



Panduan Pengguna

Penjelajah Sumber Daya AWS



Penjelajah Sumber Daya AWS: Panduan Pengguna

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

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

Table of Contents

Penjelajah Sumber Daya	1
Pengguna pertama kali	2
Fitur Resource Explorer	2
Wilayah yang Didukung	3
Layanan terkait	6
Harga	7
Memulai	8
Mengakses Resource Explorer	8
Istilah dan konsep	9
Administrator Resource Explorer	12
Pengguna Resource Explorer	13
Indeks	14
Lihat	15
Sumber daya	17
Pencarian terpadu di Konsol Manajemen AWS	17
Pencarian multi-akun	18
Prasyarat	18
Mendaftar untuk Akun AWS	19
Buat pengguna dengan akses administratif	19
Menyiapkan Resource Explorer	20
Pengaturan cepat	21
Pengaturan lanjutan	23
Identifikasi status Resource Explorer di Wilayah AWS	28
Memeriksa status Resource Explorer di Region	28
Menghidupkan Wilayah	30
Membuat indeks Resource Explorer di Wilayah	31
Tentang Wilayah keikutsertaan	34
Perilaku memilih keluar	34
Mengaktifkan pencarian lintas wilayah	35
Tentang indeks agregator	35
Membuat indeks agregator	37
Menurunkan indeks agregator	39
Mengaktifkan pencarian multi-akun	41
Prasyarat	41

Aktifkan pencarian multi-akun	41
Pengaturan Cepat Multi-Akun	42
Pengaruh tindakan akun pada pencarian multi-akun	43
Resource Explorer dinonaktifkan	43
Akun anggota dihapus dari organisasi	43
Akun ditangguhkan	43
Akun ditutup	44
Penyisihan akun	44
Mendukung pencarian terpadu konsol	45
Menyebarkan ke organisasi	46
Prasyarat	46
Membuat set tumpukan untuk Resource Explorer	47
Contoh CloudFormation template	48
Mematikan Resource Explorer	52
Mematikan Resource Explorer dalam satu AWS Region	52
Mematikan semua Wilayah AWS	54
Mengelola tampilan	57
Tampilan default	59
Membuat tampilan	60
Memberikan akses ke tampilan	64
Menggunakan otorisasi berbasis tanda untuk mengontrol akses ke tampilan Anda	66
Mengatur tampilan default	68
Tampilan penandaan	69
Menambahkan tag ke tampilan Anda	69
Mengontrol izin dengan tag	70
Referensi tag dalam kebijakan ABAC	71
Berbagi tampilan	72
Kebijakan izin untuk berbagi tampilan dengan Akun AWS	73
Menghapus tampilan	74
Mencari sumber daya	76
Ekspor hasil pencarian ke file.csv	79
Jenis sumber daya yang mendukung	81
Layanan dan jenis sumber daya yang didukung	82
APIGerbang Amazon	85
AWS App Runner	85
Amazon AppStream 2.0	85

AWS AppSync	85
Amazon Athena	85
AWS Backup	85
AWS Batch	86
CloudFormation	86
Amazon CloudFront	86
AWS CloudTrail	86
Amazon CloudWatch	86
Amazon CloudWatch Terbukti	87
CloudWatch Log Amazon	87
AWS CodeArtifact	87
AWS CodeBuild	87
AWS CodeCommit	87
Amazon CodeGuru Profiler	87
AWS CodePipeline	88
AWS CodeConnections	88
Amazon Cognito	88
Amazon Connect	88
Kebijakan Amazon Connect	88
Amazon Detective	88
Amazon DynamoDB	88
EC2Image Builder	89
Amazon ECR Publik	89
AWS Elastic Beanstalk	89
Amazon ElastiCache	89
Amazon Elastic Compute Cloud (AmazonEC2)	90
Amazon Elastic Container Registry	92
Amazon Elastic Container Service	92
Amazon Elastic File System	92
Penyeimbang Beban Elastis	92
AWS Elemental MediaPackage	92
AWS Elemental MediaTailor	93
Amazon Tanpa EMR Server	93
Amazon EventBridge	93
AWS Fault Injection Service	93
Amazon Forecast	93

Amazon Fraud Detector	93
Amazon GameLift	94
AWS Global Accelerator	94
AWS Glue	94
AWS Glue DataBrew	94
AWS Identity and Access Management	94
Amazon Interactive Video Service	95
AWS IoT	95
AWS IoT Analytics	95
AWS IoT Events	95
AWS IoT Greengrass Version 1	96
AWS IoT SiteWise	96
AWS IoT TwinMaker	96
AWS Key Management Service	96
Amazon Kinesis	96
Amazon Data Firehose	96
Amazon Kinesis Video Streams	97
AWS Lambda	97
Amazon Lex	97
Amazon Location Service	97
Amazon Lookout for Metrics	97
Amazon Lookout for Vision	97
Amazon Managed Service for Apache Flink	97
Layanan Terkelola Amazon untuk Prometheus	98
Layanan Terkelola Amazon untuk Prometheus	98
Amazon Managed Streaming untuk Apache Kafka	98
AWS Migration Hub Refactor Spaces	98
AWS Network Firewall	98
AWS Network Manager	98
OpenSearch Layanan Amazon	99
AWS Panorama	99
Amazon Personalize	99
AWS Private Certificate Authority	99
Amazon QLDB	99
Amazon Redshift	99
Amazon Rekognition	100

Amazon Relational Database Service (AmazonRDS)	100
AWS Resilience Hub	100
AWS Resource Groups	100
Penjelajah Sumber Daya AWS	101
Amazon Route 53	101
Kesiapan Pemulihan Amazon Route 53	101
Amazon Route 53 Resolver	101
Amazon SageMaker	101
AWS Secrets Manager	101
AWS Service Catalog	102
Amazon Simple Notification Service	102
Amazon Simple Queue Service	102
Amazon Simple Storage Service (Amazon S3)	102
AWS Step Functions	102
AWS Systems Manager	102
Akses Terverifikasi AWS	103
AWS Wavelength	103
Mengakses daftar jenis sumber daya yang didukung secara terprogram	103
Jenis sumber daya yang muncul sebagai tipe lain	104
Sintaks kueri penelusuran	106
Cara kerja kueri di Resource Explorer	106
Sintaks string kueri	106
Hal-hal mendasar	107
Filter	107
Operator filter	111
Contoh kueri	117
Sumber daya yang tidak ditandai	117
Sumber daya yang diberi tag	118
Tanda tidak ditemukan	118
Tag tidak valid	118
Subset Daerah	119
Sumber daya global	119
Filter beberapa	119
Menggunakan tanda kutip untuk istilah multi-kata	120
CloudFormation anggota stack	120
Pencarian terpadu	121


Memeriksa apakah pencarian terpadu diaktifkan	122
Mengaktifkan pencarian terpadu	122
Bekerja dengan CloudFormation	123
Resource Explorer dan CloudFormation template	123
Pelajari selengkapnya tentang CloudFormation	126
Menggunakan Amazon Q Developer dalam aplikasi obrolan	127
AWS pertanyaan sumber daya	127
Prasyarat	127
Pertanyaan sumber daya yang umum diajukan	128
Keamanan	129
Tingkatkan IAM kebijakan ke IPv6	130
Pelanggan terpengaruh oleh peningkatan dari ke IPv4 IPv6	130
Apa yang dimaksud dengan IPv6?	130
Memperbarui IAM kebijakan untuk IPv6	131
Verifikasi klien Anda dapat mendukung IPv6	132
Pengelolaan identitas dan akses	134
Audiens	134
Mengautentikasi dengan identitas	135
Mengelola akses menggunakan kebijakan	138
Penjelajah Sumber Daya dan IAM	141
Contoh kebijakan berbasis identitas	148
Contoh SCP	153
AWS kebijakan terkelola	155
Menggunakan peran terkait layanan	172
Izin pemecahan masalah	174
Perlindungan data	176
Enkripsi diam	177
Enkripsi bergerak	177
Validasi Kepatuhan	177
Ketahanan	178
Keamanan infrastruktur	179
Memantau	180
CloudTrail log	180
Informasi Resource Explorer di CloudTrail	180
Memahami entri berkas log Resource	182
Pemecahan Masalah	192

Masalah umum	192
Tautan ke Resource Explorer hilangAWS Region	192
CloudTrail Kesalahan pencarian terpadu	193
Penyiapan	194
Saya mendapatkan pesan "akses ditolak" ketika saya mengajukan permintaan ke Resource Explorer	195
Saya mendapatkan pesan "akses ditolak" ketika saya membuat permintaan dengan kredensial keamanan sementara	195
Masalah pencarian	196
Mengapa beberapa sumber daya hilang dari hasil pencarian Resource Explorer saya?	196
Mengapa sumber daya saya tidak muncul di hasil penelusuran terpadu di konsol?	199
Mengapa pencarian terpadu di konsol dan Resource Explorer terkadang memberikan hasil yang berbeda?	199
Izin apa yang saya perlukan untuk dapat mencari sumber daya?	199
Quotas	201
Bekerja dengan AWS SDKs	202
Riwayat dokumen	204
.....	ccx

Apa itu Penjelajah Sumber Daya AWS?

Penjelajah Sumber Daya AWS adalah 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 IDs 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 Akun 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?](#)
- [Fitur Resource Explorer](#)
- [Wilayah yang didukung Resource Explorer](#)
- [Terkait Layanan AWS](#)
- [Harga](#)

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 AWS Region atau di seluruh Wilayah di wilayah mereka Akun 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 lainnya Layanan 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.

Wilayah yang didukung Resource Explorer

Nama Wilayah	Wilayah	Titik Akhir	Protokol
AS Timur (Ohio)	us-east-2	resource-explorer-2.us-east-2.amazonaws.com	HTTPS
		resource-explorer-2-fips.us-east-2.amazonaws.com	HTTPS
		resource-explorer-2-fips.us-east-2.api.aws	HTTPS
AS Timur (Virginia Utara)	us-east-1	resource-explorer-2.us-east-1.amazonaws.com	HTTPS
		resource-explorer-2-fips.us-east-1.amazonaws.com	HTTPS
		resource-explorer-2-fips.us-east-1.api.aws	HTTPS
US West (N. California)	us-west-1	resource-explorer-2.us-west-1.amazonaws.com	HTTPS
		resource-explorer-2-fips.us-west-1.amazonaws.com	HTTPS
		resource-explorer-2-fips.us-west-1.api.aws	HTTPS
AS Barat (Oregon)	us-west-2	resource-explorer-2.us-west-2.amazonaws.com	HTTPS
		resource-explorer-2-fips.us-west-2.amazonaws.com	HTTPS
		resource-explorer-2-fips.us-west-2.api.aws	HTTPS
Afrika (Cape Town)	af-south-1	resource-explorer-2.af-south-1.amazonaws.com	HTTPS
Asia Pasifik	ap-east-1	resource-explorer-2.ap-east-1.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
(Hong Kong)			
Asia Pasifik (Hyderabad)	ap-south-2	resource-explorer-2.ap-south-2.amazonaws.com	HTTPS
Asia Pasifik (Jakarta)	ap-southeast-3	resource-explorer-2.ap-southeast-3.amazonaws.com	HTTPS
Asia Pasifik (Melbourne)	ap-southeast-4	resource-explorer-2.ap-southeast-4.amazonaws.com	HTTPS
Asia Pasifik (Mumbai)	ap-south-1	resource-explorer-2.ap-south-1.amazonaws.com	HTTPS
Asia Pasifik (Osaka)	ap-northeast-3	resource-explorer-2.ap-northeast-3.amazonaws.com	HTTPS
Asia Pasifik (Seoul)	ap-northeast-2	resource-explorer-2.ap-northeast-2.amazonaws.com	HTTPS
Asia Pasifik (Singapura)	ap-southeast-1	resource-explorer-2.ap-southeast-1.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Asia Pasifik (Sydney)	ap-southeast-2	resource-explorer-2.ap-southeast-2.amazonaws.com	HTTPS
Asia Pasifik (Tokyo)	ap-northeast-1	resource-explorer-2.ap-northeast-1.amazonaws.com	HTTPS
Kanada (Pusat)	ca-central-1	resource-explorer-2.ca-central-1.amazonaws.com	HTTPS
		resource-explorer-2-fips.ca-central-1.amazonaws.com	HTTPS
		resource-explorer-2-fips.ca-central-1.api.aws	HTTPS
Kanada Barat (Calgary)	ca-west-1	resource-explorer-2.ca-west-1.amazonaws.com	HTTPS
		resource-explorer-2-fips.ca-west-1.amazonaws.com	HTTPS
		resource-explorer-2-fips.ca-west-1.api.aws	HTTPS
Eropa (Frankfurt)	eu-central-1	resource-explorer-2.eu-central-1.amazonaws.com	HTTPS
Eropa (Irlandia)	eu-west-1	resource-explorer-2.eu-west-1.amazonaws.com	HTTPS
Eropa (London)	eu-west-2	resource-explorer-2.eu-west-2.amazonaws.com	HTTPS
Eropa (Milan)	eu-south-1	resource-explorer-2.eu-south-1.amazonaws.com	HTTPS

Nama Wilayah	Wilayah	Titik Akhir	Protokol
Eropa (Paris)	eu-west-3	resource-explorer-2.eu-west-3.amazonaws.com	HTTPS
Eropa (Spanyol)	eu-south-2	resource-explorer-2.eu-south-2.amazonaws.com	HTTPS
Eropa (Stockholm)	eu-north-1	resource-explorer-2.eu-north-1.amazonaws.com	HTTPS
Eropa (Zürich)	eu-central-2	resource-explorer-2.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	resource-explorer-2.il-central-1.amazonaws.com	HTTPS
Timur Tengah (Bahrain)	me-south-1	resource-explorer-2.me-south-1.amazonaws.com	HTTPS
Timur Tengah (UAE)	me-central-1	resource-explorer-2.me-central-1.amazonaws.com	HTTPS
Amerika Selatan (Sao Paulo)	sa-east-1	resource-explorer-2.sa-east-1.amazonaws.com	HTTPS

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 lain Akun AWS. Jika akun Anda dikelola oleh AWS 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](#).

