aws

Panduan Pengguna

# Penjelajah Sumber Daya AWS

# Penjelajah Sumber Daya AWS: Panduan Pengguna

# Table of Contents

# Apakah Penjelajah Sumber Daya AWS itu?

Penjelajah Sumber Daya AWSadalah layanan pencarian dan penemuan sumber daya. Dengan Resource Explorer, Anda dapat menjelajahi sumber daya Anda, seperti instans Amazon Elastic Compute Cloud, stream Amazon Kinesis, atau tabel Amazon DynamoDB, menggunakan pengalaman seperti mesin pencari internet. Anda dapat mencari sumber daya menggunakan metadata sumber daya seperti nama, tag, dan ID. Resource Explorer bekerja Wilayah AWS di seluruh akun Anda untuk menyederhanakan beban kerja Lintas wilayah Anda.

Resource Explorer memberikan respons cepat terhadap kueri penelusuran Anda dengan menggunakan indeks yang dibuat dan dikelola oleh layanan. Penjelajah Sumber Daya AWS Resource Explorer menggunakan berbagai sumber data untuk mengumpulkan informasi tentang sumber daya di AndaAkun AWS. Resource Explorer menyimpan informasi tersebut dalam indeks untuk Resource Explorer untuk mencari.

> Kami ingin umpan balik Anda tentang dokumentasi ini
>
> Tujuan kami adalah membantu Anda mendapatkan semua yang Anda bisa dari Resource Explorer. Jika panduan ini membantu Anda melakukannya, beri tahu kami. Jika panduan ini tidak membantu Anda, maka kami ingin mendengar dari Anda sehingga kami dapat mengatasi masalah ini. Gunakan tautan Umpan Balik yang ada di sudut kanan atas setiap halaman. Itu mengirimkan komentar Anda langsung ke penulis panduan ini. Kami meninjau setiap kiriman, mencari peluang untuk meningkatkan dokumentasi. Terima kasih sebelumnya atas bantuan Anda!

Topik

# Apakah Anda pengguna Resource Explorer pertama kali?

Jika Anda pengguna pertama kali Resource Explorer, kami sarankan Anda memulai dengan membaca topik berikut di bagian Memulai:

- Syarat dan konsep untuk Resource Explorer
- Menyiapkan Resource Explorer menggunakan Pengaturan cepat

# Fitur Resource Explorer

Resource Explorer menyediakan fitur-fitur berikut:

- Pengguna dapat mencari sumber daya di Wilayah AWS atau di seluruh Wilayah di wilayah merekaAkun AWS.
- Pengguna dapat menggunakan kata kunci, operator pencarian, dan atribut seperti tag untuk memfilter hasil pencarian ke sumber daya yang hanya cocok.
- Ketika pengguna menemukan sumber daya di hasil pencarian, mereka dapat segera pergi ke konsol asli sumber daya untuk bekerja dengan sumber daya itu.
- Administrator dapat membuat tampilan yang menentukan sumber daya mana yang tersedia di hasil penelusuran. Administrator dapat membuat tampilan berbeda untuk grup pengguna yang berbeda berdasarkan tugas mereka, dan memberikan izin untuk tampilan hanya kepada pengguna yang membutuhkannya.
- Resource Explorer, seperti banyak lainnyaLayanan AWS, pada akhirnya konsisten. Resource Explorer mencapai ketersediaan tinggi dengan mereplikasi data di beberapa server dalam pusat data Amazon di seluruh dunia. Jika permintaan untuk mengubah beberapa data berhasil, perubahan tersebut akan dilakukan dan disimpan dengan aman. Namun, maka perubahan harus direplikasi di seluruh Resource Explorer, yang dapat memakan waktu. Sebagai contoh, ini termasuk Resource Explorer menemukan sumber daya di satu Wilayah, dan mereplikasi itu ke Wilayah yang berisi indeks agregator untuk akun.

# Terkait Layanan AWS

Berikut ini adalah Layanan AWS yang lain yang tujuan utamanya adalah membantu Anda mengelola AWS sumber daya Anda:

AWS Resource Access Manager (AWS RAM)

Bagikan sumber daya dalam satu Akun AWS dengan yang lainAkun AWS. Jika akun Anda dikelola olehAWS Organizations, Anda dapat menggunakannya AWS RAM untuk berbagi sumber daya dengan akun di unit organisasi, atau semua akun di organisasi. Sumber daya bersama berfungsi untuk pengguna di akun tersebut seperti yang mereka lakukan jika dibuat di akun lokal.

AWS Resource Groups

Buat grup untuk AWS sumber daya Anda. Kemudian, Anda dapat menggunakan dan mengelola setiap grup sebagai satu unit daripada harus mereferensikan setiap sumber daya secara individual. Grup Anda dapat terdiri dari sumber daya yang merupakan bagian dari AWS CloudFormation tumpukan yang sama, atau yang ditandai dengan tag yang sama. Beberapa jenis sumber daya juga mendukung penerapan konfigurasi ke grup sumber daya untuk memengaruhi semua sumber daya yang relevan dalam grup tersebut.

Tag editor dan AWS Resource Groups Tagging API

Tag adalah metadata yang ditentukan pelanggan yang dapat Anda lampirkan ke sumber daya Anda. Anda dapat mengkategorikan sumber daya Anda untuk tujuan seperti alokasi biaya dan kontrol akses berbasis atribut.

# Mengakses Resource Explorer

Anda dapat berinteraksi dengan Resource Explorer dengan cara berikut:

Konsol Resource Explorer

Resource Explorer menyediakan antarmuka pengguna berbasis web, konsol Resource Explorer. Jika mendaftarAkun AWS, Anda dapat mengakses konsol Resource Explorer dengan masuk ke AWS Management Consoledan memilih Resource Explorer dari beranda konsol.

Anda juga dapat menavigasi di browser Anda langsung ke halaman dasbor Resource Explorer, atau ke halaman pencarian Sumber Daya. Jika Anda belum masuk, Anda diminta untuk melakukannya sebelum konsol muncul.

> **Note**
>
> Konsol Resource Explorer adalah konsol global, artinya Anda tidak perlu memilih Wilayah AWS untuk bekerja. Namun, saat Anda menggunakan Resource Explorer untuk membuat indeks atau tampilan, Anda perlu menentukan Wilayah mana indeks atau tampilan

disimpan. Saat Anda menggunakan Resource Explorer untuk mencari, Anda dapat memilih tampilan apa pun yang dapat Anda akses. Hasilnya secara otomatis berasal dari Wilayah yang terkait dengan tampilan yang dipilih. Jika tampilan berasal dari Wilayah yang berisi indeks agregator, hasilnya menyertakan sumber daya dari semua Wilayah tempat Anda membuat indeks Resource Explorer.

AWS Management Consolepencarian terpadu

Di bagian atas setiap halamanAWS Management Console, ada bilah pencarian. Anda dapat mengonfigurasi Resource Explorer untuk berpartisipasi dalam pencarian terpadu. Kemudian, pengguna Anda dapat menggunakan sintaks kueri penelusuran Resource Explorer di kotak teks penelusuran terpadu, dan melihat sumber daya yang cocok di hasil penelusuran tersebut. Dengan mengaktifkan fitur ini, pengguna dapat mencari sumber daya dari konsol apa pun Layanan AWS tanpa harus terlebih dahulu beralih ke konsol Resource Explorer.

> **Important**
>
> Pencarian terpadu selalu mencari menggunakan tampilan default di Wilayah AWS yang berisi indeks agregator.

Perintah Resource Explorer di AWS CLI dan Alat untuk Windows PowerShell

The AWS CLI and Tools untuk PowerShell menyediakan akses langsung ke operasi API publik Resource Explorer. Alat-alat ini bekerja di 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 untuk Resource Explorer, lihat Referensi AWS CLIPerintah atau Referensi AWS Tools for Windows PowerShell Cmdlet.

Operasi Resource Explorer di AWS SDK

AWSmenyediakan perintah API untuk serangkaian bahasa pemrograman yang luas. Untuk informasi lebih lanjut tentang memulai, lihatMenggunakan Penjelajah Sumber Daya AWS dengan AWS SDK.

API Kueri

Jika Anda tidak menggunakan salah satu bahasa pemrograman yang didukung, Resource Explorer HTTPS Query API memberi Anda akses terprogram ke Resource Explorer. Dengan

Resource Explorer API, Anda dapat mengeluarkan permintaan HTTPS langsung ke layanan. Saat Anda menggunakan Resource Explorer API, Anda harus menyertakan kode yang dapat menandatangani permintaan secara digital menggunakan kredensil AndaAWS. Untuk informasi lebih lanjut, lihat Referensi API Penjelajah Sumber Daya AWS.

# Harga

Tidak ada biaya untuk mencari sumber daya dengan menggunakanPenjelajah Sumber Daya AWS, termasuk membuat tampilan, mengaktifkan Wilayah, atau mencari sumber daya. Dalam proses membangun inventaris sumber daya Anda, Resource Explorer memanggil API atas nama Anda yang dapat mengakibatkan biaya. Berinteraksi dengan sumber daya yang Anda temukan di hasil penelusuran dapat mengakibatkan biaya penggunaan yang bervariasi tergantung pada jenis sumber daya dan nyaLayanan AWS. Untuk informasi selengkapnya tentang cara AWS tagihan untuk penggunaan normal jenis sumber daya tertentu, lihat dokumentasi untuk layanan pemilik jenis sumber daya tersebut.

# Memulai Resource Explorer

Gunakan topik di bagian ini untuk mendapatkan pemahaman dasar tentang konsep dan istilah yang digunakan olehPenjelajah Sumber Daya AWS. Pelajari tentang prasyarat yang harus Anda penuhi untuk berhasil menggunakan Resource Explorer dan cara mengaktifkan Resource Explorer di Anda. Akun AWS

Topik

- Syarat dan konsep untuk Resource Explorer
- Prasyarat untuk menggunakan Resource Explorer
- Menyiapkan dan mengonfigurasi Resource Explorer

## Syarat dan konsep untuk Resource Explorer

Penjelajah Sumber Daya AWSadalah layanan pencarian dan penemuan sumber daya. Dengan Resource Explorer, Anda dapat menjelajahi sumber daya Anda dengan menggunakan pengalaman seperti mesin pencari internet. Anda dapat mencari sumber daya Anda, seperti instans Amazon Elastic Compute Cloud, aliran Amazon Kinesis, atau tabel Amazon DynamoDB dengan menggunakan metadata sumber daya seperti nama, tag, dan ID. Resource Explorer bekerja Wilayah AWS di seluruh akun Anda untuk menyederhanakan beban kerja Lintas wilayah Anda.

Resource Explorer memberikan respons cepat terhadap kueri penelusuran Anda dengan menggunakan indeks yang dibuat dan dikelola oleh layanan. Penjelajah Sumber Daya AWS Resource Explorer menggunakan berbagai sumber data untuk mengumpulkan informasi tentang sumber daya di AndaAkun AWS. Resource Explorer menyimpan informasi tersebut dalam indeks untuk Resource Explorer untuk mencari.

Anda harus memahami konsep-konsep berikut agar berhasil mengelola dan mengkonfigurasi Penjelajah Sumber Daya AWS untuk pengguna Anda.

Konsep

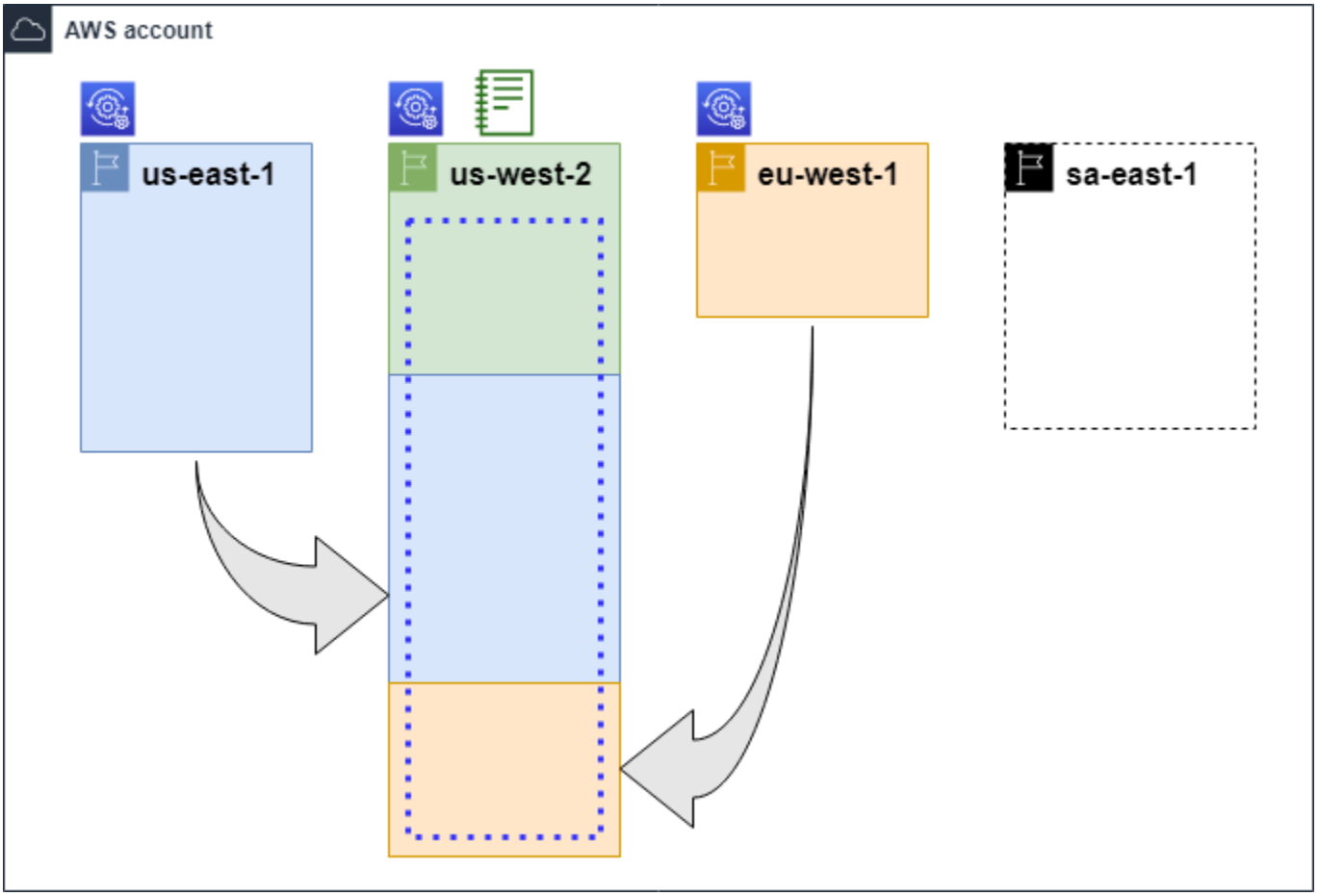
- Administrator Resource Explorer
- Pengguna Resource Explorer
- Indeks
- Lihat

- Sumber daya
- Pencarian terpadu di AWS Management Console
- Pencarian multi-akun

Diagram berikut menunjukkan tiga Wilayah AWS di mana administrator mengaktifkan Resource Explorer, dan satu Wilayah administrator memilih untuk tidak menghidupkan. Wilayah tempat Resource Explorer tidak diaktifkan tidak memiliki indeks. Oleh karena itu, sumber dayanya tidak dapat dicari oleh kueri Resource Explorer.

Dalam skenario contoh ini, administrator memilih Wilayah AS Barat (Oregon) (`us-west-2`) untuk memuat indeks agregator untuk akun tersebut. Semua Wilayah yang Anda aktifkan mereplikasi indeks lokal mereka ke Region dengan indeks agregator.

Tampilan default yang dibuat oleh Resource Explorer tidak memiliki filter apa pun. Oleh karena itu, hasil dari pencarian dengan tampilan ini dapat mencakup sumber daya dari jenis apa pun di semua Wilayah di akun tempat Resource Explorer dihidupkan.



| Legenda | |
|---|---|
|  | Resource Explorer diaktifkan dalam hal ini Wilayah AWS dan informasi tentang sumber daya Wilayah disimpan dalam indeks lokal di Wilayah tersebut. Setiap indeks lokal Wilayah juga direplikasi (ditunjukkan oleh panah) ke Wilayah yang berisi indeks agregator. |
|  | Indeks dalam hal ini Wilayah AWS dikonfigurasi menjadi indeks agregator untuk akun. Resource Explorer mereplikasi informasi sumber daya yang dikumpulkan dalam indeks lokal semua Wilayah lain di mana Resource Explorer diaktifkan menjadi indeks agregator di Wilayah ini. Pencarian yang dilakukan di Wilayah ini dapat mencakup hasil dari semua Wilayah di akun. |
|  | Tampilan default yang dibuat oleh Quick Setup mencakup semua sumber daya di semuaWilayah AWS. |

## Administrator Resource Explorer

Administrator Resource Explorer adalah kepala sekolah AWS Identity and Access Management (IAM) yang memiliki izin untuk mengelola Resource Explorer dan pengaturannya di Akun AWS . Administrator Resource Explorer dapat mengonfigurasi fitur-fitur berikut:

- Aktifkan Resource Explorer untuk individu Wilayah AWS Akun AWS dengan membuat indeks di Wilayah tersebut. Ini memungkinkan Resource Explorer menemukan sumber daya dan mengisi indeks dengan informasi tentang sumber daya tersebut sehingga pengguna dapat mencari sumber daya di Wilayah tersebut.
- Perbarui jenis indeks Wilayah AWS menjadi satu untuk menjadikannya indeks agregator untuknya. Akun AWS Indeks agregator di Wilayah ini menerima salinan informasi sumber daya yang direplikasi dari semua Wilayah lain di akun tempat Resource Explorer diaktifkan.
- Buat tampilan yang menentukan subset informasi yang diindeks pengguna dapat mencari dan menemukan di Resource Explorer.
- Meskipun bukan bagian dari tindakan Resource Explorer, administrator Resource Explorer juga harus dapat memberikan izin pencarian ke kepala sekolah di akun. Administrator dapat memberikan izin ini kepada prinsipal dengan menambahkan izin yang relevan ke kebijakan izin IAM yang ada, atau dengan menggunakan kebijakan terkelola baca Resource Explorer. AWS

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

- Pengguna dan grup di AWS IAM Identity Center:

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

- Pengguna yang dikelola di IAM melalui penyedia identitas:

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

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

Administrator biasanya memiliki semua izin Resource Explorer (`resource-explorer-2:*`) pada semua sumber daya Resource Explorer, termasuk indeks dan tampilan. Izin ini dapat diberikan dengan menggunakan kebijakan AWS terkelola akses penuh Resource Explorer.

## Pengguna Resource Explorer

Pengguna Resource Explorer adalah prinsipal IAM yang memiliki izin untuk melakukan satu atau beberapa tugas berikut:

- Lakukan pencarian sumber daya dengan menggunakan tampilan untuk menanyakan Resource Explorer. Pengguna Resource Explorer ingin menemukan dan menemukan AWS sumber daya dan biasanya menggunakan konsol Resource Explorer, atau `Search` operasi Resource Explorer yang disediakan oleh AWS SDK atau. AWS CLI

  Peran atau pengguna dapat menggunakan IAM mendapatkan izin untuk mencari dengan salah satu dari dua metode:

  - Resource Explorer hanya membaca kebijakan AWS terkelola untuk peran, grup, atau pengguna IAM.
  - Kebijakan izin IAM dengan pernyataan yang berisi izin minimum berikut untuk peran, grup, atau pengguna IAM.

```
{
    "Effect": "Allow",
    "Action": [
        "resource-explorer-2:Search",
        "resource-explorer-2:GetView",
    "Resource": "<ARN of the view>"
}
```

- Meskipun biasanya dianggap sebagai tugas administrator, Anda dapat mendelegasikan kepada pengguna tepercaya kemampuan untuk menentukan tampilan buat. Untuk melakukan ini, administrator dapat memberikan izin untuk memanggil `resource-explorer-2:CreateView` operasi dalam kebijakan izin IAM yang dilampirkan pada peran, grup, atau pengguna yang relevan. Jika tampilan memerlukan izin khusus, maka ketentuan untuk menambahkan atau memodifikasi kebijakan IAM untuk pengguna yang relevan harus dibuat.

Untuk informasi tentang cara mencari sumber daya menggunakan Resource Explorer, lihatMenggunakanPenjelajah Sumber Daya AWSuntuk mencari sumber daya.

## Indeks

Indeks adalah kumpulan informasi yang dikelola oleh Resource Explorer tentang semua AWS sumber daya Wilayah AWS di salah satu sumber daya AndaAkun AWS. Resource Explorer mempertahankan indeks di setiap Wilayah tempat Anda mengaktifkan Resource Explorer. Resource Explorer memperbarui indeks secara otomatis saat Anda membuat dan menghapus sumber daya diAkun AWS. Pada diagram sebelumnya, kotak di bawah Wilayah AWS nama mewakili indeks Resource Explorer yang dipertahankan di masing-masingWilayah AWS. Indeks di Wilayah adalah sumber informasi untuk setiap tampilan yang dibuat di Wilayah tersebut. Pengguna tidak dapat langsung menanyakan indeks. Sebagai gantinya, mereka harus selalu melakukan kueri menggunakan tampilan.

Ada dua jenis indeks:

Indeks lokal

Ada satu indeks lokal Wilayah AWS di setiap tempat Anda mengaktifkan Resource Explorer. Indeks lokal hanya berisi informasi tentang sumber daya di Wilayah yang sama.

Indeks agregator

Administrator Resource Explorer juga dapat menunjuk indeks dalam satu Wilayah AWS untuk menjadi indeks agregator untuk. Akun AWS Indeks agregator menerima dan menyimpan salinan indeks untuk setiap Wilayah lain di mana Resource Explorer diaktifkan di akun. Indeks agregator juga menerima dan menyimpan informasi tentang sumber daya di Wilayahnya sendiri. Pada diagram sebelumnya, Region `us-west-2` berisi indeks agregator untuk akun tersebut. Alasan utama untuk menunjuk indeks agregator untuk akun adalah agar Anda dapat membuat tampilan yang dapat menyertakan sumber daya dari semua Wilayah di akun. Hanya ada satu indeks agregator dalam sebuahAkun AWS.

Saat Anda mengaktifkan Resource Explorer, Anda dapat menentukan Wilayah AWS mana yang berisi indeks agregator. Anda juga dapat mengubah yang Wilayah AWS digunakan untuk indeks agregator nanti. Untuk informasi tentang cara mempromosikan indeks lokal untuk menjadikannya indeks agregatorAkun AWS, lihatMengaktifkan pencarian lintas wilayah dengan membuat indeks agregator.

Indeks adalah sumber daya dengan nama sumber daya Amazon (ARN). Namun, Anda dapat menggunakan ARN ini hanya dalam kebijakan izin untuk memberikan akses ke operasi yang berinteraksi langsung dengan indeks. Dengan operasi tersebut, Anda dapat membuat tampilan dan mengaturnya sebagai default di Wilayah, mengaktifkan atau menonaktifkan Resource Explorer di Wilayah, dan membuat indeks agregator untuk akun. ARN indeks terlihat mirip dengan contoh berikut:

```
arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-
abcd11111111
```

## Lihat

Tampilan adalah mekanisme yang digunakan untuk menanyakan sumber daya yang tercantum dalam indeks. Tampilan mendefinisikan informasi apa dalam indeks yang terlihat dan tersedia untuk tujuan pencarian dan penemuan. Pengguna tidak pernah secara langsung menanyakan indeks Resource Explorer. Sebagai gantinya, kueri harus selalu melalui tampilan yang memungkinkan pembuat tampilan membatasi sumber daya mana yang dapat dilihat pengguna di hasil penelusuran.

Saat membuat tampilan, Anda menentukan filter yang membatasi sumber daya mana yang disertakan dalam hasil penelusuran. Misalnya, Anda dapat memilih untuk menyertakan hanya sumber daya dari beberapa jenis sumber daya tertentu yang digunakan oleh mereka yang Anda berikan akses ke tampilan ini. Hasil dari kueri yang dibuat pengguna dengan tampilan selalu difilter secara otomatis untuk menyertakan hanya sumber daya yang sesuai dengan kriteria tampilan.

Untuk memberikan akses untuk menggunakan tampilan, Anda dapat menggunakan izin menetapkan menggunakan salah satu metode berikut.

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

- Pengguna dan grup di AWS IAM Identity Center:

  Buat set izin. Ikuti instruksi di Buat set izin di Panduan Pengguna AWS IAM Identity Center.
- Pengguna yang dikelola di IAM melalui penyedia identitas:

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

Berikan izin untuk mengizinkan peran, grup, atau pengguna Anda memanggil `resource-explorer-2:GetView` dan `resource-explorer-2:Search` operasi pada tampilan yang diidentifikasi dengan nama sumber daya Amazon (ARN). Atau, Anda dapat menggunakan kebijakan AWS terkelola baca saja Resource Explorer untuk semua kepala sekolah yang perlu menggunakan tampilan untuk mencari. Anda dapat membuat beberapa tampilan yang memiliki filter dan cakupan yang berbeda dan dengan demikian mengembalikan subset yang berbeda dari informasi sumber daya Anda. Kemudian, Anda dapat memberikan izin untuk setiap tampilan kepada pengguna yang perlu melihat informasi yang disertakan oleh hasil tampilan tersebut.

Untuk mencari dengan Resource Explorer, setiap pengguna harus memiliki izin untuk menggunakan setidaknya satu tampilan. Anda tidak dapat melakukan pencarian di Resource Explorer tanpa menggunakan tampilan.

Tampilan disimpan berdasarkan per wilayah. Tampilan hanya dapat mengakses indeks Resource Explorer di dalamnyaWilayah AWS. Untuk mengakses hasil penelusuran seluruh akun, Anda harus menggunakan tampilan di Wilayah yang berisi indeks agregator untuk akun tersebut. Opsi pengaturan Cepat membuat tampilan default di Wilayah AWS dengan indeks agregator dan dengan filter yang mencakup semua sumber daya di semua yang Wilayah AWS digunakan oleh akun.

Untuk informasi tentang cara membuat tampilan, lihatMengelola tampilan Resource Explorer untuk menyediakan akses ke penelusuran. Untuk informasi tentang cara menggunakan tampilan dalam kueri, lihatMenggunakanPenjelajah Sumber Daya AWSuntuk mencari sumber daya.

Setiap tampilan memiliki nama sumber daya Amazon (ARN) yang dapat Anda rujuk dalam kebijakan izin untuk memberikan akses ke tampilan individual. Anda juga dapat meneruskan ARN tampilan sebagai parameter ke API atau AWS CLI operasi apa pun yang berinteraksi dengan tampilan. ARN tampilan terlihat mirip dengan contoh berikut.

```
arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-View-
Name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

> **Note**
>
> Setiap tampilan ARN menyertakan UUID yang AWS dihasilkan di akhir. Ini membantu memastikan bahwa pengguna yang mungkin memiliki akses ke tampilan dengan nama tertentu yang dihapus tidak dapat secara otomatis mengakses tampilan baru yang dibuat dengan nama yang sama.

## Sumber daya

Sumber daya adalah entitas di AWS mana Anda dapat bekerja dengan. Sumber daya dibuat oleh Layanan AWS saat Anda menggunakan fitur layanan. Contohnya termasuk instans Amazon EC2, bucket Amazon S3, atau tumpukan. AWS CloudFormation Beberapa jenis sumber daya dapat berisi data pelanggan. Semua jenis sumber daya memiliki atribut atau metadata untuk mendeskripsikan sumber daya, termasuk nama, deskripsi, dan nama sumber daya Amazon (ARN) yang Anda gunakan untuk mereferensikan sumber daya secara unik. Sebagian besar jenis sumber daya juga mendukung tag. Tag adalah metadata khusus yang dapat Anda lampirkan ke sumber daya Anda untuk berbagai tujuan, seperti alokasi biaya dalam penagihan Anda, otorisasi keamanan menggunakan kontrol akses berbasis atribut, atau untuk mendukung kebutuhan kategorisasi Anda yang lain.

Tujuan utama Resource Explorer adalah untuk membantu Anda menemukan sumber daya yang ada di AndaAkun AWS. Resource Explorer menggunakan berbagai teknik untuk menemukan semua sumber daya Anda dan menempatkan informasi tentang mereka dalam indeks. Kemudian, Anda dapat menanyakan indeks melalui tampilan apa pun yang disediakan administrator untuk Anda.

**Important**

Resource Explorer secara sengaja mengecualikan jenis sumber daya yang penyertaannya akan mengekspos data pelanggan. Jenis sumber daya berikut tidak diindeks oleh Resource Explorer dan oleh karena itu tidak pernah dikembalikan dalam hasil pencarian.

- Objek Amazon S3 yang terkandung dalam ember
- Item tabel Amazon DynamoDB
- Nilai atribut DynamoDB

## Pencarian terpadu di AWS Management Console

Di bagian atasAWS Management Console, di setiapLayanan AWS, ada bilah pencarian yang dapat Anda gunakan untuk mencari berbagai hal AWS terkait. Anda dapat mencari layanan dan fitur, dan mendapatkan tautan langsung ke halaman yang relevan di konsol layanan tersebut. Anda juga dapat mencari dokumentasi dan artikel blog yang terkait dengan istilah pencarian Anda.

Setelah Anda mengaktifkan Resource Explorer dan membuat indeks agregator dan tampilan default, pencarian terpadu juga dapat menyertakan sumber daya akun Anda dalam hasil penelusuran. Pencarian terpadu secara otomatis menggunakan tampilan default di Wilayah AWS yang berisi indeks agregator untuk akun. Ini memungkinkan Anda mencari sumber daya dari halaman mana pun diAWS Management Console, tanpa harus terlebih dahulu membuka Resource Explorer. Jika Anda tidak mempromosikan indeks lokal menjadi indeks agregator untuk akun, atau jika Anda tidak membuat tampilan default di Wilayah indeks agregator, pencarian terpadu tidak menyertakan sumber daya dalam hasil penelusurannya. Selain itu, setiap prinsipal yang melakukan pencarian harus memiliki izin untuk menggunakan tampilan default di Wilayah yang berisi indeks agregator atau pencarian terpadu tidak menyertakan sumber daya dalam hasil pencariannya.

**Important**

Pencarian terpadu secara otomatis menyisipkan operator karakter wildcard (*) di akhir kata kunci pertama dalam string. Ini berarti bahwa hasil pencarian terpadu menyertakan sumber daya yang cocok dengan string apa pun yang dimulai dengan kata kunci yang ditentukan. Pencarian yang dilakukan oleh kotak teks Kueri pada halaman pencarian Sumber daya di konsol Resource Explorer tidak secara otomatis menambahkan karakter wildcard. Anda dapat memasukkan secara * manual setelah istilah apa pun dalam string pencarian.

Untuk informasi selengkapnya tentang pencarian terpadu dan integrasinya dengan Resource Explorer, lihatMenggunakan pencarian terpadu di AWS Management Console.

## Pencarian multi-akun

Dengan pencarian multi-akun, Anda dapat mencari dan menemukan sumber daya di seluruh AWS Organizations dan Wilayah AWS dengan pencarian kata kunci tunggal.

Untuk informasi selengkapnya tentang penelusuran multi-akun dan cara mengaktifkannya untuk Resource Explorer, lihatMengaktifkan pencarian multi-akun.

# Prasyarat untuk menggunakan Resource Explorer

Sebelum Anda menggunakan Penjelajah Sumber Daya AWS untuk pertama kalinya, selesaikan tugas-tugas berikut sesuai kebutuhan.

Tugas

- Mendaftar untuk Akun AWS
- Buat pengguna dengan akses administratif

## Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/signup.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan mengunjungi https://aws.amazon.com/ dan memilih Akun Saya.

## Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Pengguna root akun AWS

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

   Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.
2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .
2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuknya, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.
2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

# Menyiapkan dan mengonfigurasi Resource Explorer

Sebelum Anda dapat mengatur dan mengkonfigurasi Penjelajah Sumber Daya AWS, pertama-tama pastikan bahwa Anda memenuhi prasyarat. Setelah itu, masuk sebagai peran IAM atau pengguna yang memiliki izin yang diperlukan untuk melakukan operasi Resource Explorer untuk prosedur berikut.

Anda dapat menggunakan prosedur pengaturan dan konfigurasi ini untuk menyiapkan Resource Explorer di akun yang ada, dan di akun baru apa pun yang ditambahkan ke organisasi Anda.

Ada dua cara untuk mengatur Resource Explorer:

- Pengaturan cepat
- Pengaturan lanjutan

> **Important**
>
> Jika Anda memilih untuk mengatur Resource Explorer menggunakan opsi apa pun yang mengatakan Wilayah AWS “semua “, Wilayah AWS itu hanya mengaktifkan yang ada dan yang diaktifkan Akun AWS pada saat Anda melakukan prosedur. Resource Explorer tidak secara otomatis menyala di semua Wilayah AWS yang AWS menambahkan di masa depan. Saat AWS memperkenalkan Region baru, Anda dapat memilih untuk mengaktifkan Resource

Explorer di Region secara manual saat muncul di halaman Pengaturan konsol Resource Explorer, atau dengan memanggil CreateIndexoperasi.

> **Note**
>
> Menyiapkan Resource Explorer juga dapat mengaktifkan kemampuan untuk mencari sumber daya dengan menggunakan bilah pencarian terpadu di AWS Management Console. Agar pengguna dapat melihat sumber daya dalam hasil penelusuran terpadu, Anda harus mengonfigurasi Resource Explorer dengan indeks agregator lintas wilayah dan tampilan default. Untuk detailnya, lihat prosedur berikut. Anda juga harus memastikan bahwa pengguna pencarian Anda memiliki izin untuk menggunakan tampilan default di Wilayah AWS yang berisi indeks agregator. Untuk informasi selengkapnya, lihat Menggunakan pencarian terpadu di AWS Management Console.

## Menyiapkan Resource Explorer menggunakan Pengaturan cepat

Jika Anda memilih opsi Pengaturan cepat, Resource Explorer melakukan hal berikut:

- Membuat indeks di setiap Wilayah AWS di Anda Akun AWS.
- Memperbarui indeks di Wilayah yang Anda tentukan sebagai indeks agregator untuk akun tersebut.
- Membuat tampilan default di Region indeks agregator. Tampilan ini tidak memiliki filter sehingga mengembalikan semua sumber daya yang ditemukan dalam indeks.

Izin minimum

Untuk melakukan langkah-langkah dalam prosedur berikut, Anda harus memiliki izin berikut:

- Tindakan: `resource-explorer-2:*` — Sumber daya: tidak ada sumber daya tertentu (`*`)
- Tindakan: `iam:CreateServiceLinkedRole` — Sumber daya: tidak ada sumber daya tertentu (`*`)

AWS Management Console

Untuk mengatur Resource Explorer menggunakan Penyiapan cepat

1. Buka Penjelajah Sumber Daya AWS konsol dihttps://console.aws.amazon.com/resource-explorer.
2. Pilih Aktifkan Resource Explorer.
3. Pada halaman Aktifkan Resource Explorer, pilih Pengaturan cepat.
4. Pilih yang Wilayah AWS Anda inginkan untuk memuat indeks agregator. Anda harus memilih Wilayah yang sesuai untuk lokasi geografis untuk pengguna Anda.
5. Di bagian bawah halaman, pilih Aktifkan Resource Explorer.
6. Pada halaman Progress, Anda dapat memantau masing-masing Wilayah AWS saat Resource Explorer membuat indeksnya. Halaman menampilkan status pembuatan indeks agregator dan membuat tampilan default.

Setelah semua langkah menunjukkan bahwa mereka berhasil diselesaikan, Anda dan pengguna Anda dapat menavigasi ke halaman pencarian Sumber Daya dan mulai mencari sumber daya.

> **Note**
>
> Sumber daya yang ditandai lokal ke indeks muncul di hasil pencarian dalam beberapa menit. Sumber daya yang tidak ditandai biasanya membutuhkan waktu kurang dari dua jam untuk muncul, tetapi dapat memakan waktu lebih lama ketika ada permintaan yang besar. Ini juga dapat memakan waktu hingga satu jam untuk menyelesaikan replikasi awal ke indeks agregator baru dari semua indeks lokal yang ada.

Langkah selanjutnya: Sebelum pengguna Anda dapat mencari dengan tampilan default yang baru saja Anda buat, Anda harus memberi mereka izin untuk mencarinya. Untuk informasi selengkapnya, lihat Memberikan akses ke tampilan Resource Explorer untuk pencarian.

AWS CLI

Menyiapkan Resource Explorer di Anda Akun AWS dengan menggunakan AWS CLI is, menurut definisi, setara dengan opsi Pengaturan lanjutan. Ini karena operasi CLI Resource Explorer tidak melakukan langkah apa pun untuk Anda secara otomatis seperti yang dilakukan konsol Resource Explorer. Lihat AWS CLI tab di Menyiapkan Resource Explorer menggunakan Pengaturan lanjutan untuk melihat perintah apa yang setara dengan menggunakan konsol.

# Menyiapkan Resource Explorer menggunakan Pengaturan lanjutan

Jika Anda memilih opsi Pengaturan lanjutan, Anda dapat melakukan hal berikut:

- Pilih Wilayah AWS tempat untuk mengaktifkan Resource Explorer.
- Pilih apakah akan mengonfigurasi satu Wilayah dengan indeks agregator. Jika Anda melakukannya, Anda menentukan Wilayah AWS untuk menempatkannya. Indeks ini memungkinkan Anda membuat tampilan yang dapat menyertakan sumber daya dari semua Wilayah di akun. Untuk informasi selengkapnya, lihat Mengaktifkan pencarian lintas wilayah dengan membuat indeks agregator.
- Pilih apakah akan membuat tampilan default. Tampilan itu memungkinkan pencarian secara otomatis untuk AWS sumber daya apa pun di Wilayah tempat Anda mengaktifkan Resource Explorer. Anda harus memastikan bahwa setiap prinsipal yang perlu menggunakan tampilan default untuk mencari di Resource Explorer memiliki izin pada tampilan. Untuk informasi selengkapnya, lihat Memberikan akses ke tampilan Resource Explorer untuk pencarian.

> **Note**
>
> Anda dapat mengonfigurasi Resource Explorer untuk menyertakan sumber daya Anda dalam hasil penelusuran yang disediakan oleh fitur pencarian terpadu di AWS Management Console. Untuk mengaktifkan fitur ini, Anda harus mengonfigurasi Resource Explorer dengan indeks agregator dan tampilan default yang dapat dicari oleh semua peran dan pengguna. Opsi pengaturan Cepat membuat indeks agregator dan tampilan default dan merupakan cara kami menyarankan Anda mengaktifkan Resource Explorer.

Izin minimum

Untuk melakukan langkah-langkah dalam prosedur berikut, Anda harus memiliki izin berikut:

- Tindakan: `resource-explorer-2:*` — Sumber daya: tidak ada sumber daya tertentu (*)
- Tindakan: `iam:CreateServiceLinkedRole` — Sumber daya: tidak ada sumber daya tertentu (*)

AWS Management Console

Untuk mengaktifkan Resource Explorer menggunakan Pengaturan lanjutan

1. Buka Penjelajah Sumber Daya AWS konsol dihttps://console.aws.amazon.com/resource-explorer.
2. Pilih Aktifkan Resource Explorer.
3. Pada halaman Aktifkan Resource Explorer, pilih Pengaturan lanjutan.
4. Di Wilayah AWSkotak, di bawah Wilayah, pilih apakah Anda ingin mengaktifkan Resource Explorer di semua Wilayah AWS, atau hanya Wilayah tertentu.

   Jika Anda memilih Aktifkan Resource Explorer hanya dalam yang ditentukan Wilayah AWS dalam akun ini, pilih setiap Wilayah yang sumber dayanya ingin Anda sertakan dalam hasil penelusuran.
5. Untuk indeks Aggregator, pilih apakah Anda ingin membuat indeks agregator. Jika Anda memilih untuk membuat indeks agregator, semua lainnya Wilayah AWS mereplikasi indeksnya ke Wilayah ini. Ini memungkinkan pengguna mencari sumber daya di semua Wilayah yang dipilih di Akun AWS. Pilih Wilayah AWS yang berisi indeks agregator. Kami menyarankan Anda menentukan Wilayah tempat pengguna Anda menghabiskan sebagian besar waktunya, atau setidaknya di tempat yang Anda harapkan untuk melakukan sebagian besar pencarian sumber daya mereka.
6. Di kotak tampilan Default, di bawah Pembuatan tampilan, pilih apakah akan membuat tampilan default. Opsi ini hanya tersedia jika Anda memilih untuk membuat indeks agregator. Jika Anda memilih untuk membuat tampilan default, Resource Explorer menempatkan tampilan ini Wilayah AWS sama dengan indeks agregator. Ini memungkinkan tampilan default menyertakan hasil dari semua Wilayah AWS tempat Anda mendaftarkan Resource Explorer. Setiap kali pengguna melakukan pencarian di Wilayah dengan tampilan default dan tidak secara eksplisit menentukan tampilan, pencarian menggunakan tampilan default untuk Wilayah tersebut.

   > **Note**
   >
   > Sebelum pengguna dapat mencari dengan tampilan, Anda harus memberi mereka izin untuk menggunakan tampilan itu. Untuk informasi selengkapnya, lihat Memberikan akses ke tampilan Resource Explorer untuk pencarian.
7. Pilih Aktifkan Penjelajah Sumber Daya.

> **Note**
>
> Sumber daya yang ditandai lokal ke indeks muncul di hasil pencarian dalam beberapa menit. Sumber daya yang tidak ditandai biasanya membutuhkan waktu kurang dari dua jam untuk muncul, tetapi dapat memakan waktu lebih lama ketika ada permintaan yang besar. Ini juga dapat memakan waktu hingga satu jam untuk menyelesaikan replikasi awal ke indeks agregator baru dari semua indeks lokal yang ada.

AWS CLI

Untuk mengatur Resource Explorer menggunakan Pengaturan lanjutan

Konsol Resource Explorer melakukan banyak panggilan operasi API atas nama Anda berdasarkan pilihan yang Anda buat. Contoh AWS CLI perintah berikut menggambarkan cara melakukan prosedur dasar yang sama di luar konsol menggunakan. AWS CLI

Example Langkah 1: Aktifkan Resource Explorer dengan membuat indeks yang diinginkan Wilayah AWS

Jalankan perintah berikut Wilayah AWS di masing-masing tempat Anda ingin mengaktifkan Resource Explorer. Contoh perintah berikut mengaktifkan Resource Explorer di Wilayah AWS yang merupakan default untuk file AWS CLI.

