallPolicy</code> | Buat dan kelola kebijakan firewall secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan beberapa akun dalam suatu organisasi untuk berbagi serangkaian perilaku pemantauan, perlindungan, dan penyaringan jaringan yang umum. Untuk informasi selengkapnya, lihat Berbagi kebijakan firewall dan grup aturan di Panduan AWS Network Firewall Pengembang. |  Y |  Y Dapat berbagi dengan apa saja Akun AWS. |  T |  Tidak |
| Kelompok aturan | Buat dan kelola grup aturan tanpa kewarganegaraan |  Y |  Y |  T |  Tidak |

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|--|---|---|---|--|---|
| <p>network-firewall:StatefulRuleGroup</p> <p>network-firewall:StatelessRuleGroup</p> | <p>dan stateful secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan beberapa akun dalam organisasi AWS Organizations untuk berbagi serangkaian kriteria untuk memeriksa dan menangani lalu lintas jaringan. Untuk informasi selengkapnya, lihat Berbagi kebijakan firewall dan grup aturan di Panduan AWS Network Firewall Pengembang.</p> | | <p>Dapat berbagi dengan apa saja Akun AWS.</p> | | |

AWS Outposts

Anda dapat membagikan AWS Outposts sumber daya berikut dengan menggunakan AWS RAM.

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|---|---|--|--|--|--|
| <p>Outposts</p> <p>outposts: Outpost</p> | <p>Buat dan kelola Outposts secara terpusat, dan bagikan dengan orang lain Akun AWS di organisasi Anda. Ini memungkinkan beberapa akun membuat subnet dan volume EBS di Outposts bersama yang dikelola secara terpusat. Untuk informasi selengkapnya, lihat Bekerja dengan sumber daya AWS Outposts bersama di AWS Outposts Panduan Pengguna.</p> | <p> T</p> | <p> T</p> <p>Dapat berbagi dengan hanya Akun AWS di organisasinya sendiri.</p> | <p> Y</p> | <p> Tidak</p> |
| <p>Tabel rute gateway lokal</p> <p>ec2:LocalGatewayRouteTable</p> | <p>Buat dan kelola asosiasi VPC ke gateway lokal secara terpusat, dan bagikan dengan yang lain Akun AWS di organisasi Anda. Ini memungkinkan beberapa akun</p> | <p> T</p> | <p> T</p> <p>Dapat berbagi dengan hanya Akun</p> | <p> T</p> | <p> Tidak</p> |

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasi | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|----------------------------|--|---|--|--|---|
| | membuat asosiasi VPC ke gateway lokal, dan melihat tabel rute dan konfigurasi antarmuka virtual. Untuk informasi selengkapnya, lihat Sumber daya Pos Luar yang Dapat Dibagikan di AWS Outposts Panduan Pengguna. | | AWS di organisasi sendiri. | | |

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|----------------------------|---|---|---|---|---|
| Situs outposts: Site | Buat dan kelola situs Outpost dan bagikan dengan yang lain Akun AWS di organisasi Anda. Ini memungkinkan beberapa akun membuat dan mengelola Outposts di situs bersama dan mendukung kontrol terpisah antara sumber daya Outpost dan situs. Untuk informasi selengkapnya, lihat Bekerja dengan sumber daya AWS Outposts bersama di AWS Outposts Panduan Pengguna. |  T |  Y Dapat berbagi dengan apa saja Akun AWS. |  T |  Tidak |





Amazon S3 di Outposts

Anda dapat membagikan sumber daya Amazon S3 berikut di Outposts dengan menggunakan AWS RAM

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|--------------------------------------|--|---|---|--|---|
| S3 di Outpost s3-outposts:Outpost | Buat dan kelola bucket Amazon S3, titik akses, dan titik akhir di Outpost. Ini memungkinkan beberapa akun membuat dan mengelola Outposts di situs bersama dan mendukung kontrol terpisah antara sumber daya Outpost dan situs. Untuk informasi selengkapnya, lihat Bekerja dengan sumber daya AWS Outposts bersama di AWS Outposts Panduan Pengguna. |  Tidak |  Tidak Dapat berbagi dengan hanya Akun AWS di organisasinya sendiri. |  Ya |  Tidak |





Penjelajah Sumber Daya AWS

Anda dapat membagikan Penjelajah Sumber Daya AWS sumber daya berikut dengan menggunakan AWS RAM.

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|--|--|---|---|---|---|
| Tampilan <code>resource-explorer-2:View</code> | Buat dan konfigurasi tampilan Resource Explorer secara terpusat, dan bagikan dengan yang lain Akun AWS di organisasi Anda. Ini memungkinkan peran dan pengguna dalam beberapa Akun AWS pencarian dan menemukan sumber daya yang dapat diakses melalui tampilan. Untuk informasi selengkapnya, lihat Berbagi tampilan Resource Explorer di Panduan Penjelajah Sumber Daya AWS Pengguna. |  Tidak |  Tidak Dapat berbagi dengan hanya Akun AWS di organisasinya sendiri. |  Tidak |  Tidak |

AWS Resource Groups

Anda dapat membagikan AWS Resource Groups sumber daya berikut dengan menggunakan AWS RAM.



| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|--|---|---|--|---|---|
| Resource Groups resource-groups:Group | Buat dan kelola grup sumber daya host secara terpusat, dan bagikan dengan orang lain Akun AWS di organisasi Anda. Ini memungkinkan beberapa Akun AWS berbagi grup Host Khusus Amazon EC2 yang dibuat menggunakan. AWS License Manager Untuk informasi selengkapnya, lihat Grup sumber daya host AWS License Manager di Panduan AWS License Manager Pengguna . |  Tidak |  Ya Dapat berbagi dengan apa saja Akun AWS. |  Tidak |  Tidak |





Amazon Route 53

Anda dapat membagikan sumber daya Amazon Route 53 berikut dengan menggunakan AWS RAM.

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|---|--|---|---|---|---|
| <p>Route 53 Resolver DNS Firewall grup aturan</p> <p><code>route53resolver:FirewallRuleGroup</code></p> | <p>Buat dan kelola grup aturan Route 53 Resolver DNS Firewall secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan beberapa akun untuk berbagi serangkaian kriteria untuk memeriksa dan menangani kueri DNS keluar yang melalui Resolver Route 53. Untuk informasi selengkapnya, lihat Berbagi grup aturan DNS Firewall Resolver Route 53 Akun AWS di antara dalam Panduan Pengembang Amazon Route 53.</p> |  Y |  Y Dapat berbagi dengan apa saja Akun AWS. |  T |  Tidak |
| <p>Route 53 Profiles</p> <p><code>route53profiles:Profile</code></p> | <p>Buat dan kelola Route 53 Profiles secara terpusat, dan bagikan dengan orang lain Akun</p> |  Y |  Y |  Y |  Tidak |





| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasi | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|----------------------------|--|---|--|--|---|
| | AWS atau organisasi Anda. Ini memungkinkan beberapa akun menerapkan konfigurasi DNS yang ditentukan dalam Route 53 Profiles ke beberapa VPC. Untuk informasi selengkapnya, lihat Amazon Route 53 Profiles di Panduan Pengembang Amazon Route 53. | | Dapat berbagi dengan apa saja Akun AWS. | | |

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasi | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|---|---|--|--|--|--|
| <p>Aturan penyelesai</p> <p><code>route53resolver:ResolverRule</code></p> | <p>Buat dan kelola aturan Resolver secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan beberapa akun meneruskan kueri DNS dari virtual private cloud (VPC) mereka ke alamat IP target yang ditentukan dalam aturan Resolver bersama yang dikelola secara terpusat. Untuk informasi selengkapnya, lihat Berbagi aturan Resolver dengan aturan lain Akun AWS dan menggunakan aturan bersama di Panduan Pengembangan Amazon Route 53.</p> | <p> T</p> | <p> Y</p> <p>Dapat berbagi dengan apa saja Akun AWS.</p> | <p> T</p> | <p> Tidak</p> |

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasi | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|--|--|---|---|---|---|
| Log kueri <code>route53resolver:ResolverQueryLogConfig</code> | Buat dan kelola log kueri secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan beberapa Akun AWS untuk mencatat kueri DNS yang berasal dari VPC mereka ke log kueri yang dikelola secara terpusat. Untuk informasi selengkapnya, lihat Berbagi konfigurasi pencatatan kueri Resolver dengan yang lain Akun AWS di Panduan Pengembang Amazon Route 53 . |  Y |  Y Dapat berbagi dengan apa saja Akun AWS. |  Y |  Tidak |

Pengendali Pemulihan Aplikasi Amazon Route 53

Anda dapat membagikan sumber daya Pengontrol Pemulihan Aplikasi Amazon Route 53 berikut dengan menggunakan AWS RAM.

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|--|---|--|--|--|--|
| <p>Route 53 ARC cluster</p> <p><code>route53-recovery-control:Cluster</code></p> | <p>Buat dan kelola kluster Route 53 ARC secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan beberapa akun membuat panel kontrol dan kontrol perutean dalam satu cluster bersama, mengurangi kompleksitas dan jumlah total cluster yang dibutuhkan organisasi. Untuk informasi selengkapnya, lihat Berbagi kluster di seluruh akun di Panduan Pengembang Pengontrol Pemulihan Aplikasi Amazon Route 53.</p> | <p> Y</p> | <p> Y</p> <p>Dapat berbagi dengan apa saja Akun AWS.</p> | <p> Y</p> | <p> Tidak</p> |





Amazon Simple Storage Service

Anda dapat membagikan Amazon Simple Storage Service sumber daya berikut dengan menggunakan AWS RAM.





| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasi | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|--|---|--|--|--|--|
| Hibah Akses <code>s3:Access Grants</code> | Buat dan kelola Instans Hibah Akses S3 secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan beberapa akun melihat dan menghapus sumber daya bersama. Untuk informasi selengkapnya, lihat S3 Access Grants Cross-account Access di Panduan Pengguna. Amazon Simple Storage Service |  Ya |  Ya Dapat berbagi dengan apa saja Akun AWS. |  Ya |  Ya |





Amazon SageMaker

Anda dapat membagikan SageMaker sumber daya Amazon berikut dengan menggunakan AWS RAM.

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|---|---|---|--|---|---|
| <p>SageMaker Katalog</p> <p>sagemaker :SagemakerCatalog</p> | <p>Untuk dapat ditemukan — memungkinkan pemilik akun memberikan izin untuk dapat ditemukan ke akun lain, untuk semua sumber daya grup fitur dalam katalog. SageMaker Setelah diberikan akses, pengguna akun tersebut dapat melihat grup fitur yang telah dibagikan dengan mereka dari katalog. Untuk informasi selengkapnya, lihat Kemampuan ditemukan dan akses grup fitur lintas akun di Panduan Pengembang Amazon SageMaker .</p> <div data-bbox="397 1612 743 1843" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 20px;"> <p> Note</p> <p>Dapat ditemukan dan akses adalah</p> </div> |  |  |  | |





| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasi | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|----------------------------|----------------------------|---|--|--|---|
| | izin terpisah di SageMaker | | | | |

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|--|--|---|---|---|---|
| SageMaker Grup fitur sagemaker:FeatureGroup | <p>Untuk akses — memungkinkan pemilik akun untuk memberikan izin akses ke akun lain, untuk memilih sumber daya grup fitur. Setelah diberikan akses, pengguna akun tersebut dapat menggunakan grup fitur yang telah dibagikan dengan mereka. Untuk informasi selengkapnya, lihat Kemampuan ditemukan dan akses grup fitur lintas akun di Panduan Pengembang Amazon SageMaker.</p> <div data-bbox="402 1402 743 1759" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 20px;"> <p> Note</p> <p>Dapat ditemukan dan akses adalah izin terpisah di SageMaker</p> </div> |  Ya |  Ya Dapat berbagi dengan apa saja Akun AWS. |  Ya | |

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasi | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|--|---|--|--|--|--|
| <p>Kelompok silsilah sagemaker :LineageGroup</p> | <p>Amazon SageMaker memungkinkan Anda membuat grup silsilah dari metadata pipeline Anda untuk mendapatkan pemahaman yang lebih dalam tentang sejarah dan hubungannya. Bagikan grup silsilah dengan akun lain Akun AWS atau akun di organisasi Anda. Ini memungkinkan beberapa Akun AWS dan pengguna melihat informasi tentang grup silsilah dan menanyakan entitas pelacakan di dalamnya. Untuk informasi selengkapnya, lihat Pelacakan Silsilah Lintas Akun di Panduan Pengembangan Amazon SageMaker .</p> | <p> Y</p> | <p> Y</p> <p>Dapat berbagi dengan apa saja Akun AWS.</p> | <p> T</p> | <p> Tidak</p> |

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|--|---|---|---|---|---|
| SageMaker Kartu Model sagemaker:ModelCard | Amazon SageMaker membuat Kartu Model untuk mendokumentasikan detail penting tentang model pembelajaran mesin (ML) Anda di satu tempat untuk tata kelola dan pelaporan yang efisien. Bagikan Kartu Model Anda dengan akun lain Akun AWS atau akun di organisasi Anda untuk mencapai strategi multi-akun untuk operasi pembelajaran mesin Anda. Hal ini memungkinkan Akun AWS untuk berbagi akses kartu model untuk aktivitas ML mereka ke akun lain. Untuk informasi selengkapnya, lihat Kartu SageMaker Model Amazon di |  Y |  Y Dapat berbagi dengan apa saja Akun AWS. |  Tidak | |





| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasi | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|----------------------------|--------------------------------------|---|--|--|---|
| | Panduan SageMaker Pengembang Amazon. | | | | |



| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|---|--|--|--|--|--|
| <p>SageMaker pipa sagemaker :Pipeline</p> | <p>Dengan Amazon SageMaker Model Building Pipelines, Anda dapat membuat, mengotomatisasi, dan mengelola alur kerja pembelajaran end-to-end mesin dalam skala besar. Bagikan pipeline Anda dengan akun lain Akun AWS atau akun di organisasi Anda untuk mencapai strategi multi-akun untuk operasi pembelajaran mesin Anda. Hal ini memungkinkan beberapa pengguna Akun AWS dan melihat informasi tentang pipeline dan eksekusinya dengan akses opsional untuk memulai, menghentikan, dan mencoba lagi pipeline dari akun lain. Untuk informasi selengkapnya, lihat</p> | <p> Y</p> | <p> Y</p> <p>Dapat berbagi dengan apa saja Akun AWS.</p> | <p> Y</p> | <p> Tidak</p> |

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasi | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|----------------------------|---|---|--|--|---|
| | Dukungan Lintas Akun untuk SageMaker Saluran Pipa di Panduan SageMaker Pengembang Amazon. | | | | |

AWS Service Catalog AppRegistry








Anda dapat membagikan AWS Service Catalog AppRegistry sumber daya berikut dengan menggunakan AWS RAM.

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasi | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|-------------------------------------|---|---|---|--|---|
| Aplikasi servicecatalog:Application | Buat aplikasi, dan gunakan untuk melacak sumber daya milik aplikasi itu di seluruh AWS lingkungan Anda. Bagikan aplikasi dengan orang lain Akun AWS atau organisasi Anda. Ini mungkin |  Tidak |  Tidak Dapat berbagi dengan hanya Akun |  Ya |  Tidak |

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|--|--|--|---|--|--|
| | <p>kan beberapa Akun AWS dan pengguna melihat informasi tentang aplikasi dan sumber daya terkait dengannya secara lokal. Untuk informasi selengkapnya, lihat Membuat aplikasi di Panduan Pengguna Service Catalog.</p> | | <p>AWS di organisasi sendiri.</p> | | |
| <p>Grup Atribut <code>servicecatalog:AttributeGroup</code></p> | <p>Buat grup atribut, dan gunakan untuk menyimpan meta-data yang berkaitan dengan aplikasi Anda. Bagikan grup atribut dengan orang lain Akun AWS atau organisasi Anda. Hal ini memungkinkan beberapa Akun AWS dan pengguna melihat informasi tentang grup atribut. Untuk informasi selengkapnya, lihat Membuat grup atribut di Panduan Pengguna Service Catalog.</p> | <p> T</p> | <p> T</p> <p>Dapat berbagi dengan hanya Akun AWS di organisasi sendiri.</p> | <p> Y</p> | <p> Tidak</p> |

AWS Systems Manager Incident Manager





Anda dapat membagikan AWS Systems Manager Incident Manager sumber daya berikut dengan menggunakan AWS RAM.