Harga

Tidak ada biaya untuk mencari sumber daya dengan menggunakan Penjelajah Sumber Daya AWS, termasuk membuat tampilan, mengaktifkan Wilayah, atau mencari sumber daya. Dalam proses membangun inventaris sumber daya Anda, Resource Explorer memanggil APIs 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 nya Layanan 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 oleh Penjelajah Sumber Daya AWS. Pelajari tentang prasyarat yang harus Anda penuhi agar berhasil menggunakan Resource Explorer dan cara mengaktifkan Resource Explorer di Resource Explorer. Akun AWS

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 mendaftar Akun AWS, Anda dapat mengakses konsol Resource Explorer dengan masuk ke [Konsol Manajemen AWS](#) dan 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, maka Anda diminta untuk melakukannya sebelum konsol muncul.

Note

Konsol Resource Explorer adalah konsol global, artinya Anda tidak perlu memilih AWS Region 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.

Konsol Manajemen AWS pencarian terpadu

Di bagian atas setiap halaman Konsol Manajemen AWS, 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 AWS Region 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 API operasi 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 CLI Perintah atau Referensi AWS Tools for Windows PowerShell Cmdlet](#).

Operasi Resource Explorer di AWS SDKs

AWS menyediakan API perintah untuk serangkaian bahasa pemrograman yang luas. Untuk informasi lebih lanjut tentang memulai, lihat [Menggunakan Penjelajah Sumber Daya AWS dengan AWS SDK](#).

Permintaan API

Jika Anda tidak menggunakan salah satu bahasa pemrograman yang didukung, Resource Explorer HTTPS Query API memberi Anda akses terprogram ke Resource Explorer. Dengan Resource ExplorerAPI, Anda dapat mengeluarkan HTTPS permintaan langsung ke layanan. Saat Anda menggunakan Resource ExplorerAPI, Anda harus menyertakan kode yang dapat menandatangani permintaan secara digital menggunakan kredensi Anda AWS . Untuk informasi selengkapnya, lihat [Penjelajah Sumber Daya AWS APIReferensi](#).

Syarat dan konsep untuk Resource Explorer

Penjelajah Sumber Daya AWS adalah 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.

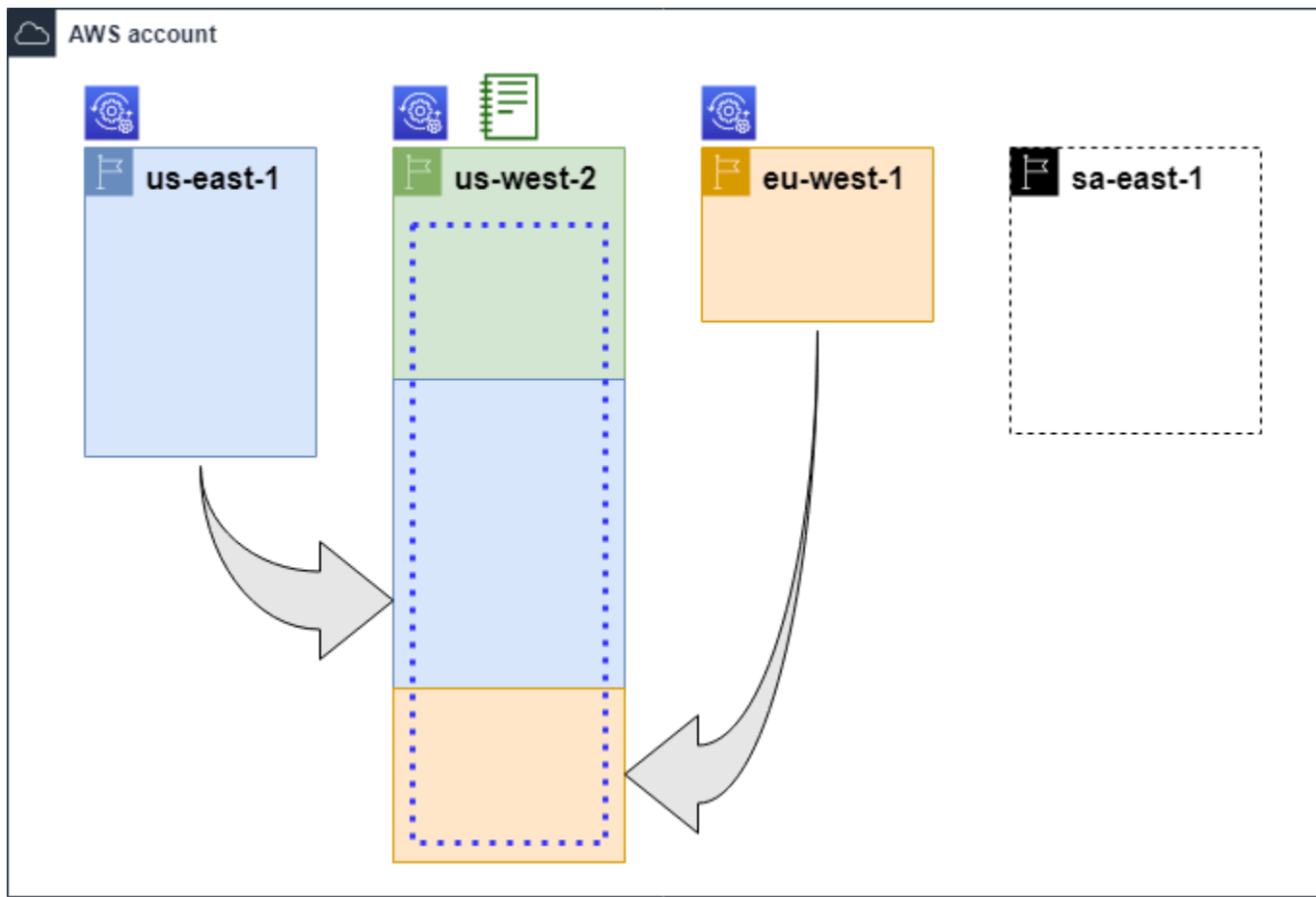
Konsep

- [Administrator Resource Explorer](#)
- [Pengguna Resource Explorer](#)
- [Indeks](#)
- [Lihat](#)
- [Sumber daya](#)
- [Pencarian terpadu di Konsol Manajemen AWS](#)
- [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 AWS Region 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 AWS Region 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 semua Wilayah 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 AWS Region 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, lihat [Menggunakan Penjelajah Sumber Daya AWS untuk mencari sumber daya](#).

Indeks

Indeks adalah kumpulan informasi yang dikelola oleh Resource Explorer tentang semua AWS sumber daya AWS Region di salah satu sumber daya Anda Akun 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 di Akun AWS. Pada diagram sebelumnya, kotak di bawah AWS Region nama mewakili indeks Resource Explorer yang dipertahankan di masing-masing AWS Region. 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 AWS Region 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 AWS Region 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 sebuah Akun AWS.

Saat Anda mengaktifkan Resource Explorer, Anda dapat menentukan AWS Region mana yang berisi indeks agregator. Anda juga dapat mengubah yang AWS Region digunakan untuk indeks agregator nanti. Untuk informasi tentang cara mempromosikan indeks lokal untuk menjadikannya indeks agregator Akun AWS, lihat [Mengaktifkan 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 dalamnya AWS Region. 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 AWS Region 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, lihat [Mengelola tampilan Resource Explorer untuk menyediakan akses ke pencarian](#). Untuk informasi tentang cara menggunakan tampilan dalam kueri, lihat [Menggunakan Penjelajah Sumber Daya AWS untuk 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. 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 Konsol Manajemen AWS

Di bagian atasKonsol Manajemen AWS, 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 AWS Region yang berisi

indeks agregator untuk akun. Ini memungkinkan Anda mencari sumber daya dari halaman mana pun di Konsol Manajemen AWS, 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, lihat [Menggunakan pencarian terpadu di Konsol Manajemen AWS](#).

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, lihat [Mengaktifkan 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/pendaftaran>.
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 AWS dibuat. 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 mengirimkan email konfirmasi setelah proses pendaftaran selesai. Kapan saja, Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan masuk <https://aws.amazon.com/ke/> 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 Anda Pengguna root akun AWS

1. Masuk ke [Konsol Manajemen AWS](#) sebagai 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. Aktifkan otentikasi multi-faktor (MFA) untuk pengguna root Anda.

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

Buat pengguna dengan akses administratif

1. Aktifkan Pusat IAM Identitas.

Untuk mendapatkan petunjuk, silakan lihat [Mengaktifkan AWS IAM Identity Center](#) di Panduan Pengguna AWS IAM Identity Center .

2. Di Pusat IAM Identitas, 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 IAM Identitas, gunakan login URL yang dikirim ke alamat email saat Anda membuat pengguna Pusat IAM Identitas.

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

Tetapkan akses ke pengguna tambahan

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

Untuk petunjuk, 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 IAM peran 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 [CreateIndex](#) operasi.

Note

Menyiapkan Resource Explorer juga dapat mengaktifkan kemampuan untuk mencari sumber daya dengan menggunakan bilah pencarian terpadu di Konsol Manajemen AWS. 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 AWS Region yang berisi indeks agregator. Untuk informasi selengkapnya, lihat [Menggunakan pencarian terpadu di Konsol Manajemen AWS](#).

Menyiapkan Resource Explorer menggunakan Pengaturan cepat

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

- Membuat indeks di setiap AWS Region 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 (*)

Konsol Manajemen AWS

Untuk mengatur Resource Explorer menggunakan Penyiapan cepat

1. Buka [Penjelajah Sumber Daya AWS konsol](https://console.aws.amazon.com/resource-explorer) di <https://console.aws.amazon.com/resource-explorer>.
2. Pilih Aktifkan Resource Explorer.
3. Pada halaman Aktifkan Resource Explorer, pilih Pengaturan cepat.
4. Pilih yang AWS Region 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 AWS Region 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 CLI operasi 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 AWS Region 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 Konsol Manajemen AWS. 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 (*)

Konsol Manajemen AWS

Untuk mengaktifkan Resource Explorer menggunakan Pengaturan lanjutan

1. Buka [Penjelajah Sumber Daya AWS konsol](https://console.aws.amazon.com/resource-explorer) di <https://console.aws.amazon.com/resource-explorer>.
2. Pilih Aktifkan Resource Explorer.
3. Pada halaman Aktifkan Resource Explorer, pilih Pengaturan lanjutan.
4. Di Wilayah AWS kotak, 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 Agregator, 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 AWS Region 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 AWS Region 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 API operasi 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 AWS Region di masing-masing tempat Anda ingin mengaktifkan Resource Explorer. Contoh perintah berikut mengaktifkan Resource Explorer di AWS Region 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 AWS Region untuk menjadi indeks agregator untuk akun

Jalankan perintah berikut AWS Region 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 AWS Region yang berisi indeks agregator

Jalankan perintah berikut AWS Region di mana Anda membuat indeks agregator. Contoh perintah berikut membuat tampilan identik dengan yang dibuat oleh proses setup 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 AWS Region

Contoh berikut menetapkan tampilan yang Anda buat pada langkah sebelumnya sebagai default untuk Wilayah. Anda harus menjalankan perintah berikut di tempat yang sama AWS Region 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 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 tersebut juga berisi tampilan yang memungkinkan IAM peran 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.

Identifikasi Resource Explorer mana Wilayah AWS yang diaktifkan

Anda dapat mengidentifikasi mana yang Wilayah AWS telah Penjelajah Sumber Daya AWS diaktifkan dengan memverifikasi apakah Wilayah berisi indeks untuk Resource Explorer. Untuk melihat Wilayah mana yang memiliki indeks, gunakan prosedur di halaman ini.

Important

Pengguna dapat mencari sumber daya hanya di Wilayah yang mengaktifkan Resource Explorer. 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 Region

Anda dapat memeriksa Wilayah mana yang memiliki indeks untuk Resource Explorer dengan menggunakan Konsol Manajemen AWS, dengan menggunakan perintah di AWS Command Line Interface (AWS CLI), atau dengan menggunakan API operasi dalam file AWS SDK.

Konsol Manajemen AWS

Untuk memeriksa Wilayah mana yang memiliki indeks untuk Resource Explorer

1. Buka halaman [Pengaturan](#) di konsol Resource Explorer.
2. Daftar di bagian Indeks hanya mencakup Wilayah yang berisi indeks Resource Explorer. Nilai di kolom Type menunjukkan apakah indeks adalah indeks Lokal untuk Region, atau indeks Agregator untuk Akun AWS
3. Untuk melihat Wilayah mana yang tidak berisi Resource Explorer, pilih Buat indeks. Jika Region tidak ada, maka Region tidak berisi Resource Explorer.

AWS CLI

Untuk memeriksa Wilayah mana yang memiliki indeks untuk Resource Explorer

Jalankan perintah berikut untuk melihat mana yang Wilayah AWS memiliki 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 Resource Explorer AWS Region untuk mengindeks sumber daya Anda

Ketika Anda awalnya menghidupkan Penjelajah Sumber Daya AWS Akun AWS, Anda membuat indeks untuk layanan dalam satu atau lebih Wilayah AWS. Jika Anda menggunakan opsi [Quick setup](#), Resource Explorer secara otomatis membuat indeks di semua [Wilayah AWS yang diaktifkan di Anda Akun 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.

Topik

- [Membuat indeks Resource Explorer di Wilayah](#)
- [Pertimbangan untuk Wilayah AWS keikutsertaan](#)

Saat Anda mengaktifkan Resource Explorer di sebuah AWS Region, layanan melakukan tindakan berikut:

- Saat Anda memulai Resource Explorer di Region pertama di sebuah Akun 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 seperti AWS CloudTrail dan layanan penandaan. Pembuatan peran terkait layanan hanya terjadi ketika Anda mendaftarkan yang pertama AWS Region di akun. Resource Explorer menggunakan peran terkait layanan yang sama untuk semua Wilayah tambahan yang Anda tambahkan nanti.
- Resource Explorer membuat indeks di Wilayah tertentu untuk menyimpan detail tentang sumber daya Wilayah tersebut.
- Resource Explorer mulai menemukan sumber daya di Wilayah tertentu dan menambahkan informasi yang ditemukannya tentang mereka ke indeks Wilayah tersebut.
- Jika akun Anda sudah berisi [indeks agregator](#) di Wilayah lain, Resource Explorer mulai mereplikasi informasi dari indeks Region 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 ditentukan di Wilayah yang sama atau Wilayah yang berisi indeks agregator.

Membuat indeks Resource Explorer di Wilayah

Anda dapat membuat indeks Resource Explorer dalam tambahan AWS Region menggunakan Konsol Manajemen AWS, dengan menggunakan perintah di AWS Command Line Interface (AWS CLI), atau dengan menggunakan API operasi dalam file AWS SDK. Anda hanya dapat membuat satu indeks di Wilayah.

