aws

Panduan Pengguna

AWS Resource Access Manager

AWS Resource Access Manager: Panduan Pengguna

Table of Contents

Apa itu AWS Resource Access Manager?

AWS Resource Access Manager (AWS RAM) membantu Anda berbagi sumber daya dengan aman di seluruh Akun AWS, di dalam organisasi atau unit organisasi (OUs), dan dengan peran AWS Identity and Access Management (IAM) dan pengguna untuk jenis sumber daya yang didukung. Jika Anda memiliki beberapa Akun AWS, Anda dapat membuat sumber daya sekali dan menggunakannya 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 beberapa unit organisasi tertentu (OUs). 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

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 sumber daya Anda AWS . Untuk informasi selengkapnya, lihat ???.

Video ini menunjukkan cara membuat dan mengaitkan izin terkelola pelanggan mengikuti praktik terbaik dengan hak istimewa paling sedikit. Untuk informasi lebih lanjut lihat,???.

Manfaat dari AWS RAM

Mengapa menggunakan AWS RAM? Ini menawarkan manfaat berikut:

- Mengurangi overhead operasional Anda — Buat sumber daya sekali, lalu gunakan AWS RAM untuk berbagi 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 itu tanpa harus menggunakan kebijakan izin berbasis identitas.
- Menyediakan keamanan dan konsistensi — Sederhanakan manajemen keamanan untuk sumber daya bersama Anda dengan menggunakan satu set kebijakan dan izin. Jika Anda malah membuat sumber daya duplikat di semua akun terpisah Anda, Anda akan memiliki tugas untuk menerapkan kebijakan dan izin yang identik, dan kemudian harus menjaganya tetap identik di semua akun tersebut. Sebagai gantinya, semua pengguna berbagi AWS RAM sumber daya dikelola oleh satu set kebijakan dan izin. AWS RAM menawarkan pengalaman yang konsisten untuk berbagi berbagai jenis AWS sumber daya.
- Menyediakan visibilitas dan auditabilitas — Lihat detail penggunaan untuk sumber daya bersama Anda melalui integrasi dengan AWS RAM 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 berbagi beberapa jenis AWS sumber daya dengan yang lain Akun AWS dengan melampirkan kebijakan berbasis sumber daya yang mengidentifikasi AWS Identity and Access Management (IAM) prinsipal (peran dan pengguna IAM) di luar Anda. Akun AWS Namun, berbagi sumber daya dengan melampirkan kebijakan tidak mengambil keuntungan dari manfaat tambahan yang AWS RAM disediakan. Dengan menggunakan AWS RAM Anda mendapatkan fitur-fitur berikut:

- Anda dapat berbagi dengan organisasi atau unit organisasi (OU) tanpa harus menghitung semua. Akun AWS IDs
- Pengguna dapat melihat sumber daya yang dibagikan dengan mereka secara langsung di Layanan AWS konsol asal dan operasi API seolah-olah sumber daya tersebut langsung ada di akun pengguna. Misalnya, jika Anda menggunakan AWS RAM untuk berbagi subnet VPC Amazon dengan akun lain, pengguna di akun tersebut dapat melihat subnet di konsol VPC Amazon dan dalam hasil operasi API VPC Amazon 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 Nama Sumber Daya Amazon (ARN) -nya.

- Pemilik sumber daya dapat melihat kepala sekolah 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 Anda, maka AWS RAM mulailah proses undangan. Penerima harus menerima undangan sebelum kepala sekolah dapat mengakses sumber daya bersama. Setelah Anda mengaktifkan kemampuan untuk berbagi dalam organisasi Anda, 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 PromoteResourceShareCreatedFromPolicyOperasi API.
- Gunakan ekuivalen operasi API, yaitu AWS Command Line Interface (AWS CLI) promote-resource-share-created-from-policyperintah.

Cara kerja berbagi sumber daya

Ketika Anda berbagi sumber daya di akun pemilik dengan yang lain Akun AWS, akun konsumsi, Anda memberikan akses untuk prinsipal di 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 di tempat Akun AWS Anda membagikannya.

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 berbagi sumber daya yang Anda miliki dengan membuat pembagian sumber daya. Untuk membuat pembagian sumber daya, Anda menentukan yang berikut ini:

- Wilayah AWS Di mana Anda ingin membuat berbagi sumber daya. Di konsol, Anda memilih dari menu tarik-turun Wilayah di sudut kanan atas konsol. Di AWS CLI, Anda menggunakan `--region` parameter.

  - Pembagian sumber daya hanya dapat berisi sumber daya Regional yang Wilayah AWS sama dengan pembagian sumber daya.
  - Pembagian sumber daya dapat berisi sumber daya global hanya jika pembagian sumber daya berada di Wilayah asal yang ditunjuk untuk sumber daya global, US East (Virginia N.),`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. Prinsipal dapat berupa individu Akun AWS, akun dalam organisasi atau unit organisasi (OU) di AWS Organizations, atau peran individu AWS Identity and Access Management (IAM) atau pengguna.

  > **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
- Izin terkelola untuk mengaitkan dengan setiap jenis sumber daya yang Anda sertakan dalam pembagian sumber daya. Izin terkelola menentukan apa yang dapat dilakukan oleh prinsipal di akun lain dengan sumber daya dalam pembagian sumber daya.

  Perilaku izin tergantung pada jenis kepala sekolah:

  - Jika prinsipal berada di akun yang berbeda dari akun yang memiliki sumber daya, maka izin yang dilampirkan pada pembagian 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 akses pengguna 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 pemilik 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 pada 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 Anda mengakses sumber daya bersama menggunakan layanan sumber daya tersebut, Anda memiliki kemampuan dan batasan yang sama dengan Akun AWS yang memiliki sumber daya tersebut.

- Jika sumber dayanya Regional, maka Anda dapat mengaksesnya Wilayah AWS hanya dari yang ada di akun yang dimiliki.
- 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 pembagian sumber daya dan sumber daya globalnya di AWS RAM konsol dan alat hanya di Wilayah asal yang ditunjuk, AS Timur (Virginia Utara),`us-east-1`.

Mengakses AWS RAM

Anda dapat bekerja AWS RAM dengan salah satu cara berikut:

AWS RAM konsol

AWS RAM menyediakan antarmuka pengguna berbasis web, AWS RAM konsol. Jika Anda telah mendaftar Akun AWS, Anda dapat mengakses AWS RAM konsol dengan masuk ke AWS Management Consoledan memilih AWS RAM dari beranda konsol.

Anda juga dapat menavigasi di browser Anda langsung ke AWS RAM konsol. Jika Anda belum masuk, Anda diminta untuk melakukannya sebelum konsol muncul.

AWS CLI dan Alat untuk Windows PowerShell

Ini AWS CLI dan Alat AWS untuk PowerShell menyediakan akses langsung ke operasi API AWS RAM publik. AWS mendukung alat-alat ini pada Windows, macOS, dan Linux. Untuk informasi

selengkapnya tentang memulai, lihat Panduan AWS Command Line Interface Pengguna, atau Panduan AWS Tools for Windows PowerShell Pengguna. Untuk informasi selengkapnya tentang perintah AWS RAM, lihat Referensi AWS CLI Perintah atau Referensi AWS Tools for Windows PowerShell Cmdlet.

AWS SDKs

AWS menyediakan perintah API untuk serangkaian bahasa pemrograman yang luas. Untuk informasi selengkapnya tentang memulai, lihat Panduan Referensi Alat AWS SDKs 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 kredensi 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 pembagian sumber daya dan berbagi sumber daya Anda di seluruh akun. Biaya penggunaan sumber daya bervariasi tergantung pada jenis sumber daya. Untuk informasi selengkapnya tentang cara AWS menagih sumber daya yang dapat dibagikan, lihat dokumentasi untuk layanan yang dimiliki sumber daya.

Kepatuhan dan standar internasional

PCI DSS

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

Untuk informasi tentang DSS PCI selengkapnya, termasuk cara meminta salinan AWS PCI Compliance Package, lihat DSS PCI Level 1.

FedRAMP

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

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

Federal Risk and Authorization Management Program (FedRAMP) adalah program pemerintah AS yang memberikan pendekatan standar untuk penilaian keamanan, otorisasi, dan pemantauan berkelanjutan untuk produk dan layanan cloud.

Untuk informasi selengkapnya 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, dan AWS sertifikat ISO dan CSA STAR di. AWS Artifact

Untuk informasi selengkapnya 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 yang Anda miliki dengan orang 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 peran individu AWS Identity and Access Management (IAM) 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 mendapatkan akses ke sumber daya bersama.

Konten

Syarat dan konsep untuk AWS RAM

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 pembagian sumber daya. Pembagian sumber daya memiliki tiga elemen berikut:

- Daftar satu atau lebih AWS sumber daya untuk dibagikan.
- Daftar satu atau lebih kepala sekolah kepada siapa akses ke sumber daya diberikan.
- Izin terkelola untuk setiap jenis sumber daya yang Anda sertakan dalam pembagian. 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 mengaktifkan AWS RAM berbagi dengan AWS Organizations, dan prinsipal 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 kebijakan izin (IAM). AWS Identity and Access Management
- Jika Anda tidak mengaktifkan 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 lihat kolom Dapat berbagi dengan akun di luar organisasinya.

Berbagi akun

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

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

Prinsip konsumsi

Akun konsumsi adalah tempat Akun AWS 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 lihat kolom Dapat berbagi dengan peran & pengguna IAM.

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 lihat kolom Dapat berbagi dengan prinsipal layanan.

Prinsipal di akun konsumsi hanya dapat melakukan tindakan yang diizinkan oleh kedua izin berikut:

- Izin terkelola yang dilampirkan ke pembagian sumber daya. Ini menentukan izin maksimum yang dapat diberikan kepada prinsipal 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 yang ditentukan dan ke Nama Sumber Daya Amazon (ARN) 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 konsumen.
- Peran IAM individu atau pengguna di akun lain — Beberapa jenis sumber daya mendukung berbagi langsung dengan peran IAM individu atau pengguna. Tentukan tipe utama ini dengan ARN-nya.
  - 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 tarik-turun. 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 di kunci `aws:SourceAccount` kondisi.
- Akun dalam organisasi — Jika akun berbagi dikelola oleh AWS 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 berbagi dengan organisasinya sendiri atau OU IDs dalam organisasinya sendiri. Tentukan akun dalam suatu organisasi oleh ARN organisasi atau OU.

- Semua akun dalam suatu organisasi — Berikut ini adalah contoh ARN dari sebuah organisasi di: AWS Organizations

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

- Semua akun dalam 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. 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 sumber ARNs 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 JSON yang menerapkan bahasa kebijakan IAM. Tidak seperti kebijakan berbasis identitas yang Anda lampirkan ke prinsipal, seperti peran IAM atau pengguna, Anda melampirkan 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 elemen `Principal` 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 () SCPs untuk itu mungkin berlaku untuk. AWS Organizations Akun AWS Kebijakan berbasis sumber daya yang dihasilkan dengan AWS RAM berpartisipasi dalam logika evaluasi kebijakan yang sama seperti semua kebijakan IAM lainnya. Untuk detail lengkap tentang 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 kebijakan berbasis sumber daya easy-to-use abstraksi.

Untuk jenis sumber daya yang mendukung kebijakan berbasis sumber daya, AWS RAM secara otomatis membuat dan mengelola kebijakan berbasis sumber daya untuk Anda. Untuk sumber daya tertentu, AWS RAM buat kebijakan berbasis sumber daya dengan menggabungkan informasi dari semua pembagian sumber daya yang mencakup sumber daya tersebut. Misalnya, pertimbangkan saluran Amazon SageMaker AI yang Anda bagikan dengan menggunakan AWS RAM dan sertakan 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 untuk hanya memberikan izin eksekusi SageMaker AI ke satu akun. AWS RAM secara otomatis menggabungkan dua set izin yang berbeda ke dalam kebijakan sumber daya tunggal dengan beberapa pernyataan. Kemudian melampirkan kebijakan berbasis sumber daya gabungan ke sumber daya pipa. Anda dapat melihat kebijakan sumber daya dasar ini dengan memanggil GetResourcePolicyoperasi. 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 secara manual membuat kebijakan berbasis sumber daya dan melampirkannya ke sumber daya Anda dengan meneleponPutResourcePolicy, kami sarankan Anda menggunakannya AWS RAM karena memberikan keuntungan berikut:

- Dapat ditemukan untuk konsumen berbagi — 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 konsumer dapat melihat proyek di CodeBuild konsol dan hasil operasi CodeBuild API yang dilakukan. Sumber daya yang dibagikan

dengan melampirkan kebijakan berbasis sumber daya secara langsung 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 melihat secara terpusat 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 memberikan izin ready-to-use AWS 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 tersebut, AWS RAM secara otomatis membuat kebijakan berbasis sumber daya sebagai representasi dari izin yang sebenarnya. 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 — IPv4 Alamat milik pelanggan, daftar awalan, subnet, target cermin lalu lintas, gateway transit, dan domain multicast gateway transit

Contoh kebijakan berbasis sumber daya yang AWS RAM dihasilkan

Jika Anda membagikan sumber daya EC2 gambar Image Builder dengan akun individual AWS RAM , buat kebijakan yang terlihat seperti contoh berikut dan lampirkan 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 EC2 gambar Image Builder dengan peran IAM atau pengguna lain Akun AWS, buat AWS RAM kebijakan yang terlihat seperti contoh berikut dan lampirkan 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 membagikan sumber daya gambar Image Builder dengan semua akun di organisasi atau dengan akun OU, buat AWS RAM kebijakan yang terlihat seperti contoh berikut dan lampirkan ke sumber daya gambar apa pun yang disertakan dalam pembagian sumber daya. EC2

> **Note**
>
> Kebijakan ini menggunakan `"Principal": "*"` dan kemudian menggunakan `"Condition"` elemen untuk membatasi izin 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 tersebut memberikan akses ke semua prinsip IAM di akun yang berisi sumber daya, tunduk pada batasan apa pun yang diberlakukan oleh elemen, jika ada. `Condition` `Deny`Pernyataan eksplisit dalam kebijakan apa pun yang berlaku untuk prinsipal panggilan akan mengesampingkan izin yang diberikan oleh kebijakan ini. Namun, implisit `Deny` (artinya kurangnya eksplisit`Allow`) dalam kebijakan identitas yang berlaku, kebijakan batas izin, atau kebijakan sesi tidak mengakibatkan kepada prinsipal yang diberikan akses `Deny` ke tindakan oleh kebijakan berbasis sumber daya tersebut.

Jika perilaku ini tidak diinginkan untuk skenario Anda, maka Anda dapat membatasi perilaku ini dengan menambahkan `Deny` pernyataan eksplisit ke 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 yang dapat dilakukan oleh prinsipal dengan sumber daya yang digunakan bersama. AWS RAM

Anda hanya dapat melampirkan satu izin terkelola untuk setiap jenis sumber daya dalam pembagian sumber daya. 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 izin AWS terkelola untuk setiap jenis sumber daya yang didukung. Beberapa jenis sumber daya mendukung lebih dari satu izin AWS terkelola, dengan satu izin terkelola ditetapkan sebagai AWS default. Izin AWS terkelola default dikaitkan kecuali Anda menentukan sebaliknya.

Izin terkelola 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 digunakan bersama. 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 prinsipal memiliki akses ke sumber daya. Izin ini dapat digunakan dalam satu atau lebih AWS RAM saham. Izin terkelola pelanggan bersifat spesifik Wilayah.

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. Saat 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 pada izin AWS 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 yang dikelola 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 izin 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 sumber daya 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 AWS terkelola. `AWSResourceAccessManagerServiceRolePolicy`

> **Note**
>
> Ketika berbagi dengan AWS Organizations diaktifkan, setiap berbagi sumber daya dalam organisasi dibatasi untuk konsumen dalam organisasi yang sama. Ini berarti jika konsumen

meninggalkan organisasi, mereka akan kehilangan akses ke sumber daya dalam pembagian sumber daya. Ini benar ketika sumber daya dibagikan dengan OU, seluruh organisasi, atau akun individu dalam organisasi.

Jika Anda tidak perlu lagi berbagi sumber daya dengan seluruh organisasi Anda atau OUs, 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

- 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 diSumber 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, lihatBerbagi 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 sumber ARNs 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 OUs dari organisasi itu ke pembagian sumber daya Anda. Anda tidak dapat menambahkan OUs 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 — IPv4 Alamat 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, lihatBerbagi 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 Availability Zone IDs 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 Berikutnya.
6. 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 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 mengetahui 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 Berikutnya.
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 sumber ARNs 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 anaknya OUs 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 GetUserTindakan API.