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|---|---|---|---|---|---|
| Kontak <code>ssm-contacts:Contact</code> | Buat dan kelola kontak dan rencana eskalasi secara terpusat, dan bagikan detail kontak dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan banyak Akun AWS melihat keterlibatan yang terjadi selama suatu insiden. Untuk informasi selengkapnya, lihat Bekerja dengan kontak bersama dan rencana respons di Panduan Pengguna Manajer Insiden AWS Systems Manager. |  Y |  Y Dapat berbagi dengan apa saja Akun AWS. |  Y |  Tidak |
| Rencana respons | Buat dan kelola rencana respons secara terpusat, dan bagikan dengan orang |  Y |  Y |  Y |  Tidak |

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|----------------------------|--|---|---|--|---|
| ssm-incidents:ResponsePlan | lain Akun AWS atau organisasi Anda. Ini memungkinkan mereka Akun AWS menghubungkan CloudWatch alarm Amazon dan aturan EventBridge acara Amazon ke rencana respons, secara otomatis membuat insiden saat terdeteksi. Insiden ini juga memiliki akses ke metrik yang lain Akun AWS ini. Untuk informasi selengkapnya, lihat Bekerja dengan kontak bersama dan rencana respons di Panduan Pengguna Manajer Insiden AWS Systems Manager. | | Dapat berbagi dengan apa saja Akun AWS. | | |





AWS Systems Manager Toko Parameter

Anda dapat membagikan sumber daya AWS Systems Manager Parameter Store berikut dengan menggunakan AWS RAM.



| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|---|--|---|---|---|---|
| Parameter <code>ssm:Parameter</code> | <p>Buat parameter, dan gunakan untuk menyimpan data konfigurasi yang dapat Anda referensikan dalam skrip, perintah, dokumen SSM, serta alur kerja konfigurasi dan otomatisasi. Bagikan parameter dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan beberapa Akun AWS dan pengguna melihat informasi tentang string dan meningkatkan keamanan dengan memisahkan data Anda dari kode Anda. Untuk informasi selengkapnya, lihat Bekerja dengan parameter bersama di Panduan AWS Systems Manager Pengguna.</p> |  Y |  Y Dapat berbagi dengan apa saja Akun AWS. |  Y |  Tidak |





Amazon VPC

Anda dapat membagikan sumber daya Amazon Virtual Private Cloud (Amazon VPC) berikut dengan menggunakan AWS RAM






| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|--|--|--|--|--|--|
| <p>Alamat IPv4 milik pelanggan</p> <p>ec2:CoipPool</p> | <p>Selama proses AWS Outposts instalasi, AWS buat kumpulan alamat, yang dikenal sebagai kumpulan alamat IP milik pelanggan, berdasarkan informasi yang Anda berikan tentang jaringan lokal Anda.</p> <p>Alamat IP milik pelanggan menyediakan konektivitas lokal, atau eksternal ke sumber daya di subnet Outposts Anda melalui jaringan lokal Anda. Anda dapat menetapkan alamat ini ke sumber daya di Outpost Anda, seperti instans EC2, menggunak</p> | <p> Tidak</p> | <p> Tidak</p> <p>Dapat berbagi dengan hanya Akun AWS di organisasinya sendiri.</p> | <p> Tidak</p> | <p> Tidak</p> |

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasi | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|----------------------------|--|---|--|--|---|
| | <p>an alamat IP Elastic atau menggunakan pengaturan subnet yang secara otomatis menetapkan alamat IP milik pelanggan. Untuk informasi selengkapnya, lihat Alamat IP milik pelanggan di Panduan Pengguna AWS Outposts .</p> | | | | |

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|---|--|---|---|---|---|
| Kumpulan Manajer Alamat IP (IPAM) ec2:IpamPool | Bagikan kumpulan IPAM VPC Amazon secara terpusat dengan peran atau pengguna IAM lainnya Akun AWS, atau seluruh organisasi atau unit organisasi (OU) di dalamnya. AWS Organizations Ini memungkinkan para prinsipal tersebut mengalokasikan CIDR dari kumpulan ke AWS sumber daya, seperti VPC, di akun masing-masing. Untuk informasi selengkapnya, lihat Berbagi kumpulan IPAM menggunakan AWS RAM Panduan Pengguna Pengelola Alamat IP VPC Amazon. |  Y |  Y Dapat berbagi dengan apa saja Akun AWS. |  Y |  Tidak |






| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasi | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|---|--|---|---|---|---|
| Penemuan sumber daya IP Address Manager (IPAM) ec2:IpamResourceDiscovery | Bagikan penemuan sumber daya dengan yang lain. Akun AWS Penemuan sumber daya adalah komponen Amazon VPC IPAM yang memungkinkan IPAM mengelola dan memantau sumber daya milik akun yang dimiliki. Untuk informasi selengkapnya, lihat Bekerja dengan penemuan sumber daya di Panduan Pengguna Amazon VPC IPAM . |  T |  Y Dapat berbagi dengan apa saja Akun AWS. |  T |  Tidak |





| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan lainnya |
|---|--|---|---|---|---|
| Daftar prefiks <code>ec2:PrefixList</code> | Buat dan kelola daftar awalan secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan beberapa daftar awalan Akun AWS referensi dalam sumber daya mereka, seperti grup keamanan VPC dan tabel rute subnet. Untuk informasi selengkapnya, lihat Bekerja dengan daftar awalan bersama di Panduan Pengguna Amazon VPC. |  T |  Y Dapat berbagi dengan apa saja Akun AWS. |  T |  Tidak |





| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|---------------------------------|---|---|--|---|---|
| <p>Subnet</p> <p>ec2:Subnet</p> | <p>Buat dan kelola subnet secara terpusat, dan bagikan dengan Akun AWS di dalam organisasi Anda. Ini memungkinkan beberapa Akun AWS peluncuran sumber daya aplikasi mereka ke dalam VPC yang dikelola secara terpusat. Sumber daya ini mencakup instans Amazon EC2, database Amazon Relational Database Service (RDS), cluster Amazon Redshift, dan fungsi. AWS Lambda Untuk informasi selengkapnya, lihat Bekerja dengan berbagi VPC di Panduan Pengguna Amazon VPC.</p> <div data-bbox="399 1686 745 1869" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px; margin-top: 20px;"> <p> Note</p> <p>Untuk menyertakan</p> </div> |  |  |  |  |

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|----------------------------|---|---|---|--|---|
| | <p>subnet saat Anda membuat pembagian sumber daya, Anda harus memiliki <code>ec2:DescribeSubnets</code> dan <code>ec2:DescribeVpcs</code> izin, sebagai tambahan. <code>ram:CreateResourceShare</code> Subnet default tidak dapat dibagikan. Anda hanya dapat membagikan subnet yang Anda buat sendiri.</p> | | | | |

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|--|---|--|--|--|--|
| <p>Target cermin lalu lintas</p> <p><code>ec2:TrafficMirrorTarget</code></p> | <p>Buat dan kelola target cermin lalu lintas secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan beberapa Akun AWS mengirim lalu lintas jaringan cermin dari sumber cermin lalu lintas di akun mereka ke target mirror lalu lintas yang dikelola secara terpusat dan terpusat. Untuk informasi selengkapnya, lihat Target pencerminan lalu lintas akun di Panduan Pencerminan Lalu Lintas.</p> | <p> T</p> | <p> Y</p> <p>Dapat berbagi dengan apa saja Akun AWS.</p> | <p> T</p> | <p> Tidak</p> |









| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|--|---|---|--|---|---|
| <p>Transit gateway</p> <p>ec2:TransitGateway</p> | <p>Buat dan kelola gateway transit secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan beberapa lalu lintas Akun AWS rute antara VPC mereka dan jaringan lokal melalui gateway transit bersama yang dikelola secara terpusat. Untuk informasi selengkapnya, lihat Berbagi gateway transit di Gateway Transit VPC Amazon.</p> <div data-bbox="399 1398 745 1869" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 20px;"> <p> Note</p> <p>Untuk menyertakan gateway transit saat Anda membuat pembagian sumber daya, Anda harus</p> </div> |  T |  Y <p>Dapat berbagi dengan apa saja Akun AWS.</p> |  T |  Tidak |

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|---|---|---|---|---|---|
| | <p>memiliki <code>ec2:DescribeTransitGateway</code> izin selain <code>itram:CreateResourceShare</code> .</p> | | | | |
| <p>Domain multicast gerbang transit</p> <p><code>ec2:TransitGatewayMulticastDomain</code></p> | <p>Buat dan kelola domain multicast gateway transit secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan beberapa anggota grup Akun AWS register dan deregister atau sumber grup dalam domain multicast . Untuk informasi selengkapnya, lihat Bekerja dengan domain multicast bersama di Panduan Gerbang Transit.</p> | <p> T</p> | <p> Y</p> <p>Dapat berbagi dengan apa saja Akun AWS.</p> | <p> T</p> | <p> Tidak</p> |

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|---|--|--|--|--|--|
| <p>Akses Terverifikasi AWS kelompok</p> <p><code>ec2:VerifiedAccessGroup</code></p> | <p>Buat dan Akses Terverifikasi AWS kelola grup secara terpusat, lalu bagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan aplikasi di beberapa akun menggunakan satu set Akses Terverifikasi AWS titik akhir bersama. Untuk informasi selengkapnya, lihat Berbagi Akses Terverifikasi AWS grup Anda AWS Resource Access Manager di Panduan Akses Terverifikasi AWS Pengguna.</p> | <p> Y</p> | <p> Y</p> <p>Dapat berbagi dengan apa saja Akun AWS.</p> | <p> T</p> | <p> Tidak</p> |

Kisi VPC Amazon





Anda dapat membagikan sumber daya Amazon VPC Lattice berikut dengan menggunakan AWS RAM

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|---|--|--|---|---|--|
| <p>Layanan Amazon VPC Lattice</p> <p><code>vpc-lattice:Service</code></p> | <p>Buat dan kelola layanan Amazon VPC Lattice secara terpusat, dan bagikan dengan individu Akun AWS atau organisasi Anda. Hal ini memungkinkan pemilik layanan untuk terhubung, mengamankan, dan mengamati service-to-service komunikasi dalam lingkungan multi-akun. Untuk informasi selengkapnya, lihat Bekerja dengan sumber daya bersama di Panduan Pengguna Kisi VPC.</p> | <p> Tidak</p> | <p> Ya</p> <p>Dapat berbagi dengan apa saja Akun AWS.</p> | <p> Ya</p> | <p> Tidak</p> |
| <p>Jaringan layanan Amazon VPC Lattice</p> <p><code>vpc-lattice:ServiceNetwork</code></p> | <p>Buat dan kelola jaringan layanan Amazon VPC Lattice secara terpusat, dan bagikan dengan individu Akun AWS atau organisasi Anda. Hal ini memungkin</p> | <p> Tidak</p> | <p> Ya</p> <p>Dapat berbagi dengan apa saja</p> | <p> Ya</p> | <p> Tidak</p> |

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasi | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|----------------------------|---|---|--|--|---|
| | <p>kan pemilik jaringan layanan untuk terhubung, mengamankan, dan mengamati service-to-service komunikasi dalam lingkungan multi-akun. Untuk informasi selengkapnya, lihat Bekerja dengan sumber daya bersama di Panduan Pengguna Amazon VPC Lattice.</p> | | Akun AWS. | | |

AWS Awan WAN

Anda dapat membagikan sumber daya AWS Cloud WAN berikut dengan menggunakan AWS RAM.

| Jenis dan kode sumber daya | Kasus penggunaan | Dapat berbagi dengan pengguna dan peran IAM | Dapat berbagi dengan akun di luar organisasinya | Dapat menggunakan izin yang dikelola pelanggan | Dapat berbagi dengan kepala sekolah layanan |
|---|---|--|--|--|--|
| <p>Jaringan inti WAN awan</p> <p>networkmanager:CoreNetwork</p> | <p>Buat dan kelola jaringan inti Cloud WAN secara terpusat, dan bagikan dengan yang lain Akun AWS. Ini memungkinkan beberapa Akun AWS akses dan penyediaan host pada satu jaringan inti Cloud WAN. Untuk informasi selengkapnya, lihat Berbagi jaringan inti di Panduan Pengguna AWS Cloud WAN.</p> | <p> Y</p> | <p> Y</p> <p>Dapat berbagi dengan apa saja Akun AWS.</p> | <p> T</p> | <p> Tidak</p> |

Mengelola izin diAWS RAM

DiAWS RAM, ada [dua jenis izin terkelola, izinAWS terkelola](#), dan izin terkelola pelanggan.

Izin terkelola menentukan bagaimana konsumen dapat bertindak berdasarkan sumber daya dalam pangsa sumber daya. Saat membuat berbagi sumber daya, Anda harus menentukan izin terkelola mana yang akan digunakan untuk setiap jenis sumber daya yang disertakan dalam pembagian sumber daya. Template kebijakan dalam izin terkelola berisi semua yang diperlukan untuk kebijakan berbasis sumber daya kecuali untuk pokok dan sumber daya. Amazon Resource Name (ARN) dari sumber daya dan ARN dari principals yang terkait dengan berbagi sumber daya melengkapi elemen dari kebijakan berbasis sumber daya. AWS RAMkemudian penulis kebijakan berbasis sumber daya yang melekat pada semua sumber daya dalam berbagi sumber daya.

Setiap izin terkelola dapat memiliki satu atau beberapa versi. Satu versi ditetapkan sebagai versi default untuk izin terkelola itu. Kadang-kadang,AWS memperbarui izinAWS terkelola untuk jenis sumber daya dengan membuat versi baru dan menunjuk versi baru itu sebagai default. Anda juga dapat memperbarui izin terkelola pelanggan Anda dengan membuat versi baru. Izin terkelola yang sudah dilampirkan ke pembagian sumber daya tidak diperbarui secara otomatis. AWS RAMKonsol menunjukkan kapan versi default baru tersedia, dan Anda dapat meninjau perubahan dalam versi default baru dibandingkan dengan yang sebelumnya.

Note

Kami menyarankan agar Anda memperbarui ke versi baru dari izinAWS terkelola sesegera mungkin. Pembaruan ini biasanya menambahkan dukungan untuk yang baru atau diperbaruiLayanan AWS yang dapat berbagi jenis sumber daya tambahan menggunakanAWS RAM. Versi default baru juga dapat mengatasi dan memperbaiki kerentanan keamanan.

Important

Anda hanya dapat melampirkan versi default izin terkelola ke berbagi sumber daya baru.

Anda dapat mengambil daftar izin terkelola yang tersedia kapan saja. Untuk informasi selengkapnya, lihat [Melihat izin yang dikelola](#).

Topik

- [Melihat izin yang dikelola](#)
- [Membuat dan menggunakan izin terkelola pelanggan diAWS RAM](#)
- [Memperbarui izinAWS terkelola ke versi yang lebih baru](#)
- [Pertimbangan untuk menggunakan izin terkelola pelanggan diAWS RAM](#)
- [Cara kerja izin terkelola](#)
- [Jenis izin terkelola](#)

Melihat izin yang dikelola

Anda dapat melihat detail tentang izin terkelola yang tersedia untuk ditetapkan ke jenis sumber daya di berbagai sumber daya Anda. Anda dapat mengidentifikasi izin terkelola yang ditetapkan untuk berbagai sumber daya. Untuk melihat detail ini, gunakan pustaka Izin terkelola diAWS RAM konsol.

Console

Untuk melihat detail tentang izin yang dikelolaAWS RAM

1. Arahkan ke halaman [Pustaka izin terkelola](#) diAWS RAM konsol.
2. Karena sahamAWS RAM sumber daya ada dalam spesifikWilayah AWS, memilih yang sesuaiWilayah AWS dari daftar dropdown di sudut kanan atas konsol. Untuk melihat saham sumber daya yang berisi sumber daya global, Anda harus mengaturWilayah AWS ke US East (N. Virginia), (us-east-1). Untuk informasi lebih lanjut tentang berbagi sumber daya global, lihat[Berbagi sumber daya Regional dibandingkan dengan sumber daya global](#). Meskipun semua Wilayah memiliki izinAWS terkelola yang tersedia yang sama, hal ini memengaruhi jumlah saham sumber daya terkait yang ditampilkan untuk setiap izin terkelola[Step 5](#). Izin yang dikelola pelanggan hanya tersedia di Region tempat izin dibuat.
3. Di daftar izin terkelola, pilih izin terkelola yang ingin Anda lihat detailnya. Anda dapat menggunakan kotak pencarian untuk memfilter daftar izin yang dikelola dengan memasukkan bagian nama atau jenis sumber daya, atau memilih jenis izin yang dikelola dari daftar dropdown.
4. (Opsional) Untuk mengubah preferensi tampilan, pilih ikon roda gigi di kanan atas panel izin terkelola. Anda dapat mengubah preferensi berikut:
 - Ukuran halaman - Jumlah sumber daya yang ditampilkan pada setiap halaman.

- Bungkus garis - Apakah akan membungkus garis dalam baris tabel.
- Kolom - Apakah akan menampilkan atau menyembunyikan informasi tentang jenis sumber daya dan saham terkait.

Setelah Anda selesai mengatur preferensi tampilan, pilih Konfirmasi.

5. Untuk setiap izin yang dikelola, daftar menampilkan informasi berikut ini:

- Nama izin terkelola - Nama izin terkelola.
- Jenis sumber daya - Jenis sumber daya yang dikaitkan dengan izin terkelola.
- Jenis izin terkelola — Apakah izin terkelola adalah izinAWS terkelola atau izin terkelola pelanggan.
- Saham terkait - Jumlah saham sumber daya yang terkait dengan izin terkelola. Jika nomor muncul, maka Anda dapat memilih nomor untuk menampilkan tabel berbagi sumber daya dengan informasi berikut:
 - Nama berbagi sumber daya - Nama berbagi sumber daya yang dikaitkan dengan izin terkelola.
 - Versi izin terkelola - Versi izin terkelola yang dilampirkan ke berbagi sumber daya ini.
 - Pemilik -Akun AWS Jumlah pemilik saham sumber daya.
 - Izinkan prinsipal eksternal - Apakah pembagian sumber daya itu memungkinkan berbagi dengan prinsipal di luar organisasiAWS Organizations.
 - Status - Status hubungan saat ini antara pembagian sumber daya dan izin terkelola.
- Status - Menjelaskan apakah izin terkelola adalah:
 - Dapat dilampirkan - Anda dapat melampirkan izin terkelola ke pembagian sumber daya Anda.
 - Tidak dapat dilampirkan — Anda tidak dapat melampirkan izin terkelola ke bagian sumber daya Anda.
 - Menghapus - Izin terkelola tidak lagi aktif dan akan segera dihapus.
 - Dihapus - Izin terkelola telah dihapus. Ini tetap terlihat selama dua jam sebelum menghilang dari pustaka Izin terkelola.

Anda dapat memilih nama izin terkelola untuk menampilkan informasi selengkapnya tentang izin terkelola tersebut. Halaman detail untuk izin yang dikelola menampilkan informasi berikut ini:

- Jenis sumber daya - Jenis AWS sumber daya yang digunakan izin terkelola ini.
- Jumlah versi - Anda dapat memiliki izin terkelola pelanggan.
- Versi default - Menentukan versi mana yang default dan oleh karena itu ditetapkan secara otomatis ke semua sumber daya baru yang menggunakan izin terkelola ini. Setiap saham sumber daya yang ada yang menggunakan versi berbeda menampilkan prompt bagi Anda untuk memperbarui berbagi sumber daya ke versi default.
- ARN — [Amazon Resource Name \(ARN\)](#) dari izin terkelola. ARN untuk izin yang AWS dikelola menggunakan format berikut ini:

```
arn:aws:ram::aws:permission/  
AWSRAM[DefaultPermission]ShareableResourceType
```

Substring[DefaultPermission] (tanpa tanda kurung dalam ARN yang sebenarnya) hadir dalam nama hanya satu izin terkelola untuk jenis sumber daya yang ditetapkan default.

- Versi izin terkelola - Anda dapat memilih informasi versi mana yang akan ditampilkan di tab di bawah daftar dropdown ini.
 - Detail tab:
 - Waktu pembuatan - Tanggal dan waktu ketika versi izin terkelola ini dibuat.
 - Waktu terakhir diperbarui - Tanggal dan waktu ketika versi izin terkelola ini terakhir diperbarui.
 - Tab template kebijakan - Daftar tindakan dan ketentuan layanan, jika berlaku, bahwa versi izin terkelola ini memungkinkan prinsipal untuk melakukan pada jenis sumber daya terkait.
 - Berbagi sumber daya terkait - Daftar saham sumber daya yang menggunakan versi izin terkelola ini.