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 (*)

Konsol Manajemen AWS

Untuk membuat indeks Resource Explorer di AWS Region

1. Pada halaman [Pengaturan](#) Resource Explorer.
2. Di bagian Indeks, pilih Buat indeks.
3. Pada halaman Buat indeks, pilih kotak centang Wilayah AWS di sebelah tempat 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 Tag bagian, Anda dapat menentukan kunci tag 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 membuat indeks di satu atau beberapa 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. 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 Wilayah baru secara otomatis mulai mereplikasi informasi indeksnya ke indeks agregator. Jika di situlah pengguna Anda melakukan semua pencarian mereka, maka sumber daya di Wilayah baru akan muncul di hasil penelusuran tersebut dan Anda selesai.

Namun, jika Anda ingin pengguna dapat mencari sumber daya hanya di Wilayah yang baru diindeks, Anda juga harus membuat tampilan untuk pengguna di Wilayah tersebut dan memberikan izin kepada pengguna Anda untuk tampilan tersebut. Untuk petunjuk tentang cara membuat tampilan, lihat [Mengelola tampilan Resource Explorer untuk menyediakan akses ke pencarian](#).

AWS CLI

Untuk membuat indeks Resource Explorer di AWS Region

Jalankan perintah berikut untuk masing-masing AWS Region di mana Anda ingin membuat indeks untuk mendukung pencarian sumber daya Wilayah tersebut. Contoh perintah berikut mendaftarkan Resource Explorer di Timur AS (Virginia N.) (us-east-1).

```
$ 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, menggantikan kode Wilayah yang sesuai untuk `--region` parameter.

Karena Resource Explorer melakukan beberapa pembuatan indeks sebagai tugas asinkron di latar belakang, responsnya bisa `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. 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 Wilayah baru secara otomatis mulai mereplikasi informasi indeksnya ke indeks agregator. Jika di situlah pengguna Anda melakukan semua pencarian mereka, maka sumber daya di Wilayah baru akan muncul di hasil penelusuran tersebut dan Anda selesai.

Namun, jika Anda ingin pengguna dapat mencari sumber daya hanya di Wilayah yang baru diindeks, Anda juga harus membuat tampilan untuk pengguna di Wilayah tersebut dan memberikan izin kepada pengguna Anda untuk tampilan tersebut. Untuk petunjuk tentang cara membuat tampilan, lihat [Mengelola tampilan Resource Explorer untuk menyediakan akses ke pencarian](#).

Pertimbangan untuk Wilayah AWS keikutsertaan

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

Anda dapat mengaktifkan Wilayah keikutsertaan menggunakan [Penjelajah Sumber Daya AWS konsol](#). Lihat [Mengaktifkan Resource Explorer di sebuah AWS Region 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 IAM akses ke sumber daya di Wilayah.
- Resource Explorer menonaktifkan indeks untuk Wilayah yang dipilih keluar dan berhenti menelan data. Itu 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

Dengan penelusuran lintas wilayah diaktifkan, Anda dapat mencari sumber daya di semua Wilayah di Anda Akun AWS.

Topik

- [Tentang indeks agregator](#)
- [Mempromosikan indeks lokal menjadi indeks agregator untuk akun](#)
- [Menurunkan indeks agregator ke indeks lokal](#)

Tentang indeks agregator

Penjelajah Sumber Daya AWS menyimpan informasi yang dikumpulkannya tentang sumber daya dalam indeks AWS Region lokal yang dibuat dan dikelola Resource Explorer di Wilayah tersebut. Misalnya, asumsikan bahwa Anda memiliki EC2 instans Amazon 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.

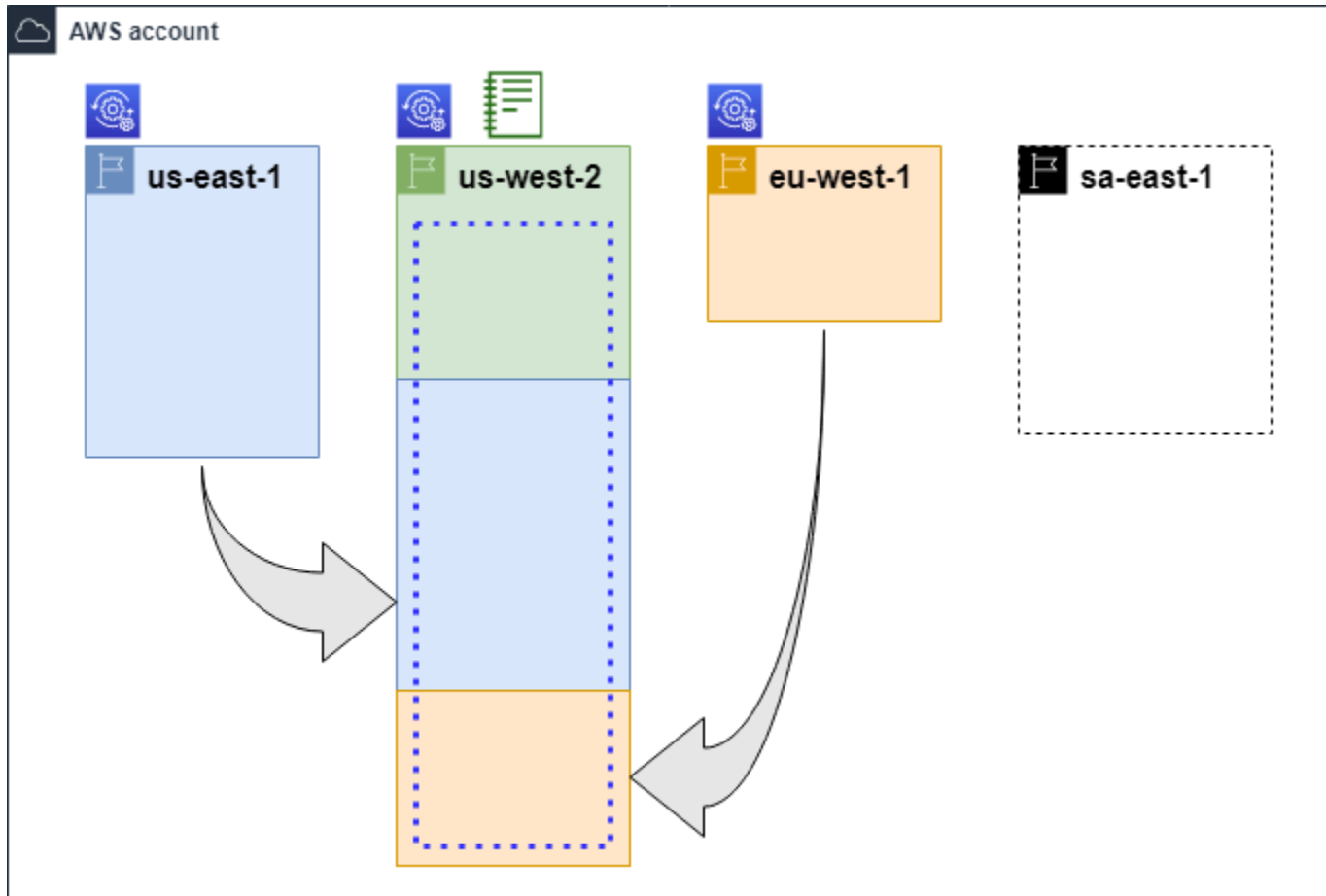
Indeks agregator berisi salinan indeks lokal yang direplikasi di setiap Wilayah lain tempat Anda mengaktifkan Resource Explorer. Ini memungkinkan Anda membuat tampilan di Wilayah yang berisi indeks agregator yang hasilnya dapat menyertakan sumber daya dari semua Wilayah AWS akun.

Diagram berikut menunjukkan contoh bagaimana indeks agregator bekerja. Dalam contoh ini Akun 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

	<p>Resource Explorer diaktifkan dalam hal ini AWS Region, dan sumber dayanya dikatalogkan ke dalam indeks di Wilayah itu. Indeks Wilayah ini juga direplikasi (ditunjukkan oleh panah) ke AWS Region yang berisi indeks agregator.</p>
	<p>Ini AWS Region berisi indeks agregator. Resource Explorer mereplikasi informasi sumber daya yang dikumpulkan di semua lainnya Wilayah AWS ke Wilayah ini.</p>



Tampilan default yang dibuat oleh Quick Setup mencakup semua sumber daya di semua Wilayah AWS.

Mempromosikan indeks lokal menjadi indeks agregator untuk akun

Anda memiliki pilihan untuk membuat indeks agregator dalam satu AWS Region ketika Anda pertama kali mengatur Penjelajah 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 agregator dalam sebuah Akun 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.

Konsol Manajemen AWS

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 ditentukan AWS Region dari jenis LOCAL ke jenis AGGREGATOR. Anda harus memanggil operasi dari AWS Region 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. AWS Region

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 [GetIndex](#) operasi. 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.

Konsol Manajemen AWS

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 AWS Region 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"  
}
```

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](#)
- [Pengaruh tindakan akun pada pencarian multi-akun Resource Explorer](#)

Prasyarat

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

- Untuk [Wilayah keikutsertaan](#), verifikasi akun manajemen Anda juga ikut serta di tempat Anda mengaktifkan penelusuran 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 [Quick Setup](#) untuk Resource Explorer di konsol Systems Manager.
2. Pilih Region indeks Agregator 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 (OUs).

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.

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 AWS Region 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 ditangguhkan AWS, 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](#).

Mendukung pencarian terpadu di Konsol Manajemen AWS

Ini Konsol Manajemen AWS memiliki bilah pencarian di bagian atas setiap halaman konsol. Ini memberikan pengalaman pencarian terpadu di semua Layanan AWS. Hasil pencarian terpadu dapat mencakup hal-hal seperti:

- Layanan AWS dan fitur halaman konsol.
- AWS halaman dokumentasi.
- AWS blog dan artikel Basis Pengetahuan
- Sumber daya di akun Anda — jika Anda mengikuti langkah-langkah di bawah ini.

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

- Anda harus [membuat indeks agregator](#) dalam satu AWS Region untuk. Akun AWS
- Anda harus [membuat tampilan default di AWS Region yang berisi indeks agregator](#).
- Anda harus memberikan semua prinsipal yang perlu mencari sumber daya di bilah pencarian terpadu [izin untuk mencari menggunakan](#) tampilan default itu.

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

Menerapkan Resource Explorer ke akun di organisasi

Dengan menggunakan AWS CloudFormation StackSets, Anda dapat menentukan dan menyebarkan ke semua akun yang dikelola dalam organisasi oleh AWS 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 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 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 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

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 CloudFormation dan Organizations](#). Ini memberikan CloudFormation izin untuk membuat peran yang diperlukan dalam akun manajemen organisasi dan akun anggota 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. CloudFormation adalah 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 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"

```



```

    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"
        }
      }
    }
  }
}
```

Mematikan Resource Explorer

Bila Anda tidak perlu lagi mencari sumber daya tertentu AWS Region, Anda dapat mematikan hanya Penjelajah Sumber Daya AWS di Wilayah itu dengan menghapus indeksnya, atau Anda dapat menghapus Resource Explorer secara keseluruhan Wilayah AWS. 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 pertama AWS Region, Resource Explorer [membuat peran terkait layanan \(SLR\) yang dinamai `AWSServiceRoleForResourceExplorer`](#) dalam Akun AWS. Resource Explorer tidak menghapus ini SLR secara otomatis. Setelah menghapus indeks Resource Explorer di setiap Wilayah di akun, Anda dapat menggunakan IAM konsol 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 satu AWS Region, Resource Explorer akan membuat ulang peran terkait layanan secara otomatis.

Mematikan Resource Explorer dalam satu AWS Region

Anda dapat menonaktifkan Resource Explorer di sebuah AWS Region dengan menggunakan Konsol Manajemen AWS, dengan menggunakan perintah di AWS Command Line Interface (AWS CLI), atau dengan menggunakan API operasi dalam file 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 untuk Akun 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.

Konsol Manajemen AWS

Untuk menghapus indeks Resource Explorer di AWS Region

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 AWS Region

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 keDELETED.

```
$ 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 semua Wilayah AWS

Jika Anda ingin mematikan Penjelajah Sumber Daya AWS sepenuhnya, lakukan prosedur berikut.

Note

Resource Explorer membuat peran terkait layanan yang dinamai `AWSServiceRoleForResourceExplorer` di akun saat Anda membuat indeks di akun pertama AWS Region. Resource Explorer tidak secara otomatis menghapus peran terkait layanan ini. Setelah menghapus indeks Resource Explorer di setiap Wilayah, Anda kemudian dapat menggunakan IAM konsol untuk menghapus peran jika Anda yakin tidak akan menggunakan Resource Explorer lagi di masa mendatang. Jika Anda menghapus peran dan kemudian memilih untuk memulai Resource Explorer di setidaknya satu AWS Region, Resource Explorer akan membuat ulang peran terkait layanan.

Anda dapat menonaktifkan Resource Explorer dengan menggunakan Konsol Manajemen AWS, dengan menggunakan perintah di AWS Command Line Interface (AWS CLI), atau dengan menggunakan API operasi dalam file AWS SDK.

Konsol Manajemen AWS

Jika Anda tidak lagi ingin mendukung pencarian sumber daya AWS Region di salah satu sumber daya Anda Akun AWS, lakukan langkah-langkah dalam prosedur berikut.

Untuk menonaktifkan Resource Explorer di semua Wilayah AWS

1. Buka halaman [Pengaturan](#) Resource Explorer.
2. Di bagian Indeks, pilih kotak centang di samping semua yang terdaftar Wilayah 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 Delete indexes, 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 beberapa Wilayah yang dipilih.

AWS CLI

Untuk menonaktifkan Resource Explorer di semua Wilayah AWS

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

```
$ 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 Region 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 selesai. 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"
}
```

Mengelola tampilan Resource Explorer untuk menyediakan akses ke pencarian

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 Akun AWS.

Tampilan hanya dapat diakses oleh prinsipal (IAM peran 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 tampilan [ARN](#).

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 AWS Region 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.

Ada beberapa elemen kunci untuk setiap tampilan:

Izin untuk mencari

Anda dapat menggunakan kebijakan AWS 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 kebijakan AWS terkelola yang dinamai `AWSResourceExplorerReadOnlyAccess` dengan kepala sekolah Anda, itu memberi mereka kemampuan untuk mencari menggunakan tampilan apa pun di akun.