```
$ aws resource-explorer-2 create-index
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-27T16:17:12.130000+00:00",
    "State": "CREATING"
}
```

Example Langkah 2: Perbarui indeks menjadi satu Wilayah AWS untuk menjadi indeks agregator untuk akun

Jalankan perintah berikut Wilayah AWS di mana Anda ingin Resource Explorer memperbarui indeks lokal ke indeks agregator untuk akun. Contoh perintah berikut memperbarui indeks agregator di Timur AS (Virginia N.) (`us-east-1`).

```
$ aws resource-explorer-2 update-index-type \
    --arn arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --type AGGREGATOR
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "LastUpdatedAt": "2022-07-27T16:29:49.231000+00:00",
    "State": "UPDATING",
    "Type": "AGGREGATOR"
}
```

Example Langkah 3: Buat tampilan di Wilayah AWS yang berisi indeks agregator

Jalankan perintah berikut Wilayah AWS di mana Anda membuat indeks agregator. Perintah contoh berikut membuat tampilan identik dengan yang dibuat oleh proses penyiapan konsol Resource Explorer. Tampilan baru ini mencakup tag yang dilampirkan ke sumber daya sebagai bagian dari informasi yang diindeks dan mendukung pencarian sumber daya berdasarkan kunci tag atau nilai.

```
$ aws resource-explorer-2 create-view \
    --view-name My-New-View \
    --included-properties Name=tags
{
    "View": {
        "Filters": {
            "FilterString": ""
        },
        "IncludedProperties": [
            {
                "Name": "tags"
            }
        ],
        "LastUpdatedAt": "2022-07-27T16:34:14.960000+00:00",
        "Owner": "123456789012",
        "Scope": "arn:aws:iam::123456789012:root",
        "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-New-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222"
    }
}
```

Example Langkah 4: Tetapkan tampilan baru Anda sebagai default untuk Wilayah AWS

Contoh berikut menetapkan tampilan yang Anda buat pada langkah sebelumnya sebagai default untuk Wilayah. Anda harus menjalankan perintah berikut di tempat yang sama Wilayah AWS di mana Anda membuat tampilan default.

```
$ aws resource-explorer-2 associate-default-view \
    --view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-New-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
{
    "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-New-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
}
```

Sebelum pengguna dapat mencari dengan tampilan, Anda harus memberi mereka izin untuk menggunakan tampilan itu. Untuk informasi selengkapnya, lihat Memberikan akses ke tampilan Resource Explorer untuk pencarian.

Setelah Anda menjalankan perintah tersebut, Resource Explorer berjalan di Wilayah yang ditentukan di bagian Anda Akun AWS. Resource Explorer membangun dan memelihara indeks di setiap Wilayah dengan rincian sumber daya yang ada di sana. Resource Explorer mereplikasi setiap indeks Wilayah individual ke indeks agregator di Wilayah yang ditentukan. Wilayah itu juga berisi tampilan yang memungkinkan peran IAM atau pengguna apa pun di akun untuk mencari sumber daya di semua Wilayah yang diindeks.

> **Note**
>
> Sumber daya yang ditandai lokal ke indeks muncul di hasil pencarian dalam beberapa menit. Sumber daya yang tidak ditandai biasanya membutuhkan waktu kurang dari dua jam untuk muncul, tetapi dapat memakan waktu lebih lama ketika ada permintaan yang besar. Ini juga dapat memakan waktu hingga satu jam untuk menyelesaikan replikasi awal ke indeks agregator baru dari semua indeks lokal yang ada.

# Mengelola Resource Explorer untuk mendukung pencarian sumber daya

Setelah Anda pertama kali mengaktifkan setidaknya satu Wilayah AWS di AndaAkun AWS, ada tugas administratif yang mungkin perlu Anda lakukan sesekali. Penjelajah Sumber Daya AWS Bagian ini menjelaskan tugas pemeliharaan dan konfigurasi yang membantu Anda membuat Resource Explorer bekerja seperti yang Anda inginkan saat penggunaan Akun AWS dan sumber daya Anda berkembang.

Topik



## Memeriksa yang manaWilayah AWSmengaktifkan Resource Explorer

Anda bisa mencari tahu yang manaWilayah AWSmemilikiPenjelajah Sumber Daya AWSdiaktifkan dengan memeriksa Wilayah mana yang berisi indeks untuk Resource Explorer. Untuk melihat Wilayah mana yang memiliki indeks, gunakan prosedur di halaman ini.

> **Important**
>
> Pengguna dapat mencari sumber daya dicumaWilayah yang memiliki Resource Explorer diaktifkan. Anda juga dapat membuat indeks agregator di satu Wilayah untuk mendukung

pencarian sumber daya di semua Wilayah Anda. Resource Explorer mereplikasi informasi sumber daya ke Wilayah dengan indeks agregator dari semua Wilayah lain yang berisi indeks Resource Explorer. Pengguna tidak dapat menggunakan Resource Explorer untuk menemukan sumber daya di Wilayah yang tidak memiliki indeks.

## Memeriksa status Resource Explorer di Wilayah

Anda dapat memeriksa Wilayah mana yang memiliki indeks untuk Resource Explorer dengan menggunakanAWS Management Console, dengan menggunakan perintah diAWS Command Line Interface(AWS CLI), atau dengan menggunakan operasi API dalamAWSSDK.

AWS Management Console

Untuk memeriksa Wilayah mana yang memiliki indeks untuk Resource Explorer

1. BukaPengaturanhalaman di konsol Resource Explorer.
2. Daftar diIndeksbagian hanya mencakup Wilayah yang berisi indeks Resource Explorer. Nilai dalamJeniskolom menunjukkan apakah indeks adalahLokalindeks untuk Wilayahnya, atauAgregatorindeks untukAkun AWS.
3. Untuk melihat Wilayah mana yang tidak berisi Resource Explorer, pilihBuat indeks. Jika Region tidak ada, maka Region tidak mengandung Resource Explorer.

AWS CLI

Untuk memeriksa Wilayah mana yang memiliki indeks untuk Resource Explorer

Jalankan perintah berikut untuk melihat manaWilayah AWSmemiliki indeks untuk Resource Explorer.

```
$ aws resource-explorer-2 list-indexes
{
    "Indexes": [
        {
            "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
            "Region": "us-east-1",
            "Type": "AGGREGATOR"
        },
```

```
        {
            "Arn": "arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222",
            "Region":"us-west-2",
            "Type":"LOCAL"
        }
    ]
}
```

# Mengaktifkan pencarian multi-akun

Dengan pencarian multi-akun, Anda dapat mencari sumber daya di seluruh akun dengan indeks aktif di unit organisasi AWS Organizations atau organisasi (OU) Anda.

Topik

- Prasyarat
- Aktifkan pencarian multi-akun
- Pengaturan Cepat Multi-Akun

## Prasyarat

Untuk mengaktifkan pencarian multi-akun untuk organisasi Anda, lengkapi yang berikut ini:

- Untuk Wilayah keikutsertaan, verifikasi akun manajemen Anda juga ikut serta di mana Anda mengaktifkan pencarian multi-akun.
- Buat pengguna administratif.
- Buat peran terkait layanan di akun administrator dengan. `aws iam create-service-linked-role --aws-service-name resource-explorer-2.amazonaws.com`
- Aktifkan akses tepercaya di AWS Organizations. Ini memungkinkan integrasi penuh dengan Resource Explorer untuk mencantumkan sumber daya di semua akun di organisasi Anda.
- Tetapkan administrator yang didelegasikan (disarankan). Untuk informasi selengkapnya, lihat Administrator yang didelegasikan untuk AWS layanan yang berfungsi dengan Organizations dalam Panduan AWS Organizations Pengguna.
  - Resource Explorer hanya mendukung 1 administrator yang didelegasikan yang melakukan tindakan serupa ke akun manajemen.

- Menghapus atau mengubah administrator yang didelegasikan untuk organisasi Anda menghasilkan penghapusan semua tampilan multi-akun yang dibuat di akun mereka.

## Aktifkan pencarian multi-akun

Untuk mencari dan menemukan sumber daya di seluruh akun organisasi, Anda harus menyelesaikan langkah-langkah berikut:

1. Aktifkan Penjelajah Sumber Daya AWS di satu atau beberapa akun di akun Anda AWS Organizations.
2. Daftarkan satu Wilayah untuk memuat indeks agregator.
3. Pilih Wilayah untuk membuat indeks agregator. Wilayah ini harus konsisten di seluruh wilayah Anda AWS Organizations.
4. Buat tampilan Resource Explorer yang tercakup ke unit Anda AWS Organizations atau organisasi. Buat tampilan ini di Wilayah agregator dari langkah sebelumnya.
5. Bagikan tampilan dengan akun di seluruh organisasi Anda.

## Pengaturan Cepat Multi-Akun

Aktifkan Resource Explorer di beberapa akun di organisasi Anda dengan Pengaturan Cepat.

> **Note**
>
> Proses ini tidak menyebarkan sumber daya apa pun di akun manajemen. Jika Anda menggunakan akun manajemen dan ingin indeks di akun, Anda harus menambahkannya secara manual dengan alur orientasi Resource Explorer.

1. Arahkan ke Pengaturan Cepat untuk Resource Explorer di konsol Systems Manager.
2. Pilih Wilayah indeks Aggregator Anda. Ini memungkinkan Anda untuk mencari sumber daya yang terletak di semua Wilayah di akun target yang dipilih. Jika salah satu akun target yang dipilih sudah memiliki indeks agregator yang dikonfigurasi di Wilayah lain, indeks agregator yang ada akan secara otomatis diganti dengan Wilayah baru ini.
3. Pilih Target akun Anda. Anda dapat mengaktifkan Resource Explorer untuk seluruh organisasi Anda atau untuk unit organisasi tertentu (OU).

> **Note**
>
> Anda dapat menyebarkan hingga maksimum 50.000 AWS CloudFormation tumpukan sekaligus. Jika Anda memiliki organisasi besar yang mencakup beberapa Wilayah, Anda harus menerapkan di tingkat OU dalam batch yang lebih kecil.

4. Baca ringkasan ucapan terima kasih sebelum Anda memilih Buat.

# Mengaktifkan Resource ExplorerWilayah AWS untuk mengindeks sumber daya Anda

Ketika Anda awalnya menghidupkanPenjelajah Sumber Daya AWS AndaAkun AWS, Anda membuat indeks untuk layanan dalam satu atau lebihWilayah AWS. Jika Anda menggunakan opsi Pengaturan cepat, Resource Explorer secara otomatis membuat indeks di semua Wilayah AWSyang diaktifkan diAkun AWS. Layanan Resource Explorer juga mempromosikan indeks di Wilayah yang ditentukan menjadi indeks agregator untuk akun tersebut. Jika Anda menggunakan opsi Pengaturan lanjutan, Anda menentukan Wilayah untuk membuat indeks.

Untuk mengaktifkan Resource Explorer di Wilayah tambahan, gunakan prosedur dalam topik ini.

Saat Anda mengaktifkan Resource Explorer di sebuahWilayah AWS, layanan akan melakukan tindakan berikut:

- Ketika Anda memulai Resource Explorer di Wilayah pertama diAkun AWS, Resource Explorer akan membuat peran terkait layanan di akun bernama`AWSServiceRoleForResourceExplorer`. Peran ini memberikan izin kepada Resource Explorer untuk menemukan dan mengindeks sumber daya di akun Anda dengan menggunakan layanan sepertiAWS CloudTrail dan layanan penandaan. Pembuatan peran terkait layanan hanya terjadi ketika Anda mendaftarkan yang pertamaWilayah AWS di akun. Resource Explorer menggunakan peran terkait layanan yang sama untuk semua Wilayah tambahan yang Anda tambahkan nanti.
- Resource Explorer membuat indeks di Wilayah yang ditentukan untuk menyimpan rincian tentang sumber daya Region itu.
- Resource Explorer mulai menemukan sumber daya di Wilayah yang ditentukan dan menambahkan informasi yang ditemukan tentang mereka ke indeks Region itu.

- Jika akun Anda sudah berisi indeks agregator di Wilayah yang berbeda, Resource Explorer mulai mereplikasi informasi dari indeks Wilayah baru ke indeks agregator untuk mendukung pencarian lintas wilayah.

Ketika langkah-langkah tersebut selesai, informasi tentang sumber daya Anda tersedia untuk ditemukan oleh pengguna. Mereka dapat mencari dengan menggunakan salah satu tampilan yang didefinisikan di Wilayah yang sama atau Wilayah yang berisi indeks agregator.

## Membuat indeks Resource Explorer di Wilayah

Anda dapat membuat indeks Resource Explorer di tambahanWilayah AWS dengan menggunakanAWS Management Console, dengan menggunakan perintah diAWS Command Line Interface (AWS CLI), atau dengan menggunakan operasi API diAWS SDK. Anda hanya dapat membuat satu indeks di Wilayah.

Izin minimum

Untuk melakukan langkah-langkah dalam prosedur ini, Anda harus memiliki izin berikut:

- Tindakan:`resource-explorer-2:*` - Sumber daya: tidak ada sumber daya tertentu (`*`)
- Tindakan:`iam:CreateServiceLinkedRole` - Sumber daya: tidak ada sumber daya tertentu (`*`)

AWS Management Console

Untuk membuat indeks Resource Explorer diWilayah AWS

1. Pada halaman Pengaturan Resource Explorer.
2. Di bagian Indeks, pilih Buat indeks.
3. Pada halaman Buat indeks, pilih kotak centangWilayah AWS di sebelah di mana Anda ingin membuat indeks untuk mendukung pencarian sumber daya Wilayah tersebut. Kotak centang yang tidak tersedia menunjukkan Wilayah yang sudah berisi indeks Resource Explorer.
4. (Opsional) di bagian, Anda dapat menentukan kunci dan pasangan nilai ke indeks.
5. Pilih Buat indeks.

   Resource Explorer menampilkan spanduk hijau di bagian atas halaman untuk menunjukkan keberhasilan, atau spanduk merah jika ada kesalahan saat membuat indeks di satu atau lebih Wilayah yang dipilih.

> **Note**
>
> Sumber daya yang ditandai lokal ke indeks muncul di hasil pencarian dalam beberapa menit. Sumber daya yang tidak ditandai biasanya membutuhkan waktu kurang dari dua jam untuk muncul, tetapi dapat memakan waktu lebih lama ketika ada permintaan yang besar. Hal ini juga dapat memakan waktu hingga satu jam untuk menyelesaikan replikasi awal ke indeks agregator baru dari semua indeks lokal yang ada.

Langkah selanjutnya - Jika Anda sudah membuat indeks agregator, maka Regions baru secara otomatis mulai mereplikasi informasi indeks mereka ke indeks agregator. Jika di situlah pengguna Anda melakukan semua pencarian mereka, maka sumber daya di Wilayah baru muncul di hasil pencarian tersebut dan Anda selesai.

Namun, jika Anda ingin pengguna dapat mencari sumber daya hanya di Wilayah yang baru diindeks, maka Anda juga harus membuat tampilan untuk pengguna di Wilayah tersebut dan memberikan izin kepada pengguna Anda ke tampilan itu. Untuk petunjuk tentang cara membuat tampilan, lihatMengelola tampilan Resource Explorer untuk menyediakan akses ke penelusuran.

AWS CLI

Untuk membuat indeks Resource Explorer diWilayah AWS

Jalankan perintah berikut untuk masing-masingWilayah AWS di mana Anda ingin membuat indeks untuk mendukung pencarian sumber daya Region itu. Perintah contoh ini mendaftar Resource Explorer di US East (N. Virginia) (N. Virginia) (N. Virginia) (N. Virginia) (N. Virginia`us-east-1`) (N.

```
$ aws resource-explorer-2 create-index \
    --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-11-01T20:00:59.149Z",
    "State": "CREATING"
}
```

Ulangi perintah ini untuk setiap Wilayah di mana Anda ingin mengaktifkan Resource Explorer, mengganti kode Region yang sesuai untuk`--region` parameter.

Karena Resource Explorer melakukan beberapa pembuatan indeks sebagai tugas asinkron di latar belakang, responsnya bisa jadi`CREATING`, yang menunjukkan bahwa proses latar belakang belum selesai.

> **Note**
>
> Sumber daya yang ditandai lokal ke indeks muncul di hasil pencarian dalam beberapa menit. Sumber daya yang tidak ditandai biasanya membutuhkan waktu kurang dari dua jam untuk muncul, tetapi dapat memakan waktu lebih lama ketika ada permintaan yang besar. Hal ini juga dapat memakan waktu hingga satu jam untuk menyelesaikan replikasi awal ke indeks agregator baru dari semua indeks lokal yang ada.

Anda dapat memeriksa penyelesaian akhir dengan menjalankan perintah berikut, dan memeriksa`ACTIVE` status.

```
$ aws resource-explorer-2 get-index \
    --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-12T18:59:10.503000+00:00",
    "LastUpdatedAt": "2022-07-13T18:41:58.799000+00:00",
    "ReplicatingFrom": [],
    "State": "ACTIVE",
    "Tags": {},
    "Type": "LOCAL"
}
```

Langkah selanjutnya - Jika Anda sudah membuat indeks agregator, maka Regions baru secara otomatis mulai mereplikasi informasi indeks mereka ke indeks agregator. Jika di situlah pengguna Anda melakukan semua pencarian mereka, maka sumber daya di Wilayah baru muncul di hasil pencarian tersebut dan Anda selesai.

Namun, jika Anda ingin pengguna dapat mencari sumber daya hanya di Wilayah yang baru diindeks, maka Anda juga harus membuat tampilan untuk pengguna di Wilayah tersebut dan memberikan izin kepada pengguna Anda ke tampilan itu. Untuk petunjuk tentang cara membuat tampilan, lihatMengelola tampilan Resource Explorer untuk menyediakan akses ke penelusuran.

# Pertimbangan untuk Wilayah AWS keikutsertaan

Wilayah Keikutsertaan memiliki persyaratan keamanan yang lebih tinggi daripada Wilayah komersial karena berkaitan dengan berbagi data IAM melalui akun di Wilayah keikutsertaan. Semua data yang dikelola melalui layanan IAM dianggap sebagai data identitas.

Anda dapat mengaktifkan Wilayah keikutsertaan menggunakan Penjelajah Sumber Daya AWS konsol. Lihat Mengaktifkan Resource Explorer di sebuah Wilayah AWS untuk mengindeks sumber daya Anda untuk informasi selengkapnya.

## Perilaku memilih keluar

Pertimbangkan perilaku berikut sebelum Anda memilih keluar dari Wilayah keikutsertaan:

> **Important**
>
> Sebelum Anda memilih keluar dari Wilayah dengan indeks agregator, kami sarankan Anda menghapus indeks agregator atau menurunkannya ke indeks lokal. Resource Explorer mendukung satu indeks agregator di semua Wilayah dalam partisi.

- Indeks Anda tidak dihapus, hanya dinonaktifkan. Jika Anda memilih untuk ikut serta lagi nanti, pengaturan Anda akan kembali.
- IAM menonaktifkan akses IAM ke sumber daya di Wilayah.
- Resource Explorer menonaktifkan indeks untuk Wilayah yang dipilih keluar dan berhenti menelan data. `ListIndexes`API tidak akan menampilkan indeks Wilayah lagi.
- Jika indeks agregator Anda berada di Wilayah yang berbeda, Resource Explorer menghentikan replikasi data dari Wilayah yang dipilih dan membersihkan data dalam waktu 24 jam.
- Jika Anda memilih keluar dari Wilayah indeks agregator Anda, Anda harus ikut serta lagi untuk menghapus atau menurunkan indeks.
- Jika Anda memilih masuk ke Region lagi, Resource Explorer mengaktifkan kembali indeks dan mulai menyerap data.
- Setiap perubahan status Wilayah keikutsertaan membutuhkan waktu sekitar 24 jam untuk mulai berlaku.

# Mengaktifkan pencarian lintas wilayah dengan membuat indeks agregator

Topik



## Tentang indeks agregator

Penjelajah Sumber Daya AWSmenyimpan informasi yang dikumpulkannya tentang sumber daya dalam indeks Wilayah AWS lokal yang dibuat dan dikelola Resource Explorer di Wilayah tersebut. Misalnya, asumsikan bahwa Anda memiliki instans Amazon EC2 di Wilayah AS Barat (Oregon). Resource Explorer menyimpan detail tentang sumber daya itu di indeks lokal di Wilayah Barat AS (Oregon).

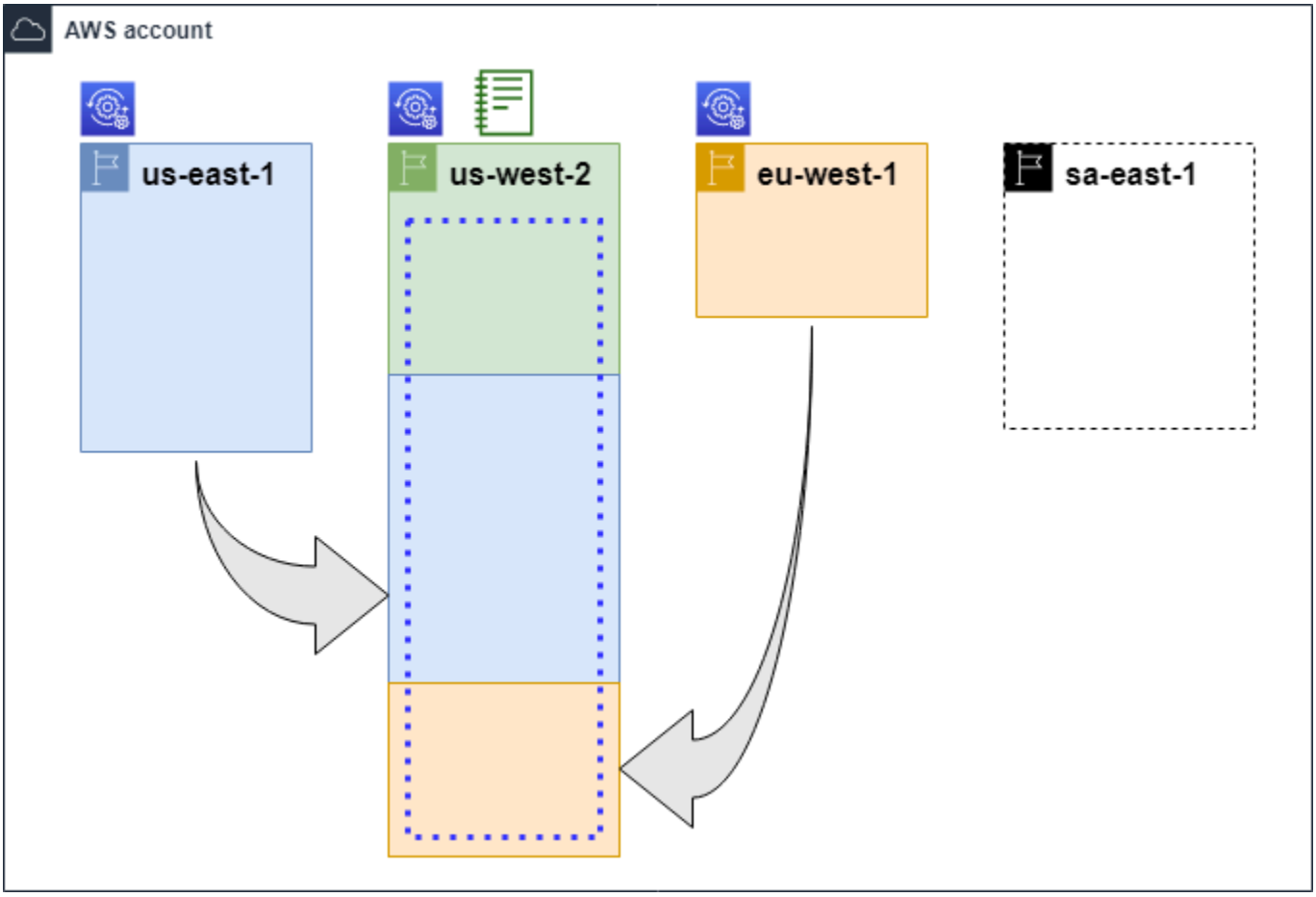
Untuk mendukung pencarian sumber daya Wilayah AWS di semua akun Anda, Anda dapat mengonversi indeks lokal di satu Wilayah menjadi indeks agregator untuk akun Anda.

Indeks agregator berisi salinan indeks lokal yang direplikasi di setiap Wilayah lain tempat Anda mengaktifkan Resource Explorer. Ini memungkinkan Anda membuat tampilan di Wilayah yang berisi indeks agregator yang hasilnya dapat menyertakan sumber daya dari semua Wilayah AWS akun.

Diagram berikut menunjukkan contoh bagaimana indeks agregator bekerja. Dalam contoh iniAkun AWS, administrator melakukan hal berikut:

- Mengaktifkan Resource Explorer di tiga Wilayah AWS (`us-east-1`us-west-2,, dan`eu-west-1`) dengan membuat indeks di Wilayah tersebut. Setiap wilayah memiliki indeks lokalnya sendiri.
- Memilih untuk tidak membuat indeks di `sa-east-1` Wilayah. Pengguna tidak dapat melakukan penelusuran`sa-east-1`, dan tidak ada sumber daya dari Wilayah tersebut yang muncul di hasil penelusuran apa pun.
- Membuat indeks agregator untuk akun di `us-west-2` Wilayah. Hal ini menyebabkan Resource Explorer mereplikasi informasi dari indeks lokal di semua Wilayah lain di mana Resource Explorer diaktifkan ke indeks agregator. Hal ini memungkinkan pencarian dilakukan `us-west-2` untuk menyertakan sumber daya dari ketiga Wilayah di mana Resource Explorer diaktifkan.

Konfigurasi ini berarti bahwa pengguna hanya dapat melakukan pencarian lintas wilayah`us-west-2`, yang berisi indeks agregator. Hanya tampilan dari Wilayah tersebut yang dapat mengembalikan hasil dari semua Wilayah di akun.




| Legenda | |
|---|---|
| | Resource Explorer diaktifkan dalam hal iniWilayah AWS, dan sumber dayanya dikatalogkan ke dalam indeks di Wilayah itu. Indeks Wilayah ini juga direplikasi (ditunjukkan oleh panah) ke Wilayah AWS yang berisi indeks agregator. |
| | Ini Wilayah AWS berisi indeks agregator. Resource Explorer mereplika si informasi sumber daya yang dikumpulkan di semua lainnya Wilayah AWS ke Wilayah ini. |
| | Tampilan default yang dibuat oleh Quick Setup mencakup semua sumber daya di semuaWilayah AWS. |

# Mempromosikan indeks lokal menjadi indeks agregator untuk akun

Anda memiliki pilihan untuk membuat indeks agregator dalam satuWilayah AWS ketika Anda pertama kali mengaturPenjelajah Sumber Daya AWS. Untuk informasi selengkapnya, lihat Menyiapkan dan mengonfigurasi Resource Explorer. Prosedur ini adalah tentang mempromosikan salah satu indeks lokal menjadi indeks agregator untuk akun jika Anda tidak melakukannya pada pengaturan awal.

**Important**

- Anda hanya dapat memiliki satu indeks aggregator dalam sebuahAkun AWS. Jika akun sudah memiliki indeks agregator, Anda harus terlebih dahulu menurunkannya ke indeks lokal atau menghapusnya.
- Setelah menghapus atau mengubah Wilayah mana yang berisi indeks agregator, Anda harus menunggu 24 jam sebelum dapat mempromosikan indeks lain untuk menjadi indeks agregator.

AWS Management Console

Untuk mempromosikan indeks lokal menjadi indeks agregator untuk akun

1. Buka halaman Pengaturan Resource Explorer.
2. Di bagian Indeks, pilih kotak centang di sebelah indeks yang ingin Anda promosikan, lalu pilih Ubah jenis indeks.
3. Dalam Ubah tipe indeks untuk < Nama wilayah> dialog, pilih indeks agregator, lalu pilih Simpan perubahan.

AWS CLI

Untuk mempromosikan indeks lokal menjadi indeks agregator untuk akun

Berikut contoh perintah update indeks dalam ditentukanWilayah AWS dari jenis`LOCAL` ke jenis`AGGREGATOR`. Anda harus memanggil operasi dariWilayah AWS yang ingin Anda isi indeks agregator.

```
$ aws resource-explorer-2 update-index-type \
    --arn arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
```

```
    --type AGGREGATOR \
    --region us-east-1
{
    "Arn":"arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "LastUpdatedAt":"2022-07-13T18:41:58.799Z",
    "State":"UPDATING",
    "Type":"AGGREGATOR"
}
```

Operasi bekerja secara asinkron dan dimulai dengan`State` set ke`UPDATING`. Untuk memeriksa apakah operasi telah selesai, Anda dapat menjalankan perintah berikut dan mencari nilai`ACTIVE` di bidang`State` respons. Anda harus menjalankan perintah ini di Wilayah yang berisi indeks yang ingin Anda periksa.

```
$ aws resource-explorer-2 get-index --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-10-12T21:31:37.277000+00:00",
    "LastUpdatedAt": "2022-10-12T21:31:37.677000+00:00",
    "ReplicatingFrom": [
        "us-west-2",
        "us-east-2",
        "us-west-1"
    ],
    "State": "ACTIVE",
    "Tags": {},
    "Type": "AGGREGATOR"
}
```

## Menurunkan indeks agregator ke indeks lokal

Anda dapat menurunkan indeks agregator ke indeks lokal, seperti saat Anda ingin memindahkan indeks agregator ke indeks lain. Wilayah AWS

Saat Anda menurunkan indeks agregator ke indeks lokal, Resource Explorer berhenti mereplikasi indeks dari indeks lainnya. Wilayah AWS Ini juga memulai tugas latar belakang asinkron untuk menghapus informasi yang direplikasi dari Wilayah lain. Sampai tugas asinkron itu selesai, beberapa hasil lintas wilayah dapat terus muncul di hasil pencarian.

> **Catatan**
>
> - Setelah menurunkan indeks agregator, Anda harus menunggu 24 jam sebelum dapat mempromosikan indeks yang sama atau indeks di Wilayah yang berbeda untuk menjadi indeks agregator baru untuk akun tersebut.
> - Setelah menurunkan indeks agregator, diperlukan waktu hingga 36 jam untuk menyelesaikan proses latar belakang dan agar semua informasi sumber daya dari Wilayah lain menghilang dari hasil pencarian yang dilakukan di Wilayah ini.
> - Jika Anda menurunkan akun anggota dalam tampilan luas organisasi, anggota dapat dihapus dari pencarian multi-akun.

Anda dapat memeriksa status tugas latar belakang dengan melihat daftar indeks pada halaman Pengaturan atau dengan menggunakan GetIndexoperasi. Ketika tugas asinkron selesai, `Status` bidang dari indeks berubah dari ke. `UPDATING` `ACTIVE` Pada saat itu, hanya hasil dari Wilayah lokal yang muncul di hasil kueri.

AWS Management Console

Untuk menurunkan indeks agregator ke indeks lokal

1. Buka halaman Pengaturan Resource Explorer.
2. Di bagian Indeks, pilih kotak centang di samping Wilayah yang berisi indeks agregator yang ingin diturunkan ke indeks lokal, lalu pilih Ubah jenis indeks.
3. Dalam Ubah jenis indeks untuk < Nama wilayah> dialog, pilih Indeks lokal, lalu pilih Simpan perubahan.

AWS CLI

Untuk menurunkan indeks agregator ke indeks lokal

Contoh berikut mendemotasikan indeks agregator yang ditentukan ke indeks lokal. Anda harus memanggil operasi di Wilayah AWS yang saat ini berisi indeks agregator.

```
$ aws resource-explorer-2 update-index-type \
    --arn arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
```

```
    --type LOCAL \
    --region us-east-1
{
    "Arn":"arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "LastUpdatedAt":"2022-07-13T18:41:58.799Z",
    "State":"UPDATING",
    "Type":"LOCAL"
}
```

Operasi bekerja secara asinkron dan dimulai dengan `State` set ke. `UPDATING` Untuk memeriksa apakah operasi telah selesai, Anda dapat menjalankan perintah berikut dan mencari nilai `ACTIVE` di bidang `State` respons. Anda harus menjalankan perintah ini di Wilayah berisi indeks yang ingin Anda periksa.