- Prinsipal layanan — Untuk menambahkan prinsipal layanan, pilih Prinsipal layanan dari dropbox 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 Berikutnya.
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 create-resource-shareperintah. 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. Lihat informasi yang lebih lengkap di 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 AWS Resource Access Manager, selesaikan tugas-tugas berikut.

Tugas

- Menanggapi undangan berbagi sumber daya
- Gunakan sumber daya yang dibagikan dengan Anda

Menanggapi undangan berbagi sumber daya

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

Undangan tidak digunakan dalam skenario berikut:

- Jika Anda bagian dari organisasi AWS Organizations dan berbagi di organisasi Anda diaktifkan, maka kepala sekolah di organisasi secara otomatis mendapatkan akses ke sumber daya 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 Berbagi dengan saya: Berbagi sumber daya di AWS RAM konsol.

   > **Note**
   >
   > Pembagian sumber daya hanya terlihat Wilayah AWS di tempat pembuatannya. Jika pembagian sumber daya yang diharapkan tidak muncul di konsol, Anda mungkin perlu beralih ke yang lain Wilayah AWS menggunakan kontrol tarik-turun di sudut kanan atas.

2. Tinjau daftar pembagian sumber daya yang telah Anda akses.

   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.

3. 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 memulai, dapatkan daftar undangan berbagi sumber daya yang tersedia untuk Anda. Contoh perintah berikut dijalankan di `us-west-2` Wilayah, dan menunjukkan satu pembagian 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 Nama Sumber Daya Amazon (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 itu sekarang tersedia untuk kepala sekolah di akun penerima.

Gunakan sumber daya yang dibagikan dengan Anda

Setelah menerima undangan untuk bergabung dengan pembagian 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 bersifat global, maka Anda harus menggunakan wilayah rumah yang ditunjuk, AS Timur (Virginia N.), `us-east-1` Untuk melihat sumber daya AWS RAM, Anda harus membuka AWS RAM konsol ke tempat Wilayah AWS pembagian sumber daya dibuat.

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

Topik ini membahas perbedaan cara kerja AWS Resource Access Manager (AWS RAM) 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 Regional atau global. Sumber daya regional menunjukkan Wilayah AWS. Jika kosong, maka sumber dayanya 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 membuatnya dalam yang ditentukan 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 instance Amazon Elastic Compute Cloud (Amazon EC2) dengan instans 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. AWS SDKs Masing-masing memiliki mekanisme ekuivalennya sendiri 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 dalam AWS CLI perintah, maka Anda tidak dapat lagi melihat atau berinteraksi dengan sumber daya yang dapat Anda lihat di Wilayah sebelumnya.

Saat Anda melihat Nama Sumber Daya Amazon (ARN) untuk sumber daya Regional, Wilayah yang berisi sumber daya ditentukan sebagai bidang keempat di ARN. Misalnya, EC2 instans Amazon adalah sumber daya Regional. Sumber daya tersebut memiliki ARNs yang terlihat mirip dengan sampel 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 contoh sumber daya tertentu yang dapat eksis pada satu waktu. Dalam skenario seperti itu, replikasi atau sinkronisasi antar salinan di Wilayah yang berbeda tidak memadai. Harus mengakses satu titik akhir global, dengan kemungkinan peningkatan latensi, dianggap dapat diterima untuk memastikan bahwa setiap perubahan langsung terlihat oleh konsumen sumber daya. Misalnya, ketika Anda membuat jaringan inti AWS Cloud WAN sebagai sumber daya global, itu konsisten untuk semua pengguna. Ini muncul sebagai jaringan global tunggal yang berdekatan di semua Wilayah.

Nama Sumber Daya Amazon (ARN) untuk sumber daya global tidak menyertakan Wilayah. Bidang keempat dari ARN semacam itu kosong, seperti contoh ARN berikut untuk jaringan inti Cloud WAN.

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

Pembagian sumber daya dan Wilayahnya

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

> **Important**
>
> Saat ini, Anda dapat membuat pembagian sumber daya dengan sumber daya global hanya di wilayah asal yang ditunjuk Wilayah AS Timur (Virginia N.),`us-east-1`. Meskipun Anda dapat membuat pembagian sumber daya hanya di Wilayah beranda tunggal itu, sumber daya global bersama akan muncul sebagai sumber daya global standar jika dilihat di konsol layanan atau operasi CLI dan SDK. Pembatasan ke Wilayah asal hanya berlaku untuk pembagian sumber daya, bukan sumber daya yang dikandungnya.

Untuk berbagi sumber daya Regional yang Anda buat di `us-west-2` Wilayah, Anda harus mengonfigurasi AWS RAM konsol untuk menggunakan `us-west-2` dan membuat pembagian

sumber daya di sana. Anda tidak dapat membuat pembagian sumber daya yang menyertakan 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 pembagian sumber daya yang berbeda. Anda tidak dapat menggabungkan sumber daya dari dua Wilayah yang berbeda menjadi satu pembagian sumber daya.

Untuk berbagi sumber daya global di AWS RAM konsol, Anda harus mengonfigurasi AWS RAM konsol untuk menggunakan Wilayah rumah yang ditunjuk, AS Timur (Virginia N.)`us-east-1`. Kemudian, buat pembagian 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 pembagian AWS RAM sumber daya hanya di Wilayah asal yang ditunjuk, itu masih merupakan sumber daya global setelah Anda membagikannya. Anda dapat mengaksesnya di yang dibagikan Akun AWS dari Wilayah mana pun dari mana Anda dapat mengaksesnya di aslinya Akun AWS.

Pertimbangan

- Untuk membuat pembagian 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 pembagian sumber daya di `us-east-1` Wilayah.
- Untuk melihat atau mengubah pembagian sumber daya di AWS RAM konsol, Anda harus menggunakan Wilayah yang berisi pembagian sumber daya. Demikian pula, operasi AWS RAM AWS CLI dan SDK memungkinkan Anda berinteraksi hanya dengan pembagian sumber daya yang ada di Wilayah yang Anda tentukan dalam operasi Anda. Untuk melihat atau memodifikasi pembagian sumber daya yang berisi 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 menyertakannya dalam pembagian sumber daya, Anda harus menggunakan Wilayah yang berisi sumber daya Regional.
- Untuk melihat sumber daya global di AWS RAM konsol untuk memasukkannya ke dalam pembagian sumber daya, Anda harus menggunakan Wilayah asal yang ditunjuk, AS Timur (Virginia Utara),`us-east-1`.
- Anda dapat membuat pembagian sumber daya dengan sumber daya Regional dan global hanya di Wilayah asal yang ditunjuk, AS Timur (Virginia N.),`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 pembagian sumber daya baru, memodifikasi pembagian sumber daya yang ada, dan menghapus pembagian sumber daya yang tidak lagi Anda perlukan.

Topik

Melihat pembagian sumber daya yang Anda buat AWS RAM

Anda dapat melihat daftar pembagian sumber daya yang telah Anda buat. Anda dapat melihat sumber daya mana yang Anda bagikan dan prinsipal dengan siapa mereka berbagi.

Console

Untuk melihat pembagian sumber daya Anda

1. Buka halaman Shared by me: Resource share 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, lihatBerbagi 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 akan menampilkan spanduk untuk mengingatkan 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 pembagian sumber daya tersebut.

4. (Opsional) Terapkan filter untuk menemukan pembagian 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 mencantumkan hanya pembagian sumber daya yang menyertakan teks tersebut dalam nama. Pilih kotak teks untuk melihat daftar dropdown bidang atribut yang disarankan. Setelah Anda memilih 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 untuk ditinjau. Konsol menampilkan informasi berikut tentang pembagian sumber daya:

   - Ringkasan — Daftar nama berbagi sumber daya, ID, pemilik, Nama Sumber Daya Amazon (ARN), tanggal pembuatan, apakah memungkinkan berbagi dengan akun eksternal, dan statusnya saat ini.
   - Izin Terkelola - Daftar izin terkelola yang dilampirkan ke pembagian sumber daya ini. Mungkin ada paling banyak 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 ini bukan versi default, maka konsol menampilkan tautan Pembaruan ke versi default. Jika Anda memilih tautan itu, maka Anda diberi kesempatan untuk memperbarui pembagian sumber daya untuk menggunakan versi default.
   - Sumber daya bersama — Daftar sumber daya individu yang disertakan dalam pembagian sumber daya. Pilih ID sumber daya untuk membuka tab browser baru untuk melihat sumber daya di konsol layanan aslinya.
   - Prinsipal bersama — Daftar kepala sekolah dengan siapa sumber daya dibagikan.
   - Tag - Daftar pasangan nilai kunci tag yang dilampirkan ke pembagian sumber daya itu sendiri; ini bukan tag yang dilampirkan ke sumber daya individu yang termasuk dalam pembagian sumber daya.

AWS CLI

Untuk melihat pembagian sumber daya Anda

Anda dapat menggunakan get-resource-sharesperintah dengan parameter yang `--resource-owner` disetel `SELF` untuk menampilkan detail pembagian sumber daya yang dibuat di file Anda Akun AWS.

Contoh berikut menunjukkan pembagian sumber daya yang dibagikan di current Wilayah AWS (`us-east-1`) untuk pemanggilan Akun AWS. Untuk mendapatkan pembagian 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 AS Timur (Virginia N.),`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

- 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 diSumber 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, lihatBerbagi 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 ruang lingkup tersebut 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 sumber ARNs 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 OUs dari organisasi itu ke pembagian sumber daya Anda. Anda tidak dapat menambahkan OUs 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 — IPv4 Alamat 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, lihatBerbagi 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 Availability Zone IDs 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 Berikutnya.
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 Berikutnya.
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 ruang lingkup tersebut 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 sumber ARNs 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 anaknya OUs 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. Sebagai contoh:

    ```
    123456789012
    ```

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

    ```
    o-abcd1234
    ```

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

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

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

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

    Sebagai contoh:

    ```
    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`*

  Sebagai contoh:

  `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 GetUserTindakan API.

- Prinsipal layanan — Untuk menambahkan prinsipal layanan, pilih Prinsipal layanan dari dropbox tipe utama Pilih. Masukkan nama kepala AWS layanan. Gunakan sintaks berikut:
  - *`service-id`*`.amazonaws.com`

    Sebagai contoh:

    `pca-connector-ad.amazonaws.com`

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

9. Pilih Berikutnya.
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 create-resource-shareperintah. 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"
    }
}
```

Perbarui pembagian sumber daya di AWS RAM

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

- Anda dapat menambahkan prinsipal, sumber daya, atau tag ke berbagi sumber daya yang Anda buat.
- Untuk jenis sumber daya yang mendukung lebih dari izin AWS terkelola default, Anda dapat memilih izin terkelola mana yang berlaku untuk sumber daya dari setiap jenis.
- Jika izin terkelola yang dilampirkan ke pembagian 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 pembagian sumber daya. Jika Anda mencabut akses, kepala sekolah tidak lagi memiliki akses ke sumber daya bersama.

> **Note**
>
> Prinsipal dengan siapa Anda berbagi sumber daya dapat meninggalkan bagian sumber daya Anda jika berbagi kosong atau hanya berisi jenis sumber daya yang mendukung meninggalkan pembagian sumber daya. Jika pembagian sumber daya berisi jenis sumber daya yang tidak mendukung keberangkatan, pesan akan muncul untuk memberi tahu kepala sekolah bahwa mereka harus menghubungi pemilik berbagi. Dalam hal ini, Anda, sebagai pemilik pembagian sumber daya, harus menghapus prinsipal dari pembagian sumber daya Anda. Untuk daftar jenis sumber daya yang tidak mendukung tindakan ini, lihatPrasyarat untuk meninggalkan pembagian sumber daya.

Console

Untuk memperbarui pembagian sumber daya

1. Arahkan ke halaman Shared by me: Resource share 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, lihatBerbagi sumber daya regional dibandingkan dengan sumber daya global.
3. Pilih pembagian sumber daya dan kemudian pilih Ubah.
4. Pada Langkah 1: Tentukan detail berbagi sumber daya, tinjau detail berbagi sumber daya, dan jika diperlukan, perbarui salah satu dari berikut ini:
   a. (Opsional) Untuk mengubah nama pembagian sumber daya, edit Nama.
   b. (Opsional) Untuk menambahkan sumber daya ke pembagian sumber daya, di bawah Sumber daya, pilih jenis sumber daya, lalu pilih kotak centang di sebelah sumber daya untuk menambahkannya ke pembagian sumber daya. Sumber daya global hanya muncul jika Anda menyetel Wilayah ke AS Timur (Virginia N.), (`us-east-1`) di AWS Management Console.
   c. (Opsional) Untuk menghapus sumber daya dari pembagian sumber daya, cari sumber daya di bawah Sumber daya yang dipilih, lalu pilih X di sebelah ID sumber daya.
   d. (Opsional) Untuk menambahkan tag ke pembagian sumber daya, di bawah Tag, masukkan kunci tag dan nilai di kotak teks kosong. Untuk menambahkan lebih dari satu kunci tag dan pasangan nilai, pilih Tambahkan tag baru. Anda dapat menambahkan hingga 50 tanda.
   e. Untuk menghapus tag dari berbagi sumber daya, di bawah Tag, cari tag dan pilih Hapus di sebelahnya.
5. Pilih Berikutnya.
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 Anda 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 Anda dari daftar tarik-turun izin terkelola.

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

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

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

8. Pilih Berikutnya.
9. Pada Langkah 3: Pilih prinsipal yang diizinkan untuk mengakses, tinjau prinsip yang dipilih, dan jika diperlukan, perbarui salah satu dari berikut ini:

   a. (Opsional) Untuk mengubah apakah berbagi 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 kepala sekolah eksternal.
      - Untuk membatasi berbagi sumber daya hanya pada prinsipal di organisasi Anda AWS Organizations, pilih Izinkan berbagi dengan kepala sekolah 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 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 sumber ARNs daya individu dalam pembagian sumber daya. Izin dalam kebijakan tersebut tidak dapat melebihi yang ditentukan dalam izin terkelola yang terkait dengan pembagian sumber daya.

> **Note**
>
> Sakelar struktur organisasi tampilan hanya muncul jika berbagi dengan AWS Organizations diaktifkan dan Anda masuk sebagai prinsipal 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 pengenalnya, yang ditampilkan di kotak teks di bawah sakelar struktur organisasi Tampilan. Lihat bullet point berikutnya.

- (Opsional) Untuk menambahkan prinsipal dengan pengenalnya, pilih jenis utama 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 pembagian sumber daya. Anda dapat memilih salah satu dari opsi berikut.

  - Lain Akun 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 pembagian sumber daya.
  - Ini Akun AWS (pemilik sumber daya) — Semua peran dan pengguna di akun pemilik sumber daya secara otomatis menerima akses yang ditentukan oleh izin terkelola yang dilampirkan pada pembagian sumber daya.
- Penambahan segera muncul di daftar Prinsipal yang dipilih.

  Anda kemudian dapat menambahkan akun tambahan OUs, atau organisasi Anda dengan mengulangi langkah ini.
- (Opsional) Untuk menghapus prinsipal, temukan di bawah Prinsipal yang dipilih, pilih kotak centang, lalu pilih Batalkan pilihan.

10. Pilih Berikutnya.
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 pembagian sumber daya

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

- Untuk mengganti nama pembagian sumber daya, atau untuk mengubah apakah prinsipal eksternal diizinkan, gunakan perintah update-resource-share. Contoh berikut mengganti nama berbagi sumber daya yang ditentukan dan menetapkannya untuk mengizinkan hanya prinsipal dari organisasinya. Anda harus menggunakan titik akhir layanan untuk Wilayah AWS yang berisi pembagian 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 untuk berbagi sumber daya tertentu.

```
$ 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 pembagian 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 izin terkelola yang tersedia ARNs untuk subnet Amazon Elastic Compute Cloud EC2 (Amazon), lalu menggunakan salah satu izin tersebut ARNs untuk mengganti izin AWS terkelola yang saat ini ditetapkan untuk jenis sumber daya tersebut dalam pembagian 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 EC2 subnet Amazon dengan ARN yang ditentukan dari pembagian 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 pembagian sumber daya, gunakan perintah tag-resource dan untag-resource. Contoh berikut menambahkan tag `project=lima` untuk berbagi sumber daya tertentu.

```
$ 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 kunci `project` dari berbagi sumber daya tertentu.