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

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

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

- Pengguna dan grup di AWS IAM Identity Center:

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

- Pengguna yang dikelola IAM melalui penyedia identitas:

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

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

Untuk informasi selengkapnya tentang izin yang terkait dengan tampilan, lihat [Memberikan 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 [Menelusuri](#).

Tampilan juga dapat menentukan potongan informasi opsional mana 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 daya.

Lingkup pencarian

- **Lingkup wilayah** — Saat Anda mencari AWS Region dengan Resource Explorer, hasilnya hanya dapat menyertakan 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. Saat Anda melakukan ini, semua Wilayah lain tempat Resource Explorer diaktifkan mereplikasi informasi indeksnya ke Region dengan indeks agregator. Jika Anda mencari di Wilayah tersebut, hasil tersebut menyertakan 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 secara eksplisit menentukan tampilan, Resource Explorer menggunakan tampilan default yang ditentukan untuk itu. AWS Region

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 menggunakan Konsol Manajemen AWS dan memilih opsi Pengaturan cepat, Anda harus menentukan Wilayah mana yang berisi indeks agregator untuk akun tersebut. Resource Explorer secara otomatis membuat tampilan default di Region indeks agregator yang ditentukan.
- Jika Anda mendaftarkan Resource Explorer menggunakan Konsol Manajemen AWS dan memilih opsi Pengaturan lanjutan, Anda dapat memilih untuk membuat indeks agregator untuk akun di Wilayah tertentu. Jika Anda melakukan ini, Resource Explorer akan membuat tampilan default secara otomatis di Region indeks agregator.

- Jika Anda mendaftarkan Resource Explorer menggunakan konsol dan memilih untuk tidak mendaftarkan Region indeks agregator, Resource Explorer akan membuat tampilan default untuk indeks lokal di setiap Wilayah.
- Jika Anda mendaftarkan Resource Explorer menggunakan AWS CLI atau API operasi, 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 mencari.

Membuat tampilan Resource Explorer untuk digunakan untuk pencarian

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 AWS Region, 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 Konsol Manajemen AWS atau dengan menjalankan AWS CLI perintah atau API operasi yang setara dalam file 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 AWS Region .

Konsol Manajemen AWS

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 AWS Region.

3. Pilih AWS Region di mana Anda ingin membuat tampilan. Untuk membuat tampilan yang mengembalikan sumber daya dari semua Wilayah di akun, pilih AWS Region 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 hasil.

- 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, lihat [Filter](#).

- 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 (ABAC) berbasis atribut. 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. Untuk informasi selengkapnya, silakan lihat [Memberikan akses ke tampilan Resource Explorer untuk pencarian](#)

AWS CLI

Untuk membuat tampilan

Jalankan perintah berikut untuk membuat tampilan di ditentukan AWS Region. Contoh berikut membuat tampilan yang hanya mengembalikan sumber daya yang terkait dengan EC2 layanan Amazon 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 organisasi AndaARN.
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 organisasi AndaARN.
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 ke Penjelajah Sumber Daya AWS tampilan. Untuk melakukannya, gunakan kebijakan izin berbasis identitas ke prinsipal AWS Identity and Access Management (IAM) yang perlu mencari dengan tampilan.

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

- Pengguna dan grup di AWS IAM Identity Center:

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

- Pengguna yang dikelola dalam IAM melalui penyedia identitas:

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, lihat [AWS 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 di AWS 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 semua AWS 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}"} }
```

}

Bahwa `Condition` dalam contoh sebelumnya menetapkan bahwa permintaan diperbolehkan hanya jika `Environment` tag melekat pada prinsipal membuat permintaan cocok `Environment` 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 dilampirkan ke 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 mengakses AWS sumber daya berdasarkan tanda](#)
- [Mengontrol akses ke AWS 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 dalam AWS Region

Di Penjelajah Sumber Daya AWS, Anda dapat menentukan banyak tampilan dalam AWS Region, 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 setiap Konsol Manajemen AWS 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 menggunakan Konsol Manajemen AWS atau dengan menjalankan AWS CLI perintah atau operasi API yang setara dalam AWS SDK.

Konsol Manajemen AWS

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 tag AWS sumber daya, lihat [Menandai AWS Sumber Daya](#) di Referensi Umum Amazon Web Services.

Menambahkan tag ke tampilan Anda

Anda dapat menambahkan tag ke tampilan Resource Explorer dengan menggunakan Konsol Manajemen AWS atau dengan menjalankan AWS CLI perintah atau operasi API yang setara di AWS SDK.

Konsol Manajemen AWS

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 utama dan nilai 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 pengguna daya dapat dilampirkan hingga 50 tag daya. Setiap tag yang dibuat dan dikelola secara otomatis oleh tag yang dibuat dan dikelola secara otomatis AWS 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 kunci `environment` dan nilai `production` 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, gunakan `untag-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 disebut `ViewA`, Anda melampirkan `tagenvironment=prod` (key name=value). Lain `ViewB` mungkin ditandai `environment=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 izin AWS 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 memiliki `environment` tag dengan nilai yang sama dengan `environment` 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 dapat `Search` menggunakan tampilan apa pun yang ditandai dengan nilai `environment` tag yang sama persis dengan `environment` 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 memiliki `environment` tag tetapi nilainya tidak cocok, atau jika salah satu hilang `environment` 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 itu AWS?](#)

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. Hal ini berbeda dengan AWS Identity and Access Management (IAM) kebijakan berbasis identitas. Kebijakan IAM berbasis identitas 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 RAM menangani kompleksitas kebijakan berbasis sumber daya untuk Anda. Sebelum Anda dapat berbagi, Anda harus melakukan tugas-tugas berikut:

- [Aktifkan pencarian multi-akun.](#)

- Pastikan kebijakan berbasis sumber daya atau kebijakan IAM berbasis identitas yang Anda gunakan untuk berbagi dan membatalkan pembagian tampilan mencakup, dan izin. `resource-explorer-2:GetResourcePolicy` `resource-explorer-2:PutResourcePolicy` `resource-explorer-2>DeleteResourcePolicy`

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 RAM sepenuhnya mendukung tampilan Resource Explorer. AWS RAM menggunakan 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, OUs, 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 IAM berbasis identitas 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, lihat [Menambahkan 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 IAM Pengguna.

Menghapus tampilan di Resource Explorer

Bila Anda tidak lagi memerlukan Penjelajah Sumber Daya AWS tampilan, Anda dapat menghapusnya. Anda dapat menghapus tampilan dengan menggunakan Konsol Manajemen AWS atau dengan menjalankan AWS CLI perintah atau operasi API yang setara di AWS SDK.

Note

Anda tidak dapat menghapus tampilan yang saat ini ditetapkan sebagai default untuk tampilan tersebut AWS Region. Untuk menghapus tampilan, Anda harus menghapus tampilan sebagai default. Untuk melakukan ini, Anda dapat menjalankan operasi [DisassociateDefaultView](#) API 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

Konsol Manajemen AWS

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"
}
```

Menggunakan Penjelajah Sumber Daya AWS untuk mencari sumber daya

Tujuan utama mengaktifkan Penjelajah Sumber Daya AWS di dalam akun AWS adalah untuk memungkinkan pengguna Anda untuk mencari sumber daya di akun. Gunakan Konsol Manajemen AWS atau AWS 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 dari [kebijakan izin berbasis identitas](#) melekat 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, lihat [Mengelola tampilan Resource Explorer untuk menyediakan akses ke pencarian](#).

- 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 dalam AWS Region.

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 semua Wilayah 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 semua Wilayah AWS di 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 Explorer](#) digabungkan 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 implisit AND, 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 satu AWS Region. Oleh karena itu, query berikut tidak mengembalikan hasil.

```
region:us-east-1 region:us-west-1
```

Keterbatasan ini tidak berlaku untuk filter untuk atribut yang dapat memiliki beberapa nilai pada saat yang sama, seperti `tag:tag.key:`, dan `tag.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, lihat [Kuota untuk Resource Explorer](#).

Konsol Manajemen AWS

Untuk mencari sumber daya menggunakan Resource Explorer

1. Pada [Pencarian sumber daya](#) halaman, mulailah dengan memilih tampilan yang ingin Anda gunakan. Anda dapat memilih dari antara hanya pandangan yang Anda memiliki izin untuk mengakses.
2. Untuk Kueri, masukkan istilah pencarian dan [saringan](#) yang mengidentifikasi sumber daya yang ingin Anda lihat. Untuk informasi tentang semua opsi sintaks yang tersedia, lihat [Referensi sintaks kueri pencarian untuk Resource Explorer](#).
3. Tekan **Memasukkan** untuk mengirimkan permintaan Anda.

Resource Explorer menampilkan semua hasil yang cocok dengan `Filter` yang didefinisikan dalam tampilan dan Kueri 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 pengenalan 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, lihat [Referensi 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 hasil Pencarian sumber daya `query` ke nilai dipisahkan koma (.csv) berkas. File.csv mencakup pengenalan, jenis sumber daya, Wilayah, Akun AWS, jumlah total tag, dan kolom untuk setiap kunci tag unik dalam koleksi. File.csv dapat membantu Anda mengonfigurasi AWS sumber daya di organisasi Anda, atau tentukan di mana terdapat tumpang tindih atau ketidakkonsistenan dalam memberi tag di seluruh sumber daya.

1. Dalam hasil Pencarian sumber daya `query`, pilih Ekspor 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.

Search criteria

View [Info](#) Query [Info](#)

Resources (1000+) [Info](#)

All AWS Regions All types < 1 2

Export 1000 resources to CSV ▲

Export visible columns

Export all columns

Identifier 🔗	Resource type	Region	AWS Account	Tag: SoftwareType
○ DeploymentStack-	logs:log-group	US East (N. Virginia) us-east-1	This account	(not tagged)

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

Jenis sumber daya yang dapat Anda cari dengan Resource Explorer

Resource Explorer mendukung jenis sumber daya di berbagai AWS layanan.

Topik

- [Layanan dan jenis sumber daya yang didukung](#)
- [Mengakses daftar jenis sumber daya yang didukung secara terprogram](#)
- [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. Untuk daftar jenis sumber daya yang terpengaruh oleh masalah ini, lihat [Jenis 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 penelusuran.

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.

Tabel berikut mencantumkan jenis sumber daya yang didukung untuk penelusuran Penjelajah Sumber Daya AWS.

Note

Per 9 Juli 2024, Resource Explorer tidak lagi mendukung jenis sumber daya berikut:

- Layanan Kontainer Elastis Amazon - `ecs:task`
- AWS Systems Manager — `ssm:automation-execution`
- AWS Systems Manager — `ssm:patchbaseline`

Anda masih dapat menggunakan jenis sumber daya ini di layanan mereka sendiri, tetapi mereka tidak lagi diindeks atau dicari di Resource Explorer.

Layanan dan jenis sumber daya yang didukung

Didukung Layanan AWS

- [API Gerbang Amazon](#)
- [AWS App Runner](#)
- [Amazon AppStream 2.0](#)
- [AWS AppSync](#)
- [Amazon Athena](#)
- [AWS Backup](#)
- [AWS Batch](#)
- [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](#)
- [Kebijakan Amazon Connect](#)
- [Amazon Detective](#)
- [Amazon DynamoDB](#)
- [EC2 Image Builder](#)
- [Amazon ECR Publik](#)
- [AWS Elastic Beanstalk](#)

- [Amazon ElastiCache](#)
- [Amazon Elastic Compute Cloud \(AmazonEC2\)](#)
- [Amazon Elastic Container Registry](#)
- [Amazon Elastic Container Service](#)
- [Amazon Elastic File System](#)
- [Penyeimbang Beban Elastis](#)
- [AWS Elemental MediaPackage](#)
- [AWS Elemental MediaTailor](#)
- [Amazon Tanpa EMR 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](#)
- [Amazon Managed Service for 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 \(AmazonRDS\)](#)
- [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](#)

API Gerbang Amazon

- `apigateway:restapis`

AWS App Runner

- `apprunner:vpconnector`

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`

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`

EC2Image Builder

- `imagebuilder:component`
- `imagebuilder:containerrecipe`
- `imagebuilder:distributionconfiguration`
- `imagebuilder:image`
- `imagebuilder:imagepipeline`
- `imagebuilder:imagerecipe`
- `imagebuilder:infrastructureconfiguration`

Amazon ECR Publik

- `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 (AmazonEC2)

- 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-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 Tanpa EMR Server

- `emr-serverless:applications`

Amazon EventBridge

- `events:event-bus`
- `events:rule`

AWS Fault Injection Service

- `fis:experimenttemplate`

Amazon Forecast

- `forecast:dataset`
- `forecast: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:virtualmfadvice`

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`

Amazon Managed Service for 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:eventssubscription`
- `redshift:parametergroup`
- `redshift:snapshot`
- `redshift:snapshotcopygrant`
- `redshift:snapshotschedule`
- `redshift:subnetgroup`
- `redshift:usagelimit`

Amazon Rekognition

- `rekognition:project`

Amazon Relational Database Service (AmazonRDS)

- `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:document`
- `ssm:maintenancewindow`
- `ssm:managed-instance`
- `ssm:parameter`
- `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 memanggil [ListSupportedResourceTypes](#) operasi dari mana pun AWS SDK.

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 ec2:securitygroupingress	ec2:security-group-rule
elasticloadbalancingv2:loadbalancer	elasticloadbalancing:loadbalancer
docdb:dbcluster neptune:dbcluster rds:dbcluster	rds:cluster
docdb:dbclusterparametergroup neptune:dbclusterparametergroup rds:dbclusterparametergroup	rds:cluster-pg
docdb:clustersnapshot neptune:dbclustersnapshot rds:clustersnapshot	rds:cluster-snapshot
docdb:dbinstance neptune:dbinstance rds:dbinstance	rds:db

Jenis sumber daya aktual	Dilaporkan sebagai tipe sumber daya
docdb:eventssubscription neptune:eventssubscription rds:eventssubscription	rds:es
docdb:globalcluster rds:globalcluster	rds:global-cluster
neptune:dbparametergroup rds:dbparametergroup	rds:pg
docdb:dbsubnetgroup neptune:dbsubnetgroup rds:dbsubnetgroup	rds:subgrp

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, lihat [Contoh 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 AWS Region 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, lihat [Memberikan 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 untuk 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 memperbaiki 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 AND operator. 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 ANDlogis. 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) AWS Region 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 AWS Region. 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.