```
$ aws resource-explorer-2 get-index --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-10-12T21:31:37.277000+00:00",
    "LastUpdatedAt": "2022-10-12T21:31:37.677000+00:00",
    "ReplicatingFrom": [
        "us-west-2",
        "us-east-2",
        "us-west-1"
    ],
    "State": "ACTIVE",
    "Tags": {},
    "Type": "LOCAL"
}
```

# Mendukung pencarian terpadu diAWS Management Console

AWS Management ConsoleMemiliki bilah pencarian di bagian atas setiap halaman konsol. Ini memberikan pengalaman pencarian terpadu di semuaLayanan AWS. Hasil pencarian terpadu dapat mencakup hal-hal seperti:

- Layanan AWSdan fitur halaman konsol.
- AWShalaman dokumentasi.
- AWSblog dan artikel Basis Pengetahuan

- Sumber daya di akun Anda — jika Anda mengikuti langkah-langkah di bawah ini.

Untuk melihat sumber daya akun Anda di hasil pencarian terpadu Anda, Anda harus melakukan langkah-langkah berikut in. Anda dapat melakukan ini selama pengaturan awalPenjelajah Sumber Daya AWS. Semuanya terjadi secara otomatis jika Anda menggunakan opsi Pengaturan cepat.

- Anda harus membuat indeks agregator dalam satuWilayah AWS untukAkun AWS.
- Anda harus membuat tampilan default diWilayah AWS yang berisi indeks agregator.
- Anda harus memberikan semua prinsipal yang perlu mencari sumber daya di izin bilah pencarian terpadu untuk mencari menggunakan tampilan default tersebut.

Pencarian terpadu selalu menggunakan tampilan default diWilayah AWS yang berisi indeks agregator untuk melakukan semua pencarian.

# Pengaruh tindakan akun pada pencarian multi-akun Resource Explorer

> **Note**
>
> Diperlukan waktu hingga 24 jam untuk menghapus akun dan sumber daya dari hasil pencarian multi-akun.

Tindakan akun memiliki efek berikut pada pencarian Penjelajah Sumber Daya AWS multi-akun.

## Resource Explorer dinonaktifkan

Ketika Anda menonaktifkan Resource Explorer untuk sebuah akun, itu dinonaktifkan hanya untuk akun itu di Wilayah AWS yang dipilih saat Anda menonaktifkannya.

Anda harus menonaktifkan Resource Explorer secara terpisah di setiap Wilayah yang diaktifkan.

Setelah 24 jam, sumber daya dari akun ini tidak akan muncul di hasil penelusuran.

Data dan pengaturan Resource Explorer lainnya tidak dihapus.

## Akun anggota dihapus dari organisasi

Ketika akun anggota dihapus dari organisasi, akun administrator Resource Explorer kehilangan izin untuk melihat sumber daya di akun anggota.

Jika akun yang dihapus adalah administrator atau akun administrator yang didelegasikan, semua tampilan multi-akun yang sebelumnya dibuat oleh akun ini juga akan dihapus.

Resource Explorer terus berjalan di kedua akun.

Hasil pencarian sumber daya tidak lagi menyertakan sumber daya dari akun ini.

## Akun ditangguhkan

Ketika akun ditangguhkanAWS, akun kehilangan izin untuk melihat sumber daya di Resource Explorer. Akun administrator untuk akun yang ditangguhkan dapat melihat sumber daya yang ada.

Untuk akun organisasi, status akun anggota juga dapat berubah menjadi Akun Ditangguhkan. Ini terjadi jika akun ditangguhkan pada saat yang sama ketika akun administrator mencoba mengaktifkan akun. Akun administrator untuk Akun yang ditangguhkan tidak dapat melihat sumber daya untuk akun tersebut.

Jika tidak, status yang ditangguhkan tidak akan memengaruhi status akun anggota.

Setelah 90 hari, akun dinonaktifkan atau diaktifkan kembali. Ketika akun diaktifkan kembali, izin Resource Explorer dipulihkan. Jika status akun anggota adalah Akun Ditangguhkan, akun administrator harus mengaktifkan akun secara manual.

## Akun ditutup

Ketika AWS akun ditutup, Resource Explorer merespons penutupan sebagai berikut:

- Resource Explorer menyimpan sumber daya untuk akun selama 90 hari sejak tanggal efektif penutupan akun. Pada akhir periode 90 hari, Resource Explorer menghapus semua sumber daya untuk akun secara permanen.
- Untuk mempertahankan sumber daya selama lebih dari 90 hari, Anda dapat menggunakan tindakan kustom dengan EventBridge aturan untuk menyimpan sumber daya di bucket Amazon S3. Selama Resource Explorer mempertahankan sumber daya, saat Anda membuka kembali akun yang ditutup, Resource Explorer mengembalikan sumber daya untuk akun tersebut.

- Jika akun tersebut adalah akun administrator Resource Explorer, akun tersebut dihapus sebagai administrator dan semua akun anggota dihapus. Jika akun tersebut adalah akun anggota, akun tersebut dipisahkan dan dihapus sebagai anggota dari akun administrator Resource Explorer.
- Untuk informasi selengkapnya, lihat Menutup akun.

### Penyisihan akun

Jika akun memilih keluar dari suatu Wilayah, Anda masih akan melihat sumber daya mereka di hasil penelusuran hingga 24 jam.

Setelah 24 jam, sumber daya dari akun ini tidak akan muncul di hasil penelusuran. Untuk informasi selengkapnya, lihat Perilaku memilih keluar.

## Mematikan Resource Explorer di Wilayah AWS

Bila Anda tidak perlu lagi mencari sumber daya tertentuWilayah AWS, Anda dapat mematikan hanya Penjelajah Sumber Daya AWS di Wilayah itu dengan menghapus indeksnya. Ketika Anda melakukan ini, Resource Explorer berhenti memindai sumber daya baru atau yang diperbarui di Wilayah tersebut. Jika akun Anda berisi indeks agregator, maka replikasi dari indeks yang dihapus berhenti, dan informasi dari indeks yang dihapus dihapus dari indeks agregator dan berhenti muncul di hasil pencarian. Diperlukan waktu hingga 24 jam agar semua sumber daya dari indeks yang dihapus menghilang dari hasil pencarian di Wilayah dengan indeks agregator.

> **Note**
>
> Saat Anda mendaftarkan yang pertamaWilayah AWS, Resource Explorer membuat peran terkait layanan (SLR) yang dinamai `AWSServiceRoleForResourceExplorer` dalamAkun AWS. Resource Explorer tidak menghapus SLR ini secara otomatis. Setelah menghapus indeks Resource Explorer di setiap Wilayah di akun, Anda dapat menggunakan konsol IAM untuk menghapus SLR jika Anda tidak akan menggunakan Resource Explorer di masa mendatang. Jika Anda menghapus peran dan kemudian memilih untuk mengaktifkan Resource Explorer lagi dalam setidaknya satuWilayah AWS, Resource Explorer akan membuat ulang peran terkait layanan secara otomatis.

Anda dapat menonaktifkan Resource Explorer Wilayah AWS dengan menggunakanAWS Management Console, dengan menggunakan perintah di AWS Command Line Interface (AWS CLI), atau dengan menggunakan operasi API di AWS SDK.

Jika Anda menonaktifkan Resource Explorer untuk akun anggota, dan anggota berada dalam tampilan luas organisasi, itu akan dihapus dari hasil pencarian multi-akun.

Jika Anda tidak lagi ingin mendukung pencarian sumber daya di satu atau lebih akun Anda, lakukan langkah-langkah dalam prosedur berikut. Wilayah AWS

> **Note**
>
> Jika indeks yang Anda hapus adalah indeks agregator untukAkun AWS, Anda harus menunggu 24 jam sebelum Anda dapat mempromosikan indeks lokal lain untuk menjadi indeks agregator untuk akun. Pengguna tidak dapat melakukan penelusuran di seluruh akun menggunakan Resource Explorer hingga indeks agregator lain dikonfigurasi.

AWS Management Console

Untuk menghapus indeks Resource Explorer di Wilayah AWS

1. Buka halaman Pengaturan Resource Explorer.
2. Di bagian Indeks, pilih kotak centang di sebelah Wilayah AWS dengan indeks yang ingin Anda hapus, lalu pilih Hapus.
3. Pada halaman Hapus indeks, verifikasi bahwa Anda hanya memilih indeks yang ingin Anda hapus. Ketik **`delete`** kotak teks Konfirmasi, lalu pilih Hapus indeks.

   Resource Explorer menampilkan spanduk hijau di bagian atas halaman untuk menunjukkan keberhasilan, atau spanduk merah jika ada kesalahan dengan satu atau beberapa Wilayah yang dipilih.

AWS CLI

Untuk menghapus indeks Resource Explorer di Wilayah AWS

Jika Anda tidak lagi ingin mendukung pencarian sumber daya di satu atau lebih akun Anda, jalankan perintah berikut. Wilayah AWS

Jalankan perintah berikut untuk setiap Wilayah dengan indeks yang ingin Anda hapus. Anda harus menjalankan perintah di Wilayah dengan indeks yang ingin Anda hapus. Contoh perintah berikut menghapus indeks Resource Explorer di AS Barat (Oregon) (`us-west-2`).

```
$ aws resource-explorer-2 delete-index \
    --arn arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222 \
    --region us-west-2
{
    "Arn": "arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222",
    "State": "DELETING"
}
```

Karena Resource Explorer melakukan beberapa pekerjaan pembersihan penghapusan sebagai tugas asinkron di latar belakang, respons mungkin menunjukkan bahwa operasi tersebut. `DELETING` Status ini menunjukkan bahwa proses latar belakang belum selesai. Anda dapat memeriksa penyelesaian akhir dengan menjalankan perintah berikut, dan memeriksa `State` untuk mengubah ke`DELETED`.

```
$ aws resource-explorer-2 get-index \
    --region us-west-2
{
    "Arn": "arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-12T18:59:10.503000+00:00",
    "LastUpdatedAt": "2022-07-13T18:41:58.799000+00:00",
    "ReplicatingFrom": [],
    "State": "DELETED",
    "Tags": {},
    "Type": "LOCAL"
}
```

# Mematikan Resource Explorer di semuaWilayah AWS

Jika Anda ingin mematikanPenjelajah Sumber Daya AWS sepenuhnya, lakukan prosedur berikut ini.

> **Note**
>
> Resource Explorer membuat layanan terkait peran bernama AWSServiceRoleForResourceExplorer dalam account ketika Anda membuat indeks di pertamaWilayah AWS untuk account. Resource Explorer tidak secara otomatis menghapus peran terkait layanan ini. Setelah menghapus indeks Resource Explorer di setiap Wilayah, Anda kemudian dapat menggunakan konsol IAM untuk menghapus peran jika Anda yakin Anda tidak akan menggunakan Resource Explorer lagi di future. Jika Anda menghapus peran dan kemudian Anda memilih untuk memulai Resource Explorer dalam setidaknya satuWilayah AWS, Resource Explorer membuat ulang peran terkait layanan.

## Matikan Resource Explorer di semuaWilayah AWS

Anda dapat menonaktifkan Resource Explorer dengan menggunakanAWS Management Console, dengan menggunakan perintah diAWS Command Line Interface (AWS CLI), atau dengan menggunakan operasi API diAWS SDK.

AWS Management Console

Jika Anda belum lagi ingin mendukung pencarian sumber daya dalam apa punWilayah AWS di AndaAkun AWS, lakukan langkah-langkah dalam prosedur berikut ini.

Menonaktifkan Resource Explorer di semuaWilayah AWS

1. Buka halaman Pengaturan Resource Explorer.
2. Di bagian Indeks, pilih kotak centang di samping semua yang terdaftarWilayah AWS, lalu pilih Hapus.

   > **Tip**
   >
   > Anda dapat mencentang kotak di baris header tabel di sebelah Indeks untuk mencentang kotak untuk semua Wilayah dalam satu langkah.

3. Pada halaman Hapus indeks, verifikasi bahwa Anda ingin menghapus semua indeks. Ketik**`delete`** kotak teks Konfirmasi, lalu pilih Hapus indeks.

Resource Explorer menampilkan spanduk hijau di bagian atas halaman untuk menunjukkan keberhasilan, atau spanduk merah jika ada kesalahan dengan satu atau lebih Wilayah yang dipilih.

AWS CLI

Menonaktifkan Resource Explorer di semuaWilayah AWS

Jika Anda tidak lagi ingin mendukung pencarian sumber daya di akun Anda, jalankan perintah berikut untuk menemukan ARN dari setiap indeksWilayah AWS di masing-masing tempat Anda mengaktifkan Resource Explorer sebelumnya.Wilayah AWS

```
$ aws resource-explorer-2 list-indexes --query Indexes[*].Arn[
"arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
"arn:aws:resource-explorer-2:us-west-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222",
"arn:aws:resource-explorer-2:us-west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd33333333"
]
```

Untuk setiap respons, jalankan perintah berikut untuk menghapus indeks Resource Explorer di Wilayah tersebut.

```
$ aws resource-explorer-2 delete-index \
    --arn arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "State": "DELETING"
}
```

Ulangi perintah sebelumnya di setiap Wilayah tambahan.

Karena Resource Explorer melakukan beberapa pembersihan sebagai tugas asinkron di latar belakang, respons mungkin menunjukkan bahwa operasi tersebut`DELETING`. Status ini menunjukkan bahwa proses latar belakang belum lengkap. Anda dapat memeriksa penyelesaian akhir dengan menjalankan perintah berikut, dan memeriksa status yang akan diubah`DELETED`.

```
$ aws resource-explorer-2 get-index \
    --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-12T18:59:10.503000+00:00",
    "LastUpdatedAt": "2022-07-13T18:41:58.799000+00:00",
    "ReplicatingFrom": [],
    "State": "DELETED",
    "Tags": {},
    "Type": "LOCAL"
}
```

# Menerapkan Resource Explorer ke akun di organisasi

Dengan menggunakan AWS CloudFormation StackSets, Anda dapat menentukan dan menyebarkan ke semua akun yang dikelola dalam organisasi olehAWS Organizations. Saat Anda menentukan kumpulan tumpukan, Anda menentukan AWS sumber daya yang ingin Anda buat di seluruh Wilayah AWS dan di semua akun target yang Anda tentukan. Ketika semua akun merupakan bagian dari organisasi yang sama, Anda dapat memanfaatkan AWS CloudFormation integrasi dengan Organizations dan membiarkan layanan tersebut menangani pembuatan peran lintas akun. Anda dapat mengaktifkan penerapan otomatis di organisasi, yang secara otomatis menyebarkan instance tumpukan ke akun baru yang mungkin Anda tambahkan ke organisasi target atau unit organisasi (OU) di masa mendatang. Jika Anda menghapus akun dari organisasi, maka AWS CloudFormation secara otomatis menghapus sumber daya apa pun yang digunakan sebagai bagian dari instance tumpukan organisasi. Untuk informasi selengkapnya StackSets, lihat Bekerja dengan AWS CloudFormation StackSets di Panduan AWS CloudFormation Pengguna.

Anda dapat menggunakan AWS CloudFormation StackSets untuk mengaktifkan dan mengonfigurasi semua akun Penjelajah Sumber Daya AWS di organisasi Anda, membuat indeks di setiap Wilayah yang diaktifkan, dan membuat tampilan di mana Anda membutuhkannya.

> **Important**
>
> Jika Anda mencoba menyiapkan indeks agregator di Wilayah, Anda harus memastikan akun tersebut tidak memiliki indeks agregator yang ada di Wilayah lain mana pun. Setelah Anda

menurunkan indeks agregator ke indeks lokal, Anda harus menunggu 24 jam sebelum Anda dapat mempromosikan indeks lain untuk menjadi indeks agregator baru untuk akun tersebut.

## Prasyarat

AWS CloudFormation StackSets Untuk menggunakan Resource Explorer ke akun di organisasi, Anda, atau administrator organisasi Anda, harus terlebih dahulu melakukan langkah-langkah berikut untuk mengaktifkan tumpukan dengan izin yang dikelola layanan:

1. Organisasi harus mengaktifkan semua fitur. Jika organisasi hanya mengaktifkan fitur penagihan gabungan, Anda tidak dapat membuat kumpulan tumpukan dengan izin yang dikelola layanan.
2. Aktifkan akses tepercaya antara AWS CloudFormation dan Organizations. Ini memberikan AWS CloudFormation izin untuk membuat peran yang diperlukan dalam akun manajemen organisasi dan akun anggota AWS CloudFormation akan menyebarkan indeks dan tampilan Resource Explorer.

Sekarang Anda dapat membuat set tumpukan dengan izin yang dikelola layanan.

**Important**

Anda harus membuat kumpulan tumpukan di akun manajemen organisasi. AWS CloudFormationadalah layanan Regional, sehingga Anda dapat melihat dan mengelola kumpulan tumpukan yang Anda buat hanya dari Wilayah tempat Anda membuatnya.

## Membuat set tumpukan untuk Resource Explorer

Dengan sepenuhnya menyebarkan Resource Explorer, Anda harus menyebarkan dua set tumpukan.

- Kumpulan tumpukan pertama membuat indeks agregator dan tampilan default yang memungkinkan pengguna mencari sumber daya di semua Wilayah di akun.

  Terapkan tumpukan ini disetel ke hanya Wilayah tunggal di mana Anda ingin membuat indeks agregator.
- Set tumpukan kedua membuat indeks lokal dan tampilan default. Indeks lokal mereplikasi kontennya ke indeks agregator.

Terapkan kumpulan tumpukan ini ke setiap Wilayah yang diaktifkan di akun kecuali Wilayah yang berisi indeks agregator. Jangan memilih Wilayah mana pun yang tidak diaktifkan di akun tempat Anda menerapkan tumpukan. Jika Anda melakukannya, penerapan gagal.

Contoh template untuk masing-masing ini ada di bagian berikut. Untuk step-by-step petunjuk tentang cara membuat kumpulan tumpukan menggunakan templat ini, lihat Membuat kumpulan tumpukan dengan izin yang dikelola layanan di Panduan Pengguna. AWS CloudFormation

Setelah Anda menerapkan kumpulan tumpukan ini ke organisasi Anda, setiap akun dalam lingkup yang Anda pilih, organisasi atau unit organisasi, memiliki indeks agregator di Wilayah yang ditentukan, dan indeks lokal di setiap Wilayah lainnya.

## Contoh AWS CloudFormation template

Contoh template berikut membuat indeks agregator akun dan tampilan default yang dapat mencari sumber daya di semua Wilayah di akun tempat Anda menerapkan indeks.

YAML

```
Description: >-
  CFN Stack setting up ResourceExplorer with an Aggregator Index, and a new Default
 View.
Resources:
  Index:
    Type: 'AWS::ResourceExplorer2::Index'
    Properties:
      Type: AGGREGATOR
      Tags:
        Purpose: ResourceExplorer CFN Stack
  View:
    Type: 'AWS::ResourceExplorer2::View'
    Properties:
      ViewName: DefaultView
      IncludedProperties:
        - Name: tags
      Tags:
        Purpose: ResourceExplorer CFN Stack
    DependsOn: Index
  DefaultViewAssociation:
    Type: 'AWS::ResourceExplorer2::DefaultViewAssociation'
```

```
    Properties:
      ViewArn: !Ref View
```

JSON

```
{
    "Description": "CFN Stack setting up ResourceExplorer with an Aggregator Index,
 and a new Default View.",
    "Resources": {
        "Index": {
            "Type": "AWS::ResourceExplorer2::Index",
            "Properties": {
                "Type": "AGGREGATOR",
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
                }
            }
        },
        "View": {
            "Type": "AWS::ResourceExplorer2::View",
            "Properties": {
                "ViewName": "DefaultView",
                "IncludedProperties": [{
                    "Name": "tags"
                }],
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
                }
            },
            "DependsOn": "Index"
        },
        "DefaultViewAssociation": {
            "Type": "AWS::ResourceExplorer2::DefaultViewAssociation",
            "Properties": {
                "ViewArn": {
                    "Ref": "View"
                }
            }
        }
    }
}
```

Contoh template berikut membuat indeks lokal di setiap Wilayah yang diaktifkan di semua akun selain akun dengan indeks agregator. Ini juga menciptakan tampilan default bahwa pengguna dapat mencari sumber daya hanya di Wilayah itu. Pengguna harus mencari dengan tampilan di Wilayah agregator untuk mencari sumber daya di semua Wilayah.

YAML

```
Description: >-
  CFN Stack setting up ResourceExplorer with a Local Index, and a new Default View.
Resources:
  Index:
    Type: 'AWS::ResourceExplorer2::Index'
    Properties:
      Type: LOCAL
      Tags:
        Purpose: ResourceExplorer CFN Stack
  View:
    Type: 'AWS::ResourceExplorer2::View'
    Properties:
      ViewName: DefaultView
      IncludedProperties:
        - Name: tags
      Tags:
        Purpose: ResourceExplorer CFN Stack
    DependsOn: Index
  DefaultViewAssociation:
    Type: 'AWS::ResourceExplorer2::DefaultViewAssociation'
    Properties:
      ViewArn: !Ref View
```

JSON

```
{
    "Description": "CFN Stack setting up ResourceExplorer with a Local Index, and a
 new Default View.",
    "Resources": {
        "Index": {
            "Type": "AWS::ResourceExplorer2::Index",
            "Properties": {
                "Type": "LOCAL",
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
                }
```

```
            }
        },
        "View": {
            "Type": "AWS::ResourceExplorer2::View",
            "Properties": {
                "ViewName": "DefaultView",
                "IncludedProperties": [{
                    "Name": "tags"
                }],
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
                }
            },
            "DependsOn": "Index"
        },
        "DefaultViewAssociation": {
            "Type": "AWS::ResourceExplorer2::DefaultViewAssociation",
            "Properties": {
                "ViewArn": {
                    "Ref": "View"
                }
            }
        }
    }
}
```

# Mengelola tampilan Resource Explorer untuk menyediakan akses ke penelusuran

Tampilan adalah kunci untuk mencari sumber daya Anda. Setiap operasi Penjelajah Sumber Daya AWS pencarian harus menggunakan tampilan.

Tampilan adalah metode yang dapat digunakan administrator untuk mengontrol akses ke informasi tentang sumber daya di AndaAkun AWS.

Tampilan hanya dapat diakses oleh prinsipal (peran IAM atau pengguna) yang memiliki izin untuk menggunakan tampilan itu. Agar berhasil mencari dengan Resource Explorer, prinsipal harus memiliki `Allow` akses ke kedua `resource-explorer-2:GetView` dan `resource-explorer-2:Search` operasi pada ARN tampilan.

Tampilan berisi filter bawaan yang dapat digunakan administrator untuk membatasi hasil hanya pada item yang menarik. Misalnya, Anda dapat membuat tampilan yang hanya mencakup sumber daya yang terkait dengan proyek tertentu. Pengguna yang tidak perlu melihat informasi tentang proyek lain dapat menggunakan tampilan ini hanya untuk melihat sumber daya yang diminati.

Pandangan adalah sumber daya Regional. Tampilan dibuat dan disimpan secara spesifik Wilayah AWS dan mengembalikan hasilnya hanya informasi dari indeks di Wilayah tersebut. Untuk menyertakan hasil dari seluruh Wilayah dalam akun, tampilan harus berada di Wilayah yang berisi indeks agregator. Wilayah itu berisi replika indeks dari semua Wilayah lain di akun.

Untuk informasi selengkapnya tentang membuat dan menggunakan tampilan, lihat topik berikut.

Topik

- Tentang tampilan Resource Explorer
- Membuat tampilan Resource Explorer yang akan digunakan untuk penelusuran
- Memberikan akses ke tampilan Resource Explorer untuk pencarian
- Mengatur tampilan default dalamWilayah AWS
- Menambahkan tag ke tampilan yang sudah ditonton
- Berbagi tampilan Resource Explorer
- Menghapus tampilan di Resource Explorer

# Tentang tampilan Resource Explorer

Penjelajah Sumber Daya AWSindeks sumber daya Anda di latar belakang dan kemudian membuat indeks yang tersedia bagi Anda untuk query. Anda dapat melakukan kueri penelusuran untuk sumber daya Anda menggunakan Resource Explorer API yang didokumentasikan dalam panduan ini, atau dengan menggunakan konsol Resource Explorer. Resource Explorer menggunakan API-nya untuk menyediakan antarmuka grafis interaktif dengan apa yang seharusnya hanya API yang dapat diakses secara terprogram. Konsep yang dijelaskan dalam topik ini berlaku untuk API dan konsol.

Tampilan disimpan dalamWilayah AWS dan mengembalikan hasil dari hanya indeks Region itu.

Karena administrator mungkin ingin membatasi akses ke informasi yang terkandung dalam indeks sumber daya, indeks itu sendiri tidak dapat diakses secara langsung. Sebaliknya, semua pencarian harus melalui tampilan yang pengguna harus memiliki izin untuk mencari.

Ada beberapa elemen kunci untuk setiap tampilan:

Izin untuk mencari

Anda dapat menggunakan kebijakanAWS izin standar untuk mengontrol siapa yang dapat menggunakan setiap tampilan. Ini disediakan oleh kebijakan izin berbasis identitas yang dilampirkan pada prinsipal yang memberi Anda kontrol terperinci atas siapa yang dapat melihat informasi yang diberikan oleh setiap tampilan. Misalnya, Anda dapat memberikan akses ke`Production-resources` tampilan untuk memungkinkan pencarian hanya oleh teknisi yang mengoperasikan layanan produksi Anda. Kemudian, Anda dapat memberikan izin yang berbeda ke`Pre-production-resources` tampilan untuk memungkinkan pencarian sumber daya pra-produksi oleh pengembang Anda.

Jika Anda menggunakan kebijakanAWS terkelola yang dinamai`AWSResourceExplorerReadOnlyAccess` dengan prinsipal, kebijakan tersebut memberi mereka kemampuan untuk mencari menggunakan tampilan apa pun di akun.

Atau, Anda dapat membuat kebijakan izin Anda sendiri dan memberikan izin berikut hanya untuk tampilan tertentu:

- `resource-explorer-2:GetView`
- `resource-explorer-2:Search`

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

- Pengguna dan grup diAWS IAM Identity Center:

  Buat set izin. Ikuti petunjuk di Buat set izin di PanduanAWS IAM Identity Center Pengguna.

- Pengguna yang dikelola dalam IAM melalui penyedia identitas:

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

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

Untuk informasi lebih lanjut tentang izin, lihatMemberikan akses ke tampilan Resource Explorer untuk pencarian.

Memfilter pencarian

Tampilan berfungsi sebagai jendela virtual di mana pengguna dapat melihat sumber daya di akun. Anda dapat membuat beberapa tampilan, masing-masing menyajikan tampilan yang berbeda dari gambar yang lebih besar. Misalnya, Anda dapat membuat tampilan yang memungkinkan pencarian hanya sumber daya yang terkait dengan lingkungan pra-produksi Anda, seperti yang diidentifikasi oleh tag yang dilampirkan ke sumber daya Anda. Kemudian, Anda dapat membuat tampilan terpisah yang memungkinkan pencarian hanya sumber daya di lingkungan produksi Anda, berdasarkan nilai yang berbeda dalam tag. Jika Anda mengonfigurasi beberapa tampilan dengan`FilterString` nilai yang berbeda, Anda tidak perlu memasukkan kembali parameter kueri tersebut setiap kali Anda Mencari.

Tampilan juga dapat menentukan bagian opsional informasi tentang sumber daya yang akan disertakan dalam hasil. Daftar default bidang selalu disertakan dalam hasil. Selain daftar default, Anda dapat meminta agar tampilan juga menyertakan tag apa pun yang dilampirkan ke sumber .

Lingkup pencarian

- Cakupan wilayah - Saat Anda menelusuriWilayah AWS dengan Resource Explorer, hasilnya hanya dapat mencakup sumber daya yang diindeks di Wilayah tersebut. Indeks di sebagian besar Wilayah diberi label`LOCAL` karena berisi informasi tentang sumber daya hanya dalam Wilayah tersebut. Pencarian di Wilayah tersebut hanya dapat mengembalikan sumber daya tersebut.

- Cakupan akun - Anda dapat mempromosikan satu indeks lokal untuk menjadi indeks agregator untuk akun tersebut. Ketika Anda melakukan ini, semua Wilayah lain di mana Resource Explorer diaktifkan mereplikasi informasi indeks mereka ke Wilayah dengan indeks agregator. Jika Anda mencari di Wilayah tersebut, hasil tersebut mencakup sumber daya dari semua Wilayah di akun. Saat Anda menggunakan opsi Pengaturan cepat untuk mengonfigurasi server, Resource Explorer secara otomatis membuat indeks agregator di Wilayah yang Anda tentukan. Selain itu, opsi Pengaturan Cepat membuat tampilan default di Wilayah tersebut untuk mendukung pencarian semua sumber daya di akun di semua Wilayah.

## Tampilan default

Jika pengguna mencoba mencari tanpa menentukan tampilan secara eksplisit, Resource Explorer menggunakan tampilan default yang ditentukan untuk ituWilayah AWS.

Jika tampilan default tidak ada untuk Wilayah tersebut dan pengguna tidak menentukan tampilan yang akan digunakan, maka pencarian gagal dan menghasilkan pengecualian.

Resource Explorer secara otomatis membuat tampilan default sebagai berikut:

- Jika Anda mengaktifkan Resource Explorer menggunakanAWS Management Console dan memilih opsi Pengaturan cepat, Anda harus menentukan Wilayah mana yang berisi indeks agregator untuk akun tersebut. Resource Explorer secara otomatis membuat tampilan default dalam indeks agregator tertentu Region.
- Jika Anda mendaftarkan Resource Explorer menggunakanAWS Management Console dan memilih opsi Pengaturan lanjutan, Anda dapat memilih untuk membuat indeks agregator untuk akun di Wilayah tertentu. Jika Anda melakukan ini, Resource Explorer membuat tampilan default secara otomatis di Region indeks agregator.
- Jika Anda mendaftarkan Resource Explorer dengan menggunakan konsol dan memilih untuk tidak mendaftarkan Region indeks agregator, Resource Explorer membuat tampilan default untuk indeks lokal di setiap Wilayah.
- Jika Anda mendaftarkan Resource Explorer dengan menggunakan operasi APIAWS CLI atau, Resource Explorer tidak secara otomatis membuat tampilan default. Sebagai gantinya, Anda harus mengonfigurasi tampilan default secara manual untuk setiap Wilayah tempat Anda mengharapkan pengguna untuk menelusuri.

# Membuat tampilan Resource Explorer yang akan digunakan untuk penelusuran

Semua pencarian harus menggunakan tampilan. Tampilan mendefinisikan filter yang menentukan sumber daya mana yang dapat dikembalikan oleh kueri yang menggunakan tampilan. Tampilan juga mengontrol siapa yang dapat mencari sumber daya.

Tampilan disimpan dalam Wilayah AWS, dan mengembalikan hasil pencarian hanya dari indeks Wilayah tersebut. Jika Region berisi indeks agregator, maka tampilan menampilkan hasil pencarian dari indeks di setiap Wilayah di akun.

Tampilan multi-akun memungkinkan Anda mencari sumber daya di akun di seluruh organisasi Anda. Akun apa pun yang ingin Anda cari memerlukan indeks. Hanya akun manajemen, atau administrator yang didelegasikan untuk organisasi, yang dapat membuat tampilan multi-akun.

Penjelajah Sumber Daya AWS dapat membuat tampilan default untuk Anda selama pengaturan awal jika Anda memilih opsi yang relevan baik dalam Pengaturan Cepat untuk Resource Explorer di konsol Systems Manager atau penyiapan lanjutan. Di lain waktu, Anda dapat membuat tampilan tambahan yang memiliki filter berbeda untuk kumpulan pengguna yang berbeda.

Anda dapat membuat tampilan dengan menggunakan AWS Management Console atau dengan menjalankan AWS CLI perintah atau operasi API yang setara di AWS SDK.

Izin minimum

Untuk menjalankan prosedur ini, Anda harus memiliki izin berikut:

- Tindakan: `resource-explorer-2:CreateView`

  Sumber daya: Ini bisa * untuk memungkinkan pembuatan tampilan di akun mana pun Wilayah AWS .

AWS Management Console

Untuk membuat tampilan

1. Buka halaman Tampilan konsol Resource Explorer dan pilih Buat tampilan.
2. Pada halaman Buat tampilan, untuk Nama, masukkan nama untuk tampilan.

Nama harus tidak lebih dari 64 karakter, dan dapat mencakup huruf, digit, dan karakter tanda hubung (-). Nama harus unik di dalamnya Wilayah AWS.

3. Pilih Wilayah AWS di mana Anda ingin membuat tampilan. Untuk membuat tampilan yang mengembalikan sumber daya dari semua Wilayah di akun, pilih Wilayah AWS yang berisi indeks agregator.
4. (Opsional) Untuk Cakupan, pilih apakah pencarian Anda mengembalikan sumber daya multi-akun, atau mengembalikan sumber daya hanya dari akun Anda. Cakupan tingkat akun adalah default.

   Hanya akun manajemen atau administrator yang didelegasikan yang dapat melihat opsi untuk membuat tampilan multi-akun.
5. Pilih apakah akan memfilter hasilnya.

   - Sertakan semua sumber daya

     Tidak ada filter kueri yang disertakan. Semua sumber daya dalam indeks yang terkait dengan tampilan dapat dikembalikan dalam hasil pencarian.
   - Sertakan hanya sumber daya yang cocok dengan filter tertentu

     Mengaktifkan kotak centang Filter sumber daya di mana Anda dapat memilih nama filter dan operator. Untuk penjelasan tentang masing-masing nama filter dan operator yang tersedia, lihatFilter.
   - Pilih atribut sumber daya opsional untuk disertakan dalam hasil dari tampilan ini. Pilih kotak centang di samping Tag untuk memungkinkan pengguna mencari sumber daya berdasarkan nama dan nilai kunci tag mereka. Jika Anda tidak menyertakan tag dalam tampilan maka pengguna tidak dapat membuat permintaan pencarian yang menggunakan kunci tag dan nilai untuk memfilter hasil lebih lanjut.
   - Secara opsional, Anda dapat melampirkan tag ke tampilan. Perluas kotak Tag, dan masukkan hingga 50 pasangan kunci tag/nilai. Anda dapat menggunakan tag untuk mengkategorikan sumber daya, atau sebagai bagian dari strategi izin keamanan kontrol akses berbasis atribut (ABAC). Untuk informasi selengkapnya, lihat Menambahkan tag ke tampilan yang sudah ditonton.
   - Pilih Buat tampilan.

Konsol kembali ke halaman Penelusuran tempat Anda dapat menggunakan tampilan baru untuk melakukan pencarian.

Langkah selanjutnya: Berikan prinsipal di izin akun Anda untuk mencari dengan tampilan baru Anda. Lihat informasi yang lebih lengkap di Memberikan akses ke tampilan Resource Explorer untuk pencarian

AWS CLI

Untuk membuat tampilan

Jalankan perintah berikut untuk membuat tampilan di ditentukan Wilayah AWS. Contoh berikut membuat tampilan yang hanya mengembalikan sumber daya yang terkait dengan layanan Amazon EC2 yang ditandai dengan `Stage` kunci dan nilainya. `prod`

```
$ aws resource-explorer-2 create-view \
    --region us-west-2 \
    --view-name "My-EC2-Prod-Resources" \
    --filters FilterString="service:ec2 tag:stage=prod" \
    --included-properties Name=tags
{
    "View": {
        "Filters": {
            "FilterString": "service:ec2 tag:stage=prod"
        },
        "IncludedProperties": [
            {
                "Name": "tags"
            }
        ],
        "LastUpdatedAt": "2022-08-03T16:13:37.625000+00:00",
        "Owner": "123456789012",
        "Scope": "arn:aws:iam::123456789012:root",
        "ViewArn": "arn:aws:resource-explorer-2:us-west-2:123456789012:view/My-EC2-
Prod-Resources/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }
}
```

Untuk membuat tampilan tingkat organisasi

Contoh berikut membuat tampilan yang mengembalikan sumber daya dari seluruh organisasi Anda. Ini harus dilakukan oleh akun manajemen organisasi, atau akun administrator yang didelegasikan.

1. Jalankan `aws organizations describe-organization` perintah untuk mendapatkan ARN organisasi Anda.
2. Jalankan perintah berikut untuk membuat tampilan untuk organisasi tertentu.

```
$ aws resource-explorer-2 create-view \
    --region us-west-2 \
    --view-name entire-org-view \
    --scope "arn:aws:organizations::111111111111:organization/o-exampleorgid"
{
    "View": {
        "Filters": {
            "FilterString": ""
        },
        "IncludedProperties": [],
        "LastUpdatedAt": "2022-08-03T16:13:37.625000+00:00",
        "Owner": "111111111111",
        "Scope": "arn:aws:organizations::111111111111:organization/o-
exampleorgid",
        "ViewArn": "arn:aws:resource-explorer-2:us-west-2:111111111111:view/
entire-org-view/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }
}
```

Untuk membuat tampilan tingkat unit organisasi

Contoh berikut menciptakan tampilan yang mengembalikan sumber daya dari semua anggota unit organisasi ini. Pandangan ini berperilaku mirip dengan tampilan tingkat organisasi. Ini harus dilakukan oleh akun manajemen organisasi, atau akun administrator yang didelegasikan.

1. Jalankan `aws organizations describe-organizational-unit` perintah untuk mendapatkan ARN organisasi Anda.
2. Jalankan perintah berikut untuk membuat tampilan untuk unit organisasi tertentu.

