aws

Guida per l'utente

Esploratore di risorse AWS

Esploratore di risorse AWS: Guida per l'utente

Table of Contents

Resource Explorer 1
Utente per la prima volta 1
Caratteristiche di Resource Explorer 2
Servizi correlati 2
Accesso a Resource Explor 3
Prezzi 5
Nozioni di base 6
Termini e concetti 6
amministratore Resource Explorer 8
Utente Resource Explorer 9
Indice 10
Vista 11
Risorsa 13
Ricerca unificata in AWS Management Console 14
Ricerca su più account 15
Prerequisiti 15
Registrati per un Account AWS 15
Crea un utente con accesso amministrativo 16
Configurazione di Resource Explorer 17
Configurazione rapida 18
Configurazione avanzata 20
Gestione delle risorse di Explorer 25
Controllo delle regioni 25
Verifica dello stato di Resource Explorer in una regione 26
Attivazione della ricerca su più account 27
Prerequisiti 27
Abilita la ricerca su più account 28
Configurazione rapida per più account 28
Attivazione 29
Creare un indice Resource Explorer in una regione 30
Informazioni sulle regioni che aderiscono 33
Comportamenti di opt-out 33
Attivazione della ricerca tra aree geografiche 34
Informazioni sull'indice degli aggregatori 34

Creazione dell'indice aggregatore ... 36
Ridurre di livello l'indice dell'aggregatore ... 37
Supporta la ricerca unificata da console ... 39
Effetto delle azioni dell'account sulla ricerca tra più account ... 40
Resource Explorer è ... 40
L'account del membro viene rimosso da un'organizzazione ... 41
L'account è sospeso ... 41
L'account è chiuso ... 41
Disattivazione dell'account ... 42
Disattivarne uno Regione AWS ... 42
Disattivazione di tuttoRegioni AWS ... 44
Disattiva Resource Explorer in tuttoRegioni AWS ... 45
Distribuzione in un'organizzazione ... 47
Prerequisiti ... 48
Creazione dei set di stack per Resource Explorer ... 48
Modelli di esempio AWS CloudFormation ... 49
Gestione delle visualizzazioni ... 53
Informazioni sulle visualizzazioni ... 54
Visualizzazioni predefinite ... 56
Creazione di visualizzazioni ... 56
Concedere l'accesso alle visualizzazioni ... 61
Utilizzo dell'autorizzazione basata sui tag per controllare l'accesso alle visualizzazioni ... 63
Impostazione della ... 64
Etichettatura delle visualizzazioni ... 65
Aggiungi tag alle tue visualizzazioni ... 66
Controllo delle autorizzazioni tramite tag ... 67
Riferimenti ai tag in una politica ABAC ... 67
Condivisione delle visualizzazioni ... 68
Politica di autorizzazione con cui condividere la visualizzazione Account AWS ... 69
Eliminazione delle viste ... 71
Alla ricerca di risorse ... 73
Esporta i risultati della ricerca in un file.csv ... 76
Sintassi delle query di ricerca ... 77
Come funzionano le interrogazioni in Resource Explorer ... 77
Sintassi della stringa di query ... 77
Nozioni di base ... 78

Filtri 78
Operatori di filtro 82
Query di esempio 86
Risorse senza tag 86
Risorse con tag 87
Aggiunta di tag 87
Aggiunta di tag non validi 87
Sottoinsieme di regioni 88
Risorse globali 88
Più filtri 88
Uso delle virgolette per termini composti da più parole 89
AWS CloudFormationmembri dello stack 89
Ricerca unificata 90
Verifica se la ricerca unificata è abilitata 91
Attivazione della ricerca unificata 91
Uso di AWS Chatbot 92
AWSdomande sulle risorse 92
Prerequisiti 92
Domande frequenti sulle risorse 92
Sicurezza 93
Gestione dell'identità e degli accessi 94
Destinatari 94
Autenticazione con identità 95
Gestione dell'accesso con policy 98
Resource Explorer e IAM 101
Esempi di policy basate su identità 108
SCP di esempio 113
AWS politiche gestite 115
Uso di ruoli collegati ai servizi 133
uzione uzione uzione uzione uzione uzione uzione 135
Protezione dei dati 137
Crittografia dei dati a riposo 138
Crittografia in transito 138
Convalida della conformità 138
Resilienza 139
Sicurezza dell'infrastruttura 139

Monitoraggio 141
CloudTrail registri 141
Informazioni su Resource Explorer in CloudTrail 141
Informazioni sulle voci del log di Resource Explorer Explorer 143
Utilizzo di CloudFormation 153
Resource Explorer e CloudFormation modelli 153
Ulteriori informazioni su AWS CloudFormation 156
Risoluzione dei problemi 157
Problemi generali 157
In un collegamento a Resource Explorer manca ilRegione AWS 157
CloudTrail Errori di ricerca unificati 158
Problemi di configurazione 159
Messaggio accesso rifiutato quando effettua una richiesta a Resource Explorer 159
Visualizzo un messaggio di accesso negato quando effettuo una richiesta con credenziali di sicurezza provvisorie. 160
Problemi di ricerca 161
Perché mancano alcune risorse nei risultati di ricerca di Resource Explorer? 161
Perché le mie risorse non vengono visualizzate nei risultati di ricerca unificati della console? 164
Perché la ricerca unificata nella console e in Resource Explorer a volte dà risultati diversi? . 164
Di quali autorizzazioni ho bisogno per poter cercare risorse? 164
Tipi di risorse supportati 166
Servizi e tipi di risorse supportati 166
Amazon API Gateway 169
AWS App Runner 170
Amazon AppStream 2.0 170
AWS AppSync 170
Amazon Athena 170
AWS Backup 170
AWS Batch 170
AWS CloudFormation 170
Amazon CloudFront 171
AWS CloudTrail 171
Amazon CloudWatch 171
Amazon CloudWatch evidentemente 171
CloudWatch Registri Amazon 172

AWS CodeArtifact 172
AWS CodeBuild 172
AWS CodeCommit 172
Amazon CodeGuru Profiler 172
AWS CodePipeline 172
AWS CodeConnections 172
Amazon Cognito 172
Amazon Connect 173
Amazon Connect Wisdom 173
Amazon Detective 173
Amazon DynamoDB 173
EC2 Image Builder 173
Amazon ECR 173
AWS Elastic Beanstalk 174
Amazon ElastiCache 174
Amazon Elastic Compute Cloud (Amazon EC2) 174
Amazon Elastic Container Registry 176
Amazon Elastic Container Service 176
Amazon Elastic File System 177
Sistema di bilanciamento del carico elastico 177
AWS Elemental MediaPackage 177
AWS Elemental MediaTailor 177
Amazon EMR Serverless 178
Amazon EventBridge 178
AWS Fault Injection Service 178
Amazon Forecast 178
Amazon Fraud Detector 178
Amazon GameLift 178
AWS Global Accelerator 179
AWS Glue 179
AWS Glue DataBrew 179
AWS Identity and Access Management 179
Amazon Interactive Video Service 180
AWS IoT 180
AWS IoT Analytics 180
AWS IoT Events 180

AWS IoT Greengrass Version 1 181
AWS IoT SiteWise 181
AWS IoT TwinMaker 181
AWS Key Management Service 181
Amazon Kinesis 181
Amazon Data Firehose 181
Flusso di video Amazon Kinesis 181
AWS Lambda 182
Amazon Lex 182
Servizio di posizione Amazon 182
Amazon Lookout per le metriche 182
Amazon Lookout per Vision 182
Servizio gestito da Amazon per Apache Flink 182
Amazon Managed Service per Prometheus 182
Amazon Managed Service per Prometheus 183
Amazon Managed Streaming per Apache Kafka 183
AWS Migration Hub Refactor Spaces 183
AWS Network Firewall 183
AWS Network Manager 183
OpenSearch Servizio Amazon 183
AWS Panorama 184
Amazon Personalize 184
AWS Private Certificate Authority 184
Amazon QLDB 184
Amazon Redshift 184
Amazon Rekognition 184
Amazon Relational Database Service (Amazon RDS) 185
AWS Resilience Hub 185
AWS Resource Groups 185
Esploratore di risorse AWS 185
Amazon Route 53 186
Preparazione al ripristino di Amazon Route 53 186
Amazon Route 53 Resolver 186
Amazon SageMaker 186
AWS Secrets Manager 186
AWS Service Catalog 186

Amazon Simple Notification Service 187
Amazon Simple Queue Service 187
Amazon Simple Storage Service (Amazon S3) 187
AWS Step Functions 187
AWS Systems Manager 187
Accesso verificato da AWS 188
AWS Wavelength 188
Accesso programmatico all'elenco dei tipi di risorse supportati 188
Tipi di risorse che appaiono come altri tipi 189
Quote 191
Lavorare con AWS gli SDK 192
Cronologia dei documenti 194
..... cxcix

Cos'è Esploratore di risorse AWS?

Esploratore di risorse AWS è un servizio di ricerca e rilevamento di risorse. Con Resource Explorer, puoi esplorare le tue risorse, come istanze Amazon Elastic Compute Cloud, flussi Amazon Kinesis o tabelle Amazon DynamoDB, utilizzando un'esperienza simile a quella dei motori di ricerca Internet. Puoi cercare le tue risorse utilizzando metadati di risorse come nomi, tag e ID. Resource Explorer funziona Regioni AWS all'interno del tuo account per semplificare i carichi di lavoro interregionali.

Resource Explorer fornisce risposte rapide alle query di ricerca utilizzando indici creati e gestiti dal servizio. Esploratore di risorse AWS Resource Explorer utilizza una varietà di fonti di dati per raccogliere informazioni sulle risorse del tuo. Account AWS Resource Explorer memorizza tali informazioni negli indici per consentire la ricerca in Resource Explorer.

> **Desideriamo il tuo feedback su questa documentazione**
>
> Il nostro obiettivo è aiutarti a ottenere tutto ciò che puoi da Resource Explorer. Se questa guida ti aiuta a farlo, faccelo sapere. Se la guida non ti aiuta, vorremmo sentire la tua opinione per risolvere il problema. Usa il link Feedback che si trova nell'angolo in alto a destra di ogni pagina. In questo modo i tuoi commenti verranno inviati direttamente agli autori di questa guida. Esaminiamo ogni invio, alla ricerca di opportunità per migliorare la documentazione. Grazie in anticipo per il tuo aiuto!

Argomenti

- Sei un utente di Resource Explorer per la prima volta?
- Caratteristiche di Resource Explorer
- Servizi AWS correlati
- Accesso a Resource Explor
- Prezzi

Sei un utente di Resource Explorer per la prima volta?

Se sei un utente alle prime armi di Resource Explorer, ti consigliamo di iniziare leggendo i seguenti argomenti nella sezione Guida introduttiva:

- Termini e concetti per Resource Explorer
- Configurazione di Resource Explorer utilizzando la configurazione rapida

Caratteristiche di Resource Explorer

Resource Explorer offre le seguenti funzionalità:

- Gli utenti possono cercare risorse nella propria regione Regione AWS o in più regioni del proprioAccount AWS.
- Gli utenti possono utilizzare parole chiave, operatori di ricerca e attributi come i tag per filtrare i risultati della ricerca solo in base alle risorse corrispondenti.
- Quando gli utenti trovano una risorsa nei risultati di ricerca, possono accedere immediatamente alla console nativa della risorsa per utilizzarla.
- Gli amministratori possono creare viste che definiscono quali risorse sono disponibili nei risultati di ricerca. Gli amministratori possono creare visualizzazioni diverse per diversi gruppi di utenti in base alle loro attività e concedere le autorizzazioni per le visualizzazioni solo agli utenti che ne hanno bisogno.
- Resource Explorer, come molti altriServizi AWS, alla fine è coerente. Resource Explorer raggiunge un'elevata disponibilità replicando i dati su più server all'interno dei data center Amazon in tutto il mondo. Se una richiesta per modificare alcuni dati ha successo, la modifica viene completata e memorizzata in maniera sicura. Tuttavia, la modifica deve essere replicata su Resource Explorer, operazione che può richiedere del tempo. Ad esempio, ciò include Resource Explorer che trova una risorsa in una regione e la replica nella regione che contiene l'indice di aggregazione per l'account.

Servizi AWS correlati

I seguenti sono gli altri il Servizi AWS cui scopo principale è aiutarti a gestire le tue AWS risorse:

AWS Resource Access Manager (AWS RAM)

Condividete le risorse l'una Account AWS con l'altraAccount AWS. Se il tuo account è gestito daAWS Organizations, puoi AWS RAM utilizzarlo per condividere le risorse con gli account di un'unità organizzativa o con tutti gli account dell'organizzazione. Le risorse condivise funzionano per gli utenti di tali account proprio come se fossero state create nell'account locale.

AWS Resource Groups

Crea gruppi per AWS le tue risorse. Quindi, puoi utilizzare e gestire ogni gruppo come un'unità invece di dover fare riferimento a ogni risorsa singolarmente. I tuoi gruppi possono essere costituiti da risorse che fanno parte dello stesso AWS CloudFormation stack o che sono etichettate con gli stessi tag. Alcuni tipi di risorse supportano anche l'applicazione di una configurazione a un gruppo di risorse per influire su tutte le risorse pertinenti di quel gruppo.

L'editor di tag e il AWS Resource Groups Tagging API

I tag sono metadati definiti dal cliente che puoi allegare alle tue risorse. Puoi classificare le tue risorse per scopi quali l'allocazione dei costi e il controllo degli accessi basato sugli attributi.

Accesso a Resource Explor

È possibile interagire con Resource Explorer nei seguenti modi:

console Resource Explorer

Resource Explorer fornisce un'interfaccia utente basata sul Web, la console Resource Explorer. Se ti sei registrato aAccount AWS, puoi accedere alla console Resource Explorer accedendo AWS Management Consolee scegliendo Resource Explorer dalla home page della console.

Nel browser puoi anche accedere direttamente alla pagina della dashboard di Resource Explorer o alla pagina di ricerca delle risorse. Se non hai già effettuato l'accesso, ti verrà chiesto di farlo prima che venga visualizzata la console.

> **Note**
>
> La console Resource Explorer è una console globale, il che significa che non devi Regione AWS selezionarne una su cui lavorare. Tuttavia, quando si utilizza Resource Explorer per creare un indice o una vista, è necessario specificare in quale regione è archiviato l'indice o la vista. Quando si utilizza Resource Explorer per la ricerca, è possibile scegliere qualsiasi visualizzazione a cui si ha accesso. I risultati provengono automaticamente dalla regione associata alla vista selezionata. Se la vista proviene dalla regione che contiene l'indice dell'aggregatore, i risultati includono le risorse di tutte le regioni in cui sono stati creati gli indici di Resource Explorer.

AWS Management Consolericerca unificata

Nella parte superiore di ogni pagina diAWS Management Console, c'è una barra di ricerca. È possibile configurare Resource Explorer per partecipare alla ricerca unificata. Gli utenti possono quindi utilizzare la sintassi delle query di ricerca di Resource Explorer nella casella di testo di ricerca unificata e visualizzare le risorse corrispondenti nei risultati di ricerca. Attivando questa funzionalità, gli utenti possono cercare risorse dalla console di qualsiasi dispositivo Servizio AWS senza dover prima passare alla console Resource Explorer.

> **Important**
>
> La ricerca unificata esegue sempre la ricerca utilizzando la visualizzazione predefinita nell'indice dell'aggregatore Regione AWS che contiene l'indice dell'aggregatore.

Comandi Resource Explorer in AWS CLI and Tools per Windows PowerShell

Gli strumenti AWS CLI and PowerShell forniscono l'accesso diretto alle operazioni dell'API pubblica di Resource Explorer. Questi strumenti funzionano su Windows, macOS e Linux. Per ulteriori informazioni su come iniziare, consulta la Guida per l'AWS Command Line Interfaceutente o la Guida per l'AWS Tools for Windows PowerShellutente. Per ulteriori informazioni sui comandi per Resource Explorer, vedere AWS CLICommand Reference o AWS Tools for Windows PowerShellCmdlet Reference.

Operazioni di Resource Explorer negli SDK AWS

AWSfornisce comandi API per un'ampia gamma di linguaggi di programmazione. Per ulteriori informazioni sulle nozioni di base, consulta Utilizzo Esploratore di risorse AWS con un SDK AWS.

API della query

Se non utilizzi uno dei linguaggi di programmazione supportati, l'API HTTPS Query di Resource Explorer ti offre l'accesso programmatico a Resource Explorer. Con l'API Resource Explorer, puoi inviare richieste HTTPS direttamente al servizio. Quando utilizzi l'API Resource Explorer, devi includere codice in grado di firmare digitalmente le tue richieste utilizzando le tue AWS credenziali. Per ulteriori informazioni, consulta la Documentazione di riferimento delle API di Esploratore di risorse AWS.

Prezzi

La ricerca di risorse mediante utilizzoEsploratore di risorse AWS, tra cui la creazione di viste, l'attivazione delle regioni o la ricerca di risorse, è gratuita. Nel processo di creazione dell'inventario delle risorse, Resource Explorer richiama le API per conto dell'utente, il che può comportare addebiti. L'interazione con le risorse che trovi nei risultati di ricerca può comportare costi di utilizzo che variano a seconda del tipo e del tipo di risorsa. Servizio AWS Per ulteriori informazioni su come AWS fatturare l'uso normale di un tipo di risorsa specifico, consulta la documentazione relativa al servizio proprietario di quel tipo di risorsa.

Guida introduttiva a Resource Explorer

Utilizza gli argomenti di questa sezione per acquisire una conoscenza di base dei concetti e dei termini utilizzati daEsploratore di risorse AWS. Scopri i prerequisiti che devi soddisfare per utilizzare correttamente Resource Explorer e come attivare Resource Explorer nel tuoAccount AWS.

Argomenti

- Termini e concetti per Resource Explorer
- Prerequisiti per utilizzare Resource Explorer
- Impostazione e configurazione di Resource Explorer

Termini e concetti per Resource Explorer

Esploratore di risorse AWS è un servizio di ricerca e rilevamento di risorse. Con Resource Explorer, puoi esplorare le tue risorse utilizzando un'esperienza simile a quella dei motori di ricerca su Internet. Puoi cercare le tue risorse, come istanze Amazon Elastic Compute Cloud, flussi Amazon Kinesis o tabelle Amazon DynamoDB utilizzando metadati di risorse come nomi, tag e ID. Resource Explorer funziona all'interno del tuo account per semplificare i carichi Regioni AWS di lavoro tra le regioni.

Resource Explorer fornisce risposte rapide alle query di ricerca utilizzando indici creati e gestiti dal servizio. Esploratore di risorse AWS Resource Explorer utilizza una varietà di fonti di dati per raccogliere informazioni sulle risorse del tuo. Account AWS Resource Explorer memorizza tali informazioni negli indici per consentire la ricerca in Resource Explorer.

È necessario comprendere i seguenti concetti per amministrare e configurare correttamente Esploratore di risorse AWS gli utenti.

Concetti

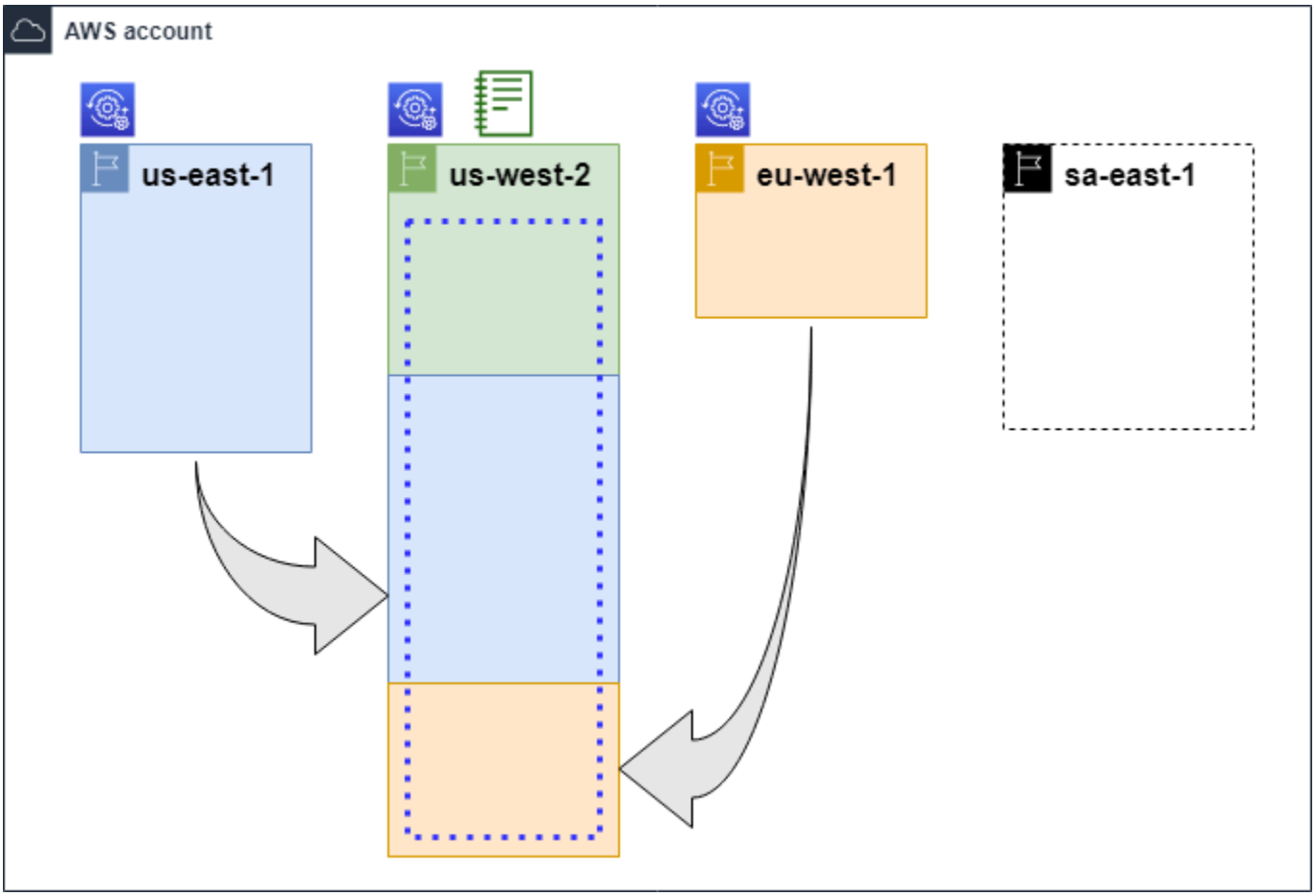
- amministratore Resource Explorer
- Utente Resource Explorer
- Indice
- Vista
- Risorsa
- Ricerca unificata in AWS Management Console

- Ricerca su più account

Il diagramma seguente mostra tre aree Regioni AWS in cui l'amministratore ha attivato Resource Explorer e una regione che l'amministratore ha scelto di non attivare. La regione in cui Resource Explorer non è attivato non ha un indice. Pertanto, le sue risorse non possono essere ricercate tramite le query di Resource Explorer.