Filter nama	Deskripsi dan contoh
<code>accountid:</code>	Akun AWS Yang memiliki sumber daya. Resource Explorer termasuk dalam hasil hanya sumber daya yang dimiliki oleh akun yang ditentukan. <code>accountid:123456789012</code>
<code>application:</code>	Filter ini memungkinkan Anda untuk mencari sumber daya dengan kunci <code>awsApplication tag</code> dan nilai grup sumber daya. Anda dapat mencari berdasarkan nama aplikasi atau grup sumber daya aplikasiARN. <code>application:MyApplicationName</code>


Filter nama	Deskripsi dan contoh
	<p>application:arn:aws:resource-groups: us-east-1 :123456789012:group/MyApplicationName/123456789abcd</p> <p>arn:aws:resource-groups: us-east-1 :123456789012:group/MyApplicationName/123456789abcd</p> <div data-bbox="402 512 1507 730" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>Untuk menggunakan filter ini, tampilan Anda harus memiliki akses ke data penandaan.</p> </div>
id:	<p>Pengidentifikasi sumber daya individu, dinyatakan sebagai nama sumber daya Amazon (ARN).</p> <p>id:arn:aws:license-manager: us-east-1 :123456789012:license-configuration:lic-ecbd5574fd92cb0d312baea26EXAMPLE</p>
region:	<p>Di AWS Region mana sumber daya berada. Resource Explorer termasuk dalam hasil hanya sumber daya yang berada di ditentukan AWS Region.</p> <p>region:us-east-1</p> <div data-bbox="402 1276 1507 1738" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>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 individu. Misalnya, us-east-1 dicari sebagai us, east, dan 1. Perincian menjadi komponen ini tidak terjadi saat Anda menggunakan region: awalan.</p> </div>

Filter nama	Deskripsi dan contoh
<code>region:global</code>	<p>Kasus khusus untuk <code>region:</code> filter yang dapat Anda gunakan untuk menemukan sumber daya yang tidak terkait dengan individu AWS Region tetapi dianggap cakupan global.</p> <p><code>region:global</code></p> <div data-bbox="402 478 1507 842" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>Mengetik hanya kata kunci <code>global</code> tidak mengembalikan hasil yang sama <code>region:global</code> karena kata literal “global” tidak melekat pada sumber daya global. Mengetik <code>global</code> sebagai kata kunci hanya mengembalikan sumber daya yang memiliki string literal yang terkait dengan sumber daya.</p> </div>
<code>resourcetype:</code>	<p>Jenis sumber daya dalam <i>service:type</i> notasi. Resource Explorer termasuk dalam hasil hanya sumber daya dari jenis yang ditentukan.</p> <p><code>resourcetype:ec2:instance</code></p>
<code>resourcetype.supports:</code>	<p>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.</p> <p><code>resourcetype.supports:tags</code></p>
<code>service:</code>	<p>Layanan AWS Yang terkait dengan jenis sumber daya. Resource Explorer termasuk dalam hasil hanya sumber daya yang dibuat dan dikelola oleh layanan yang ditentukan.</p> <p><code>service:ec2</code></p>
<code>tag:</code>	<p>Sebuah pasangan kunci tag/nilai dinyatakan sebagai. <code><key>=<value></code> Resource Explorer menyertakan dalam hasil hanya sumber daya yang memiliki tag dengan kunci yang cocok dan nilai yang ditentukan.</p> <p><code>tag:environment=production</code></p>

Filter nama	Deskripsi dan contoh
<code>tag:all</code>	<p>Kasus khusus <code>tag: filter</code> yang memungkinkan Anda mencari sumber daya yang memiliki satu atau beberapa tag buatan pengguna yang dilampirkan, meskipun jenis sumber daya tidak didukung di Resource Explorer.</p> <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>Sumber daya dengan tag AWS yang dibuat layanan masih muncul di hasil untuk filter ini.</p> </div>
<code>tag:none</code>	<p>Kasus khusus <code>tag: filter</code> yang memungkinkan Anda mencari sumber daya apa pun yang tidak memiliki tag yang dibuat pengguna.</p> <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>Sumber daya dengan tag AWS yang dibuat layanan masih muncul di hasil untuk filter ini.</p> </div>
<code>tag.key:</code>	<p>Sebuah kunci tag. Resource Explorer menyertakan dalam hasil hanya sumber daya yang memiliki tag dengan kunci yang cocok, terlepas dari nilainya.</p> <p><code>tag.key:environment</code></p>
<code>tag.value:</code>	<p>Nilai tag. Resource Explorer menyertakan dalam hasil hanya sumber daya yang memiliki tag dengan nilai yang cocok, terlepas dari nama kuncinya.</p> <p><code>tag.value:production</code></p>

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
<p><i>"multiple word phrase"</i></p> <p>atau</p> <p><i>"hyphenate d-phrase "</i></p>	<p>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.</p> <p>Jika Anda tidak menggunakan tanda kutip ganda, Resource Explorer memecah frasa menjadi komponennya dengan spasi atau tanda hubung, dan menyertakan 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.</p> <p>"This matches only resources with the whole sentence."</p> <p>This matches resources with any of the words.</p> <p>"us-east-1" — hanya cocok dengan sumber daya yang terkait dengan Wilayah yang tepat itu.</p> <p>us-east-1 — cocok dengan sumber daya apa pun yang berisi "kami" atau "timur" atau "1".</p> <p>-tag:"environment=production"</p>
<p><i>keyword*</i></p>	<p>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.</p> <p>region:us-east*</p> <div data-bbox="391 1591 1507 1864" style="border: 1px solid #f08080; padding: 10px; margin-top: 10px;"> <p> Important</p> <p>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.</p> </div>

Operator	Deskripsi dan contoh
	<p>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.</p>

Operator	Deskripsi dan contoh
<p><i>-keyword</i></p>	<p>Not operator. Anda dapat menempatkan tanda hubung (-) di awal kata kunci atau filter untuk membalikkan hasil pencarian. Resource Explorer mengecualikan 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 EC2 layanan Amazon dikecualikan dari hasil.</p> <p><code>-service:ec2</code></p> <div data-bbox="418 604 609 646"><p> Important</p></div> <p>Jika Anda menggunakan AWS CLI search perintah dan nilai <code>--query-string</code> parameter Anda memiliki <code>-</code> 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.</p> <pre data-bbox="472 982 1474 1100">aws resource-explorer-2 search --query-string "-tag:none region:us-east-1"</pre> <p>String kueri yang dikoreksi berikut, dengan <code>=</code> mengganti spasi, berfungsi seperti yang diharapkan.</p> <pre data-bbox="472 1255 1474 1373">aws resource-explorer-2 search --query-string "=tag:none region:us-east-1"</pre> <p>Jika Anda mengubah urutan filter dalam string kueri sehingga <code>-</code> bukan karakter pertama dalam nilai parameter, Anda dapat menggunakan karakter spasi standar. String query berikut berfungsi.</p> <pre data-bbox="472 1570 1474 1688">aws resource-explorer-2 search --query-string "region:us-east-1 -tag:none"</pre>

Operator	Deskripsi dan contoh
<code>\<special character></code>	<p>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 menggunakan kata kunci teks bentuk bebas yang menyertakan tanda hubung (-) karakter (). "my-key-word"</p> <p>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.</p> <pre>"my\ -key\ -word"</pre> <p>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.</p> <pre>"some_text\\some_more_text"</pre>

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 file. 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 dalam Penjelajah Sumber Daya AWS.

Important

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 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 oleh AWS dibebaskan dari filter ini dan masih muncul dalam hasil.

```
tag:none
```

Untuk juga mengecualikan semua tag sistem yang AWS 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. AWS tag 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 cocok `PROD`, `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 subset Wilayah 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 satuAWS Region. 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:.`

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-2AWS Region (atau Wilayah lain yang termasukwest 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 dariCloudFormation 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 Konsol Manajemen AWS

Konsol Manajemen AWS Termasuk 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 Anda Akun 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

- [Memeriksa apakah pencarian terpadu diaktifkan](#)
- [Mengaktifkan pencarian terpadu](#)

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 satu AWS Region. 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.](#)

Membuat sumber daya Resource Explorer dengan CloudFormation

Penjelajah Sumber Daya AWS terintegrasi dengan AWS 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 AWS Region

Saat menggunakan CloudFormation, 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 CloudFormation untuk menyebarkan Resource Explorer ke AWS Organizations

Anda dapat menggunakan 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-masing AWS Region, 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 [CloudFormation templat](#). 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 CloudFormation Designer untuk membantu Anda memulai dengan templat CloudFormation. Untuk informasi selengkapnya, lihat [Apa yang dimaksud dengan CloudFormation Designer?](#) dalam Panduan Pengguna AWS CloudFormation.

Resource Explorer mendukung pembuatan jenis sumber daya berikut di CloudFormation:

- [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 Explorer AWS Region 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 pencarian](#).

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 dalam AWS Region](#)

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 CloudFormation

Untuk mempelajari selengkapnya tentang CloudFormation, lihat sumber daya berikut:

- [AWS CloudFormation](#)
- [AWS CloudFormationPanduan Pengguna](#)
- [AWS CloudFormationPanduan](#)

Menggunakan Amazon Q Developer dalam aplikasi obrolan untuk mencari sumber daya

Anda dapat mencari dan menemukan informasi tentang Layanan AWS dan AWS sumber daya Anda dengan mengajukan pertanyaan bahasa Amazon Q Developer dalam aplikasi obrolan alami. Amazon Q Developer dalam aplikasi obrolan menjawab pertanyaan terkait layanan langsung di saluran obrolan Anda dengan AWS dokumentasi yang relevan dan kutipan artikel dukungan. Amazon Q Developer dalam aplikasi obrolan menggunakan Resource Explorer untuk mencari dan menemukan jawaban atas pertanyaan terkait sumber daya Anda.

Untuk informasi lebih lanjut, lihat [Apa itu Amazon Q Developer dalam aplikasi obrolan?](#) dalam Panduan Amazon Q Developer dalam aplikasi obrolan Administrator.

AWS pertanyaan sumber daya

Amazon Q Developer dalam aplikasi obrolan menggunakan Resource Explorer untuk mencari dan menemukan sumber daya Anda. Amazon Q Developer dalam aplikasi obrolan menampilkan hasil pencarian ini dalam daftar. Daftar ini menunjukkan lima sumber daya pencocokan teratas dan mencakup kemampuan untuk memfilter hasil lebih lanjut berdasarkan jenis sumber daya AWS Region, dan tag.

Prasyarat

Untuk mengajukan pertanyaan terkait Amazon Q Developer dalam aplikasi obrolan sumber daya, Anda harus:

- Pastikan Anda memiliki indeks dan tampilan aktif dengan setidaknya satu tampilan default di Anda AWS Region. 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 adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. [Model tanggung jawab bersama](#) menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang berjalan Layanan AWS di dalamnya AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari [Program AWS Kepatuhan Program AWS Kepatuhan](#) . Untuk mempelajari tentang program kepatuhan yang berlaku untuk Resource Explorer, lihat [Layanan AWS di Cakupan berdasarkan Program Kepatuhan Layanan AWS](#) .
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh Layanan AWS yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup kepekaan data Anda, persyaratan perusahaan, serta peraturan perundangan yang berlaku

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Penjelajah Sumber Daya AWS. Ini menunjukkan kepada Anda cara mengkonfigurasi Resource Explorer untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga mempelajari cara menggunakan Layanan AWS yang lain yang membantu Anda memantau dan mengamankan sumber daya Resource Explorer Anda.

Konten

- [Tingkatkan IAM kebijakan ke IPv6](#)
- [Identitas dan manajemen akses untuk Penjelajah Sumber Daya AWS](#)
- [Perlindungan data di Penjelajah Sumber Daya AWS](#)
- [Validasi kepatuhan untuk Penjelajah Sumber Daya AWS](#)
- [Ketahanan di Penjelajah Sumber Daya AWS](#)
- [Keamanan infrastruktur di Penjelajah Sumber Daya AWS](#)

Tingkatkan IAM kebijakan ke IPv6

Penjelajah Sumber Daya AWS pelanggan menggunakan IAM kebijakan untuk menetapkan rentang alamat IP yang diizinkan dan mencegah alamat IP apa pun di luar rentang yang dikonfigurasi agar tidak dapat mengakses Resource Explorer APIs.

Sumber daya-penjelajah-2.*region*Domain.api.aws tempat Resource Explorer di-host APIs sedang ditingkatkan untuk mendukung IPv6 sebagai tambahan. IPv4

Kebijakan pemfilteran alamat IP yang tidak diperbarui untuk menangani IPv6 alamat dapat mengakibatkan klien kehilangan akses ke sumber daya pada API domain Resource Explorer.

Pelanggan terpengaruh oleh peningkatan dari ke IPv4 IPv6

Pelanggan yang menggunakan pengalamatan ganda dengan kebijakan yang berisi aws: sourceIp terpengaruh oleh peningkatan ini. Pengalamatan ganda berarti bahwa jaringan mendukung keduanya IPv4 dan IPv6.

Jika Anda menggunakan pengalamatan ganda, Anda harus memperbarui IAM kebijakan yang saat ini dikonfigurasi dengan alamat IPv4 format untuk menyertakan alamat IPv6 format.

Untuk bantuan terkait masalah akses, hubungi [Dukungan](#).

Note

Pelanggan berikut tidak terpengaruh oleh peningkatan ini:

- Pelanggan yang hanya berada di IPv4 jaringan.
- Pelanggan yang hanya berada di IPv6 jaringan.

Apa yang dimaksud dengan IPv6?

IPv6 adalah standar IP generasi berikutnya yang dimaksudkan untuk akhirnya menggantikan IPv4. Versi sebelumnya, IPv4, menggunakan skema pengalamatan 32-bit untuk mendukung 4,3 miliar perangkat. IPv6 sebaliknya menggunakan pengalamatan 128-bit untuk mendukung sekitar 340 triliun triliun (atau 2 hingga daya 128) perangkat.

```
2001:cdba:0000:0000:0000:0000:3257:9652
```

```
2001:cdba:0:0:0:0:3257:9652
2001:cdba::3257:965
```

Memperbarui IAM kebijakan untuk IPv6

IAMkebijakan saat ini digunakan untuk menetapkan rentang alamat IP yang diizinkan menggunakan `aws:SourceIp` filter.