AWS CLI

Untuk melihat detail tentang izin yang dikelola AWS RAM

Anda dapat menggunakan [list-permissions](#) perintah untuk mendapatkan daftar izin terkelola yang tersedia untuk digunakan pada saham sumber daya saat ini Wilayah AWS untuk akun panggilan.

```
$ aws ram list-permissions  
{
```



```

"permissions": [
  {
    "arn": "arn:aws:ram::aws:permission/
AWSRAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority",
    "version": "1",
    "defaultVersion": true,
    "name":
"AWSRAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority",
    "resourceType": "acm-pca:CertificateAuthority",
    "status": "ATTACHABLE",
    "creationTime": "2022-06-30T13:03:31.732000-07:00",
    "lastUpdatedTime": "2022-06-30T13:03:31.732000-07:00",
    "isResourceTypeDefault": false,
    "permissionType": "AWS_MANAGED"
  },
  {
    "arn": "arn:aws:ram::aws:permission/
AWSRAMBlankEndEntityCertificateAPIPassthroughIssuanceCertificateAuthority",
    "version": "1",
    "defaultVersion": true,
    "name":
"AWSRAMBlankEndEntityCertificateAPIPassthroughIssuanceCertificateAuthority",
    "resourceType": "acm-pca:CertificateAuthority",
    "status": "ATTACHABLE",
    "creationTime": "2022-11-18T07:05:46.976000-08:00",
    "lastUpdatedTime": "2022-11-18T07:05:46.976000-08:00",
    "isResourceTypeDefault": false,
    "permissionType": "AWS_MANAGED"
  },
  ... TRUNCATED FOR BREVITY ... RUN COMMAND TO SEE COMPLETE LIST OF
  PERMISSIONS ...

  {
    "arn": "arn:aws:ram::aws:permission/
AWSRAMVPCPermissionsNetworkManagerCoreNetwork",
    "version": "1",
    "defaultVersion": true,
    "name": "AWSRAMVPCPermissionsNetworkManagerCoreNetwork",
    "resourceType": "networkmanager:CoreNetwork",
    "status": "ATTACHABLE",
    "creationTime": "2022-06-30T13:03:46.557000-07:00",
    "lastUpdatedTime": "2022-06-30T13:03:46.557000-07:00",
    "isResourceTypeDefault": false,

```

```

    "permissionType": "AWS_MANAGED"
  },
  {
    "arn": "arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP",
    "version": "1",
    "defaultVersion": true,
    "name": "My-Test-CMP",
    "resourceType": "ec2:IpamPool",
    "status": "ATTACHABLE",
    "creationTime": "2023-03-08T06:54:10.038000-08:00",
    "lastUpdatedTime": "2023-03-08T06:54:10.038000-08:00",
    "isResourceTypeDefault": false,
    "permissionType": "CUSTOMER_MANAGED"
  }
]
}

```

Anda juga dapat menemukan ARN dari izin terkelola tertentu dengan namanya dalam `--query` parameter `list-permissions` AWS CLI perintah. Contoh berikut menyaring output untuk menyertakan hanya elemen dalam hasil `permissions` array yang cocok dengan nama tertentu. Kami juga menentukan bahwa kami ingin melihat hanya bidang ARN dalam hasil, dan dalam format teks biasa bukan JSON default.

```

$ aws ram list-permissions \
  --query "permissions[?name == 'My-Test-CMP'].arn \
  --output text
arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP

```

Setelah menemukan ARN izin terkelola tertentu yang Anda minati, Anda dapat mengambil detailnya, termasuk teks kebijakan JSON-nya, dengan menjalankan perintah [get-permission](#).

```

$ aws ram get-permission \
  --permission-arn arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP
{
  "permission": {
    "arn": "arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP",
    "version": "1",
    "defaultVersion": true,
    "name": "My-Test-CMP",
    "resourceType": "ec2:IpamPool",
    "permission": "{\n\t\t\"Effect\": \"Allow\",\n\t\t\"Action\": [\n\t\t\t\t\"ec2:GetIpamPoolAllocations\",\n\t\t\t\t\"ec2:GetIpamPoolCidrs\",\n\t\t\t\t\"ec2:AllocateIpamPoolCidr\",\n\t\t\t\t\"ec2:AssociateVpcCidrBlock\",\n\t\t\t\t\"ec2:DisassociateVpcCidrBlock\"

```

```
\t\t"ec2:CreateVpc",\n\t\t"ec2:ProvisionPublicIpv4PoolCidr",\n\t\t"ec2:ReleaseIpamPoolAllocation"\n\t\t}],\n\t\t"creationTime": "2023-03-08T06:54:10.038000-08:00",\n\t\t"lastUpdatedTime": "2023-03-08T06:54:10.038000-08:00",\n\t\t"isResourceTypeDefault": false,\n\t\t"permissionType": "CUSTOMER_MANAGED",\n\t\t"featureSet": "STANDARD",\n\t\t"status": "ATTACHABLE"\n\t\t}\n\t\t}
```

Membuat dan menggunakan izin terkelola pelanggan diAWS RAM

AWS Resource Access Manager(AWS RAM) menyediakan setidaknya satu izinAWS terkelola untuk setiap jenis sumber daya yang dapat Anda bagikan. Namun, izin terkelola tersebut mungkin tidak memberikan [akses hak istimewa paling sedikit](#) untuk kasus penggunaan berbagi Anda. Ketika salah satu izinAWS terkelola yang disediakan tidak berfungsi, Anda dapat membuat izin terkelola pelanggan Anda sendiri.

Izin terkelola pelanggan adalah izin terkelola yang Anda buat dan pertahankan dengan menentukan secara tepat tindakan mana yang dapat dilakukan di bawah kondisi dengan sumber daya yang digunakan bersamaAWS RAM. Misalnya, Anda ingin membatasi akses baca untuk pool Amazon VPC IP Address Manager (IPAM), yang membantu Anda mengelola alamat IP Anda dalam skala besar. Anda dapat membuat izin terkelola pelanggan untuk pengembang Anda untuk menetapkan alamat IP, tetapi tidak melihat kisaran alamat IP yang ditetapkan akun pengembang lainnya. Anda dapat mengikuti praktik terbaik dengan hak istimewa yang paling tidak, hanya memberikan izin yang diperlukan untuk melakukan tugas pada sumber daya bersama.

Selain itu, Anda dapat memperbarui atau menghapus izin yang dikelola pelanggan sesuai kebutuhan.

Topik

- [Membuat izin terkelola pelanggan](#)
- [Membuat versi baru izin terkelola pelanggan](#)
- [Pilih versi yang berbeda untuk menjadi default untuk izin yang dikelola pelanggan](#)
- [Menghapus versi izin terkelola pelanggan](#)
- [Menghapus izin terkelola pelanggan](#)

Membuat izin terkelola pelanggan

Izin yang dikelola pelanggan khusus untuk Wilayah AWS. Pastikan Anda membuat izin terkelola pelanggan ini di Wilayah yang sesuai.

Console

Untuk membuat izin terkelola pelanggan

1. Lakukan salah satu dari berikut:
 - Buka [pustaka Izin terkelola](#), lalu pilih Buat izin terkelola pelanggan.
 - Arahkan langsung ke halaman [Buat izin terkelola pelanggan](#) di konsol.
2. Untuk detail izin terkelola Pelanggan, masukkan nama izin terkelola pelanggan.
3. Pilih jenis sumber daya yang berlaku izin terkelola ini.
4. Untuk template Kebijakan, Anda menentukan operasi mana yang diizinkan untuk dilakukan pada jenis sumber daya ini.
 - Anda dapat memilih Izin terkelola impor untuk menggunakan tindakan dari izin terkelola yang ada.
 - Pilih atau batalkan pilihan informasi tingkat akses untuk memenuhi kebutuhan Anda di editor visual.
 - Menambah atau memodifikasi kondisi menggunakan editor JSON.
5. (Opsional) Untuk melampirkan tag ke izin terkelola, untuk Tag, masukkan kunci tag dan nilai. Tambahkan tag tambahan dengan memilih Tambahkan tag baru. Ulangi langkah ini seperlunya.
6. Setelah selesai, pilih Buat izin terkelola pelanggan.

AWS CLI

Untuk membuat izin terkelola pelanggan

- Jalankan perintah [create-permission](#) dan tentukan nama, jenis sumber daya yang diterapkan izin terkelola pelanggan, dan teks isi template kebijakan.

Contoh perintah berikut membuat izin dikelola untuk jenis `imagebuilder:Component` sumber daya.

```
$ aws ram create-permission \  
  --name TestCMP \  
  --resource-type imagebuilder:Component \  
  --policy-template "{\"Effect\":\"Allow\",\"Action\":[\"imagebuilder:ListComponents\"]}" \  
{  
  "permission": {  
    "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",  
    "version": "1",  
    "defaultVersion": true,  
    "isResourceTypeDefault": false,  
    "name": "TestCMP",  
    "resourceType": "imagebuilder:Component",  
    "status": "ATTACHABLE",  
    "creationTime": 1680033769.401,  
    "lastUpdatedTime": 1680033769.401  
  }  
}
```

Membuat versi baru izin terkelola pelanggan

Jika kasus penggunaan izin terkelola pelanggan Anda berubah, Anda dapat membuat versi baru dari izin terkelola. Ini tidak memengaruhi pembagian sumber daya Anda yang ada, hanya saham sumber daya baru yang akan menggunakan izin terkelola pelanggan ini.

Setiap izin terkelola dapat memiliki hingga lima versi, tetapi Anda hanya dapat mengaitkan versi default.

Console

Membuat versi baru izin terkelola pelanggan

1. Arahkan ke [pustaka Izin terkelola](#).
2. Filter daftar izin terkelola oleh Pelanggan yang dikelola, atau cari nama izin terkelola pelanggan yang ingin Anda ubah.
3. Dari halaman detail izin terkelola, di bagian Versi izin terkelola, pilih Buat versi.
4. Untuk template Kebijakan, Anda dapat menambah atau menghapus tindakan dan kondisi dengan editor visual atau editor JSON.

Anda juga memiliki opsi untuk memilih Izin terkelola impor untuk menggunakan templat kebijakan yang ada.

5. Setelah selesai, pilih Buat versi di bagian bawah halaman.

AWS CLI

Membuat versi baru izin terkelola pelanggan

1. Temukan Nama Sumber Daya Amazon (ARN) dari izin terkelola pelanggan yang ingin Anda buat versi baru. Lakukan ini dengan memanggil [izin daftar](#) dengan `--permission-type CUSTOMER_MANAGED` parameter untuk hanya menyertakan izin yang dikelola pelanggan.

```
$ aws ram-cmp list-permissions --permission-type CUSTOMER_MANAGED
{
  "permissions": [
    {
      "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
      "version": "2",
      "defaultVersion": true,
      "isResourceTypeDefault": false,
      "name": "TestCMP",
      "permissionType": "CUSTOMER_MANAGED",
      "resourceType": "imagebuilder:Component",
      "status": "ATTACHABLE",
      "creationTime": 1680035597.346,
      "lastUpdatedTime": 1680035597.346
    }
  ]
}
```

2. Setelah Anda memiliki ARN, Anda dapat menghubungi [create-permission-version](#) operasi dan memberikan template kebijakan yang diperbarui.

```
$ aws ram create-permission-version \
  --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP \
  --policy-template {"Effect":"Allow","Action":
["imagebuilder:ListComponents"]}
{
  "permission": {
    "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
```

```
    "version": "2",
    "defaultVersion": true,
    "isResourceTypeDefault": false,
    "name": "TestCMP",
    "status": "ATTACHABLE",
    "resourceType": "imagebuilder:Component",
    "permission": "{\"Effect\":\"Allow\",\"Action\":[\"imagebuilder:ListComponents\"]}\",
    "creationTime": 1680038973.79,
    "lastUpdatedTime": 1680038973.79
  }
}
```

Outputnya mencakup nomor versi versi baru.

Pilih versi yang berbeda untuk menjadi default untuk izin yang dikelola pelanggan

Anda dapat mengatur versi izin terkelola pelanggan lain sebagai versi default baru.

Console

Untuk menetapkan versi default baru untuk izin terkelola pelanggan

1. Arahkan ke [pustaka Izin terkelola](#).
2. Filter daftar izin terkelola oleh Pelanggan yang dikelola, atau cari nama izin terkelola pelanggan yang ingin Anda ubah.
3. Dari halaman Rincian izin terkelola Pelanggan, di bagian Versi izin terkelola, gunakan daftar tarik-turun untuk memilih versi yang ingin Anda tetapkan sebagai default baru.
4. Pilih Tetapkan sebagai versi default.
5. Ketika kotak dialog muncul, konfirmasi bahwa Anda ingin versi ini menjadi default untuk semua pembagian sumber daya baru yang menggunakan izin terkelola pelanggan ini. Jika Anda setuju, pilih Tetapkan sebagai versi default.

AWS CLI

Untuk menetapkan versi default baru untuk izin terkelola pelanggan

1. Temukan nomor versi yang ingin Anda tetapkan sebagai versi default dengan menelepon [list-permission-versions](#).

Contoh perintah berikut mengambil versi saat ini untuk izin terkelola pelanggan.

```
$ aws ram list-permission-versions \
  --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP
{
  "permissions": [
    {
      "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
      "version": "1",
      "defaultVersion": false,
      "isResourceTypeDefault": false,
      "name": "TestCMP",
      "permissionType": "CUSTOMER_MANAGED",
      "featureSet": "STANDARD",
      "resourceType": "imagebuilder:Component",
      "status": "UNATTACHABLE",
      "creationTime": 1680033769.401,
      "lastUpdatedTime": 1680035597.345
    },
    {
      "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
      "version": "2",
      "defaultVersion": true,
      "isResourceTypeDefault": false,
      "name": "TestCMP",
      "permissionType": "CUSTOMER_MANAGED",
      "featureSet": "STANDARD",
      "resourceType": "imagebuilder:Component",
      "status": "ATTACHABLE",
      "creationTime": 1680035597.346,
      "lastUpdatedTime": 1680035597.346
    }
  ]
}
```


2. Setelah Anda memiliki nomor versi untuk ditetapkan sebagai default, Anda dapat memanggil [set-default-permission-version](#) operasi.

```
$ aws ram-cmp set-default-permission-version \
  --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP \
  --version 2
```

Perintah ini mengembalikan tidak ada output jika berhasil. Anda dapat menjalankan [list-permission-versions](#) lagi dan memverifikasi bahwa defaultVersion bidang versi yang dipilih sekarang diatur ke true.

Menghapus versi izin terkelola pelanggan

Anda dapat memiliki sampai dengan lima versi dari setiap izin terkelola pelanggan. Saat versi tidak lagi diperlukan, dan tidak digunakan, Anda dapat menghapusnya. Anda tidak dapat menghapus versi standar izin terkelola pelanggan. Versi yang dihapus tetap terlihat di konsol hingga dua jam dengan status dihapus sebelum dihapus sepenuhnya.

Console

Menghapus versi izin terkelola pelanggan

1. Arahkan ke [pustaka Izin terkelola](#).
2. Filter daftar izin terkelola oleh Pelanggan yang dikelola, atau cari nama izin terkelola pelanggan dengan versi yang ingin Anda hapus.
3. Pastikan versi yang ingin Anda hapus saat ini tidak default.
4. Untuk bagian Versi halaman, pilih tab Shares sumber daya terkait untuk melihat apakah ada saham yang menggunakan versi ini.

Jika ada saham yang terkait, Anda harus mengubah versi izin terkelola pelanggan sebelum dapat menghapus versi ini.

5. Pilih Hapus versi di sisi kanan bagian Versi.
6. Di kotak dialog konfirmasi, pilih Hapus untuk mengonfirmasi bahwa Anda ingin menghapus versi izin terkelola pelanggan ini.

Pilih Batal jika Anda tidak ingin menghapus versi izin terkelola pelanggan ini.

AWS CLI

Untuk menghapus satu versi izin terkelola pelanggan

1. Panggil [list-permission-versions](#) operasi untuk mengambil nomor versi yang tersedia.
2. Setelah Anda memiliki nomor versi, berikan sebagai parameter untuk [delete-permission-version](#).

```
$ aws ram-cmp delete-permission-version \
  --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP \
  --version 1
```

Perintah ini mengembalikan tidak ada output jika berhasil. Anda dapat menjalankan [list-permission-versions](#) lagi dan memverifikasi bahwa versi tidak lagi termasuk dalam output.

Menghapus izin terkelola pelanggan

Jika izin yang dikelola pelanggan tidak lagi diperlukan, dan tidak digunakan, Anda dapat menghapusnya. Anda tidak dapat menghapus izin terkelola pelanggan yang terkait dengan berbagi sumber daya. Izin terkelola pelanggan yang dihapus menghilang setelah dua jam. Sampai saat itu, itu tetap terlihat di pustaka izin terkelola dengan status dihapus.

Console

Menghapus izin terkelola pelanggan

1. Arahkan ke [pustaka Izin terkelola](#).
2. Filter daftar izin terkelola oleh Pelanggan yang dikelola, atau cari nama izin terkelola pelanggan yang ingin Anda hapus.
3. Konfirmasikan ada 0 saham terkait dari daftar izin terkelola sebelum memilih izin terkelola pelanggan.

Jika masih ada saham sumber daya yang terkait dengan izin terkelola, Anda harus menetapkan izin terkelola lain untuk semua saham sumber daya sebelum Anda dapat melanjutkan.

4. Di sudut kanan atas halaman detail terkelola pelanggan, pilih Hapus izin terkelola pelanggan, pilih Hapus izin terkelola pelanggan,
5. Saat kotak dialog konfirmasi muncul, pilih Hapus untuk menghapus izin terkelola.

AWS CLI

Untuk menghapus izin terkelola pelanggan

1. Temukan ARN izin terkelola yang ingin Anda hapus dengan memanggil [izin daftar](#) dengan `--permission-type CUSTOMER_MANAGED` parameter untuk hanya menyertakan izin yang dikelola pelanggan.

```
$ aws ram-cmp list-permissions --permission-type CUSTOMER_MANAGED
{
  "permissions": [
    {
      "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
      "version": "2",
      "defaultVersion": true,
      "isResourceTypeDefault": false,
      "name": "TestCMP",
      "permissionType": "CUSTOMER_MANAGED",
      "resourceType": "imagebuilder:Component",
      "status": "ATTACHABLE",
      "creationTime": 1680035597.346,
      "lastUpdatedTime": 1680035597.346
    }
  ]
}
```

2. Setelah Anda memiliki ARN izin terkelola untuk dihapus, berikan sebagai parameter untuk [menghapus-izin](#).

```
$ aws ram delete-permission \
  --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP
{
  "returnValue": true,
  "permissionStatus": "DELETING"
}
```

Memperbarui izinAWS terkelola ke versi yang lebih baru

Terkadang, AWS memperbarui izinAWS terkelola yang tersedia untuk dilampirkan ke pangsa sumber daya untuk jenis sumber daya tertentu. Ketika AWS melakukan ini, itu menciptakan versi baru dari

izinAWS dikelola. Berbagi sumber yang menyertakan jenis sumber daya yang ditentukan tidak diperbarui secara otomatis untuk menggunakan versi izin terkelola terbaru. Anda harus secara eksplisit memperbarui izin terkelola untuk setiap berbagi sumber daya. Langkah tambahan ini diperlukan agar Anda dapat mengevaluasi perubahan sebelum menerapkannya pada pembagian sumber daya Anda.