```
$ 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 penandaan tidak menghasilkan output saat berhasil.

Melihat sumber daya bersama Anda di AWS RAM

Anda dapat melihat daftar sumber daya individual yang telah Anda bagikan, di semua pembagian 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 sana.

Console

Untuk melihat sumber daya yang sedang Anda bagikan

1. Buka halaman Shared by me: Shared resources 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, lihatBerbagi 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.
   - Jenis sumber daya — Jenis sumber daya.
   - Tanggal berbagi terakhir — Tanggal di mana sumber daya terakhir dibagikan.
   - Pembagian sumber daya — Jumlah pembagian sumber daya yang mencakup sumber daya. Untuk melihat daftar pembagian sumber daya, pilih nomornya.
   - Prinsipal — Jumlah kepala sekolah yang dapat mengakses sumber daya. Pilih nilai untuk melihat prinsipal.

AWS CLI

Untuk melihat sumber daya yang sedang 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 pembagian sumber daya di Wilayah AWS (`us-east-1`) untuk pemanggilan 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 prinsipal tempat Anda berbagi sumber daya di AWS RAM

Anda dapat melihat prinsipal tempat Anda berbagi sumber daya, di semua pembagian sumber daya. Melihat daftar prinsipal ini membantu Anda menentukan siapa yang memiliki akses ke sumber daya bersama Anda.

Console

Untuk melihat prinsipal yang Anda bagikan sumber daya

1. Arahkan ke halaman Shared by me: Principals di 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, lihatBerbagi sumber daya regional dibandingkan dengan sumber daya global.

3. Terapkan filter untuk menemukan prinsip tertentu. Anda dapat menerapkan beberapa filter untuk mempersempit pencarian Anda. Pilih kotak teks untuk melihat daftar dropdown bidang atribut yang disarankan. Setelah Anda memilih 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 prinsipal dalam daftar, konsol menampilkan informasi berikut:

   - Principal ID — ID kepala sekolah. Pilih ID untuk membuka tab browser baru untuk melihat prinsipal di konsol aslinya.
   - Pembagian sumber daya — Jumlah pembagian sumber daya yang Anda bagikan dengan prinsipal yang ditentukan. Pilih nomor untuk melihat daftar pembagian 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 prinsipal yang Anda bagikan sumber daya

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

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 pembagian sumber daya yang berbeda. Anda harus menggunakan titik akhir layanan untuk Wilayah AWS yang berisi pembagian 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 pembagian sumber daya di AWS RAM

Anda dapat menghapus pembagian sumber daya kapan saja. Saat Anda menghapus pembagian sumber daya, semua prinsipal yang terkait dengan pembagian sumber daya kehilangan akses ke sumber daya bersama. Menghapus pembagian sumber daya tidak menghapus sumber daya bersama.

> **Untuk menghapus sumber AWS daya**
>
> Jika Anda perlu menghapus AWS sumber daya yang disertakan dalam pembagian sumber daya, AWS sarankan agar Anda terlebih dahulu memastikan bahwa Anda menghapus sumber daya dari pembagian sumber daya apa pun yang menyertakannya, atau menghapus pembagian sumber daya.

Bagian sumber daya yang dihapus tetap terlihat di AWS RAM konsol untuk waktu yang singkat setelah penghapusan, tetapi statusnya berubah menjadi. `Deleted`

Console

Untuk menghapus pembagian sumber daya

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 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, lihatBerbagi sumber daya regional dibandingkan dengan sumber daya global.

3. Pilih pembagian sumber daya yang ingin Anda hapus.

> **Warning**
>
> Pastikan untuk memilih pembagian sumber daya yang benar. Anda tidak dapat memulihkan pembagian sumber daya setelah Anda menghapusnya.

4. Pilih Hapus, lalu di pesan konfirmasi, pilih Hapus.
5. Bagian sumber daya yang dihapus menghilang setelah dua jam. Sampai saat itu, itu tetap terlihat di konsol dengan status yang dihapus.

AWS CLI

Untuk menghapus pembagian sumber daya

Anda dapat menggunakan delete-resource-shareperintah untuk menghapus pembagian sumber daya yang tidak lagi Anda butuhkan.

Contoh berikut pertama-tama menggunakan get-resource-sharesperintah untuk mendapatkan Amazon Resource Name (ARN) dari resource share yang ingin Anda hapus. Kemudian digunakan delete-resource-shareuntuk menghapus berbagi sumber daya yang ditentukan.

```
$  aws ram get-resource-shares \
    --region us-east-1 \
    --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"
        }
    ]
}
$ 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

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 untuk 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 — IPv4 Alamat 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, lihatBerbagi 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-invitationsperintah untuk mengambil daftar semua undangan yang tersedia untuk pengguna. Akun AWS AWS CLI `query`Parameter 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` ke`ACCEPTED`.

Jika Anda ingin menolak undangan, jalankan reject-resource-share-invitationperintah, 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-fbf6-4336-8377-06c559dfee49
{
    "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": "REJECTED"
    }
}
```

Melihat pembagian sumber daya yang dibagikan dengan Anda

Anda dapat melihat pembagian sumber daya yang dapat Anda akses. Anda dapat melihat kepala sekolah mana yang berbagi sumber daya dengan Anda dan sumber daya mana yang mereka bagikan.

Console

Untuk melihat 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, lihatBerbagi sumber daya regional dibandingkan dengan sumber daya global.
3. (Opsional) Terapkan filter untuk menemukan pembagian 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 mencantumkan hanya pembagian sumber daya yang menyertakan teks tersebut dalam nama. Pilih kotak teks untuk melihat daftar dropdown bidang atribut yang disarankan. Setelah Anda memilih 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 pembagian sumber daya. Pilih ID untuk melihat halaman detail untuk berbagi sumber daya.
   - Pemilik — ID Akun AWS yang membuat pembagian sumber daya.
   - Status — Status saat ini dari pembagian sumber daya. Nilai yang mungkin termasuk:
     - `Active`— Pembagian sumber daya aktif dan tersedia untuk digunakan.
     - `Deleted`— Pembagian sumber daya dihapus dan tidak lagi tersedia untuk digunakan.
     - `Pending`— Undangan untuk menerima pembagian sumber daya sedang menunggu tanggapan.

AWS CLI

Untuk melihat pembagian sumber daya

Gunakan get-resource-sharesperintah dengan `--resource-owner` parameter yang disetel ke`OTHER-ACCOUNTS`.

Contoh berikut menunjukkan daftar pembagian 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 kepala sekolah mana yang berbagi sumber daya dengan Anda dan pembagian sumber daya mana yang menyertakan sumber daya.

Console

Untuk melihat sumber daya yang dibagikan dengan Anda

1. Arahkan ke halaman Shared with me: Shared resources 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, lihatBerbagi 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.
   - Jenis sumber daya — Jenis sumber daya.
   - Tanggal berbagi terakhir — Tanggal di mana sumber daya dibagikan dengan Anda.
   - Pembagian sumber daya — Jumlah pembagian sumber daya di mana sumber daya disertakan. Pilih nilai untuk melihat pembagian sumber daya.
   - ID Pemilik — ID kepala sekolah yang memiliki sumber daya.

AWS CLI

Untuk melihat sumber daya yang dibagikan dengan Anda

Anda dapat menggunakan perintah list-resources untuk melihat sumber daya yang dibagikan dengan Anda.

Contoh perintah berikut menampilkan rincian tentang sumber daya yang dapat diakses melalui berbagi sumber daya yang 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 prinsipal berbagi dengan Anda

Anda dapat melihat daftar semua prinsipal yang berbagi sumber daya dengan Anda. Anda dapat melihat sumber daya dan sumber daya mana yang mereka bagikan dengan Anda.

Console

Untuk melihat prinsipal yang berbagi sumber daya dengan Anda

1. Buka AWS RAM konsol di https://console.aws.amazon.com/ram/rumah.
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, lihatBerbagi 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 prinsip tertentu. Anda dapat menerapkan beberapa filter untuk mempersempit pencarian Anda.
5. Konsol menampilkan informasi berikut:
   - Principal ID — ID kepala sekolah yang berbagi dengan Anda.
   - Pembagian sumber daya — Jumlah pembagian sumber daya yang telah ditambahkan prinsipal kepada Anda. Pilih nomor untuk melihat daftar pembagian sumber daya.
   - Sumber Daya — Jumlah sumber daya yang dibagikan kepala sekolah dengan Anda. Pilih nilai untuk melihat daftar sumber daya.

AWS CLI

Untuk melihat prinsipal yang berbagi sumber daya dengan Anda

Anda dapat menggunakan perintah list-principals untuk mengambil daftar prinsipal yang berbagi sumber daya dengan Anda. Akun AWS

Contoh perintah berikut menampilkan rincian tentang Akun AWS yang berbagi berbagi sumber daya dengan akun yang digunakan untuk memanggil operasi dalam yang ditentukan Wilayah 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 pembagian.

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

Layanan	Jenis sumber daya
Amazon Aurora	`rds:Cluster`
Amazon EC2	`ec2:CapacityReservation` `ec2:DedicatedHost`
AWS License Manager	`license-manager:LicenseConfiguration`

AWS Outposts	`ec2:LocalGatewayRouteTable`
	`outposts:Outpost`
	`outposts:Site`

Amazon Route 53	`route53resolver:ResolverRule`

Amazon VPC	`ec2:CoipPool`
	`ec2:PrefixList`
	`ec2:Subnet`
	`ec2:TrafficMirrorTarget`
	`ec2:TransitGateway`
	`ec2:TransitGatewayMulticastDomain`

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, lihatBerbagi 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-shareperintah 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 akun111111111111.