Pengalamatan ganda mendukung keduanya IPv4 dan IPV6 lalu lintas. Jika jaringan Anda menggunakan pengalamatan ganda, Anda harus memastikan bahwa setiap IAM kebijakan yang digunakan untuk pemfilteran alamat IP diperbarui untuk menyertakan IPv6 rentang alamat.

Misalnya, kebijakan bucket Amazon S3 ini mengidentifikasi rentang IPv4 alamat yang diizinkan `192.0.2.0.*` dan elemen `203.0.113.0.*`. `Condition`

```
# https://docs.aws.amazon.com/IAM/latest/UserGuide/
reference_policies_examples_aws_deny-ip.html
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NotIpAddress": {
        "*aws:SourceIp": [
          "*192.0.2.0/24*",
          "*203.0.113.0/24*"
        ]
      },
      "Bool": {
        "aws:ViaAWSService": "false"
      }
    }
  }
}
```

Untuk memperbarui kebijakan ini, `Condition` elemen kebijakan diperbarui untuk menyertakan rentang IPv6 alamat `2001:DB8:1234:5678::/64` dan `2001:cdba:3257:8593::/64`.

Note

LAKUKAN IPv4 alamat NOT REMOVE yang ada karena diperlukan untuk kompatibilitas mundur.

```
"Condition": {
  "NotIpAddress": {
    "*aws:SourceIp*": [
      "*192.0.2.0/24*", <<DO NOT REMOVE existing IPv4 address>>
      "*203.0.113.0/24*", <<DO NOT REMOVE existing IPv4 address>>
      "*2001:DB8:1234:5678::/64*", <<New IPv6 IP address>>
      "*2001:cdba:3257:8593::/64*" <<New IPv6 IP address>>
    ]
  },
  "Bool": {
    "aws:ViaAWSService": "false"
  }
}
```

Untuk informasi selengkapnya tentang mengelola izin akses dengan IAM, lihat [Kebijakan terkelola dan kebijakan sebaris](#) di AWS Identity and Access Management Panduan Pengguna.

Verifikasi klien Anda dapat mendukung IPv6

Pelanggan menggunakan resource-explorer-2. Endpoint {region}.api.aws disarankan untuk memverifikasi apakah klien mereka dapat mengakses Layanan AWS Endpoint lain yang sudah diaktifkan. IPv6 Langkah-langkah berikut menjelaskan cara memverifikasi titik akhir tersebut.

Contoh ini menggunakan Linux dan curl versi 8.6.0 dan menggunakan [titik akhir layanan Amazon Athena yang telah IPv6 mengaktifkan titik akhir](#) yang terletak di domain api.aws.

Note

Beralih AWS Region ke Wilayah yang sama di mana klien berada. Dalam contoh ini, kita menggunakan US East (N. Virginia) — us-east-1 endpoint.

1. Tentukan apakah titik akhir menyelesaikan dengan IPv6 alamat menggunakan perintah curl berikut.

```
dig +short AAAA athena.us-east-1.api.aws
2600:1f18:e2f:4e05:1a8a:948e:7c08:d2d6
2600:1f18:e2f:4e03:4a1e:83b0:8823:4ce5
2600:1f18:e2f:4e04:34c3:6e9a:2b0d:dc79
```

2. Tentukan apakah jaringan klien dapat membuat koneksi menggunakan IPv6 menggunakan perintah curl berikut.

```
curl --ipv6 -o /dev/null --silent -w "\nremote ip: %{remote_ip}\nresponse code:
%{response_code}\n" https://athena.us-east-1.api.aws

remote ip: 2600:1f18:e2f:4e05:1a8a:948e:7c08:d2d6
response code: 404
```

Jika IP jarak jauh diidentifikasi dan kode respons tidak 0, koneksi jaringan berhasil dibuat ke titik akhir menggunakan IPv6.

Jika IP jarak jauh kosong atau kode responsnya 0, jaringan klien atau jalur jaringan ke titik akhir adalah IPv4 -only. Anda dapat memverifikasi konfigurasi ini dengan perintah curl berikut.

```
curl -o /dev/null --silent -w "\nremote ip: %{remote_ip}\nresponse code:
%{response_code}\n" https://athena.us-east-1.api.aws

remote ip: 3.210.103.49
response code: 404
```

Jika IP jarak jauh diidentifikasi dan kode respons tidak 0, koneksi jaringan berhasil dibuat ke titik akhir menggunakan IPv4. IP jarak jauh harus menjadi IPv4 alamat karena sistem operasi harus memilih protokol yang valid untuk klien. Jika IP jarak jauh bukan IPv4 alamat, gunakan perintah berikut untuk memaksa curl untuk digunakan IPv4.

```
curl --ipv4 -o /dev/null --silent -w "\nremote ip: %{remote_ip}\nresponse code:
%{response_code}\n" https://athena.us-east-1.api.aws

remote ip: 35.170.237.34
response code: 404
```

Identitas dan manajemen akses untuk Penjelajah Sumber Daya AWS

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

Topik

- [Audiens](#)
- [Mengautentikasi dengan identitas](#)
- [Mengelola akses menggunakan kebijakan](#)
- [Bagaimana Resource Explorer bekerja dengan IAM](#)
- [Contoh kebijakan berbasis identitas Penjelajah Sumber Daya AWS](#)
- [Contoh kebijakan kontrol layanan untuk AWS Organizations dan Resource Explorer](#)
- [AWS kebijakan terkelola untuk Penjelajah Sumber Daya AWS](#)
- [Menggunakan peran terkait layanan untuk Resource Explorer](#)
- [Izin pemecahan masalah Penjelajah Sumber Daya AWS](#)

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, lihat [izin pemecahan masalah Penjelajah Sumber Daya AWS](#).

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. Anda kemudian harus mengirimkan permintaan ke IAM administrator Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasar IAM. Untuk mempelajari selengkapnya tentang cara perusahaan Anda dapat menggunakan IAM Resource Explorer, lihat [Bagaimana Resource Explorer bekerja dengan IAM](#).

IAM administrator - Jika Anda seorang IAM administrator, 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, lihat. IAM [Contoh kebijakan berbasis identitas Penjelajah Sumber Daya AWS](#)

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai IAM pengguna, atau dengan mengambil peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensi yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (Pusat IAM Identitas), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas federasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan IAM peran. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke Konsol Manajemen AWS atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat [Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS](#).

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 AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang menggunakan metode yang disarankan untuk menandatangani permintaan sendiri, lihat [Menandatangani AWS API permintaan](#) di Panduan IAM Pengguna.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari lebih lanjut, lihat [Autentikasi multi-faktor](#) di Panduan AWS IAM Identity Center Pengguna dan [Menggunakan otentikasi multi-faktor \(MFA\) AWS di Panduan Pengguna. IAM](#)

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar 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, lihat [Tugas yang memerlukan kredensi pengguna root](#) di IAMPanduan Pengguna.

Pengguna dan grup

[IAMPengguna](#) adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, sebaiknya mengandalkan kredensi sementara daripada membuat IAM pengguna yang memiliki kredensi jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensial jangka panjang dengan IAM pengguna, kami sarankan Anda memutar kunci akses. Untuk informasi selengkapnya, lihat [Memutar kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensi jangka panjang](#) di IAMPanduan Pengguna.

[IAMGrup](#) adalah identitas yang menentukan kumpulan IAM pengguna. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup bernama IAMAdmins dan memberikan izin grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari lebih lanjut, lihat [Kapan membuat IAM pengguna \(bukan peran\)](#) di Panduan IAM Pengguna.

Peran

[IAMPeran](#) adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Ini mirip dengan IAM pengguna, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil IAM peran sementara Konsol Manajemen AWS dengan [beralih peran](#). Anda dapat mengambil peran dengan

memanggil AWS CLI atau AWS API operasi atau dengan menggunakan kustomURL. Untuk informasi selengkapnya tentang metode penggunaan peran, lihat [Metode untuk mengambil peran](#) dalam Panduan IAM Pengguna.

IAMperan dengan kredensi sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat [Membuat peran untuk Penyedia Identitas pihak ketiga](#) di Panduan IAM Pengguna. Jika Anda menggunakan Pusat IAM Identitas, Anda mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah diautentikasi, Pusat IAM Identitas menghubungkan izin yang disetel ke peran. IAM Untuk informasi tentang set izin, lihat [Set izin](#) dalam Panduan Pengguna AWS IAM Identity Center .
- Izin IAM pengguna sementara — IAM Pengguna atau peran dapat mengambil IAM peran untuk sementara mengambil izin yang berbeda untuk tugas tertentu.
- Akses lintas akun — Anda dapat menggunakan IAM peran untuk memungkinkan seseorang (prinsipal tepercaya) di akun lain mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Akses sumber daya lintas akun di IAM](#) Panduan Pengguna. IAM
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
- Sesi akses teruskan (FAS) — Saat Anda menggunakan IAM pengguna atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FASmenggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. FASPermintaan hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat FAS permintaan, lihat [Meneruskan sesi akses](#).

- Peran layanan — Peran layanan adalah [IAMperan](#) yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAMAdministrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalamIAM. Untuk informasi selengkapnya, lihat [Membuat peran untuk mendelegasikan izin ke Layanan AWS](#) dalam IAMPanduan Pengguna.
- Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. IAMAdministrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan IAM peran untuk mengelola kredensial sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI atau AWS API meminta. Ini lebih baik untuk menyimpan kunci akses dalam EC2 instance. Untuk menetapkan AWS peran ke EC2 instance dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat [Menggunakan IAM peran untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon](#) di IAMPanduan Pengguna.

Untuk mempelajari apakah akan menggunakan IAM peran atau IAM pengguna, lihat [Kapan membuat IAM peran \(bukan pengguna\)](#) di Panduan IAM Pengguna.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai JSON dokumen. Untuk informasi selengkapnya tentang struktur dan isi dokumen JSON kebijakan, lihat [Ringkasan JSON kebijakan](#) di Panduan IAM Pengguna.

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

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka butuhkan, IAM administrator dapat

membuat IAM kebijakan. Administrator kemudian dapat menambahkan IAM kebijakan ke peran, dan pengguna dapat mengambil peran.

IAMkebijakan menentukan izin untuk tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasi. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan itu bisa mendapatkan informasi peran dari Konsol Manajemen AWS, AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan JSON izin yang dapat dilampirkan ke identitas, seperti pengguna, grup IAM pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat [Membuat IAM kebijakan di Panduan Pengguna](#). IAM

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan terkelola atau kebijakan sebaris, lihat [Memilih antara kebijakan terkelola dan kebijakan sebaris](#) di IAMPanduan Pengguna.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen JSON kebijakan yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan IAM peran 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 tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus [menentukan prinsipal](#) dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

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

Penjelajah Sumber Daya AWS tidak mendukung kebijakan berbasis sumber daya.

Daftar kontrol akses (ACLs)

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLs mirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan. JSON

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACLs. Untuk mempelajari selengkapnya ACLs, lihat [Ikhtisar daftar kontrol akses \(ACL\)](#) di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon.

Penjelajah Sumber Daya AWS tidak mendukung ACLs.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- **Batas izin** — Batas izin adalah fitur lanjutan tempat Anda menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas (pengguna atau peran). IAM IAM Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan 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 akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batas izin, lihat [Batas izin untuk IAM entitas](#) di IAMPanduan Pengguna.
- **Kebijakan kontrol layanan (SCPs)** — SCPs adalah JSON kebijakan yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di AWS Organizations. AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCPMembatasi izin untuk entitas di akun anggota, termasuk masing-masing Pengguna root akun AWS. Untuk informasi selengkapnya tentang Organizations dan SCPs, lihat [Kebijakan kontrol layanan](#) di Panduan AWS Organizations Pengguna.
- **Kebijakan sesi** – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan

secara tegas dalam salah satu kebijakan ini membatalkan izin. Untuk informasi selengkapnya, lihat [Kebijakan sesi](#) di Panduan IAM Pengguna.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat [Logika evaluasi kebijakan](#) di Panduan IAM Pengguna.

Bagaimana Resource Explorer bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Penjelajah Sumber Daya AWS, Anda harus memahami IAM fitur apa yang tersedia untuk digunakan dengan Resource Explorer. Untuk mendapatkan tampilan tingkat tinggi tentang cara Layanan AWS kerja Resource Explorer dan lainnya IAM, lihat Layanan AWS cara [kerjanya IAM](#) di Panduan IAM Pengguna.

Topik

- [Kebijakan berbasis identitas Resource Explorer](#)
- [Otorisasi berdasarkan tag Resource Explorer](#)
- [IAM Peran Resource Explorer](#)

Seperti yang lainnya Layanan AWS, Resource Explorer memerlukan izin untuk menggunakan operasinya untuk berinteraksi dengan sumber daya Anda. Untuk mencari, pengguna harus memiliki izin untuk mengambil detail 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 IAM berbasis identitas yang memberikan izin tersebut kepada prinsipal yang sesuai. IAM Resource Explorer menyediakan [beberapa kebijakan terkelola](#) yang menentukan set izin umum. Anda dapat menetapkan ini ke IAM kepala sekolah Anda.

Kebijakan berbasis identitas Resource Explorer

Dengan kebijakan IAM berbasis identitas, Anda dapat menentukan tindakan yang diizinkan atau ditolak terhadap sumber daya tertentu dan kondisi di mana tindakan tersebut diizinkan atau ditolak. Resource Explorer mendukung tindakan, sumber daya, dan kunci kondisi tertentu. Untuk mempelajari semua elemen yang Anda gunakan dalam JSON kebijakan, lihat [referensi elemen IAM JSON kebijakan](#) di Panduan IAM Pengguna.

Tindakan

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

ActionElemen JSON kebijakan menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan AWS API operasi terkait. Ada beberapa pengecualian, seperti tindakan khusus izin yang tidak memiliki operasi yang cocok. API Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

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

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 Ditentukan oleh Penjelajah Sumber Daya AWS](#) dalam Referensi Otorisasi AWS Layanan.

Sumber daya

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

Elemen `Resource` JSON kebijakan menentukan objek atau objek yang tindakan tersebut berlaku. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Sebagai praktik terbaik, tentukan sumber daya menggunakan [Amazon Resource Name \(ARN\)](#). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

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

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

Tayang

Jenis sumber daya Resource Explorer utama adalah tampilan.