Console

Setiap kali konsol menampilkan halaman yang mencantumkan izin yang terkait dengan berbagi sumber daya, dan satu atau lebih izin tersebut menggunakan versi selain default untuk izin, konsol menampilkan spanduk di bagian atas halaman konsol. Banner menunjukkan bahwa berbagi sumber daya Anda menggunakan versi selain default.

Selain itu, izin individu dapat menampilkan tombol Perbarui ke versi default di sebelah nomor versi saat ini ketika versi itu bukan default.

Memilih tombol itu akan memulai Wisaya [pembagian sumber daya Perbarui](#). Pada Langkah 2 wizard Anda dapat memperbarui versi izin non-default untuk menggunakan versi default mereka.

Perubahan tidak disimpan sampai Anda menyelesaikan wizard dengan memilih Kirim di halaman terakhir wizard.

Note

Anda hanya dapat melampirkan versi default, dan Anda tidak dapat kembali ke versi lain. Untuk izin terkelola pelanggan, setelah memperbarui izin ke versi default, Anda tidak dapat menerapkan versi lain ke berbagi sumber daya kecuali Anda terlebih dahulu menetapkan versi lain sebagai default. Misalnya, jika Anda memperbarui izin ke versi default dan kemudian menemukan kesalahan yang ingin Anda putar kembali, Anda dapat menetapkan versi sebelumnya sebagai default. Atau, Anda dapat membuat versi baru yang berbeda dan menunjuknya sebagai default. Setelah Anda melakukan salah satu opsi tersebut, Anda kemudian akan memperbarui berbagi sumber daya Anda untuk menggunakan versi default yang sekarang.

AWS CLI

Untuk memperbarui versi izinAWS terkelola

1. Jalankan perintah [get-resource-shares](#) dengan `--permission-arn` parameter untuk menentukan [Amazon Resource Name \(ARN\)](#) dari izin terkelola yang ingin Anda perbarui. Ini menghasilkan perintah yang hanya mengembalikan saham sumber daya yang menggunakan izin terkelola tersebut.

Misalnya, perintah contoh berikut menampilkan detail untuk setiap pembagian sumber daya yang menggunakan izin AWS terkelola default untuk reservasi kapasitas Amazon EC2.

```
$ aws ram get-resource-shares \  
  --resource-owner SELF \  
  --permission-arn arn:aws:ram::aws:permission/  
AWSRAMDefaultPermissionCapacityReservation
```

Outputnya mencakup ARN dari setiap pembagian sumber daya dengan setidaknya satu sumber daya yang aksesnya dikendalikan oleh izin terkelola tersebut.

2. Untuk setiap sumber daya yang ditentukan dalam perintah sebelumnya, jalankan perintah [associate-resource-share-permission](#). Sertakan `--resource-share-arn` untuk menentukan pangsa sumber daya yang akan diperbarui, `--permission-arn` untuk menentukan izin AWS terkelola mana yang Anda perbarui, dan `--replace` parameter untuk menentukan bahwa Anda ingin memperbarui berbagi untuk menggunakan versi terbaru dari izin terkelola tersebut. Anda tidak perlu menentukan nomor versi; versi default digunakan secara otomatis.

```
$ aws ram associate-resource-share-permission \  
  --resource-share-arn < ARN of one of the shares from the output of the  
previous command > \  
  --permission-arn arn:aws:ram::aws:permission/  
AWSRAMDefaultPermissionCapacityReservation \  
  --replace
```

3. Ulangi perintah pada langkah sebelumnya untuk masing-masing `ResourceShareArn` yang Anda terima dalam hasil dari perintah pada langkah 1.

Pertimbangan untuk menggunakan izin terkelola pelanggan di AWS RAM

Izin terkelola pelanggan hanya tersedia di tempat Wilayah AWS Anda membuatnya. Tidak semua jenis sumber daya mendukung izin terkelola pelanggan. Untuk daftar jenis sumber daya yang didukung AWS Resource Access Manager, lihat [Sumber daya yang dapat dibagikan AWS](#).

Izin terkelola pelanggan dengan beberapa pernyataan tidak didukung. Anda hanya dapat menggunakan operator tunggal yang tidak meniadakan dalam izin yang dikelola pelanggan.

Kondisi berikut tidak didukung dalam izin terkelola pelanggan:

- Kepala sekolah dalam organisasi terkait:
 - `aws:PrincipalOrgId`
 - `aws:PrincipalOrgPaths`
 - `aws:PrincipalAccount`
- Principal untuk layanan tertentu terkait:
 - `aws:SourceArn`
 - `aws:SourceAccount`
- Tag sistem:
 - `aws:PrincipalTag/aws:`
 - `aws:ResourceTag/aws:`
 - `aws:RequestTag/aws:`

Cara kerja izin terkelola

Untuk ringkasan singkat, tonton video berikut yang menunjukkan cara izin terkelola memungkinkan Anda menerapkan praktik terbaik dengan akses hak istimewa keAWS sumber daya Anda.

Video ini menunjukkan cara menulis dan mengasosiasikan izin terkelola pelanggan mengikuti praktik terbaik dengan hak istimewa yang paling tidak. Untuk informasi, [???](#)

Saat membuat berbagi sumber daya, Anda mengaitkan izinAWS terkelola dengan setiap jenis sumber daya yang ingin Anda bagikan. Jika izin terkelola memiliki lebih dari satu versi, pangsa sumber daya baru selalu menggunakan versi yang ditetapkan sebagai default.

Setelah Anda membuat berbagi sumber daya,AWS RAM gunakan izin terkelola untuk menghasilkan kebijakan berbasis sumber daya yang dilampirkan ke setiap sumber daya bersama.

Template kebijakan dalam izin terkelola menetapkan hal berikut:

Efek

Menunjukkan apakah `Deny` akan `Allow` atau izin utama untuk melakukan operasi pada sumber daya bersama. Untuk izin yang dikelola, efeknya selalu `Allow`. Untuk informasi selengkapnya, lihat [Efek](#) di Panduan Pengguna IAM.

Action

Daftar operasi yang kepala sekolah diberikan izin untuk melakukan. Ini bisa menjadi tindakan dalam AWS Management Console atau operasi di AWS Command Line Interface (AWS CLI) atau AWS API. Tindakan didefinisikan oleh AWS izin. Untuk informasi selengkapnya, lihat [Tindakan](#) di Panduan Pengguna IAM.

Kondisi

Kapan dan bagaimana prinsipal dapat berinteraksi dengan sumber daya dalam berbagi sumber daya. Kondisi menambahkan lapisan keamanan tambahan ke sumber daya bersama Anda. Gunakan mereka untuk membatasi akses untuk tindakan sensitif ke sumber daya bersama Anda. Misalnya, Anda dapat menyertakan kondisi yang mengharuskan tindakan berasal dari rentang alamat IP perusahaan tertentu, atau bahwa tindakan harus dilakukan oleh pengguna yang diautentikasi dengan autentikasi multi-faktor. Untuk informasi selengkapnya tentang kondisi, lihat [kunci konteks kondisi AWS global](#) di Panduan Pengguna IAM. Untuk informasi, [AWS](#)

Note

Ketentuan tersedia untuk izin yang dikelola pelanggan dan jenis sumber daya yang didukung untuk izin AWS terkelola.

Untuk informasi tentang kondisi yang dikecualikan dari penggunaan dengan izin yang dikelola pelanggan, lihat [Pertimbangan untuk menggunakan izin terkelola pelanggan di AWS RAM](#).

Jenis izin terkelola

Saat membuat berbagi sumber daya, Anda memilih izin terkelola untuk diasosiasikan dengan setiap jenis sumber daya yang Anda sertakan dalam berbagi sumber daya. AWS izin terkelola ditentukan oleh layanan yang AWS memiliki sumber daya dan dikelola oleh AWS RAM. Anda penulis dan memelihara izin pelanggan Anda sendiri dikelola.

- AWSizin terkelola - Ada satu izin terkelola default yang tersedia untuk setiap jenis sumber daya yangAWS RAM mendukung. Izin terkelola default adalah izin yang digunakan untuk jenis sumber daya kecuali Anda secara eksplisit memilih salah satu izin terkelola tambahan. Izin terkelola default dimaksudkan untuk mendukung skenario pelanggan yang paling umum untuk berbagi sumber daya dari jenis yang ditentukan. Izin terkelola default memungkinkan prinsipal untuk melakukan tindakan spesifik yang ditentukan oleh layanan untuk jenis sumber daya. Misalnya, untuk jenisec2:Subnet sumber daya Amazon VPC, izin terkelola default memungkinkan prinsipal untuk melakukan tindakan berikut:
 - ec2:RunInstances
 - ec2:CreateNetworkInterface
 - ec2:DescribeSubnets

Nama-nama izinAWS terkelola default menggunakan format berikut:AWSRAMDefaultPermission*ShareableResourceType*. Misalnya, untuk jenisec2:Subnet sumber daya, nama izinAWS terkelola default adalahAWSRAMDefaultPermissionSubnet.

Note

Izin terkelola default terpisah dari [versi](#) default izin terkelola. Semua izin terkelola, baik default atau salah satu izin terkelola tambahan yang didukung oleh beberapa jenis sumber daya, merupakan izin terpisah dan lengkap dengan efek dan tindakan berbeda yang mendukung skenario berbagi yang berbeda, seperti akses baca-tulis versus akses hanya-baca. Setiap izin terkelola,AWS apakah pelanggan yang dikelola dapat memiliki beberapa versi, salah satunya adalah versi default untuk izin itu.

Misalnya, ketika Anda berbagi jenis sumber daya yang mendukung akses penuh (Read dan Write) izin terkelola dan izin terkelola hanya-baca, Anda dapat membuat satu berbagi sumber daya untuk administrator dengan izin terkelola akses penuh. Anda kemudian dapat membuat pangsa sumber daya terpisah untuk pengembang lain menggunakan izin terkelola hanya-baca untuk mengikuti [praktik pemberian hak istimewa paling sedikit](#).

Note

SemuaAWS layanan yang bekerja denganAWS RAM dukungan setidaknya satu izin terkelola default. Anda dapat melihat izin yang tersedia untuk masing-masingLayanan

AWS di halaman [pustaka Izin terkelola](#). Halaman ini memberikan rincian tentang setiap izin terkelola yang tersedia, termasuk setiap saham sumber daya yang saat ini terkait dengan izin dan apakah berbagi dengan prinsipal eksternal diperbolehkan, jika berlaku. Untuk informasi selengkapnya, lihat [Melihat izin yang dikelola](#).

Untuk layanan yang tidak mendukung izin terkelola tambahan, saat Anda membuat berbagi sumber daya, AWS RAM secara otomatis menerapkan izin default yang ditentukan untuk jenis sumber daya yang Anda pilih. Jika didukung, Anda juga akan memiliki opsi untuk memilih Buat izin terkelola pelanggan di halaman izin terkelola Rekanan.

- Izin terkelola pelanggan - Izin terkelola pelanggan adalah izin terkelola yang Anda buat dan pertahankan dengan menentukan secara tepat tindakan mana yang dapat dilakukan di bawah kondisi dengan sumber daya yang digunakan bersama AWS RAM. Misalnya, Anda ingin membatasi akses baca untuk pool Amazon VPC IP Address Manager (IPAM), yang membantu Anda mengelola alamat IP Anda dalam skala besar. Anda dapat membuat izin terkelola pelanggan untuk pengembang Anda untuk menetapkan alamat IP, tetapi tidak melihat kisaran alamat IP yang ditetapkan akun pengembang lainnya. Anda dapat mengikuti praktik terbaik dengan hak istimewa yang paling tidak, hanya memberikan izin yang diperlukan untuk melakukan tugas pada sumber daya bersama.

Keamanan di AWS RAM

Keamanan cloud di AWS merupakan prioritas tertinggi. Sebagai pelanggan AWS, Anda akan mendapatkan manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara AWS dan Anda. [Model tanggung jawab bersama](#) menggambarkan ini sebagai keamanan dari cloud dan keamanan di cloud:

- Keamanan dari cloud – AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan layanan AWS di Cloud AWS Cloud. AWS juga menyediakan layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari [program kepatuhan AWS](#). Untuk mempelajari tentang program kepatuhan yang berlaku di AWS Resource Access Manager (AWS RAM), lihat [AWS Layanan dalam Cakupan melalui Program Kepatuhan](#).
- Keamanan di cloud – Tanggung jawab Anda ditentukan menurut layanan AWS yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain termasuk sensitivitas data Anda, persyaratan perusahaan Anda, serta hukum dan peraturan yang berlaku.

Dokumentasi ini akan membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan AWS RAM. Topik berikut akan menunjukkan kepada Anda cara membuat konfigurasi AWS RAM untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan layanan AWS lain yang membantu Anda memantau dan mengamankan sumber daya AWS RAM Anda.

Topik

- [Perlindungan data di AWS RAM](#)
- [Identity and access management untuk AWS RAM](#)
- [Pencatatan dan pemantauan di AWS RAM](#)
- [Ketahanan di AWS RAM](#)
- [Keamanan infrastruktur dalam AWS RAM](#)

Perlindungan data di AWS RAM

[Model tanggung jawab bersama](#) AWS diterapkan untuk perlindungan data AWS Resource Access Manager. Sebagaimana dijelaskan dalam model ini, AWS bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda harus bertanggung jawab untuk memelihara kendali terhadap konten yang di-hosting pada infrastruktur ini. Anda juga bertanggung jawab atas tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat [FAQ Privasi Data](#). Untuk informasi tentang perlindungan data di Eropa, silakan lihat postingan blog [Model Tanggung Jawab Bersama AWS dan GDPR](#) di Blog Keamanan AWS.

Untuk tujuan perlindungan data, sebaiknya Anda melindungi kredensial Akun AWS dan menyiapkan AWS IAM Identity Center atau AWS Identity and Access Management (IAM) untuk pengguna individu. Dengan cara seperti itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugas mereka. Kami juga merekomendasikan agar Anda mengamankan data Anda dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk melakukan komunikasi dengan sumber daya AWS. Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Siapkan API dan log aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi enkripsi AWS, bersama dengan semua kontrol keamanan default dalam Layanan AWS.
- Gunakan layanan keamanan terkelola lanjutan seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 ketika mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Untuk informasi selengkapnya tentang titik akhir FIPS yang tersedia, silakan lihat [Standar Pemrosesan Informasi Federal \(FIPS\) 140-2](#).

Sebaiknya Anda tidak memasukkan informasi rahasia atau sensitif, seperti alamat email pelanggan, ke dalam tanda atau bidang teks bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan AWS RAM atau lainnya Layanan AWS menggunakan konsol, APIAWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang teks bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau diagnostik. Saat Anda memberikan URL ke server eksternal, sebaiknya Anda tidak menyertakan informasi kredensial di URL untuk memvalidasi permintaan Anda ke server tersebut.

Identity and access management untuk AWS RAM

AWS Identity and Access Management (IAM) adalah layanan AWS yang membantu administrator mengontrol akses ke sumber daya AWS secara aman. Administrator dalam kontrol IAM yang dapat diautentikasi (login) dan diotorisasi (memiliki izin) untuk menggunakan sumber daya. AWS Dengan menggunakan IAM, Anda membuat princiapals, seperti peran, pengguna, dan grup di Anda. Akun AWS Anda mengontrol izin bahwa prinsipal harus melakukan tugas-tugas menggunakan sumber daya. AWS Anda dapat menggunakan IAM tanpa biaya tambahan. Untuk informasi selengkapnya tentang mengelola dan membuat kebijakan IAM kustom, lihat [Mengelola kebijakan IAM](#) di Panduan Pengguna IAM.

Topik

- [Cara kerja AWS RAM dengan IAM](#)
- [Kebijakan terkelola AWS untuk AWS RAM](#)
- [Menggunakan Peran Tertaut Layanan untuk AWS RAM](#)
- [Contoh kebijakan IAM untuk AWS RAM](#)
- [Contoh kebijakan kontrol layanan untuk AWS Organizations dan AWS RAM](#)
- [Menonaktifkan berbagi sumber daya dengan AWS Organizations](#)

Cara kerja AWS RAM dengan IAM

Secara default, prinsipal IAM tidak memiliki izin untuk membuat atau memodifikasi AWS RAM sumber daya. Untuk mengizinkan prinsipal IAM membuat atau memodifikasi sumber daya dan melakukan tugas, Anda melakukan salah satu langkah berikut. Tindakan ini memberikan izin untuk menggunakan sumber daya tertentu dan tindakan API.

Untuk menyediakan akses, tambahkan izin ke pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

Buat set izin. Ikuti petunjuk di [Buat set izin](#) di Panduan AWS IAM Identity Center Pengguna.

- Pengguna yang dikelola dalam IAM melalui penyedia identitas:

Membuat peran untuk federasi identitas. Ikuti petunjuk dalam [Membuat peran untuk penyedia identitas pihak ketiga \(federasi\)](#) di Panduan Pengguna IAM.

- Pengguna IAM:

- Buat peran yang dapat diasumsikan pengguna Anda. Ikuti petunjuk dalam [Membuat peran untuk pengguna IAM](#) di Panduan Pengguna IAM.
- (Tidak disarankan) Lampirkan kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti petunjuk dalam [Menambahkan izin ke pengguna \(konsol\)](#) di Panduan Pengguna IAM.

AWS RAM menyediakan beberapa kebijakan AWS terkelola yang dapat Anda gunakan yang akan memenuhi kebutuhan banyak pengguna. Untuk informasi lebih lanjut tentang ini, lihat [Kebijakan terkelola AWS untuk AWS RAM](#).

Jika Anda memerlukan kontrol yang lebih baik atas izin yang Anda berikan kepada pengguna, Anda dapat membuat kebijakan Anda sendiri di konsol IAM. Untuk informasi tentang membuat kebijakan dan melampirkannya ke peran dan pengguna IAM Anda, lihat [Kebijakan dan izin di IAM](#) dalam Panduan AWS Identity and Access Management Pengguna.

Bagian berikut memberikan rincian AWS RAM spesifik untuk membangun kebijakan izin IAM.

Daftar Isi

- [Struktur kebijakan](#)
 - [Efek](#)
 - [Action](#)
 - [Resource](#)
 - [Kondisi](#)

Struktur kebijakan

Kebijakan izin IAM adalah dokumen JSON yang mencakup pernyataan berikut: Efek, Tindakan, Sumber Daya, dan Kondisi. Kebijakan IAM biasanya mengambil bentuk sebagai berikut.

```
{
  "Statement": [{
    "Effect": "<effect>",
    "Action": "<action>",
    "Resource": "<arn>",
    "Condition": {
      "<comparison-operator>": {
        "<key>": "<value>"
      }
    }
  }]
}
```

```
    }
  }
}]
}
```

Efek

Pernyataan Efek menunjukkan apakah kebijakan mengizinkan atau menolak izin utama untuk melakukan suatu tindakan. Nilai yang mungkin termasuk: `Allow` dan `Deny`.