In questo scenario di esempio, l'amministratore ha scelto la regione degli Stati Uniti occidentali (Oregon) (`us-west-2`) per contenere l'indice di aggregazione per l'account. Tutte le regioni attivate replicano i rispettivi indici locali nella regione con l'indice di aggregazione.

La visualizzazione predefinita creata da Resource Explorer non ha filtri. Pertanto, i risultati della ricerca con questa visualizzazione possono includere risorse di qualsiasi tipo in tutte le regioni dell'account in cui è attivato Resource Explorer.



Legenda

	In questo caso, Resource Explorer è attivato Regione AWS e le informazioni sulle risorse della regione sono archiviate in un indice locale di quella regione. L'indice locale di ogni regione viene inoltre replicato (indicato dalle frecce) nella regione che contiene l'indice aggregatore.
	L'indice in esso contenuto Regione AWS è configurato per essere l'indice di aggregazi one per l'account. Resource Explorer replica le informazioni sulle risorse raccolte negli indici locali di tutte le altre regioni in cui Resource Explorer è attivato nell'indice di aggregazione di questa regione. Le ricerche effettuate in questa regione possono includere i risultati di tutte le regioni dell'account.
	La visualizzazione predefinita creata da Quick Setup include tutte Regioni AWS le risorse.

amministratore Resource Explorer

Un amministratore di Resource Explorer è un responsabile AWS Identity and Access Management (IAM) che dispone dell'autorizzazione per gestire Resource Explorer e le relative impostazioni all'interno Account AWS . L'amministratore di Resource Explorer può configurare le seguenti funzionalità:

- Attiva Resource Explorer per i singoli Regioni AWS utenti Account AWS creando indici in tali regioni. Ciò consente a Resource Explorer di scoprire le risorse e di compilare l'indice con informazioni su tali risorse in modo che gli utenti possano cercare le risorse in quella regione.
- Aggiorna il tipo di indice in uno solo Regione AWS per renderlo l'indice aggregatore corrispondente. Account AWS L'indice di aggregazione in questa regione riceve copie replicate delle informazioni sulle risorse da tutte le altre regioni dell'account in cui è attivato Resource Explorer.
- Crea viste che definiscono il sottoinsieme di informazioni indicizzate che gli utenti possono cercare e scoprire in Resource Explorer.
- Sebbene non faccia parte delle azioni di Resource Explorer, l'amministratore di Resource Explorer deve anche essere in grado di concedere le autorizzazioni di ricerca ai responsabili dell'account. L'amministratore può concedere queste autorizzazioni ai responsabili aggiungendo le autorizzazioni pertinenti alle politiche di autorizzazione IAM esistenti o utilizzando la politica gestita di sola lettura di Resource Explorer. AWS

Per fornire l'accesso, aggiungi autorizzazioni ai tuoi utenti, gruppi o ruoli:

- Utenti e gruppi in AWS IAM Identity Center:

  Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center.

- Utenti gestiti in IAM tramite un provider di identità:

  Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina Creating a role for a third-party identity provider (federation) (Creazione di un ruolo per un provider di identità di terze parti [federazione]) nella Guida per l'utente di IAM.

- Utenti IAM:
  - Crea un ruolo che l'utente possa assumere. Per istruzioni, consulta la pagina Creating a role for an IAM user (Creazione di un ruolo per un utente IAM) nella Guida per l'utente di IAM.
  - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente di IAM.

L'amministratore dispone in genere di tutte le autorizzazioni di Resource Explorer (`resource-explorer-2:*`) su tutte le risorse di Resource Explorer, inclusi gli indici e le viste. Queste autorizzazioni possono essere concesse utilizzando la politica di accesso completo gestita di Resource Explorer. AWS

Utente Resource Explorer

Un utente Resource Explorer è un titolare IAM che dispone dell'autorizzazione per eseguire una o più delle seguenti attività:

- Esegui una ricerca di risorse utilizzando una vista per interrogare Resource Explorer. Un utente di Resource Explorer desidera scoprire e trovare AWS risorse e in genere utilizza la console Resource Explorer o le `Search` operazioni Resource Explorer fornite dagli AWS SDK o dalAWS CLI.

  Un ruolo o un utente può utilizzare IAM get permission per effettuare ricerche con uno dei due metodi seguenti:

  - La policy AWS gestita in sola lettura da Resource Explorer per il ruolo, il gruppo o l'utente IAM.

- Una politica di autorizzazione IAM con una dichiarazione contenente le seguenti autorizzazioni minime per il ruolo, il gruppo o l'utente IAM.

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

- Sebbene in genere sia considerata un'attività di amministratore, puoi delegare a utenti fidati la possibilità di definire viste di creazione. A tale scopo, l'amministratore può concedere l'autorizzazione a richiamare l'`resource-explorer-2:CreateView`operazione in una politica di autorizzazione IAM allegata ai ruoli, ai gruppi o agli utenti pertinenti. Se la vista richiede autorizzazioni specifiche, è necessario provvedere all'aggiunta o alla modifica delle politiche IAM per gli utenti pertinenti.

Per informazioni su come cercare risorse utilizzando Resource Explorer, consulta. UsandoEsploratore di risorse AWSper cercare risorse

Indice

Un indice è la raccolta di informazioni gestita da Resource Explorer su tutte le AWS risorse Regione AWS in un'unica risorsaAccount AWS. Resource Explorer mantiene un indice in ogni regione in cui è attivo Resource Explorer. Resource Explorer aggiorna automaticamente l'indice man mano che crei ed elimini risorse nel tuoAccount AWS. Nel diagramma precedente, le caselle sotto i Regione AWS nomi rappresentano gli indici di Resource Explorer mantenuti in ciascuno di essi. Regione AWS L'indice di una regione è la fonte di informazioni per tutte le viste create in quella regione. Gli utenti non possono interrogare direttamente l'indice. Al contrario, devono sempre eseguire una query utilizzando una vista.

Esistono due tipi di indici:

Indice locale

Esiste un indice locale in ogni momento Regione AWS in cui si attiva Resource Explorer. Un indice locale contiene informazioni solo sulle risorse della stessa regione.

Indice dell'aggregatore

L'amministratore di Resource Explorer può anche designare l'indice di uno come indice di aggregazione Regione AWS per. Account AWS L'indice dell'aggregatore riceve e archivia una copia dell'indice per ogni altra regione in cui Resource Explorer è attivato nell'account. L'indice dell'aggregatore riceve e archivia inoltre informazioni sulle risorse della propria regione. Nel diagramma precedente, la regione `us-west-2` contiene l'indice di aggregazione per l'account. Il motivo principale per cui è necessario designare un indice aggregatore per l'account è la possibilità di creare viste che possano includere risorse provenienti da tutte le regioni dell'account. Può esserci un solo indice di aggregazione in un. Account AWS

Quando attivi Resource Explorer, puoi specificare quale deve contenere Regione AWS l'indice dell'aggregatore. È inoltre possibile modificare l'indice Regione AWS utilizzato per l'indice di aggregazione in un secondo momento. Per informazioni su come promuovere un indice locale per renderlo il suo indice di aggregazioneAccount AWS, consulta. Attivazione della ricerca tra aree geografiche creando un indice di aggregazione

Un indice è una risorsa con un nome di risorsa Amazon (ARN). Tuttavia, è possibile utilizzare questo ARN solo nelle politiche di autorizzazione per concedere l'accesso alle operazioni che interagiscono direttamente con l'indice. Con queste operazioni, è possibile creare viste e impostarle come predefinite in una regione, attivare o disattivare Resource Explorer in una regione e creare un indice aggregatore per l'account. L'ARN di un indice è simile all'esempio seguente:

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

Vista

Una vista è il meccanismo utilizzato per interrogare le risorse elencate in un indice. La visualizzazione definisce quali informazioni nell'indice sono visibili e disponibili per scopi di ricerca e scoperta. Un utente non interroga mai direttamente l'indice Resource Explorer. Invece, le query devono sempre passare attraverso una visualizzazione che consenta al creatore della vista di limitare le risorse che l'utente può visualizzare nei risultati di ricerca.

Quando si crea una visualizzazione, si specificano filtri che limitano le risorse incluse nei risultati di ricerca. Ad esempio, puoi scegliere di includere solo le risorse di alcuni tipi di risorse specificati che vengono utilizzate da coloro a cui concedi l'accesso a questa visualizzazione. I risultati delle query eseguite dagli utenti con una vista vengono sempre filtrati automaticamente per includere solo le risorse che corrispondono ai criteri della vista.

Per concedere l'accesso all'utilizzo di una visualizzazione, puoi utilizzare Assign Permissions utilizzando uno dei seguenti metodi.

Per fornire l'accesso, aggiungi autorizzazioni ai tuoi utenti, gruppi o ruoli:

- Utenti e gruppi in AWS IAM Identity Center:

  Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center.
- Utenti gestiti in IAM tramite un provider di identità:

  Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina Creating a role for a third-party identity provider (federation) (Creazione di un ruolo per un provider di identità di terze parti [federazione]) nella Guida per l'utente di IAM.
- Utenti IAM:
  - Crea un ruolo che l'utente possa assumere. Per istruzioni, consulta la pagina Creating a role for an IAM user (Creazione di un ruolo per un utente IAM) nella Guida per l'utente di IAM.
  - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente di IAM.

Concedi l'autorizzazione per consentire ai tuoi ruoli, gruppi o utenti di richiamare le `resource-explorer-2:Search` operazioni `resource-explorer-2:GetView` and su una vista identificata dal relativo Amazon Resource Name (ARN). In alternativa, puoi utilizzare la politica AWS gestita di sola lettura di Resource Explorer per tutti i responsabili che devono utilizzare la vista per la ricerca. È possibile creare più visualizzazioni con filtri e ambiti diversi e quindi restituire diversi sottoinsiemi delle informazioni sulle risorse. Quindi, puoi concedere le autorizzazioni per ogni visualizzazione agli utenti che hanno bisogno di vedere le informazioni incluse nei risultati di quella vista.

Per eseguire ricerche con Resource Explorer, ogni utente deve disporre dell'autorizzazione per utilizzare almeno una visualizzazione. Non è possibile eseguire una ricerca in Resource Explorer senza utilizzare una visualizzazione.

Le visualizzazioni vengono archiviate in base alla regione. Una vista può accedere solo all'indice Resource Explorer in questione. Regione AWS Per accedere ai risultati della ricerca a livello di account, è necessario utilizzare una visualizzazione nella regione che contenga l'indice di aggregazione per l'account. L'opzione di configurazione rapida crea una visualizzazione predefinita

Regione AWS con l'indice dell'aggregatore e con filtri che includono tutte le risorse Regioni AWS utilizzate dall'account.

Per informazioni su come creare viste, consultaGestione delle visualizzazioni di Resource Explorer per fornire l'accesso alla ricerca. Per informazioni su come utilizzare le viste in una query, vedereUsandoEsploratore di risorse AWSper cercare risorse.

Ogni vista ha un Amazon Resource Name (ARN) a cui puoi fare riferimento nelle politiche di autorizzazione per concedere l'accesso a singole visualizzazioni. Puoi anche passare l'ARN di una vista come parametro a qualsiasi API o AWS CLI operazione che interagisce con una vista. L'ARN di una vista è simile all'esempio seguente.

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

> **Note**
>
> Ogni ARN di visualizzazione include un UUID AWS generato alla fine. Questo aiuta a garantire che gli utenti che potrebbero aver avuto accesso a viste con un nome specifico che è stato eliminato non possano accedere automaticamente a una nuova vista creata con lo stesso nome.

Risorsa

Una risorsa è un'entità con AWS cui è possibile lavorare. Le risorse vengono create Servizi AWS man mano che utilizzi le funzionalità del servizio. Gli esempi includono un'istanza Amazon EC2, un bucket Amazon S3 o uno stack. AWS CloudFormation Alcuni tipi di risorse possono contenere dati dei clienti. Tutti i tipi di risorse hanno attributi o metadati per descrivere la risorsa, tra cui un nome, una descrizione e il nome della risorsa Amazon (ARN) che usi per fare riferimento univoco a una risorsa. La maggior parte dei tipi di risorse supporta anche i tag. I tag sono metadati personalizzati che puoi allegare alle tue risorse per diversi scopi, come l'allocazione dei costi nella fatturazione, l'autorizzazione di sicurezza tramite il controllo degli accessi basato sugli attributi o per supportare altre esigenze di categorizzazione.

Lo scopo principale di Resource Explorer è aiutarti a trovare le risorse esistenti nel tuo. Account AWS Resource Explorer utilizza una varietà di tecniche per scoprire tutte le risorse e inserire le informazioni su di esse in un indice. Quindi, puoi interrogare l'indice utilizzando le visualizzazioni che l'amministratore ti mette a disposizione.

Important

Resource Explorer esclude intenzionalmente quei tipi di risorse la cui inclusione esporrebbe i dati dei clienti. I seguenti tipi di risorse non sono indicizzati da Resource Explorer e pertanto non vengono mai restituiti nei risultati di ricerca.

- Oggetti Amazon S3 contenuti in un bucket
- Elementi della tabella Amazon DynamoDB
- Valori degli attributi DynamoDB

Ricerca unificata in AWS Management Console

Nella parte superiore di ogni AWS Management ConsoleServizio AWS, c'è una barra di ricerca che puoi usare per cercare una varietà di cose AWS correlate. Puoi cercare servizi e funzionalità e ottenere collegamenti direttamente alla pagina pertinente nella console del servizio. Puoi anche cercare documentazione e articoli di blog correlati al termine di ricerca.

Dopo aver attivato Resource Explorer e creato un indice di aggregazione e una visualizzazione predefinita, la ricerca unificata può includere anche le risorse del tuo account nei risultati di ricerca. La ricerca unificata utilizza automaticamente la visualizzazione predefinita Regione AWS che contiene l'indice aggregatore per l'account. Ciò consente di cercare una risorsa da qualsiasi pagina diAWS Management Console, senza dover prima aprire Resource Explorer. Se non promuovi un indice locale come indice di aggregazione per l'account o se non crei una visualizzazione predefinita nella regione dell'indice di aggregazione, la ricerca unificata non include risorse nei risultati di ricerca. Inoltre, qualsiasi principale che esegue una ricerca deve avere l'autorizzazione a utilizzare la visualizzazione predefinita nella regione che contiene l'indice aggregatore o la ricerca unificata non include risorse nei risultati di ricerca.

Important

La ricerca unificata inserisce automaticamente un operatore di caratteri jolly (*) alla fine della prima parola chiave della stringa. Ciò significa che i risultati della ricerca unificata includono risorse che corrispondono a qualsiasi stringa che inizia con la parola chiave specificata. La ricerca eseguita dalla casella di testo Query nella pagina di ricerca delle risorse della console Resource Explorer non aggiunge automaticamente un carattere jolly. È possibile inserire * manualmente un dopo qualsiasi termine nella stringa di ricerca.

Per ulteriori informazioni sulla ricerca unificata e sulla sua integrazione con Resource Explorer, vedereUtilizzo della ricerca unificata in AWS Management Console.

Ricerca su più account

Con la ricerca su più account, puoi cercare e scoprire risorse utilizzando AWS Organizations e utilizzando Regioni AWS una sola parola chiave.

Per ulteriori informazioni sulla ricerca su più account e su come abilitarla per Resource Explorer, consulta. Attivazione della ricerca su più account

Prerequisiti per utilizzare Resource Explorer

Prima di Esploratore di risorse AWS utilizzarlo per la prima volta, completa le seguenti attività come richiesto.

Attività

- Registrati per un Account AWS
- Crea un utente con accesso amministrativo

Registrati per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

AWS ti invia un'e-mail di conferma dopo il completamento della procedura di registrazione. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .
2. In IAM Identity Center, concedi l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con le impostazioni predefinite IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accedi come utente con accesso amministrativo

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso ad altri utenti

1. In IAM Identity Center, crea un set di autorizzazioni che segua la migliore pratica di applicazione delle autorizzazioni con privilegi minimi.

   Per istruzioni, consulta Creare un set di autorizzazioni nella Guida per l'utente.AWS IAM Identity Center
2. Assegna gli utenti a un gruppo, quindi assegna l'accesso Single Sign-On al gruppo.

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente.AWS IAM Identity Center

Impostazione e configurazione di Resource Explorer

Prima di procedere all'installazione e alla configurazione Esploratore di risorse AWS, assicurati di soddisfare i prerequisiti. Successivamente, accedi come ruolo o utente IAM con le autorizzazioni necessarie per eseguire le operazioni di Resource Explorer per la procedura seguente.

È possibile utilizzare questa procedura di installazione e configurazione per configurare Resource Explorer negli account esistenti e in tutti i nuovi account aggiunti all'organizzazione.

Esistono due modi per configurare Resource Explorer:

- Configurazione rapida
- Configurazione avanzata

> **Important**
>
> Se scegli di configurare Resource Explorer utilizzando qualsiasi opzione che dice Regioni AWS «tutte», verranno attivate solo quelle Regioni AWS esistenti e abilitate nel Account AWS momento in cui si esegue la procedura. Resource Explorer non si attiva automaticamente in Regioni AWS quelli che verranno AWS aggiunti in futuro. Quando si AWS introduce una nuova regione, è possibile scegliere di attivare Resource Explorer nella regione manualmente

quando viene visualizzato nella pagina Impostazioni della console Resource Explorer oppure richiamando l'CreateIndexoperazione.

> **Note**
>
> La configurazione di Resource Explorer può anche attivare la capacità di cercare risorse utilizzando la barra di ricerca unificata su. AWS Management Console Affinché gli utenti possano visualizzare le risorse nei risultati di ricerca unificati, è necessario configurare Resource Explorer con un indice di aggregazione interregionale e una visualizzazione predefinita. Per i dettagli, consulta le seguenti procedure. È inoltre necessario assicurarsi che gli utenti che effettuano la ricerca siano autorizzati a utilizzare la visualizzazione predefinita in Regione AWS quella che contiene l'indice dell'aggregatore. Per ulteriori informazioni, consulta Utilizzo della ricerca unificata in AWS Management Console.

Configurazione di Resource Explorer utilizzando la configurazione rapida

Se scegli l'opzione di configurazione rapida, Resource Explorer esegue le seguenti operazioni:

- Crea un indice Regione AWS in ogni tuo Account AWS.
- Aggiorna l'indice nella regione specificata come indice di aggregazione per l'account.
- Crea una vista predefinita nella regione dell'indice di aggregazione. Questa vista non ha filtri, quindi restituisce tutte le risorse trovate nell'indice.