Sumber daya tampilan Resource Explorer memiliki ARN format berikut.

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

ARNFormat Resource Explorer ditampilkan 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 IAM kebijakan 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 tidak pernah ARNs digunakan kembali.

Untuk informasi selengkapnya tentang format ARNs, lihat [Amazon Resource Names \(ARNs\)](#).

Anda menggunakan kebijakan IAM berbasis identitas yang ditetapkan ke IAM prinsipal dan menentukan tampilan sebagai. Resource Melakukan hal ini memungkinkan Anda memberikan akses penelusuran melalui satu tampilan ke satu set prinsipal, dan mengakses melalui tampilan yang sama sekali berbeda ke kumpulan prinsip yang berbeda.

Misalnya, untuk memberikan izin ke satu tampilan bernama `ProductionResourcesView` dalam pernyataan IAM kebijakan, pertama-tama dapatkan [nama sumber daya Amazon \(ARN\)](#) dari tampilan tersebut. Anda dapat menggunakan halaman [Tampilan](#) di konsol untuk melihat detail tampilan, atau menjalankan [ListViews](#) operasi untuk mengambil tampilan penuh ARN yang Anda inginkan. Kemudian, sertakan dalam pernyataan kebijakan, seperti yang ditunjukkan dalam contoh berikut yang memberikan izin untuk mengubah 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 pada semua tampilan yang dimiliki oleh akun tertentu, gunakan karakter wildcard (*) di bagian yang relevan dari akun. ARN Contoh berikut memberikan izin pencarian ke semua tampilan di akun AWS Region dan yang ditentukan.

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

Beberapa tindakan `Resource ExplorerCreateView`, seperti, tidak dilakukan terhadap sumber daya tertentu, karena, seperti pada contoh berikut, sumber daya belum ada. Dalam kasus seperti itu, 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 `jalurview/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 Explorer AWS Region 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 tampilan, dan bukan indeks. ARN

Indeks memiliki [ARN](#) yang dapat Anda referensikan dalam kebijakan izin. Indeks Resource Explorer ARN memiliki format berikut.

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

Lihat contoh indeks Resource Explorer berikut 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, [CreateView](#) operasi mengotorisasi terhadap indeks dan tampilan seperti ARN yang akan terjadi setelah Resource Explorer membuatnya. ARN Untuk memberikan izin kepada administrator untuk mengelola layanan Resource Explorer, Anda dapat menggunakan "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 resource Resource Explorer di Wilayah tertentu, Anda dapat menyertakan ARN templat yang cocok dengan indeks dan tampilan, tetapi hanya memanggil satu Wilayah. Dalam contoh berikut, ARN cocok dengan indeks atau tampilan hanya di `us-west-2` Wilayah akun yang ditentukan. Tentukan Wilayah di bidang ketigaARN, tetapi gunakan karakter wildcard (*) di bidang terakhir untuk mencocokkan jenis sumber daya apa pun.

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

Untuk informasi selengkapnya, lihat [Sumber Daya yang Ditentukan oleh Penjelajah Sumber Daya AWS](#) dalam Referensi Otorisasi AWS Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat [Tindakan yang Ditentukan oleh Penjelajah Sumber Daya AWS](#).

Kunci syarat

Resource Explorer tidak menyediakan kunci kondisi khusus layanan apa pun, tetapi mendukung penggunaan beberapa kunci kondisi global. Untuk melihat semua kunci kondisi AWS global, lihat [kunci konteks kondisi AWS global](#) di Panduan IAM Pengguna.

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

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan [operator kondisi](#), misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi AND logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan OR operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Misalnya, Anda dapat memberikan izin IAM pengguna untuk mengakses sumber daya hanya jika ditandai dengan nama IAM pengguna mereka. Untuk informasi selengkapnya, lihat [elemen IAM kebijakan: variabel dan tag](#) di Panduan IAM Pengguna.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat [kunci konteks kondisi AWS global](#) di Panduan IAM Pengguna.

Untuk melihat daftar kunci kondisi yang dapat Anda gunakan dengan Resource Explorer, lihat [Condition Keys untuk Penjelajah Sumber Daya AWS](#) dalam Referensi Otorisasi AWS Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat digunakan untuk menggunakan kunci kondisi, lihat [Tindakan yang Ditentukan oleh Penjelajah Sumber Daya AWS](#).

Contoh

Untuk melihat contoh kebijakan berbasis identitas Resource Explorer, lihat. [Contoh 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 tag, berikan informasi tentang tag di [elemen kondisi](#) dari kebijakan menggunakan kunci kondisi `resource-explorer-2:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`. Untuk informasi selengkapnya tentang menandai resource Resource Explorer, lihat [Menambahkan tag ke tampilan yang sudah ditonton](#). Untuk menggunakan otorisasi berbasis tag di Resource Explorer, lihat. [Menggunakan otorisasi berbasis tanda untuk mengontrol akses ke tampilan Anda](#)

IAM Peran Resource Explorer

[IAM Peran](#) adalah prinsip dalam diri Anda Akun AWS yang memiliki izin khusus.

Menggunakan kredensi sementara dengan Resource Explorer

Anda dapat menggunakan kredensi sementara untuk masuk dengan federasi, mengambil IAM peran, atau untuk mengambil peran lintas akun. Anda memperoleh kredensi keamanan sementara dengan memanggil AWS Security Token Service (AWS STS) API operasi seperti [AssumeRole](#) atau [GetFederationToken](#)

Resource Explorer mendukung penggunaan kredensial sementara.

Peran terkait layanan

[Peran terkait layanan](#) memungkinkan Layanan AWS untuk mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama Anda. Peran terkait layanan muncul di IAM akun Anda dan dimiliki oleh layanan. IAM Administrator dapat melihat tetapi tidak mengedit izin untuk peran terkait layanan.

Resource Explorer menggunakan peran terkait layanan untuk melakukan pekerjaannya. Untuk detail tentang peran terkait layanan Resource Explorer, lihat [Menggunakan 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 menggunakan Konsol Manajemen AWS, AWS Command Line Interface (AWS CLI), atau AWS 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 di AWS IAM Identity Center:

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

- Pengguna yang dikelola dalam IAM melalui penyedia identitas:

Membuat 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 kebijakan AWS terkelola dan beralih ke izin paling sedikit hak istimewa — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang spesifik untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat [kebijakan AWS 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 spesifik Layanan AWS, seperti 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 Akun 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 bernamaAWSResourceExplorerReadOnlyAccess untuk memberikan kemampuan menggunakan konsol Resource Explorer untuk mencari menggunakan tampilan apa pun di akun. Untuk memberikan izin untuk mencari hanya dengan satu tampilan, lihat[Memberikan 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 manaSearch-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 di Konsol Manajemen AWS, prinsipal harus memiliki keduanya `GetView` dan `Search` izin untuk tampilan default di AWS Region 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 di AWS Region 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:ListGroupsWithUser",
        "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 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, lihat [Menggunakan 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 AWS Region 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	Resource Explorer menambahkan izin ke kebijakan peran terkait layanan AWSResour	Desember 12, 2023

Perubahan	Deskripsi	Tanggal
<p>untuk melihat jenis sumber daya tambahan</p>	<p>ceExplorerServiceRolePolicy yang memungkinkan Resource Explorer melihat jenis sumber daya tambahan:</p> <ul style="list-style-type: none"> • <code>apprunner:ListVpcConnectors</code> • <code>backup:ListReportPlans</code> • <code>emr-serverless:ListApplications</code> • <code>events:ListEventBuses</code> • <code>geo:ListPlaceIndexes</code> • <code>geo:ListTrackers</code> • <code>greengrass:ListComponents</code> • <code>greengrass:ListComponentVersions</code> • <code>iot:ListRoleAliases</code> • <code>iottwinmaker:ListComponentTypes</code> • <code>iottwinmaker:ListEntities</code> • <code>iottwinmaker:ListScenes</code> • <code>kafka:ListConfigurations</code> • <code>kms:ListKeys</code> 	

Perubahan	Deskripsi	Tanggal
	<ul style="list-style-type: none"> • kinesisanalytics:ListApplications • lex:ListBots • lex:ListBotAliases • mediapackage-vod:ListPackagingConfigurations • mediapackage-vod:ListPackagingGroups • mq:ListBrokers • personalize:ListDatasetGroups • personalize:ListDatasets • personalize:ListSchemas • route53:ListHealthChecks • route53:ListHostedZones • secretsmanager:ListSecrets 	
Kebijakan terkelola baru	<p>Resource Explorer menambahkan kebijakan AWS terkelola berikut:</p> <ul style="list-style-type: none"> • AWSResourceExplorerOrganizationsAccess 	14 November 2023

Perubahan	Deskripsi	Tanggal
Kebijakan terkelola yang diperbarui	<p>Resource Explorer memperbarui kebijakan AWS terkelola berikut untuk mendukung penelusuran multi-akun:</p> <ul style="list-style-type: none"> • AWSResourceExplorerFullAccess • AWSResourceExplorerReadOnlyAccess 	14 November 2023
<p>AWSResourceExplorerServiceRolePolicy—Kebijakan yang diperbarui untuk mendukung pencarian multi-akun dengan Organizations</p>	<p>Resource Explorer menambahkan izin ke kebijakan peran terkait layanan AWSResourceExplorerServiceRolePolicy yang memungkinkan Resource Explorer mendukung penelusuran multi-akun dengan Organizations:</p> <ul style="list-style-type: none"> • organizations:ListAWSServiceAccessForOrganization • organizations:DescribeAccount • organizations:DescribeOrganization • organizations:ListAccounts • organizations:ListDelegatedAdministrators 	14 November 2023

Perubahan	Deskripsi	Tanggal
<p>AWSResourceExplorerServiceRolePolicy— Kebijakan yang diperbarui untuk mendukung jenis sumber daya tambahan</p>	<p>Resource Explorer menambahkan izin ke kebijakan peran terkait layanan AWSResourceExplorerServiceRolePolicy yang memungkinkan layanan mengindeks jenis sumber daya berikut:</p> <ul style="list-style-type: none"> • accessanalyzer: analyzer • acmpca:sertifikat otoritas • amplify:aplikasi • amplify:backendenvironment • amplify:cabang • amplify:domainasosiasi • amplifyuibuilder:komponen • amplifyuibuilder:tema • appintegration:eventintegration • apprunner:layanan • appstream: appblock • appstream: aplikasi • appstream: armada • appstream: imagebuilder • appstream: tumpukan • appsync:graphqlapi • aps:rulegroupsnamespace • aps:ruang kerja • apigateway:restapi 	<p>17 Oktober 2023</p>

Perubahan	Deskripsi	Tanggal
	<ul style="list-style-type: none"> • apigateway:penyebaran • athena:atacatalog • athena:kelompok kerja • penskalaan otomatis: autoscalinggroup • backup: backupplan • batch: computeenvironment • batch: jobqueue • batch: penjadwalan kebijakan • cloudformation:tumpukan • cloudformation:stackset • cloudfront:fieldlevelencryp tionconfig • cloudfront:fieldlevelencryp tionprofile • cloudfront:originaccesscont rol • cloudtrail: jejak • codeartifact:domain • codeartifact:repositori • kodekomit: repositori • codeguruprofiler:profilingg roup • codestarconnection s:koneksi • databrew: dataset • databrew: resep • databrew: aturan • detektif: grafik 	

Perubahan	Deskripsi	Tanggal
	<ul style="list-style-type: none"> • layanan direktori:direktori • ec2:carriergateway • ec2: verifiedaccessendpoint • ec2: verifiedaccessgroup • ec2:verifiedaccessinstance • ec2: verifiedaccesstrustprovider • ecr: repositori • elasticache:cachesecuritygroup • elasticfilesystem:accesspoint • acara:aturan • terbukti:percobaan • jelas:fitur • terbukti:peluncuran • terbukti:proyek • ruang sirip: lingkungan • firehose:deliverystream • faultinjectionsimulator:experimenttemplate • perkiraan:datasetgroup • prakiraan: dataset • detektor penipu: detektor • penipu detektor: entitytype • penipu detektor: eventtype • pendeteksi penipu: label • pendeteksi penipu: hasil • pendeteksi penipu: variabel • gamelift:alias 	

Perubahan	Deskripsi	Tanggal
	<ul style="list-style-type: none"> • globalaccelerator: akselerator • globalaccelerator: endpointgroup • globalaccelerator: pendengar • lem: database • lem: pekerjaan • lem: meja • lem: pemicu • greengrass:kelompok • healthlake:thirddatastore • iam:virtualmfadvice • imagebuilder:componentbuildversion • imagebuilder:komponen • imagebuilder:containerrecipe • imagebuilder:distributionconfiguration • imagebuilder:imagebuildversion • imagebuilder:imagepipeline • imagebuilder:imagerecipe • imagebuilder:gambar • imagebuilder:infrastrukturonfigurasi • iot: otorisasi • IOT: JobTemplate • IOT: mitigasiaksi 	

Perubahan	Deskripsi	Tanggal
	<ul style="list-style-type: none"> • iot: provisioningtemplate • iot: profil keamanan • IOT: hal • iot:topikruledestinas • iotanalitik: saluran • iotanalitik: dataset • iotanalitik: datastore • iotanalitik: pipa • iotevents:alarmmodel • iotevents:detectormodel • iotevents:masukan • iotsitewisewise:model aset • iotsitewisewise:aset • iotsitewisewise:gateway • iottwinmaker: ruang kerja • iv:saluran • iv:streamkey • kafka:cluster • kinesisvideo:aliran • lambda:alias • lambda: layerversion • lambda: lapisan • lookoutmetrics:alert • lookoutvision:proyek • mediapackage:saluran • mediapackage:origi nendpoint • mediatailor:konfigurasi pemutaran 	

Perubahan	Deskripsi	Tanggal
	<ul style="list-style-type: none"> • memoridb: acl • memorydb: cluster • memorydb: parametergroup • memorydb: pengguna • penargetan mobile:aplikasi • penargetan mobile:segmen • Penargetan Mobilet:T emplate • networkfirewall:firewallpolicy • networkfirewall:firewall • manajer jaringan: globalnet work • manajer jaringan: perangkat • manajer jaringan:tautan • manajer jaringan: lampiran • manajer jaringan: corenetwo rk • panorama:paket • qldb:jurnalkinesisstreamsfo rledger • qldb: buku besar • rds:bluegreendeployment • refactorospace: aplikasi • refactorospace: lingkungan • refactorospace: rute • refactorospace: layanan • rekognisi: proyek • resiliencehub: aplikasi • resiliencehub:resiliencypol icy 	