Action

Pernyataan Action menentukan tindakan AWS RAM API yang kebijakan mengizinkan atau menolak izin. Untuk daftar lengkap tindakan yang diizinkan, lihat [Tindakan yang ditentukan oleh AWS Resource Access Manager](#) dalam Panduan Pengguna IAM.

Resource

Pernyataan Resource menentukan AWS RAM sumber daya yang dipengaruhi oleh kebijakan. Untuk menentukan sumber daya dalam sebuah pernyataan, gunakan Amazon Resource Name (ARN) yang unik. Untuk daftar lengkap sumber daya yang diizinkan, lihat [Sumber daya yang ditentukan oleh AWS Resource Access Manager](#) dalam Panduan Pengguna IAM.

Kondisi

pernyataan kondisi adalah opsional. Mereka dapat digunakan untuk menyempurnakan lebih lanjut kondisi yang berlaku untuk kebijakan. AWS RAM mendukung kunci kondisi berikut:

- `aws:RequestTag/${TagKey}`- Tes apakah permintaan layanan menyertakan tag dengan kunci tag yang ditentukan ada dan memiliki nilai yang ditentukan.
- `aws:ResourceTag/${TagKey}`- Pengujian apakah sumber daya yang ditindaklanjuti oleh permintaan layanan memiliki tag terlampir dengan kunci tag yang Anda tentukan dalam kebijakan.

Contoh kondisi berikut memeriksa bahwa sumber daya yang direferensikan dalam permintaan layanan memiliki tag terlampir dengan nama kunci "Pemilik" dan nilai "Tim Pengembang".

```
"Condition" : {
  "StringEquals" : {
    "aws:ResourceTag/Owner" : "Dev Team"
  }
}
```

- `aws:TagKeys`- Menentukan kunci tag yang harus digunakan untuk membuat atau menandai pangsa sumber daya.
- `ram:AllowsExternalPrincipals`- Menguji apakah pangsa sumber daya dalam permintaan layanan memungkinkan berbagi dengan prinsipal eksternal. Prinsipal eksternal adalah Akun AWS bagian luar organisasi Anda di AWS Organizations. Jika ini mengevaluasi `False`, maka Anda dapat berbagi sumber daya ini dengan akun hanya di organisasi yang sama.
- `ram:PermissionArn`- Menguji apakah ARN izin yang ditentukan dalam permintaan layanan cocok dengan string ARN yang Anda tentukan dalam kebijakan.
- `ram:PermissionResourceType`- Membuat tes apakah izin yang ditentukan dalam permintaan layanan valid untuk tipe sumber daya yang Anda sebutkan dalam kebijakan. Tentukan jenis sumber daya menggunakan format yang ditunjukkan dalam daftar [jenis sumber daya yang dapat dibagikan](#).
- `ram:Principal`- Menguji apakah ARN dari prinsipal yang ditentukan dalam permintaan layanan cocok dengan string ARN yang Anda tentukan dalam kebijakan.
- `ram:RequestedAllowsExternalPrincipals`- Menguji apakah permintaan layanan menyertakan `allowExternalPrincipals` parameter dan apakah argumennya cocok dengan nilai yang Anda tentukan dalam kebijakan.
- `ram:RequestedResourceType`- Menguji apakah jenis sumber daya sumber daya yang ditindaklanjuti cocok dengan string jenis sumber daya yang Anda tentukan dalam kebijakan. Tentukan jenis sumber daya menggunakan format yang ditunjukkan dalam daftar [jenis sumber daya yang dapat dibagikan](#).
- `ram:ResourceArn`- Menguji apakah ARN sumber daya yang ditindaklanjuti oleh permintaan layanan cocok dengan ARN yang Anda tentukan dalam kebijakan.
- `ram:ResourceShareName`- Menguji apakah nama pangsa sumber daya yang ditindaklanjuti oleh permintaan layanan cocok dengan string yang Anda tentukan dalam kebijakan.
- `ram:ShareOwnerAccountId`- Menguji nomor ID akun dari pangsa sumber daya yang ditindaklanjuti oleh permintaan layanan cocok dengan string yang Anda tentukan dalam kebijakan.

Kebijakan terkelola AWS untuk AWS RAM

AWS Resource Access Manager saat ini menyediakan beberapa AWS RAM kebijakan terkelola, yang dijelaskan dalam topik ini.

Kebijakan yang dikelola AWS

- [Kebijakan terkelola AWS: AWSResourceAccessManagerReadOnlyAccess](#)
- [Kebijakan terkelola AWS: AWSResourceAccessManagerFullAccess](#)
- [Kebijakan terkelola AWS: AWSResourceAccessManagerResourceShareParticipantAccess](#)
- [Kebijakan terkelola AWS: AWSResourceAccessManagerServiceRolePolicy](#)
- [AWS RAM memperbarui pada kebijakan terkelola AWS](#)

Dalam daftar sebelumnya, Anda dapat melampirkan tiga kebijakan pertama ke peran IAM, grup, dan pengguna untuk memberikan izin. Kebijakan terakhir dalam daftar dicadangkan untuk AWS RAM peran layanan terkait.

Sebuah AWS kebijakan terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS kebijakan terkelola dirancang untuk memberikan izin untuk banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa AWS kebijakan terkelola mungkin tidak memberikan izin paling sedikit hak istimewa untuk kasus penggunaan spesifik Anda karena tersedia untuk semua AWS pelanggan untuk digunakan. Kami menyarankan Anda mengurangi izin lebih lanjut dengan mendefinisikan [kebijakan yang dikelola pelanggan](#) yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam AWS kebijakan yang dikelola. Jika AWS memperbarui izin yang didefinisikan dalam AWS kebijakan terkelola, pembaruan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan. AWS kemungkinan besar akan memperbarui AWS kebijakan terkelola saat baru Layanan AWS diluncurkan atau operasi API baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat [Kebijakan terkelola AWS](#) dalam Panduan Pengguna IAM.

Kebijakan terkelola AWS: AWSResourceAccessManagerReadOnlyAccess

Anda dapat melampirkan kebijakan `AWSResourceAccessManagerReadOnlyAccess` ke identitas-identitas IAM Anda.

Kebijakan ini memberikan izin hanya-baca untuk berbagi sumber daya yang dimiliki oleh Anda Akun AWS.

Hal ini dilakukan dengan memberikan izin untuk menjalankan salah satu `Get*` atau `List*` operasi. Ini tidak memberikan kemampuan apa pun untuk memodifikasi pangsa sumber daya apa pun.

Detail izin

Kebijakan ini mencakup izin berikut.

- `ram`- Memungkinkan prinsipal untuk melihat rincian tentang saham sumber daya yang dimiliki oleh akun.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ram:Get*",
        "ram:List*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Kebijakan terkelola AWS: `AWSResourceAccessManagerFullAccess`

Anda dapat melampirkan kebijakan `AWSResourceAccessManagerFullAccess` ke identitas-identitas IAM Anda.

Kebijakan ini menyediakan akses administratif penuh untuk melihat atau memodifikasi saham sumber daya yang dimiliki oleh AndaAkun AWS.

Hal ini dilakukan dengan memberikan izin untuk menjalankan `ram` operasi.

Detail izin

Kebijakan ini mencakup izin berikut.

- `ram`- Memungkinkan prinsipal untuk melihat atau memodifikasi informasi tentang saham sumber daya yang dimiliki oleh Akun AWS.

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

```

        "Action": [
            "ram:*"
        ],
        "Effect": "Allow",
        "Resource": "*"
    }
]
}

```

Kebijakan terkelola AWS:

AWSResourceAccessManagerResourceShareParticipantAccess

Anda dapat melampirkan kebijakan

AWSResourceAccessManagerResourceShareParticipantAccess ke identitas-identitas IAM Anda.

Kebijakan ini memberikan prinsip-prinsip kemampuan untuk menerima atau menolak saham sumber daya yang dibagikan dengan iniAkun AWS, dan untuk melihat rincian tentang saham sumber daya ini. Itu tidak memberikan kemampuan apa pun untuk memodifikasi saham sumber daya tersebut.

Hal ini dilakukan dengan memberikan izin untuk menjalankan beberaparamoperasi.

Detail izin

Kebijakan ini mencakup izin berikut.

- `ram-` Memungkinkan prinsipal untuk menerima atau menolak undangan berbagi sumber daya dan untuk melihat rincian tentang saham sumber daya yang dibagikan dengan akun.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ram:AcceptResourceShareInvitation",
        "ram:GetResourcePolicies",
        "ram:GetResourceShareInvitations",
        "ram:GetResourceShares",
        "ram:ListPendingInvitationResources",
        "ram:ListPrincipals",
        "ram:ListResources",

```

```

        "ram:RejectResourceShareInvitation"
    ],
    "Effect": "Allow",
    "Resource": "*"
  }
]
}

```

Kebijakan terkelola AWS: AWSResourceAccessManagerServiceRolePolicy

Yang AWS kebijakan terkelola AWSResourceAccessManagerServiceRolePolicy hanya dapat digunakan dengan peran terkait layanan untuk AWS RAM. Anda tidak dapat melampirkan, melepaskan, memodifikasi, atau menghapus kebijakan ini.

Kebijakan ini menyediakan AWS RAM dengan akses hanya-baca ke struktur organisasi Anda. Ketika Anda mengaktifkan integrasi antara AWS RAM dan AWS Organizations, AWS RAM secara otomatis membuat peran terkait layanan bernama [AWSServiceRoleForResourceAccessManager](#) bahwa layanan mengasumsikan ketika perlu mencari informasi tentang organisasi Anda dan akunnya, misalnya, ketika Anda melihat struktur organisasi di AWS RAM konsol.

Hal ini dilakukan dengan memberikan izin read-only untuk menjalankan `organizations:Describe` dan `organizations:List` operasi yang memberikan rincian struktur dan akun organisasi.

Detail izin

Kebijakan ini mencakup izin berikut.

- `organizations`- Memungkinkan prinsipal untuk melihat informasi tentang struktur organisasi, termasuk unit organisasi, dan Akun AWS mereka mengandung.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:ListAccounts",

```

```

        "organizations:ListAccountsForParent",
        "organizations:ListChildren",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListRoots"
    ],
    "Resource": "*"
},
{
    "Sid": "AllowDeletionOfServiceLinkedRoleForResourceAccessManager",
    "Effect": "Allow",
    "Action": [
        "iam:DeleteRole"
    ],
    "Resource": [
        "arn:aws:iam::*:role/aws-service-role/ram.amazonaws.com/*"
    ]
}
]
}

```

AWS RAM memperbarui pada kebijakan terkelola AWS

Lihat detail tentang pembaruan terhadap kebijakan terkelola AWS untuk AWS RAM sejak layanan ini mulai melacak perubahan-perubahan tersebut. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman Riwayat dokumen AWS RAM.

| Perubahan | Deskripsi | Tanggal |
|---|---|--------------------|
| AWS Resource Access Manager mulai melacak perubahan | AWS RAM mendokumentasikan kebijakan terkelola yang ada dan mulai melacak perubahan. | September 16, 2021 |

Menggunakan Peran Tertaut Layanan untuk AWS RAM

AWS Resource Access Manager menggunakan AWS Identity and Access Management (IAM) [peran tertaut layanan](#). Peran terkait layanan adalah jenis peran IAM unik yang ditautkan langsung ke layanan. AWS RAM Peran terkait layanan telah ditentukan sebelumnya oleh AWS dan menyertakan semua izin yang AWS RAM perlu memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat konfigurasi AWS RAM lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. AWS RAM mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya AWS RAM dapat mengambil peran terkait layanannya. Izin yang ditetapkan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas IAM lainnya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, silakan lihat [Layanan AWS yang bisa digunakan dengan IAM](#) dan carilah layanan yang memiliki opsi Ya di kolom Peran Terkait Layanan. Pilih Ya dengan tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Izin Peran Tertaut Layanan untuk AWS RAM

AWS RAM menggunakan nama peran terkait layanan `AWSServiceRoleForResourceAccessManager` saat Anda mengaktifkan berbagi dengan AWS Organizations. Peran ini memberikan izin ke AWS RAM layanan untuk melihat detail organisasi, seperti daftar akun anggota dan unit organisasi mana setiap akun berada.

Peran terkait layanan ini mempercayai layanan berikut untuk mengambil peran:

- `ram.amazonaws.com`

Kebijakan izin peran bernama `AWSResourceAccessManagerServiceRolePolicy` dilampirkan ke peran terkait layanan ini, dan memungkinkan AWS RAM untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan: tindakan hanya-baca yang mengambil detail tentang struktur organisasi Anda. Untuk daftar tindakan lengkap, Anda dapat melihat kebijakan di konsol IAM: [AWSResourceAccessManagerServiceRolePolicy](#).

Agar prinsipal mengaktifkan AWS RAM berbagi dalam organisasi Anda, prinsipal tersebut (entitas IAM seperti pengguna, grup, atau peran), harus memiliki izin untuk membuat peran terkait layanan. Untuk informasi selengkapnya, silakan lihat [Izin Peran Terkait Layanan](#) di Panduan Pengguna IAM.

Membuat Peran Terkait Layanan untuk AWS RAM

Anda tidak perlu membuat peran tertaut layanan secara manual. Saat Anda mengaktifkan AWS RAM berbagi dalam organisasi Anda di AWS Management Console, atau menjalankan

[EnableSharingWithAwsOrganization](#) di akun Anda menggunakan AWS CLI atau AWS API, AWS RAM buat peran terkait layanan untuk Anda.

Hubungi `enable-sharing-with-aws-organizations` untuk membuat peran terkait layanan di akun Anda.

Jika Anda menghapus peran terkait layanan ini, maka AWS RAM tidak lagi memiliki izin untuk melihat detail struktur organisasi Anda.

Mengedit peran terkait layanan untuk AWS RAM

AWS RAM tidak memungkinkan Anda untuk mengedit peran `AWSResourceAccessManagerServiceRolePolicy` terkait layanan. Setelah membuat peran tertaut layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengedit deskripsi peran menggunakan IAM. Untuk informasi selengkapnya, silakan lihat [Mengedit peran tertaut layanan](#) dalam Panduan Pengguna IAM.

Menghapus Peran Tertaut Layanan untuk AWS RAM

Anda dapat menggunakan konsol IAM, AWS CLI atau AWS API untuk menghapus peran terkait layanan secara manual.

Untuk menghapus peran terkait layanan secara manual menggunakan IAM

Gunakan konsol IAM, AWS CLI, atau API AWS untuk menghapus peran tertaut layanan `AWSResourceAccessManagerServiceRolePolicy`. Untuk informasi lebih lanjut, lihat [Menghapus Peran Terkait Layanan](#) dalam Panduan Pengguna IAM.

Wilayah yang Didukung untuk AWS RAM Peran Terkait Layanan

AWS RAM memberikan dukungan dengan peran yang terhubung dengan layanan di semua Wilayah tempat layanan tersedia. Untuk informasi selengkapnya, lihat [AWS Wilayah dan Titik Akhir](#) di Referensi Umum Amazon Web Services

Contoh kebijakan IAM untuk AWS RAM

Topik ini mencakup contoh kebijakan IAM untuk AWS RAM yang menunjukkan berbagi sumber daya tertentu dan jenis sumber daya serta membatasi berbagi.

Contoh kebijakan IAM

- [Contoh 1: Izinkan berbagi sumber daya tertentu](#)

- [Contoh 2: Izinkan berbagi jenis sumber daya tertentu](#)
- [Contoh 3: Batasi berbagi dengan eksternal Akun AWS](#)

Contoh 1: Izinkan berbagi sumber daya tertentu

Anda dapat menggunakan kebijakan izin IAM untuk membatasi prinsipal untuk mengaitkan hanya sumber daya tertentu dengan berbagi sumber daya.

Misalnya, kebijakan berikut membatasi prinsipal untuk hanya membagikan aturan resolver dengan Amazon Resource Name (ARN) yang ditentukan. Operator `StringEqualsIfExists` mengizinkan permintaan jika permintaan tidak menyertakan `ResourceArn` parameter, atau jika itu menyertakan parameter itu, nilainya sama persis dengan ARN yang ditentukan.

Untuk informasi lebih lanjut tentang kapan dan mengapa menggunakan `...IfExists` operator, lihat... [IfExistsoperator kondisi](#) di Panduan Pengguna IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
    "Resource": "*",
    "Condition": {
      "StringEqualsIfExists": {
        "ram:ResourceArn": "arn:aws:route53resolver:us-
west-2:123456789012:resolver-rule/rslvr-rr-5328a0899aexample"
      }
    }
  }]
}
```

Contoh 2: Izinkan berbagi jenis sumber daya tertentu

Anda dapat menggunakan kebijakan IAM untuk membatasi prinsipal untuk mengaitkan hanya jenis sumber daya tertentu dengan berbagi sumber daya.

Misalnya, kebijakan berikut membatasi prinsipal untuk hanya membagikan aturan penyelesai.

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

```

    "Effect": "Allow",
    "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
    "Resource": "*",
    "Condition": {
      "StringEqualsIfExists": {
        "ram:RequestedResourceType": "route53resolver:ResolverRule"
      }
    }
  }
}

```

Contoh 3: Batasi berbagi dengan eksternal Akun AWS

Anda dapat menggunakan kebijakan IAM untuk mencegah prinsipal berbagi sumber daya dengan Akun AWS yang berada di luar organisasinya. AWS

Misalnya, kebijakan IAM berikut mencegah prinsipal menambahkan eksternal Akun AWS ke saham sumber daya.

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "ram:CreateResourceShare",
    "Resource": "*",
    "Condition": {
      "Bool": {
        "ram:RequestedAllowsExternalPrincipals": "false"
      }
    }
  }]
}

```

Contoh kebijakan kontrol layanan untuk AWS Organizations dan AWS RAM

AWS RAM mendukung kebijakan kontrol layanan (SCP). SCP adalah kebijakan yang Anda lampirkan ke elemen dalam organisasi untuk mengelola izin dalam organisasi tersebut. SCP berlaku untuk semua Akun AWS [di bawah elemen yang Anda lampirkan SCP](#). SCP menawarkan kontrol pusat atas izin maksimum yang tersedia untuk semua akun di organisasi Anda. Mereka dapat membantu Anda memastikan Anda Akun AWS tetap berada dalam pedoman kontrol akses organisasi Anda. Untuk informasi selengkapnya, lihat [Kebijakan kontrol layanan](#) di Panduan AWS Organizations Pengguna.