```
$ aws resource-explorer-2 create-view \
    --region us-west-2 \
    --view-name entire-ou-view \
```

```
    --scope "arn:aws:organizations::222222222222:ou/o-exampleorgid/ou-
exampleouid"
{
    "View": {
        "Filters": {
            "FilterString": ""
        },
        "IncludedProperties": [],
        "LastUpdatedAt": "2022-08-03T16:13:37.625000+00:00",
        "Owner": "222222222222",
        "Scope": "arn:aws:organizations::222222222222:ou/o-exampleorgid/ou-
exampleouid",
        "ViewArn": "arn:aws:resource-explorer-2:us-west-2:222222222222:view/
entire-ou-view/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }
}
```

Langkah selanjutnya: Berikan prinsipal di izin akun Anda untuk mencari dengan tampilan baru Anda. Untuk informasi selengkapnya, lihat Memberikan akses ke tampilan Resource Explorer untuk pencarian

## Memberikan akses ke tampilan Resource Explorer untuk pencarian

Sebelum pengguna dapat mencari dengan tampilan baru, Anda harus memberikan akses kePenjelajah Sumber Daya AWS tampilan. Untuk melakukannya, gunakan kebijakan izin berbasis identitas ke prinsipalAWS Identity and Access Management (IAM) yang perlu mencari dengan tampilan.

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

- Pengguna dan grup diAWS IAM Identity Center:

  Buat set izin. Ikuti petunjuk di Buat set izin di PanduanAWS IAM Identity Center Pengguna.
- Pengguna yang dikelola dalam IAM melalui penyedia identitas:

  Buat peran untuk federasi identitas. Ikuti petunjuk dalam Membuat peran untuk penyedia identitas pihak ketiga (federasi) di Panduan Pengguna IAM.
- Pengguna IAM:

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

Anda dapat menggunakan salah satu metode berikut:

- Gunakan kebijakanAWS terkelola yang ada. Resource Explorer menyediakan beberapa kebijakanAWS terkelola yang telah ditentukan sebelumnya untuk Anda gunakan. Untuk detail semua kebijakanAWS terkelola yang tersedia, lihatAWS kebijakan terkelola untuk Penjelajah Sumber Daya AWS.

  Misalnya, Anda dapat menggunakan`AWSResourceExplorerReadOnlyAccess` kebijakan untuk memberikan izin pencarian ke semua tampilan di akun.
- Buat kebijakan izin Anda sendiri dan tetapkan ke prinsipal. Jika Anda membuat kebijakan sendiri, Anda dapat membatasi akses ke satu tampilan, atau subset tampilan yang tersedia dengan menentukan nama sumber daya Amazon (ARN) dari setiap tampilan dalam`Resource` elemen pernyataan kebijakan. Misalnya, Anda dapat menggunakan kebijakan contoh berikut untuk memberikan prinsipal kemampuan untuk mencari hanya menggunakan satu tampilan tersebut.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:Search",
                "resource-explorer-2:GetView"
            ],
            "Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyTestView/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
        }
    ]
}
```

Gunakan konsol IAM untuk membuat kebijakan izin dan menggunakannya dengan prinsipal yang memerlukan izin tersebut. Untuk informasi selengkapnya tentang IAM kebijakan izin, lihat topik berikut:

- Kebijakan dan izin di IAM
- Menambahkan dan menghapus izin identitas IAM
- Memahami izin yang diberikan oleh kebijakan

## Menggunakan otorisasi berbasis tanda untuk mengontrol akses ke tampilan Anda

Jika Anda memilih untuk membuat beberapa tampilan dengan filter yang mengembalikan hasil hanya dengan sumber daya tertentu, maka Anda mungkin juga ingin membatasi akses ke tampilan tersebut hanya untuk prinsipal yang perlu melihat sumber daya tersebut. Anda dapat memberikan jenis keamanan ini untuk tampilan di akun Anda dengan menggunakan strategi kontrol akses berbasis atribut (ABAC). Atribut yang digunakan oleh ABAC adalah tag yang dilampirkan baik ke prinsipal yang mencoba melakukan operasi diAWS dan ke sumber daya yang mereka coba akses.

ABAC menggunakan kebijakan izin IAM standar yang melekat pada prinsipal. Kebijakan menggunakan`Condition` elemen dalam pernyataan kebijakan untuk mengizinkan akses hanya jika tag yang dilampirkan pada prinsipal yang meminta dan tag yang dilampirkan ke sumber daya yang terpengaruh sesuai dengan persyaratan dalam kebijakan.

Misalnya, Anda dapat melampirkan tag`"Environment" = "Production"` ke semuaAWS sumber daya yang mendukung aplikasi produksi perusahaan Anda. Untuk memastikan bahwa hanya prinsipal yang diizinkan untuk mengakses lingkungan produksi yang dapat melihat sumber daya tersebut, buat tampilan Resource Explorer yang menggunakan tag tersebut sebagai filter. Kemudian, untuk membatasi akses ke tampilan hanya ke prinsipal yang sesuai, Anda memberikan izin menggunakan kebijakan yang memiliki kondisi yang mirip dengan elemen contoh berikut.

```
{
    "Effect": "Allow",
    "Action": [ "service:Action1", "service:Action2" ],
    "Resource": "arn:aws:arn-of-a-resource",
    "Condition": { "StringEquals": {"aws:ResourceTag/Environment":
 "${aws:PrincipalTag/Environment}"} }
}
```

BahwaCondition dalam contoh sebelumnya menetapkan bahwa permintaan diperbolehkan hanya jikaEnvironment tag melekat pada prinsipal membuat permintaan cocokEnvironment tag melekat sumber daya yang ditentukan dalam permintaan. Jika kedua tag tersebut tidak sama persis, atau jika salah satu tag hilang, maka Resource Explorer menolak permintaan tersebut.

> **Important**
>
> Agar berhasil menggunakan ABAC untuk mengamankan akses ke sumber daya Anda, Anda harus terlebih dahulu membatasi akses ke kemampuan untuk menambah atau memodifikasi tag yang melekat pada prinsipal dan sumber daya Anda. Jika pengguna dapat menambah atau memodifikasi tag yang dilampirkanAWS pokok atau sumber daya maka pengguna tersebut dapat memengaruhi izin yang dikendalikan oleh tag tersebut. Di lingkungan ABAC yang aman, hanya administrator keamanan yang disetujui yang memiliki izin untuk menambah atau memodifikasi tag yang dilampirkan ke prinsipal, dan hanya administrator keamanan dan pemilik sumber daya yang dapat menambahkan atau memodifikasi tag yang dilampirkan ke sumber daya.

Untuk informasi selengkapnya tentang IAM strategi ABAC strategi, lihat topik-topik berikut di Panduan Panduan Pengguna IAM:

- Tutorial IAM: Menentukan izin untuk mengaksesAWS sumber daya berdasarkan tanda
- Mengontrol akses keAWS sumber daya menggunakan tanda

Setelah Anda memiliki infrastruktur ABAC yang diperlukan, Anda dapat menggunakan mulai menggunakan tag untuk mengontrol siapa yang dapat mencari menggunakan tampilan Resource Explorer di akun Anda. Misalnya kebijakan yang menggambarkan prinsip, lihat contoh kebijakan izin berikut:

- Memberikan akses ke tampilan berdasarkan tag
- Memberikan akses untuk membuat tampilan berdasarkan tag

## Mengatur tampilan default dalamWilayah AWS

DiPenjelajah Sumber Daya AWS, Anda dapat menentukan banyak tampilan dalamWilayah AWS, di mana setiap tampilan alamat persyaratan pencarian yang berbeda. Kami menyarankan Anda menetapkan satu tampilan di setiap Wilayah sebagai tampilan default untuk Wilayah tersebut.

Resource Explorer menggunakan tampilan default setiap kali pengguna melakukan pencarian dan tidak secara eksplisit menentukan tampilan mana yang akan digunakan. Bilah pencarian terpadu di bagian atas setiapAWS Management Console halaman juga secara otomatis menggunakan tampilan default di Wilayah yang berisi indeks agregator untuk menemukan sumber daya yang cocok dengan kueri pencarian pengguna.

Anda hanya dapat memilih tampilan yang ada di Wilayah untuk menjadi tampilan default Region tersebut. Jika Wilayah lain memiliki tampilan yang ingin Anda gunakan, Anda harus terlebih dahulu membuat salinan tampilan itu di Wilayah di mana Anda ingin menjadikannya tampilan default.

> **Tip**
>
> Tidak ada operasi tampilan salinan. Anda harus membuat tampilan di Wilayah target dan kemudian menyalin pengaturan dari tampilan yang ada ke tampilan baru.

Anda dapat menentukan tampilan sebagai default untuk Regionnya dengan menggunakanAWS Management Console atau dengan menjalankanAWS CLI perintah atau operasi API yang setara dalamAWS SDK.

AWS Management Console

Untuk mengatur tampilan default

1. Pada halaman Resource Explorer Views, pilih tombol opsi di sebelah tampilan yang ingin Anda buat default untuk Regionnya.
2. Pilih Tindakan, lalu pilih Tetapkan sebagai default.

AWS CLI

Untuk mengatur tampilan default

Jalankan perintah berikut ini untuk mengatur tampilan tertentu sebagai default untuk Wilayah. Contoh berikut menetapkan tampilan yang ditentukan menjadi default untuk semua pencarian yang dilakukan di us-east-1 Region. Pandangan itu harus ada di Wilayah tempat Anda menjalankan perintah.

```
$ aws resource-explorer-2 associate-default-view \
    --region us-east-1 \
```

```
    --view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
{
    "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
}
```

# Menambahkan tag ke tampilan yang sudah ditonton

Anda dapat menambahkan tag ke tampilan Anda dapat mengkategorikannya. Tag adalah metadata yang disediakan pelanggan yang berbentuk string nama kunci dan string nilai opsional terkait. Untuk informasi umum tentang pemberian tagAWS sumber daya, lihat MenandaiAWS Sumber Daya di Referensi Umum Amazon Web Services.

## Menambahkan tag ke tampilan Anda

Anda dapat menambahkan tag ke tampilan Resource Explorer dengan menggunakanAWS Management Console atau dengan menjalankanAWS CLI perintah atau operasi API yang setara diAWS SDK.

AWS Management Console

Untuk menambahkan tag ke tampilan daya ke tampilan daya. Untuk menambahkan tag ke tampilan

1. Buka halaman Resource Explorer Views dan pilih nama tampilan yang ingin Anda tandai untuk menampilkan halaman Detail-nya.
2. Di bagian Tanda, pilih Kelola tanda.
3. Untuk menambahkan tag, pilih Tambahkan tag dan masukkan nama kunci kunci kunci kunci kunci kunci kunci kunci kunci utama dan nilai kunci kunci kunci kunci kunci kunci utama dan nilai kunci utama tag dan nilai opsional.

> **Note**
>
> Anda juga dapat menghapus tag dengan memilih X di samping tag.

Anda dapat melampirkan hingga 50 tag buatan buatan pengguna daya dapat dilampirkan hingga 50 tag daya. Setiap tag yang dibuat dan dikelola secara otomatis oleh tag yang dibuat dan dikelola secara otomatisAWS tidak dihitung masuk dalam kuota ini.

4. Setelah selesai dengan semua perubahan tag, pilih Simpan perubahan.

AWS CLI

Untuk menambahkan tag ke tampilan daya ke tampilan daya. Untuk menambahkan tag ke tampilan

Jalankan perintah berikut untuk menambahkan tag ke tampilan. Contoh berikut menambahkan tag dengan nama kuncienvironment dan nilaiproduction ke tampilan yang ditentukan.

```
$ aws resource-explorer-2 tag-resource \
    --resource-id arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --tags environment=production
```

Perintah sebelumnya tidak menghasilkan output jika berhasil.

> **Note**
>
> Untuk menghapus tag yang ada dari tampilan, gunakanuntag-resource perintah.

## Mengontrol izin dengan tag

Salah satu penggunaan utama dari penandaan adalah untuk mendukung strategi kontrol akses berbasis atribut (ABAC). ABAC dapat membantu menyederhanakan manajemen izin dengan membiarkan Anda menandai sumber daya. Kemudian, Anda memberikan izin kepada pengguna untuk sumber daya yang ditandai dengan cara tertentu.

Misalnya, pertimbangkan skenario ini. Untuk tampilan yang disebutViewA, Anda melampirkan tagenvironment=prod (key name=value). LainViewB mungkin ditandaienvironment=beta. Anda menandai peran dan pengguna Anda dengan tag dan nilai yang sama, berdasarkan lingkungan mana yang dapat diakses oleh setiap peran atau pengguna.

Kemudian, Anda dapat menetapkan kebijakan izinAWS Identity and Access Management (IAM) ke peran, grup, dan pengguna IAM Anda. Kebijakan ini memberikan izin untuk mengakses dan mencari menggunakan tampilan hanya jika peran atau pengguna yang membuat permintaan penelusuran memilikienvironment tag dengan nilai yang sama denganenvironment tag yang dilampirkan ke tampilan.

Manfaat dari pendekatan ini adalah bahwa hal itu dinamis dan tidak mengharuskan Anda untuk mempertahankan daftar siapa yang memiliki akses ke sumber daya mana. Sebagai gantinya, Anda memastikan bahwa semua sumber daya (pandangan Anda) dan prinsipal (peran dan pengguna IAM) diberi tag dengan benar. Kemudian, izin diperbarui secara otomatis tanpa Anda harus mengubah kebijakan apa pun.

## Referensi tag dalam kebijakan ABAC

Setelah tampilan Anda ditandai, Anda dapat memilih untuk menggunakan tag tersebut untuk mengontrol akses secara dinamis ke tampilan tersebut. Kebijakan contoh berikut mengasumsikan bahwa prinsipal IAM dan tampilan Anda diberi tag dengan kunci tagenvironment dan beberapa nilai. Ketika hal itu selesai, Anda dapat melampirkan kebijakan contoh berikut untuk kepala sekolah utama Anda. Peran dan pengguna Anda kemudian dapatSearch menggunakan tampilan apa pun yang ditandai dengan nilaienvironment tag yang sama persis denganenvironment tag yang dilampirkan ke prinsipal.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetView",
                "resource-explorer-2:Search"
            ],
            "Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:ResourceTag/environment": "${aws:PrincipalTag/environment}"
                }
            }
        }
    ]
}
```

Jika prinsipal dan tampilan memilikienvironment tag tetapi nilainya tidak cocok, atau jika salah satu hilangenvironment tag maka Resource Explorer menolak permintaan pencarian.

Untuk informasi selengkapnya tentang penggunaan ABAC untuk memberikan akses ke sumber daya Anda dengan aman, lihat Untuk apa ABAC ituAWS?

# Berbagi tampilan Resource Explorer

Tampilan Penjelajah Sumber Daya AWS terutama menggunakan kebijakan berbasis sumber daya untuk memberikan akses. Mirip dengan kebijakan bucket Amazon S3, kebijakan ini dilampirkan ke tampilan dan menentukan siapa yang dapat menggunakan tampilan tersebut. Ini berbeda dengan kebijakan berbasis identitas AWS Identity and Access Management (IAM). Kebijakan berbasis identitas IAM ditetapkan ke peran, grup, atau pengguna, dan menentukan tindakan dan sumber daya yang dapat diakses oleh peran, grup, atau pengguna. Anda dapat menggunakan salah satu jenis kebijakan dengan tampilan Resource Explorer, sebagai berikut:

- Dalam akun manajemen atau akun administrator yang didelegasikan yang memiliki sumber daya, gunakan salah satu jenis kebijakan untuk memberikan akses, asalkan tidak ada kebijakan lain yang secara eksplisit menolak akses ke tampilan untuk prinsipal tersebut.
- Di seluruh akun, Anda harus menggunakan kedua jenis kebijakan. Kebijakan berbasis sumber daya yang dilampirkan pada tampilan di akun berbagi mengaktifkan berbagi dengan akun konsumsi lain. Namun, kebijakan tersebut tidak memberikan akses ke pengguna individu atau peran dalam akun konsumen. Administrator di akun konsumsi juga harus menetapkan kebijakan berbasis identitas ke peran dan pengguna yang diinginkan dalam akun konsumsi. Kebijakan tersebut memberikan akses ke nama sumber daya Amazon (ARN) tampilan.

Untuk berbagi tampilan dengan akun lain, Anda harus menggunakan AWS Resource Access Manager (AWS RAM). AWS RAMmenangani kompleksitas kebijakan berbasis sumber daya untuk Anda. Sebelum Anda dapat berbagi, Anda harus mengikuti langkah-langkah ini untuk mengaktifkan pencarian multi-akun.

Untuk berbagi tampilan, Anda harus menjadi akun manajemen organisasi atau administrator yang didelegasikan. Anda menentukan akun atau identitas yang ingin Anda bagikan sumber daya. AWS RAMsepenuhnya mendukung tampilan Resource Explorer. AWS RAMmenggunakan kebijakan yang serupa dengan yang dijelaskan di bagian berikut, berdasarkan jenis prinsipal yang Anda pilih untuk dibagikan. Untuk petunjuk tentang cara berbagi sumber daya, lihat Berbagi AWS sumber daya Anda di Panduan AWS Resource Access Manager Pengguna.

Administrator dan administrator yang didelegasikan dapat membuat dan berbagi 3 jenis tampilan: tampilan lingkup organisasi, tampilan lingkup unit organisasi (OU), dan tampilan cakupan tingkat akun. Mereka dapat berbagi dengan organisasi, OU, atau akun. Saat akun bergabung atau keluar dari organisasi, AWS RAM secara otomatis memberikan atau mencabut tampilan bersama.

## Kebijakan izin untuk berbagi tampilan dengan Akun AWS

Contoh kebijakan berikut menunjukkan bagaimana Anda dapat membuat tampilan tersedia untuk prinsipal dalam dua hal yang berbeda: Akun AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [ "111122223333", "444455556666" ]
            },
            "Action": [
                "resource-explorer-2:Search",
                "resource-explorer-2:GetView",
            ],
            "Resource": "arn:aws:resource-explorer-2:us-
east-1:123456789012:view/policy-name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
            "Condition": {"StringEquals": {"aws:PrincipalOrgID": "o-123456789012"},
                "StringNotEquals": {"aws:PrincipalAccount": "123456789012"}
            }
        }
    ]
    }"
}
```

Administrator di setiap akun yang ditentukan sekarang harus menentukan peran dan pengguna mana yang dapat mengakses tampilan dengan melampirkan kebijakan izin berbasis identitas ke peran, grup, dan pengguna. Administrator akun 111122223333 atau 444455556666 dapat membuat contoh kebijakan berikut. Kemudian, mereka dapat menetapkan kebijakan ke peran, grup, dan pengguna di akun tersebut yang diizinkan untuk mencari menggunakan tampilan yang dibagikan dari akun asal.

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

```
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:Search",
                "resource-explorer-2:GetView",
            "Resource": "arn:aws:resource-explorer-2:us-
east-1:123456789012:view/policy-name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
        }
    ]
}
```

Anda dapat menggunakan kebijakan berbasis identitas IAM ini sebagai bagian dari strategi keamanan kontrol akses berbasis atribut (ABAC). Dalam paradigma itu, Anda memastikan bahwa semua sumber daya Anda dan semua identitas Anda ditandai. Kemudian, Anda menentukan dalam kebijakan Anda kunci dan nilai tag mana yang harus cocok antara identitas dan sumber daya agar akses diizinkan. Untuk informasi tentang menandai tampilan di akun Anda, lihatMenambahkan tag ke tampilan yang sudah ditonton. Untuk informasi selengkapnya tentang kontrol akses berbasis atribut, lihat Untuk apa ABAC? AWS dan Mengontrol akses ke AWS sumber daya menggunakan tag, baik di Panduan Pengguna IAM.

## Menghapus tampilan di Resource Explorer

Bila Anda tidak lagi memerlukanPenjelajah Sumber Daya AWS tampilan, Anda dapat menghapusnya. Anda dapat menghapus tampilan dengan menggunakanAWS Management Console atau dengan menjalankanAWS CLI perintah atau operasi API yang setara diAWS SDK.

> **Note**
>
> Anda tidak dapat menghapus tampilan yang saat ini ditetapkan sebagai default untuk tampilan tersebutWilayah AWS. Untuk menghapus tampilan, Anda harus menghapus tampilan sebagai default. Untuk melakukan ini, Anda dapat menjalankan operasi DisassociateDefaultViewAPI di Wilayah tersebut.

Izin minimum

Untuk menjalankan prosedur ini, Anda harus memiliki izin berikut:

- Tindakan:`resource-explorer-2:DeleteView`

Sumber Daya: ARN tampilan yang akan dihapus

### AWS Management Console

#### Menghapus tampilan

1. Pada halaman Tampilan konsol Resource Explorer, pilih tombol opsi di sebelah tampilan yang ingin Anda hapus.
2. Pilih Actions (Tindakan), lalu pilih Delete (Hapus).
3. Dalam kotak dialog konfirmasi, ketik nama tampilan, dan kemudian pilih Hapus.

### AWS CLI

#### Menghapus tampilan

Jalankan perintah berikut untuk menghapus tampilan dengan Amazon Resource Name (ARN).

```
$ aws resource-explorer-2 delete-view \
    --view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
{
    "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
}
```

# MenggunakanPenjelajah Sumber Daya AWSuntuk mencari sumber daya

Tujuan utama mengaktifkanPenjelajah Sumber Daya AWSdi dalam kamuAkun AWSadalah untuk memungkinkan pengguna Anda untuk mencari sumber daya di akun. GunakanAWS Management ConsoleatauAWS Command Line Interface(AWS CLI) untuk mencari sumber daya menggunakan Resource Explorer.

Berikut ini adalah beberapa karakteristik utama pencarian Resource Explorer.

- Setiap pencarian harus menggunakan tampilan.

  Tampilan adalah apa yang digunakan Resource Explorer untuk menentukan siapa yang memiliki izin untuk melihat sumber daya mana. Untuk menggunakan tampilan dalam operasi pencarian Resource Explorer, pengguna harus memiliki`Allow`pada`resource-explorer-2:Search`operasi untuk tampilan yang ditentukan. Izin ini berasal darikebijakan izin berbasis identitasmelekat pada kepala sekolah membuat permintaan.

  Tampilan dapat menyertakan filter yang membatasi sumber daya mana yang dapat dimasukkan dalam hasil. Dengan membuat tampilan berbeda yang menggunakan filter dan dengan memberikan akses prinsipal yang berbeda ke tampilan yang berbeda, Anda dapat mengonfigurasi lingkungan di mana setiap kelompok pengguna hanya dapat melihat sumber daya yang relevan dengannya.

  Untuk informasi selengkapnya tentang penayangan, lihatMengelola tampilan Resource Explorer untuk menyediakan akses ke penelusuran.
- Resource Explorer menggunakan proses latar belakang asinkron untuk mempertahankan indeksnya.

  Diperlukan Resource Explorer beberapa waktu untuk proses pengindeksan untuk menemukan sumber daya yang baru dibuat atau dimodifikasi dan menambahkannya ke indeks lokal. Diperlukan waktu tambahan bagi Resource Explorer untuk mereplikasi perubahan indeks lokal ke indeks agregator.

  Hal yang sama berlaku untuk sumber daya yang Anda hapus. Hal ini dapat mengambil beberapa waktu setelah Anda menghapus sumber daya untuk penghapusan yang akan ditemukan oleh proses pengindeksan dan informasi sumber daya yang akan dihapus dari indeks lokal. Waktu

tambahan diperlukan untuk Resource Explorer untuk mereplikasi penghapusan dari indeks lokal ke indeks agregator akun.

Penambahan, modifikasi, dan penghapusan sumber daya dapat memakan waktu maksimal 36 jam bagi Resource Explorer untuk menampilkan perubahan tersebut dalam hasil penelusuran di semua Wilayah tempat Anda mengaktifkan Resource Explorer.

- Pencarian di Resource Explorer terjadi dalamWilayah AWS.

  Setiap Wilayah tempat Anda mengaktifkan Resource Explorer berisi indeks hanya sumber daya yang disimpan di Wilayah tersebut. Tampilan juga terkait dengan Regions, dan hanya dapat mengembalikan sumber daya yang ditemukan dalam indeks Region tersebut. Satu pengecualian untuk ini adalah indeks agregator, yang menerima salinan direplikasi dari semua indeks lokal untuk mendukung pencarian di semua Wilayah di akun.
- Pencarian lintas wilayah memerlukan indeks agregator untuk akun tersebut.

  Untuk memungkinkan pengguna mencari sumber daya di semuaWilayah AWS, administrator harus menunjuk satu Wilayah untuk memuat indeks agregator untuk akun tersebut. Salinan setiap indeks lokal secara otomatis direplikasi ke indeks agregator.

  Karena itu, hanya tampilan dalam indeks agregator Region yang dapat mengembalikan hasil yang menyertakan sumber daya dari semuaWilayah AWSdi akun.
- Sebuah query terdiri dari sejumlah bentuk bebas kata kunci teks dan filter.

  Kata kunci bebas-bentuk digabungkan dalam query menggunakan logis**OR**operator. Filter yang menggunakan nama filter yang ditentukan Resource Explorerdigabungkan dalam query menggunakan logis**AND**operator. Pertimbangkan contoh query berikut.

  ```
  test instance service:EC2 region:us-west-2
  ```

  Ini dievaluasi oleh Resource Explorer sebagai berikut.

  ```
  test OR instance AND service:EC2 AND region:us-west-2
  ```

  Kueri ini mengharuskan sumber daya yang cocok harus merupakan sumber daya Amazon EC2 di Wilayah AS Barat (Oregon), dan memiliki setidaknya satu kata kunci (uji,contoh) dilampirkan dalam beberapa cara, seperti dalam nama, deskripsi, atau tag.

> **Note**
>
> Karena implisitAND, Anda dapat berhasil menggunakan hanya satu filter untuk atribut yang hanya dapat memiliki satu nilai yang terkait dengan sumber daya. Misalnya, sumber daya dapat menjadi bagian dari hanya satuWilayah AWS. Oleh karena itu, query berikut tidak mengembalikan hasil.
>
> ```
> region:us-east-1 region:us-west-1
> ```
>
> Keterbatasan ini tidaktidakberlaku untuk filter untuk atribut yang dapat memiliki beberapa nilai pada saat yang sama, sepertitag:,tag.key:, dantag.value:.

- Pencarian hanya dapat mengembalikan 1.000 hasil pertama.

  Persyaratan ini mencakup pencarian dengan string kueri kosong yang cocok dengan semua sumber daya. Untuk melihat sumber daya di luar 1.000 yang dikembalikan oleh string kueri kosong, Anda harus menggunakan kueri untuk membatasi hasil yang cocok dengan yang ingin Anda lihat dan membatasi jumlah kecocokan hingga kurang dari 1.000.

- Ada kuota per akun pada jumlah operasi pencarian yang dapat Anda lakukan.

  Kuota membatasi berapa banyak kueri yang dapat Anda buat per detik, dan berapa banyak kueri yang dapat Anda buat setiap bulan. Untuk nomor kuota tertentu, lihatKuota untuk Resource Explorer.

AWS Management Console

Untuk mencari sumber daya menggunakan Resource Explorer

1. PadaPencarian sumber dayahalaman, mulailah dengan memilih tampilan yang ingin Anda gunakan. Anda dapat memilih dari antara hanya pandangan yang Anda memiliki izin untuk mengakses.
2. UntukKueri, masukkan istilah pencarian dansaringanyang mengidentifikasi sumber daya yang ingin Anda lihat. Untuk informasi tentang semua opsi sintaks yang tersedia, lihatReferensi sintaks kueri pencarian untuk Resource Explorer.
3. TekanMemasukkanuntuk mengirimkan permintaan Anda.

Resource Explorer menampilkan semua hasil yang cocok dengan`Filter`didefinisikan dalam tampilan dan`Query`yang Anda berikan. Hasilnya diurutkan berdasarkan relevansi, dengan sumber daya yang cocok dengan lebih banyak istilah kueri Anda yang muncul lebih tinggi dalam daftar dan sumber daya yang cocok dengan lebih sedikit istilah yang muncul lebih jauh ke bawah daftar.

4. Pilih pengenal sumber daya untuk menavigasi ke konsol asli jenis sumber daya tersebut, tempat Anda dapat berinteraksi dengan sumber daya dalam semua cara yang didukung oleh layanan tersebut.

AWS CLI

Untuk mencari sumber daya menggunakan Resource Explorer

Jalankan perintah berikut untuk mencari sumber daya menggunakan tampilan yang ditentukan. Tampilan itu harus ada di Wilayah tempat Anda menjalankan operasi. Contoh berikut mencari instans Amazon EC2 yang ditandai`env=production`di AS Timur (Ohio) (kami-timur-2). Untuk informasi tentang semua opsi sintaks yang tersedia untuk`query-string`parameter, lihatReferensi sintaks kueri pencarian untuk Resource Explorer.

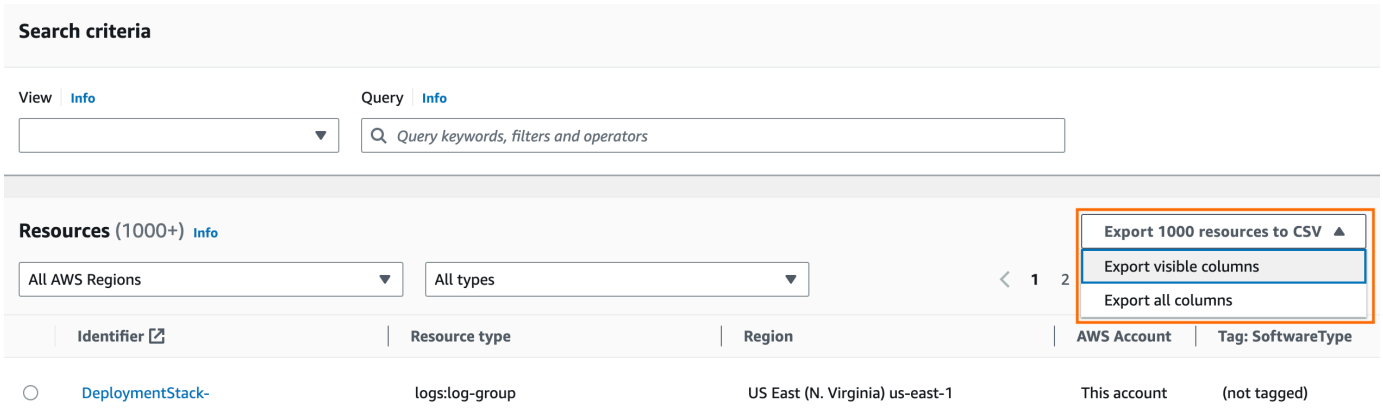
```
$ aws resource-explorer-2 search \
    --region us-east-1 \
    --query-string "resourcetype:AWS::EC2::Instance tag:env=production"
    --view-arn arn:aws:resource-explorer-2:us-east-2:123456789012:view/My-Resources-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

# Ekspor hasil pencarian ke file.csv

Anda dapat mengekspor hasilPencarian sumber dayaquery ke nilai dipisahkan koma (.csv) berkas. File.csv mencakup pengenal, jenis sumber daya, Wilayah,Akun AWS, jumlah total tag, dan kolom untuk setiap kunci tag unik dalam koleksi. File.csv dapat membantu Anda mengonfigurasiAWSsumber daya di organisasi Anda, atau tentukan di mana terdapat tumpang tindih atau ketidakkonsistenan dalam memberi tag di seluruh sumber daya.

1. Dalam hasilPencarian sumber dayaquery, pilihEkspor sumber daya ke CSV.

   Anda dapat memilih untuk mengekspor hasil Anda hanya dengan kolom yang saat ini dapat Anda lihat, atau ekspor dengan semua kolom yang tersedia.




2. Ketika Anda diminta oleh browser Anda, pilih untuk membuka file.csv, atau menyimpannya ke lokasi yang nyaman.

# Referensi sintaks kueri pencarian untuk Resource Explorer

Penjelajah Sumber Daya AWS membantu Anda menemukan AWS sumber daya individu di Anda Akun AWS. Untuk membantu Anda menemukan sumber daya yang tepat yang Anda cari, Resource Explorer menerima string kueri penelusuran yang mendukung sintaks yang dijelaskan dalam topik ini. Misalnya kueri yang menunjukkan cara menggunakan fitur yang dijelaskan di sini, lihatContoh permintaan pencarian Resource Explorer.

> **Note**
>
> Pada saat ini, tag yang dilampirkan ke sumber daya AWS Identity and Access Management (IAM), seperti peran atau pengguna, tidak diindeks.

## Cara kerja kueri di Resource Explorer

Kueri penelusuran selalu menggunakan tampilan. Jika Anda tidak menentukannya secara eksplisit, Resource Explorer menggunakan tampilan yang ditetapkan sebagai default untuk tempat Wilayah AWS Anda bekerja.

Tampilan menentukan sumber daya mana yang tersedia untuk Anda kueri. Anda dapat membuat tampilan berbeda yang masing-masing mengembalikan kumpulan sumber daya yang berbeda.

Misalnya, Anda dapat membuat tampilan yang hanya menyertakan sumber daya yang ditandai dengan kunci `Environment` dan nilainya`Production`. Kemudian, Anda dapat memilih untuk memberikan akses untuk tampilan itu hanya kepada pengguna yang memiliki alasan bisnis untuk melihat sumber daya tersebut. Tampilan terpisah yang mencakup sumber daya `Alpha` atau `Beta` lingkungan dapat diakses oleh pengguna yang berbeda yang perlu melihat sumber daya tersebut. Untuk informasi tentang mengontrol siapa yang mendapatkan akses ke tampilan mana, lihatMemberikan akses ke tampilan Resource Explorer untuk pencarian.

## Sintaks string kueri

Bagian ini memberikan informasi tentang aspek dasar sintaks kueri, filter, dan operator filter.

## Hal-hal mendasar

Pada dasarnya, a `QueryString` adalah satu set kata kunci teks bentuk bebas yang secara implisit bergabung dengan operator logis. **`OR`** Pisahkan setiap kata kunci dari yang lain dengan menggunakan spasi, seperti yang ditunjukkan pada contoh berikut:

```
ec2 billing test gamma
```

Resource Explorer mengevaluasi daftar kata kunci ini berarti:

```
ec2 OR billing OR test OR gamma
```

Resource Explorer mengurutkan hasil berdasarkan relevansi, memberikan preferensi yang lebih tinggi ke sumber daya yang cocok dengan jumlah istilah pencarian yang lebih banyak. Sumber daya yang tidak cocok dengan satu atau beberapa persyaratan tidak dikecualikan dari hasil. Namun, Resource Explorer menganggapnya memiliki relevansi yang lebih rendah dan mendorongnya lebih jauh ke bawah dalam hasil pencarian.

Jika Anda menentukan string kosong untuk `QueryString` parameter, kueri Anda mengembalikan 1.000 sumber daya pertama yang tersedia melalui tampilan yang digunakan untuk operasi. Jumlah maksimum sumber daya yang dapat dikembalikan oleh kueri apa pun adalah 1.000.

> **Note**
>
> AWS berhak memperbarui logika pencocokan dan algoritma relevansi untuk mengevaluasi kata kunci teks bentuk bebas sehingga kami dapat memberikan hasil yang paling relevan kepada pelanggan. Oleh karena itu, hasil yang dikembalikan untuk kueri yang sama menggunakan kata kunci teks bentuk bebas mungkin berubah seiring waktu. Jika Anda memerlukan hasil yang lebih deterministik, kami sarankan Anda menggunakan filter. Logika pencocokan filter tidak berubah seiring waktu.

## Filter

Anda dapat membatasi hasil kueri Anda lebih ketat dengan memasukkan filter. Tidak seperti kata kunci teks, filter dievaluasi dalam kueri dengan operator AND. Misalnya, pertimbangkan kueri berikut yang terdiri dari dua kata kunci bentuk bebas dan dua filter:

```
test instance service:EC2 region:us-west-2
```

Kueri ini dievaluasi sebagai berikut:

```
( test OR instance ) AND service:EC2 AND region:us-west-2
```

Filter selalu dievaluasi menggunakan operator logis AND. Jika sumber daya tidak cocok dengan filter, sumber daya tersebut tidak disertakan dalam hasil. Hasil kueri contoh mencakup sumber daya apa pun yang terkait dengan Amazon EC2 dan berada di AS Barat (Oregon) Wilayah AWS dan memiliki setidaknya satu kata kunci yang dilampirkan dalam beberapa cara.

> **Note**
>
> Karena implisitAND, Anda dapat berhasil menggunakan hanya satu filter untuk atribut yang hanya dapat memiliki satu nilai yang terkait dengan sumber daya. Misalnya, sumber daya hanya dapat menjadi bagian dari satu Wilayah AWS. Oleh karena itu, query berikut tidak mengembalikan hasil.
>
> ```
> region:us-east-1 region:us-west-1
> ```
>
> Batasan ini tidak berlaku untuk filter untuk atribut yang dapat memiliki beberapa nilai pada saat yang sama, seperti`tag:`,`tag.key:`, dan`tag.value:`.

Tabel berikut mencantumkan nama filter yang tersedia yang dapat Anda gunakan dalam kueri penelusuran Resource Explorer.

| Nama filter | Deskripsi dan contoh |
| --- | --- |
| `accountid:` | Akun AWS Yang memiliki sumber daya. Resource Explorer termasuk dalam hasil hanya sumber daya yang dimiliki oleh akun yang ditentukan.<br><br>`accountid:123456789012` |
| `applicati on:` | Filter ini memungkinkan Anda untuk mencari sumber daya dengan kunci `awsApplication` tag dan nilai grup sumber daya. Anda dapat mencari berdasarkan nama aplikasi atau grup sumber daya aplikasi ARN.<br><br>`application:MyApplicationName` |

| Nama filter | Deskripsi dan contoh |
| --- | --- |
| | `application:arn:aws:resource-groups: us-east-1 :123456789012:group/MyApplicationName/123456789abced`<br><br>`arn:aws:resource-groups: us-east-1 :123456789012:group/MyApplicationName/123456789abced`<br><br>**Note**<br>Untuk menggunakan filter ini, tampilan Anda harus memiliki akses ke data penandaan. |
| `id:` | Pengidentifikasi sumber daya individu, dinyatakan sebagai nama sumber daya Amazon (ARN).<br><br>`id:arn:aws:license-manager: us-east-1 :123456789012:license-configuration:lic-ecbd5574fd92cb0d312baea26EXAMPLE` |
| `region:` | Di Wilayah AWS mana sumber daya berada. Resource Explorer termasuk dalam hasil hanya sumber daya yang berada di ditentukan Wilayah AWS.<br><br>`region:us-east-1`<br><br>**Note**<br>Mengetik hanya kode Wilayah (tanpa filter, seperti`us-east-1` ) tidak mengembalikan hasil yang sama seperti`region:us-east-1` . Hasil ini karena, sebagai kata kunci teks bentuk bebas yang bukan filter, kode Wilayah dipecah menjadi potongan-potongan individua lnya. Misalnya, `us-east-1` dicari sebagai`us`,`east`, dan`1`. Perincian menjadi komponen ini tidak terjadi saat Anda menggunakan `region:` awalan. |

| Nama filter | Deskripsi dan contoh |
| --- | --- |
| `region:global` | Kasus khusus untuk `region:` filter yang dapat Anda gunakan untuk menemukan sumber daya yang tidak terkait dengan individu Wilayah AWS tetapi dianggap cakupan global.<br><br>`region:global`<br><br>**Note**<br>Mengetik hanya kata kunci `global` tidak mengembalikan hasil yang sama `region:global` karena kata literal “global” tidak melekat pada sumber daya global. Mengetik `global` sebagai kata kunci hanya mengembalikan sumber daya yang memiliki string literal yang terkait dengan sumber daya. |
| `resourcetype:` | Jenis sumber daya dalam *`service`*`:`*`type`* notasi. Resource Explorer termasuk dalam hasil hanya sumber daya dari jenis yang ditentukan.<br><br>`resourcetype:ec2:instance` |
| `resourcetype.supports:` | Filter ini memungkinkan Anda untuk mencari sumber daya yang mendukung tag. `tags`adalah satu-satunya nilai yang didukung. Resource Explorer menyertakan dalam hasil hanya sumber daya yang dapat diberi tag.<br><br>`resourcetype.supports:tags` |
| `service:` | Layanan AWS Yang terkait dengan jenis sumber daya. Resource Explorer termasuk dalam hasil hanya sumber daya yang dibuat dan dikelola oleh layanan yang ditentukan.<br><br>`service:ec2` |
| `tag:` | Sebuah pasangan kunci tag/nilai dinyatakan sebagai. `<key>=<value>` Resource Explorer menyertakan dalam hasil hanya sumber daya yang memiliki tag dengan kunci yang cocok dan nilai yang ditentukan.<br><br>`tag:environment=production` |

| Nama filter | Deskripsi dan contoh |
| --- | --- |
| `tag:none` | Kasus khusus `tag:` filter yang memungkinkan Anda mencari sumber daya apa pun yang tidak memiliki tag yang dibuat pengguna.<br><br>**Note**<br>Sumber daya dengan tag AWS yang dibuat layanan masih muncul di hasil untuk filter ini. |
| `tag.key:` | Kunci tag. Resource Explorer menyertakan dalam hasil hanya sumber daya yang memiliki tag dengan kunci yang cocok, terlepas dari nilainya.<br><br>`tag.key:environment` |
| `tag.value:` | Nilai tag. Resource Explorer menyertakan dalam hasil hanya sumber daya yang memiliki tag dengan nilai yang cocok, terlepas dari nama kuncinya.<br><br>`tag.value:production` |

## Operator filter

Anda dapat memodifikasi kata kunci dan filter dengan menyertakan salah satu operator yang ditampilkan dalam tabel berikut sebagai bagian dari string.

| Operator | Deskripsi dan contoh |
| --- | --- |
| "*multiple word phrase*"<br><br>atau<br><br>“*frase tanda hubung*” | Kelilingi frase multi-kata yang harus diperlakukan sebagai kata kunci tunggal dengan tanda kutip ganda karakter (). " " Resource Explorer hanya mencakup sumber daya yang cocok dengan seluruh frasa, dengan semua kata bersama-sama, dan dalam urutan yang ditentukan.<br><br>Jika Anda tidak menggunakan tanda kutip ganda, Resource Explorer memecah frasa menjadi komponennya dengan spasi atau tanda hubung, dan menyertak an sumber daya yang cocok dengan masing-masing komponen, meskipun tidak bersama-sama atau dalam urutan yang berbeda. Kutipan harus ada di sekitar segalanya setelah operator. |

| Operator | Deskripsi dan contoh |
| --- | --- |
| | `"This matches only resources with the whole sentence."`<br><br>`This matches resources with any of the words.`<br><br>`"us-east-1"` — hanya cocok dengan sumber daya yang terkait dengan Wilayah yang tepat itu.<br><br>`us-east-1` — cocok dengan sumber daya apa pun yang berisi “kami” atau “timur” atau “1".<br><br>`-tag:"enviornment=production"` |
| *`keyword`*`*` | Pencocokan wildcard awalan. Anda dapat menempatkan karakter wildcard (tanda bintang*) hanya di akhir string. Resource Explorer menyertakan dalam hasil hanya sumber daya dengan nilai yang dimulai dengan teks awalan sebelum. * Contoh berikut cocok dengan semua Wilayah AWS yang dimulai`us-east`.<br><br>`region:us-east*`<br><br>**Important**<br>Pencarian terpadu secara otomatis menyisipkan operator karakter wildcard (*) di akhir kata kunci pertama dalam string. Ini berarti bahwa hasil pencarian terpadu menyertakan sumber daya yang cocok dengan string apa pun yang dimulai dengan kata kunci yang ditentukan. Pencarian yang dilakukan oleh kotak teks Kueri pada halaman pencarian Sumber daya di konsol Resource Explorer tidak secara otomatis menambahkan karakter wildcard. Anda dapat memasukkan secara * manual setelah istilah apa pun dalam string pencarian. |

| Operator | Deskripsi dan contoh |
| --- | --- |
| `-keyword` | Notoperator. Anda dapat menempatkan tanda hubung (`-`) di awal kata kunci atau filter untuk membalikkan hasil pencarian. Resource Explorer mengecual ikan dari hasil sumber daya apa pun yang cocok dengan kata kunci atau filter yang mengikuti operator ini. Contoh berikut menyebabkan semua sumber daya yang terkait dengan layanan Amazon EC2 dikecualikan dari hasil.<br><br>`-service:ec2`<br><br>**Important**<br><br>Jika Anda menggunakan AWS CLI `search` perintah dan nilai `--query-string` parameter Anda memiliki `-` operator sebagai karakter pertama, Anda harus memisahkan nama parameter dari nilainya dengan karakter tanda sama dengan (=) alih-alih karakter spasi biasa. Jika Anda menggunakan karakter spasi, CLI salah menafsirkan string. Misalnya, kueri berikut gagal.<br><br>`aws resource-explorer-2 search --query-string "-tag:none region:us-east-1"`<br><br>String kueri yang dikoreksi berikut, dengan = mengganti spasi, berfungsi seperti yang diharapkan.<br><br>`aws resource-explorer-2 search --query-string ="-tag:none region:us-east-1"`<br><br>Jika Anda mengubah urutan filter dalam string kueri sehingga `-` bukan karakter pertama dalam nilai parameter, Anda dapat menggunakan karakter spasi standar. String query berikut berfungsi.<br><br>`aws resource-explorer-2 search --query-string "region:us-east-1 -tag:none"` |

| Operator | Deskripsi dan contoh |
| --- | --- |
| `\<special character>` | Anda dapat melarikan diri dari karakter khusus yang harus disertakan persis seperti yang ditunjukkan daripada ditafsirkan. Jika teks Anda menyertakan salah satu karakter khusus ( `* " - : = \`), Anda harus mendahului karakter tersebut dengan garis miring terbalik (\) untuk memastikan bahwa karakter tersebut diambil secara harfiah. Contoh berikut menunjukkan cara menggunak an kata kunci teks bentuk bebas yang menyertakan tanda hubung (-) karakter (). `"my-key-word"`<br><br>Selain itu, untuk mencegah Resource Explorer memecah ekspresi pada tanda hubung menjadi tiga kata kunci terpisah, Anda dapat mengelilingi seluruh frasa dalam tanda kutip ganda.<br><br>`"my\-key\-word"`<br><br>Untuk menyisipkan garis miring terbalik literal, masukkan dua karakter garis miring terbalik berturut-turut. Garis miring terbalik pertama ditafsirkan sebagai escape dan backslash kedua adalah karakter literal untuk disisipkan.<br><br>`"some_text\\some_more_text"` |

> **Note**
>
> Jika tampilan menyertakan tag yang dilampirkan ke sumber daya, maka `Search` operasi tidak menampilkan kesalahan validasi untuk string pencarian, karena filter yang tidak valid juga dapat ditafsirkan sebagai pencarian teks bentuk bebas. Misalnya, meskipun `cat:blue` terlihat seperti filter, Resource Explorer tidak dapat menguraikannya sebagai satu karena `cat:` bukan salah satu filter yang valid dan ditentukan. Sebagai gantinya Resource Explorer menafsirkan seluruh string sebagai string pencarian bentuk bebas untuk memungkinkannya mencocokkan hal-hal seperti nama kunci tag atau sepotong ARN.
> Operasi ini memunculkan kesalahan validasi jika salah satu dari berikut ini benar:
>
> - Tampilan tidak menyertakan informasi tentang tag

- Kueri penelusuran secara eksplisit menggunakan filter tag (`tag.key:`,`tag.value:`, atau) `tag:`

# Contoh permintaan pencarian Resource Explorer

Contoh berikut menunjukkan sintaks untuk jenis umum dari query yang dapat Anda gunakan dalamPenjelajah Sumber Daya AWS.

> **Important**
>
> Jika Anda menggunakanAWS CLI`search` perintah dan nilai`--query-string` parameter Anda memiliki`-` operator sebagai karakter pertama, Anda harus memisahkan nama parameter dari nilainya dengan karakter tanda yang sama (=) alih-alih karakter spasi biasa. Jika Anda menggunakan karakter spasi, CLI salah menafsirkan string. Misalnya, kueri berikut gagal:
>
> ```
> aws resource-explorer-2 search --query-string "-tag:none region:us-east-1"
> ```
>
> Berikut dikoreksi query, dengan= mengganti ruang, bekerja seperti yang diharapkan.
>
> ```
> aws resource-explorer-2 search --query-string="-tag:none region:us-east-1"
> ```
>
> Jika Anda mengubah urutan filter dalam string kueri sehingga`-` bukan karakter pertama dalam nilai parameter, Anda dapat menggunakan karakter ruang standar. Query berikut bekerja.
>
> ```
> aws resource-explorer-2 search --query-string "region:us-east-1 -tag:none"
> ```

## Pencarian untuk sumber daya yang tidak ditandai

Jika Anda ingin menggunakan kontrol akses berbasis atribut (ABAC) di akun Anda, menggunakan alokasi berbasis biaya, atau melakukan otomatisasi berbasis tag terhadap sumber daya Anda, Anda perlu mengetahui sumber daya mana di akun Anda yang mungkin kehilangan tag. Contoh kueri berikut menggunakan tag filter kasus khusus: none untuk mengembalikan semua sumber daya yang hilang tag buatan pengguna.

`tag:none`Filter hanya berlaku untuk tag yang dibuat oleh pengguna. Tag yang dihasilkan dan dikelola olehAWS dibebaskan dari filter ini dan masih muncul dalam hasil.

```
tag:none
```

Untuk juga mengecualikan semua tag sistem yangAWS dibuat, tambahkan filter kedua seperti yang ditunjukkan dalam contoh berikut. Elemen pertama dalam string kueri menduplikasi contoh sebelumnya dengan memfilter semua tag yang dibuat pengguna. AWStag sistem yang dibuat selalu dimulai dengan huruf-hurufnya`aws`. Oleh karena itu, Anda dapat menggunakan operator NOT logis (-) dengan filter tag.key untuk juga mengecualikan sumber daya apa pun yang memiliki tag dengan nama kunci yang dimulai dengan`aws`.

```
tag:none -tag.key:aws*
```

## Cari sumber daya yang diberi tag

Untuk menemukan semua sumber daya yang memiliki tag jenis apa pun, Anda dapat menggunakan operator NOT logis (-) dengan tag kasus khusus: tidak ada filter sebagai berikut.

```
-tag:none
```

## Mencari sumber daya yang kehilangan tag tertentu

Juga terkait dengan ABAC, Anda mungkin ingin mencari semua sumber daya yang tidak memiliki tag dengan kunci tertentu. Contoh berikut menggunakan operator NOT logis`-` untuk mengembalikan semua sumber daya yang hilang tag dengan nama kunci`Department`.

```
-tag.key:Department
```

## Mencari sumber daya yang memiliki nilai tag tidak valid

Untuk alasan kepatuhan, Anda mungkin ingin mencari semua sumber daya yang memiliki nilai tag yang hilang atau salah eja pada tag penting. Contoh berikut mengembalikan semua sumber daya yang memiliki tag dengan nama kunci`environment`. Namun, kueri menyaring sumber daya apa pun yang memiliki salah satu nilai yang valid`prod`,`integ`, atau`dev`. Setiap hasil yang muncul dari kueri ini memiliki beberapa nilai lain yang harus Anda selidiki dan diperbaiki.

> **Important**
>
> Pencarian Resource Explorer tidak peka huruf besar dan tidak dapat membedakan antara nama kunci dan nilai yang hanya berbeda berdasarkan cara mereka dikapitalisasi. Misalnya, nilai-nilai dalam contoh berikut cocokPROD,prod,Prod, atau variasi apapun. Namun, beberapa aplikasi menggunakan tag dalam cara-case-sensitive. Kami menyarankan Anda untuk menstandarisasi strategi kapitalisasi untuk organisasi Anda, seperti hanya menggunakan nama dan nilai kunci tag huruf kecil. Pendekatan yang konsisten dapat membantu menghindari kebingungan yang dapat disebabkan oleh memiliki tag yang hanya berbeda dengan cara mereka dikapitalisasi.

```
tag.key:environment -tag:environment=prod -tag:environment=integ -tag:environment=dev
```

## Cari sumber daya dalam subsetWilayah AWS

Gunakan operator`'*'` wildcard untuk mencocokkan semua Wilayah di area tertentu di dunia. Contoh berikut mengembalikan semua sumber daya yang ada di Wilayah di Eropa (UE).

```
region:eu-*
```

## Cari sumber daya global

Gunakan`global` nilai kasus khusus untuk`region:` filter untuk menemukan sumber daya Anda yang dianggap global dan tidak terkait dengan Wilayah individual.

```
region:global
```

## Cari sumber daya dari jenis tertentu yang terletak di Wilayah tertentu

Bila Anda menggunakan beberapa filter, Resource Explorer mengevaluasi ekspresi dengan menggabungkan awalan dengan`AND` operator logis implisit. Contoh berikut menampilkan semua sumber daya yang ada di Wilayah Asia Pacific (Hong Kong)`AND` adalah instans Amazon EC2.

```
region:ap-east-1 resourcetype:ec2:instance
```

> **Note**
>
> Karena implisitAND, Anda dapat berhasil menggunakan hanya satu filter untuk atribut yang hanya dapat memiliki satu nilai yang terkait dengan sumber daya. Misalnya, sumber daya dapat menjadi bagian dari hanya satuWilayah AWS. Oleh karena itu, query berikut tidak mengembalikan hasil.
>
> ```
> region:us-east-1 region:us-west-1
> ```
>
> Batasan ini tidak berlaku untuk filter untuk atribut yang dapat memiliki beberapa nilai pada saat yang sama, sepertitag:,tag.key:, dantag.value:.

## Cari sumber daya yang memiliki istilah multi-kata

Kelilingi istilah multi-kata dengan tanda kutip ganda (") untuk mengembalikan hanya hasil yang memiliki seluruh istilah dalam urutan yang ditentukan. Tanpa tanda kutip ganda, Resource Explorer mengembalikan sumber daya yang cocok dengan setiap kata individual yang membentuk istilah tersebut. Misalnya, kueri berikut menggunakan tanda kutip ganda untuk mengembalikan hanya sumber daya yang cocok dengan istilah tersebut`"west wing"`. Kueri tidak cocok dengan sumber daya di`us-west-2`Wilayah AWS (atau Wilayah lain yang termasuk`west` dalam kodenya) atau sumber daya yang cocok dengan kata “sayap” tanpa kata “barat”.

```
"west wing"
```

## Pencarian sumber daya yang merupakan bagian dari CloudFormation tumpukan tertentu

Ketika Anda membuat sumber daya sebagai bagian dariAWS CloudFormation tumpukan, mereka semua ditandai dengan nama stack secara otomatis. Contoh berikut mengembalikan semua sumber daya yang dibuat sebagai bagian dari tumpukan tertentu.

```
tag:aws:cloudformation:stack-name=my-stack-name
```

# Menggunakan pencarian terpadu di AWS Management Console

AWS Management ConsoleTermasuk bilah pencarian di bagian atas setiap halaman AWS konsol. Bilah pencarian ini dapat mencari Layanan AWS dokumentasi dan topik blog, dan membawa Anda langsung ke halaman konsol AWS layanan. Hal ini juga dapat mengembalikan sumber daya di AndaAkun AWS, jika Anda mengaktifkan fitur pencarian terpadu dengan mengaktifkan fitur Resource Explorer yang diperlukan.

Dengan pencarian terpadu, pengguna Anda dapat mencari sumber daya dari Layanan AWS konsol apa pun tanpa harus terlebih dahulu menavigasi ke Penjelajah Sumber Daya AWS konsol.

> **Tip**
>
> Saat Anda ingin menggunakan bilah pencarian terpadu untuk mencari sumber daya secara khusus, mulailah kueri penelusuran dengan mengetik**`/Resources`**. Hal ini menyebabkan AWS sumber daya diberi peringkat lebih tinggi dalam hasil pencarian daripada hasil yang tidak mewakili sumber daya.

Topik



> **Important**
>
> Pencarian terpadu secara otomatis menyisipkan karakter wildcard (*) operator pada akhir kata kunci pertama dalam string. Ini berarti bahwa hasil pencarian terpadu menyertakan sumber daya yang cocok dengan string apa pun yang dimulai dengan kata kunci yang ditentukan.
>
> Pencarian yang dilakukan oleh kotak teks Query pada halaman pencarian sumber daya di konsol Resource Explorer tidak secara otomatis menambahkan karakter wildcard. Anda dapat memasukkan secara * manual setelah istilah apa pun dalam string pencarian.

# Memeriksa apakah pencarian terpadu diaktifkan

Untuk melihat apakah pencarian terpadu diaktifkan di AndaAkun AWS, lihat bagian atas halaman Pengaturan. Resource Explorer menampilkan status saat ini dari setiap persyaratan di sana. Persyaratan untuk pencarian terpadu adalah sebagai berikut:

- Anda harus mengaktifkan Resource Explorer setidaknya dalam satuWilayah AWS. Hanya sumber daya di Wilayah dengan indeks Resource Explorer yang dapat muncul di hasil pencarian terpadu.
- Anda harus membuat indeks agregator di Wilayah pilihan Anda. Pencarian yang dilakukan di Wilayah ini mengembalikan hasil dari semua Wilayah terdaftar di akun.
- Anda harus membuat tampilan default di Wilayah yang berisi indeks agregator. Semua pengguna yang perlu menggunakan pencarian terpadu untuk sumber daya harus memiliki izin untuk menggunakan tampilan default ini.
- Pengguna harus memiliki kebijakan izin AWS Identity and Access Management (IAM) yang ditetapkan ke pokok IAM mereka yang memberikan izin untuk melakukan,,,, tindakan. `resource-explorer-2:Get*` `resource-explorer-2:List*` `resource-explorer-2:Describe*` `resource-explorer-2:Search` Anda dapat memberikan izin ini dengan menggunakan kebijakan IAM khusus untuk mengizinkan izin khusus. Izin ini sudah disertakan sebagai bagian dari kebijakan AWS terkelola berikut yang tersedia untuk Anda gunakan:
  - AWSResourceExplorerReadOnlyAccess
  - AWSResourceExplorerFullAccess

# Mengaktifkan pencarian terpadu

Untuk mengaktifkan menyertakan sumber daya akun Anda dalam hasil pencarian untuk pencarian terpadu dari AWS konsol mana pun, Anda harus menyelesaikan langkah-langkah berikut:

1. Aktifkan Penjelajah Sumber Daya AWS dalam satu atau lebih Wilayah AWS di akun Anda.
2. Daftarkan satu Wilayah untuk berisi indeks agregator.
3. Buat tampilan default di Wilayah dengan indeks agregator.

# Menggunakan AWS Chatbot untuk mencari sumber daya

Anda dapat mencari dan menemukan informasi tentang Layanan AWS dan AWS sumber daya Anda dengan mengajukan pertanyaan bahasa AWS Chatbot alami. AWS Chatbotmenjawab pertanyaan terkait layanan langsung di saluran obrolan Anda dengan AWS dokumentasi yang relevan dan kutipan artikel dukungan. AWS Chatbotmenggunakan Resource Explorer untuk mencari dan menemukan jawaban atas pertanyaan terkait sumber daya Anda.

Untuk informasi lebih lanjut, lihat Apa ituAWS Chatbot? dalam Panduan AWS Chatbot Administrator.

## AWSpertanyaan sumber daya

AWS Chatbotmenggunakan Resource Explorer untuk mencari dan menemukan sumber daya Anda. AWS Chatbotmenampilkan hasil pencarian ini dalam daftar. Daftar ini menunjukkan lima sumber daya pencocokan teratas dan mencakup kemampuan untuk memfilter hasil lebih lanjut berdasarkan jenis sumber dayaWilayah AWS,, dan tag.

### Prasyarat

Untuk mengajukan pertanyaan terkait AWS Chatbot sumber daya, Anda harus:

- Pastikan Anda memiliki indeks dan tampilan aktif dengan setidaknya satu tampilan default di AndaWilayah AWS. Indeks dan tampilan memungkinkan Resource Explorer untuk membuat katalog dan menanyakan sumber daya Anda. Untuk informasi selengkapnya, lihat Syarat dan konsep untuk Resource Explorer.
- Tambahkan AWSResourceExplorerReadOnlyAccess kebijakan ke peran channel Anda atau setiap peran pengguna yang sesuai, tergantung pada skema izin channel Anda.
- Verifikasi bahwa kebijakan pagar pembatas saluran Anda mengizinkan AWSResourceExplorerReadOnlyAccess izin.

### Pertanyaan sumber daya yang umum diajukan

Anda dapat mengajukan pertanyaan ini langsung dari saluran obrolan Anda. Ganti kata-kata dengan teks merah dengan informasi Anda sendiri.

```
@aws What services am I using in Region?
```

```
@aws What are the resources in my account with tags?

@aws What lambda functions do I have?
```

# Keamanan di Penjelajah Sumber Daya AWS

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

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

- Keamanan cloud —AWS bertanggung jawab untuk melindungi infrastruktur yang berjalanLayanan AWS diAWS Cloud. AWSjuga menyediakan layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga melakukan pengujian dan verifikasi secara berkala terhadap efektivitas keamanan kami sebagai bagian dari Program Kepatuhan AWS. Untuk mempelajari tentang program kepatuhan yang berlaku di Resource Explorer, lihat Layanan AWSLayanan AWSdalam Cakupan .
- Keamanan di cloud — Tanggung jawab Anda ditentukan menurutLayanan AWS yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, mencakup kepekaan data Anda, persyaratan perusahaan Anda, serta peraturan perundangan yang berlaku

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Penjelajah Sumber Daya AWS. Teks berikut menunjukkan kepada Anda cara mengonfigurasi Resource Explorer untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakanLayanan AWS sumber daya Resource Explorer Anda.

Konten

# Identity and access management untuk Penjelajah Sumber Daya AWS

(IAM) AWS Identity and Access Management adalah Layanan AWS yang membantu seorang administrator dalam mengendalikan akses ke sumber daya AWS secara aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Resource Explorer. IAM adalah sebuah layanan Layanan AWS yang dapat Anda gunakan tanpa dikenakan biaya tambahan.

Topik



## Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Resource Explorer.

Pengguna layanan — Jika Anda menggunakan layanan Resource Explorer untuk melakukan pekerjaan Anda, administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur Resource Explorer untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Resource Explorer, lihatIzinPenjelajah Sumber Daya AWS pemecahan masalah.

Administrator layanan — Jika Anda bertanggung jawab atas sumber daya Resource Explorer di perusahaan Anda, Anda mungkin memiliki akses penuh ke Resource Explorer. Tugas Anda adalah

menentukan fitur dan sumber daya Resource Explorer mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasar IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan Resource Explorer, lihatCara kerja Resource Explorer dengan IAM.

Administrator IAM - Jika Anda seorang administrator IAM, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Resource Explorer. Untuk melihat contoh kebijakan berbasis identitas Resource Explorer yang dapat Anda gunakan di IAM, lihat. Contoh kebijakan berbasis identitas Penjelajah Sumber Daya AWS

## Mengautentikasi dengan identitas

Autentikasi merupakan cara Anda untuk masuk ke AWS dengan menggunakan kredensial identitas Anda. Anda harus terautentikasi (masuk keAWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengambil peran IAM.

Anda dapat masuk ke AWS sebagai identitas terfederasi dengan menggunakan kredensial yang disediakan melalui sumber identitas. AWS IAM Identity Center Para pengguna (Pusat Identitas IAM), otentikasi sign-on tunggal perusahaan Anda, dan kredensial Google atau Facebook Anda merupakan contoh identitas terfederasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas dengan menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil suatu peran.

Tergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal akses AWS. Untuk informasi selengkapnya tentang masuk ke AWS, silakan lihat Cara masuk ke Akun AWS Anda di Panduan Pengguna AWS Sign-In.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensial Anda. Jika Anda tidak menggunakan peralatan AWS, maka Anda harus menandatangani sendiri permintaan tersebut. Untuk informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, silakan lihat Menandatangani permintaan API AWS di Panduan Pengguna IAM.

Terlepas dari metode autentikasi yang Anda gunakan, Anda mungkin juga diminta untuk menyediakan informasi keamanan tambahan. Sebagai contoh, AWS menyarankan supaya Anda menggunakan autentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk

mempelajari selengkapnya, silakan lihat Autentikasi multi-faktor di Panduan Pengguna AWS IAM Identity Center dan Menggunakan autentikasi multi-faktor (MFA) di AWS di Panduan Pengguna IAM.

### Pengguna root Akun AWS

Ketika Anda membuat Akun AWS, Anda memulai dengan satu identitas masuk yang memiliki akses ke semua Layanan AWS dan sumber daya di akun tersebut. Identitas ini disebut pengguna root Akun AWS dan diakses dengan cara masuk ke alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, silakan lihat Tugas yang memerlukan kredensial pengguna root di Panduan Pengguna IAM.

### Pengguna dan grup

Pengguna IAM adalah identitas dalam Akun AWS Anda yang memiliki izin khusus untuk satu orang atau aplikasi. Apabila memungkinkan, kami menyarankan untuk mengandalkan pada kredensial temporer alih-alih membuat pengguna IAM yang memiliki kredensyal jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami menyarankan Anda memutar kunci akses. Untuk informasi selengkapnya, silakan lihat Memutar kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang di Panduan Pengguna IAM.

Grup IAM adalah identitas yang menerangkan secara spesifik kumpulan pengguna IAM. Anda tidak dapat masuk sebagai kelompok. Anda dapat menggunakan grup untuk menerangkan secara spesifik izin untuk beberapa pengguna sekaligus. Grup membuat izin lebih mudah dikelola untuk sekelompok besar pengguna. Sebagai contoh, Anda dapat memiliki grup yang diberi nama AdminIAM dan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran tersebut dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial temporer. Untuk mempelajari selengkapnya, silakan lihat Kapan harus membuat pengguna IAM (alih-alih peran) di Panduan Pengguna IAM.

### Peran

Peran IAM merupakan identitas dalam Akun AWS Anda yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat menggunakan peran

IAM untuk sementara dalam AWS Management Console dengan berganti peran. Anda dapat mengambil peran dengan cara memanggil operasi API AWS CLI atau AWS atau menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, silakan lihat menggunakan peran IAM di Panduan Pengguna IAM.

IAM role dengan kredensial temporer berguna dalam situasi berikut:

- Akses pengguna gabungan – Untuk menetapkan izin ke sebuah identitas terfederasi, Anda harus membuat sebuah peran dan menentukan izin untuk peran tersebut. Ketika identitas gabungan terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberikan izin yang ditentukan oleh peran. Untuk informasi tentang peran-peran untuk federasi, silakan lihat Membuat sebuah peran untuk Penyedia Identitas pihak ketiga di Panduan Pengguna IAM. Jika Anda menggunakan Pusat Identitas IAM, Anda mengonfigurasi serangkain izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM mengkorelasikan izin yang diatur ke peran dalam IAM. Untuk informasi tentang rangkaian izin, silakan lihat Rangkaian izin di Panduan Pengguna AWS IAM Identity Center.
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM untuk sementara mengambil izin berbeda untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (pengguna utama tepercaya) di akun berbeda untuk mengakses sumber daya yang ada di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, pada beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan suatu peran sebagai proksi). Untuk mempelajari perbedaan antara kebijakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, silakan lihat Bagaimana peran IAM role berbeda dari kebijakan berbasis sumber daya dalam Panduan Pengguna IAM.
- Akses lintas layanan – Sebagian Layanan AWS menggunakan fitur di Layanan AWS lainnya. Sebagai contoh, ketika Anda melakukan panggilan dalam suatu layanan, lazim pada layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Suatu layanan mungkin melakukan hal tersebut menggunakan izin pengguna utama panggilan, menggunakan peran layanan, atau peran tertaut layanan.
  - Sesi akses maju (FAS) – Ketika Anda menggunakan pengguna IAM atau peran IAM untuk melakukan tindakan-tindakan di AWS, Anda akan dianggap sebagai seorang pengguna utama. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian dilanjutkan oleh tindakan lain pada layanan yang berbeda. FAS menggunakan izin dari pengguna utama untuk memanggil Layanan AWS, yang dikombinasikan dengan Layanan AWS yang diminta untuk membuat pengajuan ke layanan hilir. Permintaan FAS hanya diajukan

ketika sebuah layanan menerima pengajuan yang memerlukan interaksi dengan Layanan AWS lain atau sumber daya lain untuk diselesaikan. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, silakan lihat Meneruskan sesi akses.

- Peran layanan – Sebuah peran layanan adalah sebuah peran IAM yang dijalankan oleh suatu layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, silakan lihat Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
- Peran tertaut layanan – Peran tertaut layanan adalah tipe peran layanan yang tertaut dengan Layanan AWS. Layanan tersebut dapat menjalankan peran untuk melakukan sebuah tindakan atas nama Anda. Peran tertaut layanan akan muncul di Akun AWS Anda dan dimiliki oleh layanan tersebut. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran tertaut layanan.

- Aplikasi yang berjalan di Amazon EC2 – Anda dapat menggunakan peran IAM untuk mengelola kredensial temporer untuk aplikasi yang berjalan di instans EC2 dan mengajukan permintaan AWS CLI atau API AWS. Cara ini lebih baik daripada menyimpan kunci akses dalam instans EC2. Untuk menugaskan sebuah peran AWS ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda dapat membuat sebuah profil instans yang dilampirkan ke instans. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 untuk mendapatkan kredensial sementara. Untuk informasi selengkapnya, silakan lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di instans Amazon EC2 di Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, silakan lihat Kapan harus membuat peran IAM (alih-alih pengguna) di Panduan Pengguna IAM.

## Mengelola kebijakan menggunakan akses

Anda mengendalikan akses di AWS dengan membuat kebijakan dan melampirkannya ke identitas atau sumber daya AWS. Kebijakan adalah objek di AWS yang, ketika terkait dengan identitas atau sumber daya, akan menentukan izinnya. AWS mengevaluasi kebijakan-kebijakan tersebut ketika seorang pengguna utama (pengguna, root user, atau sesi peran) mengajukan permintaan. Izin dalam kebijakan menentukan apakah permintaan diberikan atau ditolak. Sebagian besar kebijakan disimpan di AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, silakan lihat Gambaran Umum kebijakan JSON di Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses pada apa. Yaitu, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan syarat apa.

Secara bawaan, para pengguna dan peran tidak memiliki izin. Untuk mengabulkan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian akan dapat menambahkan kebijakan IAM ke peran, dan para pengguna dapat mengambil peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk pengoperasiannya. Sebagai contoh, anggap saja Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole` . Pengguna dengan kebijakan tersebut dapat memperoleh informasi peran dari AWS Management Console, AWS CLI, atau APIAWS.

## Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, misalnya pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol apa yang pengguna tindakan dan peran dapat kerjakan, pada sumber daya mana, dan dalam keadaan apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, silakan lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan terkelola. Kebijakan inline ditanam secara langsung ke pengguna tunggal, grup, atau peran. Kebijakan terkelola adalah kebijakan yang berdiri sendiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran di Akun AWS Anda. Kebijakan terkelola mencakup kebijakan terkelola AWS dan kebijakan terkelola pelanggan. Untuk mempelajari cara memilih antara kebijakan terkelola atau kebijakan inline, silakan lihat Memilih antara kebijakan terkelola dan kebijakan inline diPanduan Pengguna IAM.

## Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan-kebijakan berbasis sumber daya adalah kebijakan terpercaya peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya yang dilampiri kebijakan, kebijakan tersebut menentkan tindakan apa yang dapat dilakukan oleh pengguna utama yang ditentukan di sumber daya tersebut dan dalam kondisi apa.

Anda harus menentukan pengguna utama dalam kebijakan berbasis sumber daya. Pengguna utama dapat mencakup akun, pengguna, peran, pengguna gabungan, atau Layanan AWS.

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan terkelola AWS dari IAM dalam kebijakan berbasis sumber daya.

Penjelajah Sumber Daya AWS tidak mendukung kebijakan berbasis sumber daya.

### Daftar kontrol akses (ACL)

Daftar kontrol akses (ACL) mengendalikan pengguna utama mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan-kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh-contoh layanan yang mendukung ACL. Untuk mempelajari lebih lanjut tentang ACL, lihat Gambaran umum Access control list (ACL) dalam Panduan Developer Amazon Simple Storage Service.

Penjelajah Sumber Daya AWS tidak mendukung ACL.

### Jenis kebijakan lainnya

AWS mendukung tipe kebijakan tambahan, yang kurang umum. Tipe-tipe kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh tipe kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM (pengguna IAM atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batas izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini menindihi izin. Untuk informasi selengkapnya tentang batasan izin, silakan lihat Batasan izin untuk entitas IAM di Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) – SCP adalah kebijakan JSON yang menentukan izin maksimum untuk sebuah organisasi atau unit organisasi (OU) di AWS Organizations. AWS Organizations adalah layanan untuk mengelompokkan dan secara terpusat mengelola beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur di suatu organisasi, maka Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke salah satu atau ke semua akun Anda. SCP membatasi izin untuk entitas dalam akun anggota, termasuk setiap Pengguna root akun

AWS. Untuk informasi selengkapnya tentang Organisasi dan SCP, silakan lihat Cara kerja SCP di Panduan Pengguna AWS Organizations.

- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara terprogram untuk peran atau pengguna gabungan. Izin sesi yang dihasilkan adalah perpotongan kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga dapat berasal dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini menindihi izin. Untuk informasi selengkapnya, silakan lihat Kebijakan sesi di Panduan Pengguna IAM.

### Berbagai tipe kebijakan

Ketika beberapa tipe kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan ketika beberapa tipe kebijakan dilibatkan, silakan lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

## Cara kerja Resource Explorer dengan IAM

Sebelum menggunakan IAM apa yang tersedia untukPenjelajah Sumber Daya AWS digunakan dengan Resource Explorer. Untuk mendapatkan tampilan tingkat tinggi tentang caraLayanan AWS kerja Resource Explorer dan lainnya dengan IAM, lihat Layanan AWSkerja dengan IAM dalam Panduan Pengguna IAM.

Topik

- Kebijakan berbasis identitas Resource Explorer
- Otorisasi berdasarkan tag Resource Explorer
- Peran IAM Penjelajah Sumber Daya

Seperti yang lainnyaLayanan AWS, Resource Explorer memerlukan izin untuk menggunakan operasinya untuk berinteraksi dengan sumber daya Anda. Untuk mencari, pengguna harus memiliki izin untuk mengambil rincian tentang tampilan, dan juga untuk mencari menggunakan tampilan. Untuk membuat indeks atau tampilan, atau untuk memodifikasinya atau pengaturan Resource Explorer lainnya, Anda harus memiliki izin tambahan.

Tetapkan kebijakan berbasis identitas IAM yang memberikan izin tersebut kepada prinsipal IAM yang sesuai. Resource Explorer menyediakan beberapa kebijakan terkelola yang menentukan set izin umum sebelumnya. Anda dapat menetapkan ini ke kepala sekolah IAM Anda.

## Kebijakan berbasis identitas Resource Explorer

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan tindakan yang diizinkan atau ditolak terhadap sumber daya tertentu dan ketentuan di mana tindakan tersebut diperbolehkan atau ditolak. Resource Explorer mendukung tindakan, dan kunci syarat tertentu. Untuk mempelajari semua elemen yang Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan IAM JSON dalam Panduan Pengguna IAM.

Tindakan

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan siapa yang memiliki akses ke hal apa. Yaitu, principal mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam syarat apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan-tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama sebagai operasi API AWS terkait. Ada beberapa pengecualian, misalnya tindakan hanya dengan izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Sertakan tindakan dalam kebijakan untuk memberikan izin guna melakukan operasi yang terkait.

Tindakan kebijakan di Resource Explorer menggunakan awalan`resource-explorer-2` layanan sebelum tindakan. Misalnya, untuk memberikan seseorang izin untuk mencari menggunakan operasi Resource Explorer`Search`, Anda menyertakan`resource-explorer-2:Search` tindakan dalam kebijakan yang ditetapkan ke pokok tersebut. Pernyataan kebijakan harus memuat elemen `Action` atau `NotAction`. Resource Explorer menentukan serangkaian tindakannya sendiri yang dapat Anda lakukan dengan layanan ini. Ini sejajar dengan operasi Resource Explorer API.

Untuk menetapkan beberapa tindakan dalam satu pernyataan, pisahkan dengan koma seperti yang ditunjukkan dalam contoh berikut.