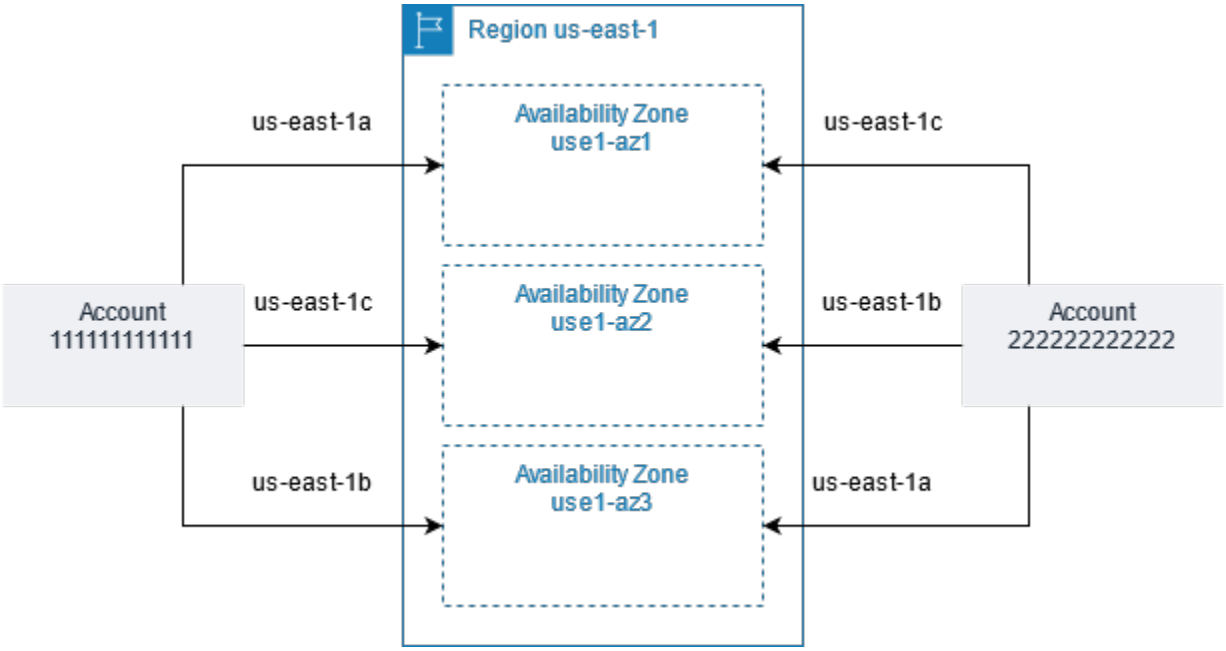
```
$ aws ram disassociate-resource-share \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e \
    --principals 123456789012
                        {
    "resourceShareAssociations": [
        {
            "resourceShareArn":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

Availability Zone IDs untuk AWS sumber daya Anda

AWS memetakan Availability Zone fisik secara acak ke nama Availability Zone untuk masing-masing Akun AWS nama. Pendekatan ini membantu mendistribusikan sumber daya di seluruh Availability Zone di Wilayah AWS, alih-alih sumber daya yang kemungkinan 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 lain. `us-east-1a` Untuk informasi selengkapnya, lihat Wilayah dan Zona Ketersediaan di Panduan EC2 Pengguna Amazon.

Ilustrasi berikut menunjukkan bagaimana AZ IDs 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. Tapi, 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 pengidentifikasi 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 AZ IDs untuk menentukan lokasi sumber daya dalam satu akun relatif terhadap sumber daya di akun lain. Misalnya, jika Anda membagikan subnet di Zona Ketersediaan dengan ID AZ `use1-az2` dengan akun lain, subnet ini tersedia untuk akun tersebut di Zona Ketersediaan yang juga memiliki ID AZ yang juga `use1-az2`. ID AZ untuk setiap subnet ditampilkan di konsol VPC Amazon, dan dapat ditanyakan menggunakan file. AWS CLI

Console

Untuk melihat AZ IDs untuk Availability Zones di akun Anda

1. Arahkan ke halaman AWS RAM konsol di AWS RAM konsol.
2. Anda dapat melihat AZ IDs untuk saat ini Wilayah AWS di bawah ID AZ Anda.

AWS CLI

Untuk melihat AZ IDs untuk Availability Zones di akun Anda

Perintah contoh berikut menunjukkan AZ IDs untuk Availability Zones 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 (OUs) 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	 — Anda dapat berbagi sumber daya jenis ini dengan peran individu AWS Identity and Access Management (IAM) dan pengguna, selain akun.	Ya
	 - Anda dapat berbagi sumber daya jenis ini hanya dengan akun.	Tidak
Dapat berbagi dengan akun di luar organisasinya	 — Anda hanya dapat berbagi sumber daya jenis ini dengan akun individu, di dalam atau di luar organisasinya. Lihat Pertimbangan untuk informasi lebih lanjut.	Ya

	 - Anda dapat berbagi sumber daya jenis ini hanya dengan akun yang merupakan anggota dari organisasi yang sama.	Tidak
Dapat menggunakan izin yang dikelola pelanggan	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.	
	 — sumber daya jenis ini mendukung penggunaan izin yang dikelola pelanggan.	Ya
	 - sumber daya jenis ini tidak mendukung penggunaan izin yang dikelola pelanggan.	Tidak
Dapat berbagi dengan prinsipal layanan	 - Anda dapat berbagi sumber daya jenis ini dengan Layanan AWS.	Ya
	 - Anda tidak dapat berbagi sumber daya jenis ini dengan Layanan AWS.	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 prinsipal layanan
Mesh `appmesh: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 prinsipal layanan
API GraphyQL `appsync:APis`	Kelola AWS AppSync APIs GraphQL secara terpusat, dan bagikan dengan Akun AWS orang lain atau organisasi Anda. Ini memungkinkan beberapa akun berbagi AWS AppSync APIs sebagai bagian dari pembuatan API AWS AppSync Gabungan terpadu yang dapat mengakses data dari beberapa subskema APIs di berbagai akun di Wilayah yang sama. Untuk informasi selengkapnya, lihat Digabungkan APIs dalam Panduan AWS AppSync Pengembang.	 Y	 Y Dapat berbagi dengan apa saja Akun AWS.	 Y	 Tidak

Amazon API Gateway

Anda dapat membagikan sumber daya Amazon API Gateway 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 prinsipal layanan
Nama domain `apigateway:Domainnames`	Buat dan kelola nama domain secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan beberapa akun memanggil nama domain Anda yang dipetakan ke pribadi. APIs Untuk informasi selengkapnya, lihat Nama domain khusus untuk pribadi APIs di API Gateway di Panduan Pengembang Amazon API Gateway.	 T	 Y Dapat berbagi dengan apa saja Akun AWS.	 T	 Tidak

Pengontrol Pemulihan Aplikasi Amazon (ARC)

Anda dapat membagikan sumber daya Amazon Application Recovery Controller (ARC) 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 prinsipal layanan
Gugus ARC `route53-recovery-control:Cluster`	Buat dan kelola cluster 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 Amazon Application Recovery Controller (ARC).	 Y	 Y Dapat berbagi dengan apa saja Akun AWS.	 Y	 Tidak

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 prinsipal layanan
Klaster 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	 Dapat berbagi dengan apa saja Akun AWS. Y	 T	 Tidak

AWS Backup

Anda dapat membagikan AWS Backup 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 prinsipal layanan
BackupVault `backup:BackupVault`	Buat dan kelola kubah celah udara secara logis secara terpusat dan bagikan dengan orang lain atau organisasi Anda. Akun AWS Opsi ini memungkinkan beberapa akun mengakses dan memulihkan cadangan dari brankas. Untuk informasi selengkapnya, lihat Ikhtisar brankas celah udara secara logis di Panduan Pengembang.AWS Backup	 Y	 Y Dapat berbagi dengan apa saja Akun AWS.	 Y	 Tidak

Amazon Bedrock

Anda dapat membagikan sumber daya Amazon Bedrock 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 prinsipal layanan
Model Kustom `bedrock:CustomModel`	Buat dan kelola model kustom secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan beberapa akun menggunakan model kustom yang sama untuk aplikasi AI generatif. Untuk informasi selengkapnya, lihat Membagikan model untuk akun lain di Panduan Pengguna Amazon Bedrock.	 Y	 Tidak Dapat berbagi dengan hanya Akun AWS di organisasinya sendiri.	 Y	 Tidak

AWS Billing Lihat Layanan

Anda dapat membagikan sumber daya AWS Billing Lihat Layanan 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 prinsipal layanan
Tampilan Penagihan `billing:billingview`	Buat dan kelola tampilan penagihan kustom secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan pemilik aplikasi dan unit bisnis mengakses AWS pengeluaran tingkat unit bisnis dari akun anggota. Untuk informasi selengkapnya, lihat Mengontrol akses data manajemen biaya dengan Tampilan Penagihan di Panduan AWS Cost Management Pengguna.	 T	 T Dapat berbagi dengan hanya Akun AWS di organisasinya sendiri.	 Y	 Tidak

AWS CloudHSM

Anda dapat membagikan AWS CloudHSM 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 prinsipal layanan
AWS CloudHSM Backup `cloudhsm:Backup`	Kelola AWS CloudHSM Backup secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Hal ini memungkinkan beberapa Akun AWS dan pengguna melihat informasi tentang Backup dan menggunakannya untuk memulihkan AWS CloudHSM Cluster. Untuk informasi selengkapnya, lihat Mengelola AWS CloudHSM cadangan di AWS CloudHSM Panduan Pengguna.	Y	Y	Y	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 prinsipal layanan
Proyek `codebuild:Project`	Buat proyek, dan gunakan untuk menjalankan build. Bagikan proyek dengan orang lain Akun AWS atau organisasi Anda. Hal 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 AWS CodeBuild Pengguna.	 Y	 Y Dapat berbagi dengan apa saja Akun AWS.	 Y	 Tidak
Kelompok laporan `codebuild:ReportGroup`	Buat grup laporan, dan gunakan untuk membuat laporan saat Anda membangun proyek. Bagikan grup laporan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkin	 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 prinsipal layanan
	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.				

AWS CodeConnections

Anda dapat membagikan CodeConnections 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 prinsipal layanan
Koneksi Kode `codeconnections:Connection`	Kelola penggunaan kembali koneksi kode di beberapa akun. Dengan kata lain, berbagi koneksi kode mengurangi beban administrator dan kebutuhan untuk akses administrator di setiap akun yang memerlukan koneksi kode. Untuk informasi selengkapnya, lihat Berbagi koneksi dengan Akun AWS di Panduan Pengguna Konsol Alat Pengembang.	 T	 Y Dapat berbagi dengan apa saja Akun AWS.	 Y	 Tidak

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 prinsipal 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.	T	Y Dapat berbagi dengan apa saja Akun AWS.	T	Tidak

Amazon EC2

Anda dapat membagikan EC2 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 prinsipal layanan
Reservasi Kapasitas `ec2:CapacityReservation`	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 EC2 instans Amazon mereka ke dalam kapasitas cadangan yang dikelola secara terpusat. Untuk informasi selengkapnya, lihat Bekerja dengan Reservasi Kapasitas bersama di Panduan EC2 Pengguna Amazon. **Important** Jika Anda tidak memenuhi semua prasyarat untuk berbagi reservasi	 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 prinsipal layanan
	kapasitas, maka operasi berbagi dapat gagal. Jika ini terjadi dan pengguna mencoba meluncurkan EC2 instans Amazon ke dalam reservasi kapasitas itu, itu diluncurkan sebagai instance sesuai permintaan yang dapat menghasilkan biaya lebih tinggi. Kami menyarankan Anda memverifikasi bahwa Anda dapat mengakses reservasi kapasitas bersama dengan				

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 prinsipal layanan
	mencoba melihatnya di EC2 konsol Amazon. 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: Peringatan tentang kegagalan				

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 prinsipal layanan
	berbagi sumber daya.				
Host Khusus `ec2:DedicatedHost`	Alokasikan dan kelola host EC2 khusus Amazon secara terpusat, dan bagikan kapasitas instans host dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan beberapa Akun AWS peluncuran EC2 instans Amazon mereka ke host khusus yang dikelola secara terpusat. Untuk informasi selengkapnya, lihat Bekerja dengan Host Khusus bersama di Panduan EC2 Pengguna Amazon.	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 prinsipal layanan
Grup penempatan `ec2:PlacementGroup`	Bagikan grup penempatan yang Anda miliki di seluruh Anda Akun AWS, baik di dalam maupun di luar organisasi Anda. Anda dapat meluncurkan EC2 instans Amazon dari salah satu akun yang Anda bagikan ke grup penempatan bersama. Untuk informasi selengkapnya, lihat Berbagi grup penempatan di Panduan EC2 Pengguna Amazon.	 Y	 Y Dapat berbagi dengan apa saja Akun AWS.	 T	 Tidak

EC2 Image Builder

Anda dapat membagikan sumber daya EC2 Image Builder 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 prinsipal layanan
Komponen-komponen `imagebuilder:Component`	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 Berbagi sumber daya EC2 Image Builder di Panduan Pengguna EC2 Image Builder.	 Y	 Y Dapat berbagi dengan apa saja Akun AWS.	 Y	 Tidak
tanda terima kontainer `imagebuilder:ContainerRecipe`	Buat dan kelola resep kontainer Anda secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan Anda untuk mengelola siapa yang dapat menggunak	 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 prinsipal layanan
	an dokumen yang telah ditentukan untuk menduplikasi build gambar kontainer . Untuk informasi selengkapnya, lihat Berbagi sumber daya EC2 Image Builder di Panduan Pengguna EC2 Image Builder.				
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 Berbagi 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 prinsipal layanan
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 Berbagi sumber daya EC2 Image Builder di Panduan Pengguna EC2 Image Builder.	 Y	 Y Dapat berbagi dengan apa saja Akun AWS.	 Y	 Tidak

Penyeimbang Beban Elastis

Anda dapat membagikan sumber daya Elastic Load Balancing 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 prinsipal layanan
Toko kepercayaan `elasticloadbalancing:TrustStore`	Buat dan kelola toko kepercayaan Elastic Load Balancing secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Admin keamanan dapat mempertahankan jumlah penyimpanan kepercayaan tunggal atau lebih kecil dan mengaktifkan konfigurasi Mutual TLS di seluruh Application Load Balancer. Untuk informasi selengkapnya, lihat Bagikan toko trust Elastic Load Balancing Anda untuk Application Load Balancer di Panduan Pengguna untuk Application Load Balancers.	 Y	 Y	 T	 Tidak

AWS Olah Pesan Pengguna Akhir SMS

Anda dapat membagikan AWS Olah Pesan Pengguna Akhir SMS 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 prinsipal layanan
Daftar opt-out `sms-voice:OptOutList`	Buat daftar opt-out dan bagikan dengan orang lain Akun AWS di organisasi Anda. Anda dapat membagikan daftar opt-out sehingga aplikasi lain dapat memilih keluar nomor telepon pengguna dari yang berbeda Akun AWS atau mereka dapat memeriksa status nomor telepon pengguna. Untuk informasi selengkapnya, lihat Bekerja dengan sumber daya bersama di Panduan AWS Olah Pesan Pengguna Akhir SMS Pengguna.	T	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 prinsipal layanan
Nomor telepon `sms-voice:PhoneNumber`	Buat dan kelola nomor telepon untuk dibagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan beberapa Akun AWS mengirim pesan menggunakan nomor telepon bersama. Untuk informasi selengkapnya, lihat Bekerja dengan sumber daya bersama di Panduan AWS Olah Pesan Pengguna Akhir SMS Pengguna.	 T	 Y Dapat berbagi dengan apa saja Akun AWS.	 Y	 Ya

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 prinsipal layanan
Kolam `sms-voice:Pool`	Buat dan kelola kumpulan untuk membagikannya dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan beberapa Akun AWS mengirim pesan menggunakan kolam bersama. Untuk informasi selengkapnya, lihat Bekerja dengan sumber daya bersama di Panduan AWS Olah Pesan Pengguna Akhir SMS Pengguna.	 T	 Y Dapat berbagi dengan apa saja Akun AWS.	 Y	 Ya

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 prinsipal layanan
ID Pengirim `sms-voice:SenderId`	Buat dan kelola pengirim IDs dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan beberapa Akun AWS mengirim pesan menggunakan ID pengirim bersama. Untuk informasi selengkapnya, lihat Bekerja dengan sumber daya bersama di Panduan AWS Olah Pesan Pengguna Akhir SMS Pengguna.	 T	 Y Dapat berbagi dengan apa saja Akun AWS.	 Y	 Ya

Amazon FSx untuk OpenZFS

Anda dapat membagikan Amazon berikut FSx 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 prinsipal layanan
FSx Volume `fsx:Volume`	Buat dan kelola FSx volume OpenZFS secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan beberapa akun melakukan replikasi data menggunakan OpenZfs snapshot di bawah volume bersama melalui FSx APIs `CreateVolume` atau. `CopySnapshotAndUpdateVolume` 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 prinsipal layanan
Katalog data `glue:Catalog`	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 Pengembang.	 T	 Y Dapat berbagi dengan apa saja Akun AWS.	 T	 Tidak
Basis Data `glue:Database`	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	 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 prinsipal 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 prinsipal layanan
Tabel `glue:Table`	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.	 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 organisasinya	Dapat menggunakan izin yang dikelola pelanggan	Dapat berbagi dengan prinsipal layanan
Konfigurasi lisensi `license-manager:LicenseConfiguration`	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.	 T	 Y Dapat berbagi dengan apa saja Akun AWS.	 T	 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 prinsipal layanan
Entitas Katalog Marketplace `aws-marketplace:Entity`	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 prinsipal 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

Persetujuan multi-pihak

Anda dapat membagikan sumber daya persetujuan Multi-pihak 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 prinsipal layanan
Tim persetujuan `mpa:ApprovalTeam`	Buat dan kelola tim persetujuan dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Hal ini memungkinkan Akun AWS orang lain untuk menggunakan tim persetujuan yang terkait dengan operasi yang dilindungi. Operasi yang dilindungi adalah daftar operasi yang telah ditentukan sebelumnya yang memerlukan persetujuan tim sebelum dapat dieksekusi. Untuk informasi selengkapnya, lihat Syarat dan Konsep di Panduan Pengguna persetujuan multi-pihak.	 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 prinsipal layanan
firewall `network-firewall:Firewall`	Buat dan kelola firewall secara terpusat, dan bagikan dengan yang lain Akun AWS sehingga mereka dapat membuat titik akhir firewall. Ini memungkinkan beberapa akun untuk menggunakan perlindungan dari satu firewall. Untuk informasi selengkapnya, lihat Berbagi AWS Network Firewall sumber daya di Panduan AWS Network Firewall Pengembang.	Y	Y Dapat berbagi dengan apa saja Akun AWS.	T	Tidak
Kebijakan Firewall `network-firewall:FirewallPolicy`	Buat dan kelola kebijakan firewall secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan	Y	Y Dapat berbagi dengan	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 prinsipal layanan
	beberapa akun dalam suatu organisasi untuk berbagi serangkaian perilaku pemantauan, perlindungan, dan penyaringan jaringan yang umum. Untuk informasi selengkapnya, lihat Berbagi AWS Network Firewall sumber daya di Panduan AWS Network Firewall Pengembang.		apa saja Akun AWS.		

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 prinsipal layanan

Kelompok aturan
 	
`network-firewall:StatefulRuleGroup`
 	
`network-firewall:StatelessRuleGroup`
	Buat dan kelola grup aturan tanpa kewarganegaraan dan stateful secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan beberapa akun dalam suatu organisasi AWS Organizations untuk berbagi serangkaian kriteria untuk memeriksa dan menangani lalu lintas jaringan. Untuk informasi selengkapnya, lihat Berbagi AWS Network Firewall sumber daya di Panduan AWS Network Firewall Pengembang.	 Y	 Y
			
			Dapat berbagi dengan apa saja Akun AWS.
				 T	 Tidak

Oracle Database@AWS

Anda dapat membagikan Oracle Database@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 prinsipal layanan
Oracle Database@AWS Infrastruktur Exadata `odb:CloudExadataInfrastructure`	Dengan Oracle Database@AWS, Anda dapat berbagi infrastruktur Exadata dan jaringan ODB Anda di beberapa Akun AWS di organisasi yang sama. AWS Ini memungkinkan Anda untuk menyediakan infrastruktur sekali dan menggunakannya kembali di seluruh akun tepercaya, memungkinkan Anda mengurangi biaya sambil memisahkan tanggung jawab. Untuk informasi selengkapnya, lihat Berbagi sumber daya Oracle Database@AWS di Panduan Oracle Database@AWS Pengguna.	 T	 T Dapat berbagi dengan hanya Akun AWS di organisasinya sendiri.	 T	 Tidak
Oracle Database@AWS Jaringan ODB	Dengan Oracle Database@AWS, Anda dapat berbagi	 T	 T	 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 prinsipal layanan
`odb:OdbNetwork`	infrastruktur Exadata dan jaringan ODB di beberapa Akun AWS di organisasi yang sama. AWS Ini memungkinkan Anda untuk menyediakan infrastruktur sekali dan menggunakannya kembali di seluruh akun tepercaya, memungkinkan Anda mengurangi biaya sambil memisahkan tanggung jawab. Untuk informasi selengkapnya, lihat Berbagi sumber daya Oracle Database@AWS di Panduan Oracle Database@AWS Pengguna.		Dapat berbagi dengan hanya Akun AWS di organisasinya sendiri.		

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 prinsipal layanan
Outposts `outposts:Outpost`	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.	T	T Dapat berbagi dengan hanya Akun AWS di organisasinya sendiri.	Y	Tidak