Perubahan	Deskripsi	Tanggal
	<ul style="list-style-type: none">• kumpulan sumber daya:kelopok• route53:recoverygroup• route53:resourceset• route53:firewalldomain• route53:firewallrulegroup• route53:resolverendpoint• route53:resolVERRule• pembuat sagemaker:model• pembuat sagemaker:notebookinstance• penandatanganan:signingprofile• ssm:incidents:responseplan• ssm:inventoryentry• ssm:resourcedatasync• negara bagian:aktivitas• aliran waktu:database• kebijaksanaan: asisten• kebijaksanaan: asisten asosiasi• kebijaksanaan:pengetahuan	

Perubahan	Deskripsi	Tanggal
<p>AWSResourceExplorerServiceRolePolicy— Kebijakan yang diperbarui untuk mendukung jenis sumber daya tambahan</p>	<p>Resource Explorer menambahkan izin ke kebijakan peran terkait layanan AWSResourceExplorerServiceRolePolicy yang memungkinkan layanan mengindeks jenis sumber daya berikut:</p> <ul style="list-style-type: none">• codebuild: proyek• codepipeline:pipa• cognito:identitypool• cognito:userpool• ecr: repositori• efs:sistem file• elasticbeanstalk:aplikasi• elasticbeanstalk:applicationversion• elasticbeanstalk:lingkungan• iot: kebijakan• iot: topicrule• langkah-langkah:statefulmachine• s3: ember	1 Agustus 2023

Perubahan	Deskripsi	Tanggal
<p>AWSResourceExplorerServiceRolePolicy— Kebijakan yang diperbarui untuk mendukung jenis sumber daya tambahan</p>	<p>Resource Explorer menambahkan izin ke kebijakan peran terkait layanan AWSResourceExplorerServiceRolePolicy yang memungkinkan layanan mengindeks jenis sumber daya berikut:</p> <ul style="list-style-type: none">• elastisis:cluster• elasticache:globalreplikatingroup• elasticache:parametergroup• elasticache:replikasi grup• elasticache:reserved-instance• elastisis:snapshot• elasticache:subnetgroup• elastis: pengguna• elasticache:usergroup• lambda: konfigurasi penandatanganan kode• lambda: pemetaan sumber-acara• sqs:antrian	7 Maret 2023

Perubahan	Deskripsi	Tanggal
Kebijakan terkelola baru	Resource Explorer menambahkan kebijakan AWS terkelola berikut: <ul style="list-style-type: none"> • AWSResourceExplorerFullAccess • AWSResourceExplorerReadOnlyAccess • 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 [terkait layanan](#). Peran terkait layanan adalah jenis peran unik yang ditautkan langsung ke Resource Explorer. IAM 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 ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat ditetapkan ke entitas lain mana pun. IAM

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat [AWS layanan yang berfungsi IAM](#) di IAMPanduan Pengguna. Di sana, cari layanan yang memiliki Ya di kolom Peran terkait layanan. Pilih Ya bersama 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 IAM konsol.

Principal adalah IAM entitas 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, lihat [Izin peran terkait layanan di Panduan Pengguna](#). IAM

Membuat peran terkait layanan untuk Resource Explorer

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda mengaktifkan Resource Explorer di Konsol Manajemen AWS, atau menjalankan [CreateIndex](#) yang pertama AWS Region 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 [RegisterResourceExplorer](#) berada 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 mengedit deskripsi peran menggunakan IAM. Untuk informasi selengkapnya, lihat [Mengedit peran terkait layanan](#) di IAMPanduan Pengguna.

Menghapus peran terkait layanan untuk Resource Explorer

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

Gunakan IAM konsol, AWS CLI, atau AWS API untuk menghapus peran `AWSServiceRoleForResourceExplorer` terkait layanan. Untuk informasi selengkapnya, lihat [Menghapus peran terkait layanan di 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, silakan lihat [titik akhir Layanan AWS](#) di Referensi Umum Amazon Web Services.

Izin pemecahan masalah Penjelajah Sumber Daya AWS

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

Topik

- [Saya tidak berwenang untuk melakukan tindakan di Resource Explorer](#)
- [Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Resource Explorer saya](#)

Saya tidak berwenang untuk melakukan tindakan di Resource Explorer

Jika Konsol Manajemen AWS memberitahu Anda bahwa Anda tidak berwenang untuk melakukan tindakan, maka Anda harus menghubungi administrator Anda untuk bantuan. Administrator Anda adalah orang yang memberi Anda kredensi yang Anda gunakan untuk mencoba operasi ini.

Misalnya, kesalahan berikut terjadi ketika seseorang mengasumsikan peran IAM `MyExampleRole` mencoba menggunakan konsol untuk melihat detail tentang 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 untuk memperbarui kebijakan izin peran untuk mengizinkan akses ke tampilan menggunakan `resource-explorer-2:GetView` tindakan.

Saya ingin mengizinkan orang di luar saya Akun AWS untuk mengakses sumber daya Resource Explorer saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja 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 orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mempelajari apakah Resource Explorer mendukung fitur ini, lihat [Bagaimana Resource Explorer bekerja dengan IAM](#).

- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat [Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki](#) di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat [Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat [Menyediakan akses ke pengguna terautentikasi eksternal \(federasi identitas\)](#) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM](#).

Perlindungan data di Penjelajah Sumber Daya AWS

[Model tanggung jawab AWS bersama model](#) berlaku untuk perlindungan data di Penjelajah Sumber Daya AWS. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat [Privasi Data FAQ](#). Untuk informasi tentang perlindungan data di Eropa, lihat [Model Tanggung Jawab AWS Bersama dan](#) posting GDPR blog di Blog AWS Keamanan.

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

- Gunakan otentikasi multi-faktor (MFA) dengan setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat [Bekerja dengan CloudTrail jejak](#) di AWS CloudTrail Panduan Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.

- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan FIPS 140-3 modul kriptografi yang divalidasi saat mengakses AWS melalui antarmuka baris perintah atau, gunakan titik akhir. API FIPS Untuk informasi selengkapnya tentang FIPS titik akhir yang tersedia, lihat [Federal Information Processing Standard \(FIPS\) 140-3](#).

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Resource Explorer atau lainnya Layanan AWS menggunakan konsol, API, AWS CLI, atau AWS SDKs. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Jika Anda memberikan URL ke server eksternal, kami sangat menyarankan agar Anda tidak menyertakan informasi kredensial dalam URL untuk memvalidasi permintaan Anda ke server tersebut.

Enkripsi diam

Data yang disimpan oleh Resource Explorer mencakup daftar sumber daya yang diindeks dan yang terkait ARNs 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 \(\) dengan kunci 256-bit \(-256-GCM\)](#). AES GCM

Enkripsi bergerak

Permintaan pelanggan dan semua data terkait dienkripsi dalam perjalanan menggunakan [Transport Layer 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 AWS titik 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 AWS di 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. AWS menyediakan 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 CSPM](#) – 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

Infrastruktur AWS global dibangun di sekitar Wilayah 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 di Penjelajah Sumber Daya AWS

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

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

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

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

Untuk informasi selengkapnya tentang prosedur keamanan jaringan AWS global, lihat [whitepaper Amazon Web Services: Ikhtisar Proses Keamanan](#).

Penjelajah Sumber Daya AWS Pemantauan

Pemantauan adalah bagian penting dari pemeliharaan keandalan, ketersediaan, dan kinerja Penjelajah Sumber Daya AWS dan AWS solusi Anda yang lain. AWS menyediakan 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 AWS terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau Layanan 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 [Panduan AWS CloudTrail Pengguna](#).

Informasi Resource Explorer di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Ketika aktivitas terjadi di Penjelajah Sumber, aktivitas tersebut dicatat dalam CloudTrail peristiwa bersama Layanan 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](#)
- [AWSintegrasikan 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 keCreateIndex,DeleteIndex, danUpdateIndex 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.
- Kredensyal 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": "AROEXAMPLEEXAMPLE:botocore-session-166EXAMPLE",
    "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-session-166EXAMPLE",
    "accountId": "123456789012",
```

```

    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROEXAMPLEEXAMPLE",
        "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": "AROEXAMPLEEXAMPLE: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": "AROEXAMPLEEXAMPLE",
        "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": "AROEXAMPLEEXAMPLE:botocore-session-1661282039",
    "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROEXAMPLEEXAMPLE",
        "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": "AROEXAMPLEEXAMPLE:botocore-session-1661282039",
    "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-session-1661282039",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROEXAMPLEEXAMPLE",
        "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": "AROEXAMPLEEXAMPLE:botocore-session-1661282039",
    "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-session-1661282039",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROEXAMPLEEXAMPLE",
        "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 sama AWS Region.

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": "AROEXAMPLEEXAMPLE:botocore-session-1661282039",
    "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROEXAMPLEEXAMPLE",

```

```

        "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"
}
```

Pemecahan Masalah Explorer Sumber Daya Explorer

Jika Anda mengalami masalah saat bekerja dengan Resource Explorer, konsultasikan topik tersebut di bagian ini. Lihat juga [izin pemecahan masalah Penjelajah Sumber Daya AWS](#) 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 tertentu AWS Region. 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 diKonsol Manajemen AWS](#) memungkinkan prinsipal mencari dari halaman manapun di halamanKonsol Manajemen AWS. 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)

Kebijakan AWS terkelola berikut ini mencakup izin untuk menelepon `resource-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 mengonfigurasi Penjelajah 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 izin AWS 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 di AWS IAM Identity Center:

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

- Pengguna yang dikelola dalam IAM melalui penyedia identitas:

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

- Pengguna IAM:

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

Kebijakan harus mengizinkan yang diminta `Action` pada `Resource` 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 kredensial 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 dengan AWS 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?](#)
- [Mengapa sumber daya saya tidak muncul di hasil penelusuran terpadu di konsol?](#)
- [Mengapa pencarian terpadu di konsol dan Resource Explorer terkadang memberikan hasil yang berbeda?](#)
- [Izin apa yang saya perlukan untuk dapat mencari sumber daya?](#)

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 awalnya AWS Region, 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 disebarikan 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, lihat [Filter](#).

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](#).

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 Konsol Manajemen AWS 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 (IAMperan dan pengguna) 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 Konsol Manajemen AWS 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 IAM kepala sekolah 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.

Kuota untuk Resource Explorer

Anda Akun AWS memiliki kuota default untuk masing-masing Layanan AWS. Kecuali dinyatakan lain, kuota bersifat khusus per Wilayah. Anda dapat meminta peningkatan untuk beberapa kuota dan kuota lainnya tidak dapat ditingkatkan.

Untuk melihat kuota Penjelajah Sumber Daya AWS, buka [konsol Service Quotas](#). Di panel navigasi, pilih Layanan AWS dan 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 dalam AWS Region	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 (SDKs) tersedia untuk banyak bahasa pemrograman populer. Masing-masing SDK menyediakan API, contoh kode, dan dokumentasi yang memudahkan pengembang untuk membangun aplikasi dalam bahasa pilihan mereka.

SDK dokumentasi	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 for SAP ABAP	AWS SDK for 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 pemberitahuan tentang pembaruan dokumentasi ini, Anda dapat berlangganan RSS umpan.

Perubahan	Deskripsi	Tanggal
Filter pencarian baru ditambahkan	Resource Explorer menambahkan filter kueri <code>tag:all</code> penelusuran baru, memungkinkan Anda untuk mencari sumber daya yang memiliki satu atau beberapa tag buatan pengguna yang dilampirkan, bahkan jika jenis sumber daya tidak didukung di Resource Explorer.	September 6, 2024
Perbaikan organisasi konten	Judul topik yang diperbarui dan konten yang direorganisasi untuk meningkatkan keterbacaan dan kemampuan ditemukan.	Agustus 29, 2024
Pemberitahuan untuk meningkatkan IAM kebijakan ke IPv6	Pelanggan yang menggunakan pengalamatan ganda dengan ASPEN kebijakan yang mengandung <code>aws:sourceIp</code> dipengaruhi oleh peningkatan ini. Pengalamatan ganda berarti bahwa jaringan mendukung keduanya IPv4 dan IPv6.	Juli 15, 2024

Dukungan yang dihentikan untuk tiga jenis sumber daya	Resource Explorer menghentikan dukungan untuk tiga jenis sumber daya berikut: <code>ecs:task</code> , <code>ssm:automation-execution</code> , dan <code>ssm:patchbaseline</code> .	9 Juli 2024
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 baru dari Layanan AWS termasuk CloudFormation AWS Glue,, dan Amazon SageMaker.

15 November 2023

[Resource Explorer mendukung pencarian multi-akun](#)

Sekarang Anda dapat menggunakan Resource Explorer untuk mencari dan menemukan sumber daya di Akun AWS dalam organisasi atau unit organisasi Anda. Untuk informasi selengkapnya, lihat [Mengaktifkan pencarian 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 didelegasikan.

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 organisasi, 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 masuk BAH dan sekarang CGK 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 Functions Kebijakan 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 [mengeksport hasil pencarian Anda](#) di halaman pencarian Sumber Daya ke file yang CSV diformat.

4 April 2023

[Gunakan Amazon Q Developer dalam aplikasi obrolan untuk mencari dan menemukan AWS sumber daya Anda](#)

Anda sekarang dapat menggunakan Amazon Q Developer dalam aplikasi obrolan untuk mencari sumber daya Anda menggunakan pertanyaan bahasa alami. Untuk informasi selengkapnya, lihat [Menggunakan Amazon Q Developer dalam aplikasi obrolan 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 (AmazonSQS). [Kebijakan AWS terkelola](#) yang memberikan akses Resource Explorer ke sumber daya indeks diperbarui untuk menyertakan jenis sumber daya baru tersebut.

7 Maret 2023

IAM pembaruan praktik terbaik	Panduan yang diperbarui untuk menyelaraskan dengan praktik IAM terbaik. Untuk informasi selengkapnya, lihat Praktik terbaik keamanan di IAM .	6 Desember 2022
Kebijakan AWS terkelola baru	Resource Explorer menambahkan <code>AWSResourceExplorerFullAccess</code> , <code>AWSResourceExplorerReadOnlyAccess</code> , dan <code>AWSResourceExplorerServiceRolePolicy</code> 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.