```
"Action": [
      "resource-explorer-2:action1",
      "resource-explorer-2:action2"
]
```

Anda dapat menentukan beberapa tindakan menggunakan karakter wildcard (*). Misalnya, untuk menentukan semua tindakan yang dimulai dengan kata `Describe`, sertakan tindakan berikut.

```
"Action": "resource-explorer-2:Describe*"
```

Untuk daftar tindakan Resource Explorer, lihat Tindakan yang Ditetapkan olehPenjelajah Sumber Daya AWS dalam Referensi OtorisasiAWS Layanan.

Sumber daya

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan siapa yang memiliki akses ke hal apa. Yaitu, principal mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam syarat apa.

Elemen kebijakan JSON `Resource` menentukan objek atau objek-objek yang menjadi target penerapan tindakan. Pernyataan harus mencakup elemen `Resource` atau `NotResource`. Sebagai praktik terbaik, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung tipe sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin tingkat sumber daya, misalnya operasi pencantuman, gunakan karakter wildcart (*) untuk menunjukkan bahwa pernyataan tersebut berlaku bagi semua sumber daya.

```
"Resource": "*"
```

Lihat

Jenis sumber daya Resource Explorer utama adalah tampilan.

Sumber daya tampilan Resource Explorer memiliki format ARN berikut.

```
arn:${Partition}:resource-explorer-2:${Region}:${Account}:view/${ViewName}/${unique-id}
```

Format Resource Explorer ARN seperti yang ditunjukkan dalam contoh berikut.

```
arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-Search-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

> **Note**
>
> ARN untuk tampilan menyertakan pengenal unik di bagian akhir untuk memastikan bahwa setiap tampilan unik. Ini membantu memastikan bahwa kebijakan IAM yang memberikan

akses ke tampilan lama yang dihapus tidak dapat digunakan untuk secara tidak sengaja memberikan akses ke tampilan baru yang kebetulan memiliki nama yang sama dengan tampilan lama. Setiap tampilan baru menerima ID baru yang unik di bagian akhir untuk memastikan bahwa ARN tidak pernah digunakan kembali.

Untuk informasi lebih lanjut tentang format ARN, lihat Amazon Resource Name (ARN).

Anda menggunakan kebijakan berbasis identitas IAM yang ditetapkan ke prinsipal IAM dan menentukan tampilan sebagai`Resource`. Dengan melakukan ini, Anda dapat memberikan akses pencarian melalui satu tampilan ke satu set prinsipal, dan mengakses melalui tampilan yang sama sekali berbeda ke sekumpulan prinsipal yang berbeda.

Misalnya, untuk memberikan izin ke tampilan tunggal yang dinamai`ProductionResourcesView` dalam pernyataan kebijakan IAM, pertama-tama dapatkan nama sumber daya Amazon (ARN) tampilan. Anda dapat menggunakan halaman Tampilan di konsol untuk melihat detail tampilan, atau memanggil`ListViews` operasi untuk mengambil ARN penuh dari tampilan yang Anda inginkan. Kemudian, sertakan dalam pernyataan kebijakan, seperti yang ditunjukkan dalam contoh berikut yang memberikan izin untuk memodifikasi definisi hanya satu tampilan.

```
"Effect": "Allow",
"Action": "UpdateView",
"Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
ProductionResourcesView/<unique-id>"
```

Untuk mengizinkan tindakan di semua tampilan yang terkait, gunakan karakter kartubebas (*) di bagian ARN yang relevan. Contoh berikut memberikan izin pencarian untuk semua tampilan dalam akunWilayah AWS dan tertentu.

```
"Effect": "Allow",
"Action": "Search",
"Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/*"
```

Beberapa tindakan Resource Explorer`CreateView`, seperti, tidak dilakukan terhadap sumber daya tertentu, karena, seperti pada contoh berikut, sumber daya belum ada. Dalam kondisi tersebut, Anda harus menggunakan karakter wildcard (*) untuk seluruh sumber daya ARN.

```
"Effect": "Allow",
"Action": "resource-explorer-2:CreateView"
```

```
"Resource": "*"
```

Jika Anda menentukan jalur yang berakhir dengan karakter wildcard, maka Anda dapat membatasi`CreateView` operasi untuk membuat tampilan hanya dengan jalur yang disetujui. Bagian kebijakan contoh berikut menunjukkan cara mengizinkan prinsipal untuk membuat tampilan hanya di jalur`view/ProductionViews/`.

```
"Effect": "Allow",
"Action": "resource-explorer-2:CreateView"
"Resource": "arn:aws:resource-explorer-2:us-
east-1:123456789012:view/ProductionViews/*""
```

Indeks

Jenis sumber daya lain yang dapat Anda gunakan untuk mengontrol akses ke fungsionalitas Resource Explorer adalah indeks.

Cara utama Anda berinteraksi dengan indeks adalah mengaktifkan Resource ExplorerWilayah AWS dengan membuat indeks di Wilayah tersebut. Setelah itu, Anda melakukan hampir semua hal lain dengan berinteraksi dengan tampilan.

Satu hal yang dapat Anda lakukan dengan indeks adalah mengontrol siapa yang dapat membuat tampilan di setiap Wilayah.

> **Note**
>
> Setelah Anda membuat tampilan, IAM mengotorisasi semua tindakan tampilan lainnya hanya terhadap ARN tampilan, dan bukan indeks.

Indeks memiliki ARN yang dapat Anda referensi dalam kebijakan izin. Sebuah indeks Resource Explorer memiliki format berikut.

```
arn:${Partition}:resource-explorer-2:${Region}:${Account}:index/${unique-id}
```

Lihat contoh berikut indeks Resource Explorer ARN.

```
arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-
abcd22222222
```

Beberapa tindakan Resource Explorer memeriksa otentikasi terhadap beberapa jenis sumber daya. Misalnya, CreateViewoperasi mengotorisasi terhadap ARN indeks dan ARN tampilan karena akan terjadi setelah Resource Explorer membuatnya. Untuk memberikan izin kepada administrator untuk mengelola layanan Resource Explorer, Anda dapat menggunakannya`"Resource": "*"` untuk mengotorisasi tindakan untuk sumber daya, indeks, atau tampilan apa pun.

Atau, Anda dapat membatasi prinsipal untuk hanya dapat bekerja dengan sumber daya Resource Explorer tertentu. Misalnya, untuk membatasi tindakan hanya pada sumber daya Resource Explorer di Wilayah tertentu, Anda dapat menyertakan template ARN yang cocok dengan indeks dan tampilan, tetapi hanya memanggil satu Wilayah. Pada contoh berikut, ARN cocok dengan indeks atau tampilan hanya di`us-west-2` Wilayah akun yang ditentukan. Tentukan Wilayah di bidang ketiga dari ARN, tetapi menggunakan karakter kartubebas (*) di bidang akhir untuk mencocokkan jenis sumber daya apa pun.

```
"Resource": "arn:aws:resource-explorer-2:us-west-2:123456789012:*
```

Untuk informasi selengkapnya, lihat Sumber Daya yang Ditetapkan olehPenjelajah Sumber Daya AWS di Referensi OtorisasiAWS Layanan. Untuk mempelajari tindakan mana yang dapat menentukan ARN setiap sumber daya, lihat Tindakan yang Ditentukan oleh Penjelajah Sumber Daya AWS.

Kunci syarat

Resource Explorer tidak menyediakan kunci syarat khusus layanan, tetapi mendukung penggunaan beberapa kunci syarat global. Untuk melihat semua kunci syarat global AWS, lihat Kunci konteks syarat global AWS dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan siapa yang memiliki akses ke hal apa. Yaitu, prinsipal mana yang dapat melakukan tindakan pada sumber daya apa, dan menurut persyaratan apa.

Elemen `Condition` (atau `Condition` blok) memungkinkan Anda menentukan syarat di mana suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator syarat, seperti sama dengan atau kurang dari, untuk mencocokkan syarat dalam kebijakan dengan nilai dalam permintaan.

Jika Anda menentukan beberapa elemen `Condition` dalam pernyataan, atau beberapa kunci dalam satu elemen `Condition`, AWS akan mengevaluasinya denga menggunakan operasi logika `AND`. Jika Anda menetapkan beberapa nilai untuk kunci syarat tunggal, AWS akan mengevaluasi syarat

tersebut dengan menggunakan operasi logika `OR`. Semua persyaratan harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan syarat. Sebagai contoh, Anda dapat memberikan izin pengguna IAM untuk mengakses sumber daya hanya jika ditandai dengan nama pengguna IAM mereka. Untuk informasi lebih lanjut, lihat Elemen kebijakan IAM: variabel dan tag dalam Panduan Pengguna IAM.

AWS mendukung kunci syarat global dan kunci syarat khusus layanan. Untuk melihat semua kunci syarat global AWS, lihat Kunci konteks syarat global AWS dalam Panduan Pengguna IAM.

Untuk melihat daftar kunci kondisi yang dapat Anda gunakan dengan Resource Explorer, lihat Kunci Kondisi untukPenjelajah Sumber Daya AWS di Referensi OtorisasiAWS Layanan. Untuk mempelajari tindakan dan sumber daya mana yang dapat Anda gunakan bersama, lihat Tindakan yang Ditentukan olehPenjelajah Sumber Daya AWS.

Contoh

Untuk melihat contoh kebijakan berbasis identitas Resource Explorer, lihatContoh kebijakan berbasis identitas Penjelajah Sumber Daya AWS.

## Otorisasi berdasarkan tag Resource Explorer

Anda dapat melampirkan tag ke tampilan Resource Explorer atau meneruskan tag dalam permintaan ke Resource Explorer. Untuk mengendalikan akses berdasarkan tanda, Anda dapat memberikan informasi tentang tanda di kebijakan elemen syarat menggunakan kunci syarat `resource-explorer-2:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, atau `aws:TagKeys`. Untuk informasi lebih lanjut tentang penandaan sumber daya, lihatMenambahkan tag ke tampilan yang sudah ditonton. Untuk menggunakan otorisasi berbasis tag di Resource Explorer, lihatMenggunakan otorisasi berbasis tanda untuk mengontrol akses ke tampilan Anda.

## Peran IAM Penjelajah Sumber Daya

IAM role adalah pokok dalam AndaAkun AWS yang memiliki izin khusus.

Menggunakan kredensi sementara dengan Resource Explorer

Anda dapat menggunakan kredensial sementara untuk masuk dengan gabungan, menjalankan IAM role, atau menjalankan peran lintas akun. Anda memperoleh kredensi keamanan sementara dengan memanggilAWS Security Token Service (AWS STS) operasi API seperti AssumeRoleatau GetFederationToken.

Resource Explorer mendukung penggunaan kredensial sementara.

Peran terkait layanan

Peran terkait layananLayanan AWS memungkinkan Anda mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama Anda. Peran terkait layanan muncul di akun IAM Anda dan dimiliki oleh layanan tersebut. Administrator IAM dapat melihat tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Resource Explorer menggunakan peran terkait layanan untuk melakukan pekerjaannya. Untuk informasi selengkapnya tentang peran terkait layanan Resource Explorer, lihatMenggunakan peran terkait layanan untuk Resource Explorer.

## Contoh kebijakan berbasis identitas Penjelajah Sumber Daya AWS

Secara default,AWS Identity and Access Management IAM), seperti peran, grup, pengguna, tidak memiliki izin untuk membuat atau memodifikasi sumber daya Resource Explorer. Mereka juga tidak dapat melakukan tugas menggunakanAWS Management Console,AWS Command Line Interface (AWS CLI), atauAWS API. Administrator IAM harus membuat kebijakan IAM yang memberi izin kepada prinsipal untuk melakukan operasi API tertentu pada sumber daya yang diperlukan. Kemudian, administrator harus menetapkan kebijakan tersebut ke prinsipal IAM yang memerlukan izin tersebut.

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

- Pengguna dan grup diAWS IAM Identity Center:

  Buat set izin. Ikuti petunjuk di Buat set izin di PanduanAWS IAM Identity Center Pengguna.
- Pengguna yang dikelola dalam IAM melalui penyedia identitas:

  Membuat PERM. Ikuti petunjuk dalam Membuat peran untuk penyedia identitas pihak ketiga (federasi) di Panduan Pengguna IAM.
- Pengguna IAM:
  - Buat peran yang dapat diasumsikan pengguna Anda. Ikuti petunjuk dalam Membuat peran untuk pengguna IAM di Panduan Pengguna IAM.
  - (Tidak disarankan) Lampirkan kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti petunjuk dalam Menambahkan izin ke pengguna (konsol) di Panduan Pengguna IAM.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat Kebijakan pada Tab JSON dalam Panduan Pengguna IAM.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol Resource Explorer
- Memberikan akses ke tampilan berdasarkan tag
- Memberikan akses untuk membuat tampilan berdasarkan tag
- Izinkan para prinsipal untuk melihat izin mereka sendiri

## Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Resource Explorer di akun Anda. Tindakan ini membuat Akun AWS Anda terkena biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Memulai kebijakanAWS terkelola dan beralih ke izin paling sedikit hak istimewa — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakanAWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di AndaAkun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelolaAWS pelanggan yang spesifik untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat kebijakanAWSAWS terkelola atau kebijakan terkelola untuk fungsi pekerjaan di Panduan Pengguna IAM.
- Gunakan izin hak akses IAM — Saat Anda mengatur izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melaksanakan tugas. Anda melakukan ini dengan menentukan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, juga dikenal sebagai izin paling tidak memiliki hak istimewa. Untuk informasi selengkapnya tentang penggunaan IAM untuk menerapkan izin, lihat Kebijakan dan izin di IAM dalam Panduan Pengguna IAM.
- Gunakan ketentuan dalam kebijakan IAM untuk membatasi akses lebih lanjut — Anda dapat menambahkan kondisi pada kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Misalnya, Anda dapat menulis sebuah kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan kondisi untuk memberikan akses ke tindakan layanan jika digunakan melalui spesifikLayanan AWS, sepertiAWS CloudFormation. Untuk mengetahui informasi lebih lanjut, lihat Elemen Kebijakan IAM JSON: Syarat dalam Panduan Pengguna IAM.

- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional - IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat validasi kebijakan IAM Access Analyzer di Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) — Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di AndaAkun AWS, aktifkan MFA untuk keamanan tambahan. Untuk mewajibkan MFA saat operasi API dipanggil, tambahkan kondisi MFA ke kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi akses API yang dilindungi MFA di Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat praktik terbaik keamanan di IAM dalam Panduan Pengguna IAM.

## Menggunakan konsol Resource Explorer

Agar prinsipal dapat mencari diPenjelajah Sumber Daya AWS konsol tersebut, mereka harus memiliki satu set izin minimum. Jika Anda tidak membuat kebijakan berbasis identitas dengan izin minimum yang diperlukan, konsol Resource Explorer tidak akan berfungsi sebagaimana dimaksudkan untuk prinsipal di akun.

Anda dapat menggunakan kebijakanAWS terkelola bernama`AWSResourceExplorerReadOnlyAccess` untuk memberikan kemampuan menggunakan konsol Resource Explorer untuk mencari menggunakan tampilan apa pun di akun. Untuk memberikan izin untuk mencari hanya dengan satu tampilan, lihatMemberikan akses ke tampilan Resource Explorer untuk pencarian, dan contoh dalam dua bagian berikut.

Anda tidak perlu memberikan izin konsol minimum untuk prinsipal yang melakukan panggilan hanya keAWS CLI atauAWS API. Sebagai gantinya, Anda dapat memilih untuk memberikan akses hanya ke tindakan yang cocok dengan operasi API yang perlu dilakukan oleh prinsipal.

## Memberikan akses ke tampilan berdasarkan tag

Dalam contoh ini, Anda ingin memberi akses ke tampilan Resource Explorer pada prinsipal di akun tersebut.Akun AWS Untuk melakukan ini, Anda menetapkan kebijakan berbasis identitas IAM ke prinsipal yang ingin Anda cari di Resource Explorer. Contoh berikut kebijakan IAM memberikan akses ke setiap permintaan di mana`Search-Group` tag yang dilampirkan ke prinsipal panggilan

sama persis dengan nilai untuk tag yang sama yang dilampirkan ke tampilan yang digunakan dalam permintaan.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetView",
                "resource-explorer-2:Search"
            ],
            "Resource": "arn:aws:resource-explorer-2:*:*:view/*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Search-Group": "${aws:PrincipalTag/
Search-Group}"}
            }
        }
    ]
}
```

Anda dapat menetapkan kebijakan ini ke prinsipal IAM di akun Anda. Jika prinsipal dengan tag`Search-Group=A` mencoba mencari menggunakan tampilan Resource Explorer, tampilan juga harus ditandai`Search-Group=A`. Jika tidak, maka kepala sekolah ditolak aksesnya. Kunci tanda syarat `Search-Group` sama dengan kedua `Search-group` dan `search-group` karena nama kunci syarat tidak terpengaruh huruf besar/kecil. Untuk informasi lebih lanjut, lihat Elemen Kebijakan IAM JSON: Persyaratan dalam Panduan Pengguna IAM.

**Important**

Untuk melihat sumber daya Anda dalam hasil pencarian terpadu diAWS Management Console, prinsipal harus memiliki keduanya`GetView` dan`Search` izin untuk tampilan default diWilayah AWS yang berisi indeks agregator. Cara paling sederhana untuk memberikan izin tersebut adalah dengan meninggalkan izin berbasis sumber daya default yang dilampirkan ke tampilan saat Anda mengaktifkan Resource Explorer menggunakan penyiapan Cepat atau Lanjutan.

Untuk skenario ini, Anda dapat mempertimbangkan untuk mengatur tampilan default untuk memfilter sumber daya sensitif dan kemudian menyiapkan tampilan tambahan yang Anda berikan akses berbasis tag seperti yang dijelaskan dalam contoh sebelumnya.

## Memberikan akses untuk membuat tampilan berdasarkan tag

Dalam contoh ini, Anda ingin mengizinkan hanya prinsipal yang ditandai sama dengan indeks untuk dapat membuat tampilan diWilayah AWS yang berisi indeks. Untuk melakukan ini, buat izin berbasis identitas untuk memungkinkan prinsipal mencari dengan tampilan.

Sekarang Anda siap untuk membuat izin untuk membuat tampilan. Anda dapat menambahkan pernyataan dalam contoh ini ke kebijakan izin yang sama yang Anda gunakan untuk memberikan`Search` izin kepada prinsipal yang sesuai. Tindakan diperbolehkan atau ditolak berdasarkan tag yang dilampirkan pada prinsipal yang memanggil operasi dan indeks bahwa pandangan harus dikaitkan dengan. Contoh berikut kebijakan IAM menolak permintaan apa pun untuk membuat tampilan saat nilai`Allow-Create-View` tag yang dilampirkan pada prinsipal pemanggil tidak sama persis dengan nilai tag yang sama yang dilampirkan ke indeks di Wilayah tempat tampilan dibuat.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "resource-explorer-2:CreateView",
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {"aws:ResourceTag/Allow-Create-View":
 "${aws:PrincipalTag/Allow-Create-View}"}
            }
        }
    ]
}
```

## Izinkan para prinsipal untuk melihat izin mereka sendiri

Contoh ini menunjukkan cara Anda dapat membuat kebijakan yang mengizinkan para pengguna IAM untuk melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan pada konsol atau secara terprogram menggunakan API AWS CLI atau AWS.

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

```
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

## Contoh kebijakan kontrol layanan untuk AWS Organizations dan Resource Explorer

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

## Prasyarat

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

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

## Contoh kebijakan kontrol layanan

Contoh berikut menunjukkan bagaimana Anda dapat menggunakan kontrol akses berbasis atribut (ABAC) untuk mengontrol akses ke operasi administratif Resource Explorer. Kebijakan contoh ini menolak akses ke semua operasi Resource Explorer kecuali dua izin yang diperlukan untuk mencari, `resource-explorer-2:Search` dan`resource-explorer-2:GetView`, kecuali jika prinsipal IAM yang membuat permintaan diberi tag. `ResourceExplorerAdmin=TRUE` Untuk diskusi yang lebih lengkap tentang penggunaan ABAC dengan Resource Explorer, lihatMenggunakan otorisasi berbasis tanda untuk mengontrol akses ke tampilan Anda.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "resource-explorer-2:AssociateDefaultView",
        "resource-explorer-2:BatchGetView",
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:CreateView",
        "resource-explorer-2:DeleteIndex",
        "resource-explorer-2:DeleteView",
        "resource-explorer-2:DisassociateDefaultView",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
```

```
        "resource-explorer-2:TagResource",
        "resource-explorer-2:UntagResource",
        "resource-explorer-2:UpdateIndexType",
        "resource-explorer-2:UpdateView""
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
          "StringNotEqualsIgnoreCase": {"aws:PrincipalTag/ResourceExplorerAdmin":
 "TRUE"}
      }
    ]
}
```

## AWS kebijakan terkelola untuk Penjelajah Sumber Daya AWS

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 AWS kebijakan yang dikelola dalam Panduan Pengguna IAM.

Kebijakan AWS terkelola umum yang menyertakan izin Resource Explorer

- AdministratorAccess— Memberikan akses penuh ke Layanan AWS dan sumber daya.
- ReadOnlyAkses — Memberikan akses dan sumber daya hanya-baca. Layanan AWS
- ViewOnlyAkses — Memberikan izin untuk melihat sumber daya dan metadata dasar untuk. Layanan AWS

> **Note**
>
> `Get*`Izin Resource Explorer yang disertakan dalam `ViewOnlyAccess` kebijakan berfungsi seperti `List` izin meskipun izin tersebut hanya menampilkan satu nilai, karena Region hanya dapat berisi satu indeks dan satu tampilan default.

AWS kebijakan terkelola untuk Resource Explorer

- AWSResourceExplorerFullAccess
- AWSResourceExplorerReadOnlyAccess
- AWSResourceExplorerServiceRolePolicy

## AWS kebijakan terkelola: AWSResourceExplorerFullAccess

Anda dapat menetapkan `AWSResourceExplorerFullAccess` kebijakan untuk identitas IAM Anda.

Kebijakan ini memberikan izin yang memungkinkan kontrol administratif penuh atas layanan Resource Explorer. Anda dapat melakukan semua tugas yang terlibat dalam mengaktifkan dan mengelola Resource Explorer Wilayah AWS di akun Anda.

Detail izin

Kebijakan ini mencakup izin yang memungkinkan semua tindakan untuk Resource Explorer, termasuk mengaktifkan dan menonaktifkan Resource Explorer di Wilayah AWS, membuat atau menghapus indeks agregator untuk akun, membuat, memperbarui, dan menghapus tampilan, dan mencari. Kebijakan ini juga mencakup izin yang bukan bagian dari Resource Explorer:

- `ec2:DescribeRegions`— memungkinkan Resource Explorer untuk mengakses detail tentang Wilayah di akun Anda.
- `ram:ListResources`— memungkinkan Resource Explorer untuk membuat daftar pembagian sumber daya yang menjadi bagian dari sumber daya.
- `ram:GetResourceShares`— memungkinkan Resource Explorer untuk mengidentifikasi rincian tentang pembagian sumber daya yang Anda miliki atau yang dibagikan dengan Anda.
- `iam:CreateServiceLinkedRole`— memungkinkan Resource Explorer untuk membuat peran terkait layanan yang diperlukan saat Anda mengaktifkan Resource Explorer dengan membuat indeks pertama.

- `organizations:DescribeOrganization`— memungkinkan Resource Explorer untuk mengakses informasi tentang organisasi Anda.

Untuk melihat versi terbaru dari kebijakan AWS terkelola ini, lihat `AWSResourceExplorerFullAccess` di Panduan Referensi Kebijakan AWS Terkelola.

## AWS kebijakan terkelola: AWSResourceExplorerReadOnlyAccess

Anda dapat menetapkan `AWSResourceExplorerReadOnlyAccess` kebijakan untuk identitas IAM Anda.

Kebijakan ini memberikan izin hanya-baca yang memungkinkan pengguna akses penelusuran dasar untuk menemukan sumber daya mereka.

Detail izin

Kebijakan ini mencakup izin yang memungkinkan pengguna menjalankan Resource Explorer `Get*` `List*`, dan `Search` operasi untuk melihat informasi tentang komponen Resource Explorer dan setelan konfigurasi, tetapi tidak memungkinkan pengguna untuk mengubahnya. Pengguna juga dapat mencari. Kebijakan ini juga mencakup dua izin yang bukan merupakan bagian dari Resource Explorer:

- `ec2:DescribeRegions`— memungkinkan Resource Explorer untuk mengakses detail tentang Wilayah di akun Anda.
- `ram:ListResources`— memungkinkan Resource Explorer untuk membuat daftar pembagian sumber daya yang menjadi bagian dari sumber daya.
- `ram:GetResourceShares`— memungkinkan Resource Explorer untuk mengidentifikasi rincian tentang pembagian sumber daya yang Anda miliki atau yang dibagikan dengan Anda.
- `organizations:DescribeOrganization`— memungkinkan Resource Explorer untuk mengakses informasi tentang organisasi Anda.

Untuk melihat versi terbaru dari kebijakan AWS terkelola ini, lihat `AWSResourceExplorerReadOnlyAccess` di Panduan Referensi Kebijakan AWS Terkelola.

## AWS kebijakan terkelola: AWSResourceExplorerServiceRolePolicy

Anda tidak dapat melampirkan `AWSResourceExplorerServiceRolePolicy` ke entitas IAM apa pun sendiri. Kebijakan ini hanya dapat dilampirkan ke peran terkait layanan yang memungkinkan

Resource Explorer melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk Resource Explorer.

Kebijakan ini memberikan izin yang diperlukan untuk Resource Explorer untuk mengambil informasi tentang sumber daya Anda. Resource Explorer mengisi indeks yang dipertahankannya di setiap Wilayah AWS yang Anda daftarkan.

Untuk melihat versi terbaru dari kebijakan AWS terkelola ini, lihat `AWSResourceExplorerServiceRolePolicy` di konsol IAM.

## AWS kebijakan terkelola: AWSResourceExplorerOrganizationsAccess

Anda dapat menetapkan identitas `AWSResourceExplorerOrganizationsAccess` IAM Anda.

Kebijakan ini memberikan izin administratif ke Resource Explorer dan memberikan izin hanya-baca kepada orang lain untuk mendukung akses ini. Layanan AWS AWS Organizations Administrator memerlukan izin ini untuk mengatur dan mengelola pencarian multi-akun di konsol.

Detail izin

Kebijakan ini mencakup izin yang memungkinkan administrator menyiapkan penelusuran multi-akun untuk organisasi:

- `ec2:DescribeRegions`— Memungkinkan Resource Explorer untuk mengakses detail tentang Wilayah di akun Anda.
- `ram:ListResources`— Memungkinkan Resource Explorer untuk mencantumkan pembagian sumber daya yang menjadi bagian dari sumber daya.
- `ram:GetResourceShares`— Memungkinkan Resource Explorer untuk mengidentifikasi rincian tentang pembagian sumber daya yang Anda miliki atau yang dibagikan dengan Anda.
- `organizations:ListAccounts`— Memungkinkan Resource Explorer untuk mengidentifikasi akun dalam suatu organisasi.
- `organizations:ListRoots`— Memungkinkan Resource Explorer untuk mengidentifikasi akun root dalam suatu organisasi.
- `organizations:ListOrganizationalUnitsForParent`— Memungkinkan Resource Explorer untuk mengidentifikasi unit organisasi (OU) dalam unit organisasi induk atau root.
- `organizations:ListAccountsForParent`— Memungkinkan Resource Explorer untuk mengidentifikasi akun dalam organisasi yang terkandung oleh root target yang ditentukan atau OU.

- `organizations:ListDelegatedAdministrators`— Memungkinkan Resource Explorer untuk mengidentifikasi AWS akun yang ditetapkan sebagai administrator yang didelegasikan dalam organisasi ini.
- `organizations:ListAWSServiceAccessForOrganization`— Memungkinkan Resource Explorer untuk mengidentifikasi daftar Layanan AWS yang diaktifkan untuk diintegrasikan dengan organisasi Anda.
- `organizations:DescribeOrganization`— Memungkinkan Resource Explorer untuk mengambil informasi tentang organisasi yang menjadi milik akun pengguna.
- `organizations:EnableAWSServiceAccess`— Memungkinkan Resource Explorer untuk mengaktifkan integrasi Layanan AWS (layanan yang ditentukan oleh`ServicePrincipal`) dengan AWS Organizations.
- `organizations:DisableAWSServiceAccess`— Memungkinkan Resource Explorer untuk menonaktifkan integrasi Layanan AWS (layanan yang ditentukan oleh ServicePrincipal) dengan AWS Organizations.
- `organizations:RegisterDelegatedAdministrator`— Memungkinkan Resource Explorer untuk mengaktifkan akun anggota yang ditentukan untuk mengelola fitur organisasi dari AWS layanan yang ditentukan.
- `organizations:DeregisterDelegatedAdministrator`— Memungkinkan Resource Explorer untuk menghapus anggota yang ditentukan Akun AWS sebagai administrator yang didelegasikan untuk yang ditentukan Layanan AWS.
- `iam:GetRole`— Memungkinkan Resource Explorer untuk mengambil informasi tentang peran yang ditentukan, termasuk jalur peran, GUID, ARN, dan kebijakan kepercayaan peran yang memberikan izin untuk mengambil peran.
- `iam:CreateServiceLinkedRole`— Memungkinkan Resource Explorer untuk membuat peran terkait layanan yang diperlukan saat Anda mengaktifkan Resource Explorer dengan membuat indeks pertama.

Untuk melihat versi terbaru dari kebijakan AWS terkelola ini, lihat `AWSResourceExplorerOrganizationsAccess` di konsol IAM.