Tabel rute gateway lokal `ec2:LocalGatewayRouteTable`	Buat dan kelola asosiasi VPC ke gateway lokal secara terpusat, dan bagikan dengan yang lain Akun AWS di organisasi Anda. Ini memungkinkan beberapa akun	T	T Dapat berbagi dengan hanya Akun	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 prinsipal 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 organisasinya 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 prinsipal 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 on 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 prinsipal 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.	 T	 T Dapat berbagi dengan hanya Akun AWS di organisasinya sendiri.	 Y	 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 prinsipal layanan
Otoritas sertifikat swasta (CA) `acm-pca:CertificateAuthority`	Buat dan kelola otoritas sertifikat pribadi (CAs) untuk infrastruktur kunci publik internal organisasi Anda (PKI), dan bagikan CAs 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.	 Y	 Y Dapat berbagi dengan apa saja Akun AWS.	 T	 Ya

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 prinsipal layanan
Tampilan `resource-explorer-2:View`	Buat dan konfigurasikan 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.	 T	 T Dapat berbagi dengan hanya Akun AWS di organisasinya sendiri.	 T	 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 prinsipal 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 EC2 Khusus Amazon yang dibuat menggunakan AWS License Manager. Untuk informasi selengkapnya, lihat Grup sumber daya host AWS License Manager di Panduan AWS License Manager Pengguna.	 T	 Y Dapat berbagi dengan apa saja Akun AWS.	 T	 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 prinsipal layanan
Route 53 Resolver DNS Firewall grup aturan `route53resolver:FirewallRuleGroup`	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.	 Y	 Y Dapat berbagi dengan apa saja Akun AWS.	 T	 Tidak
Rute 53 Profiles `route53profiles:Profile`	Buat dan kelola Route 53 Profiles secara terpusat, dan bagikan dengan orang lain Akun	 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 prinsipal layanan
	AWS atau organisasi Anda. Ini memungkinkan beberapa akun menerapkan konfigurasi DNS yang ditentukan dalam Route 53 Profiles ke beberapa. VPCs 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 organisasinya	Dapat menggunakan izin yang dikelola pelanggan	Dapat berbagi dengan prinsipal layanan
Aturan penyelesai `route53resolver:ResolverRule`	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 (VPCs) 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 Pengembang Amazon Route 53.	 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 prinsipal layanan
Log kueri `route53resolver:ResolverQueryLogConfig`	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 mereka VPCs 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

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 organisasinya	Dapat menggunakan izin yang dikelola pelanggan	Dapat berbagi dengan prinsipal layanan
Hibah Akses `s3:AccessGrants`	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 Access di Panduan Pengguna. Amazon Simple Storage Service	 Y	 Y Dapat berbagi dengan apa saja Akun AWS.	 Y	 Ya

Amazon SageMaker AI

Anda dapat membagikan sumber daya Amazon SageMaker AI 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 prinsipal layanan
SageMaker Katalog AI `sagemaker:SagemakerCatalog`	Untuk dapat ditemukan — memungkinkan pemilik akun memberikan izin untuk dapat ditemukan ke akun lain, untuk semua sumber daya grup fitur dalam katalog AI. 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 AI. **Note** Dapat ditemukan dan akses adalah	 T	 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 prinsipal layanan
	izin terpisah di AI. 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 prinsipal layanan
SageMaker Grup Fitur AI `sagemaker:FeatureGroup`	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 AI. **Note** Dapat ditemukan dan akses adalah izin terpisah di AI. SageMaker	 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 prinsipal layanan
SageMaker AI JumpStart `sagemaker:Hub`	Dengan Amazon SageMaker AI JumpStart, Anda dapat membuat dan mengelola `sagemaker:Hub` secara terpusat, dan membagikannya dengan orang lain Akun AWS di organisasi yang sama. Untuk informasi selengkapnya, lihat Mengontrol akses model foundation menggunakan hub kurasi pribadi di Amazon SageMaker AI JumpStart di Panduan Pengembang Amazon SageMaker AI.	 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 prinsipal layanan
Kelompok silsilah `sagemaker:LineageGroup`	Amazon SageMaker AI memungkinkan Anda membuat grup garis keturunan 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 Pengembang Amazon SageMaker AI.	 Y	 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 prinsipal layanan
SageMaker Kartu Model AI `sagemaker:ModelCard`	Amazon SageMaker AI 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 Model SageMaker AI Amazon di Panduan	 Y	 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 prinsipal layanan
	Pengembang Amazon SageMaker AI.				
SageMaker Grup Package Model Registry Model AI `sagemaker:model-package-group`	Dengan Amazon SageMaker AI Model Registry, Anda dapat membuat dan mengelola `sagemaker:model-package-group` secara terpusat, dan membagikannya dengan yang lain Akun AWS untuk mendaftarkan versi model. Untuk informasi selengkapnya, lihat Amazon SageMaker AI Model Registry di Panduan Pengembang Amazon SageMaker AI.	 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 prinsipal layanan
SageMaker Aplikasi Mitra AI `sagemaker:PartnerApp`	Dengan SageMaker AI Partner AI Apps, Anda dapat membuat dan mengelola SageMaker AI Partner AI Apps secara terpusat, dan berbagi akses kepada mereka dengan yang lain Akun AWS.	 Y	 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 prinsipal layanan
SageMaker Pipa AI `sagemaker:Pipeline`	Dengan Amazon SageMaker AI 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	 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 prinsipal layanan
	Dukungan Lintas Akun untuk Saluran Pipa SageMaker AI di Panduan Pengembang Amazon SageMaker AI.				

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 organisasinya	Dapat menggunakan izin yang dikelola pelanggan	Dapat berbagi dengan prinsipal layanan
Aplikasi `servicecatalog:Applications`	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 memungkin	T	T Dapat berbagi dengan hanya Akun	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 prinsipal layanan
	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.		AWS di organisasinya sendiri.		
Grup Atribut `servicecatalog:AttributeGroups`	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 selengkapnya, lihat Membuat grup atribut di Panduan Pengguna Service Catalog.	 T	 T Dapat berbagi dengan hanya Akun AWS di organisasinya sendiri.	 Y	 Tidak

Manajer Insiden AWS Systems Manager

Anda dapat membagikan Manajer Insiden AWS Systems 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 prinsipal layanan
Kontak `ssm-contacts:Contact`	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. **Note** Saat ini, kemampuan untuk menambahkan kontak yang dibagikan dari akun lain ke rencana	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 prinsipal layanan
	respons insiden tidak didukung. Untuk informasi selengkapnya, lihat Bekerja dengan kontak bersama dan rencana respons di Panduan Pengguna Manajer Insiden AWS Systems Manager.				

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 prinsipal layanan
Rencana respons `ssm-incidents:ResponsePlan`	Buat dan kelola rencana respons secara terpusat, dan bagikan dengan orang 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.	 Y	 Y Dapat berbagi dengan apa saja Akun AWS.	 Y	 Tidak

AWS Systems Manager

Anda dapat membagikan AWS Systems 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 prinsipal layanan
Kebijakan Deny-Access `ssm:Document`	Buat kebijakan persetujuan untuk akses just-in-time node dengan Systems Manager. Kebijakan deny-access secara eksplisit mencegah persetujuan otomatis permintaan akses ke node yang Anda tentukan. Bagikan kebijakan akses penolakan dengan orang lain Akun AWS atau organisasi Anda. Ini memastikan kebijakan akses penolakan Anda untuk akses just-in-time node berlaku untuk semua akun di organisasi Anda. Untuk informasi selengkapnya, lihat akses Just-in-time node	 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 prinsipal layanan
	menggunakan Systems Manager di Panduan AWS Systems Manager Pengguna.				

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 prinsipal layanan
Parameter `ssm:Parameter`	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.	 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 prinsipal layanan
Alamat milik pelanggan IPv4 `ec2:CoipPool`	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. 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 EC2 instance, menggunak	 T	 T Dapat berbagi dengan hanya Akun AWS di organisasinya sendiri.	 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 prinsipal layanan
	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 .				

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 prinsipal 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 prinsipal tersebut mengalokasikan CIDRs dari kumpulan ke AWS sumber daya, seperti VPCs, 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 organisasinya	Dapat menggunakan izin yang dikelola pelanggan	Dapat berbagi dengan prinsipal 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 prinsipal layanan
Daftar prefiks `ec2:PrefixList`	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 prinsipal layanan
Subnet `ec2:Subnet`	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 dikelola VPCs secara terpusat. Sumber daya ini mencakup EC2 instans Amazon, 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. **Note** Untuk menyertakan	 T	 T Dapat berbagi dengan hanya Akun AWS di organisasinya sendiri.	 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 prinsipal layanan
	subnet saat Anda membuat pembagian sumber daya, Anda harus memiliki `ec2:DescribeSubnets` dan `ec2:DescribeVpcs` izin, sebagai tambahan. `ram:CreateResourceShare` Subnet default tidak dapat dibagikan. Anda hanya dapat membagikan subnet yang Anda buat 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 prinsipal layanan
Grup keamanan `ec2:SecurityGroup`	Buat dan kelola grup keamanan secara terpusat, dan bagikan dengan orang lain Akun AWS atau organisasi Anda. Ini memungkinkan beberapa orang Akun AWS mengasosiasikan grup keamanan dengan antarmuka jaringan Elastis mereka. Untuk informasi selengkapnya, lihat Berbagi grup keamanan di Panduan Pengguna Amazon VPC.	 Y	 T Dapat berbagi dengan hanya Akun AWS di organisasinya sendiri.	 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 prinsipal layanan
Target cermin lalu lintas `ec2:TrafficMirrorTarget`	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.	 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 prinsipal layanan
Transit gateway `ec2:TransitGateway`	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 jaringan mereka VPCs dan jaringan lokal melalui gateway transit bersama yang dikelola secara terpusat. Untuk informasi selengkapnya, lihat Berbagi gateway transit di Gateway Transit VPC Amazon. **Note** Untuk menyertakan gateway transit saat Anda membuat pembagian sumber daya, Anda harus	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 prinsipal layanan
	memiliki `ec2:DescribeTransitGateway` izin selain `ituram:CreateResourceShare` .				
Domain multicast gerbang transit `ec2:TransitGatewayMulticastDomain`	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.	 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 prinsipal layanan
Akses Terverifikasi AWS kelompok `ec2:VerifiedAccessGroup`	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.	 Y	 Y Dapat berbagi dengan apa saja Akun AWS.	 T	 Tidak

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 prinsipal layanan
Konfigurasi sumber daya Amazon VPC Lattice `vpc-lattice:ResourceConfiguration`	Buat konfigurasi sumber daya di Amazon VPC Lattice untuk berbagi sumber daya VPC di seluruh akun dan. VCPs Dalam konfigurasi sumber daya, Anda mengidentifikasi siapa yang dapat mengakses sumber daya tersebut dan menentukan gateway sumber daya yang ingin Anda bagikan sumber daya. Konsumen dapat mengakses sumber daya VPC melalui titik akhir VPC sumber daya yang mereka buat. AWS PrivateLinkUntuk informasi selengkapnya, lihat Mengakses sumber daya VPC melalui AWS PrivateLink Panduan AWS PrivateLink Pengguna dan konfigurasi Sumber Daya untuk sumber	 T	 Dapat berbagi dengan apa saja Akun AWS. 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 prinsipal layanan
	daya VPC di Panduan Pengguna Kisi VPC.				
Layanan Amazon VPC Lattice `vpc-lattice:Service`	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.	 T	 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 prinsipal layanan
Jaringan layanan Amazon VPC Lattice `vpc-lattice:ServiceNetwork`	Buat dan kelola jaringan layanan Amazon VPC Lattice secara terpusat, dan bagikan dengan individu Akun AWS atau organisasi Anda. Ini memungkinkan 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.	 T	 Y Dapat berbagi dengan apa saja Akun AWS.	 Y	 Tidak

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 prinsipal layanan
Jaringan inti WAN awan `networkmanager:CoreNetwork`	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.	 Y	 Y Dapat berbagi dengan apa saja Akun AWS.	 T	 Tidak

Mengelola izin di AWS RAM

Di AWS RAM, ada dua jenis izin terkelola, izin AWS terkelola, dan izin terkelola pelanggan.

Izin terkelola menentukan bagaimana konsumen dapat bertindak atas sumber daya 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. Templat kebijakan dalam izin terkelola berisi semua yang diperlukan untuk kebijakan berbasis sumber daya kecuali untuk prinsipal dan sumber daya. Nama Sumber Daya Amazon (ARN) sumber daya dan ARN dari prinsipal yang terkait dengan pembagian sumber daya melengkapi elemen kebijakan berbasis sumber daya. AWS RAM kemudian menulis kebijakan berbasis sumber daya yang dilampirkan ke semua sumber daya dalam pembagian sumber daya itu.

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

> **Note**
>
> Kami menyarankan Anda memperbarui ke versi baru dari izin AWS terkelola sesegera mungkin. Pembaruan ini biasanya menambahkan dukungan untuk yang baru atau Layanan AWS yang diperbarui yang dapat berbagi jenis sumber daya tambahan menggunakan AWS RAM. Versi default baru juga dapat mengatasi dan memperbaiki kerentanan keamanan.

> **Important**
>
> Anda hanya dapat melampirkan versi default izin terkelola ke pembagian sumber daya baru.

Anda dapat mengambil daftar izin terkelola yang tersedia kapan saja. Untuk informasi selengkapnya, lihat Melihat izin terkelola.

Topik

Melihat izin terkelola

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

Console

Untuk melihat detail tentang izin terkelola yang tersedia di AWS RAM

1. Arahkan ke halaman pustaka izin terkelola 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, lihatBerbagi sumber daya regional dibandingkan dengan sumber daya global. Meskipun semua Wilayah berbagi izin AWS terkelola yang tersedia sama, hal ini memengaruhi jumlah pembagian sumber daya terkait yang ditampilkan untuk setiap izin terkelola. Step 5 Izin terkelola pelanggan hanya tersedia di Wilayah tempat mereka dibuat.
3. Dalam daftar Izin terkelola, pilih izin terkelola yang ingin Anda lihat detailnya. Anda dapat menggunakan kotak pencarian untuk memfilter daftar izin terkelola dengan memasukkan bagian dari nama atau jenis sumber daya, atau memilih jenis izin terkelola dari daftar tarik-turun.
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 terkelola, daftar menampilkan informasi berikut:

   - Nama izin terkelola — Nama izin terkelola.
   - Jenis sumber daya — Jenis sumber daya yang terkait dengan izin terkelola.
   - Jenis izin terkelola — Apakah izin terkelola adalah izin AWS terkelola atau izin yang dikelola pelanggan.
   - Saham terkait — Jumlah pembagian sumber daya yang terkait dengan izin yang dikelola. Jika nomor muncul, maka Anda dapat memilih nomor untuk menampilkan tabel pembagian sumber daya dengan informasi berikut:
     - Nama berbagi sumber daya — Nama pembagian sumber daya yang terkait dengan izin terkelola.
     - Versi izin terkelola — Versi izin terkelola yang dilampirkan ke pembagian sumber daya ini.
     - Pemilik — Akun AWS Jumlah pemilik pembagian sumber daya.
     - Izinkan prinsipal eksternal — Apakah pembagian sumber daya itu memungkinkan berbagi dengan kepala sekolah di luar organisasi. AWS Organizations
     - Status — Status asosiasi saat ini antara pembagian sumber daya dan izin terkelola.
   - Status - Menjelaskan apakah izin yang dikelola adalah:
     - Dapat dilampirkan - Anda dapat melampirkan izin terkelola ke pembagian sumber daya Anda.
     - Tidak dapat dilampirkan - Anda tidak dapat melampirkan izin terkelola ke pembagian sumber daya Anda.
     - Menghapus - Izin terkelola tidak lagi aktif dan akan segera dihapus.
     - Dihapus - Izin terkelola telah dihapus. Itu 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 terkelola menampilkan informasi berikut:

- Jenis sumber daya — Jenis AWS sumber daya yang berlaku izin terkelola ini.
- Jumlah versi — Anda dapat memiliki hingga lima versi izin yang dikelola pelanggan.
- Versi default - Menentukan versi mana yang merupakan default dan oleh karena itu ditetapkan secara otomatis ke semua berbagi sumber daya baru yang menggunakan izin terkelola ini. Setiap pembagian sumber daya yang ada yang menggunakan versi berbeda menampilkan prompt bagi Anda untuk memperbarui pembagian sumber daya ke versi default.
- ARN - Nama Sumber Daya Amazon (ARN) dari izin yang dikelola. Izin AWS terkelola ARNs untuk menggunakan format berikut:

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

  Substring *[DefaultPermission]* (tanpa tanda kurung dalam ARN sebenarnya) hadir dalam nama hanya satu izin terkelola untuk jenis sumber daya yang ditetapkan sebagai default.
- Versi izin terkelola - Anda dapat memilih informasi versi mana yang akan ditampilkan di tab di bawah daftar tarik-turun ini.
  - Tab Detail:
    - 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 Templat kebijakan — Daftar tindakan dan ketentuan layanan, jika berlaku, yang memungkinkan pengelola izin terkelola versi ini untuk dilakukan pada jenis sumber daya terkait.
  - Berbagi sumber daya terkait — Daftar pembagian sumber daya yang menggunakan versi izin terkelola ini.

AWS CLI

Untuk melihat detail tentang izin terkelola yang tersedia di AWS RAM

Anda dapat menggunakan list-permissionsperintah untuk mendapatkan daftar izin terkelola yang tersedia untuk digunakan pada pembagian 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 di `--query` parameter perintah. `list-permissions` AWS CLI Contoh berikut menyaring output untuk menyertakan hanya elemen dalam hasil `permissions` array yang cocok dengan nama yang ditentukan. Kami juga menentukan bahwa kami hanya ingin melihat bidang ARN di hasil, dan dalam format teks biasa alih-alih 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 Anda menemukan ARN dari 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\"Effect\": \"Allow\",\n\t\"Action\": [\n
\t\t\"ec2:GetIpamPoolAllocations\",\n\t\t\"ec2:GetIpamPoolCidrs\",\n\t
\t\"ec2:AllocateIpamPoolCidr\",\n\t\t\"ec2:AssociateVpcCidrBlock\",\n
\t\t\"ec2:CreateVpc\",\n\t\t\"ec2:ProvisionPublicIpv4PoolCidr\",\n\t\t
\"ec2:ReleaseIpamPoolAllocation\"\n\t]\n}",
        "creationTime": "2023-03-08T06:54:10.038000-08:00",
        "lastUpdatedTime": "2023-03-08T06:54:10.038000-08:00",
        "isResourceTypeDefault": false,
        "permissionType": "CUSTOMER_MANAGED",
        "featureSet": "STANDARD",
        "status": "ATTACHABLE"
    }
}
```