Prasyarat

Untuk menggunakan SCP, Anda harus terlebih dahulu melakukan hal berikut:

- Aktifkan semua fitur di organisasi Anda. Untuk informasi selengkapnya, lihat [Mengaktifkan semua fitur di organisasi Anda](#) di AWS Organizations Panduan Pengguna
- Aktifkan SCP untuk digunakan dalam organisasi Anda. Untuk informasi selengkapnya, lihat [Mengaktifkan dan menonaktifkan jenis kebijakan di Panduan](#) Pengguna AWS Organizations
- Buat SCP yang Anda butuhkan. Untuk informasi selengkapnya tentang membuat SCP, lihat [Membuat dan memperbarui SCP](#) di AWS Organizations Panduan Pengguna.

Contoh Kebijakan Kontrol Layanan

Daftar Isi

- [Contoh 1: Mencegah berbagi eksternal](#)
- [Contoh 2: Mencegah pengguna menerima undangan berbagi sumber daya dari akun eksternal di luar organisasi Anda](#)
- [Contoh 3: Izinkan akun tertentu untuk berbagi jenis sumber daya tertentu](#)
- [Contoh 4: Mencegah berbagi dengan seluruh organisasi atau dengan unit organisasi](#)
- [Contoh 5: Izinkan berbagi hanya dengan prinsipal tertentu](#)

Contoh berikut menunjukkan bagaimana Anda dapat mengontrol berbagai aspek berbagi sumber daya dalam suatu organisasi.

Contoh 1: Mencegah berbagi eksternal

SCP berikut mencegah pengguna membuat pembagian sumber daya yang memungkinkan berbagi dengan prinsipal yang berada di luar organisasi pengguna berbagi.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:CreateResourceShare",
        "ram:UpdateResourceShare"
      ],
    },
  ],
}
```

```

        "Resource": "*",
        "Condition": {
            "Bool": {
                "ram:RequestedAllowsExternalPrincipals": "true"
            }
        }
    }
]
}

```

Contoh 2: Mencegah pengguna menerima undangan berbagi sumber daya dari akun eksternal di luar organisasi Anda

SCP berikut memblokir prinsipal apa pun di akun yang terpengaruh agar tidak menerima undangan untuk menggunakan pembagian sumber daya. Pembagian sumber daya yang dibagikan ke akun lain di organisasi yang sama dengan akun berbagi tidak menghasilkan undangan dan karenanya tidak terpengaruh oleh SCP ini.

```

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

```

Contoh 3: Izinkan akun tertentu untuk berbagi jenis sumber daya tertentu

SCP berikut hanya mengizinkan akun 111111111111 dan 222222222222 membuat pembagian sumber daya baru yang berbagi daftar awalan Amazon EC2 atau untuk mengaitkan daftar awalan dengan pembagian sumber daya yang ada.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:AssociateResourceShare",

```

```

        "ram:CreateResourceShare"
    ],
    "Resource": "*",
    "Condition": {
        "StringNotEquals": {
            "aws:PrincipalAccount": [
                "111111111111",
                "222222222222"
            ]
        },
        "StringEqualsIfExists": {
            "ram:RequestedResourceType": "ec2:PrefixList"
        }
    }
}
]
}

```

Contoh 4: Mencegah berbagi dengan seluruh organisasi atau dengan unit organisasi

SCP berikut mencegah pengguna membuat pembagian sumber daya yang berbagi sumber daya dengan seluruh organisasi atau dengan unit organisasi apa pun. Pengguna dapat berbagi dengan individu Akun AWS dalam organisasi, atau dengan peran IAM atau pengguna.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:CreateResourceShare",
        "ram:AssociateResourceShare"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "ram:Principal": [
            "arn:aws:organizations::*:organization/*",
            "arn:aws:organizations::*:ou/*"
          ]
        }
      }
    }
  ]
}

```

```
]
}
```

Contoh 5: Izinkan berbagi hanya dengan prinsipal tertentu

Contoh SCP berikut memungkinkan pengguna untuk berbagi sumber daya dengan hanya unit organisasi o-12345abcdef, organisasiou-98765fedcba, dan Akun AWS111111111111.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:AssociateResourceShare",
        "ram:CreateResourceShare"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringNotEquals": {
          "ram:Principal": [
            "arn:aws:organizations::123456789012:organization/
o-12345abcdef",
            "arn:aws:organizations::123456789012:ou/o-12345abcdef/
ou-98765fedcba",
            "111111111111"
          ]
        }
      }
    }
  ]
}
```

Menonaktifkan berbagi sumber daya dengan AWS Organizations

Jika sebelumnya Anda mengaktifkan berbagi dengan AWS Organizations dan Anda tidak perlu lagi berbagi sumber daya dengan seluruh organisasi atau unit organisasi (OU), Anda dapat menonaktifkan berbagi. Saat Anda menonaktifkan berbagi AWS Organizations, semua organisasi atau OU dihapus dari pembagian sumber daya yang telah Anda buat dan mereka kehilangan akses ke sumber daya bersama. Akun eksternal (akun yang ditambahkan ke pembagian sumber daya melalui undangan) tidak akan terpengaruh, dan akan terus dikaitkan dengan pembagian sumber daya.

Untuk menonaktifkan berbagi dengan AWS Organizations

1. Nonaktifkan akses tepercaya untuk AWS Organizations menggunakan AWS Organizations [disable-aws-service-access](#) AWS CLI perintah.

```
$ aws organizations disable-aws-service-access --service-principal  
ram.amazonaws.com
```

Important

Saat Anda menonaktifkan akses tepercaya ke AWS Organizations, prinsipal dalam organisasi Anda akan dihapus dari semua pembagian sumber daya dan kehilangan akses ke sumber daya bersama tersebut.

2. Gunakan konsol IAM, operasi API IAM AWS CLI, atau IAM untuk menghapus peran terkait `AWSServiceRoleForResourceAccessManager` layanan. Untuk informasi selengkapnya, lihat [Menghapus peran tertaut layanan](#) dalam Panduan Pengguna IAM.

Pencatatan dan pemantauan di AWS RAM

Pemantauan adalah bagian penting dari pemeliharaan keandalan, ketersediaan, dan performa AWS RAM serta solusi AWS Anda. Anda harus mengumpulkan data pemantauan dari semua bagian dari AWS solusi Anda sehingga Anda dapat dengan lebih mudah melakukan debug kegagalan multi-titik jika terjadi. AWS menyediakan beberapa alat untuk memantau AWS RAM sumber daya Anda dan merespons potensi insiden:

CloudWatch Acara Amazon

Memberikan near-real-time aliran peristiwa sistem yang menjelaskan perubahan dalam AWS sumber daya. CloudWatch Events memungkinkan komputasi berbasis peristiwa otomatis, karena Anda dapat menulis peraturan yang mengawasi peristiwa tertentu dan memicu tindakan otomatis dalam AWS layanan lainnya saat peristiwa ini terjadi. Untuk informasi selengkapnya, lihat [Pemantauan AWS RAM menggunakan CloudWatch Acara](#).

AWS CloudTrail

Menangkap panggilan API dan kejadian terkait yang dibuat atas nama Anda Akun AWS dan mengirimkan berkas log ke bucket Amazon S3 Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun yang memanggil AWS, alamat IP asal panggilan dilakukan, dan waktu

panggilan terjadi. Untuk informasi selengkapnya, lihat [Mencatat log panggilan API AWS RAM dengan AWS CloudTrail](#).

PemantauanAWS RAM menggunakan CloudWatch Acara

Menggunakan Amazon CloudWatch Events, Anda dapat menyiapkan notifikasi otomatis untuk peristiwa tertentu diAWS RAM. Peristiwa dariAWS RAM dikirimkan ke CloudWatch Peristiwa dalam hampir waktu nyata. Anda dapat mengonfigurasi CloudWatch Acara untuk memantau peristiwa dan memanggil target sebagai respons terhadap peristiwa yang menunjukkan perubahan pada pembagian sumber daya Anda. Perubahan pada pembagian sumber daya memicu peristiwa untuk pemilik pangsa sumber daya dan prinsipal yang diberikan akses ke pangsa sumber daya.

Saat Anda membuat pola acara, sumbernya adalah `aws . ram`.

Note

Berhati-hatilah menulis kode yang tergantung pada peristiwa ini. Peristiwa ini tidak dijamin dijamin, tetapi dipancarkan atas dasar upaya terbaik. Jika terjadi kesalahan saatAWS RAM mencoba memancarkan peristiwa, layanan akan mencoba beberapa kali lagi. Namun, dapat waktu keluar dan mengakibatkan hilangnya peristiwa tertentu.

Untuk informasi selengkapnya, lihat [Panduan Pengguna Amazon CloudWatch Events](#).

Contoh: Memberi tahu kegagalan pembagian sumber daya

Pertimbangkan skenario tempat Anda ingin berbagi reservasi kapasitas Amazon EC2 dengan akun lain di organisasi Anda. Melakukan hal ini adalah cara yang baik untuk mengurangi biaya Anda.

Namun, jika Anda tidak memenuhi semua [prasyarat untuk berbagi reservasi kapasitas](#), maka secara diam-diam dapat gagal melakukan tugas asinkron yang terlibat dalam berbagi sumber daya. Jika operasi berbagi gagal, dan pengguna Anda di akun lain mencoba meluncurkan instans dengan salah satu reservasi kapasitas tersebut, maka Amazon EC2 bertindak seolah-olah reservasi kapasitas penuh dan meluncurkan instans sebagai instans sesuai permintaan. Hal ini dapat menghasilkan biaya yang lebih tinggi dari yang diharapkan.

Untuk memantau kegagalan berbagi sumber daya, siapkan aturan Amazon CloudWatch Events yang memberi tahu Anda setiap kali pembagianAWS RAM sumber daya gagal. Prosedur tutorial

berikut ini menggunakan topik Amazon Simple Notification Service (SNS) untuk memberi tahu semua pelanggan topik saat EventBridge menemukan kegagalan berbagi sumber daya. Untuk informasi selengkapnya tentang Amazon SNS, lihat [Panduan Developer Amazon Simple Notification Service](#).

Membuat aturan yang memberi tahu Anda saat berbagi sumber daya gagal

1. Buka [EventBridge konsol Amazon](#).
2. Di panel navigasi, pilih Aturan, dan kemudian dalam daftar Aturan, pilih Buat aturan.
3. Masukkan nama dan deskripsi opsional untuk aturan Anda, lalu pilih Berikutnya.
4. Gulir ke bawah ke kotak Event pattern, dan pilih Custom patterns (JSON editor).
5. Salin dan menempelkan pola event berikut ini:

```
{
  "source": ["aws.ram"],
  "detail-type": ["Resource Sharing State Change"],
  "detail": {
    "event": ["Resource Share Association"],
    "status": ["failed"]
  }
}
```

6. Pilih Selanjutnya.
7. Untuk Target 1, di bawah Jenis target, pilih Layanan AWS.
8. Di bawah Pilih target, pilih topik SNS.
9. Untuk topik, pilih topik SNS tempat Anda ingin menerbitkan notifikasi. Topik ini harus ada ada ada ada ada ada ada ada ada
10. Pilih Berikutnya, lalu pilih Berikutnya lagi untuk melihat untuk meninjau konfigurasi Anda.
11. Setelah Anda puas dengan opsi Anda puas, pilih Buat aturan Anda puas menggunakan opsi Anda, pilih Buat aturan.
12. Kembali ke halaman Aturan, pastikan aturan baru Anda ditandai Diaktifkan. Jika perlu, pilih tombol radio di sebelah nama aturan Anda, lalu pilih Aktifkan.

Selama aturan tersebut diaktifkan, setiap bagian AWS RAM sumber daya yang gagal menghasilkan peringatan SNS ke penerima topik yang Anda publikasikan.

Anda juga dapat mengonfirmasi bahwa reservasi kapasitas bersama dapat diakses oleh akun yang Anda bagikan dengan mencoba [melihatnya di konsol Amazon EC2 dari akun tersebut](#).

Mencatat log panggilan API AWS RAM dengan AWS CloudTrail

AWS RAM terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di AWS RAM. CloudTrail merekam semua panggilan API untuk AWS RAM sebagai kejadian. Panggilan yang direkam mencakup panggilan dari AWS RAM konsol dan panggilan kode ke operasi API AWS RAM ini. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman berkelanjutan CloudTrail peristiwa ke bucket Amazon S3 yang Anda tentukan, termasuk peristiwa untuk AWS RAM. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru dalam CloudTrail konsol di Riwayat peristiwa. Gunakan informasi yang dikumpulkan oleh CloudTrail untuk menentukan permintaan yang diajukan ke AWS RAM, alamat IP yang meminta, peminta, kapan dibuat, dan detail tambahan.

Untuk informasi selengkapnya CloudTrail, lihat [Panduan AWS CloudTrail Pengguna](#).

AWS RAM informasi dalam CloudTrail

CloudTrail diaktifkan pada Anda Akun AWS saat Anda membuat akun tersebut. Saat aktivitas terjadi di AWS RAM, aktivitas tersebut dicatat dalam CloudTrail peristiwa AWS layanan lainnya di Riwayat peristiwa peristiwa. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di Akun AWS Anda. Untuk informasi selengkapnya, lihat [Melihat Kejadian dengan Riwayat CloudTrail Kejadian](#).

Untuk catatan berkelanjutan tentang peristiwa di Akun AWS, termasuk peristiwa untuk AWS RAM, buat jejak. Jejak memungkinkan CloudTrail untuk mengirim berkas log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di dalam konsol tersebut, jejak diterapkan ke semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lainnya untuk dianalisis lebih lanjut dan bertindak berdasarkan data kejadian yang dikumpulkan di CloudTrail log. Untuk informasi selengkapnya, lihat yang berikut:

- [Membuat jejak untuk Anda Akun AWS](#)
- [Layanan AWS integrasi dengan CloudTrail log](#)
- [Mengonfigurasi Notifikasi Amazon SNS untuk CloudTrail](#)
- [Menerima berkas CloudTrail log dari beberapa Wilayah](#) dan [Menerima berkas CloudTrail log dari beberapa akun](#)

Semua AWS RAM tindakan dicatat oleh CloudTrail dan didokumentasikan dalam [Referensi AWS RAM API](#). Misalnya, panggilan untuk tindakan `CreateResourceShare`, `AssociateResourceShare`, dan `EnableSharingWithAwsOrganization` menghasilkan entri dalam file log CloudTrail.

Setiap entri kejadian atau log berisi informasi yang membantu Anda menentukan siapa yang membuat permintaan tersebut.

- Akun AWSkredenal root
- Kredensi keamanan sementara dari peranAWS Identity and Access Management (IAM) atau pengguna federasi.
- Kredenal keamanan jangka panjang dari pengguna IAM.
- AWSLayanan lain.

Untuk informasi selengkapnya, lihat [Elemen userIdentity CloudTrail](#).

Memahami entri file log AWS RAM

Jejak adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai berkas log ke bucket Amazon S3 yang Anda tentukan. CloudTrail berkas log berisi satu atau lebih entri log. Sebuah peristiwa mewakili permintaan tunggal dari sumber apa pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail berkas log bukan jejak tumpukan terurut dari panggilan API publik, sehingga berkas tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log untukCreateResourceShare tindakan tersebut.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "NOPIOSFODNN7EXAMPLE",
    "arn": "arn:aws:iam::111122223333:user/admin",
    "accountId": "111122223333",
    "accessKeyId": "BCDIOSFODNN7EXAMPLE",
    "userName": "admin"
  },
  "eventTime": "2018-11-03T04:23:19Z",
  "eventSource": "ram.amazonaws.com",
  "eventName": "CreateResourceShare",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.1.0",
  "userAgent": "aws-cli/1.16.2 Python/2.7.10 Darwin/16.7.0 botocore/1.11.2",
  "requestParameters": {
    "name": "foo"
  }
}
```