Autorizzazioni minime

Per eseguire i passaggi della procedura seguente, è necessario disporre delle seguenti autorizzazioni:

- Azione: `resource-explorer-2:*` — Risorsa: nessuna risorsa specifica () *
- Azione: `iam:CreateServiceLinkedRole` — Risorsa: nessuna risorsa specifica (*)

AWS Management Console

Per configurare Resource Explorer utilizzando la configurazione rapida

1. Apri la Esploratore di risorse AWS console all'indirizzohttps://console.aws.amazon.com/resource-explorer.
2. Scegli Attiva Resource Explorer.
3. Nella pagina Attiva Resource Explorer, scegli Configurazione rapida.
4. Scegli quale Regione AWS vuoi che contenga l'indice dell'aggregatore. Devi selezionare la regione appropriata per la posizione geografica dei tuoi utenti.
5. Nella parte inferiore della pagina, scegli Attiva Resource Explorer.
6. Nella pagina Avanzamento, puoi monitorarli tutti Regione AWS mentre Resource Explorer crea il relativo indice. La pagina mostra lo stato della creazione dell'indice dell'aggregatore e della creazione della visualizzazione predefinita.

Dopo che tutti i passaggi dimostrano che sono stati completati correttamente, tu e i tuoi utenti potete accedere alla pagina di ricerca delle risorse e iniziare a cercare le risorse.

> **Note**
>
> Le risorse con tag locali all'indice vengono visualizzate nei risultati di ricerca entro pochi minuti. Le risorse senza tag richiedono in genere meno di due ore per essere visualizzate, ma possono richiedere più tempo in caso di forte richiesta. Inoltre, può essere necessaria fino a un'ora per completare la replica iniziale su un nuovo indice di aggregazione da tutti gli indici locali esistenti.

Passaggi successivi: prima che gli utenti possano eseguire la ricerca con la visualizzazione predefinita appena creata, è necessario concedere loro le autorizzazioni per la ricerca con essa. Per ulteriori informazioni, consulta Concessione dell'accesso alle visualizzazioni di Resource Explorer per la ricerca.

AWS CLI

La configurazione di Resource Explorer Account AWS utilizzando l'opzione di configurazione avanzata AWS CLI è, per definizione, equivalente all'opzione di configurazione avanzata. Questo perché le operazioni CLI di Resource Explorer non eseguono automaticamente

nessuno dei passaggi come fa la console di Resource Explorer. Consulta la AWS CLI scheda in Configurazione di Resource Explorer utilizzando la configurazione avanzata alto per vedere quali comandi equivalgono all'utilizzo della console.

Configurazione di Resource Explorer utilizzando la configurazione avanzata

Se scegli l'opzione Configurazione avanzata, puoi fare quanto segue:

- Scegli il modo Regioni AWS in cui attivare Resource Explorer.
- Scegli se configurare una regione con un indice di aggregazione. Se lo fai, specifichi in Regione AWS cui inserirlo. Questo indice consente di creare viste che possono includere risorse provenienti da tutte le regioni dell'account. Per ulteriori informazioni, consulta Attivazione della ricerca tra aree geografiche creando un indice di aggregazione.
- Scegli se creare una vista predefinita. Questa visualizzazione consente di cercare automaticamente qualsiasi AWS risorsa nelle regioni in cui è attivo Resource Explorer. È necessario assicurarsi che tutti gli amministratori che devono utilizzare la visualizzazione predefinita per la ricerca in Resource Explorer dispongano delle autorizzazioni per la visualizzazione. Per ulteriori informazioni, consulta Concessione dell'accesso alle visualizzazioni di Resource Explorer per la ricerca.

> **Note**
>
> È possibile configurare Resource Explorer per includere le risorse nei risultati di ricerca forniti dalla funzionalità di ricerca unificata di. AWS Management Console Per attivare questa funzionalità, è necessario configurare Resource Explorer con un indice di aggregazione e una visualizzazione predefinita che consenta la ricerca di tutti i ruoli e gli utenti. L'opzione di configurazione rapida crea sia l'indice dell'aggregatore che la visualizzazione predefinita ed è il modo in cui consigliamo di attivare Resource Explorer.

Autorizzazioni minime

Per eseguire i passaggi della procedura seguente, è necessario disporre delle seguenti autorizzazioni:

- Azione: `resource-explorer-2:*` — Risorsa: nessuna risorsa specifica () *
- Azione: `iam:CreateServiceLinkedRole` — Risorsa: nessuna risorsa specifica (*)

AWS Management Console

Per attivare Resource Explorer utilizzando la configurazione avanzata

1. Apri la Esploratore di risorse AWS console all'indirizzohttps://console.aws.amazon.com/resource-explorer.
2. Scegli Attiva Resource Explorer.
3. Nella pagina Attiva Resource Explorer, scegli Configurazione avanzata.
4. Nella Regioni AWScasella, in Regioni, scegli se attivare Resource Explorer in tutte le Regioni AWS aree o solo in alcune aree.

   Se scegli Attiva Resource Explorer solo nelle aree specificate Regioni AWS in questo account, seleziona ogni regione di cui desideri includere le risorse nei risultati di ricerca.
5. Per l'indice di aggregazione, scegli se desideri creare un indice di aggregazione. Se scegli di creare un indice aggregatore, tutti gli altri indici Regioni AWS replicano i propri indici in questa regione. Ciò consente agli utenti di cercare risorse in tutte le regioni selezionate in. Account AWS Scegli Regione AWS quello che contiene l'indice dell'aggregatore. Ti consigliamo di specificare la regione in cui gli utenti trascorrono la maggior parte del loro tempo o almeno dove ti aspetti che eseguano la maggior parte delle ricerche nelle risorse.
6. Nella casella Visualizzazione predefinita, in Creazione della vista, scegli se creare una visualizzazione predefinita. Questa opzione è disponibile solo se avete scelto di creare un indice aggregatore. Se scegli di creare una vista predefinita, Resource Explorer colloca questa vista nella Regione AWS stessa posizione dell'indice dell'aggregatore. Ciò consente alla visualizzazione predefinita di includere i risultati di tutti i risultati Regioni AWS in cui è stato registrato Resource Explorer. Ogni volta che un utente esegue una ricerca in una regione con una visualizzazione predefinita e non specifica esplicitamente una vista, la ricerca utilizza la visualizzazione predefinita per quella regione.

   > **Note**
   >
   > Prima che gli utenti possano eseguire ricerche con una vista, è necessario concedere loro le autorizzazioni per utilizzare tale visualizzazione. Per ulteriori informazioni, consulta Concessione dell'accesso alle visualizzazioni di Resource Explorer per la ricerca.
7. Scegli Attiva Resource Explorer.

> **Note**
>
> Le risorse con tag locali all'indice vengono visualizzate nei risultati di ricerca entro pochi minuti. Le risorse senza tag richiedono in genere meno di due ore per essere visualizzate, ma possono richiedere più tempo in caso di forte richiesta. Inoltre, può essere necessaria fino a un'ora per completare la replica iniziale su un nuovo indice di aggregazione da tutti gli indici locali esistenti.

AWS CLI

Per configurare Resource Explorer utilizzando la configurazione avanzata

La console Resource Explorer esegue molte chiamate operative API per conto dell'utente in base alle scelte effettuate. I AWS CLI comandi di esempio seguenti illustrano come eseguire le stesse procedure di base al di fuori della console utilizzando il AWS CLI.

Example Passo 1: Attiva Resource Explorer creando indici nel formato desiderato Regioni AWS

Esegui il seguente comando in ognuna delle aree Regione AWS in cui desideri attivare Resource Explorer. Il comando di esempio seguente attiva Resource Explorer nell' Regione AWS impostazione predefinita per 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 Passaggio 2: Aggiorna l'indice in uno in Regione AWS modo che diventi l'indice di aggregazione per l'account

Esegui il seguente comando Regione AWS in cui desideri che Resource Explorer aggiorni l'indice locale all'indice di aggregazione per l'account. Il comando di esempio seguente aggiorna l'indice dell'aggregatore negli Stati Uniti orientali (Virginia settentrionale) (). `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 Passaggio 3: Creare una vista Regione AWS che contiene l'indice dell'aggregatore

Esegui il comando seguente Regione AWS nel quale hai creato l'indice dell'aggregatore. Il comando di esempio seguente crea una vista identica a quella creata dal processo di configurazione della console Resource Explorer. Questa nuova visualizzazione include i tag allegati alla risorsa come parte delle informazioni indicizzate e supporta la ricerca di risorse per chiave o valore del tag.

```
$ 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 Passaggio 4: Imposta la nuova visualizzazione come predefinita per la sua Regione AWS

L'esempio seguente imposta la vista creata nel passaggio precedente come predefinita per la Regione. È necessario eseguire il comando seguente nello stesso modo Regione AWS in cui è stata creata la vista predefinita.

```
$ 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"
}
```

Prima che gli utenti possano eseguire ricerche con una vista, è necessario concedere loro le autorizzazioni per utilizzare tale visualizzazione. Per ulteriori informazioni, consulta Concessione dell'accesso alle visualizzazioni di Resource Explorer per la ricerca.

Dopo aver eseguito questi comandi, Resource Explorer viene eseguito nelle regioni specificate nel tuo Account AWS. Resource Explorer crea e mantiene un indice in ogni regione con i dettagli delle risorse che vi si trovano. Resource Explorer replica ciascuno dei singoli indici di regione nell'indice di aggregazione nella regione specificata. Tale regione contiene anche una vista che consente a qualsiasi ruolo o utente IAM dell'account di cercare risorse in tutte le regioni indicizzate.

> **Note**
>
> Le risorse con tag locali all'indice vengono visualizzate nei risultati di ricerca entro pochi minuti. Le risorse senza tag richiedono in genere meno di due ore per essere visualizzate, ma possono richiedere più tempo in caso di forte richiesta. Inoltre, può essere necessaria fino a un'ora per completare la replica iniziale su un nuovo indice di aggregazione da tutti gli indici locali esistenti.

Gestione di Resource Explorer per supportare la ricerca di risorse

Dopo aver inizialmente attivato Esploratore di risorse AWS almeno un Regione AWS dispositivoAccount AWS, ci sono attività amministrative che potresti dover eseguire occasionalmente. Questa sezione descrive le attività di manutenzione e configurazione che consentono di far funzionare Resource Explorer nel modo desiderato man mano Account AWS che l'utilizzo delle risorse si evolve.

Argomenti

- Verifica di qualiRegioni AWSavere Resource Explorer attivato
- Attivazione della ricerca su più account
- Attivazione di Resource Explorer in unRegione AWS per indicizzare le risorse
- Considerazioni per le regioni che AWS aderiscono
- Attivazione della ricerca tra aree geografiche creando un indice di aggregazione
- Supporta la ricerca unificata inAWS Management Console
- Effetto delle azioni dell'account sulla ricerca multi-account di Resource Explorer
- Disattivazione di Resource Explorer in un Regione AWS
- Disattivare completamente Resource ExplorerRegioni AWS
- Distribuzione di Resource Explorer agli account di un'organizzazione

Verifica di qualiRegioni AWSavere Resource Explorer attivato

Puoi scoprire qualiRegioni AWSavereEsploratore di risorse AWSattivato controllando quali regioni contengono un indice per Resource Explorer. Per visualizzare quali regioni dispongono di un indice, utilizzare le procedure in questa pagina.

> **Important**
>
> Gli utenti possono cercare risorse insoloquelle regioni in cui Resource Explorer è attivato. Puoi anche creare un indice aggregatore in una regione per supportare la ricerca di risorse in tutte le tue regioni. Resource Explorer replica le informazioni sulle risorse nella regione con l'indice aggregatore di tutte le altre regioni che contengono un indice di Resource Explorer.

Gli utenti non possono utilizzare Resource Explorer per scoprire risorse in regioni che non dispongono di un indice.

Verifica dello stato di Resource Explorer in una regione

Puoi verificare quali regioni dispongono di indici per Resource Explorer utilizzandoAWS Management Console, utilizzando i comandi inAWS Command Line Interface(AWS CLI) o utilizzando le operazioni API in unAWSSDK.

AWS Management Console

Per verificare quali regioni dispongono di indici per Resource Explorer

1. Apri ilImpostazionipagina nella console di Resource Explorer.
2. L'elenco nelIndicila sezione include solo le regioni che contengono un indice di Resource Explorer. Il valore nelTipola colonna indica se l'indice è unLocaleindice per la sua regione, oAggregatoreindice perAccount AWS.
3. Per vedere quali regioni non contengono un Resource Explorer, scegliCreare indici. Se una regione non è presente, la regione non contiene Resource Explorer.

AWS CLI

Per verificare quali regioni dispongono di indici per Resource Explorer

Esegui il seguente comando per vedere qualeRegioni AWSdispongono di indici per 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"
        }
    ]
}
```

Attivazione della ricerca su più account

Con la ricerca su più account, puoi cercare risorse tra gli account con indici attivi nella tua unità organizzativa (AWS Organizations OU).

Argomenti

- Prerequisiti
- Abilita la ricerca su più account
- Configurazione rapida per più account

Prerequisiti

Per attivare la ricerca su più account per la tua organizzazione, completa quanto segue:

- Per le Regioni con attivazione attiva, verifica che il tuo account di gestione sia attivo anche quando attivi la ricerca su più account.
- Creazione di un utente amministratore.
- Crea un ruolo collegato al servizio nell'account amministratore con. `aws iam create-service-linked-role --aws-service-name resource-explorer-2.amazonaws.com`
- Abilita l'accesso affidabile in. AWS Organizations Ciò consente la piena integrazione con Resource Explorer per elencare le risorse di tutti gli account dell'organizzazione.
- Assegna un amministratore delegato (consigliato). Per ulteriori informazioni, vedere Amministratore delegato per AWS i servizi che funzionano con Organizations nella Guida per l'AWS Organizations utente.
  - Resource Explorer supporta solo 1 amministratore delegato che esegue azioni simili all'account di gestione.
  - La rimozione o la modifica dell'amministratore delegato dell'organizzazione comporta la rimozione di tutte le visualizzazioni multi-account create nell'account.

Abilita la ricerca su più account

Per cercare e scoprire risorse negli account della tua organizzazione, devi completare i seguenti passaggi:

1. Esploratore di risorse AWS Attivalo in uno o più account nel tuo AWS Organizations.
2. Registra una regione per contenere l'indice dell'aggregatore.
3. Scegli una regione in cui creare un indice di aggregazione. Questa regione deve essere coerente in tutta la tua AWS Organizations.
4. Crea una visualizzazione di Resource Explorer dedicata alla tua unità AWS Organizations o alla tua unità organizzativa. Crea questa vista nella regione dell'aggregatore dal passaggio precedente.
5. Condividi la visualizzazione con gli account di tutta l'organizzazione.

Configurazione rapida per più account

Abilita Resource Explorer su più account della tua organizzazione con la configurazione rapida.

> **Note**
>
> Questo processo non distribuisce alcuna risorsa nell'account di gestione. Se utilizzi l'account di gestione e desideri inserire degli indici nell'account, devi aggiungerli manualmente con il flusso di onboarding di Resource Explorer.

1. Accedere a Quick Setup for Resource Explorer nella console Systems Manager.
2. Scegliete la regione dell'indice Aggregator. Ciò consente di cercare risorse situate in tutte le regioni negli account di destinazione selezionati. Se uno degli account di destinazione selezionati ha già un indice di aggregazione configurato in un'altra regione, l'indice di aggregazione esistente verrà automaticamente sostituito con questa nuova regione.
3. Scegli gli obiettivi del tuo account. Puoi abilitare Resource Explorer per l'intera organizzazione o per unità organizzative (OU) specifiche.

   > **Note**
   >
   > È possibile eseguire la distribuzione su un massimo di 50.000 AWS CloudFormation stack alla volta. Se hai un'organizzazione di grandi dimensioni che si estende su più

regioni, dovresti eseguire la distribuzione a livello di unità organizzativa in batch più piccoli.

4. Leggi il riepilogo dei riconoscimenti prima di scegliere Crea.

Attivazione di Resource Explorer in unRegione AWS per indicizzare le risorse

Quando inizialmente attivi ilEsploratore di risorse AWS tuoAccount AWS, hai creato indici per il servizio in uno o piùRegioni AWS. Se hai utilizzato l'opzione Configurazione rapida, Resource Explorer ha creato automaticamente gli indici in tuttoRegioni AWS ciò che è attivato nel tuoAccount AWS. Il servizio Resource Explorer ha inoltre promosso l'indice nella regione specificata come indice aggregatore per l'account. Se hai utilizzato l'opzione Configurazione avanzata, hai specificato le regioni in cui creare gli indici.

Per attivare Resource Explorer in altre regioni, utilizza le procedure descritte in questo argomento.

Quando si attiva Resource Explorer in unRegione AWS, il servizio esegue le seguenti azioni:

- Quando avvii Resource Explorer nella prima regione di unAccount AWS, Resource Explorer crea un ruolo collegato al servizio nell'account denominato`AWSServiceRoleForResourceExplorer`. Questo ruolo concede a Resource Explorer le autorizzazioni per scoprire e indicizzare le risorse del tuo account utilizzando servizi comeAWS CloudTrail il servizio di tagging. La creazione del ruolo collegato al servizio avviene solo quando si registra il primo ruoloRegione AWS nell'account. Resource Explorer utilizza lo stesso ruolo collegato al servizio per tutte le regioni aggiuntive che aggiungi in seguito.
- Resource Explorer crea un indice nella regione specificata per memorizzare i dettagli sulle risorse di quella regione.
- Resource Explorer inizia a scoprire le risorse nella regione specificata e aggiunge le informazioni che trova su di esse all'indice di quella regione.
- Se il tuo account contiene già un indice aggregatore in un'altra regione, Resource Explorer inizia a replicare le informazioni dall'indice della nuova regione all'indice aggregatore per supportare la ricerca tra regioni.

Una volta completati questi passaggi, le informazioni sulle risorse sono disponibili per essere scoperte dagli utenti. Possono effettuare la ricerca utilizzando una delle viste definite nella stessa regione o nella regione che contiene l'indice aggregatore.

Creare un indice Resource Explorer in una regione

È possibile creare un indice Resource Explorer in un altroRegione AWS utilizzandoAWS Management Console, utilizzando i comandi inAWS Command Line Interface (AWS CLI) o utilizzando le operazioni API in unAWS SDK. È possibile creare un solo indice in una regione.

Autorizzazioni minime

Per eseguire le fasi riportate nella seguente procedura, è necessario disporre delle seguenti autorizzazioni:

- Azione:`resource-explorer-2:*` — Risorsa: nessuna risorsa specifica (`*`)
- Azione:`iam:CreateServiceLinkedRole` — Risorsa: nessuna risorsa specifica (`*`)

AWS Management Console

Per creare un indice Resource Explorer in unRegione AWS

1. Nella pagina delle impostazioni di Resource Explorer.
2. Nella sezione Indici, scegli Crea indici.
3. Nella pagina Crea indici, seleziona le caselle di controllo accanto a quelleRegioni AWS in cui desideri creare un indice per supportare la ricerca nelle risorse di quella regione. Le caselle di controllo non disponibili indicano le regioni che contengono già un indice Resource Explorer.
4. (Facoltativo) Nella sezione Tag, è possibile specificare coppie di chiavi e valori del tag nell'indice.
5. Scegli Crea indici.

   Resource Explorer visualizza un banner verde nella parte superiore della pagina per indicare il successo o un banner rosso se si verifica un errore durante la creazione di un indice in una o più delle regioni selezionate.

> **Note**
>
> Le risorse con tag locali all'indice vengono visualizzate nei risultati di ricerca entro pochi minuti. La visualizzazione delle risorse senza tag richiede in genere meno di due ore, ma può richiedere più tempo in caso di forte richiesta. Può inoltre essere necessaria fino a un'ora per completare la replica iniziale su un nuovo indice aggregatore da tutti gli indici locali esistenti.

Passaggio successivo: se hai già creato un indice aggregatore, le nuove regioni iniziano automaticamente a replicare le informazioni sull'indice aggregatore. Se è qui che gli utenti effettuano tutte le loro ricerche, le risorse della nuova regione vengono visualizzate nei risultati di ricerca e il gioco è fatto.

Tuttavia, se desideri che gli utenti siano in grado di cercare risorse solo nella nuova regione indicizzata, devi anche creare una vista per gli utenti in quella regione e concedere ai tuoi utenti le autorizzazioni per quella vista. Per istruzioni su come creare una vista, consultaGestione delle visualizzazioni di Resource Explorer per fornire l'accesso alla ricerca.

AWS CLI

Per creare un indice Resource Explorer in unRegione AWS

Esegui il comando seguente per ognunoRegione AWS in cui desideri creare un indice per supportare la ricerca delle risorse di quella regione. Il comando seguente di esempio registra Resource negli Stati Uniti orientali (Virginia settentrionale`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"
}
```

Ripeti questo comando per ogni regione in cui desideri attivare Resource Explorer, sostituendo il codice Region appropriato per il`--region` parametro.

Poiché Resource Explorer esegue parte della creazione dell'indice come attività asincrone in background, la risposta può essereCREATING, il che indica che i processi in background non sono ancora completi.

> **Note**
>
> Le risorse con tag locali all'indice vengono visualizzate nei risultati di ricerca entro pochi minuti. La visualizzazione delle risorse senza tag richiede in genere meno di due ore, ma può richiedere più tempo in caso di forte richiesta. Può inoltre essere necessaria fino a un'ora per completare la replica iniziale su un nuovo indice aggregatore da tutti gli indici locali esistenti.

È possibile verificare il completamento finale eseguendo il seguente comando e controllando loACTIVE stato.