Membuat dan menggunakan izin terkelola pelanggan di AWS RAM

AWS Resource Access Manager (AWS RAM) memberikan setidaknya satu izin AWS 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. Jika salah satu izin AWS 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 dalam kondisi mana dengan sumber daya yang digunakan bersama. 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.

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 terkelola pelanggan

- Menghapus versi izin terkelola pelanggan
- Menghapus izin terkelola pelanggan

Membuat izin terkelola pelanggan

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

Console

Untuk membuat izin terkelola pelanggan

1. Lakukan salah satu hal berikut ini:
   - Arahkan ke pustaka izin terkelola, dan 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 menerapkan izin terkelola ini.
4. Untuk templat Kebijakan, Anda menentukan operasi mana yang diizinkan untuk dilakukan pada jenis sumber daya ini.
   - Anda dapat memilih Impor izin terkelola untuk menggunakan tindakan dari izin terkelola yang ada.
   - Pilih atau batalkan pilihan informasi tingkat akses untuk memenuhi kebutuhan Anda di editor visual.
   - Menambahkan 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 sesuai kebutuhan.
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 templat kebijakan.

  Perintah contoh berikut membuat izin terkelola 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 berubah, Anda dapat membuat versi baru izin terkelola. Ini tidak memengaruhi pembagian sumber daya yang ada, hanya pembagian sumber daya baru yang akan datang yang menggunakan izin yang dikelola pelanggan ini.

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

Console

Untuk 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 menambahkan atau menghapus tindakan dan kondisi dengan editor visual atau editor JSON.

   Anda juga memiliki opsi untuk memilih Impor izin terkelola untuk menggunakan templat kebijakan yang ada.
5. Setelah selesai, pilih Buat versi di bagian bawah halaman.

AWS CLI

Untuk membuat versi baru izin terkelola pelanggan

1. Temukan Nama Sumber Daya Amazon (ARN) dari izin terkelola yang Anda inginkan buat versi baru. Lakukan ini dengan memanggil izin daftar dengan `--permission-type CUSTOMER_MANAGED` parameter untuk menyertakan hanya 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 memanggil create-permission-versionoperasi dan memberikan templat 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 terkelola pelanggan

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

Console

Untuk menyetel 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 Detail 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. Saat kotak dialog muncul, konfirmasikan 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 menyetel 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 yang ditentukan.

```
$ 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-versionoperasi.

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

Perintah ini tidak mengembalikan output jika berhasil. Anda dapat menjalankan list-permission-versionslagi dan memverifikasi bahwa `defaultVersion` bidang versi yang dipilih sekarang diatur ke`true`.

Menghapus versi izin terkelola pelanggan

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

Console

Untuk 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 bahwa versi yang ingin Anda hapus saat ini bukan default.
4. Untuk bagian Versi halaman, pilih tab Berbagi sumber daya terkait untuk melihat apakah ada saham yang menggunakan versi ini.

Jika ada saham yang terkait, Anda harus mengubah versi izin yang dikelola pelanggan sebelum Anda 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 yang dikelola pelanggan ini.

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

AWS CLI

Untuk menghapus satu versi izin yang dikelola pelanggan

1. Panggil list-permission-versionsoperasi 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 tidak mengembalikan output jika berhasil. Anda dapat menjalankan list-permission-versionslagi 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 dikaitkan dengan pembagian sumber daya. Izin terkelola pelanggan yang dihapus menghilang setelah dua jam. Sampai saat itu, itu tetap terlihat di pustaka izin terkelola dengan status yang dihapus.

Console

Untuk 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 bahwa ada 0 saham terkait dari daftar izin terkelola sebelum memilih izin yang dikelola pelanggan.

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

4. Di sudut kanan atas halaman detail izin terkelola Pelanggan, pilih Hapus izin terkelola.
5. Ketika 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 yang hanya menyertakan izin terkelola 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 izin AWS terkelola ke versi yang lebih baru

Terkadang, AWS perbarui izin AWS terkelola yang tersedia untuk dilampirkan ke pembagian sumber daya untuk jenis sumber daya tertentu. Kapan AWS melakukan ini, itu membuat versi baru dari izin AWS terkelola. Pembagian sumber daya yang menyertakan jenis sumber daya tertentu tidak diperbarui secara otomatis untuk menggunakan versi terbaru dari izin terkelola. Anda harus secara eksplisit memperbarui izin terkelola untuk setiap pembagian sumber daya. Langkah ekstra ini diperlukan agar Anda dapat mengevaluasi perubahan sebelum Anda menerapkannya pada pembagian sumber daya Anda.

Console

Setiap kali konsol menampilkan halaman yang mencantumkan izin yang terkait dengan pembagian sumber daya, dan satu atau beberapa izin tersebut menggunakan versi selain default untuk izin, konsol akan menampilkan spanduk di bagian atas halaman konsol. Spanduk menunjukkan bahwa pembagian 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 tersebut bukan default.

Memilih tombol itu memulai panduan 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 pembagian sumber daya kecuali Anda terlebih dahulu menetapkan versi lain tersebut 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 kemudian menetapkannya sebagai default. Setelah Anda melakukan salah satu opsi tersebut, Anda kemudian akan memperbarui pembagian sumber daya Anda untuk menggunakan apa yang sekarang menjadi versi default.

AWS CLI

Untuk memperbarui versi izin AWS terkelola

1. Jalankan perintah get-resource-sharesdengan `--permission-arn` parameter untuk menentukan Nama Sumber Daya Amazon (ARN) dari izin terkelola yang ingin Anda perbarui. Ini menghasilkan perintah yang hanya mengembalikan pembagian 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 EC2 kapasitas Amazon.

   ```
   $ 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 pembagian sumber daya yang ditentukan dalam perintah sebelumnya, jalankan perintah associate-resource-share-permission. Sertakan `--resource-share-arn` untuk menentukan pembagian sumber daya yang akan diperbarui, `--permission-arn` untuk menentukan izin AWS terkelola 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 setiap `ResourceShareArn` yang Anda terima dalam hasil dari perintah di 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 yang dikelola pelanggan. Untuk daftar jenis sumber daya yang didukung AWS Resource Access Manager, lihatSumber 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:

- Kunci kondisi yang digunakan untuk mencocokkan properti prinsipal:
  - `aws:PrincipalOrgId`
  - `aws:PrincipalOrgPaths`
  - `aws:PrincipalAccount`

- Kunci kondisi yang digunakan untuk membatasi akses untuk prinsipal layanan:
  - `aws:SourceArn`
  - `aws:SourceAccount`
  - `aws:SourceOrgPaths`
  - `aws:SourceOrgID`
- Tag sistem:
  - `aws:PrincipalTag/aws:`
  - `aws:ResourceTag/aws:`
  - `aws:RequestTag/aws:`

> **Note**
>
> `aws:SourceAccount`Nilai secara otomatis diisi saat berbagi ke prinsipal layanan.

Cara kerja izin terkelola

Untuk ikhtisar singkat, tonton video berikut yang menunjukkan bagaimana izin terkelola memungkinkan Anda menerapkan praktik terbaik akses hak istimewa paling sedikit ke sumber daya Anda. AWS

Video ini menunjukkan cara membuat dan mengaitkan izin yang dikelola pelanggan mengikuti praktik terbaik dengan hak istimewa paling sedikit. Untuk informasi lebih lanjut lihat,???.

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

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

Templat kebijakan dalam izin terkelola menentukan hal berikut:

Efek

Menunjukkan apakah untuk `Allow` atau `Deny` izin utama untuk melakukan operasi pada sumber daya bersama. Untuk izin terkelola, efeknya selalu`Allow`. Untuk informasi selengkapnya, lihat Efek dalam Panduan Pengguna IAM.

Tindakan

Daftar operasi yang diberikan izin oleh kepala sekolah untuk dilakukan. Ini bisa berupa tindakan dalam AWS Management Console atau operasi di AWS Command Line Interface (AWS CLI) atau AWS API. Tindakan ditentukan oleh AWS izin. Untuk informasi selengkapnya, lihat Tindakan di Panduan Pengguna IAM.

Ketentuan

Kapan dan bagaimana seorang prinsipal dapat berinteraksi dengan sumber daya dalam pembagian sumber daya. Ketentuan menambahkan lapisan keamanan ekstra 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 tindakan tersebut harus dilakukan

oleh pengguna yang diautentikasi dengan otentikasi multi-faktor. Untuk informasi selengkapnya tentang kondisi, lihat kunci konteks kondisi AWS global di Panduan Pengguna IAM. Untuk informasi selengkapnya tentang kondisi khusus layanan, lihat Tindakan, sumber daya, dan kunci kondisi untuk AWS layanan di Referensi Otorisasi Layanan.

> **Note**
>
> Ketentuan tersedia untuk izin terkelola pelanggan dan jenis sumber daya yang didukung untuk izin AWS terkelola.
> Untuk informasi tentang kondisi yang dikecualikan dari penggunaan dengan izin yang dikelola pelanggan, lihatPertimbangan untuk menggunakan izin terkelola pelanggan di AWS RAM.

Jenis izin terkelola

Saat membuat pembagian sumber daya, Anda memilih izin terkelola untuk dikaitkan dengan setiap jenis sumber daya yang Anda sertakan dalam pembagian sumber daya. AWS izin terkelola ditentukan oleh layanan AWS pemilik sumber daya dan dikelola oleh. AWS RAM Anda membuat dan mempertahankan izin terkelola pelanggan Anda sendiri.

- AWS izin terkelola - Ada satu izin terkelola default yang tersedia untuk setiap jenis sumber daya yang AWS RAM mendukung. Izin terkelola default adalah 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 tertentu yang ditentukan oleh layanan untuk jenis sumber daya. Misalnya, untuk jenis `ec2:Subnet` sumber daya Amazon VPC, izin terkelola default memungkinkan prinsipal untuk melakukan tindakan berikut:
  - `ec2:RunInstances`
  - `ec2:CreateNetworkInterface`
  - `ec2:DescribeSubnets`

  Nama-nama izin AWS terkelola default menggunakan format berikut:`AWSRAMDefaultPermission`*`ShareableResourceType`*. Misalnya, untuk jenis `ec2:Subnet` sumber daya, nama izin AWS terkelola default adalah`AWSRAMDefaultPermissionSubnet`.

> **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, adalah izin terpisah dan lengkap dengan efek dan tindakan berbeda yang mendukung skenario berbagi yang berbeda, seperti akses baca-tulis versus akses hanya-baca. Izin terkelola apa pun, baik yang dikelola pelanggan AWS atau pelanggan dapat memiliki beberapa versi, salah satunya adalah versi default untuk izin tersebut.

Misalnya, saat Anda membagikan jenis sumber daya yang mendukung izin terkelola akses penuh (`ReaddanWrite`) serta izin terkelola hanya-baca, Anda dapat membuat satu pembagian sumber daya untuk administrator dengan izin terkelola akses penuh. Anda kemudian dapat membuat pembagian sumber daya terpisah untuk pengembang lain menggunakan izin terkelola hanya-baca untuk mengikuti praktik pemberian hak istimewa paling sedikit.

> **Note**
>
> Semua AWS layanan yang bekerja dengan AWS RAM dukungan setidaknya satu izin terkelola default. Anda dapat melihat izin yang tersedia untuk masing-masing Layanan AWS di halaman pustaka izin terkelola. Halaman ini memberikan rincian tentang setiap izin terkelola yang tersedia, termasuk pembagian sumber daya apa pun yang saat ini terkait dengan izin dan apakah berbagi dengan kepala sekolah eksternal diperbolehkan, jika berlaku. Untuk informasi selengkapnya, lihat Melihat izin terkelola.
>
> Untuk layanan yang tidak mendukung izin terkelola tambahan, saat Anda membuat pembagian 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 dalam kondisi mana dengan sumber daya yang digunakan bersama. 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.

Keamanan di AWS RAM

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

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara berkala menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program kepatuhan AWS. Untuk mempelajari tentang program kepatuhan yang berlaku untuk AWS Resource Access Manager (AWS RAM), lihat AWS Layanan dalam Lingkup berdasarkan Program Kepatuhan.
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

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

Topik

Perlindungan data di AWS RAM

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di AWS Resource Access Manager. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensyal dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat Bekerja dengan CloudTrail jejak di AWS CloudTrail Panduan Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-3.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan AWS RAM atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDKs. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan

atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Identitas dan manajemen akses untuk AWS RAM

AWS Identity and Access Management (IAM) adalah AWS layanan yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator dalam kontrol IAM yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya. AWS Dengan menggunakan IAM, Anda membuat prinsipal, seperti peran, pengguna, dan grup di Anda. Akun AWS Anda mengontrol izin yang dimiliki kepala sekolah tersebut untuk melakukan 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

- Bagaimana AWS RAM bekerja dengan IAM
- AWS kebijakan terkelola 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

Bagaimana AWS RAM bekerja dengan IAM

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

Untuk memberikan akses dan menambahkan izin bagi pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

  Buat rangkaian izin. Ikuti instruksi di Buat rangkaian izin di Panduan Pengguna AWS IAM Identity Center .

- Pengguna yang dikelola di IAM melalui penyedia identitas:

  Buat peran untuk federasi identitas. Ikuti instruksi dalam Buat peran untuk penyedia identitas pihak ketiga (federasi) dalam Panduan Pengguna IAM.
- Pengguna IAM:
  - Buat peran yang dapat diambil pengguna Anda. Ikuti instruksi dalam Buat peran untuk pengguna IAM dalam Panduan Pengguna IAM.
  - (Tidak disarankan) Lampirkan kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti instruksi dalam Menambahkan izin ke pengguna (konsol) dalam 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, lihatAWS kebijakan terkelola untuk AWS RAM.

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

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

Daftar Isi

Struktur kebijakan

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

Tindakan

Pernyataan Action menentukan tindakan AWS RAM API yang memungkinkan atau menolak izin oleh kebijakan tersebut. Untuk daftar lengkap tindakan yang diizinkan, lihat Tindakan yang ditentukan oleh AWS Resource Access Manager dalam Panduan Pengguna IAM.

Sumber Daya

Pernyataan Sumber Daya menentukan AWS RAM sumber daya yang dipengaruhi oleh kebijakan. Untuk menentukan sumber daya dalam pernyataan, Anda perlu menggunakan Nama Sumber Daya Amazon (ARN) yang unik. Untuk daftar lengkap sumber daya yang diizinkan, lihat Sumber daya yang ditentukan oleh AWS Resource Access Manager dalam Panduan Pengguna IAM.

Ketentuan

Pernyataan kondisi bersifat opsional. Mereka dapat digunakan untuk lebih menyempurnakan kondisi di mana kebijakan berlaku. AWS RAM mendukung kunci kondisi berikut:

- `aws:RequestTag/${TagKey}`— Menguji apakah permintaan layanan menyertakan tag dengan kunci tag yang ditentukan ada dan memiliki nilai yang ditentukan.
- `aws:ResourceTag/${TagKey}`— Menguji 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 berbagi sumber daya.
- `ram:AllowsExternalPrincipals`— Menguji apakah pembagian sumber daya dalam permintaan layanan memungkinkan berbagi dengan prinsipal eksternal. Kepala sekolah eksternal adalah Akun AWS bagian luar organisasi Anda di AWS Organizations. Jika ini dievaluasi`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`— Menguji apakah izin yang ditentukan dalam permintaan layanan valid untuk jenis sumber daya yang Anda tentukan dalam kebijakan. Tentukan jenis sumber daya menggunakan format yang ditampilkan 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 tipe sumber daya yang Anda tentukan dalam kebijakan. Tentukan jenis sumber daya menggunakan format yang ditampilkan 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 pembagian sumber daya yang ditindaklanjuti oleh permintaan layanan cocok dengan string yang Anda tentukan dalam kebijakan.
- `ram:ShareOwnerAccountId`— Menguji nomor ID akun dari pembagian sumber daya yang ditindaklanjuti oleh permintaan layanan cocok dengan string yang Anda tentukan dalam kebijakan.