## Pembaruan Resource Explorer ke kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Resource Explorer sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman riwayat Dokumen Resource Explorer.

| Perubahan | Deskripsi | Tanggal |
| --- | --- | --- |
| AWSResourceExplorerServiceRolePolicy- Izin kebijakan yang diperbarui untuk melihat jenis sumber daya tambahan | Resource Explorer menambahkan izin ke kebijakan peran terkait layanan AWSResourceExplorerServiceRolePolicy yang memungkinkan Resource Explorer melihat jenis sumber daya tambahan:<br>• apprunner:ListVpcConnectors<br>• backup:ListReportPlans<br>• emr-serverless:ListApplications<br>• events:ListEventBuses<br>• geo:ListPlaceIndexes<br>• geo:ListTrackers<br>• greengrass:ListComponents<br>• greengrass:ListComponentVersions<br>• iot:ListRoleAliases<br>• iottwinmaker:ListComponentTypes<br>• iottwinmaker:ListEntities<br>• iottwinmaker:ListScenes | Desember 12, 2023 |

| Perubahan | Deskripsi | Tanggal |
| --- | --- | --- |
| | • `kafka:ListConfigurations`<br>• `kms:ListKeys`<br>• `kinesisanalytics:ListApplications`<br>• `lex:ListBots`<br>• `lex:ListBotAliases`<br>• `mediapackage-vod:ListPackagingConfigurations`<br>• `mediapackage-vod:ListPackagingGroups`<br>• `mq:ListBrokers`<br>• `personalize:ListDatasetGroups`<br>• `personalize:ListDatasets`<br>• `personalize:ListSchemas`<br>• `route53:ListHealthChecks`<br>• `route53:ListHostedZones`<br>• `secretsmanager:ListSecrets` | |
| Kebijakan terkelola baru | Resource Explorer menambahkan kebijakan AWS terkelola berikut:<br>• AWSResourceExplorerOrganizationsAccess | 14 November 2023 |

| Perubahan | Deskripsi | Tanggal |
| --- | --- | --- |
| Kebijakan terkelola yang diperbarui | Resource Explorer memperbarui kebijakan AWS terkelola berikut untuk mendukung penelusuran multi-akun:<br>• AWSResourceExplorerFullAccess<br>• AWSResourceExplorerReadOnlyAccess | 14 November 2023 |
| AWSResourceExplorerServiceRolePolicy—Kebijakan yang diperbarui untuk mendukung pencarian multi-akun dengan Organizations | Resource Explorer menambahkan izin ke kebijakan peran terkait layanan AWSResourceExplorerServiceRolePolicy yang memungkinkan Resource Explorer mendukung penelusuran multi-akun dengan Organizations:<br>• organizations:ListAWSServiceAccessForOrganization<br>• organizations:DescribeAccount<br>• organizations:DescribeOrganization<br>• organizations:ListAccounts<br>• organizations:ListDelegatedAdministrators | 14 November 2023 |

| Perubahan | Deskripsi | Tanggal |
| --- | --- | --- |
| AWSResourceExplorerServiceRolePolicy—Kebijakan yang diperbarui untuk mendukung jenis sumber daya tambahan | Resource Explorer menambahkan izin ke kebijakan peran terkait layanan `AWSResourceExplorerServiceRolePolicy` yang memungkinkan layanan mengindeks jenis sumber daya berikut:<br>• accessanalyzer: analyzer<br>• acmpca:sertifikat otoritas<br>• amplify:aplikasi<br>• amplify:backendenvironment<br>• amplify:cabang<br>• amplify:domainasosiasi<br>• amplifyuibuilder:komponen<br>• amplifyuibuilder:tema<br>• appintegration:eventintegration<br>• apprunner:layanan<br>• appstream: appblock<br>• appstream: aplikasi<br>• appstream: armada<br>• appstream: imagebuilder<br>• appstream: tumpukan<br>• appsync:graphqlapi<br>• aps:rulegroupsnamespace<br>• aps:ruang kerja<br>• apigateway:restapi | 17 Oktober 2023 |

| Perubahan | Deskripsi | Tanggal |
| --- | --- | --- |
| | • apigateway:penyebaran<br>• athena:datacatalog<br>• athena:kelompok kerja<br>• penskalaan otomatis: autoscalinggroup<br>• backup: backupplan<br>• batch: computeenvironment<br>• batch: jobqueue<br>• batch: penjadwalan kebijakan<br>• cloudformation:tumpukan<br>• cloudformation:stackset<br>• cloudfront:fieldlevelencryptionconfig<br>• cloudfront:fieldlevelencryptionprofile<br>• cloudfront:originaccesscontrol<br>• cloudtrail: jejak<br>• codeartifact:domain<br>• codeartifact:repositori<br>• kodekomit: repositori<br>• codeguruprofiler:profilinggroup<br>• codestarconnections:koneksi<br>• databrew: dataset<br>• databrew: resep<br>• databrew: aturan<br>• detektif: grafik | |

| Perubahan | Deskripsi | Tanggal |
| --- | --- | --- |
| | • layanan direktori:direktori<br>• ec2:carriergateway<br>• ec2: verifiedaccessendpoint<br>• ec2: verifiedaccessgroup<br>• ec2:verifiedaccessinstance<br>• ec2: verifiedaccesstrustprovider<br>• ecr: repositori<br>• elasticache:cachesecuritygroup<br>• elasticfilesystem:accesspoint<br>• acara:aturan<br>• terbukti:percobaan<br>• jelas:fitur<br>• terbukti:peluncuran<br>• terbukti:proyek<br>• ruang sirip: lingkungan<br>• firehose:deliverystream<br>• faultinjectionsimulator:experimenttemplate<br>• perkiraan:datasetgroup<br>• prakiraan: dataset<br>• detektor penipu: detektor<br>• penipu detektor: entitytype<br>• penipu detektor: eventtype<br>• pendeteksi penipu: label<br>• pendeteksi penipu: hasil<br>• pendeteksi penipu: variabel<br>• gamelift:alias | |

| Perubahan | Deskripsi | Tanggal |
| --- | --- | --- |
| | • globalaccelerator: akselerator<br>• globalaccelerator: endpointgroup<br>• globalaccelerator: pendengar<br>• lem: database<br>• lem: pekerjaan<br>• lem: meja<br>• lem: pemicu<br>• greengrass:kelompok<br>• healthlake:fhirdatastore<br>• iam:virtualmfadevice<br>• imagebuilder:componentbuildversion<br>• imagebuilder:komponen<br>• imagebuilder:containerrecipe<br>• imagebuilder:distributionconfiguration<br>• imagebuilder:imagebuildversion<br>• imagebuilder:imagepipeline<br>• imagebuilder:imagerecipe<br>• imagebuilder:gambar<br>• imagebuilder:infrastrukturkonfigurasi<br>• iot: otorisasi<br>• IOT: JobTemplate<br>• IOT: mitigasiaksi | |

| Perubahan | Deskripsi | Tanggal |
| --- | --- | --- |
| | • iot: provisioningtemplate<br>• iot: profil keamanan<br>• IOT: hal<br>• iot:topikruledestinasi<br>• iotanalitik: saluran<br>• iotanalitik: dataset<br>• iotanalitik: datastore<br>• iotanalitik: pipa<br>• iotevents:alarmmodel<br>• iotevents:detectormodel<br>• iotevents:masukan<br>• iotsitewisewise:model aset<br>• iotsitewisewise:aset<br>• iotsitewisewise:gateway<br>• iottwinmaker: ruang kerja<br>• iv:saluran<br>• iv:streamkey<br>• kafka:cluster<br>• kinesisvideo:aliran<br>• lambda:alias<br>• lambda: layerversion<br>• lambda: lapisan<br>• lookoutmetrics:alert<br>• lookoutvision:proyek<br>• mediapackage:saluran<br>• mediapackage:origi nendpoint<br>• mediatailor:konfigurasi pemutaran | |

| Perubahan | Deskripsi | Tanggal |
| --- | --- | --- |
| | • memoridb: acl<br>• memorydb: cluster<br>• memorydb: parametergroup<br>• memorydb: pengguna<br>• penargetan mobile:aplikasi<br>• penargetan mobile:segmen<br>• Penargetan Mobilet:T emplate<br>• networkfirewall:firewallpolicy<br>• networkfirewall:firewall<br>• manajer jaringan: globalnet work<br>• manajer jaringan: perangkat<br>• manajer jaringan:tautan<br>• manajer jaringan: lampiran<br>• manajer jaringan: corenetwo rk<br>• panorama:paket<br>• qldb:jurnalkinesisstreamsfo rledger<br>• qldb: buku besar<br>• rds:bluegreendeployment<br>• refactorspace: aplikasi<br>• refactorspace: lingkungan<br>• refactorspace: rute<br>• refactorspace: layanan<br>• rekognisi: proyek<br>• resiliencehub: aplikasi<br>• resiliencehub:resiliencypol icy | |

| Perubahan | Deskripsi | Tanggal |
| --- | --- | --- |
| | • kumpulan sumber daya:kelompok<br>• route53:recoverygroup<br>• route53:resourceset<br>• route53:firewalldomain<br>• route53:firewallrulegroup<br>• route53:resolverendpoint<br>• route53:resolverrule<br>• pembuat sagemaker:model<br>• pembuat sagemaker :notebookinstance<br>• penandatangan:signingprofile<br>• ssmincidents:responseplan<br>• ssm:inventoryentry<br>• ssm:resourcedatasync<br>• negara bagian:aktivitas<br>• aliran waktu:database<br>• kebijaksanaan: asisten<br>• kebijaksanaan: asisten asosiasi<br>• kebijaksanaan:pengetahuan | |

| Perubahan | Deskripsi | Tanggal |
| --- | --- | --- |
| AWSResourceExplorerServiceRolePolicy—Kebijakan yang diperbarui untuk mendukung jenis sumber daya tambahan | Resource Explorer menambahkan izin ke kebijakan peran terkait layanan AWSResourceExplorerServiceRolePolicy yang memungkinkan layanan mengindeks jenis sumber daya berikut:<br>• codebuild: proyek<br>• codepipeline:pipa<br>• cognito:identitypool<br>• cognito:userpool<br>• ecr: repositori<br>• efs:sistem file<br>• elasticbeanstalk:aplikasi<br>• elasticbeanstalk:applicationversion<br>• elasticbeanstalk:lingkungan<br>• iot: kebijakan<br>• iot: topicrule<br>• langkah-langkah:statemachine<br>• s3: ember | 1 Agustus 2023 |

| Perubahan | Deskripsi | Tanggal |
| --- | --- | --- |
| AWSResourceExplorerServiceRolePolicy—Kebijakan yang diperbarui untuk mendukung jenis sumber daya tambahan | Resource Explorer menambahkan izin ke kebijakan peran terkait layanan `AWSResourceExplorerServiceRolePolicy` yang memungkinkan layanan mengindeks jenis sumber daya berikut:<br>• elastisis:cluster<br>• elasticache:globalreplicationgroup<br>• elasticache:parametergroup<br>• elasticache:replikasi grup<br>• elasticache:reserved-instance<br>• elastisis:snapshot<br>• elasticache:subnetgroup<br>• elastis: pengguna<br>• elasticache:usergroup<br>• lambda: konfigurasi penandatanganan kode<br>• lambda: pemetaan sumber-acara<br>• sqs:antrian | 7 Maret 2023 |

| Perubahan | Deskripsi | Tanggal |
| --- | --- | --- |
| Kebijakan terkelola baru | Resource Explorer menambahkan kebijakan AWS terkelola berikut:<br>• AWSResourceExplorerFullAccess<br>• AWSResourceExplorerReadOnlyAccess<br>• AWSResourceExplorerServiceRolePolicy | 7 November 2022 |
| Resource Explorer mulai melacak perubahan | Resource Explorer mulai melacak perubahan untuk kebijakan AWS terkelolanya. | 7 November 2022 |

## Menggunakan peran terkait layanan untuk Resource Explorer

Penjelajah Sumber Daya AWS menggunakan AWS Identity and Access Management (IAM) peran tertaut layanan. Peran terkait layanan adalah jenis unik peran IAM yang ditautkan langsung ke Resource Explorer. Peran terkait layanan telah ditentukan sebelumnya oleh Resource Explorer dan menyertakan semua izin yang diperlukan layanan untuk memanggil orang lain Layanan AWS atas nama Anda.

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

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat AWSlayanan yang bekerja dengan IAM di Panduan Pengguna IAM. Di sana, cari layanan yang memiliki Ya di kolom Peran terkait layanan. Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

## Izin peran terkait layanan untuk Resource Explorer

Resource Explorer menggunakan nama peran terkait layanan. `AWSServiceRoleForResourceExplorer` Peran ini memberikan izin ke layanan Resource Explorer untuk melihat sumber daya dan AWS CloudTrail peristiwa atas nama Anda Akun AWS dan untuk mengindeks sumber daya tersebut untuk mendukung penelusuran.

Peran `AWSServiceRoleForResourceExplorer` terkait layanan hanya mempercayai layanan dengan prinsip layanan berikut untuk mengambil peran:

- `resource-explorer-2.amazonaws.com`

Kebijakan izin peran bernama AWSResourceExplorerServiceRolePolicy memungkinkan akses hanya-baca Resource Explorer untuk mengambil nama dan properti sumber daya untuk sumber daya yang didukung. AWS Untuk melihat layanan dan sumber daya yang didukung Resource Explorer, lihat Jenis sumber daya yang dapat Anda cari dengan Resource Explorer. Untuk daftar lengkap semua tindakan yang dapat dilakukan peran ini, Anda dapat melihat `AWSResourceExplorerServiceRolePolicy` kebijakan di konsol IAM.

Principal adalah entitas IAM seperti pengguna, grup, atau peran. Jika Anda membiarkan Resource Explorer membuat peran terkait layanan untuk Anda saat membuat indeks di Wilayah pertama akun, maka prinsipal yang melakukan tugas hanya memerlukan izin yang diperlukan untuk membuat indeks Resource Explorer. Untuk membuat peran terkait layanan secara manual menggunakan IAM, maka prinsipal yang melakukan tugas harus memiliki izin untuk membuat peran terkait layanan. Untuk informasi selengkapnya, silakan lihat Izin peran tertaut layanan di Panduan Pengguna IAM.

## Membuat peran terkait layanan untuk Resource Explorer

Anda tidak perlu membuat peran tertaut layanan secara manual. Saat Anda mengaktifkan Resource Explorer diAWS Management Console, atau menjalankan CreateIndexyang pertama Wilayah AWS di akun Anda menggunakan AWS CLI atau AWS API, Resource Explorer akan membuat peran terkait layanan untuk Anda.

Jika Anda menghapus peran terkait layanan ini, dan kemudian perlu membuatnya lagi, Anda dapat menggunakan proses yang sama untuk membuat ulang peran di akun Anda. Saat Anda RegisterResourceExplorerberada di Wilayah pertama di akun Anda, Resource Explorer akan membuat peran terkait layanan untuk Anda lagi.

### Mengedit peran terkait layanan untuk Resource Explorer

Resource Explorer tidak mengizinkan Anda mengedit peran `AWSServiceRoleForResourceExplorer` terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat menyunting penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, silakan lihat Menyunting peran tertaut layanan dalam Panduan Pengguna IAM.

### Menghapus peran terkait layanan untuk Resource Explorer

Anda juga dapat menggunakan konsol IAM, AWS CLI, atau API AWS untuk menghapus secara manual peran tertaut layanan. Untuk melakukan ini, Anda harus terlebih dahulu menghapus indeks Resource Explorer dari setiap Wilayah AWS akun Anda dan kemudian Anda dapat menghapus peran terkait layanan secara manual.

> **Note**
>
> Jika layanan Resource Explorer menggunakan peran saat Anda mencoba menghapus sumber daya, penghapusan gagal. Jika itu terjadi, pastikan bahwa semua indeks dari semua Wilayah dihapus, lalu tunggu beberapa menit dan coba operasi lagi.

Untuk menghapus peran tertaut layanan secara manual menggunakan IAM

Gunakan konsol IAM, AWS CLI, atau AWS API untuk menghapus peran terkait layanan `AWSServiceRoleForResourceExplorer`. Untuk informasi selengkapnya, lihat Menghapus peran tertaut layanan dalam Panduan Pengguna IAM.

### Wilayah yang Didukung untuk peran terkait layanan Resource Explorer

Resource Explorer mendukung penggunaan peran terkait layanan di semua Wilayah tempat layanan tersedia. Untuk informasi selengkapnya, lihat Layanan AWSTitik akhir di. Referensi Umum Amazon Web Services

## IzinPenjelajah Sumber Daya AWS pemecahan masalah

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temukan saat bekerja dengan Resource Explorer danAWS Identity and Access Management (IAM).

Topik



## Saya tidak berwenang untuk melakukan tindakan di Resource

Jika AWS Management Console memberi tahu bahwa Anda tidak diotorisasi untuk melakukan tindakan, Anda harus menghubungi administrator untuk mendapatkan bantuan. Administrator Anda adalah orang yang memberikan kredenisasi yang Anda gunakan untuk mencoba operasi ini.

Misalnya, terjadi ketika seseorang mengasumsikan peran IAM`MyExampleRole` mencoba menggunakan konsol untuk melihat detail tentang suatu tampilan, tetapi tidak memiliki`resource-explorer-2:GetView` izin.

```
User: arn:aws:iam::123456789012:role/MyExampleRole is not authorized to perform:
 resource-explorer-2:GetView on resource: arn:aws:resource-explorer-2:us-
east-1:123456789012:view/EC2-Only-View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

Dalam hal ini, orang yang menggunakan peran harus meminta administrator memperbarui kebijakan izin peran untuk mengizinkan akses ke tampilan menggunakan`resource-explorer-2:GetView` tindakan.

## Saya ingin mengizinkan orang di luar sayaAkun AWS

Anda dapat membuat peran yang dapat digunakan para pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi akses pada orang ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa hal berikut:

- Untuk mempelajari apakah Resource Explorer mendukung fitur-fitur ini, lihatCara kerja Resource Explorer dengan IAM.
- Untuk mempelajari cara memberikan akses ke sumber daya di seluruh Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di akun Akun AWS lain yang Anda miliki dalam Panduan Pengguna IAM.

- Untuk mempelajari cara memberikan akses ke sumber daya Anda ke Akun AWS pihak ketiga, lihat Menyediakan akses ke akun Akun AWS yang dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (gabungan identitas) dalam Panduan Pengguna IAM .
- Untuk mempelajari perbedaan antara penggunaan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Perbedaan IAM role dan kebijakan berbasis sumber daya di Panduan Pengguna IAM.

# Perlindungan data di Penjelajah Sumber Daya AWS

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

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

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk melakukan komunikasi dengan sumber daya AWS. Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Siapkan API dan log aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi enkripsi AWS, bersama dengan semua kontrol keamanan default dalam Layanan AWS.
- Gunakan layanan keamanan terkelola lanjutan seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.

- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 ketika mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Untuk informasi selengkapnya tentang titik akhir FIPS yang tersedia, silakan lihat Standar Pemrosesan Informasi Federal (FIPS) 140-2.

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

### Enkripsi saat tidak aktif

Data yang disimpan oleh Resource Explorer mencakup daftar sumber daya yang diindeks dan ARN terkait yang digunakan oleh pelanggan dan pandangan untuk mengaksesnya.

Data ini dienkripsi saat diam dengan menggunakan AWS Key Management Service(AWS KMS) kunci enkripsi simetris yang mengimplementasikan Advanced Encryption Standard (AES) dalam Galois Counter Mode (GCM) dengan kunci 256-bit (AES-256-GCM).

### Enkripsi dalam transit

Permintaan pelanggan dan semua data terkait dienkripsi dalam perjalanan menggunakan Transport Later Security (TLS) 1.2 atau yang lebih baru. Semua titik akhir Resource Explorer mendukung HTTPS untuk mengenkripsi data dalam perjalanan. Untuk daftar titik akhir layanan Resource Explorer, lihat Penjelajah Sumber Daya AWStitik akhir dan kuota di. Referensi Umum AWS

## Validasi kepatuhan untuk Penjelajah Sumber Daya AWS

Untuk mengetahui apakah suatu Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWSdi Lingkup oleh Program Kepatuhan. Untuk informasi umum, silakan lihat Program Kepatuhan AWS .

Anda bisa mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat AWS ArtifactMengunduh Mengunduh laporan AWS Artifact di Panduan AWS Artifact Pengguna.

Tanggung jawab kepatuhan Anda saat menggunakan Resource Explorer ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWSmenyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Quick Start Keamanan dan Kepatuhan – Panduan deployment ini membahas pertimbangan arsitektur dan menyediakan langkah–langkah untuk melakukan deployment terhadap lingkungan dasar di AWS yang menjadi fokus keamanan dan kepatuhan.
- Arsitektur untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi yang memenuhi syarat HIPAA.

  > **Note**
  >
  > Tidak semua memenuhi syarat Layanan AWS HIPAA. Untuk informasi selengkapnya, lihat Referensi Layanan yang Memenuhi Syarat HIPAA.

- Sumber Daya Kepatuhan AWS – Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan Developer AWS Config – AWS Config menilai seberapa patuh konfigurasi sumber daya Anda terhadap praktik internal, panduan industri, dan peraturan.
- AWS Security Hub – Layanan AWS ini memberikan pandangan yang komprehensif tentang status keamanan Anda di dalam AWS yang membantu Anda memeriksa kepatuhan terhadap standar industri dan praktik terbaik yang terkait dengan keamanan.

## Ketahanan di Penjelajah Sumber Daya AWS

InfrastrukturAWS global dibangun di sekitarWilayah AWS dan Availability Zone. Wilayah memberikan beberapa Zona Ketersediaan yang terpisah dan terisolasi secara fisik, yang terkoneksi melalui jaringan latensi rendah, throughput tinggi, dan sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Availability Zone memiliki ketersediaan yang lebih baik, toleran terhadap kegagalan, dan dapat diukur skalanya jika dibandingkan dengan satu atau beberapa infrastruktur pusat data tradisional.

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

# Keamanan infrastruktur dalam Penjelajah Sumber Daya AWS

Sebagai layanan terkelola,Penjelajah Sumber Daya AWSdilindungi olehAWSkeamanan jaringan global. Untuk informasi tentangAWSlayanan keamanan dan bagaimanaAWSmelindungi infrastruktur, lihatAWSKeamanan Cloud. Untuk mendesainAWSlingkungan menggunakan praktik terbaik untuk keamanan infrastruktur, lihatPerlindungan InfrastrukturdiPilar KeamananAWSKerangka Kerja yang Diarsiteksikan.

Anda menggunakanAWSpanggilan API yang dipublikasikan untuk mengakses Resource Explorer melalui jaringan. Klien harus mendukung hal berikut:

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

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

Untuk informasi lebih lanjut tentangAWSprosedur keamanan jaringan global, lihatAmazon Web Services: Ikhtisar Proses Keamananwhitepaper.

# Penjelajah Sumber Daya AWS Pemantauan

Pemantauan adalah bagian penting dari pemeliharaan keandalan, ketersediaan, dan kinerjaPenjelajah Sumber Daya AWS danAWS solusi Anda yang lain. AWSmenyediakan alat pemantauan berikut untuk mengawasi Resource Explorer, melaporkan saat terjadi kesalahan, dan mengambil tindakan otomatis jika diperlukan:

- AWS CloudTrail merekam panggilan API dan kejadian terkait yang dilakukan oleh atau atas Akun AWS Anda dan mengirimkan berkas log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun yang memanggil AWS, alamat IP asal panggilan dilakukan, dan waktu panggilan terjadi. Untuk informasi selengkapnya, lihat Mencatat panggilan API Penjelajah Sumber Daya AWS menggunakan AWS CloudTrail dan Panduan Pengguna AWS CloudTrail.

## Mencatat panggilan API Penjelajah Sumber Daya AWS menggunakan AWS CloudTrail

Penjelajah Sumber Daya AWSterintegrasi denganAWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atauLayanan AWS di Resource. CloudTrail merekam semua panggilan API untuk Resource Explorer sebagai kejadian. Panggilan yang direkam mencakup panggilan dari konsol Resource Explorer dan panggilan kode ke operasi API Resource.

Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman berkelanjutan ke bucket Amazon S3, termasuk peristiwa untuk Resource. CloudTrail Jejak adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai berkas log ke bucket Amazon S3 yang telah Anda tentukan. Jika Anda tidak membuat konfigurasi jejak, Anda masih dapat melihat kejadian terbaru dalam konsol CloudTrail di Riwayat peristiwa. Menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat ke Resource, alamat IP asal permintaan tersebut dibuat, siapa yang membuat permintaan, kapan permintaan dibuat, dan detail lainnya.

Untuk mempelajari lebih lanjut CloudTrail, lihat PanduanAWS CloudTrail Pengguna.

### Informasi Resource Explorer di CloudTrail

CloudTrail diaktifkan pada AndaAkun AWS saat Anda membuat akun. Ketika aktivitas terjadi di Penjelajah Sumber, aktivitas tersebut dicatat dalam CloudTrail peristiwa bersamaLayanan AWS

peristiwa lainnya di Riwayat. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di Akun AWS Anda. Untuk informasi selengkapnya, lihat Menampilkan peristiwa dengan riwayat CloudTrail Peristiwa.

> **Important**
>
> Anda dapat menemukan semua peristiwa Resource Explorer dengan mencari Event source = resource-explorer-2.amazonaws.com

Untuk catatan berkelanjutan tentang peristiwa di AndaAkun AWS, termasuk peristiwa untuk Resource, buat jejak. Jejak memungkinkan CloudTrail untuk mengirim berkas log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan berkas log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi lainnyaLayanan AWS untuk menganalisis lebih lanjut dan bertindak berdasarkan data peristiwa yang dikumpulkan di CloudTrail log. Untuk informasi lebih lanjut, lihat topik berikut di Panduan Pengguna AWS CloudTrail:

- Membuat jejak untuk AndaAkun AWS
- AWSintegrasi layanan dengan CloudTrail Log
- Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima berkas CloudTrail log dari beberapa Wilayah
- Menerima berkas CloudTrail log dari beberapa akun

Semua tindakan Resource Explorer dicatat oleh CloudTrail dan didokumentasikan dalam ReferensiPenjelajah Sumber Daya AWS API. Misalnya, panggilan ke`CreateIndex`,`DeleteIndex`, dan`UpdateIndex` tindakan menghasilkan entri dalam file CloudTrail log.

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

- Akun AWSKredendenfikasi root
- Kredensyal keamanan sementara dari peranAWS Identity and Access Management (IAM) atau pengguna federasi.
- Kredenfikasi keamanan jangka panjang dari pengguna IAM.
- AWSLayanan lain.

> **Important**
>
> Untuk alasan keamanan`Tags`, semua`Filters`,, dan`QueryString` nilai-nilai dihapus dari entri CloudTrail jejak.

Untuk informasi selengkapnya, lihat Elemen userIdentity CloudTrail .

## Memahami entri berkas log Resource

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

Topik

- CreateIndex
- DeleteIndex
- UpdateIndexType
- Pencarian
- CreateView
- DeleteView
- DisassociateDefaultView

### CreateIndex

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan`CreateIndex` tindakan.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-166EXAMPLE",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-166EXAMPLE",
        "accountId": "123456789012",
```

```
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-23T19:13:59Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "CreateIndex",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.create-index",
    "requestParameters": {
        "ClientToken": "792ee665-58af-423c-bfdb-d7c9aEXAMPLE"
    },
    "responseElements": {
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
        "State": "CREATING",
        "CreatedAt": "2022-08-23T19:13:59.775Z"
    },
    "requestID": "a193afe9-17ff-4f30-ae0a-73bb0EXAMPLE",
    "eventID": "2ec50598-4de6-474d-bd0e-f5c00EXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

## DeleteIndex

Contoh berikut menunjukkan entri CloudTrail panjang yang menunjukkan`DeleteIndex` tindakan.

> **Note**
>
> Tindakan ini juga secara asinkron menghapus semua tampilan untuk akun di Wilayah tersebut, yang menghasilkan`DeleteView` peristiwa untuk setiap tampilan yang dihapus.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:My-Role-Name",
        "arn": "arn:aws:sts::123456789012:assumed-role/My-Admin-Role/My-Delegated-
Role",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/My-Admin-Role",
                "accountId": "123456789012",
                "userName": "My-Admin-Role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T18:33:06Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-23T19:04:06Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "DeleteIndex",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.delete-index",
    "requestParameters": {
```

```
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "State": "DELETING",
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    },
    "requestID": "d7d80bd2-cd2d-47fb-88d6-5133aEXAMPLE",
    "eventID": "675eab39-c514-4d32-989d-0ea98EXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


## UpdateIndexType

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan`UpdateIndexType` tindakan untuk mempromosikan indeks dari tipe`LOCAL` ke`AGGREGATOR`.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
```

```
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-23T19:21:18Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "UpdateIndexType",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.update-index-type",
    "requestParameters": {
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
        "Type": "AGGREGATOR"
    },
    "responseElements": {
        "Type": "AGGREGATOR",
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
        "LastUpdatedAt": "2022-08-23T19:21:17.924Z",
        "State": "UPDATING"
    },
    "requestID": "a145309d-df14-4c2e-a9f6-8ed45EXAMPLE",
    "eventID": "ed33ab96-f5c6-4a77-a69a-8585aEXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


## Pencarian

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan`Search` tindakan.

> **Note**
>
> Untuk alasan keamanan, semua referensi ke`TagFilters`,, dan`QueryString` parameter disunting dalam entri CloudTrail jejak.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-03T16:50:11Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "Search",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.search",
    "requestParameters": {
        "QueryString": "***"
    },
    "responseElements": null,
    "requestID": "22320db5-b194-446f-b9f4-e603bEXAMPLE",
    "eventID": "addb3bca-0c41-46bf-a5e6-42299EXAMPLE",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

## CreateView

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan`CreateView` tindakan.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-01-20T21:54:48Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "CreateView",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.create-view",
    "requestParameters": {
        "ViewName": "CTTagsTest",
        "Tags": "***"
    },
    "responseElements": {
        "View": {
            "Filters": "***",
            "IncludedProperties": [],
            "LastUpdatedAt": "2023-01-20T21:54:48.079Z",
```

```
            "Owner": "123456789012",
            "Scope": "arn:aws:iam::123456789012:root",
            "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
CTTest/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
        }
    },
    "requestID": "b22d8ced-4905-42c4-b1aa-ef713EXAMPLE",
    "eventID": "f62e339f-1070-41a8-a6ec-12491EXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

## DeleteView

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan peristiwa yang dapat terjadi ketika`DeleteView` tindakan dimulai secara otomatis karena`DeleteIndex` operasi yang samaWilayah AWS.

> **Note**
>
> Jika tampilan yang dihapus adalah tampilan default untuk Wilayah, tindakan ini secara asinkron juga melepaskan tampilan sebagai default. Ini menghasilkan sebuah`DisassociateDefaultView` acara.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
```

```
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-09-16T19:33:27Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "DeleteView",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.delete-view",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "cd174d1e-0a24-4b47-8b67-d024aEXAMPLE",
    "readOnly": false,
    "resources": [{
        "accountId": "334026708824",
        "type": "AWS::ResourceExplorer2::View",
        "ARN": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
CTTest/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }],
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


## DisassociateDefaultView

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan peristiwa yang dapat terjadi ketika`DisassociateDefaultView` tindakan dimulai secara otomatis karena`DeleteView` operasi pada tampilan default saat ini.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
```

```
        "accountId": "123456789012",
        "invokedBy": "resource-explorer-2.amazonaws.com"
    },
    "eventTime": "2022-09-16T19:33:26Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "DisassociateDefaultView",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.disassociate-default-view",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "d8016cb1-5c23-4ea4-bda2-70b03EXAMPLE",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

# Membuat sumber daya Resource Explorer dengan CloudFormation

Penjelajah Sumber Daya AWSterintegrasi denganAWS CloudFormation, layanan yang membantu Anda memodelkan dan menyiapkan AWS sumber daya Anda. Integrasi ini membantu Anda menghabiskan lebih sedikit waktu untuk membuat dan mengelola sumber daya dan infrastruktur Anda. Anda membuat templat yang menggambarkan sumber daya AWS yang Anda inginkan, dan CloudFormation memasok persediaan dan mengonfigurasi sumber daya tersebut untuk Anda. Contoh sumber daya termasuk indeks, tampilan, atau penugasan tampilan default untuk. Wilayah AWS

Saat menggunakanCloudFormation, Anda dapat menggunakan kembali templat Anda untuk menyiapkan sumber daya sumber daya sumber daya sumber daya sumber daya secara konsisten dan berulang kali. Cukup jelaskan sumber daya Anda satu kali, lalu sediakan sumber daya yang sama berulang kali dalam beberapa Akun AWS dan Wilayah.

Menggunakan AWS CloudFormation untuk menyebarkan Resource Explorer ke AWS Organizations

Anda dapat menggunakan AWS CloudFormation StackSets untuk menyebarkan Resource Explorer ke semua akun di organisasi Anda. Ketika Anda menambahkan atau membuat akun anggota di organisasi Anda, StackSets dapat secara otomatis mengkonfigurasi indeks di masing-masingWilayah AWS, termasuk indeks agregator tempat Anda menentukan, ke setiap akun anggota baru. Untuk petunjuk, lihat Menerapkan Resource Explorer ke akun di organisasi.

## Resource Explorer dan CloudFormation template

Untuk menyediakan dan mengonfigurasi sumber daya untuk sumber daya untuk sumber daya dan layanan terkait, Anda harus memahami AWS CloudFormationtemplat. Templat adalah file teks dengan format JSON atau YAML. Templat ini menjelaskan sumber daya yang ingin Anda sediakan di tumpukan CloudFormation Anda. Jika Anda tidak terbiasa dengan JSON atau YAML, Anda dapat menggunakan AWS CloudFormation Designer untuk membantu Anda memulai dengan templat CloudFormation. Untuk informasi selengkapnya, lihat Apa yang dimaksud dengan AWS CloudFormation Designer? dalam Panduan Pengguna AWS CloudFormation.

Resource Explorer mendukung pembuatan jenis sumber daya berikut diCloudFormation:

- Indeks - Membuat indeks di Wilayah dan mengaktifkan Resource Explorer di Wilayah tersebut. Anda dapat menentukan bahwa indeks menjadi baik lokal atau indeks agregator untuk. Akun

AWS Untuk informasi selengkapnya, lihat Mengaktifkan Resource ExplorerWilayah AWS untuk mengindeks sumber daya Anda dan Mengaktifkan pencarian lintas wilayah dengan membuat indeks agregator.

- Tampilan - Membuat tampilan yang menentukan hasil apa yang dapat muncul saat pengguna melakukan pencarian. Setiap operasi pencarian harus menentukan tampilan. Anda harus memberikan izin kepada pengguna untuk menggunakan tampilan yang ingin mereka akses. Untuk informasi selengkapnya, lihat Mengelola tampilan Resource Explorer untuk menyediakan akses ke penelusuran.

  > **Note**
  >
  > Anda harus membuat indeks di Wilayah sebelum Anda dapat membuat tampilan di Wilayah yang sama. Jika Anda membuat indeks dan melihat sebagai bagian dari tumpukan yang sama, gunakan `DependsOn` atribut pada tampilan, seperti yang ditunjukkan dalam contoh template berikut, untuk memastikan bahwa indeks dibuat terlebih dahulu.

- DefaultViewAssociation- Menetapkan tampilan yang ditentukan menjadi default di Daerahnya. Bila pengguna tidak secara eksplisit menentukan tampilan yang akan digunakan untuk operasi pencarian, Resource Explorer mencoba menggunakan tampilan default yang terkait dengan Wilayah tempat pengguna melakukan pencarian. Untuk informasi selengkapnya, lihat Mengatur tampilan default dalamWilayah AWS

Contoh berikut menggambarkan bagaimana Anda dapat membuat satu indeks dan tampilan di Wilayah yang sama, dan mengatur tampilan menjadi default untuk Wilayah.

YAML

```
Description: >-
  Sample CFN Stack setting up Resource Explorer with an aggregator index and a default
 view
Resources:
  SampleIndex:
    Type: 'AWS::ResourceExplorer2::Index'
    Properties:
      Type: AGGREGATOR
      Tags:
        Purpose: ResourceExplorer Sample CFN Stack
  SampleView:
    Type: 'AWS::ResourceExplorer2::View'
```

```
    Properties:
      ViewName: mySampleView
      IncludedProperties:
        - Name: tags
      Tags:
        Purpose: ResourceExplorer Sample CFN Stack
    DependsOn: SampleIndex
  SampleDefaultViewAssociation:
    Type: 'AWS::ResourceExplorer2::DefaultViewAssociation'
    Properties:
      ViewArn: !Ref SampleView
```

JSON

```
{
    "Description": "Sample CFN Stack setting up Resource Explorer with an aggregator
 index and a default view ",
    "Resources": {
        "SampleIndex": {
            "Type": "AWS::ResourceExplorer2::Index",
            "Properties": {
                "Type": "AGGREGATOR",
                "Tags": {
                    "Purpose": "ResourceExplorer Sample Stack"
                }
            }
        },
        "SampleView": {
            "Type": "AWS::ResourceExplorer2::View",
            "Properties": {
                "ViewName": "mySampleView",
                "IncludedProperties": [
                    {
                        "Name": "tags"
                    }
                ],
                "Tags": {
                    "Purpose": "ResourceExplorer Sample CFN Stack"
                }
            },
            "DependsOn": "SampleIndex"
        },
        "SampleDefaultViewAssociation": {
```

```
            "Type": "AWS::ResourceExplorer2::DefaultViewAssociation",
            "Properties": {
                "ViewArn": {
                    "Ref": "SampleView"
                }
            }
        }
    }
}
```

Untuk informasi lebih lanjut, termasuk contoh templat JSON dan YAKL untuk indeks dan tampilan sumber daya Resource Explorer, lihat referensi tipe sumber daya ResourceExplorer 2 di Panduan Pengguna. AWS CloudFormation

## Pelajari selengkapnya tentang AWS CloudFormation

Untuk mempelajari selengkapnya tentang CloudFormation, lihat sumber daya berikut:

- AWS CloudFormation
- AWS CloudFormationPanduan Pengguna
- AWS CloudFormationPanduan

# Pemecahan Masalah Explorer Sumber Daya Explorer

Jika Anda mengalami masalah saat bekerja dengan Resource Explorer, konsultasikan topik tersebut di bagian ini. Lihat jugaIzinPenjelajah Sumber Daya AWS pemecahan masalah di bagian Keamanan panduan ini.

Topik

- Masalah umum(halaman ini)
- Memecahkan masalah penyiapan dan konfigurasi Resource Explorer
- Memecahkan masalah pencarian Resource Explorer

## Masalah umum

Topik

- Saya menerima tautan ke Resource Explorer tetapi ketika saya membukanya, konsol hanya menunjukkan kesalahan.
- Mengapa pencarian terpadu di konsol menyebabkan kesalahan “akses ditolak” di CloudTrail log saya?

### Saya menerima tautan ke Resource Explorer tetapi ketika saya membukanya, konsol hanya menunjukkan kesalahan.

Beberapa alat pihak ketiga menghasilkan URL tautan ke halaman di Resource Explorer. Dalam beberapa kasus, URL tersebut tidak menyertakan parameter yang mengarahkan konsol ke tertentuWilayah AWS. Jika Anda membuka tautan semacam itu, konsol Resource Explorer tidak diberi tahu Wilayah mana yang akan digunakan, dan secara default menggunakan Wilayah terakhir yang digunakan pengguna untuk masuk. Jika pengguna tidak memiliki izin untuk mengakses Resource Explorer di Wilayah tersebut, maka konsol akan mencoba menggunakan Wilayah AS Timur (Virginia) (`us-east-1`), atau US West (Oregon) () (`us-west-2`) jika konsol tidak dapat dijangkau`us-east-1`.

Jika pengguna tidak memiliki izin untuk mengakses indeks di salah satu Regions tersebut, konsol Resource Explorer mengembalikan kesalahan.

Anda dapat mencegah masalah ini dengan memastikan bahwa semua pengguna memiliki izin berikut:

- `ListIndexes`— tidak ada sumber daya tertentu; menggunakan`*`.
- `GetIndex`untuk ARN dari setiap indeks yang dibuat di akun. Untuk menghindari keharusan mengulang kebijakan izin jika Anda menghapus dan membuat ulang indeks, sebaiknya gunakan`*`.

Kebijakan minimum untuk mencapai ini mungkin terlihat seperti contoh ini:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetIndex",
                "resource-explorer-2:ListIndexes",
            ],
            "Resource": "*"
        }
    ]
}
```

Atau, Anda dapat mempertimbangkan untuk melampirkan izinAWS terkelolaAWSResourceExplorerReadOnlyAccess untuk semua pengguna yang perlu menggunakan Resource Explorer. Itu memberikan izin yang diperlukan ini, ditambah izin yang diperlukan, lihat tampilan yang tersedia di Wilayah dan cari menggunakan tampilan tersebut.

## Mengapa pencarian terpadu di konsol menyebabkan kesalahan “akses ditolak” di CloudTrail log saya?

Pencarian terpadu diAWS Management Console memungkinkan prinsipal mencari dari halaman manapun di halamanAWS Management Console. Hasilnya dapat mencakup sumber daya dari akun kepala sekolah jika Resource Explorer diaktifkan dan dikonfigurasi untuk mendukung pencarian terpadu. Setiap kali Anda mulai mengetik di bilah pencarian terpadu, pencarian terpadu mencoba memanggil`resource-explorer-2:ListIndexes` operasi untuk memeriksa apakah itu dapat menyertakan sumber daya dari akun pengguna dalam hasil.

Pencarian terpadu menggunakan izin pengguna yang saat ini masuk untuk melakukan pemeriksaan ini. Jika pengguna tersebut tidak memiliki izin untuk memanggil`resource-explorer-2:ListIndexes` yang diberikan dalam kebijakan izin terlampirAWS Identity and Access Management (IAM), maka pemeriksaan gagal. Kegagalan itu ditambahkan sebagai`Access denied` entri di CloudTrail log Anda.

Entri CloudTrail log ini memiliki karakteristik sebagai berikut:

- Sumber acara:`resource-explorer-2.amazonaws.com`
- Nama acara:`ListIndexes`
- Kode kesalahan:`403` (Akses ditolak)

KebijakanAWS terkelola berikut ini mencakup izin untuk meneleponresource-explorer-2:ListIndexes. Jika Anda menetapkan salah satu dari ini ke prinsipal, atau kebijakan lain yang menyertakan izin ini, maka kesalahan ini tidak terjadi:

- AWSResourceExplorerReadOnlyAccess
- AWSResourceExplorerFullAccess
- ReadOnlyAccess
- ViewOnlyAccess

# Memecahkan masalah penyiapan dan konfigurasi Resource Explorer

Gunakan informasi di sini untuk membantu Anda mendiagnosis dan memperbaiki masalah yang dapat terjadi saat Anda mengatur atau mengoniapanPenjelajah Sumber Daya AWS.