```
$ 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"
}
```

Passaggio successivo: se hai già creato un indice aggregatore, le nuove regioni iniziano automaticamente a replicare le informazioni sull'indice aggregatore. Se è qui che gli utenti effettuano tutte le loro ricerche, le risorse della nuova regione vengono visualizzate nei risultati di ricerca e il gioco è fatto.

Tuttavia, se desideri che gli utenti siano in grado di cercare risorse solo nella nuova regione indicizzata, devi anche creare una vista per gli utenti in quella regione e concedere ai tuoi utenti le autorizzazioni per quella vista. Per istruzioni su come creare una vista, consultaGestione delle visualizzazioni di Resource Explorer per fornire l'accesso alla ricerca.

Considerazioni per le regioni che AWS aderiscono

Le regioni opt-in hanno requisiti di sicurezza più elevati rispetto alle regioni commerciali per quanto riguarda la condivisione dei dati IAM tramite account nelle regioni che accettano di aderire. Tutti i dati gestiti tramite il servizio IAM sono considerati dati di identità.

Puoi attivare le regioni opt-in utilizzando la Esploratore di risorse AWS console. Per ulteriori informazioni, vedi Attivazione di Resource Explorer in un Regione AWS per indicizzare le tue risorse.

Comportamenti di opt-out

Prendi in considerazione i seguenti comportamenti prima di rinunciare a una regione di opt-in:

> **Important**
>
> Prima di disattivare una regione con un indice di aggregazione, ti suggeriamo di eliminare l'indice di aggregazione o di ridurlo a indice locale. Resource Explorer supporta un indice di aggregazione per tutte le regioni all'interno della partizione.

- L'indice non viene eliminato, è solo disabilitato. Se scegli di effettuare nuovamente l'attivazione in un secondo momento, le impostazioni verranno ripristinate.
- IAM disabilita l'accesso IAM alle risorse nella regione.
- Resource Explorer disabilita l'indice per la regione esclusa e interrompe l'acquisizione dei dati. L'`ListIndexes`API non mostrerà più l'indice della regione.
- Se l'indice dell'aggregatore si trova in una regione diversa, Resource Explorer interrompe la replica dei dati dalla regione disattivata e pulisce i dati entro 24 ore.
- Se disattivi la regione dell'indice di aggregazione, dovrai effettuare nuovamente l'opt-in per eliminare o abbassare di livello l'indice.
- Se effettui nuovamente l'opt-in per la regione, Resource Explorer riattiva l'indice e inizia a importare i dati.
- Qualsiasi modifica allo stato di una regione attiva richiede circa 24 ore per entrare in vigore.

Attivazione della ricerca tra aree geografiche creando un indice di aggregazione

Argomenti

- Informazioni sull'indice degli aggregatori
- Promuovere un indice locale come indice aggregatore per l'account
- Ridurre l'indice dell'aggregatore a un indice locale

Informazioni sull'indice degli aggregatori

Esploratore di risorse AWSarchivia le informazioni raccolte sulle risorse in un indice locale creato e gestito Regione AWS da Resource Explorer in quella regione. Ad esempio, supponiamo di avere un'istanza Amazon EC2 nella regione Stati Uniti occidentali (Oregon). Resource Explorer memorizza i dettagli su tale risorsa nell'indice locale nella regione Stati Uniti occidentali (Oregon).

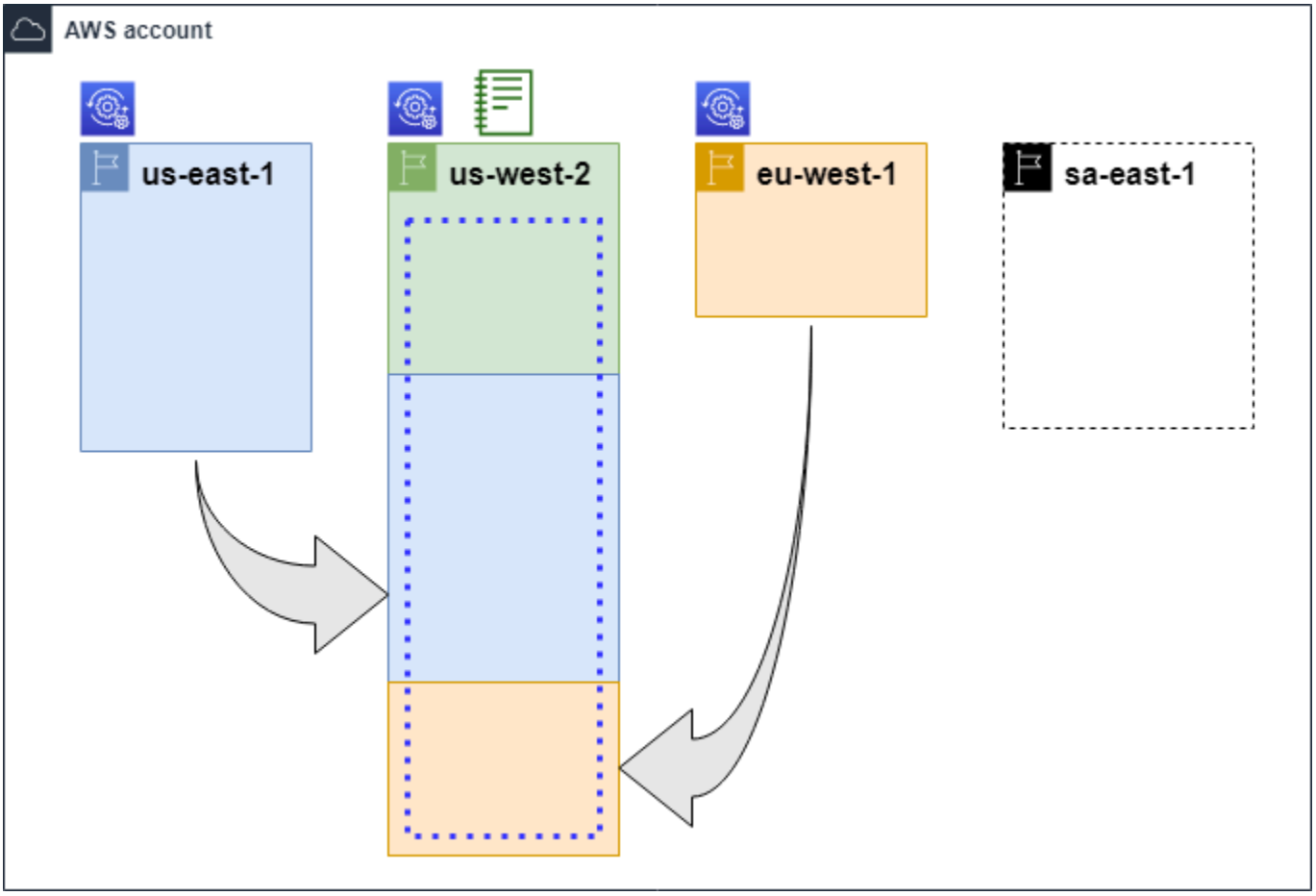
Per supportare la ricerca di risorse Regioni AWS in tutto il tuo account, puoi convertire l'indice locale di una regione in modo che diventi l'indice di aggregazione per il tuo account.

L'indice di aggregazione contiene una copia replicata dell'indice locale in ogni altra regione in cui è stato attivato Resource Explorer. Ciò consente di creare viste nella regione che contiene l'indice di aggregazione i cui risultati possono includere risorse provenienti da tutte Regioni AWS le risorse dell'account.

Il diagramma seguente mostra un esempio di come funziona l'indice di aggregazione. In questo esempioAccount AWS, l'amministratore esegue le seguenti operazioni:

- Attiva Resource Explorer in tre Regioni AWS (`us-east-1`us-west-2, `eeu-west-1`) creando indici in tali regioni. Ogni regione contiene il proprio indice locale.
- Sceglie di non creare un indice nella `sa-east-1` regione. Gli utenti non possono eseguire ricerche in e nei `sa-east-1` risultati di ricerca non viene visualizzata alcuna risorsa proveniente da tale regione.
- Crea l'indice di aggregazione per l'account nella `us-west-2` regione. Ciò fa sì che Resource Explorer replichi le informazioni dagli indici locali in tutte le altre regioni in cui Resource Explorer è attivato nell'indice dell'aggregatore. Ciò consente alle ricerche eseguite di includere risorse provenienti da tutte e tre le regioni in `us-west-2` cui Resource Explorer è attivo.

Questa configurazione significa che un utente può eseguire ricerche interregionali solo in`us-west-2`, che contiene l'indice dell'aggregatore. Solo le visualizzazioni di quella regione possono restituire risultati da tutte le regioni dell'account.



Leggenda	
	In questo Regione AWS caso Resource Explorer è attivato e le sue risorse sono catalogate in un indice in quella regione. L'indice di questa regione viene inoltre replicato (indicato dalle frecce) nell'indice Regione AWS che contiene l'indice dell'aggregatore.
	Regione AWSContiene l'indice dell'aggregatore. Resource Explorer replica le informazioni sulle risorse raccolte in tutte le altre Regioni AWS in questa regione.
	La visualizzazione predefinita creata da Quick Setup include tutte Regioni AWS le risorse.

Promuovere un indice locale come indice aggregatore per l'account

Hai la possibilità di creare un indice aggregatore in unoRegione AWS quando esegui la prima configurazioneEsploratore di risorse AWS. Per ulteriori informazioni, consulta Impostazione e configurazione di Resource Explorer. Questa procedura consiste nel promuovere uno degli indici locali come indice aggregatore per l'account se non l'hai fatto durante la configurazione iniziale.

> **Important**
>
> - Puoi disporre di un solo indice aggregatore in unAccount AWS. Se l'account dispone già di un indice aggregatore, è necessario innanzitutto ridurlo di livello a indice locale o eliminarlo.
> - Dopo aver eliminato o modificato la regione che contiene l'indice aggregatore, è necessario attendere 24 ore prima di poter promuovere un altro indice come indice aggregatore.

AWS Management Console

Promuovere un indice locale come indice aggregatore per l'account

1. Apri la pagina delle impostazioni di Resource Explorer.
2. Nella sezione Indici, seleziona la casella di controllo accanto all'indice che desideri promuovere, quindi scegli Cambia tipo di indice.
3. Nella finestra di dialogo Modifica il tipo di indice per < Nome regione >, scegliete indice aggregatore e quindi selezionate Salva modifiche.

AWS CLI

Promuovere un indice locale come indice aggregatore per l'account

Il comando di esempio seguente aggiorna l'indice nel campo specificatoRegione AWS da tipo`LOCAL` a tipo`AGGREGATOR`. È necessario richiamare l'operazione dall'indice di aggregazioneRegione AWS che si desidera contenere.

```
$ 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"
}
```

L'operazione funziona in modo asincrono e inizia con`State` set to`UPDATING`. Per verificare se l'operazione è stata completata, è possibile eseguire il comando seguente e cercare il valore`ACTIVE` nel campo di`State` risposta. È necessario eseguire questo comando nella regione che contiene l'indice che si desidera controllare.

```
$ 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"
}
```

Ridurre l'indice dell'aggregatore a un indice locale

Puoi abbassare di livello un indice di aggregazione a un indice locale, ad esempio quando desideri spostare l'indice dell'aggregatore su un altro. Regione AWS

Quando si riduce di livello un indice di aggregazione a un indice locale, Resource Explorer interrompe la replica degli indici dagli altri. Regioni AWS Avvia inoltre un'attività asincrona in background per eliminare tutte le informazioni replicate da altre regioni. Fino al completamento dell'attività asincrona, alcuni risultati interregionali possono continuare a essere visualizzati nei risultati di ricerca.

> **Note**
>
> - Dopo aver abbassato di livello un indice di aggregazione, è necessario attendere 24 ore prima di poter promuovere lo stesso indice o l'indice di un'altra regione come nuovo indice di aggregazione per l'account.
> - Dopo la riduzione di livello di un indice aggregatore, possono essere necessarie fino a 36 ore prima che i processi in background vengano completati e tutte le informazioni sulle risorse provenienti da altre regioni scompaiano dai risultati delle ricerche eseguite in questa regione.
> - Se si declassa di livello un account membro all'interno di una visualizzazione a livello di organizzazione, il membro può essere rimosso dalla ricerca su più account.

È possibile controllare lo stato dell'attività in background visualizzando l'elenco degli indici nella pagina Impostazioni o utilizzando l'operazione. GetIndex Quando le attività asincrone vengono completate, il `Status` campo dell'indice cambia da a. `UPDATING` `ACTIVE` In quel momento, nei risultati delle query vengono visualizzati solo i risultati della regione locale.

AWS Management Console

Per abbassare di livello un indice di aggregazione a un indice locale

1. Aprire la pagina delle impostazioni di Resource Explorer.
2. Nella sezione Indici, seleziona la casella di controllo accanto alla Regione che contiene l'indice di aggregazione che desideri ridurre a indice locale, quindi scegli Cambia tipo di indice.
3. Nella finestra di dialogo Cambia il tipo di indice per < nome della regione >, scegliete Indice locale, quindi scegliete Salva modifiche.

AWS CLI

Per abbassare di livello un indice di aggregazione a un indice locale

L'esempio seguente riduce di livello l'indice di aggregazione specificato a un indice locale. È necessario chiamare l'operazione Regione AWS che attualmente contiene l'indice dell'aggregatore.

```
$ 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"
}
```

L'operazione funziona in modo asincrono e inizia con impostato su. `State` `UPDATING` Per verificare se l'operazione è stata completata, è possibile eseguire il comando seguente e cercare il valore `ACTIVE` nel campo di risposta. `State` È necessario eseguire questo comando nella regione che contiene l'indice che si desidera controllare.

```
$ 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"
}
```

Supporta la ricerca unificata inAWS Management Console

AWS Management ConsoleHa una barra di ricerca nella parte superiore di ogni pagina della console. Ciò fornisce un'esperienza di ricerca unificata per tuttiServizi AWS. I risultati di ricerca unificati possono includere cose come:

- Servizio AWSe presenta pagine della console.
- AWSpagine di documentazione.
- AWSarticoli del blog e della Knowledge Base
- Risorse nei tuoi account, completa i seguenti passaggi.

Per visualizzare le risorse del tuo account nei risultati di ricerca unificati, devi eseguire i seguenti passaggi. È possibile eseguire questa operazione durante la configurazione iniziale diEsploratore di risorse AWS. Tutto avviene automaticamente se si utilizza l'opzione Configurazione rapida.

- È necessario creare un indice aggregatore in unoRegione AWS perAccount AWS.
- È necessario creare una vista predefinita inRegione AWS che contenga l'indice aggregatore.
- È necessario concedere a tutti i responsabili che devono cercare risorse nella barra di ricerca unificata il permesso di eseguire la ricerca utilizzando la visualizzazione predefinita.

La ricerca unificata utilizza sempre la vista predefinita inRegione AWS quella che contiene l'indice aggregatore per eseguire tutte le ricerche.

Effetto delle azioni dell'account sulla ricerca multi-account di Resource Explorer

> **Note**
>
> Sono necessarie fino a 24 ore per rimuovere account e risorse dai risultati di ricerca con più account.

Le azioni relative all'account hanno i seguenti effetti sulla ricerca tra Esploratore di risorse AWS più account.

Resource Explorer è

Quando si disattiva Resource Explorer per un account, viene disabilitato solo per Regione AWS l'account selezionato al momento della disattivazione.

È necessario disabilitare Resource Explorer separatamente in ogni regione in cui è abilitato.

Dopo 24 ore, le risorse di questo account non verranno visualizzate nei risultati di ricerca.

Gli altri dati e impostazioni di Resource Explorer non vengono rimossi.

L'account del membro viene rimosso da un'organizzazione

Quando un account membro viene rimosso da un'organizzazione, l'account amministratore di Resource Explorer perde le autorizzazioni per visualizzare le risorse nell'account membro.

Se l'account rimosso è un account amministratore o amministratore delegato, verranno rimosse anche tutte le viste multiaccount create in precedenza da tali account.

Resource Explorer continua a funzionare in entrambi gli account.

I risultati della ricerca delle risorse non includono più le risorse di questo account.

L'account è sospeso

Quando un account viene sospesoAWS, perde le autorizzazioni per visualizzare le risorse in Resource Explorer. L'account amministratore di un account sospeso può visualizzare le risorse esistenti.

Per un account dell'organizzazione, lo stato dell'account membro può anche cambiare in Account sospeso. Ciò accade se l'account viene sospeso nello stesso momento in cui l'account amministratore tenta di abilitarlo. L'account amministratore di un account sospeso non può visualizzare le risorse relative a quell'account.

In caso contrario, lo stato di sospensione non influisce sullo stato dell'account membro.

Dopo 90 giorni, l'account viene disattivato o riattivato. Quando l'account viene riattivato, le autorizzazioni di Resource Explorer vengono ripristinate. Se lo stato dell'account membro è Account sospeso, l'account amministratore deve abilitare l'account manualmente.

L'account è chiuso

Quando un AWS account viene chiuso, Resource Explorer risponde alla chiusura come segue:

- Resource Explorer conserva le risorse dell'account per 90 giorni dalla data effettiva della chiusura dell'account. Al termine del periodo di 90 giorni, Resource Explorer elimina definitivamente tutte le risorse dell'account.

- Per conservare le risorse per più di 90 giorni, puoi utilizzare un'azione personalizzata con una EventBridge regola per archiviare le risorse in un bucket Amazon S3. Finché Resource Explorer conserva le risorse, quando riapri l'account chiuso, Resource Explorer ripristina le risorse per l'account.
- Se l'account è un account amministratore di Resource Explorer, viene rimosso come amministratore e tutti gli account dei membri vengono rimossi. Se l'account è un account membro, viene dissociato e rimosso come membro dall'account amministratore di Resource Explorer.
- Per ulteriori informazioni, consulta Chiusura di un account.

Disattivazione dell'account

Se un account rinuncia a una regione, continuerai a vedere le sue risorse nei risultati di ricerca per un massimo di 24 ore.

Dopo 24 ore, le risorse di questo account non verranno visualizzate nei risultati di ricerca. Per ulteriori informazioni, consulta Comportamenti di opt-out.

Disattivazione di Resource Explorer in un Regione AWS

Quando non hai più bisogno di cercare risorse in una regione specificaRegione AWS, puoi disattivarla solo Esploratore di risorse AWS in quella regione eliminandone l'indice. Quando si esegue questa operazione, Resource Explorer interrompe la ricerca di risorse nuove o aggiornate in quella regione. Se l'account contiene un indice di aggregazione, la replica dall'indice eliminato si interrompe e le informazioni dell'indice eliminato vengono rimosse dall'indice di aggregazione e non vengono più visualizzate nei risultati di ricerca. Possono essere necessarie fino a 24 ore prima che tutte le risorse dell'indice eliminato scompaiano dai risultati di ricerca nella regione con l'indice di aggregazione.

> **Note**
>
> Quando si registra il primoRegione AWS, Resource Explorer crea un ruolo collegato al servizio (SLR) denominato `AWSServiceRoleForResourceExplorer` in. Account AWS Resource Explorer non elimina automaticamente questa reflex. Dopo aver eliminato l'indice Resource Explorer in ogni regione dell'account, puoi utilizzare la console IAM per eliminare la reflex se non utilizzerai Resource Explorer in futuro. Se elimini il ruolo e poi scegli di riattivare Resource Explorer in almeno unoRegione AWS, Resource Explorer ricrea automaticamente il ruolo collegato al servizio.

Puoi disattivare Resource Explorer in e Regione AWS utilizzandoAWS Management Console, utilizzando i comandi in AWS Command Line Interface (AWS CLI) o utilizzando le operazioni API in un SDK. AWS

Se disattivi Resource Explorer per un account membro e il membro è visualizzato a livello di organizzazione, verrà rimosso dai risultati della ricerca con più account.

Se non desideri più supportare la ricerca di risorse in uno o più degli Regioni AWS account, esegui i passaggi indicati nella procedura seguente.

> **Note**
>
> Se l'indice che elimini è l'indice aggregatore diAccount AWS, devi attendere 24 ore prima di poter promuovere un altro indice locale come indice di aggregazione per l'account. Gli utenti non possono eseguire ricerche a livello di account utilizzando Resource Explorer finché non viene configurato un altro indice di aggregazione.

AWS Management Console

Per eliminare l'indice Resource Explorer in un Regione AWS

1. Aprire la pagina delle impostazioni di Resource Explorer.
2. Nella sezione Indici, seleziona le caselle di controllo accanto Regioni AWS agli indici che desideri eliminare, quindi scegli Elimina.
3. Nella pagina Elimina indici, verifica di aver selezionato solo gli indici che desideri eliminare. Digitate **`delete`** nella casella di testo Conferma, quindi scegliete Elimina indici.

   Resource Explorer visualizza un banner verde nella parte superiore della pagina per indicare l'esito positivo o un banner rosso se si verifica un errore con una o più aree selezionate.

AWS CLI

Per eliminare l'indice Resource Explorer in un Regione AWS

Se non desideri più supportare la ricerca di risorse in una o più delle risorse del Regioni AWS tuo account, esegui i seguenti comandi.

Esegui il comando seguente per ogni regione con gli indici che desideri eliminare. È necessario eseguire il comando nella regione con l'indice che si desidera eliminare. Il comando di esempio seguente elimina l'indice Resource Explorer negli Stati Uniti occidentali (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"
}
```

Poiché Resource Explorer esegue alcune operazioni di eliminazione come attività asincrone in background, la risposta potrebbe indicare che l'operazione è in corso. `DELETING` Questo stato indica che i processi in background non sono ancora completi. È possibile verificare il completamento finale eseguendo il comando seguente e verificando `State` la modifica in`DELETED`.