```
    },
    "responseElements": {
      "resourceShare": {
        "allowExternalPrincipals": true,
        "name": "foo",
        "owningAccountId": "111122223333",
        "resourceShareArn": "arn:aws:ram:us-east-1:111122223333:resource-share/EXAMPLE0-1234-abcd-1212-987656789098",
        "status": "ACTIVE"
      }
    },
    "requestID": "EXAMPLE0-abcd-1234-mnop-987654567876",
    "eventID": "EXAMPLE0-1234-abcd-hijk-543234565434",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
  }
}
```

Ketahanan di AWS RAM

Infrastruktur global AWS dibangun di sekitar Wilayah AWS dan Availability Zone. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi yang terhubung dengan jaringan latensi rendah, throughput tinggi, dan jaringan yang sangat berlebihan. Dengan Availability Zone, Anda dapat merancang dan mengoperasikan aplikasi dan basis data yang secara otomatis melakukan failover di antara Availability Zone tanpa gangguan. Availability Zone memiliki ketersediaan yang tinggi, toleran terhadap kesalahan, dan dapat diskalakan jika dibandingkan dengan infrastruktur pusat data tunggal atau ganda tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat [Infrastruktur Global AWS](#).

Keamanan infrastruktur dalam AWS RAM

Sebagai layanan terkelola, AWS Resource Access Manager dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat [Keamanan AWS Cloud](#). Untuk merancang AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat [Perlindungan](#) Infrastruktur dalam Kerangka Kerja Pilar Keamanan yang AWS Diarsiteksikan dengan Baik.

Anda menggunakan panggilan API AWS yang dipublikasikan untuk mengakses AWS RAM melalui jaringan. Klien harus mendukung hal berikut:

- Transport Layer Security (TLS). Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Suite cipher dengan kerahasiaan maju sempurna (PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan sistem yang lebih baru mendukung mode ini.

Selain itu, permintaan harus ditandatangani menggunakan access key ID dan secret access key yang terkait dengan principal IAM. Atau Anda bisa menggunakan [AWS Security Token Service](#) (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

Memecahkan masalah dengan AWS RAM

Gunakan informasi di bagian panduan ini untuk membantu Anda mendiagnosis dan memperbaiki masalah umum saat Anda bekerja dengan AWS Resource Access Manager (AWS RAM).

Topik

- [Kesalahan: "ID akun Anda tidak ada di AWS organisasi"](#)
- [Kesalahan: "AccessDeniedException"](#)
- [Kesalahan: "UnknownResourceException"](#)
- [Kesalahan saat mencoba berbagi dengan akun di luar organisasi saya](#)
- [Tidak dapat melihat sumber daya bersama di akun tujuan](#)
- [Kesalahan: Batas terlampaui](#)
- [Akun lain di organisasi saya tidak pernah menerima undangan](#)
- [Anda tidak dapat berbagi subnet VPC](#)

Kesalahan: "ID akun Anda tidak ada di AWS organisasi"

Skenario

Anda mendapatkan kesalahan "ID akun Anda tidak ada di AWS organisasi" ketika mencoba berbagi sumber daya dengan akun atau unit organisasi (OU) di organisasi Anda.

Penyebab

Kesalahan ini dapat terjadi jika peran terkait layanan

[AWSServiceRoleForResourceAccessManager](#) tidak berhasil dibuat saat Anda mengaktifkan integrasi antara AWS Resource Access Manager dan AWS Organizations

Solusi

Untuk membuat ulang peran terkait layanan yang diperlukan, lakukan langkah-langkah berikut untuk mematikan integrasi dan kemudian menyalakannya lagi.

1. Masuk ke akun manajemen organisasi Anda menggunakan peran IAM atau pengguna dengan izin administratif.

2. Arahkan ke [halaman Layanan di AWS Organizations konsol](#).
3. Pilih RAM.
4. Pilih Menonaktifkan akses terpercaya.
5. Arahkan ke [halaman Pengaturan di AWS RAM konsol](#).
6. Pilih kotak Aktifkan berbagi dengan AWS Organizations, lalu pilih Simpan pengaturan.

Important

Saat Anda menonaktifkan akses terpercaya ke AWS Organizations, prinsipal dalam organisasi Anda akan dihapus dari semua pembagian sumber daya dan kehilangan akses ke sumber daya bersama tersebut.

Anda sekarang harus dapat menggunakan AWS RAM untuk berbagi sumber daya Anda dengan akun dan OU di organisasi.

Kesalahan: "AccessDeniedException"

Skenario

Anda mendapatkan pengecualian Access Denied saat mencoba membagikan sumber daya atau melihat pembagian sumber daya.

Penyebab

Anda dapat menerima kesalahan ini jika mencoba membuat pembagian sumber daya saat Anda tidak memiliki izin yang diperlukan. Hal ini dapat disebabkan oleh izin yang tidak memadai dalam kebijakan yang dilampirkan pada prinsipal AWS Identity and Access Management (IAM) Anda. Hal ini juga dapat terjadi karena pembatasan diberlakukan dari kebijakan kontrol AWS Organizations layanan (SCP) yang mempengaruhi Anda/Akun AWS.

Solusi

Untuk memberikan akses, tambahkan izin ke pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

Buat rangkaian izin. Ikuti petunjuk dalam [Buat set izin](#) dalam Panduan Pengguna AWS IAM Identity Center.

- Pengguna yang dikelola di IAM melalui penyedia identitas:

Buat peran untuk federasi identitas. Ikuti petunjuk dalam [Membuat peran untuk penyedia identitas pihak ketiga \(federasi\)](#) di Panduan Pengguna IAM.

- Pengguna IAM:
 - Buat peran yang dapat diambil pengguna Anda. Ikuti petunjuk dalam [Membuat peran untuk pengguna IAM](#) dalam Panduan Pengguna IAM.
 - (Tidak disarankan) Pasang kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti petunjuk di [Menambahkan izin ke pengguna \(konsol\)](#) dalam Panduan Pengguna IAM.

Untuk mengatasi kesalahan, Anda perlu memastikan izin diberikan oleh Allow pernyataan dalam kebijakan izin yang digunakan oleh prinsipal yang membuat permintaan. Selain itu, izin tidak boleh diblokir oleh SCP organisasi Anda.

Untuk membuat pembagian sumber daya, Anda memerlukan dua izin berikut:

- `ram:CreateResourceShare`
- `ram:AssociateResourceShare`

Untuk melihat pembagian sumber daya, Anda memerlukan izin berikut:

- `ram:GetResourceShares`

Untuk melampirkan izin ke berbagi sumber daya, Anda memerlukan izin berikut:

- *`resourceOwnerService:PutPolicyAction`*

Ini adalah placeholder. Anda harus menggantinya dengan izin `PutPolicy ""` (atau setara) untuk layanan yang memiliki sumber daya yang ingin Anda bagikan. Misalnya, jika Anda membagikan aturan resolver Route 53, maka izin yang diperlukan adalah: `route53resolver:PutResolverRulePolicy` Jika Anda ingin mengizinkan pembuatan

berbagi sumber daya yang berisi beberapa jenis sumber daya, Anda harus menyertakan izin yang relevan untuk setiap jenis sumber daya yang ingin Anda izinkan.

Contoh berikut menunjukkan seperti apa kebijakan izin IAM tersebut.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ram:CreateResourceShare",
        "ram:AssociateResourceShare",
        "ram:GetResourceShares",
        "resourceOwningService:PutPolicyAction"
      ],
      "Resource": "*"
    }
  ]
}
```

Kesalahan: "UnknownResourceException"

Skenario

Anda mendapatkan salah satu kesalahan berikut:

- "CannotCreateResourceShare: UnknownResourceException: OrganizationalUnit ou- **xxxx** tidak dapat ditemukan"
- "CannotUpdateResourceShare: UnknownResourceException: OrganizationalUnit ou- **xxxx** tidak dapat ditemukan".

Penyebab

Kesalahan ini dapat terjadi jika Anda mengaktifkan integrasi antara AWS RAM dan AWS Organizations dengan menggunakan [konsol Organizations](#) atau [Organizations Enable AWSServiceAccess API](#), bukan dengan [menggunakan AWS RAM konsol](#). Bila Anda mengaktifkan integrasi dengan menggunakan konsol Organizations atau API, layanan tidak akan membuat

`AWSServiceRoleForResourceAccessManager` peran di akun Anda. Peran itu diperlukan untuk mengakses informasi tentang organisasi Anda. Karena peran tidak dibuat, tidak AWS RAM dapat mengakses detail tentang akun atau unit organisasi (OU) di organisasi Anda.

Solusi

Untuk mengatasi masalah ini, matikan integrasi antara AWS RAM dan AWS Organizations. Kemudian nyalakan lagi dengan memanggil operasi AWS RAM [EnableSharingWithAwsOrganization](#) API, atau dengan menggunakan AWS Management Console untuk melakukan langkah-langkah berikut.

1. Masuk ke akun manajemen organisasi Anda menggunakan peran IAM atau pengguna dengan izin administratif.
2. Arahkan ke [halaman Layanan di AWS Organizations konsol](#).
3. Pilih RAM.
4. Pilih Menonaktifkan akses terpercaya.
5. Arahkan ke [halaman Pengaturan di AWS RAM konsol](#).
6. Pilih kotak Aktifkan berbagi dengan AWS Organizations, lalu pilih Simpan pengaturan.

Important

Saat Anda menonaktifkan akses terpercaya ke AWS Organizations, prinsipal dalam organisasi Anda akan dihapus dari semua pembagian sumber daya dan kehilangan akses ke sumber daya bersama tersebut.

Anda sekarang harus dapat menggunakan AWS RAM untuk berbagi sumber daya Anda dengan akun dan OU di organisasi.

Kesalahan saat mencoba berbagi dengan akun di luar organisasi saya

Skenario

Anda mendapatkan salah satu kesalahan berikut saat mencoba berbagi sumber daya dengan akun yang berada di luar organisasi Anda:

- “Anda tidak dapat berbagi sumber daya di luar organisasi Anda. “
- Sumber daya yang Anda coba bagikan hanya dapat dibagikan dalam AWS Organisasi Anda. “
- “InvalidParameterException: Principal Account-ID tidak ada di organisasi Anda AWS. Anda tidak memiliki izin untuk menambahkan eksternal Akun AWS ke berbagi sumber daya. “
- Sumber daya yang Anda coba bagikan hanya dapat dibagikan dalam AWS Organisasi Anda. OperationNotPermittedException “

Kemungkinan penyebab dan solusi

Beberapa jenis sumber daya hanya dapat dibagikan dengan akun di organisasi yang sama

Beberapa jenis sumber daya tidak dapat dibagikan dengan akun apa pun yang bukan anggota organisasi tersebut. Contoh jenis sumber daya dengan batasan ini adalah koneksi pribadi virtual (VPC) yang merupakan bagian dari Amazon Elastic Compute Cloud (Amazon EC2).

[Untuk memverifikasi apakah Anda dapat berbagi jenis sumber daya tertentu dengan akun dan kepala sekolah di luar organisasi, lihat Sumber daya yang dapat dibagikan. AWS](#)


Peran terkait layanan tidak berhasil dibuat

Masalah ini dapat terjadi jika peran terkait layanan `AWSServiceRoleForResourceAccessManager` tidak berhasil dibuat saat Anda mengaktifkan integrasi antara AWS RAM dan. AWS Organizations

Jika Anda menerima salah satu kesalahan ini saat mencoba berbagi sumber daya dengan akun yang merupakan bagian dari organisasi Anda, lakukan langkah-langkah berikut untuk menghapus dan membuat ulang peran terkait layanan.

1. Masuk ke akun manajemen organisasi Anda menggunakan peran IAM atau pengguna dengan izin administratif.
2. Arahkan ke [halaman Layanan di AWS Organizations konsol](#).
3. Pilih RAM.
4. Pilih Menonaktifkan akses terpercaya.
5. Arahkan ke [halaman Pengaturan di AWS RAM konsol](#).

6. Pilih kotak Aktifkan berbagi dengan AWS Organizations, lalu pilih Simpan pengaturan.

 Important

Saat Anda menonaktifkan akses tepercaya ke AWS Organizations, prinsipal dalam organisasi Anda akan dihapus dari semua pembagian sumber daya dan kehilangan akses ke sumber daya bersama tersebut.

Tidak dapat melihat sumber daya bersama di akun tujuan

Skenario

Pengguna tidak dapat melihat sumber daya yang mereka yakini dibagikan dengan mereka dari orang lain Akun AWS.

Kemungkinan penyebab dan solusi

Berbagi dengan AWS Organizations diaktifkan dengan menggunakan Organizations, bukan AWS RAM

Jika AWS Organizations diaktifkan dengan menggunakan Organizations alih-alih AWS RAM, maka berbagi dalam organisasi gagal. Untuk memeriksa apakah ini penyebab masalah, navigasikan ke [halaman Pengaturan di AWS RAM konsol](#) dan verifikasi bahwa kotak AWS Organizations centang Aktifkan berbagi dengan dipilih.

- Jika kotak centang dipilih, maka ini bukan penyebabnya.
 - Jika kotak centang tidak dipilih, maka ini mungkin penyebabnya. Jangan pilih kotak centang. Lakukan langkah-langkah berikut untuk memperbaiki situasi.
1. Masuk ke akun manajemen organisasi Anda menggunakan peran IAM atau pengguna dengan izin administratif.
 2. Arahkan ke [halaman Layanan di AWS Organizations konsol](#).
 3. Pilih RAM.
 4. Pilih Menonaktifkan akses tepercaya.
 5. Arahkan ke [halaman Pengaturan di AWS RAM konsol](#).

6. Pilih kotak Aktifkan berbagi dengan AWS Organizations, lalu pilih Simpan pengaturan.

⚠ Important

Saat Anda menonaktifkan akses tepercaya ke AWS Organizations, prinsipal dalam organisasi Anda akan dihapus dari semua pembagian sumber daya dan kehilangan akses ke sumber daya bersama tersebut.

Anda mungkin perlu [memperbarui pembagian dan menentukan akun atau unit organisasi](#) dalam organisasi untuk dibagikan.

Pembagian sumber daya tidak menentukan akun ini sebagai prinsipal

Dalam Akun AWS yang membuat pembagian sumber daya, [lihat pembagian sumber daya](#) di [AWS RAM konsol](#). Verifikasi bahwa akun yang tidak dapat mengakses sumber daya terdaftar sebagai Principal. Jika tidak, maka [perbarui bagian untuk menambahkan akun sebagai prinsipal](#).

Peran atau pengguna di akun tidak memiliki izin minimum yang diperlukan

Saat Anda membagikan sumber daya di akun A ke akun B lain, peran dan pengguna di akun B tidak secara otomatis mendapatkan akses ke sumber daya dalam pembagian. Administrator akun B harus terlebih dahulu memberikan izin kepada peran IAM dan pengguna di akun B yang perlu mengakses sumber daya. Sebagai contoh, kebijakan berikut menunjukkan cara Anda memberikan akses hanya-baca ke peran dan pengguna di akun B untuk sumber daya dari akun A. Kebijakan ini menentukan sumber daya berdasarkan Nama Sumber [Daya Amazon \(ARN\)](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ram:Get*",
        "ram:List*"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:<service>:<Region-code>:<Account-A-ID>:<resource-id>"
    }
  ]
}
```