AWS kebijakan terkelola untuk AWS RAM

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

AWS kebijakan terkelola

- AWS kebijakan terkelola: AWSResource AccessManagerReadOnlyAccess
- AWS kebijakan terkelola: AWSResource AccessManagerFullAccess
- AWS kebijakan terkelola: AWSResource AccessManagerResourceShareParticipantAccess
- AWS kebijakan terkelola: AWSResource AccessManagerServiceRolePolicy
- AWS RAM pembaruan kebijakan AWS terkelola

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

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

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

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS 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.

AWS kebijakan terkelola: AWSResource AccessManagerReadOnlyAccess

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

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

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

Detail izin

Kebijakan ini mencakup izin berikut.

- `ram`— Memungkinkan kepala sekolah untuk melihat detail tentang pembagian sumber daya yang dimiliki oleh akun.

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

AWS kebijakan terkelola: AWSResource AccessManagerFullAccess

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

Kebijakan ini menyediakan akses administratif penuh untuk melihat atau memodifikasi pembagian sumber daya yang dimiliki oleh Anda Akun AWS.

Ini dilakukan dengan memberikan izin untuk menjalankan `ram` operasi apa pun.

Detail izin

Kebijakan ini mencakup izin berikut.

- `ram`— Memungkinkan kepala sekolah untuk melihat atau memodifikasi informasi apa pun tentang pembagian sumber daya yang dimiliki oleh. Akun AWS

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

AWS kebijakan terkelola: AWSResource AccessManagerResourceShareParticipantAccess

Anda dapat melampirkan kebijakan `AWSResourceAccessManagerResourceShareParticipantAccess` ke identitas IAM Anda.

Kebijakan ini memberi para prinsipal kemampuan untuk menerima atau menolak pembagian sumber daya yang dibagikan dengan ini Akun AWS, dan untuk melihat detail tentang pembagian sumber daya ini. Itu tidak memberikan kemampuan apa pun untuk memodifikasi pembagian sumber daya tersebut.

Ini dilakukan dengan memberikan izin untuk menjalankan beberapa `ram` operasi.

Detail izin

Kebijakan ini mencakup izin berikut.

- `ram`— Memungkinkan prinsipal untuk menerima atau menolak undangan berbagi sumber daya dan untuk melihat detail tentang pembagian 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": "*"
        }
    ]
}
```

AWS kebijakan terkelola: AWSResource AccessManagerServiceRolePolicy

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

Kebijakan ini AWS RAM menyediakan akses hanya-baca ke struktur organisasi Anda. Saat Anda mengaktifkan integrasi antara AWS RAM dan AWS Organizations, AWS RAM secara otomatis membuat peran terkait layanan bernama AWSServiceRoleForResourceAccessManageryang diasumsikan layanan saat perlu mencari informasi tentang organisasi Anda dan akunnya, misalnya, saat Anda melihat struktur organisasi di konsol. AWS RAM

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 kepala sekolah untuk melihat informasi tentang struktur organisasi, termasuk unit organisasi, dan yang dikandungnya. Akun AWS

```
{
    "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 pembaruan kebijakan AWS terkelola

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

Perubahan	Deskripsi	Tanggal
AWS Resource Access Manager mulai melacak perubahan	AWS RAM mendokume ntasikan 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 peran terkait layanan (IAM). 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, lihat Layanan AWS yang bisa digunakan dengan IAM dan carilah layanan yang memiliki opsi Ya di kolom Peran Terkait Layanan. Pilih Ya bersama tautan untuk melihat dokumentasi peran tertaut 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 AWSResource AccessManagerServiceRolePolicy 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 Tertaut Layanan di Panduan Pengguna IAM.

Membuat Peran Tertaut Layanan untuk AWS RAM

Anda tidak perlu membuat peran terkait layanan secara manual. Ketika Anda mengaktifkan AWS RAM berbagi dalam organisasi Anda di AWS Management Console, atau menjalankan EnableSharingWithAwsOrganizationdi akun Anda menggunakan AWS CLI atau AWS API, AWS RAM membuat 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 AWSResource AccessManagerServiceRolePolicy terkait layanan. Setelah Anda membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengedit penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, 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, the AWS CLI, atau AWS API untuk menghapus peran `AWSResourceAccessManagerServiceRolePolicy` terkait layanan. Untuk informasi selengkapnya, silakan lihat Menghapus Peran Terkait Layanan di Panduan Pengguna IAM.

Wilayah yang Didukung untuk Peran AWS RAM Tertaut Layanan

AWS RAM mendukung penggunaan peran terkait 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 AWS RAM yang menunjukkan berbagi sumber daya dan jenis sumber daya tertentu dan 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 agar hanya mengaitkan sumber daya tertentu dengan pembagian sumber daya.

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

Untuk informasi selengkapnya tentang kapan dan mengapa menggunakan `...IfExists` operator, lihat... IfExists operator 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 agar hanya mengaitkan jenis sumber daya tertentu dengan pembagian sumber daya.

Tindakan, `AssociateResourceShare` dan`CreateResourceShare`, dapat menerima prinsip dan `resourceArns` sebagai parameter input independen. Oleh karena itu, AWS RAM otorisasi setiap prinsipal dan sumber daya secara independen, sehingga mungkin ada beberapa konteks permintaan. Ini berarti ketika prinsipal dikaitkan dengan pembagian AWS RAM sumber daya, kunci `ram:RequestedResourceType` kondisi tidak ada dalam konteks permintaan. Demikian pula, ketika sumber daya dikaitkan dengan pembagian AWS RAM sumber daya, kunci `ram:Principal` kondisi tidak ada dalam konteks permintaan. Oleh karena itu, untuk mengizinkan `AssociateResourceShare` dan `CreateResourceShare` ketika mengaitkan prinsipal ke pembagian AWS RAM sumber daya, Anda dapat menggunakan operator kondisi. `Null`

Misalnya, kebijakan berikut membatasi prinsipal untuk hanya membagikan aturan penyelesai Amazon Route 53 dan memungkinkan mereka untuk mengaitkan prinsipal apa pun dengan pembagian tersebut.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AllowOnlySpecificResourceType",
        "Effect": "Allow",
        "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "ram:RequestedResourceType": "route53resolver:ResolverRule"
            }
        }
    },
    {
    "Sid": "AllowAssociatingPrincipals",
     "Effect": "Allow",
        "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
        "Resource": "*",
        "Condition": {
            "Null": {
                "ram:Principal": "false"
             }
```

```
        }
    }
  ]
}
```

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 pembagian 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 (SCPs). SCPs 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. SCPs 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 menggunakannya SCPs, 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 SCPs untuk digunakan dalam organisasi Anda. Untuk informasi selengkapnya, lihat Mengaktifkan dan menonaktifkan jenis kebijakan di Panduan Pengguna AWS Organizations
- Buat SCPs yang Anda butuhkan. Untuk informasi selengkapnya tentang membuat SCPs, lihat Membuat dan memperbarui SCPs di Panduan AWS Organizations Pengguna.

Contoh Kebijakan Kontrol Layanan

Daftar Isi

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.

AWS RAM mengotorisasi APIs secara terpisah untuk setiap prinsipal dan sumber daya yang tercantum dalam panggilan.

```
{
    "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

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 EC2 awalan Amazon atau untuk mengaitkan daftar awalan dengan pembagian sumber daya yang ada.

AWS RAM mengotorisasi APIs secara terpisah untuk setiap prinsipal dan sumber daya yang tercantum dalam panggilan.

Operator `StringEqualsIfExists` mengizinkan permintaan jika permintaan tidak menyertakan parameter tipe sumber daya, atau jika menyertakan parameter itu, nilainya sama persis dengan jenis sumber daya yang ditentukan. Jika Anda termasuk kepala sekolah, Anda harus memilikinya`...IfExists`.

Untuk informasi selengkapnya tentang kapan dan mengapa menggunakan `...IfExists` operator, lihat... IfExists operator kondisi di Panduan Pengguna IAM.

```
{
    "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.

AWS RAM mengotorisasi APIs secara terpisah untuk setiap prinsipal dan sumber daya yang tercantum dalam panggilan.

```
{
    "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`, organisasi`ou-98765fedcba`, dan Akun AWS `111111111111`.

Jika Anda menggunakan `"Effect": "Deny"` elemen dengan operator kondisi yang dinegasikan`StringNotEqualsIfExists`, seperti, permintaan masih ditolak meskipun kunci kondisi tidak ada. Gunakan operator `Null` kondisi untuk memeriksa apakah kunci kondisi tidak ada pada saat otorisasi.

AWS RAM mengotorisasi APIs secara terpisah untuk setiap prinsipal dan sumber daya yang tercantum dalam panggilan.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:AssociateResourceShare",
        "ram:CreateResourceShare"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "ram:Principal": [
```

```
            "arn:aws:organizations::123456789012:organization/o-12345abcdef",
            "arn:aws:organizations::123456789012:ou/o-12345abcdef/ou-98765fedcba",
            "111111111111"
          ]
        },
        "Null": {
          "ram:Principal": "false"
        }
      }
    }
  ]
}
```

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 (OUs), Anda dapat menonaktifkan berbagi. Ketika Anda menonaktifkan berbagi dengan AWS Organizations, semua organisasi atau OUs dihapus dari berbagi 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 AWSServiceRoleForResourceAccessManagerlayanan. Untuk informasi selengkapnya, lihat Menghapus peran tertaut layanan dalam Panduan Pengguna IAM.

Penebangan dan pemantauan di AWS RAM

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

Amazon EventBridge

Memberikan near-real-time aliran peristiwa sistem yang menggambarkan perubahan AWS sumber daya. EventBridge mengaktifkan komputasi berbasis peristiwa otomatis, karena Anda dapat menulis aturan yang mengawasi peristiwa tertentu dan memicu tindakan otomatis di AWS layanan lain saat peristiwa ini terjadi. Untuk informasi selengkapnya, lihat Pemantauan AWS RAM menggunakan EventBridge.

AWS CloudTrail

Menangkap panggilan API dan peristiwa terkait yang dibuat oleh atau atas nama Anda Akun AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun mana yang dipanggil AWS, alamat IP sumber dari mana panggilan dilakukan, dan kapan panggilan terjadi. Untuk informasi selengkapnya, lihat Pencatatan panggilan AWS RAM API dengan AWS CloudTrail.

Pemantauan AWS RAM menggunakan EventBridge

Menggunakan Amazon EventBridge, Anda dapat mengatur notifikasi otomatis untuk acara tertentu di AWS RAM. Acara dari AWS RAM dikirim ke EventBridge dalam waktu hampir nyata. Anda dapat mengonfigurasi EventBridge 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 pembagian sumber daya dan prinsipal yang diberikan akses ke pembagian 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, tetapi dipancarkan atas dasar upaya terbaik. Jika terjadi kesalahan saat AWS RAM mencoba

memancarkan suatu peristiwa, layanan mencoba beberapa kali lagi. Namun, itu bisa time out dan mengakibatkan hilangnya peristiwa spesifik itu.

Untuk informasi selengkapnya, lihat Panduan EventBridge Pengguna Amazon.

Contoh: Peringatan tentang kegagalan berbagi sumber daya

Pertimbangkan skenario di mana Anda ingin berbagi reservasi EC2 kapasitas Amazon dengan akun lain di organisasi Anda. Melakukan 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 instance dengan salah satu reservasi kapasitas tersebut, Amazon EC2 bertindak seolah-olah reservasi kapasitas penuh dan meluncurkan instans sebagai instans sesuai permintaan. Ini dapat menghasilkan biaya yang lebih tinggi dari yang diharapkan.

Untuk memantau kegagalan berbagi sumber daya, siapkan EventBridge aturan Amazon yang memberi tahu Anda setiap kali pembagian AWS RAM sumber daya gagal. Prosedur tutorial berikut menggunakan topik Amazon Simple Notification Service (SNS) untuk memberi tahu semua pelanggan topik setiap kali EventBridge menemukan kegagalan berbagi sumber daya. Untuk informasi selengkapnya tentang Amazon SNS, lihat Panduan Developer Amazon Simple Notification Service.

Untuk membuat aturan yang memberi tahu Anda saat berbagi sumber daya gagal

1. Buka EventBridge konsol Amazon.
2. Di panel navigasi, pilih Aturan, lalu di daftar Aturan, pilih Buat aturan.
3. Masukkan nama dan deskripsi opsional untuk aturan Anda, lalu pilih Berikutnya.
4. Gulir ke bawah ke kotak Pola acara, dan pilih Pola kustom (editor JSON).
5. Salin dan tempel pola acara berikut:

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

```
    }
}
```

6. Pilih Berikutnya.
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 yang ingin Anda publikasikan notifikasi. Topik ini pasti sudah ada.
10. Pilih Berikutnya, lalu pilih Berikutnya lagi untuk melihat untuk meninjau konfigurasi Anda.
11. Jika Anda puas dengan pilihan 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 itu diaktifkan, pembagian AWS RAM sumber daya apa pun yang gagal menghasilkan peringatan SNS kepada penerima topik yang Anda publikasikan.

Anda juga dapat mengonfirmasi bahwa reservasi kapasitas bersama dapat diakses ke akun yang Anda bagikan dengan mencoba melihatnya di EC2 konsol Amazon dari akun tersebut.

Pencatatan panggilan AWS RAM API 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 menangkap semua panggilan API untuk AWS RAM sebagai peristiwa. Panggilan yang diambil termasuk panggilan dari AWS RAM konsol dan panggilan kode ke operasi AWS RAM API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail peristiwa secara terus menerus ke bucket Amazon S3 yang Anda tentukan, termasuk acara untuk. AWS RAM Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Gunakan informasi yang dikumpulkan oleh CloudTrail untuk menentukan permintaan yang dibuat AWS RAM, alamat IP yang meminta, pemohon, kapan dibuat, dan detail tambahan.

Untuk informasi selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

AWS RAM informasi di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi di AWS RAM, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh acara terbaru di situs

Anda Akun AWS. Untuk informasi selengkapnya, lihat Melihat Acara dengan Riwayat CloudTrail Acara.

Untuk catatan berkelanjutan tentang peristiwa di Akun AWS, termasuk peristiwa untuk AWS RAM, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua AWS Wilayah. 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 lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut ini:

- Membuat jejak untuk Anda Akun AWS
- Layanan AWS integrasi dengan log CloudTrail
- Mengkonfigurasi Notifikasi Amazon SNS untuk CloudTrail
- Menerima file CloudTrail log dari beberapa Wilayah dan Menerima file 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 acara atau entri log berisi informasi yang membantu Anda menentukan siapa yang membuat permintaan.

- Akun AWS kredensi root
- Kredensi keamanan sementara dari peran AWS Identity and Access Management (IAM) atau pengguna federasi.
- Kredensi keamanan jangka panjang dari pengguna IAM.
- AWS Layanan lain.

Untuk informasi selengkapnya, lihat Elemen userIdentity CloudTrail .

Memahami entri file AWS RAM log

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili

permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log untuk `CreateResourceShare` 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 AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang dan mengoperasikan aplikasi dan basis data yang secara otomatis melakukan failover di antara Zona Ketersediaan tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur biasa yang terdiri dari satu atau beberapa pusat data.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur AWS Global.

Keamanan infrastruktur di 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 mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

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

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan prinsipal IAM. Atau Anda bisa menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

Akses AWS Resource Access Manager menggunakan endpoint antarmuka ()AWS PrivateLink

Anda dapat menggunakan AWS PrivateLink untuk membuat koneksi pribadi antara VPC Anda dan. AWS Resource Access Manager Anda dapat mengakses AWS RAM seolah-olah itu ada di VPC Anda, tanpa menggunakan gateway internet, perangkat NAT, koneksi VPN, atau koneksi. AWS Direct Connect Instans di VPC Anda tidak memerlukan alamat IP publik untuk mengakses. AWS RAM

Anda membuat koneksi pribadi ini dengan membuat titik akhir antarmuka, yang didukung oleh AWS PrivateLink. Kami membuat antarmuka jaringan endpoint di setiap subnet yang Anda aktifkan untuk titik akhir antarmuka. Ini adalah antarmuka jaringan yang dikelola pemohon yang berfungsi sebagai titik masuk untuk lalu lintas yang ditakdirkan. AWS RAM

Untuk informasi selengkapnya, lihat Mengakses Layanan AWS melalui AWS PrivateLink di Panduan AWS PrivateLink .

Pertimbangan untuk AWS RAM

Sebelum Anda menyiapkan titik akhir antarmuka AWS RAM, tinjau Pertimbangan dalam Panduan.AWS PrivateLink

AWS RAM mendukung panggilan ke semua tindakan API-nya melalui titik akhir antarmuka.

Kebijakan titik akhir VPC didukung untuk. AWS RAM Secara default, akses penuh ke AWS RAM diizinkan melalui titik akhir antarmuka.

Buat titik akhir antarmuka untuk AWS RAM

Anda dapat membuat titik akhir antarmuka untuk AWS RAM menggunakan konsol VPC Amazon atau () AWS Command Line Interface .AWS CLI Untuk informasi selengkapnya, lihat Membuat titik akhir antarmuka di AWS PrivateLink Panduan.

Buat titik akhir antarmuka untuk AWS RAM menggunakan nama layanan berikut:

```
com.amazonaws.region.ram
```

Jika Anda mengaktifkan DNS pribadi untuk titik akhir antarmuka, Anda dapat membuat permintaan API untuk AWS RAM menggunakan nama DNS Regional default. Misalnya, `ram.us-east-1.amazonaws.com`.

Buat kebijakan titik akhir untuk titik akhir antarmuka Anda

Kebijakan endpoint adalah sumber daya IAM yang dapat Anda lampirkan ke titik akhir antarmuka. Kebijakan endpoint default memungkinkan akses penuh AWS RAM melalui titik akhir antarmuka. Untuk mengontrol akses yang diizinkan AWS RAM dari VPC Anda, lampirkan kebijakan titik akhir kustom ke titik akhir antarmuka.

kebijakan titik akhir mencantumkan informasi berikut:

- Prinsipal yang dapat melakukan tindakan (Akun AWS, pengguna IAM, dan peran IAM).
- Tindakan yang dapat dilakukan.
- Sumber daya untuk melakukan tindakan.

Untuk informasi selengkapnya, lihat Mengontrol akses ke layanan menggunakan kebijakan titik akhir di Panduan AWS PrivateLink .

Contoh: Kebijakan titik akhir VPC untuk tindakan AWS RAM

Berikut ini adalah contoh kebijakan endpoint kustom. Saat Anda melampirkan kebijakan ini ke titik akhir antarmuka Anda, kebijakan ini akan memberikan akses ke AWS RAM tindakan yang tercantum untuk semua prinsip di semua sumber daya.

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

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”

Skenario

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

Penyebab

Kesalahan ini dapat terjadi jika peran terkait layanan AWSServiceRoleForResourceAccessManagertidak 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.

> **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.

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.

Anda sekarang harus dapat menggunakan AWS RAM untuk berbagi sumber daya Anda dengan akun dan OUs 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 dan menambahkan izin bagi pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

  Buat rangkaian izin. Ikuti instruksi di Buat rangkaian izin di Panduan Pengguna AWS IAM Identity Center .

- Pengguna yang dikelola di IAM melalui penyedia identitas:

  Buat peran untuk federasi identitas. Ikuti instruksi dalam Buat peran untuk penyedia identitas pihak ketiga (federasi) dalam Panduan Pengguna IAM.

- Pengguna IAM:
  - Buat peran yang dapat diambil pengguna Anda. Ikuti instruksi dalam Buat peran untuk pengguna IAM dalam Panduan Pengguna IAM.
  - (Tidak disarankan) Lampirkan kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti instruksi dalam 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 organisasi Anda. SCPs

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:

- *`resourceOwningService`*`:`*`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- tidak *xxxx* dapat ditemukan”
- “CannotUpdateResourceShare: UnknownResourceException: OrganizationalUnit ou- tidak *xxxx* dapat ditemukan”.

Penyebab

Kesalahan ini dapat terjadi jika Anda mengaktifkan integrasi antara AWS RAM dan AWS Organizations dengan menggunakan konsol Organizations atau Organizations Enable AWSService Access 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 (OUs) di organisasi Anda.

Solusi

Untuk mengatasi masalah ini, matikan integrasi antara AWS RAM dan AWS Organizations. Kemudian nyalakan lagi dengan memanggil operasi AWS RAM EnableSharingWithAwsOrganizationAPI, atau dengan menggunakan AWS Management Console untuk melakukan langkah-langkah berikut.

> **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.

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.

Anda sekarang harus dapat menggunakan AWS RAM untuk berbagi sumber daya Anda dengan akun dan OUs 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 (VPCs) 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.

> **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.

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.

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 AWS Organizations kotak 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.

> **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.

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.

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 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 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 batasan ini. Untuk meminta kenaikan batas, hubungi Dukungan.

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 pembagian sumber daya dihitung sebagai satu terhadap kuota ini. Jika Anda berbagi sumber daya yang sama dalam tiga pembagian sumber daya yang berbeda, itu meningkatkan jumlah Anda untuk kuota ini sebanyak tiga.
- Berbagi sumber daya - Wadah 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 satu terhadap kuota Anda.
- Prinsipal bersama — Pengidentifikasi yang Anda kaitkan dengan pembagian sumber daya. Ini bisa berupa peran AWS Identity and Access Management (IAM) atau pengguna, Akun AWS pengenal, unit organisasi, atau seluruh organisasi. Setiap prinsipal bersama yang Anda referensikan dalam pembagian sumber daya menambahkan satu ke penggunaan kuota Anda. Jika Anda berbagi dengan seluruh organisasi dengan mereferensikan ID-nya, itu dihitung sebagai hanya 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 bagaimana sumber daya bersama Anda digunakan.

Sumber Daya	Batas default
Jumlah maksimum pembagian sumber daya per Wilayah AWS	25.000
Jumlah maksimum asosiasi sumber daya per pembagian sumber daya	5.000

Sumber Daya	Batas default
Jumlah maksimum asosiasi utama per pembagian sumber daya	5.000
Jumlah maksimum izin yang dikelola pelanggan	1.500
Jumlah maksimum izin terkelola pelanggan per jenis sumber daya	10
Jumlah maksimum versi per izin yang dikelola pelanggan	5
Jumlah maksimum asosiasi sumber daya di semua pembagian sumber daya dalam Wilayah AWS **Note** Setiap sumber daya yang disertakan dalam pembagian sumber daya dihitung terhadap batas ini. Jika sumber daya termasuk dalam 10 pembagian sumber daya yang berbeda, itu menghitung 10 terhadap batas.	25.000
Jumlah maksimum asosiasi utama di semua pembagian sumber daya dalam Wilayah AWS **Note** Setiap prinsipal yang termasuk dalam pembagian sumber daya dihitung terhadap batas ini. Jika prinsipal termasuk dalam 10 saham sumber daya yang berbeda, itu menghitung 10 terhadap batas.	25.000

Sumber Daya	Batas default
Jumlah maksimum undangan yang tertunda per akun berbagi • Kuota ini berlaku hanya untuk mengirim akun yang berbagi dengan akun yang bukan bagian dari akun yang sama AWS Organizations. • Tidak ada kuota untuk membatasi berapa banyak undangan yang tertunda yang dapat dimiliki oleh akun penerima. • Undangan tidak digunakan saat berbagi antar akun yang merupakan bagian dari yang sama AWS Organizations dan Anda telah mengaktifkan berbagi sumber daya di dalam akun. AWS Organizations	250

Menggunakan AWS RAM dengan AWS SDK

AWS kit pengembangan perangkat lunak (SDKs) tersedia untuk banyak bahasa pemrograman populer. Setiap SDK menyediakan API, contoh kode, dan dokumentasi yang membantu pengembang membangun aplikasi dalam bahasa pilihan mereka.

Dokumentasi SDK	Contoh kode
AWS SDK untuk C++	AWS SDK untuk C++ contoh kode
AWS SDK untuk Go	AWS SDK untuk Go contoh kode
AWS SDK untuk Java	AWS SDK untuk Java contoh kode
AWS SDK untuk JavaScript	AWS SDK untuk JavaScript contoh kode
AWS SDK untuk .NET	AWS SDK untuk .NET contoh kode
AWS SDK untuk PHP	AWS SDK untuk PHP contoh kode
AWS SDK untuk Python (Boto3)	AWS SDK untuk Python (Boto3) contoh kode
AWS SDK untuk Ruby	AWS SDK untuk Ruby contoh kode

Ketersediaan contoh

Tidak dapat 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 Oracle Database@ AWS sumber daya	Anda sekarang dapat berbagi infrastruktur Oracle Database@AWS Exadata dan jaringan ODB dengan yang lain di Akun AWS dalam organisasi Anda.	Juni 30, 2025
Menambahkan dukungan untuk berbagi sumber daya persetujuan Multi-pihak	Anda sekarang dapat berbagi tim persetujuan multi-pihak dengan orang lain Akun AWS atau di dalam organisasi Anda.	Juni 17, 2025
Menambahkan dukungan untuk berbagi sumber daya Amazon SageMaker AI	Anda sekarang dapat menggunakan AWS RAM untuk berbagi Aplikasi Mitra SageMaker AI Amazon dengan orang lain Akun AWS dan dengan organisasi Anda.	Juni 6, 2025
Ditambahkan dukungan untuk berbagi AWS Network Firewall sumber daya	Anda sekarang dapat menggunakan AWS RAM untuk berbagi AWS Network Firewall firewall dengan orang lain Akun AWS dan dengan organisasi Anda.	28 Mei 2025

Ditambahkan dukungan untuk berbagi AWS Systems Manager sumber daya	Anda dapat membagikan AWS Systems Manager kebijakan akses penolakan dengan orang lain Akun AWS atau organisasi Anda. AWS RAM	April 30, 2025
Ditambahkan dukungan untuk berbagi AWS CodeConnections sumber daya	Anda sekarang dapat berbagi koneksi AWS CodeConnections kode dengan orang lain Akun AWS atau di dalam organisasi Anda.	Maret 5, 2025
Ditambahkan dukungan untuk berbagi AWS Billing sumber daya	Sekarang Anda dapat berbagi AWS Billing tampilan dengan orang lain Akun AWS di organisasi Anda.	Desember 20, 2024
Menambahkan dukungan untuk berbagi konfigurasi sumber daya Amazon VPC Lattice	Anda sekarang dapat berbagi konfigurasi sumber daya Amazon VPC Lattice dengan yang lain. Akun AWS	Desember 1, 2024
Menambahkan dukungan untuk berbagi sumber daya Amazon API Gateway	Sekarang Anda dapat membagikan nama domain API Gateway dengan orang lain Akun AWS atau di dalam organisasi Anda.	November 21, 2024
Menambahkan dukungan untuk berbagi sumber daya Amazon VPC	Anda sekarang dapat berbagi grup Amazon VPC Security dengan yang lain Akun AWS atau di dalam organisasi Anda.	Oktober 30, 2024
Ditambahkan dukungan untuk berbagi AWS Olah Pesan Pengguna Akhir SMS sumber daya	Anda dapat berbagi AWS Olah Pesan Pengguna Akhir SMS sumber daya dengan orang lain Akun AWS atau organisasi Anda AWS RAM.	September 24, 2024

AWS PrivateLink	Dengan AWS PrivateLink for AWS RAM, Anda dapat terhubung langsung ke RAM dengan menggunakan endpoint antarmuka di virtual private cloud (VPC) Anda.	September 9, 2024
Ditambahkan dukungan untuk berbagi AWS Backup	Anda dapat berbagi brankas dengan udara secara logis di seluruh Akun AWS atau di dalam organisasi Anda.	Agustus 7, 2024
Menambahkan dukungan untuk berbagi sumber Elastic Load Balancing	Anda dapat berbagi toko kepercayaan Elastic Load Balancing di seluruh Akun AWS atau di dalam organisasi Anda.	Agustus 5, 2024
Ditambahkan dukungan untuk berbagi Amazon Bedrock Custom Models	Anda sekarang dapat menggunakan AWS RAM untuk berbagi model kustom Amazon Bedrock dengan yang lain Akun AWS dan dengan organisasi Anda.	Agustus 1, 2024
Ditambahkan dukungan untuk berbagi AWS CloudHSM Backup	Anda dapat berbagi AWS CloudHSM Backup dengan orang lain Akun AWS atau organisasi Anda dengan. AWS RAM	Juni 28, 2024
Menambahkan dukungan untuk berbagi Model Registry sumber daya Amazon SageMaker AI.	Anda sekarang dapat berbagi parameter lanjutan dengan aman dan efisien di seluruh Akun AWS atau di dalam organisasi Anda.	27 Juni 2024

Menambahkan dukungan untuk berbagi Amazon SageMaker AI JumpStart	Anda sekarang dapat berbagi Amazon SageMaker AI JumpStart Hubs dengan Akun AWS atau di dalam organisasi Anda.	27 Juni 2024
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
Ditambahkan 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 Akun AWS dalam organisasi Anda.	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 Akun AWS dalam organisasi Anda.	14 November 2023

Menambahkan dukungan untuk berbagi sumber daya Amazon Application Recovery Controller (ARC)	Anda sekarang dapat berbagi Amazon Application Recovery Controller (ARC) 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 SageMaker Model Card dengan orang lain Akun AWS atau organisasi Anda.	18 Agustus 2023
Menambahkan dukungan untuk grup fitur Amazon SageMaker AI Feature Store dan Katalog SageMaker AI sebagai sumber daya yang dapat dibagikan	Anda sekarang dapat berbagi grup fitur Amazon SageMaker AI Feature Store dan sumber daya Katalog SageMaker AI 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 APIs GraphQL sebagai sumber daya yang dapat dibagikan	Anda sekarang dapat berbagi AWS AppSync APIs GraphQL dengan yang lain dengan. Akun AWS 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	Memperbarui panduan untuk menyelaraskan dengan praktik terbaik IAM. Untuk informasi lebih lanjut, lihat Praktik terbaik keamanan di IAM.	Januari 3, 2023
Menambahkan dukungan untuk grup EC2 penempatan Amazon sebagai sumber daya yang dapat dibagikan	Anda sekarang dapat berbagi grup EC2 penempatan Amazon 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 saluran Amazon SageMaker AI	Anda sekarang dapat berbagi saluran SageMaker AI dengan yang lain Akun AWS.	2 Agustus 2022
Menambahkan dukungan untuk AWS Service Catalog AppRegistry aplikasi dan grup atribut sebagai tipe 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.	2 Desember 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.	2 Desember 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 sumber daya Amazon SageMaker AI	Anda dapat menggunakan AWS RAM untuk berbagi grup garis keturunan SageMaker AI. Untuk informasi selengkap nya, 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

Menambahkan dukungan untuk izin terkelola tambahan dan berbagi sumber daya dengan prinsipal IAM	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
Menambahkan dukungan untuk berbagi sumber daya AWS Systems Manager Incident Manager	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
Menambahkan dukungan untuk berbagi sumber daya Amazon Route 53	Anda sekarang dapat menggunakan AWS RAM untuk berbagi grup aturan Amazon Route 53 Resolver DNS Firewall dengan yang lain. Akun AWS	31 Maret 2021
Ditambahkan dukungan untuk berbagi AWS Transit Gateway sumber daya	Anda sekarang dapat menggunakan AWS RAM untuk berbagi domain multicast gateway transit dengan yang lain. Akun AWS	10 Desember 2020
Ditambahkan dukungan untuk berbagi AWS Network Firewall sumber daya	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
Ditambahkan dukungan untuk berbagi AWS Private Certificate Authority sumber daya	Anda sekarang dapat menggunakan AWS RAM untuk berbagi otoritas sertifikat AWS Private CA pribadi (CAs) 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 milik pelanggan IPv4	Anda sekarang dapat menggunakan AWS RAM untuk berbagi IPv4 alamat 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 EC2 Khusus Amazon, grup AWS Resource Groups sumber daya, dan komponen Amazon EC2 Image Builder, gambar, dan resep gambar dengan yang lain Akun AWS.	2 Desember 2019
Menambahkan dukungan untuk berbagi Reservasi 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.