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

Disattivare completamente Resource ExplorerRegioni AWS

Se si desidera disattivarloEsploratore di risorse AWS completamente, eseguire la seguente procedura.

> **Note**
>
> Resource Explorer crea un ruolo collegato al servizio denominato AWSServiceRoleForResourceExplorer nell'account quando si crea un indice nel primoRegione AWS per un account. Resource Explorer non elimina automaticamente questo ruolo collegato al servizio. Dopo aver eliminato l'indice di Resource Explorer in ogni regione, puoi utilizzare la console IAM per eliminare il ruolo se sei sicuro di non utilizzare più Resource Explorer in future. Se elimini il ruolo e poi scegli di avviare Resource Explorer in almeno unoRegione AWS, Resource Explorer ricrea il ruolo collegato al servizio.

Disattiva Resource Explorer in tuttoRegioni AWS

È possibile disattivare Resource Explorer utilizzandoAWS Management Console, utilizzando i comandi inAWS Command Line Interface (AWS CLI) o utilizzando le operazioni API in unAWS SDK.

AWS Management Console

Se non desideri più supportare la ricerca di risorseRegione AWS in nessuna delle tue risorseAccount AWS, esegui i passaggi indicati nella procedura seguente.

Per disattivare Resource Explorer in tuttiRegioni AWS

1. Apri la pagina delle impostazioni di Resource Explorer.
2. Nella sezione Indici, seleziona le caselle di controllo accanto a tutte le registrazioniRegioni AWS, quindi scegli Elimina.

   > **Tip**
   >
   > Puoi selezionare la casella nella riga dell'intestazione della tabella accanto a Indice per selezionare le caselle per tutte le regioni in un unico passaggio.

3. Nella pagina Elimina indici, verifica di voler eliminare tutti gli indici. Digita**`delete`** nella casella di testo Conferma, quindi scegli Elimina indici.

   Resource Explorer visualizza un banner verde nella parte superiore della pagina per indicare l'esito positivo o un banner rosso se c'è un errore in una o più delle regioni selezionate.

AWS CLI

Per disattivare Resource Explorer in tuttiRegioni AWS

Se non vuoi più supportare la ricerca di risorseRegioni AWS in nessuna delle risorse del tuo account, esegui il comando seguente per trovare l'ARN di ogni indice in ciascunoRegione AWS in cui hai precedentemente attivato Resource Explorer.

```
$ 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"
]
```

Per ogni risposta, esegui il comando seguente per eliminare l'indice di Resource Explorer in quella regione.

```
$ 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"
}
```

Ripetere il comando precedente in ogni regione aggiuntiva.

Poiché Resource Explorer esegue alcune operazioni di pulizia come attività asincrone in background, la risposta potrebbe indicare che l'operazione è`DELETING`. Questo stato indica che i processi in background non sono ancora completi. È possibile verificare il completamento finale eseguendo il comando seguente e verificando lo stato in cui passare`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"
}
```

Distribuzione di Resource Explorer agli account di un'organizzazione

Utilizzando AWS CloudFormation StackSets, puoi definire e distribuire su tutti gli account gestiti in un'organizzazione daAWS Organizations. Quando si definisce un set di stack, si specificano AWS le risorse che si desidera vengano create sul proprio account Regioni AWS e su tutti gli account di destinazione specificati. Quando tutti gli account fanno parte della stessa organizzazione, puoi sfruttare l'AWS CloudFormationintegrazione con Organizations e lasciare che siano questi servizi a gestire la creazione di ruoli tra account. È possibile abilitare la distribuzione automatica in un'organizzazione, che distribuisce automaticamente le istanze dello stack su nuovi account che è possibile aggiungere all'organizzazione di destinazione o a un'unità organizzativa (OU) in futuro. Se rimuovi un account dall'organizzazione, elimina AWS CloudFormation automaticamente tutte le risorse distribuite come parte di un'istanza dello stack organizzativo. Per ulteriori informazioni su StackSets, consulta Working with AWS CloudFormation StackSets nella Guida per l'AWS CloudFormationutente.

Puoi utilizzarlo AWS CloudFormation StackSets per attivare e configurare Esploratore di risorse AWS tutti gli account dell'organizzazione, creare indici in ogni regione abilitata e creare viste dove ne hai bisogno.

> **Important**
>
> Se tenti di configurare un indice di aggregazione in una regione, devi assicurarti che l'account non disponga di un indice di aggregazione esistente in altre regioni. Dopo aver ridotto di livello un indice aggregatore a un indice locale, devi attendere 24 ore prima di poter promuovere un altro indice come nuovo indice di aggregazione per l'account.

Prerequisiti

AWS CloudFormation StackSets Per utilizzare la distribuzione di Resource Explorer negli account dell'organizzazione, l'utente o l'amministratore dell'organizzazione devono prima eseguire i seguenti passaggi per abilitare gli stack con autorizzazioni gestite dal servizio:

1. L'organizzazione deve avere tutte le funzionalità abilitate. Se l'organizzazione ha abilitato solo le funzionalità di fatturazione consolidate, non è possibile creare uno stack set con autorizzazioni gestite dal servizio.
2. Attiva l'accesso affidabile tra AWS CloudFormation e Organizations. Ciò concede l'AWS CloudFormationautorizzazione a creare i ruoli necessari nell'account di gestione dell'organizzazione e gli account dei membri AWS CloudFormation distribuiranno gli indici e le visualizzazioni di Resource Explorer.

Ora puoi creare set di stack con autorizzazioni gestite dal servizio.

> **Important**
>
> È necessario creare i set di stack nell'account di gestione dell'organizzazione. AWS CloudFormationè un servizio regionale, quindi puoi visualizzare e gestire gli stack set che crei solo dalla regione in cui li hai creati originariamente.

Creazione dei set di stack per Resource Explorer

Per implementare completamente Resource Explorer, è necessario distribuire due set di stack.

- Il primo set di stack crea l'indice di aggregazione e la visualizzazione predefinita che consente agli utenti di cercare risorse in tutte le regioni dell'account.

  Distribuisci questo stack impostato solo sulla singola regione in cui desideri creare l'indice dell'aggregatore.
- Il secondo set di stack crea un indice locale e una vista predefinita. L'indice locale replica il suo contenuto nell'indice dell'aggregatore.

  Distribuisci questo set di stack in ogni regione abilitata dell'account tranne la regione che contiene l'indice dell'aggregatore. Non scegliere alcuna regione che non sia abilitata negli account in cui distribuisci lo stack. Se lo fai, la distribuzione fallisce.

I modelli di esempio per ognuno di questi sono riportati nella sezione seguente. Per step-by-step istruzioni su come creare un set di stack utilizzando questi modelli, consulta Creare un set di stack con autorizzazioni gestite dal servizio nella Guida per l'utente. AWS CloudFormation

Dopo aver distribuito questi set di stack nell'organizzazione, ogni account all'interno dell'ambito selezionato, organizzazione o unità organizzativa, dispone di un indice aggregatore nella regione specificata e di indici locali in ogni altra regione.

Modelli di esempio AWS CloudFormation

Il seguente modello di esempio crea l'indice di aggregazione dell'account e una visualizzazione predefinita in grado di cercare risorse in tutte le regioni dell'account in cui viene distribuito un indice.

YAML

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

JSON

```
{
```

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

Il seguente modello di esempio crea un indice locale in ogni regione abilitata in tutti gli account diversi da quello con l'indice di aggregazione. Crea inoltre una visualizzazione predefinita in base alla quale gli utenti possono cercare risorse solo in quella regione. Gli utenti devono effettuare la ricerca con una vista nella regione di aggregazione per cercare risorse in tutte le regioni.

YAML

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

JSON

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

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

Gestione delle visualizzazioni di Resource Explorer per fornire l'accesso alla ricerca

Le visualizzazioni sono la chiave per cercare le tue risorse. Ogni operazione Esploratore di risorse AWS di ricerca deve utilizzare una vista.

Le visualizzazioni sono il metodo che l'amministratore può utilizzare per controllare l'accesso alle informazioni sulle risorse del proprioAccount AWS.

A una vista possono accedere solo i principali (ruoli o utenti IAM) che dispongono del permesso di utilizzare tale vista. Per eseguire correttamente la ricerca con Resource Explorer, un principale deve avere `Allow` accesso `resource-explorer-2:GetView` sia alle `resource-explorer-2:Search` operazioni che all'ARN della vista.

Le visualizzazioni contengono filtri integrati che l'amministratore può utilizzare per limitare i risultati ai soli elementi di interesse. Ad esempio, puoi creare una visualizzazione che includa solo le risorse relative a un determinato progetto. Gli utenti che non hanno bisogno di visualizzare informazioni su altri progetti possono utilizzare questa visualizzazione per visualizzare solo le risorse di interesse.

Una vista è una risorsa regionale. La vista viene creata e archiviata in uno specifico Regione AWS e restituisce nei risultati solo le informazioni dell'indice di quella regione. Per includere i risultati di tutte le regioni dell'account, la vista deve risiedere nella regione che contiene l'indice dell'aggregatore. Tale regione contiene una replica degli indici di tutte le altre regioni dell'account.

Per ulteriori informazioni sulla creazione e l'utilizzo delle viste, consulta i seguenti argomenti.

Argomenti

- Informazioni sulle visualizzazioni Resource Explorer
- Creazione di viste di Resource Explorer da utilizzare per la ricerca
- Concessione dell'accesso alle visualizzazioni di Resource Explorer per la ricerca
- Impostazione di una visualizzazione predefinita in unRegione AWS
- Aggiunta di tag alle visualizzazioni
- Condivisione delle visualizzazioni di Resource Ex
- Eliminazione delle visualizzazioni in Resource Explorer

Informazioni sulle visualizzazioni Resource Explorer

Esploratore di risorse AWSindicizza le risorse in background e quindi rende tale indice disponibile per l'interrogazione. È possibile eseguire interrogazioni di ricerca per le risorse utilizzando l'API Resource Explorer documentata in questa guida o utilizzando la console Resource Explorer. Resource Explorer utilizza la sua API per fornire un'interfaccia grafica interattiva a quella che altrimenti sarebbe solo un'API accessibile a livello di programmazione. I concetti descritti in questo argomento si applicano sia all'API che alla console.

Una vista è archiviata in unRegione AWS e restituisce risultati solo dall'indice di quella regione.

Poiché l'amministratore potrebbe voler limitare l'accesso alle informazioni contenute nell'indice delle risorse, gli indici stessi non sono direttamente accessibili. Tutte le ricerche devono invece passare attraverso una visualizzazione per la quale l'utente deve disporre dell'autorizzazione alla ricerca.

Ci sono diversi elementi chiave per ogni visualizzazione:

Autorizzazioni alla ricerca

È possibile utilizzare criteri diAWS autorizzazione standard per controllare chi può utilizzare ciascuna visualizzazione. Ciò è fornito dalle politiche di autorizzazione basate sull'identità allegate ai principi che offrono un controllo granulare su chi può visualizzare le informazioni fornite da ciascuna visualizzazione. Ad esempio, puoi concedere l'accesso alla`Production-resources` vista per consentire la ricerca solo da parte dei tecnici che gestiscono i tuoi servizi di produzione. Quindi, puoi concedere diverse autorizzazioni alla`Pre-production-resources` visualizzazione per consentire ai tuoi sviluppatori di cercare risorse di preproduzione.

Se utilizzi la politicaAWS gestita indicata`AWSResourceExplorerReadOnlyAccess` con i tuoi responsabili, concede loro la possibilità di effettuare ricerche utilizzando qualsiasi visualizzazione dell'account.

In alternativa, puoi creare la tua politica delle autorizzazioni e concedere le autorizzazioni seguenti solo per le visualizzazioni specificate:

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

Per fornire l'accesso, aggiungi autorizzazioni ai tuoi utenti, gruppi o ruoli:

- Utenti e gruppi in AWS IAM Identity Center:

Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center.

- Utenti gestiti in IAM tramite un provider di identità:

  Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina Creating a role for a third-party identity provider (federation) (Creazione di un ruolo per un provider di identità di terze parti [federazione]) nella Guida per l'utente di IAM.

- Utenti IAM:
  - Crea un ruolo che l'utente possa assumere. Per istruzioni, consulta la pagina Creating a role for an IAM user (Creazione di un ruolo per un utente IAM) nella Guida per l'utente di IAM.
  - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente di IAM.

Per ulteriori informazioni sulle autorizzazioni relative alle visualizzazioni, consultareConcessione dell'accesso alle visualizzazioni di Resource Explorer per la ricerca.

Filtrare la ricerca

Una vista funge da finestra virtuale attraverso la quale l'utente può vedere le risorse dell'account. È possibile creare più viste, ognuna delle quali presenta una vista diversa dell'immagine più grande. Ad esempio, puoi creare una vista che consenta di cercare solo le risorse associate al tuo ambiente di preproduzione, identificate dai tag allegati alle tue risorse. Quindi, puoi creare una vista separata che consenta di cercare solo le risorse nel tuo ambiente di produzione, in base a diversi valori nei tag. Se si configurano più viste con`FilterString` valori diversi, non è necessario reinserire i parametri di interrogazione ogni volta che si esegue la ricerca.

Le visualizzazioni possono anche specificare quali informazioni opzionali sulle risorse includere nei risultati. L'elenco predefinito di campi è sempre incluso nei risultati. Oltre all'elenco predefinito, puoi richiedere che la visualizzazione includa anche eventuali tag allegati alla risorsa .

Ambito della ricerca

- Ambito della regione: quando si esegue una ricerca in eRegione AWS con Resource Explorer, i risultati possono includere solo le risorse indicizzate in quella regione. L'indice nella maggior parte delle regioni è etichettato`LOCAL` perché contiene informazioni sulle risorse della sola regione. Le ricerche in quelle regioni possono restituire solo quelle risorse.
- Ambito dell'account: puoi promuovere un indice locale come indice aggregatore per l'account. Quando si esegue questa operazione, tutte le altre regioni in cui Resource Explorer è attivato

replicano le informazioni relative all'indice nella Regione con l'indice aggregatore. Se effettui una ricerca in quella regione, questi risultati includono le risorse di tutte le regioni dell'account. Quando si utilizza l'opzione Configurazione rapida per configurare il server, Resource Explorer crea automaticamente un indice aggregatore nella regione specificata. Inoltre, l'opzione Configurazione rapida crea una visualizzazione predefinita in quella regione per supportare la ricerca di tutte le risorse dell'account in tutte le regioni.

Visualizzazioni predefinite

Se un utente tenta di effettuare una ricerca senza specificare esplicitamente una vista, Resource Explorer utilizza la visualizzazione predefinita definita per tale visualizzazioneRegione AWS.

Se non esiste una vista predefinita per quella regione e l'utente non ha specificato una vista da utilizzare, la ricerca fallisce e genera un'eccezione.

Resource Explorer crea automaticamente una vista predefinita come segue:

- Se si attiva Resource Explorer utilizzandoAWS Management Console e si sceglie l'opzione Configurazione rapida, è necessario specificare quale regione contiene l'indice aggregatore per l'account. Resource Explorer crea automaticamente una vista predefinita nella regione dell'indice aggregatore specificata.
- Se registri Resource Explorer utilizzandoAWS Management Console e scegli l'opzione Configurazione avanzata, puoi facoltativamente scegliere di creare l'indice aggregatore per l'account in una regione specificata. Se si esegue questa operazione, Resource Explorer crea automaticamente una vista predefinita nella regione dell'indice aggregatore.
- Se si registra Resource Explorer utilizzando la console e si sceglie di non registrare un indice aggregatore Region, Resource Explorer crea una vista predefinita per l'indice locale in ciascuna regione.
- Se registri Resource Explorer utilizzando le operazioniAWS CLI o le API, Resource Explorer non crea automaticamente una vista predefinita. È invece necessario configurare manualmente la visualizzazione predefinita per ciascuna regione da cui si prevede che gli utenti effettuino la ricerca.

Creazione di viste di Resource Explorer da utilizzare per la ricerca

Tutte le ricerche devono utilizzare una visualizzazione. Una vista definisce i filtri che determinano quali risorse possono essere restituite dalle query che utilizzano la vista. Le visualizzazioni controllano anche chi può cercare risorse.

Una visualizzazione è archiviata in un Regione AWS file e restituisce i risultati della ricerca solo dall'indice di quella regione. Se la regione contiene l'indice dell'aggregatore, la vista restituisce i risultati della ricerca dall'indice in ogni regione dell'account.

Le visualizzazioni multiaccount consentono di cercare risorse negli account dell'organizzazione. Qualsiasi account che desideri cercare richiede degli indici. Solo l'account di gestione o un amministratore delegato dell'organizzazione possono creare una visualizzazione multiaccount.

Esploratore di risorse AWS può creare una vista predefinita durante la configurazione iniziale se sono state scelte le opzioni pertinenti in Quick Setup for Resource Explorer nella console Systems Manager o nella configurazione avanzata. In qualsiasi momento successivo, è possibile creare viste aggiuntive con filtri diversi per diversi set di utenti.

Puoi creare una vista utilizzando AWS Management Console o eseguendo AWS CLI comandi o operazioni API equivalenti in un AWS SDK.

Autorizzazioni minime

Per eseguire questa procedura, è necessario disporre delle seguenti autorizzazioni:

- Operazione: `resource-explorer-2:CreateView`

  Risorsa: Ciò può consentire * la creazione di una vista Regione AWS in qualsiasi parte dell'account.

AWS Management Console

Per creare una vista

1. Apri la pagina Visualizzazioni della console Resource Explorer e scegli Crea visualizzazione.
2. Nella pagina Crea visualizzazione, in Nome, inserisci un nome per la visualizzazione.

   Il nome non deve superare i 64 caratteri e può includere lettere, cifre e il trattino (-). Il nome deve essere univoco all'interno del suo. Regione AWS
3. Scegliete il formato Regione AWS in cui desiderate creare la vista. Per creare una visualizzazione che restituisca le risorse di tutte le regioni dell'account, scegli Regione AWS quella che contiene l'indice dell'aggregatore.
4. (Facoltativo) Per Scope, scegli se la ricerca restituisce risorse multi-account o restituisce solo le risorse del tuo account. L'ambito a livello di account è l'impostazione predefinita.

Solo l'account di gestione o l'amministratore delegato possono visualizzare l'opzione per creare una visualizzazione multiaccount.

5. Scegli se filtrare i risultati.

   - Includi tutte le risorse

     Non sono inclusi filtri di interrogazione. Tutte le risorse dell'indice associato alla vista possono essere restituite nei risultati di ricerca.

   - Includi solo le risorse che corrispondono a un filtro specificato

     Attiva la casella di controllo Filtri di risorse in cui è possibile scegliere i nomi e gli operatori dei filtri. Per una spiegazione di ciascuno dei nomi e degli operatori di filtro disponibili, consultaFiltri.

   - Scegliete gli attributi opzionali delle risorse da includere nei risultati da questa vista. Seleziona la casella di controllo accanto a Tag per consentire agli utenti di cercare risorse in base ai nomi e ai valori delle chiavi dei tag. Se non includi tag nella vista, gli utenti non possono effettuare richieste di ricerca che utilizzano chiavi e valori dei tag per filtrare ulteriormente i risultati.
   - Facoltativamente, puoi allegare tag alla vista. Espandi la casella Tag e inserisci fino a 50 coppie chiave/valore del tag. Puoi utilizzare i tag per classificare le risorse o come parte di una strategia di autorizzazione di sicurezza per il controllo degli accessi basato sugli attributi (ABAC). Per ulteriori informazioni, consulta Aggiunta di tag alle visualizzazioni.
   - Scegli Crea visualizzazione.

   La console torna alla pagina di ricerca in cui è possibile utilizzare la nuova visualizzazione per eseguire una ricerca.

   Passaggio successivo: concedi ai principali del tuo account le autorizzazioni per effettuare ricerche con la nuova visualizzazione. Per ulteriori informazioni, consultare Concessione dell'accesso alle visualizzazioni di Resource Explorer per la ricerca

AWS CLI

Per creare una visualizzazione

Eseguite il comando seguente per creare una vista nell'area specificata Regione AWS. L'esempio seguente crea una visualizzazione che restituisce solo le risorse relative al servizio Amazon EC2 contrassegnate con una `Stage` chiave e il valore. `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"
    }
}
```

Per creare una visualizzazione a livello di organizzazione

L'esempio seguente crea una visualizzazione che restituisce le risorse provenienti da tutta l'organizzazione. Questa operazione deve essere eseguita dall'account di gestione dell'organizzazione o da un account amministratore delegato.