Topik

- Saya mendapatkan pesan “akses ditolak” ketika saya mengajukan permintaan ke Resource Explorer
- Saya mendapatkan pesan "akses ditolak" ketika saya membuat permintaan dengan kredensial keamanan sementara

## Saya mendapatkan pesan “akses ditolak” ketika saya mengajukan permintaan ke Resource Explorer

- Pastikan bahwa Anda memiliki izin untuk memanggil tindakan dan sumber daya yang Anda minta. Administrator dapat memberikan izin dengan menetapkan kebijakan izinAWS Identity and Access Management (IAM) ke pokok IAM Anda, seperti peran, grup, atau pengguna.

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

  - Pengguna dan grup diAWS IAM Identity Center:

    Buat set izin. Ikuti petunjuk di Buat set izin di PanduanAWS IAM Identity Center Pengguna.

  - Pengguna yang dikelola dalam IAM melalui penyedia identitas:

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

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

  Kebijakan harus mengizinkan yang dimintaAction padaResource yang ingin Anda akses.

  Jika pernyataan kebijakan yang memberikan izin tersebut menyertakan syarat apapun, seperti time-of-day atau batasan alamat IP, maka Anda juga harus memenuhi persyaratan tersebut saat Anda mengirim permintaan. Untuk informasi tentang melihat atau mengubah kebijakan untuk pokok IAM, lihat Mengelola kebijakan IAM di Panduan Pengguna IAM.

- Jika Anda menandatangani permintaan API secara manual (tanpa menggunakan AWSSDK), verifikasi bahwa Anda menandatangani permintaan dengan benar.

## Saya mendapatkan pesan "akses ditolak" ketika saya membuat permintaan dengan kredensial keamanan sementara

- Pastikan bahwa pokok IAM yang Anda gunakan untuk membuat permintaan memiliki izin yang benar. Izin untuk kredensi keamanan sementara berasal dari kepala sekolah yang didefinisikan

dalam IAM, sehingga izin terbatas pada izin yang diberikan kepada kepala sekolah. Untuk informasi lebih lanjut tentang bagaimana izin kredensi keamanan sementara ditentukan, lihat Mengontrol izin untuk kredensi keamanan sementara di Panduan Pengguna IAM.

- Verifikasi bahwa permintaan Anda ditandatangani dengan benar dan bahwa permintaan tersebut memiliki bentuk yang baik. Untuk detailnya, lihat dokumentasi toolkit untuk SDK pilihan Anda atau Menggunakan kredensi sementara denganAWS sumber daya di Panduan Pengguna IAM.
- Verifikasikan bahwa kredensial keamanan sementara Anda belum kedaluwarsa. Untuk informasi selengkapnya, lihat Meminta kredensi keamanan sementara di Panduan Pengguna IAM.

# Memecahkan masalah pencarian Resource Explorer

Gunakan informasi di sini untuk membantu Anda mendiagnosis dan memperbaiki kesalahan umum yang dapat terjadi saat Anda mencari sumber daya menggunakan Resource Explorer.

Topik



## Mengapa beberapa sumber daya hilang dari hasil pencarian Resource Explorer saya?

Daftar berikut memberikan alasan mengapa beberapa sumber daya mungkin tidak muncul di hasil penelusuran Anda seperti yang diharapkan:

Pengindeksan awal belum selesai

Setelah Anda mengaktifkan Resource Explorer pada awalnyaWilayah AWS, dibutuhkan waktu hingga 36 jam untuk pengindeksan dan replikasi ke indeks agregator untuk menyelesaikannya. Coba pencarian Anda lagi nanti.

Sumber daya baru

Diperlukan beberapa menit agar sumber daya baru ditemukan oleh Resource Explorer dan ditambahkan ke indeks lokal. Coba lagi dalam beberapa menit.

Informasi tentang sumber daya baru di satu Wilayah belum disebarkan ke indeks agregator

Diperlukan beberapa waktu untuk detail tentang sumber daya baru yang ditemukan di satu Wilayah untuk diindeks di Wilayahnya sendiri dan kemudian direplikasi ke indeks agregator untuk akun tersebut. Sumber daya baru dapat muncul di hasil pencarian lintas wilayah hanya setelah replikasi selesai. Coba pencarian Anda lagi nanti.

Wilayah dengan sumber daya tidak mengaktifkan Resource Explorer

Administrator Anda menentukan Resource Explorer mana Wilayah AWS yang dapat beroperasi. Halaman Pengaturan menunjukkan Wilayah mana yang mengaktifkan Resource Explorer dan berisi indeks. Jika Wilayah dengan sumber daya Anda tidak diaktifkan, minta administrator Anda untuk mengaktifkan Resource Explorer di Wilayah tersebut.

Sumber daya ada di Wilayah yang berbeda, dan Wilayah yang dicari tidak berisi indeks agregator

Anda dapat mencari sumber daya di semua Wilayah di akun hanya dengan menggunakan tampilan di Wilayah yang berisi indeks agregator. Pencarian di Wilayah lain mengembalikan sumber daya hanya dari Wilayah tempat Anda melakukan pencarian.

Filter pada tampilan mengecualikan sumber daya itu

Setiap tampilan dapat menyertakan filter dalam konfigurasi yang membatasi hasil mana yang dapat disertakan dalam hasil penelusuran yang dibuat dengan tampilan itu. Pastikan sumber daya yang Anda cari cocok dengan filter dalam tampilan yang Anda gunakan untuk mencari. Untuk selengkapnya tentang filter, lihatFilter. Untuk informasi selengkapnya tentang tampilan, lihatTentang tampilan Resource Explorer.

Jenis sumber daya tidak didukung oleh Resource Explorer

Beberapa jenis sumber daya tidak didukung oleh Resource Explorer. Untuk informasi selengkapnya, lihat Jenis sumber daya yang dapat Anda cari dengan Resource Explorer.

Indeks atau tampilan tidak dikonfigurasi di Wilayah konsol

Jika indeks atau tampilan tidak dikonfigurasi di Wilayah yang diharapkan oleh konsol yang menggunakan widget, Anda tidak akan melihat hasil yang Anda harapkan. Untuk informasi selengkapnya, lihat Mengaktifkan pencarian lintas wilayah dengan membuat indeks agregator, dan Tentang tampilan Resource Explorer.

Tampilan Anda tidak menyertakan tag

Tag diperlukan oleh widget Resource Explorer. Jika tampilan Anda tidak menyertakan tag, sumber daya tidak akan disertakan dalam hasil Anda. Untuk informasi selengkapnya, lihat Menambahkan tag ke tampilan yang sudah ditonton.

Pencarian Anda menggunakan sintaks kueri penelusuran yang salah

Pencarian di Resource Explorer unik untuk layanan ini. Tanpa sintaks yang benar, Anda tidak akan menemukan sumber daya yang Anda harapkan. Untuk informasi selengkapnya, lihat Referensi sintaks kueri pencarian untuk Resource Explorer.

Anda baru-baru ini menandai sumber daya Anda

Setelah Anda menandai sumber daya, ada penundaan 30 detik sebelum sumber daya muncul di hasil penelusuran Anda.

Jenis sumber daya tidak mendukung filter tag

Jika filter tag tidak didukung oleh jenis sumber daya, filter tersebut tidak akan ditampilkan di widget Resource Explorer. Jenis sumber daya yang tidak mendukung filter tag adalah:

- `cloudfront:cache-policy`
- `cloudfront:origin-access-identity`
- `cloudfront:function`
- `cloudfront:origin-request-policy`
- `cloudfront:realtime-log-config`
- `cloudfront:response-headers-policy`
- `cloudwatch:dashboard`
- `docdb:globalcluster`
- `elasticache:globalreplicationgroup`
- `iam:group`
- `lambda:code-signing-config`
- `lambda:event-source-mapping`
- `ssm:windowtarget`
- `ssm:windowtask`
- `rds:auto-backup`
- `rds:global-cluster`
- `s3:accesspoint`

## Mengapa sumber daya saya tidak muncul di hasil penelusuran terpadu di konsol?

Hasil pencarian terpadu tersedia di bilah pencarian di bagian atas setiap AWS Management Console halaman. Namun, pencarian dapat mengembalikan sumber daya yang cocok dengan kueri di hasil penelusuran hanya setelah opsi konfigurasi berikut selesai:

- Harus ada indeks agregator di salah satu Wilayah di akun.
- Harus ada tampilan default di Wilayah yang berisi indeks agregator.
- Semua kepala sekolah (peran dan pengguna IAM) harus memiliki izin untuk mencari menggunakan tampilan default itu.

## Mengapa pencarian terpadu di konsol dan Resource Explorer terkadang memberikan hasil yang berbeda?

Hasil pencarian terpadu tersedia di bilah pencarian di bagian atas setiap AWS Management Console halaman. Saat Anda menggunakan pencarian terpadu, proses pencarian terpadu secara otomatis menyisipkan karakter wildcard (*) ke akhir istilah pertama yang Anda ketik dalam string kueri. Karakter wildcard itu tidak terlihat di kotak pencarian terpadu, tetapi itu memengaruhi hasil.

> **Important**
>
> Pencarian terpadu secara otomatis menyisipkan operator karakter wildcard (*) di akhir kata kunci pertama dalam string. Ini berarti bahwa hasil pencarian terpadu menyertakan sumber daya yang cocok dengan string apa pun yang dimulai dengan kata kunci yang ditentukan. Pencarian yang dilakukan oleh kotak teks Kueri pada halaman pencarian Sumber daya di konsol Resource Explorer tidak secara otomatis menambahkan karakter wildcard. Anda dapat memasukkan secara * manual setelah istilah apa pun dalam string pencarian.

## Izin apa yang saya perlukan untuk dapat mencari sumber daya?

Untuk mencari, Anda harus memiliki izin untuk melakukan kedua operasi berikut pada tampilan yang berada di Wilayah tempat Anda memanggil operasi:

- `resource-explorer-2:GetView`

- `resource-explorer-2:Search`

Ini dapat dilakukan dengan menambahkan pernyataan yang mirip dengan contoh berikut ke kebijakan yang ditetapkan untuk prinsipal IAM Anda.

```
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetView",
                "resource-explorer-2:Search"
            ],
            "Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-
View-Name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
        }
```

Anda dapat mengganti Amazon Resource Number (ARN) dari tampilan tertentu dengan ARN yang menyertakan wildcard (*) untuk memberikan izin ke semua tampilan yang cocok.

Jika Anda tidak menentukan tampilan dalam permintaan, Resource Explorer secara otomatis menggunakan tampilan default untuk Wilayah tempat Anda membuat permintaan. Jika Anda tidak memiliki izin untuk menggunakan tampilan default, bicarakan dengan administrator Anda.

> **Note**
>
> Bahkan jika Anda melihat sumber daya dalam hasil kueri penelusuran Resource Explorer, Anda memerlukan izin pada sumber daya itu sendiri untuk dapat berinteraksi dengan sumber daya itu.

# Jenis sumber daya yang dapat Anda cari dengan Resource Explorer

Topik



Tabel berikut mencantumkan jenis sumber daya yang didukung untuk penelusuran Penjelajah Sumber Daya AWS.

> **Catatan**
>
> - Beberapa jenis sumber daya diidentifikasi oleh string nama sumber daya Amazon (ARN) yang berbagi format umum dengan jenis sumber daya lain. Ketika ini terjadi, Resource Explorer dapat melaporkan sumber daya seperti jenis sumber daya lainnya. Untuk daftar jenis sumber daya yang terpengaruh oleh masalah ini, lihatJenis sumber daya yang muncul sebagai tipe lain.
> - Pada saat ini, tag yang dilampirkan ke sumber daya AWS Identity and Access Management (IAM), seperti peran atau pengguna, tidak dapat digunakan untuk pencarian.
> - Jika Anda memiliki akses terenkripsi ke beberapa sumber daya Anda, Resource Explorer tidak dapat menemukannya. Anda tidak akan melihat sumber daya ini di hasil pencarian Anda.

## Layanan dan jenis sumber daya yang didukung

Didukung Layanan AWS

- Amazon API Gateway
- AWS App Runner
- Amazon AppStream 2.0
- AWS AppSync

- Amazon Athena
- AWS Backup
- AWS Batch
- AWS CloudFormation
- Amazon CloudFront
- AWS CloudTrail
- Amazon CloudWatch
- Amazon CloudWatch Terbukti
- CloudWatch Log Amazon
- AWS CodeArtifact
- AWS CodeBuild
- AWS CodeCommit
- Amazon CodeGuru Profiler
- AWS CodePipeline
- AWS CodeConnections
- Amazon Cognito
- Amazon Connect
- Kebijaksanaan Amazon Connect
- Amazon Detective
- Amazon DynamoDB
- EC2 Image Builder
- Amazon ECR Public
- AWS Elastic Beanstalk
- Amazon ElastiCache
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- Amazon Elastic File System
- Penyeimbang Beban Elastis

- AWS Elemental MediaPackage
- AWS Elemental MediaTailor
- Amazon EMR Tanpa Server
- Amazon EventBridge
- AWS Fault Injection Service
- Amazon Forecast
- Amazon Fraud Detector
- Amazon GameLift
- AWS Global Accelerator
- AWS Glue
- AWS Glue DataBrew
- AWS Identity and Access Management
- Amazon Interactive Video Service
- AWS IoT
- AWS IoT Analytics
- AWS IoT Events
- AWS IoT Greengrass Version 1
- AWS IoT SiteWise
- AWS IoT TwinMaker
- AWS Key Management Service
- Amazon Kinesis
- Amazon Data Firehose
- Amazon Kinesis Video Streams
- AWS Lambda
- Amazon Lex
- Amazon Location Service
- Amazon Lookout for Metrics
- Amazon Lookout for Vision
- Layanan Terkelola Amazon untuk Apache Flink

- Layanan Terkelola Amazon untuk Prometheus
- Layanan Terkelola Amazon untuk Prometheus
- Amazon Managed Streaming untuk Apache Kafka
- AWS Migration Hub Refactor Spaces
- AWS Network Firewall
- AWS Network Manager
- OpenSearch Layanan Amazon
- AWS Panorama
- Amazon Personalize
- AWS Private Certificate Authority
- Amazon QLDB
- Amazon Redshift
- Amazon Rekognition
- Amazon Relational Database Service (Amazon RDS)
- AWS Resilience Hub
- AWS Resource Groups
- Penjelajah Sumber Daya AWS
- Amazon Route 53
- Kesiapan Pemulihan Amazon Route 53
- Amazon Route 53 Resolver
- Amazon SageMaker
- AWS Secrets Manager
- AWS Service Catalog
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Simple Storage Service (Amazon S3)
- AWS Step Functions
- AWS Systems Manager
- Akses Terverifikasi AWS
- AWS Wavelength

## Amazon API Gateway

- apigateway:restapis

## AWS App Runner

- apprunner:vpcconnector

## Amazon AppStream 2.0

- appstream:appblock
- appstream:application
- appstream:fleet
- appstream:stack

## AWS AppSync

- appsync:apis

## Amazon Athena

- athena:datacatalog
- athena:workgroup

## AWS Backup

- backup:backupplan

## AWS Batch

- batch:computeenvironment
- batch:jobqueue
- batch:schedulingpolicy

## AWS CloudFormation

- cloudformation:stack
- cloudformation:stackset

## Amazon CloudFront

- cloudfront:cache-policy
- cloudfront:distribution
- cloudfront:function
- cloudfront:fieldlevelencryptionconfig
- cloudfront:fieldlevelencryptionprofile
- cloudfront:origin-access-identity
- cloudfront:originaccesscontrol
- cloudfront:origin-request-policy
- cloudfront:realtime-log-config
- cloudfront:response-headers-policy

## AWS CloudTrail

- cloudtrail:trail

## Amazon CloudWatch

- cloudwatch:alarm
- cloudwatch:dashboard
- cloudwatch:insight-rule
- cloudwatch:metric-stream
- evidently:project

## Amazon CloudWatch Terbukti

- evidently:project/experiment
- evidently:project/feature
- evidently:project/launch

## CloudWatch Log Amazon

- logs:destination
- logs:log-group

## AWS CodeArtifact

- codeartifact:domain
- codeartifact:repository

## AWS CodeBuild

- codebuild:project

## AWS CodeCommit

- codecommit:repository

## Amazon CodeGuru Profiler

- codeguru-profiler:profilingGroup

## AWS CodePipeline

- codepipeline:pipeline

## AWS CodeConnections

- codestarconnections:connect

## Amazon Cognito

- cognito:identitypool
- cognito:userpool

## Amazon Connect

- appintegrations:eventintegration

## Kebijaksanaan Amazon Connect

- wisdom:assistant
- wisdom:association
- wisdom:knowledge-base

## Amazon Detective

- detective:graph

## Amazon DynamoDB

- dynamodb:table

## EC2 Image Builder

- imagebuilder:component
- imagebuilder:containerrecipe
- imagebuilder:distributionconfiguration
- imagebuilder:image

- imagebuilder:imagepipeline
- imagebuilder:imagerecipe
- imagebuilder:infrastructureconfiguration

## Amazon ECR Public

- ecrpublic:repository

## AWS Elastic Beanstalk

- elasticbeanstalk:application
- elasticbeanstalk:applicationversion
- elasticbeanstalk:configurationtemplate
- elasticbeanstalk:environment

## Amazon ElastiCache

- elasticache:cluster
- elasticache:globalreplicationgroup
- elasticache:parametergroup
- elasticache:replicationgroup
- elasticache:reserved-instance
- elasticache:snapshot
- elasticache:subnetgroup
- elasticache:user
- elasticache:usergroup

## Amazon Elastic Compute Cloud (Amazon EC2)

- ec2:capacity-reservation
- ec2:capacity-reservation-fleet
- ec2:client-vpn-endpoint

- ec2:customer-gateway
- ec2:dedicated-host
- ec2:dhcp-options
- ec2:egress-only-internet-gateway
- ec2:elastic-gpu
- ec2:elastic-ip
- ec2:fleet
- ec2:fpga-image
- ec2:host-reservation
- ec2:image
- ec2:instance
- ec2:instance-event-window
- ec2:internet-gateway
- ec2:ipam
- ec2:ipam-pool
- ec2:ipam-scope
- ec2:ipv4pool-ec2
- ec2:key-pair
- ec2:launch-template
- ec2:natgateway
- ec2:network-acl
- ec2:network-insights-access-scope
- ec2:network-insights-access-scope-analysis
- ec2:network-insights-analysis
- ec2:network-insights-path
- ec2:network-interface
- ec2:placement-group
- ec2:prefix-list
- ec2:reserved-instances

- ec2:route-table
- ec2:security-group
- ec2:security-group-rule
- ec2:snapshot
- ec2:spot-fleet-request
- ec2:spot-instances-request
- ec2:subnet
- ec2:subnet-cidr-reservation
- ec2:traffic-mirror-filter
- ec2:traffic-mirror-filter-rule
- ec2:traffic-mirror-session
- ec2:traffic-mirror-target
- ec2:transit-gateway
- ec2:transit-gateway-attachment
- ec2:transit-gateway-connect-peer
- ec2:transit-gateway-multicast-domain
- ec2:transit-gateway-policy-table
- ec2:transit-gateway-route-table
- ec2:transitgatewayroutetableannouncement
- ec2:volume
- ec2:vpc
- ec2:vpc-endpoint
- ec2:vpc-flow-log
- ec2:vpc-peering-connection
- ec2:vpn-connection
- ec2:vpn-gateway

## Amazon Elastic Container Registry

- ecr:repository

## Amazon Elastic Container Service

- ecs:cluster
- ecs:container-instance
- ecs:service
- ecs:task
- ecs:task-definition
- ecs:task-set

## Amazon Elastic File System

- efs:filesystem
- efs:accesspoint

## Penyeimbang Beban Elastis

- elasticloadbalancing:listener
- elasticloadbalancing:listener-rule
- elasticloadbalancing:listener-rule/app
- elasticloadbalancing:listener/app
- elasticloadbalancing:listener/net
- elasticloadbalancing:loadbalancer
- elasticloadbalancing:loadbalancer/app
- elasticloadbalancing:loadbalancer/net
- elasticloadbalancing:targetgroup

## AWS Elemental MediaPackage

- mediapackage:channel
- mediapackage:originendpoint
- mediapackage-vod:packaging-configurations
- mediapackage-vod:packaging-groups

## AWS Elemental MediaTailor

- mediatailor:playbackConfiguration

## Amazon EMR Tanpa Server

- emr-serverless:applications

## Amazon EventBridge

- events:event-bus
- events:rule

## AWS Fault Injection Service

- fis:experimenttemplate

## Amazon Forecast

- forcast:dataset
- forcast:dataset-group

## Amazon Fraud Detector

- frauddetector:detector
- frauddetector:entity-type
- frauddetector:event-type
- frauddetector:label
- frauddetector:outcome
- frauddetector:variable

## Amazon GameLift

- gamelift:alias

## AWS Global Accelerator

- globalaccelerator:accelerator
- globalaccelerator:accelerator/listener
- globalaccelerator:accelerator/listener/endpoint-group

## AWS Glue

- glue:database
- glue:job
- glue:table
- glue:trigger

## AWS Glue DataBrew

- databrew:dataset
- databrew:recipe
- databrew:ruleset

## AWS Identity and Access Management

- iam:group
- iam:instance-profile
- iam:oidc-provider
- iam:policy
- iam:role
- iam:saml-provider
- iam:server-certificate

- iam:user
- iam:virtualmfadevice

## Amazon Interactive Video Service

- ivs:channel
- ivs:streamkey

## AWS IoT

- iot:authorizer
- iot:jobtemplate
- iot:mitigationaction
- iot:policy
- iot:provisioningtemplate
- iot:rolealias
- iot:securityprofile
- iot:thing
- iot:topicrule

## AWS IoT Analytics

- iotanalytics:channel
- iotanalytics:dataset
- iotanalytics:datastore
- iotanalytics:pipeline

## AWS IoT Events

- iotevents:alarmModel
- iotevents:detectorModel
- iotevents:input

## AWS IoT Greengrass Version 1

- greengrass:components
- greengrass:groups

## AWS IoT SiteWise

- iotsitewise:asset
- iotsitewise:assetmodel
- iotsitewise:gateway

## AWS IoT TwinMaker

- iottwinmaker:workspace
- iottwinmaker:workspace/component-type
- iottwinmaker:workspace/entity

## AWS Key Management Service

- kms:key

## Amazon Kinesis

- kinesis:stream

## Amazon Data Firehose

- kinesisfirehose:deliverystream

## Amazon Kinesis Video Streams

- kinesisvideo:stream

## AWS Lambda

- `lambda:code-signing-config`
- `lambda:event-source-mapping`
- `lambda:function`

## Amazon Lex

- `lex:bot`

## Amazon Location Service

- `geo:place-index`
- `geo:tracker`

## Amazon Lookout for Metrics

- `lookoutmetrics:Alert`

## Amazon Lookout for Vision

- `lookoutvision:project`

## Layanan Terkelola Amazon untuk Apache Flink

- `kinesisanalytics:application`

## Layanan Terkelola Amazon untuk Prometheus

- `aps:rulegroupsnamespace`
- `aps:workspace`

## Layanan Terkelola Amazon untuk Prometheus

- memorydb:cluster
- memorydb:parametergroup
- memorydb:user

## Amazon Managed Streaming untuk Apache Kafka

- kafka:cluster
- kafka:configuration

## AWS Migration Hub Refactor Spaces

- refactor-spaces:environment
- refactor-spaces:environment/application
- refactor-spaces:environment/application/route
- refactor-spaces:environment/application/service

## AWS Network Firewall

- network-firewall:firewall-policy

## AWS Network Manager

- networkmanager:core-network
- networkmanager:device
- networkmanager:global-network
- networkmanager:link

## OpenSearch Layanan Amazon

- es:domain

## AWS Panorama

- panorama:package

## Amazon Personalize

- personalize:dataset
- personalize:dataset-group
- personalize:schema

## AWS Private Certificate Authority

- acmpca:certificateauthority

## Amazon QLDB

- qldb:ledger
- qldb:stream

## Amazon Redshift

- redshift:cluster
- redshift:eventsubscription
- redshift:parametergroup
- redshift:snapshot
- redshift:snapshotcopygrant
- redshift:snapshotschedule
- redshift:subnetgroup
- redshift:usagelimit

## Amazon Rekognition

- rekognition:project

## Amazon Relational Database Service (Amazon RDS)

- rds:auto-backup
- rds:cev
- rds:cluster
- rds:cluster-endpoint
- rds:cluster-pg
- rds:cluster-snapshot
- rds:db
- rds:db-proxy
- rds:db-proxy-endpoint
- rds:deployment
- rds:es
- rds:global-cluster
- rds:og
- rds:pg
- rds:ri
- rds:secgrp
- rds:snapshot
- rds:subgrp

## AWS Resilience Hub

- resiliencehub:resiliencypolicy

## AWS Resource Groups

- resourcegroups:group

## Penjelajah Sumber Daya AWS

- resource-explorer-2:index

- resource-explorer-2:view

## Amazon Route 53

- route53:healthcheck
- route53:hostedzone

## Kesiapan Pemulihan Amazon Route 53

- route53-recover-readiness:recovery-group
- route53-recover-readiness:resource-set

## Amazon Route 53 Resolver

- route53resolver:firewalldomainlist
- route53resolver:firewallrulegroup
- route53resolver:resolverendpoint
- route53resolver:resolverrule

## Amazon SageMaker

- sagemaker:model
- sagemaker:notebookinstance

## AWS Secrets Manager

- secretsmanager:secret

## AWS Service Catalog

- servicecatalog:applications
- servicecatalog:attribute-groups

## Amazon Simple Notification Service

- sns:topic

## Amazon Simple Queue Service

- sqs:queue

## Amazon Simple Storage Service (Amazon S3)

- s3:accesspoint
- s3:bucket
- s3:storage-lens

## AWS Step Functions

- states:statemachine
- stepfunctions:activity

## AWS Systems Manager

- ssm:association
- ssm:automation-execution
- ssm:document
- ssm:maintenancewindow
- ssm:managed-instance
- ssm:parameter
- ssm:patchbaseline
- ssm:resourcedatasync
- ssm:windowtarget
- ssm:windowtask

### Akses Terverifikasi AWS

- `ec2:verifiedaccessendpoint`
- `ec2:verifiedaccessgroup`
- `ec2:verifiedaccessinstance`
- `ec2:verifiedaccesstrustprovider`

### AWS Wavelength

- `ec2:carriergateway`

## Mengakses daftar jenis sumber daya yang didukung secara terprogram

Untuk mengakses daftar jenis sumber daya yang didukung dari kode, Anda dapat menjalankan ListSupportedResourceTypesoperasi dari AWS SDK apa pun.

Misalnya, Anda dapat menjalankan perintah list-supported-resource-types AWS Command Line Interface (AWS CLI), seperti yang ditunjukkan pada contoh berikut.

```
$ aws resource-explorer-2 list-supported-resource-types
{
    "ResourceTypes": [
        {
            "ResourceType": "acm-pca:certificate-authority",
            "Service": "acm-pca"
        },
        {
            "ResourceType": "airflow:environment",
            "Service": "airflow"
        },
        {
            "ResourceType": "amplify:branches",
            "Service": "amplify"
        },
... truncated for brevity ...
```

# Jenis sumber daya yang muncul sebagai tipe lain

Beberapa jenis sumber daya diidentifikasi oleh string nama sumber daya Amazon (ARN) yang berbagi format umum dengan jenis sumber daya lain. Ketika ini terjadi, Resource Explorer dapat melaporkan sumber daya seperti jenis sumber daya lainnya. Ini mempengaruhi jenis sumber daya dalam tabel berikut.

| Jenis sumber daya aktual | Dilaporkan sebagai tipe sumber daya |
|---|---|
| `ec2:securitygroupegress`<br>`ec2:securitygroupingress` | `ec2:security-group-rule` |
| `elasticloadbalancingv2:loadbalancer` | `elasticloadbalancing:loadbalancer` |
| `docdb:dbcluster`<br>`neptune:dbcluster`<br>`rds:dbcluster` | `rds:cluster` |
| `docdb:dbclusterparametergroup`<br>`neptune:dbclusterparametergroup`<br>`rds:dbclusterparametergroup` | `rds:cluster-pg` |
| `docdb:clustersnapshot`<br>`neptune:dbclustersnapshot`<br>`rds:clustersnapshot` | `rds:cluster-snapshot` |
| `docdb:dbinstance`<br>`neptune:dbinstance`<br>`rds:dbinstance` | `rds:db` |
| `docdb:eventsubscription` | `rds:es` |

| Jenis sumber daya aktual | Dilaporkan sebagai tipe sumber daya |
| --- | --- |
| neptune:eventsubscription<br><br>rds:eventsubscription | |
| docdb:globalcluster<br><br>rds:globalcluster | rds:global-cluster |
| neptune:dbparametergroup<br><br>rds:dbparametergroup | rds:pg |
| docdb:dbsubnetgroup<br><br>neptune:dbsubnetgroup<br><br>rds:dbsubnetgroup | rds:subgrp |

# Kuota untuk Resource Explorer

AndaAkun AWS memiliki kuota default untuk masing-masingLayanan AWS. Kecuali dinyatakan lain, kuota bersifat khusus per Wilayah. Anda dapat meminta peningkatan untuk beberapa kuota dan kuota lainnya tidak dapat ditingkatkan.

Untuk melihat kuotaPenjelajah Sumber Daya AWS, buka konsol Service Quotas. Di panel navigasi, pilih Layanan AWSdan pilih Resource Explorer.

Untuk meminta penambahan kuota, lihat Meminta penambahan kuota di Panduan Pengguna Service Quotas. Jika kuota belum tersedia dalam Service Quotas, gunakan Formulir kenaikan batas.

Kuota berikut adalah default untuk Resource Explorer.

| Nilai kuota maksimum | Nilai default |
|---|---|
| Jumlah tampilan dalamWilayah AWS | 10 |

| Batas tarif untuk operasi | Nilai default |
|---|---|
| Operasi Pencarian Maksimum per detik | 5 |
| Operasi non-pencarian maksimum per detik | 3 |
| Operasi Pencarian Maksimum di Wilayah agregator per bulan | 10.000 |
| Operasi Pencarian Maksimum di Wilayah lokal per bulan | 500 |

# Menggunakan Penjelajah Sumber Daya AWS dengan AWS SDK

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

| Dokumentasi SDK | Contoh kode |
| --- | --- |
| AWS SDK for C++ | AWS SDK for C++ contoh kode |
| AWS CLI | AWS CLI contoh kode |
| AWS SDK for Go | AWS SDK for Go contoh kode |
| AWS SDK for Java | AWS SDK for Java contoh kode |
| AWS SDK for JavaScript | AWS SDK for JavaScript contoh kode |
| AWS SDK for Kotlin | AWS SDK for Kotlin contoh kode |
| AWS SDK for .NET | AWS SDK for .NET contoh kode |
| AWS SDK for PHP | AWS SDK for PHP contoh kode |
| AWS Tools for PowerShell | Alat untuk contoh PowerShell kode |
| AWS SDK for Python (Boto3) | AWS SDK for Python (Boto3) contoh kode |
| AWS SDK for Ruby | AWS SDK for Ruby contoh kode |
| AWS SDK for Rust | AWS SDK for Rust contoh kode |
| AWS SDK untuk SAP ABAP | AWS SDK untuk SAP ABAP contoh kode |
| AWS SDK for Swift | AWS SDK for Swift contoh kode |

Ketersediaan contoh

Tidak dapat menemukan apa yang Anda butuhkan? Minta contoh kode menggunakan tautan Berikan umpan balik di bagian bawah halaman ini.

# Riwayat dokumen untuk Panduan Pengguna Resource Explorer

Tabel berikut menjelaskan rilis dokumentasi untuk Penjelajah Sumber Daya AWS. Untuk notifikasi tentang pembaruan dokumentasi ini, Anda dapat berlangganan ke umpan RSS.

| Perubahan | Deskripsi | Tanggal |
| --- | --- | --- |
| Menambahkan dukungan untuk jenis sumber daya baru | Resource Explorer menambahkan dukungan untuk 65 sumber daya baru dari Layanan AWS termasuk AWS Key Management Service, Amazon Route 53, dan Amazon Fraud Detector. | Februari 20, 2024 |
| Kebijakan terkelola yang diperbarui | Resource Explorer menambahkan dukungan untuk melihat jenis sumber daya tambahan. Kebijakan `AWSResourceExplorerServiceRolePolicy` AWS terkelola telah diperbarui untuk memberikan akses Resource Explorer untuk melihat jenis sumber daya tambahan. | Desember 12, 2023 |
| Filter pencarian baru ditambahkan | Resource Explorer sekarang mendukung pencarian sumber daya Anda berdasarkan aplikasi. | 16 November 2023 |
| Menambahkan dukungan untuk jenis sumber daya baru | Resource Explorer menambahkan dukungan untuk 86 sumber daya | 15 November 2023 |

| | | |
|---|---|---|
| | baru dari Layanan AWS termasuk AWS CloudForm ation AWS Glue,, dan Amazon SageMaker. | |
| Resource Explorer mendukung pencarian multi-akun | Sekarang Anda dapat menggunakan Resource Explorer untuk mencari dan menemukan sumber daya di Akun AWS dalam organisas i atau unit organisasi Anda. Untuk informasi selengkapnya, lihat Mengaktifkan penelusur an multi-akun. | 14 November 2023 |
| Kebijakan terkelola baru dan diperbarui | Resource Explorer menambahkan dukungan untuk AWS Organizations. Kebijakan AWS terkelola telah ditambahkan dan diperbarui untuk memberikan Resource Explorer akses ke organisasi, struktur organisasi, akun, dan administrator yang didelegas ikan. | 14 November 2023 |
| Menambahkan dukungan untuk jenis sumber daya baru | Resource Explorer menambahkan dukungan untuk AWS Organizations. Kebijakan AWS terkelola telah diperbarui untuk memberikan Resource Explorer akses ke organisasi, struktur organisas i, akun, dan administrator yang didelegasikan. | 14 November 2023 |

| | | |
|---|---|---|
| Menambahkan dukungan untuk jenis sumber daya baru | Resource Explorer sekarang mendukung 12 jenis sumber daya baru dari layanan termasuk Amazon Cognito, AWS Elastic Beanstalk, dan Amazon Elastic File System. | 18 Oktober 2023 |
| Menambahkan dukungan untuk jenis sumber daya baru | Resource Explorer menambahkan dukungan untuk 164 sumber daya. Kebijakan AWS terkelola yang memberikan akses Resource Explorer ke sumber daya indeks diperbarui untuk menyertakan jenis sumber daya baru tersebut. | 17 Oktober 2023 |
| Resource Explorer sekarang tersedia di Wilayah keikutsertaan tertentu | Pelanggan di BAH dan CGK sekarang dapat ikut serta dalam Resource Explorer. | 5 Oktober 2023 |
| Menambahkan dukungan untuk jenis sumber daya baru | Resource Explorer menambahkan dukungan untuk sumber daya dari berikut Layanan AWS: AWS CodeBuild, AWS CodePipeline, Amazon Cognito, Amazon Elastic Container Registry, AWS Elastic Beanstalk, Amazon Elastic File System AWS IoT, dan. AWS Step FunctionsKebijakan AWS terkelola yang memberikan akses Resource Explorer ke sumber daya indeks diperbarui untuk menyertakan jenis sumber daya baru tersebut. | 1 Agustus 2023 |

| | | |
|---|---|---|
| Resource Explorer sekarang mendukung ekspor hasil pencarian ke CSV | Anda sekarang dapat mengekspor hasil pencarian Anda di halaman pencarian Sumber Daya ke file berformat CSV. | 4 April 2023 |
| Gunakan AWS Chatbot untuk mencari dan menemukan AWS sumber daya Anda | Anda sekarang dapat menggunakan AWS Chatbot untuk mencari sumber daya Anda menggunakan pertanyaan bahasa alami. Untuk informasi selengkapnya, lihat Menggunakan AWS Chatbot untuk mencari sumber daya. | 30 Maret 2023 |
| Menambahkan dukungan untuk jenis sumber daya baru | Resource Explorer menambahkan dukungan untuk sumber daya dari berikut ini Layanan AWS: Amazon ElastiCache, AWS Lambda, dan Amazon Simple Queue Service (Amazon SQS). Kebijakan AWS terkelola yang memberikan akses Resource Explorer ke sumber daya indeks diperbarui untuk menyertakan jenis sumber daya baru tersebut. | 7 Maret 2023 |
| Pembaruan praktik terbaik IAM | Panduan yang diperbarui untuk menyelaraskan dengan praktik terbaik IAM. Untuk informasi selengkapnya, lihat Praktik terbaik keamanan di IAM. | 6 Desember 2022 |

| | | |
|---|---|---|
| Kebijakan AWS terkelola baru | Resource Explorer menambahkan AWSResourceExplorerFullAccess AWSResourceExplorerReadOnlyAccess,, dan AWSResourceExplorerServiceRolePolicy mengelola kebijakan. | 7 November 2022 |
| Rilis awal | Rilis awal Panduan Pengguna Resource Explorer | 7 November 2022 |

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.