```
}
```

Sumber daya berbeda Wilayah AWS dari pengaturan konsol saat ini

AWS RAM adalah layanan regional. Sumber daya ada dalam spesifik Wilayah AWS, dan untuk melihatnya, AWS Management Console harus dikonfigurasi untuk melihat sumber daya di Wilayah itu.

Wilayah AWS yang saat ini diakses konsol ditampilkan di sudut kanan atas konsol. Untuk mengubahnya, pilih nama Wilayah saat ini dan dari menu tarik-turun, pilih Wilayah yang sumber dayanya ingin Anda lihat.

Kesalahan: Batas terlampaui

Skenario

Anda menerima "Anda telah mencapai batas jumlah sumber daya yang dapat Anda bagikan" atau "ResourceShareLimitExceededException" ketika mencoba berbagi sumber daya.

Penyebab

Kesalahan ini terjadi ketika Anda mencapai jumlah maksimum sumber daya yang dapat Anda bagikan menggunakan AWS RAM layanan atau Layanan AWS yang membuat sumber daya yang Anda coba bagikan. Kuota ini (sebelumnya disebut sebagai batas) dapat memengaruhi akun berbagi atau akun tempat Anda berbagi sumber daya.

Solusi

1. Untuk melihat kuota Anda, di Akun AWS tempat Anda melihat kesalahan, navigasikan ke salah satu halaman berikut, tergantung pada jenis kuota yang Anda capai:
 - [AWS RAM Halaman di konsol Service Quotas](#)
 - [Halaman untuk](#) sumber Layanan AWS dayanya dipengaruhi oleh kuota
2. Gulir ke bawah dan pilih kuota yang relevan.
3. Jika tersedia untuk kuota ini, pilih Minta kenaikan kuota.
4. Masukkan nilai baru untuk kuota, lalu pilih Permintaan.
5. Permintaan muncul di halaman [riwayat permintaan Kuota](#), di mana Anda dapat memeriksa status permintaan hingga selesai.

Akun lain di organisasi saya tidak pernah menerima undangan

Skenario

Ketika Anda berbagi sumber daya dengan akun lain di organisasi yang sama yang dikelola oleh AWS Organizations, mereka tidak menerima undangan.

Penyebab

Ini adalah perilaku yang diharapkan jika akun Anda mengaktifkan [pembagian dalam AWS organisasi](#).

Ketika opsi ini diaktifkan dan Anda berbagi dengan akun lain di organisasi Anda, tidak ada undangan yang dikirim dan tidak diperlukan penerimaan. Semua akun organisasi yang Anda referensikan sebagai prinsipal dalam pembagian sumber daya dapat segera mulai mengakses sumber daya dalam pembagian.

Jika akun Anda belum mengaktifkan berbagi dalam AWS organisasi, maka ketika Anda berbagi dengan akun lain, bahkan jika mereka berada di AWS organisasi yang sama, mereka diperlakukan sebagai akun mandiri. Undangan dikirim dan harus diterima sebelum pengguna dapat mengakses sumber daya dalam saham.

Anda tidak dapat berbagi subnet VPC

Skenario

Ketika Anda mencoba menggunakan AWS RAM untuk berbagi subnet VPC dengan akun lain, operasi berbagi berhasil. Namun, akun konsumsi menunjukkan LIMIT EXCEEDED sumber daya itu di AWS RAM konsol.

Penyebab

Beberapa jenis sumber daya individu memiliki batasan khusus layanan yang terpisah dari pembatasan yang diberlakukan oleh AWS RAM. Beberapa pembatasan tersebut dapat secara efektif mencegah berbagi bahkan jika Anda belum mencapai salah satu batasan di AWS RAM. Batas adalah contoh dari pembatasan ini. Amazon Virtual Private Cloud (Amazon VPC) membatasi jumlah subnet yang dapat Anda bagikan dengan akun individu lain. Jika Anda mencoba berbagi subnet dengan akun konsumsi yang sudah berisi jumlah maksimum subnet, maka akun yang mengkonsumsi itu ditampilkan LIMIT EXCEEDED di konsol untuk sumber daya itu. Untuk informasi selengkapnya

tentang batasan ini, lihat [Kuota VPC Amazon — Berbagi VPC](#) di Panduan Pengguna Amazon Virtual Private Cloud.

Untuk mengatasinya, pertama-tama periksa pembagian sumber daya lain yang mungkin membagikan sumber daya yang ditentukan dengan akun yang terpengaruh, dan hapus saham yang mungkin tidak lagi Anda perlukan. Anda juga dapat meminta kenaikan untuk batas yang mendukung penyesuaian. Gunakan [konsol Service Quotas](#) untuk meminta peningkatan batas.

 Note

AWS RAM tidak secara otomatis mendeteksi perubahan peningkatan batas. Anda harus mengaitkan kembali sumber daya atau prinsipal ke pembagian sumber daya untuk RAM untuk mendeteksi perubahan.

Kuota layanan untuk AWS RAM



Anda Akun AWS memiliki batasan berikut terkait dengan AWS Resource Access Manager (AWS RAM). Anda dapat meminta peningkatan untuk beberapa batas ini. Untuk meminta kenaikan batas, hubungi [AWS Support](#).

Note

Definisi berikut berlaku untuk deskripsi dalam kuota di bawah ini:

- Sumber Daya — Elemen Layanan AWS yang dibuat individual yang ingin Anda bagikan, seperti bucket Amazon S3 atau instans Amazon EC2. Setiap sumber daya yang direferensikan dalam pangsa sumber daya dihitung sebagai salah satu terhadap kuota ini. Jika Anda berbagi sumber daya yang sama dalam tiga saham sumber daya yang berbeda, itu meningkatkan jumlah Anda untuk kuota ini sebanyak tiga.
- Berbagi sumber daya — Container yang AWS RAM dibuat yang dapat Anda gunakan untuk berbagi sumber daya. Setiap pembagian sumber daya, terlepas dari berapa banyak sumber daya yang dikandungnya, dihitung sebagai salah satu terhadap kuota Anda.
- Prinsipal bersama - Pengenal yang telah Anda kaitkan dengan pembagian sumber daya. Ini bisa menjadi peran AWS Identity and Access Management (IAM) atau pengguna, Akun AWS pengenal, unit organisasi, atau seluruh organisasi. Setiap prinsipal bersama yang Anda referensikan dalam berbagi sumber menambahkan satu ke penggunaan kuota Anda. Jika Anda berbagi dengan seluruh organisasi dengan mereferensikan ID-nya, itu hanya dihitung sebagai satu terhadap kuota ini.
- Izin terkelola pelanggan - Izin terkelola yang Anda buat untuk mengatasi kasus penggunaan tertentu menggunakan akses hak istimewa paling sedikit untuk mengelola cara sumber daya bersama Anda digunakan.

| Resource | Batas default |
|--|---------------|
| Jumlah maksimum saham sumber daya per Wilayah AWS | 25,000 |
| Jumlah maksimum asosiasi sumber daya per pembagian sumber daya | 5,000 |

| Resource | Batas default |
|--|---------------|
| Jumlah maksimum asosiasi pokok per saham sumber daya | 5,000 |
| Jumlah maksimum izin yang dikelola pelanggan | 1,500 |
| Jumlah maksimum izin yang dikelola pelanggan per jenis sumber daya | 10 |
| Jumlah maksimum versi per izin terkelola pelanggan | 5 |
| Jumlah maksimum asosiasi sumber daya di semua saham sumber daya dalam Wilayah AWS | 25,000 |
| <div data-bbox="142 900 266 936">  Note </div> <div data-bbox="186 955 761 1234"> <p>Setiap sumber daya yang disertakan dalam pembagian sumber daya dihitung terhadap batas ini. Jika sumber daya termasuk dalam 10 saham sumber daya yang berbeda, yang menghitung 10 terhadap batas.</p> </div> | |
| Jumlah maksimum asosiasi pokok di semua saham sumber daya dalam Wilayah AWS | 25,000 |
| <div data-bbox="142 1474 266 1509">  Note </div> <div data-bbox="186 1528 756 1803"> <p>Setiap pokok yang termasuk dalam pangsa sumber daya dihitung terhadap batas ini. Jika kepala sekolah termasuk dalam 10 saham sumber daya yang berbeda, yang menghitung 10 terhadap batas.</p> </div> | |

| Resource | Batas default |
|---|---------------|
| <p>Jumlah maksimum undangan yang tertunda per akun berbagi</p> <ul style="list-style-type: none">• Kuota ini hanya berlaku untuk mengirim akun yang berbagi dengan akun yang bukan bagian yang sama AWS Organizations.• Tidak ada kuota untuk membatasi jumlah undangan yang tertunda yang dapat dimiliki akun penerima.• Undangan tidak digunakan saat berbagi antar akun yang merupakan bagian dari akun yang sama AWS Organizations dan Anda telah mengaktifkan berbagi sumber daya di dalam akun. AWS Organizations | 250 |

Menggunakan AWS RAM dengan AWS SDK

AWSKit pengembangan perangkat lunak (SDK) tersedia untuk banyak bahasa pemrograman populer. Setiap SDK menyediakan API, contoh kode, dan dokumentasi yang membantu pengembang membuat aplikasi dalam bahasa pilihan mereka.

| Dokumentasi SDK | Contoh kode |
|--|--|
| AWS SDK for C++ | AWS SDK for C++ contoh kode |
| AWS SDK for Go | AWS SDK for Go contoh kode |
| AWS SDK for Java | AWS SDK for Java contoh kode |
| AWS SDK for JavaScript | AWS SDK for JavaScript contoh kode |
| AWS SDK for .NET | AWS SDK for .NET contoh kode |
| AWS SDK for PHP | AWS SDK for PHP contoh kode |
| AWS SDK for Python (Boto3) | AWS SDK for Python (Boto3) contoh kode |
| AWS SDK for Ruby | AWS SDK for Ruby contoh kode |

Contoh ketersediaan

Tidak menemukan apa yang Anda butuhkan? Minta contoh kode dengan tautan umpan balik.

Riwayat dokumen untuk Panduan AWS RAM Pengguna

Tabel berikut menjelaskan penambahan penting pada AWS Resource Access Manager dokumentasi. Kami juga memperbarui dokumentasi untuk mengatasi umpan balik yang Anda kirimkan kepada kami.

Untuk pemberitahuan tentang pembaruan ini, Anda dapat berlangganan umpan AWS RAM RSS.

| Perubahan | Deskripsi | Tanggal |
|---|---|-------------------|
| Ditambahkan dukungan untuk berbagi Amazon Route 53 ResolverProfiles | Anda sekarang dapat menggunakan AWS RAM untuk berbagi Amazon Route 53 Resolver Profiles dengan orang lain Akun AWS dalam organisasi Anda. | April 22, 2024 |
| Menambahkan dukungan untuk berbagi sumber daya AWS Systems Manager Parameter Store. | Anda sekarang dapat berbagi parameter lanjutan dengan aman dan efisien di seluruh Akun AWS atau di dalam organisasi Anda. | Februari 21, 2024 |
| Ditambahkan dukungan untuk berbagi Amazon FSx untuk OpenZFS Snapshots. | Anda sekarang dapat berbagi Amazon FSx untuk OpenZFS Snapshots dengan yang lain dalam organisasi Anda. Akun AWS | Desember 19, 2023 |
| Menambahkan dukungan untuk berbagi Amazon Simple Storage Service sumber daya. | Anda sekarang dapat berbagi Instans Hibah Amazon Simple Storage Service Akses dengan orang lain Akun AWS atau organisasi Anda. AWS RAM | 27 November 2023 |
| Ditambahkan dukungan untuk berbagi Penjelajah Sumber Daya AWS pandangan. | Anda sekarang dapat berbagi Penjelajah Sumber Daya AWS tampilan dengan orang lain | 14 November 2023 |

| | | |
|--|---|-----------------|
| | Akun AWS dalam organisasi Anda. | |
| Menambahkan dukungan untuk berbagi sumber daya Pengontrol Pemulihan Aplikasi Amazon Route 53. | Anda sekarang dapat berbagi Amazon Route 53 Application Recovery Controller cluster dengan orang lain Akun AWS atau organisasi Anda. AWS RAM | 18 Oktober 2023 |
| Menambahkan dukungan untuk berbagi DataZone sumber daya Amazon. | Anda sekarang dapat berbagi DataZone sumber daya Amazon dengan orang lain Akun AWS atau organisasi Anda. | 4 Oktober 2023 |
| Menambahkan dukungan untuk berbagi prinsip layanan. | Anda sekarang dapat mengaitkan prinsip layanan ke pembagian sumber daya. Ini memungkinkan layanan tertentu untuk mengelola tindakan yang diperlukan untuk sumber daya pelanggan atas nama Anda. | 29 Agustus 2023 |
| Menambahkan dukungan untuk berbagi sumber daya SageMaker Model Card. | Anda sekarang dapat berbagi sumber daya Kartu SageMaker Model dengan orang lain Akun AWS atau organisasi Anda. | 18 Agustus 2023 |
| Menambahkan dukungan untuk grup SageMaker fitur Amazon Feature Store dan SageMaker Katalog sebagai sumber daya yang dapat dibagikan. | Anda sekarang dapat berbagi grup SageMaker fitur Amazon Feature Store dan sumber daya SageMaker Katalog dengan orang lain Akun AWS atau organisasi Anda. | Juli 20, 2023 |

| | | |
|--|---|----------------|
| Peningkatan batas kuota layanan untuk undangan yang tertunda. | Jumlah maksimum undangan yang tertunda per akun berbagi telah ditingkatkan dari 20 menjadi 250. | 8 Juni 2023 |
| Menambahkan dukungan untuk AWS AppSync GraphQL API sebagai sumber daya yang dapat dibagikan. | Anda sekarang dapat berbagi AWS AppSync GraphQL API dengan yang lain. Akun AWS RAM | 24 Mei 2023 |
| Menambahkan dukungan untuk Akses Terverifikasi AWS grup sebagai sumber daya yang dapat dibagikan. | Anda sekarang dapat membuat dan mengelola Akses Terverifikasi AWS grup secara terpusat, dan kemudian membagikannya dengan orang lain Akun AWS atau organisasi Anda. | 27 April 2023 |
| Menambahkan dukungan untuk izin yang dikelola pelanggan di AWS RAM konsol. | Sekarang Anda dapat dengan aman membuat dan memelihara kontrol akses sumber daya berbutir halus untuk jenis sumber daya yang didukung. | 19 April 2023 |
| Menambahkan dukungan untuk layanan Amazon VPC Lattice dan sumber daya jaringan layanan yang dapat dibagikan. | Anda sekarang dapat berbagi layanan Amazon VPC Lattice dan sumber daya jaringan layanan dengan yang lain. Akun AWS | 31 Maret 2023 |
| Menambahkan dukungan untuk entitas AWS Marketplace Katalog sebagai sumber daya yang dapat dibagikan. | Anda sekarang dapat berbagi entitas Anda dengan orang lain Akun AWS di Marketplace. | Maret 27, 2023 |

| | | |
|--|--|------------------|
| Menambahkan dukungan untuk mengelola versi izin di AWS RAM konsol. | Anda sekarang dapat menggunakan AWS RAM konsol untuk melihat detail versi dan memperbarui izin ke versi mana pun yang ditetapkan sebagai default. | Januari 16, 2023 |
| Pembaruan praktik terbaik IAM. | Panduan yang diperbarui untuk menyelaraskan dengan praktik terbaik IAM. Untuk informasi selengkapnya, lihat Praktik terbaik keamanan di IAM. | Januari 3, 2023 |
| Menambahkan dukungan untuk grup penempatan Amazon EC2 sebagai sumber daya yang dapat dibagikan. | Anda sekarang dapat berbagi grup penempatan Amazon EC2 dengan yang lain Akun AWS untuk meluncurkan instans mereka. | 8 November 2022 |
| Menambahkan tautan ke dua video pengantar tentang AWS RAM. | Menambahkan video ikhtisar yang menjelaskan AWS RAM dan memberikan panduan berbagi sumber daya dengan orang lain. Akun AWS | Agustus 29, 2022 |
| Menambahkan dukungan untuk SageMaker saluran pipa Amazon. | Anda sekarang dapat berbagi SageMaker saluran pipa dengan yang lain Akun AWS. | Agustus 2, 2022 |
| Menambahkan dukungan untuk AWS Service Catalog AppRegistry aplikasi dan grup atribut sebagai jenis sumber daya yang dapat dibagikan. | Anda sekarang dapat berbagi AppRegistry aplikasi dan grup atribut dengan yang lain Akun AWS. | Juni 17, 2022 |

| | | |
|--|---|-------------------|
| AWS Resource Access Manager menerima sertifikasi SOC dan ISO. | AWS RAM telah divalidasi sesuai dengan standar Service Organization Control (SOC) dan International Organization for Standardization (ISO) ISO 9001, ISO 27001, ISO 27017, ISO 27018 dan ISO 27701. | 31 Mei 2022 |
| AWS Resource Access Manager menerima sertifikasi FedRAMP. | AWS RAM telah divalidasi sebagai sesuai dengan Federal Risk and Authorization Management Program (FedRAMP). | 8 April 2022 |
| AWS Resource Access Manager menerima sertifikasi PCI DSS. | AWS RAM telah divalidasi sebagai sesuai dengan Payment Card Industry (PCI) Data Security Standard (DSS). | Februari 27, 2022 |
| Menambahkan dukungan untuk penemuan sumber daya Amazon VPC IPAM sebagai sumber daya yang dapat dibagikan. Selain itu, Anda sekarang dapat berbagi IPAM Pools dengan akun di luar organisasi. | Anda sekarang dapat berbagi penemuan sumber daya IPAM dengan yang lain. Akun AWS | Januari 25, 2022 |
| Menambahkan dukungan untuk berbagi sumber daya global | Anda sekarang dapat berbagi sumber daya global dengan yang lain Akun AWS. | Desember 2, 2021 |
| Menambahkan dukungan untuk jaringan inti AWS Cloud WAN sebagai sumber daya global yang dapat dibagikan. | Anda sekarang dapat berbagi jaringan inti Cloud WAN dengan yang lain Akun AWS. | Desember 2, 2021 |

| | | |
|--|---|--------------------|
| Dukungan untuk berbagi kumpulan Amazon VPC IP Address Manager (IPAM) | Anda dapat menggunakan AWS RAM untuk berbagi kolam Amazon VPC IPAM. Untuk informasi selengkapnya, lihat AWS Sumber daya yang dapat dibagikan di Panduan AWS RAM Pengguna. | 1 Desember 2021 |
| Support untuk berbagi SageMaker sumber daya Amazon | Anda dapat menggunakan AWS RAM untuk berbagi grup SageMaker silsilah. Untuk informasi selengkapnya, lihat AWS Sumber daya yang dapat dibagikan di Panduan AWS RAM Pengguna. | 30 November 2021 |
| Support untuk berbagi sumber daya AWS Migration Hub Refactor Spaces | Anda dapat menggunakan AWS RAM untuk berbagi lingkungan Hub Migrasi. Untuk informasi selengkapnya, lihat AWS Sumber daya yang dapat dibagikan di Panduan AWS RAM Pengguna. | 29 November 2021 |
| Menambahkan informasi tentang AWS RAMAWS kebijakan izin IAM yang dikelola. | Detail yang dipublikasikan tentang kebijakan izin AWS terkelola yang tersedia yang dapat Anda akses di konsol IAM dan dilampirkan ke prinsipal IAM di Anda. Akun AWS | September 16, 2021 |
| Ditambahkan dukungan untuk berbagi S3 pada sumber daya Outposts | Anda sekarang dapat menggunakan AWS RAM untuk berbagi S3 di Outposts dengan yang lain. Akun AWS | 5 Agustus 2021 |

| | | |
|--|--|------------------|
| <u>Menambahkan dukungan untuk izin terkelola tambahan dan berbagi sumber daya dengan prinsipal IAM</u> | Untuk jenis sumber daya yang didukung, Anda dapat memilih dari izin AWS RAM terkelola tambahan dan berbagi sumber daya dengan peran dan pengguna IAM individual. | 10 Juni 2021 |
| <u>Menambahkan dukungan untuk berbagi sumber daya AWS Systems Manager Incident Manager</u> | Anda sekarang dapat menggunakan AWS RAM untuk berbagi kontak AWS Systems Manager Incident Manager dan rencana respons dengan orang lain Akun AWS. | 10 Mei 2021 |
| <u>Menambahkan dukungan untuk berbagi sumber daya Amazon Route 53</u> | Anda sekarang dapat menggunakan AWS RAM untuk berbagi grup aturan Amazon Route 53 Resolver DNS Firewall dengan yang lain. Akun AWS | 31 Maret 2021 |
| <u>Ditambahkan dukungan untuk berbagi AWS Transit Gateway sumber daya</u> | Anda sekarang dapat menggunakan AWS RAM untuk berbagi domain multicast gateway transit dengan yang lain. Akun AWS | 10 Desember 2020 |
| <u>Ditambahkan dukungan untuk berbagi AWS Network Firewall sumber daya</u> | Anda sekarang dapat menggunakan AWS RAM untuk berbagi kebijakan AWS Network Firewall firewall dan grup aturan dengan yang lain Akun AWS. | 17 November 2020 |

| | | |
|---|---|------------------|
| Ditambahkan dukungan untuk berbagi untuk Outposts dan tabel rute gateway lokal | Anda sekarang dapat menggunakan AWS RAM untuk berbagi Outposts dan tabel rute gateway lokal dengan yang lain. Akun AWS | 15 Oktober 2020 |
| Ditambahkan dukungan untuk berbagi Route 53 query log | Anda sekarang dapat menggunakan AWS RAM untuk berbagi log kueri Route 53 dengan yang lain Akun AWS. | 7 September 2020 |
| Menambahkan dukungan untuk berbagi AWS Private Certificate Authority sumber daya. | Anda sekarang dapat menggunakan AWS RAM untuk berbagi otoritas sertifikasi AWS Private CA pribadi (CA) dengan yang lain Akun AWS. | 17 Agustus 2020 |
| Menambahkan dukungan untuk berbagi katalog data AWS Glue, database, dan tabel. | Anda sekarang dapat menggunakan AWS RAM untuk berbagi katalog data AWS Glue, database, dan tabel dengan yang lain. Akun AWS | 7 Juli 2020 |
| Menambahkan dukungan untuk berbagi daftar awalan Amazon VPC. | Anda sekarang dapat menggunakan AWS RAM untuk berbagi daftar awalan. | 29 Juni 2020 |
| Menambahkan dukungan untuk berbagi alamat AWS Outposts IPv4 milik pelanggan : | Anda sekarang dapat menggunakan AWS RAM untuk berbagi alamat IPv4 AWS Outposts milik pelanggan dengan yang lain. Akun AWS | 22 April 2020 |

| | | |
|--|---|------------------|
| Ditambahkan dukungan untuk berbagi AWS App Mesh jerat | Anda sekarang dapat menggunakan AWS RAM untuk berbagi jerat dengan yang lain Akun AWS. | 17 Januari 2020 |
| Menambahkan dukungan untuk berbagi AWS CodeBuild proyek dan grup laporan | Anda sekarang dapat menggunakan AWS RAM untuk berbagi AWS CodeBuild proyek dan melaporkan grup dengan yang lain Akun AWS. | 13 Desember 2019 |
| Menambahkan dukungan untuk berbagi sumber daya tambahan | Sekarang Anda dapat menggunakannya AWS RAM untuk berbagi Host Khusus Amazon EC2, grup AWS Resource Groups sumber daya, dan komponen Image Builder Amazon EC2, gambar, dan resep gambar dengan yang lain. Akun AWS | 2 Desember 2019 |
| Menambahkan dukungan untuk berbagi Pemesanan Kapasitas Sesuai Permintaan | Anda sekarang dapat menggunakan AWS RAM untuk berbagi Pemesanan Kapasitas Sesuai Permintaan dengan yang lain. Akun AWS | 29 Juli 2019 |
| Menambahkan dukungan untuk berbagi cluster Aurora DB | Anda sekarang dapat menggunakan AWS RAM untuk berbagi cluster Aurora DB dengan yang lain. Akun AWS | 2 Juli 2019 |

[Menambahkan dukungan untuk berbagi target Traffic Mirroring](#)

Anda sekarang dapat menggunakan AWS RAM untuk berbagi target Traffic Mirroring dengan yang lain Akun AWS.

25 Juni 2019

[Ditambahkan dukungan untuk berbagi konfigurasi lisensi](#)

Anda sekarang dapat menggunakan AWS RAM untuk berbagi konfigurasi AWS lisensi License Manager dengan yang lain Akun AWS.

5 Desember 2018

[Menambahkan dukungan untuk berbagi subnet](#)

Anda sekarang dapat menggunakan AWS RAM untuk berbagi subnet Amazon VPC dengan yang lain. Akun AWS

27 November 2018

[Ditambahkan dukungan untuk berbagi gateway transit](#)

Anda sekarang dapat menggunakan AWS RAM untuk berbagi gateway transit VPC Amazon dengan yang lain. Akun AWS

26 November 2018

[Ditambahkan dukungan untuk berbagi aturan Resolver](#)

Anda sekarang dapat menggunakan AWS RAM untuk berbagi aturan Route 53 Resolver dengan yang lain. Akun AWS

20 November 2018

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.