1. Esegui il `aws organizations describe-organization` comando per ottenere l'ARN della tua organizzazione.
2. Esegui il comando seguente per creare una vista per l'organizzazione specificata.

```
$ 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"
    }
}
```

Per creare una visualizzazione a livello di unità organizzativa

L'esempio seguente crea una visualizzazione che restituisce le risorse di tutti i membri di questa unità organizzativa. Questa visualizzazione si comporta in modo simile a una visualizzazione a livello organizzativo. Questa operazione deve essere eseguita dall'account di gestione dell'organizzazione o da un account amministratore delegato.

1. Esegui il `aws organizations describe-organizational-unit` comando per ottenere l'ARN della tua organizzazione.
2. Esegui il comando seguente per creare una vista per l'unità organizzativa specificata.

```
$ 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"
    }
}
```

Passaggio successivo: concedi ai principali del tuo account le autorizzazioni per effettuare ricerche con la nuova visualizzazione. Per ulteriori informazioni, consulta Concessione dell'accesso alle visualizzazioni di Resource Explorer per la ricerca

Concessione dell'accesso alle visualizzazioni di Resource Explorer per la ricerca

Prima che gli utenti possano effettuare una ricerca con una nuova visualizzazione, è necessario concedere l'accesso alleEsploratore di risorse AWS visualizzazioni. A tale scopo, utilizza una politica di autorizzazione basata sull'identità per i responsabiliAWS Identity and Access Management (IAM) che devono eseguire la ricerca con la vista.

Per fornire l'accesso, aggiungi autorizzazioni ai tuoi utenti, gruppi o ruoli:

- Utenti e gruppi in AWS IAM Identity Center:

  Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center.
- Utenti gestiti in IAM tramite un provider di identità:

  Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina Creating a role for a third-party identity provider (federation) (Creazione di un ruolo per un provider di identità di terze parti [federazione]) nella Guida per l'utente di IAM.
- Utenti IAM:
  - Crea un ruolo che l'utente possa assumere. Per istruzioni, consulta la pagina Creating a role for an IAM user (Creazione di un ruolo per un utente IAM) nella Guida per l'utente di IAM.
  - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente di IAM.

Puoi utilizzare uno dei seguenti metodi:

- Utilizza una politicaAWS gestita esistente. Resource Explorer fornisce diverse politicheAWS gestite predefinite da utilizzare. Per i dettagli di tutte le politicheAWS gestite disponibili, vedereAWS politiche gestite per Esploratore di risorse AWS.

  Ad esempio, è possibile utilizzare la`AWSResourceExplorerReadOnlyAccess` politica per concedere autorizzazioni di ricerca a tutte le visualizzazioni dell'account.

- Crea la tua politica di autorizzazione e assegnala ai responsabili. Se crei la tua politica, puoi limitare l'accesso a una singola vista o a un sottoinsieme delle viste disponibili specificando il nome della risorsa Amazon (ARN) di ciascuna vista nell'`Resource`elemento della dichiarazione sulla politica. Ad esempio, è possibile utilizzare la seguente politica di esempio per concedere al committente la possibilità di effettuare ricerche utilizzando solo quella vista.

```
{
    "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
        }
    ]
}
```

  Usa la console IAM per creare le politiche di autorizzazione e utilizzarle con i responsabili che necessitano di tali autorizzazioni. Per ulteriori informazioni sui criteri di autorizzazione IAM, consulta i seguenti argomenti:

  - Criteri e autorizzazioni in IAM
  - Aggiunta e rimozione di autorizzazioni per identità IAM
  - Informazioni sulle autorizzazioni concesse da una policy

Utilizzo dell'autorizzazione basata sui tag per controllare l'accesso alle visualizzazioni

Se scegli di creare più viste con filtri che restituiscono risultati solo con determinate risorse, potresti voler limitare l'accesso a tali viste solo ai responsabili che devono visualizzare tali risorse. Puoi fornire questo tipo di sicurezza per le visualizzazioni del tuo account utilizzando una strategia di controllo degli accessi basata sugli attributi (ABAC). Gli attributi utilizzati da ABAC sono i tag associati sia ai responsabili che tentano di eseguire operazioniAWS sia alle risorse a cui tentano di accedere.

ABAC utilizza le politiche di autorizzazione IAM standard allegate ai committenti. Le politiche utilizzano`Condition` gli elementi delle dichiarazioni politiche per consentire l'accesso solo quando sia i tag allegati al committente richiedente che i tag allegati alla risorsa interessata soddisfano i requisiti della politica.

Ad esempio, puoi allegare un tag`"Environment" = "Production"` a tutte leAWS risorse che supportano l'applicazione di produzione dell'azienda. Per garantire che solo i responsabili autorizzati ad accedere all'ambiente di produzione possano vedere tali risorse, crea una vista Resource Explorer che utilizzi quel tag come filtro. Quindi, per limitare l'accesso alla vista solo ai principali principali appropriati, si concedono le autorizzazioni utilizzando una politica con una condizione simile ai seguenti elementi di esempio.

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

Ciò`Condition` nell'esempio precedente specifica che la richiesta è consentita solo se il`Environment` tag allegato al committente che effettua la richiesta corrisponde al`Environment` tag allegato alla risorsa specificata nella richiesta. Se questi due tag non corrispondono esattamente o se uno dei tag è mancante, Resource Explorer nega la richiesta.

> **Important**
>
> Per utilizzare con successo ABAC per proteggere l'accesso alle tue risorse, devi prima limitare l'accesso alla possibilità di aggiungere o modificare i tag allegati ai tuoi presidi e alle

tue risorse. Se un utente può aggiungere o modificare i tag associati a unAWS principale o a una risorsa, tale utente può influire sulle autorizzazioni controllate da tali tag. In un ambiente ABAC sicuro, solo gli amministratori di sicurezza approvati hanno il permesso di aggiungere o modificare i tag allegati ai responsabili e solo gli amministratori della sicurezza e i proprietari delle risorse possono aggiungere o modificare i tag allegati alle risorse.

Per ulteriori informazioni su come implementare con successo una strategia ABAC, consulta i seguenti argomenti nella Guida per l'utente di IAM:

- Tutorial IAM: Definire le autorizzazioni per accedere alleAWS risorse in base ai tag
- Controllo dell'accesso alleAWS risorse mediante i tag

Dopo aver installato l'infrastruttura ABAC necessaria, puoi utilizzare start using tag per controllare chi può effettuare ricerche utilizzando le visualizzazioni Resource Explorer del tuo account. Per esempio le policy che illustrano il principio, consulta i seguenti esempi di policy di autorizzazione:

- Concessione dell'accesso a una visualizzazione basata su tag
- Concedere l'accesso per creare una vista basata sui tag

Impostazione di una visualizzazione predefinita in unRegione AWS

InEsploratore di risorse AWS, è possibile definire molte visualizzazioni in unaRegione AWS, in cui ogni vista soddisfa requisiti di ricerca diversi. Ti consigliamo di impostare una vista in ogni regione come vista predefinita per quella regione.

Resource Explorer utilizza la vista predefinita ogni volta che un utente esegue una ricerca e non specifica esplicitamente quale visualizzazione utilizzare. La barra di ricerca unificata nella parte superiore di ogniAWS Management Console pagina utilizza automaticamente anche la vista predefinita nella regione che contiene l'indice di aggregazione per trovare le risorse che corrispondono alla query di ricerca dell'utente.

È possibile selezionare solo una vista esistente nella regione come visualizzazione predefinita di quella regione. Se un'altra area ha una vista che desideri utilizzare, devi prima creare una copia di quella vista nella regione in cui desideri renderla la vista predefinita.

> **Tip**
>
> Non è disponibile alcuna operazione di copia e visualizzazione. È necessario creare una vista nella regione di destinazione e quindi copiare le impostazioni dalla vista esistente alla nuova vista.

È possibile specificare una vista come predefinita per la relativa regione utilizzandoAWS Management Console o eseguendoAWS CLI comandi o operazioni API equivalenti in unAWS SDK.

AWS Management Console

Per impostare una

1. Nella pagina Visualizzazioni di Resource Explorer, scegli il pulsante di opzione accanto alla vista che desideri impostare come predefinita per la relativa regione.
2. Scegli Azioni, quindi scegli Imposta come predefinito.

AWS CLI

Per impostare una

Eseguire il comando seguente per impostare la L'esempio seguente imposta la vista specificata come predefinita per tutte le ricerche eseguite nella regione us-east-1 . La

```
$ 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"
}
```

Aggiunta di tag alle visualizzazioni

Puoi aggiungere tag alle tue visualizzazioni per classificarle. I tag sono metadati forniti dal cliente che assumono la forma di una stringa del nome chiave e di una stringa di valore opzionale associata. Per

informazioni generali sull'assegnazione di tagAWS alle risorse, vedere TaggingAWS Resources in Riferimenti generali di Amazon Web Services.

Aggiungi tag alle tue visualizzazioni

È possibile aggiungere tag alle visualizzazioni di Resource Explorer utilizzandoAWS Management Console o eseguendoAWS CLI comandi o le relative operazioni API equivalenti in unAWS SDK.

AWS Management Console

Per aggiungere tag a una visualizzazione

1. Apri la pagina Visualizzazioni di Resource Explorer e scegli il nome della vista a cui desideri assegnare un tag per visualizzarne la pagina Dettagli.
2. In Tag, scegli Gestisci tag.
3. Per aggiungere un tag, seleziona Aggiungi tag, quindi inserisci un nome di chiave e un valore opzionale per il tag.

   > **Note**
   >
   > Puoi anche eliminare un tag scegliendo la X accanto al tag.

   Puoi associare fino a 50 tag definiti dall'utente a una risorsa. Tutti i tag creati e gestiti automaticamente daAWS non vengono conteggiati in questa quota.
4. Quando hai finito con tutte le modifiche ai tag, scegli Salva modifiche.

AWS CLI

Per aggiungere tag a una visualizzazione

Eseguire il comando riportato di seguito per aggiungere tag a una vista. L'esempio seguente aggiunge tag con il nome della chiave`environment` e il valore`production` alla vista specificata.

```
$ 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
```

Se ha esito positivo, il comando precedente non produrrà alcun output.

> **Note**
>
> Per rimuovere un tag esistente da una vista, usa il`untag-resource` comando.

Controllo delle autorizzazioni tramite tag

Uno degli usi principali dei tag consiste nel supportare una strategia di controllo di accesso basato su attributi (ABAC). ABAC può aiutarti a semplificare la gestione delle autorizzazioni consentendoti di etichettare le risorse. Quindi, concedi l'autorizzazione agli utenti per le risorse etichettate in un determinato modo.

Considera ad esempio questo scenario. Per una vista chiamata`ViewA`, si allega il tag`environment=prod` (nome chiave=valore). Un altro`ViewB` potrebbe essere taggato`environment=beta`. Taggate i ruoli e gli utenti con gli stessi tag e valori, in base all'ambiente a cui ogni ruolo o utente dovrebbe poter accedere.

Quindi, puoi assegnare una politica di autorizzazioneAWS Identity and Access Management (IAM) ai tuoi ruoli, gruppi e utenti IAM. La politica concede l'autorizzazione all'accesso e alla ricerca utilizzando una vista solo se il ruolo o l'utente che effettua la richiesta di ricerca ha un`environment` tag con lo stesso valore del`environment` tag associato alla vista.

Il vantaggio di questo approccio è che è dinamico e non richiede di mantenere un elenco di chi ha accesso a quali risorse. Ti assicuri invece che tutte le risorse (le tue visualizzazioni) e i principali (ruoli e utenti IAM) siano etichettati correttamente. Quindi, le autorizzazioni si aggiornano automaticamente senza che sia necessario modificare alcuna politica.

Riferimenti ai tag in una politica ABAC

Dopo aver contrassegnato le visualizzazioni, puoi scegliere di utilizzare tali tag per controllare l'accesso dinamico a tali viste. La seguente politica di esempio presuppone che sia i responsabili IAM che i punti di vista siano contrassegnati con la chiave del tag`environment` e un valore. Fatto ciò, puoi collegare ai tuoi dirigenti la seguente policy di esempio. I tuoi ruoli e gli utenti possono quindi`Search` utilizzare qualsiasi vista contrassegnata con un valore di`environment` tag che corrisponde esattamente al`environment` tag associato al principale.

```
{
```

```
    "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}"
                }
            }
        }
    ]
}
```

Se sia il principale che la vista hanno il`environment` tag ma i valori non corrispondono, o se uno dei due manca il`environment` tag, Resource Explorer nega la richiesta di ricerca.

Per ulteriori informazioni sull'utilizzo di ABAC per concedere l'accesso sicuro alle risorse, consulta A cosa serve ABACAWS?

Condivisione delle visualizzazioni di Resource Ex

Le visualizzazioni utilizzano Esploratore di risorse AWS principalmente politiche basate sulle risorse per concedere l'accesso. Analogamente alle policy dei bucket di Amazon S3, queste policy sono allegate alla vista e specificano chi può utilizzarla. Ciò è in contrasto con le politiche basate sull'identità AWS Identity and Access Management (IAM). Una policy basata sull'identità IAM viene assegnata a un ruolo, gruppo o utente e specifica a quali azioni e risorse può accedere quel ruolo, gruppo o utente. Puoi utilizzare entrambi i tipi di policy con le viste di Resource Explorer, come segue:

- All'interno dell'account di gestione o dell'account amministratore delegato proprietario della risorsa, utilizza uno dei due tipi di policy per concedere l'accesso, a condizione che nessun altro criterio neghi esplicitamente l'accesso alla vista per quel principale.
- In tutti gli account, è necessario utilizzare entrambi i tipi di policy. La politica basata sulle risorse allegata alla visualizzazione nell'account di condivisione attiva la condivisione con un altro account utente. Tuttavia, tale politica non concede l'accesso ai singoli utenti o ruoli nell'account utente.

L'amministratore dell'account utente deve inoltre assegnare una politica basata sull'identità ai ruoli e agli utenti desiderati nell'account utente. Questa politica garantisce l'accesso al nome di risorsa Amazon (ARN) della vista.

Per condividere le visualizzazioni con altri account, devi usare AWS Resource Access Manager ()AWS RAM. AWS RAMgestisce per te la complessità delle politiche basate sulle risorse. Prima di poter condividere, devi seguire questi passaggi per attivare la ricerca su più account.

Per condividere una visualizzazione, devi essere l'account di gestione dell'organizzazione o un amministratore delegato. Specificate gli account o le identità con cui volete condividere la risorsa. AWS RAMsupporta completamente le visualizzazioni di Resource Explorer. AWS RAMutilizza politiche simili a quelle descritte nelle sezioni seguenti, in base ai tipi di principali con cui scegli di condividere. Per istruzioni su come condividere le risorse, consulta Condivisione AWS delle risorse nella Guida per l'AWS Resource Access Managerutente.

Gli amministratori e gli amministratori delegati possono creare e condividere 3 tipi di visualizzazioni: visualizzazione dell'ambito dell'organizzazione, viste dell'ambito dell'unità organizzativa (OU) e viste dell'ambito a livello di account. Possono condividerle con organizzazioni, unità organizzative o account. Quando gli account entrano o escono dall'organizzazione, concede o revoca AWS RAM automaticamente la visualizzazione condivisa.

Politica di autorizzazione con cui condividere la visualizzazione Account AWS

La seguente politica di esempio mostra come rendere disponibile una vista ai principali in due modi diversi: Account 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"}
            }
        }
    ]
    }"
}
```

L'amministratore di ciascuno degli account specificati deve ora specificare quali ruoli e utenti possono accedere alla vista allegando politiche di autorizzazione basate sull'identità a ruoli, gruppi e utenti. Gli amministratori degli account 111122223333 o 444455556666 possono creare la seguente politica di esempio. Quindi, possono assegnare la politica a ruoli, gruppi e utenti di quegli account che devono essere autorizzati a effettuare ricerche utilizzando la visualizzazione condivisa dall'account di origine.

```
{
    "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"
        }
    ]
}
```

Puoi utilizzare queste policy basate sull'identità IAM come parte di una strategia di sicurezza ABAC (Attribute-Based Access Control). In questo paradigma, ti assicuri che tutte le tue risorse e tutte le tue identità siano etichettate. Quindi, specificate nelle vostre politiche quali chiavi e valori dei tag devono corrispondere tra l'identità e la risorsa affinché l'accesso sia consentito. Per informazioni su come aggiungere tag alle viste nel tuo account, consultaAggiunta di tag alle visualizzazioni. Per ulteriori informazioni sul controllo degli accessi basato sugli attributi, consulta A cosa serve ABAC? AWS e Controllo dell'accesso alle AWS risorse tramite tag, entrambi nella IAM User Guide.

Eliminazione delle visualizzazioni in Resource Explorer

Puoi eliminare unaEsploratore di risorse AWS visualizzazione di cui non hai più bisogno. È possibile eliminare le visualizzazioni utilizzandoAWS Management Console o eseguendoAWS CLI comandi o operazioni API equivalenti in unAWS SDK.

> **Note**
>
> Non è possibile eliminare una visualizzazione attualmente designata come predefinitaRegione AWS. Per eliminare la vista, è necessario rimuovere la vista come predefinita. Per fare ciò, è possibile eseguire l'operazione DisassociateDefaultViewAPI in quella regione.

Autorizzazioni minime

Per eseguire questa procedura, è necessario disporre delle autorizzazioni seguenti:

- Operazione: `resource-explorer-2:DeleteView`

  Risorsa: L'ARN della vista da eliminare

AWS Management Console

Per eliminare una vista

1. Nella pagina Visualizzazioni della console di Resource Explorer, completa il pulsante di opzione accanto alla visualizzazione che desideri eliminare.
2. Scegli Actions (Operazioni), quindi Delete (Elimina).
3. Nella finestra di dialogo di conferma, immettere il nome della vista, quindi scegliere Delete (Elimina).

AWS CLI

Per eliminare una vista

Eseguire il seguente comando per eliminare la vista con l'Amazon Resource Name (ARN) specificato.

```
$ 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"
}
```

UsandoEsploratore di risorse AWSper cercare risorse

Lo scopo principale di abilitareEsploratore di risorse AWSnel tuoAccount AWSconsente agli utenti di cercare risorse nell'account. Usa ilAWS Management Consoleo ilAWS Command Line Interface(AWS CLI) per cercare risorse utilizzando Resource Explorer.

Di seguito sono riportate alcune delle caratteristiche principali della ricerca in Resource Explorer.

- Ogni ricerca deve utilizzare una vista.

  La visualizzazione è quella utilizzata da Resource Explorer per determinare chi dispone delle autorizzazioni per visualizzare quali risorse. Per utilizzare una vista in un'operazione di ricerca di Resource Explorer, l'utente deve disporre di`Allow`sul`resource-explorer-2:Search`operazione per la vista specificata. Questa autorizzazione proviene da unpolitica di autorizzazione basata sull'identitàallegato al preside che effettua la richiesta.

  La vista può includere un filtro che limita le risorse che possono essere incluse nei risultati. Creando viste diverse che utilizzano filtri e concedendo a diversi utenti l'accesso a diverse visualizzazioni, è possibile configurare un ambiente in cui ogni gruppo di utenti può visualizzare solo le risorse pertinenti.

  Per ulteriori informazioni sulle visualizzazioni, vedereGestione delle visualizzazioni di Resource Explorer per fornire l'accesso alla ricerca.
- Resource Explorer utilizza processi asincroni in background per mantenere i propri indici.

  I processi di indicizzazione possono impiegare del tempo a Resource Explorer per rilevare le risorse appena create o modificate e aggiungerle all'indice locale. Resource Explorer può impiegare più tempo per replicare le modifiche negli indici locali nell'indice aggregatore.

  Lo stesso vale per le risorse che elimini. Dopo l'eliminazione di una risorsa può essere necessario del tempo prima che tale eliminazione venga rilevata dal processo di indicizzazione e che le relative informazioni vengano rimosse dall'indice locale. È necessario più tempo affinché Resource Explorer replichi l'eliminazione dall'indice locale all'indice aggregatore dell'account.

  Le aggiunte, le modifiche e le eliminazioni alle tue risorse possono richiedere fino a un massimo di 36 ore affinché Resource Explorer mostri tali modifiche nei risultati di ricerca in tutte le regioni in cui hai attivato Resource Explorer.
- Una ricerca in Resource Explorer avviene all'interno di unRegione AWS.

Ogni regione in cui attivi Resource Explorer contiene un indice delle sole risorse archiviate in quella regione. Le visualizzazioni sono anche associate alle regioni e possono restituire solo le risorse presenti nell'indice di quella regione. L'unica eccezione è l'indice aggregatore, che riceve una copia replicata di tutti gli indici locali per supportare la ricerca in tutte le regioni dell'account.

- La ricerca interregionale richiede un indice aggregatore per l'account.

  Per consentire agli utenti di cercare risorse in tutto il mondoRegioni AWS, l'amministratore deve designare una regione per contenere l'indice aggregatore dell'account. Una copia di ogni indice locale viene replicata automaticamente nell'indice aggregatore.

  Per questo motivo, solo le viste nell'indice aggregatore Region possono restituire risultati che includono risorse provenienti da tuttiRegioni AWSnell'account.

- Una query è composta da un numero qualsiasi di parole chiave e filtri di testo in formato libero.

  Le parole chiave in formato libero vengono combinate nella query utilizzando la logica**OR**operatori. Filtri che utilizzano nomi di filtro definiti da Resource Explorersono combinati nella query utilizzando la logica**AND**operatori. Considerate la seguente query di esempio.

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

  Questo viene valutato da Resource Explorer come segue.

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

  Questa query richiede che le risorse corrispondenti siano risorse Amazon EC2 nella regione Stati Uniti occidentali (Oregon) e contenere almeno una delle parole chiave (test,istanza) allegati in qualche modo, ad esempio nel nome, nella descrizione o nei tag.

> **Note**
>
> A causa dell'implicitoAND, è possibile utilizzare correttamente un solo filtro per un attributo che può avere un solo valore associato alla risorsa. Ad esempio, una risorsa può far parte di una solaRegione AWS. Pertanto, la seguente query non restituisce alcun risultato.
>
> ```
> region:us-east-1 region:us-west-1
> ```

Questa limitazione fanonsi applicano ai filtri per gli attributi che possono avere più valori contemporaneamente, ad esempio`tag:`,`tag.key:`, `etag.value:`.

- Una ricerca può restituire solo i primi 1.000 risultati.

  Questo requisito include una ricerca con una stringa di query vuota che corrisponde a tutte le risorse. Per visualizzare le risorse superiori alle 1.000 restituite da una stringa di query vuota, devi utilizzare le query per limitare i risultati corrispondenti a quelli che desideri visualizzare e limitare il numero di corrispondenze a meno di 1.000.
- Esiste una quota per account sul numero di operazioni di ricerca che è possibile eseguire.

  Le quote limitano il numero di query che è possibile effettuare al secondo e il numero di query che è possibile effettuare ogni mese. Per numeri di quota specifici, vedereQuote per Resource Explorer.

AWS Management Console

Per cercare risorse utilizzando Resource Explorer

1. SulRicerca di risorsepagina, inizia scegliendo la vista che desideri utilizzare. Puoi scegliere solo tra le visualizzazioni per le quali disponi delle autorizzazioni di accesso.
2. PerInterrogazione, inserisci i termini di ricerca efiltriche identificano le risorse che vuoi vedere. Per informazioni su tutte le opzioni di sintassi disponibili, vedereRiferimento alla sintassi delle query di ricerca per Resource Explorer.
3. PremereEntraper inviare la tua richiesta.

   Resource Explorer mostra tutti i risultati che corrispondono a entrambi`Filter`definito nella vista e nellInterrogazioneche fornisci. I risultati vengono ordinati in base alla pertinenza: le risorse che corrispondono a un numero maggiore di termini di ricerca vengono visualizzate più in alto nell'elenco e le risorse che corrispondono a meno termini vengono visualizzate più in basso nell'elenco.
4. Scegli l'identificatore di una risorsa per accedere alla console nativa di quel tipo di risorsa, dove puoi interagire con la risorsa in tutti i modi supportati da quel servizio.

AWS CLI

Per cercare risorse utilizzando Resource Explorer

Esegui il comando seguente per cercare risorse utilizzando la vista specificata. Tale visualizzazione deve esistere nella regione in cui si esegue l'operazione. L'esempio seguente cerca le istanze Amazon EC2 che sono contrassegnateenv=productionnegli Stati Uniti orientali (Ohio) (us-east-2). Per informazioni su tutte le opzioni di sintassi disponibili perquery-stringparametro, vediRiferimento alla sintassi delle query di ricerca per Resource Explorer.

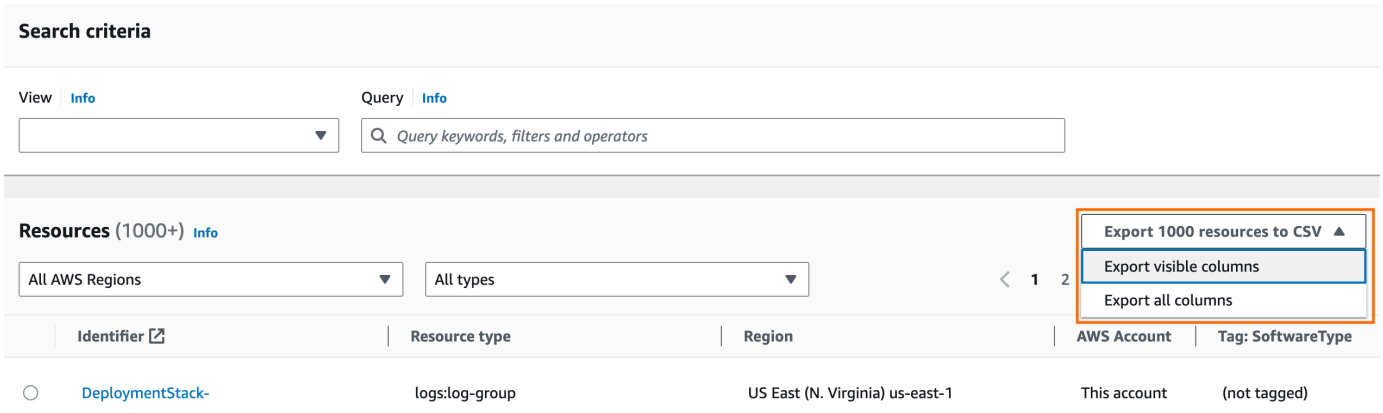
```
$ aws resource-explorer-2 search \
    --region us-east-1 \
    --query-string "resourcetype:AWS::EC2::Instance tag:env=production"
    --view-arn arn:aws:resource-explorer-2:us-east-2:123456789012:view/My-Resources-View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

Esporta i risultati della ricerca in un file.csv

È possibile esportare i risultati di unRicerca di risorseinterroga un file con valori separati da virgole (.csv). Il file.csv include l'identificatore, il tipo di risorsa, la regione,Account AWS, il numero totale di tag e una colonna per ogni chiave di tag univoca nella raccolta. Il file.csv può aiutarti a configurare il tuoAWSrisorse della tua organizzazione o determina dove vi sono sovrapposizioni o incongruenze nell'assegnazione di tag tra le risorse.

1. Nei risultati del tuoRicerca di risorseinterroga, scegliEsporta risorse in formato CSV.

   Puoi scegliere di esportare i risultati solo con le colonne che puoi visualizzare attualmente o esportare con tutte le colonne disponibili.



2. Quando richiesto dal browser, scegli di aprire il file.csv o di salvarlo in una posizione comoda.

Riferimento alla sintassi delle query di ricerca per Resource Explorer

Esploratore di risorse AWS ti aiuta a trovare AWS risorse individuali nel tuo Account AWS. Per aiutarti a trovare esattamente le risorse che stai cercando, Resource Explorer accetta stringhe di query di ricerca che supportano la sintassi descritta in questo argomento. Per le query ad esempio che dimostrano come utilizzare le funzionalità descritte qui, vedi. Esempi di query di ricerca in Resource Explorer

> **Note**
>
> Al momento, i tag allegati alle risorse AWS Identity and Access Management (IAM), come ruoli o utenti, non sono indicizzati.

Come funzionano le interrogazioni in Resource Explorer

Le query di ricerca utilizzano sempre una visualizzazione. Se non ne specifichi una in modo esplicito, Resource Explorer utilizza la visualizzazione designata come predefinita per Regione AWS quella in cui stai lavorando.

Le visualizzazioni determinano quali risorse sono disponibili per le interrogazioni. È possibile creare viste diverse, ognuna delle quali restituisce un set diverso di risorse.

Ad esempio, è possibile creare una visualizzazione che includa solo le risorse contrassegnate con la chiave `Environment` e il valore`Production`. Quindi, puoi scegliere di concedere l'accesso a quella visualizzazione solo agli utenti che hanno un motivo aziendale per visualizzare tali risorse. A una visualizzazione separata che include le risorse `Beta` dell'ambiente `Alpha` o possono accedere diversi utenti che devono visualizzare tali risorse. Per informazioni su come controllare chi può accedere a quali visualizzazioni, consultaConcessione dell'accesso alle visualizzazioni di Resource Explorer per la ricerca.

Sintassi della stringa di query

Questa sezione fornisce informazioni sugli aspetti di base della sintassi delle query, dei filtri e degli operatori di filtro.

Nozioni di base

Nella sua forma più elementare, a `QueryString` è un insieme di parole chiave di testo in formato libero unite implicitamente da un operatore logico. **`OR`** Separate ogni parola chiave dalle altre utilizzando uno spazio, come illustrato nell'esempio seguente:

```
ec2 billing test gamma
```

Resource Explorer valuta questo elenco di parole chiave per indicare:

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

Resource Explorer ordina i risultati in base alla pertinenza, dando maggiore preferenza alle risorse che corrispondono a un numero maggiore di termini di ricerca. Le risorse che non corrispondono a uno o più termini non sono escluse dai risultati. Tuttavia, Resource Explorer li considera di minore rilevanza e li colloca più in basso nei risultati di ricerca.

Se si specifica una stringa vuota per il `QueryString` parametro, la query restituisce le prime 1.000 risorse disponibili tramite la vista utilizzata per l'operazione. Il numero massimo di risorse che possono essere restituite da qualsiasi query è 1.000.

> **Note**
>
> AWS si riserva il diritto di aggiornare la logica di corrispondenza e gli algoritmi di pertinenza per la valutazione delle parole chiave di testo in formato libero in modo da poter fornire ai clienti i risultati più pertinenti. Pertanto, i risultati restituiti per le stesse query utilizzando parole chiave con testo in formato libero potrebbero cambiare nel tempo. Se hai bisogno di risultati più deterministici, ti consigliamo di utilizzare i filtri. La logica di abbinamento dei filtri non cambia nel tempo.

Filtri

Puoi limitare i risultati della tua ricerca in modo più rigoroso includendo filtri. A differenza delle parole chiave di testo, i filtri vengono valutati nella query con l'operatore AND. Ad esempio, si consideri la seguente query composta da due parole chiave in formato libero e due filtri:

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

Questa interrogazione viene valutata come segue:

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

I filtri vengono sempre valutati utilizzando operatori logici AND. Se una risorsa non corrisponde al filtro, tale risorsa non viene inclusa nei risultati. I risultati della query di esempio includono tutte le risorse associate ad Amazon EC2 che si trovano negli Stati Uniti occidentali (Oregon) Regione AWS e hanno almeno una delle parole chiave associate in qualche modo.

> **Note**
>
> A causa dell'implicitoAND, puoi utilizzare correttamente solo un filtro per un attributo che può avere un solo valore associato alla risorsa. Ad esempio, una risorsa può far parte di una Regione AWS sola risorsa. Pertanto, la seguente query non restituisce risultati.
>
> ```
> region:us-east-1 region:us-west-1
> ```
>
> Questa limitazione non si applica ai filtri per gli attributi che possono avere più valori contemporaneamente, ad esempio `tag:tag.key:`, `etag.value:`.

Nella tabella seguente sono elencati i nomi dei filtri disponibili che è possibile utilizzare in una query di ricerca di Resource Explorer.

Nome del filtro	Descrizione ed esempio
`accountid:`	Il Account AWS proprietario della risorsa. Resource Explorer include nei risultati solo le risorse di proprietà dell'account specificato. `accountid:123456789012`

`applicati on:`	Questo filtro consente di cercare risorse con una chiave di `awsApplic ation` tag e un valore di gruppo di risorse. È possibile eseguire la ricerca in base al nome dell'applicazione o al gruppo di risorse dell'applicazione ARN.
	
	`application:MyApplicationName`
	
	`application:arn:aws:resource-groups: us-east-1 :123456789012:group/MyApplicationName/1234567 89abced`

Nome del filtro	Descrizione ed esempio
	`arn:aws:resource-groups: us-east-1 :123456789012:group/MyApplicationName/123456789abced` **Note** Per utilizzare questo filtro, la visualizzazione deve avere accesso ai dati di etichettatura.
`id:`	L'identificatore di una singola risorsa, espresso come nome di risorsa Amazon (ARN). `id:arn:aws:license-manager: us-east-1 :123456789012:license-configuration:lic-ecbd5574fd92cb0d312baea26EXAMPLE`
`region:`	La posizione Regione AWS in cui si trova la risorsa. Resource Explorer include nei risultati solo le risorse che risiedono nell'area specificata Regione AWS. `region:us-east-1` **Note** Digitando solo il codice regionale (senza filtro, ad esempio `us-east-1`) non si ottengono gli stessi risultati di. `region:us-east-1` Questo risultato è dovuto al fatto che, trattandosi di una parola chiave di testo in formato libero che non è un filtro, il codice regionale viene suddiviso in singole parti. Ad esempio, `us-east-1` viene cercato come `useast`, e. 1 Questa suddivisione in componenti non si verifica quando si utilizza il `region:` prefisso.

Nome del filtro	Descrizione ed esempio
`region:global`	Un caso speciale per il `region:` filtro che è possibile utilizzare per trovare risorse che non sono associate a un individuo Regione AWS ma che sono considerate di portata globale. `region:global` **Note** Digitando solo la parola chiave `global` non si ottengono gli stessi risultati del `region:global` fatto che la parola letterale «globale» non è associata alle risorse globali. La digitazione `global` come parola chiave restituisce solo le risorse a cui è associata quella stringa letterale.
`resourcetype:`	Il tipo di risorsa in *`service`*`:`*`type`* notazione. Resource Explorer include nei risultati solo le risorse del tipo specificato. `resourcetype:ec2:instance`
`resourcetype.supports:`	Questo filtro consente di cercare risorse che supportano i tag. `tags`è l'unico valore supportato. Resource Explorer include nei risultati solo le risorse etichettabili. `resourcetype.supports:tags`
`service:`	Il Servizio AWS che è associato al tipo di risorsa. Resource Explorer include nei risultati solo le risorse create e gestite dal servizio specificato. `service:ec2`
`tag:`	Una coppia chiave/valore di tag espressa come. `<key>=<value>` Resource Explorer include nei risultati solo le risorse che hanno un tag con una chiave corrispondente e il valore specificato. `tag:environment=production`

Nome del filtro	Descrizione ed esempio
`tag:none`	Un caso speciale del `tag:` filtro che consente di cercare tutte le risorse a cui non sono allegati tag creati dall'utente. **Note** Le risorse con tag AWS creati dal servizio vengono ancora visualizz ate nei risultati di questo filtro.
`tag.key:`	Una chiave tag. Resource Explorer include nei risultati solo le risorse che hanno un tag con una chiave corrispondente, indipendentemente dal valore. `tag.key:environment`
`tag.value:`	Un valore di tag. Resource Explorer include nei risultati solo le risorse che hanno un tag con un valore corrispondente, indipendentemente dal nome della chiave. `tag.value:production`

Operatori di filtro

È possibile modificare le parole chiave e i filtri includendo uno degli operatori mostrati nella tabella seguente come parte della stringa.

Operatore	Descrizione ed esempio
"*multiple word phrase*" oppure «frase *sillabata* »	Racchiude una frase composta da più parole che deve essere trattata come una singola parola chiave con virgolette doppie (). " " Resource Explorer include solo le risorse che corrispondono all'intera frase, con tutte le parole insieme e nell'ordine specificato. Se non si utilizzano le virgolette doppie, Resource Explorer suddivide la frase nei suoi componenti mediante spazi o trattini e include risorse che corrispon dono ai singoli componenti, anche se non sono insieme o in un ordine diverso. Le virgolette devono essere racchiuse intorno a tutto ciò che segue l'operatore.

Operatore	Descrizione ed esempio

	`"This matches only resources with the whole sentence."`
	
	`This matches resources with any of the words.`
	
	`"us-east-1"` — corrisponde solo alle risorse associate a quella regione esatta.
	
	`us-east-1` — corrisponde a qualsiasi risorsa che contenga «us» o «east» o «1".
	
	`-tag:"enviornment=production"`

`keyword``*`	Corrispondenza con i caratteri jolly del prefisso. È possibile inserire un carattere jolly (un asterisco*) solo alla fine della stringa. Resource Explorer include nei risultati solo le risorse con valori che iniziano con il testo del prefisso precedente a. * L'esempio seguente corrisponde a tutto ciò Regioni AWS che inizia con`us-east`. `region:us-east*` **Important** La ricerca unificata inserisce automaticamente un operatore di caratteri jolly (*) alla fine della prima parola chiave della stringa. Ciò significa che i risultati della ricerca unificata includono risorse che corrispondono a qualsiasi stringa che inizia con la parola chiave specificata. La ricerca eseguita dalla casella di testo Query nella pagina di ricerca delle risorse della console Resource Explorer non aggiunge automatic amente un carattere jolly. È possibile inserire * manualmente un dopo qualsiasi termine nella stringa di ricerca.

Operatore	Descrizione ed esempio

`-keyword`	`Not`operatore. Puoi inserire un trattino (`-`) all'inizio della parola chiave o del filtro per invertire i risultati della ricerca. Resource Explorer esclude dai risultati tutte le risorse che corrispondono alla parola chiave o al filtro che segue questo operatore. L'esempio seguente fa sì che tutte le risorse associate al servizio Amazon EC2 vengano escluse dai risultati.
	
	`-service:ec2`
	
	Important
	
	Se si utilizza il AWS CLI `search` comando e il valore del `--query-string` parametro ha l'`-`operatore come primo carattere, è necessario separare il nome del parametro dal relativo valore con un carattere di segno uguale (=) anziché il consueto carattere di spazio. Se si utilizza il carattere spazio, la CLI interpreta erroneamente la stringa. Ad esempio, la seguente query ha esito negativo.
	
	`aws resource-explorer-2 search --query-string "-tag:none region:us-east-1"`
	
	La seguente stringa di query corretta, con uno spazio = sostitutivo, funziona come previsto.
	
	`aws resource-explorer-2 search --query-string ="-tag:none region:us-east-1"`
	
	Se modificate l'ordine dei filtri nella stringa di query in modo che `-` non sia il primo carattere del valore del parametro, potete utilizzare il carattere di spazio standard. La seguente stringa di query funziona.
	
	`aws resource-explorer-2 search --query-string "region:us-east-1 -tag:none"`

Operatore	Descrizione ed esempio

`\<special character>`	È possibile evitare caratteri speciali che devono essere inclusi esattamente come illustrati anziché interpretati. Se il testo include uno dei caratteri speciali (`* " - : = \`), dovete precedere quel carattere da una barra rovesciata (\) per assicurarvi che il carattere venga preso alla lettera. L'esempio seguente mostra come utilizzare una parola chiave di testo in formato libero che include il carattere trattino () (). `- "my-key-word"`
	
	Inoltre, per evitare che Resource Explorer suddivida l'espressione in corrispon denza dei trattini in tre parole chiave separate, è possibile racchiudere l'intera frase tra virgolette doppie.
	
	`"my\-key\-word"`
	
	Per inserire una barra rovesciata letterale, inserite due caratteri di barra rovesciata in una riga. La prima barra rovesciata viene interpretata come escape e la seconda barra rovesciata è il carattere letterale da inserire.
	
	`"some_text\\some_more_text"`

> **Note**
>
> Se la vista include i tag allegati alle risorse, l'`Search`operazione non genera errori di convalida per le stringhe di ricerca, poiché un filtro non valido potrebbe essere interpretato anche come una ricerca di testo in formato libero. Ad esempio, anche se `cat:blue` sembra un filtro, Resource Explorer non può analizzarlo come tale perché `cat:` non è uno dei filtri validi e definiti. Invece Resource Explorer interpreta l'intera stringa come una stringa di ricerca in formato libero per consentirle di abbinare elementi come il nome di una chiave di tag o una parte di un ARN.
> L'operazione genera un errore di convalida se una delle seguenti condizioni è vera:
>
> - La vista non include informazioni sui tag
> - La query di ricerca utilizza esplicitamente un filtro di tag (`tag.key:`,`tag.value:`, `otag:`)

Esempi di query di ricerca in Resource Explorer

Gli esempi seguenti mostrano la sintassi per i tipi più comuni di interrogazioni che è possibile utilizzare inEsploratore di risorse AWS.

Important

Se si utilizza ilAWS CLI`search` comando e il valore del`--query-string` parametro ha l'`-`operatore come primo carattere, è necessario separare il nome del parametro dal suo valore con un carattere di segno uguale (=) anziché il normale carattere di spazio. Se si utilizza lo spazio, la CLI interpreta erroneamente la stringa. Ad esempio, la seguente query ha esito negativo.

```
aws resource-explorer-2 search --query-string "-tag:none region:us-east-1"
```

La seguente query corretta, con una= sostituzione dello spazio, funziona come previsto.

```
aws resource-explorer-2 search --query-string="-tag:none region:us-east-1"
```

Se modificate l'ordine dei filtri nella stringa di ricerca in modo che`-` non sia il primo carattere nel valore del parametro, potete usare lo spazio standard. La seguente query funziona.

```
aws resource-explorer-2 search --query-string "region:us-east-1 -tag:none"
```

Cerca risorse senza tag

Se desideri utilizzare il controllo degli accessi basato sugli attributi (ABAC) nel tuo account, utilizzare l'allocazione basata sui costi o eseguire l'automazione basata su tag sulle tue risorse, devi sapere a quali risorse del tuo account potrebbero mancare i tag. La seguente query di esempio utilizza lo speciale tag case filter: none per restituire tutte le risorse a cui mancano i tag generati dall'utente.

Il`tag:none` filtro si applica solo ai tag creati dall'utente. I tag generati e gestiti daAWS sono esenti da questo filtro e vengono comunque visualizzati nei risultati.

```
tag:none
```

Inoltre, per escludere tutti i tag di sistemaAWS creati, aggiungi un secondo filtro come mostrato nell'esempio seguente. Il primo elemento nella stringa di query duplica l'esempio precedente filtrando tutti i tag creati dall'utente. AWSi tag di sistema creati iniziano sempre con le lettere`aws`. Pertanto, è possibile utilizzare l'operatore logico NOT (-) con il filtro tag.key per escludere anche tutte le risorse che hanno un tag con un nome chiave che inizia con`aws`.

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

Cerca risorse contrassegnate

Per trovare tutte le risorse che hanno un tag di qualsiasi tipo, puoi usare l'operatore logico NOT (-) con il filtro speciale case tag: none come segue.

```
-tag:none
```

Cerca risorse a cui manca un tag specifico

Inoltre, in relazione all'ABAC, potresti voler cercare tutte le risorse che non hanno un tag con una chiave specificata. L'esempio seguente utilizza l'operatore logico NOT- per restituire tutte le risorse a cui manca un tag con il nome della chiave`Department`.

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

Cerca risorse con valori di tag non validi

Per motivi di conformità, potresti voler cercare tutte le risorse con valori di tag mancanti o scritti in modo errato su tag importanti. L'esempio seguente restituisce tutte le risorse che hanno un tag con il nome della chiave`environment`. Tuttavia, la query filtra qualsiasi risorsa con uno dei valori validi`prod`,`inteq`, o`dev`. Tutti i risultati che appaiono da questa query hanno un altro valore che è necessario esaminare e correggere.

> **Important**
>
> Le ricerche in Resource Explorer non fanno distinzione tra maiuscole e minuscole e non possono distinguere tra nomi di chiavi e valori che differiscono solo per il modo in

cui sono scritti in maiuscolo. Ad esempio, i valori nell'esempio seguente corrispondono a`PR0Dprod`,`Pr0d`, o a qualsiasi variazione. Tuttavia, alcune applicazioni utilizzano i tag facendo distinzione tra maiuscole e minuscole. Ti consigliamo di adottare una strategia di capitalizzazione standardizzata per la tua organizzazione, ad esempio utilizzando solo i nomi e i valori delle chiavi dei tag minuscoli. Un approccio coerente può aiutare a evitare la confusione che può essere causata dalla presenza di tag che differiscono solo dal modo in cui sono scritti in maiuscolo.

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

Cerca risorse in un sottoinsieme diRegioni AWS

Usa l'operatore `'*'` jolly per abbinare tutte le regioni in una determinata area del mondo. L'esempio seguente restituisce tutte le risorse presenti in Regioni d'Europa (UE).

```
region:eu-*
```

Cerca risorse globali

Usa il`global` valore speciale del`region:` filtro per trovare le tue risorse considerate globali e non associate a una singola regione.

```
region:global
```

Cerca risorse di un determinato tipo che si trovano in una regione specifica

Quando si utilizzano più filtri, Resource Explorer valuta l'espressione combinando i prefissi con`AND` operatori logici impliciti. L'esempio seguente restituisce tutte le risorse che si trovano nella regione Asia Pacifico (Hong Kong)`AND` sono istanze Amazon EC2.

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

> **Note**
>
> A causa dell'implicitoAND, è possibile utilizzare correttamente un solo filtro per un attributo che può avere un solo valore associato alla risorsa. Ad esempio, una risorsa può far parte di una sola risorsaRegione AWS. Pertanto, la seguente query non restituisce risultati.
>
> ```
> region:us-east-1 region:us-west-1
> ```
>
> Questa limitazione non si applica ai filtri per gli attributi che possono avere più valori contemporaneamente, ad esempio`tag:tag.key:`, `etag.value:`.

Cerca risorse con un termine composto da più parole

Racchiudi un termine composto da più parole con virgolette doppie (") per restituire solo i risultati che hanno l'intero termine nell'ordine specificato. Senza virgolette doppie, Resource Explorer restituisce risorse che corrispondono a qualsiasi singola parola che compone il termine. Ad esempio, la seguente query utilizza le virgolette doppie per restituire solo le risorse che corrispondono al termine`"west wing"`. La query non corrisponde alle risorse della`us-west-2`Regione AWS (o di qualsiasi altra regione inclusa`west` nel suo codice) o alle risorse che corrispondono alla parola «ala» senza la parola «ovest».

```
"west wing"
```

Cerca le risorse che fanno parte di uno CloudFormation stack specificato

Quando crei una risorsa come parte di unoAWS CloudFormation stack, tutte vengono automaticamente etichettate con il nome dello stack. L'esempio seguente restituisce tutte le risorse create come parte dello stack specificato.

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

Utilizzo della ricerca unificata in AWS Management Console

AWS Management ConsoleInclude una barra di ricerca nella parte superiore di ogni pagina della AWS console. Questa barra di ricerca può cercare nella Servizio AWS documentazione e negli argomenti del blog e indirizzarti direttamente alle pagine della console di AWS servizio. Può anche restituire le risorse presenti nel tuoAccount AWS, se attivi la funzione di ricerca unificata attivando le funzionalità richieste di Resource Explorer.

Con la ricerca unificata, gli utenti possono cercare risorse da qualsiasi Servizio AWS console senza dover prima accedere alla Esploratore di risorse AWS console.

> **Tip**
>
> Se desideri utilizzare la barra di ricerca unificata per cercare risorse specifiche, inizia la query di ricerca **`/Resources`** digitando. Questo fa sì che AWS le risorse vengano classificate più in alto nei risultati di ricerca rispetto ai risultati che non rappresentano risorse.

Argomenti

- Verifica se la ricerca unificata è abilitata
- Attivazione della ricerca unificata

> **Important**
>
> La ricerca unificata inserisce automaticamente un operatore di caratteri jolly (*) alla fine della prima parola chiave nella stringa. Ciò significa che i risultati della ricerca unificata includono risorse che corrispondono a qualsiasi stringa che inizia con la parola chiave specificata.
> La ricerca eseguita dalla casella di testo Query nella pagina Ricerca risorse della console Resource Explorer non aggiunge automaticamente un carattere jolly. È possibile inserire * manualmente un termine dopo qualsiasi termine nella stringa di ricerca.

Verifica se la ricerca unificata è abilitata

Per vedere se la ricerca unificata è abilitata nel tuoAccount AWS, guarda nella parte superiore della pagina Impostazioni. Resource Explorer visualizza lì lo stato corrente di ogni requisito. I parametri sono i seguenti:

- È necessario attivare Resource Explorer in almeno unaRegione AWS. Solo le risorse nelle regioni con indici Resource Explorer possono essere visualizzate nei risultati di ricerca unificati.
- Devi creare un indice aggregatore nella regione di tua scelta. Le ricerche eseguite in questa regione restituiscono i risultati di tutte le regioni registrate nell'account.
- È necessario creare una vista predefinita nella regione che contiene l'indice dell'aggregatore. Tutti gli utenti che devono utilizzare la ricerca unificata delle risorse devono disporre dell'autorizzazione per utilizzare questa visualizzazione predefinita.
- Gli utenti devono disporre di una politica di autorizzazioni AWS Identity and Access Management (IAM) assegnata al proprio preside IAM che conceda l'autorizzazione a eseguire le azioni`resource-explorer-2:Get*`, `resource-explorer-2:List*resource-explorer-2:Describe*`,`resource-explorer-2:Search`. Puoi concedere queste autorizzazioni utilizzando le tue policy IAM personalizzate. Queste autorizzazioni sono già incluse nelle seguenti politiche AWS gestite disponibili per l'uso:
  - AWSResourceExplorerReadOnlyAccess
  - AWSResourceExplorerFullAccess

Attivazione della ricerca unificata

Per abilitare l'inclusione delle risorse del tuo account nei risultati di ricerca per la ricerca unificata da qualsiasi AWS console, devi completare i seguenti passaggi:

1. Attiva Esploratore di risorse AWS in uno o più Regioni AWS dei tuoi account.
2. Registra una regione per contenere l'indice dell'aggregatore.
3. Crea una vista predefinita nella regione con l'indice dell'aggregatore.

Utilizzo AWS Chatbot per la ricerca di risorse

Puoi cercare e scoprire informazioni sulle Servizi AWS tue AWS risorse ponendo domande in linguaggio AWS Chatbot naturale. AWS Chatbotrisponde alle domande relative ai servizi direttamente nei canali di chat con la AWS documentazione pertinente e gli estratti degli articoli di supporto. AWS Chatbotutilizza Resource Explorer per cercare e trovare risposte alle domande relative alle risorse.

Per ulteriori informazioni, vedi Cos'èAWS Chatbot? nella Guida per l'AWS Chatbotamministratore.

AWSdomande sulle risorse

AWS Chatbotutilizza Resource Explorer per cercare e scoprire le tue risorse. AWS Chatbotvisualizza questi risultati di ricerca in un elenco. Questo elenco mostra le prime cinque risorse corrispondenti e include la possibilità di filtrare ulteriormente i risultati per tipo di risorsa e tag. Regione AWS

Prerequisiti

Per porre domande relative alle AWS Chatbot risorse devi:

- Assicurati di avere indici e viste attivi con almeno una vista predefinita nella tua. Regione AWS Gli indici e le viste consentono a Resource Explorer di catalogare e interrogare le tue risorse. Per ulteriori informazioni, consulta Termini e concetti per Resource Explorer.
- Aggiungi la AWSResourceExplorerReadOnlyAccess policy al tuo ruolo di canale o a ciascun ruolo utente appropriato, a seconda dello schema di autorizzazioni del canale.
- Verifica che le politiche di guardrail del tuo canale consentano le AWSResourceExplorerReadOnlyAccess autorizzazioni.

Domande frequenti sulle risorse

Puoi porre queste domande direttamente dai tuoi canali di chat. Sostituisci le parole con testo rosso con le tue informazioni.

```
@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?
```

Sicurezza in Esploratore di risorse AWS

Per AWS, la sicurezza del cloud ha la massima priorità. In quanto cliente AWS, è possibile trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle organizzazioni più esigenti a livello di sicurezza.

La sicurezza è una responsabilità condivisa tra te e AWS. Il modello di responsabilità condivisa descrive questo modello come sicurezza del cloud e sicurezza nel cloud:

- La sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che esegue Servizi AWS nel Cloud AWS. AWS fornisce, inoltre, servizi utilizzabili in modo sicuro. I revisori di terze parti testano regolarmente e verificano l'efficacia della nostra sicurezza nell'ambito dei Programmi di conformità AWS. Per informazioni sui programmi di conformità applicabili a Resource Explorer, consulta Servizi AWSServiziServizi AWS coperti .
- Sicurezza nel cloud: la tua responsabilità è determinata dal Servizio AWS che viene utilizzato. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i tuoi requisiti aziendali e le leggi e le normative applicabili

Questa documentazione facilitaconsenteladicomprensionecomprenderedell'applicazionecomedelapplicare il modello di responsabilità condivisa quando utilizzisi usaEsploratore di risorse AWS. Viene illustrato come configurare Resource Explorer per soddisfare gli obiettivi di sicurezza e conformità. Vengono inoltre fornite informazioni su come utilizzare per monitorare e proteggere le risorse di Resource Explorer.Servizi AWS

Indice

- Gestione delle identità e degli accessi per l'Esploratore di risorse AWS
- Protezione dei dati in Esploratore di risorse AWS
- Convalida della conformità per Esploratore di risorse AWS
- Resilienza in Esploratore di risorse AWS
- Sicurezza dell'infrastruttura in Esploratore di risorse AWS

Gestione delle identità e degli accessi per l'Esploratore di risorse AWS

AWS Identity and Access Management (IAM) è un Servizio AWSche consente agli amministratori di controllare in modo sicuro l'accesso alle risorse AWS. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse di Resource Explorer. IAM è un Servizio AWS il cui uso non comporta costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso con policy
- Funzionamento di Resource Explorer con IAM
- Esempi di policy di Esploratore di risorse AWS basate su identità
- Esempi di politiche di controllo dei servizi per AWS Organizations e Resource Explorer
- AWS politiche gestite per Esploratore di risorse AWS
- Utilizzo di ruoli collegati ai servizi per Resource Explorer
- Risoluzione dei problemiEsploratore di risorse AWS delle autorizzazioni

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Resource Explorer.

Utente del servizio: se utilizzi il servizio Resource Explorer per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità di Resource Explorer per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di Resource Explorer, consultaRisoluzione dei problemiEsploratore di risorse AWS delle autorizzazioni.

Amministratore del servizio: se sei responsabile delle risorse di Resource Explorer presso la tua azienda, probabilmente hai pieno accesso a Resource Explorer. È tuo compito determinare a quali funzionalità e risorse di Resource Explorer gli utenti del servizio devono accedere. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio.

Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con Resource Explorer, consultaFunzionamento di Resource Explorer con IAM.

Amministratore IAM: se sei un amministratore IAM, potresti voler conoscere i dettagli su come scrivere policy per gestire l'accesso a Resource Explorer. Per visualizzare esempi di policy basate sull'identità di Resource Explorer che puoi utilizzare in IAM, consulta. Esempi di policy di Esploratore di risorse AWS basate su identità

Autenticazione con identità

L'autenticazione è la procedura di accesso ad AWScon le credenziali di identità. Devi essere autenticato (connesso a AWS) come utente root Utente root dell'account AWS, come utente IAM o assumere un ruolo IAM.

Puoi accedere ad AWScome identità federata utilizzando le credenziali fornite attraverso un'origine di identità. AWS IAM Identity Center Gli esempi di identità federate comprendono gli utenti del centro identità IAM, l'autenticazione Single Sign-On (SSO) dell'azienda e le credenziali di Google o Facebook. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Se accedi ad AWStramite la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere alla AWS Management Consoleo al portale di accesso AWS. Per ulteriori informazioni sull'accesso ad AWS, consulta la sezione Come accedere al tuo Account AWSnella Guida per l'utente di Accedi ad AWS.

Se accedi ad AWS in modo programmatico, AWS fornisce un Software Development Kit (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le richieste utilizzando le tue credenziali. Se non utilizzi gli strumenti AWS, devi firmare le richieste personalmente. Per ulteriori informazioni sulla firma delle richieste, consulta Firma delle richieste AWS nella Guida per l'utente IAM.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. AWS consiglia ad esempio di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza dell'account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWS nella Guida per l'utente di IAM.

Utente root di un Account AWS

Quando crei un Account AWS, inizi con una singola identità di accesso che ha accesso completo a tutti i Servizi AWSe le risorse nell'account. Tale identità è detta utente root Account AWSed è possibile accedervi con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conservare le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

Utenti e gruppi

Un utente IAM è una identità all'interno del tuo Account AWSche dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente di IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato Amministratori IAM e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente di IAM.

Roles

Un ruolo IAM è un'identità all'interno di Account AWSche dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. È possibile assumere temporaneamente un ruolo IAM nella AWS Management Consolemediante lo scambio di ruoli. È possibile assumere un ruolo chiamando un'operazione AWS CLIo API AWSoppure utilizzando un

URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per ulteriori informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center.
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, per alcuni dei Servizi AWS, è possibile collegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso multi-servizio: alcuni Servizi AWS utilizzano funzionalità in altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Inoltro delle sessioni di accesso (FAS): quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, tale utente o ruolo viene considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio AWS, combinate con il Servizio AWS richiedente, per effettuare richieste a servizi a valle. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che necessita di interazioni con altri Servizi AWS o risorse per essere portata a termine. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM assunto da un servizio per eseguire operazioni per conto dell'utente. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account Account AWSe sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- Applicazioni in esecuzione su Amazon EC2: è possibile utilizzare un ruolo IAM per gestire credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 che eseguono richieste di AWS CLIo dell'API AWS. Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un ruolo AWSa un'istanza EC2, affinché sia disponibile per tutte le relative applicazioni, puoi creare un profilo dell'istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Per controllare l'accesso a AWS è possibile creare policy e collegarle a identità o risorse AWS. Una policy è un oggetto in AWSche, quando associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWSvaluta queste policy quando un principale IAM (utente, utente root o sessione ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle policy viene archiviata in AWSsotto forma di documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWSJSON per specificare l'accesso ai diversi elementi. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore

IAM può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dalla AWS Management Console, la AWS CLIo l'API AWS.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono incorporate direttamente in un singolo utente, gruppo o ruolo. Le policy gestite sono policy autonome che possono essere collegate a più utenti, gruppi e ruoli in Account AWS. Le policy gestite includono le policy gestite da AWSe le policy gestite dal cliente. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o Servizi AWS.

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy gestite da AWSda IAM in una policy basata su risorse.

Esploratore di risorse AWS non supporta le policy basate su risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3, AWS WAFe Amazon VPC sono esempi di servizi che supportano le ACL. Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Esploratore di risorse AWS non supporta le ACL.

Altri tipi di policy

AWS supporta altri tipi di policy meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Policy di controllo dei servizi (SCP): le SCP sono policy JSON che specificano il numero massimo di autorizzazioni per un'organizzazione o unità organizzativa (OU) in AWS Organizations. AWS Organizationsè un servizio per il raggruppamento e la gestione centralizzata degli Account AWSmultipli di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. La SCP limita le autorizzazioni per le entità negli account membri, compreso ogni Utente root dell'account AWS. Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations.
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce

l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella Guida per l'utente di IAM.

Funzionamento di Resource Explorer con IAM

Prima di utilizzare IAM per gestire l'accesso aEsploratore di risorse AWS, è necessario comprendere quali caratteristiche IAM sono disponibili per l'uso con Resource Explorer. Per ottenere un quadro generale del funzionamento di Resource Explorer e altriServizi AWS con IAM, consulta Servizi AWSla sezione Funzionamento di con IAM nella Guida per l'utente di IAM.

Argomenti

- Policy basate su identità di Resource Explorer
- Autorizzazione basata su tag Resource Explorer
- Ruoli IAM di Resource Explorer

Come qualsiasi altroServizio AWS, Resource Explorer richiede le autorizzazioni per utilizzare le sue operazioni per interagire con le tue risorse. Per eseguire la ricerca, gli utenti devono disporre dell'autorizzazione per recuperare i dettagli su una vista e anche per effettuare ricerche utilizzando la vista. Per creare indici o visualizzazioni o modificarli o qualsiasi altra impostazione di Resource Explorer, è necessario disporre di autorizzazioni aggiuntive.

Assegna policy basate sull'identità IAM che concedono tali autorizzazioni ai responsabili IAM appropriati. Resource Explorer fornisce diverse politiche gestite che predefiniscono set di autorizzazioni comuni. Puoi assegnarli ai tuoi responsabili IAM.

Policy basate su identità di Resource Explorer

Con le policy IAM basate su identità, puoi specificare operazioni consentite o rifiutate su risorse specifiche e le condizioni in base alle quali tali operazioni sono consentite o rifiutate. Resource Explorer supporta specifiche operazioni, risorse e chiavi di condizione. Per informazioni su tutti gli elementi utilizzati in una policy JSON, consultare Documentazione di riferimento degli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Operazioni

Gli amministratori possono utilizzare le policy AWS JSON per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le operazioni della policy hanno spesso lo stesso nome dell'operazione API AWS. Ci sono alcune eccezioni, ad esempio le operazioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono chiamate operazioni dipendenti.

Includere le operazioni in una policy per concedere le autorizzazioni per eseguire l'operazione associata.

Le azioni politiche in Resource Explorer utilizzano il prefisso del`resource-explorer-2` servizio prima dell'azione. Ad esempio, per concedere a qualcuno l'autorizzazione per eseguire la ricerca tramite una vista, con l'operazione`Search` API Resource Explorer, includi l'`resource-explorer-2:Search`operazione in una policy assegnata a quel cliente. Le istruzioni della policy devono includere un elemento `Action` o `NotAction`. Resource Explorer definisce un proprio set di operazioni che descrivono le attività che è possibile eseguire con questo servizio. Questi sono in linea con le operazioni dell'API Resource Explorer.

Per specificare più operazioni in una singola istruzione, separale con virgole, come illustrato nell'esempio seguente.

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

Puoi anche specificare più operazioni tramite caratteri jolly (`*`). Ad esempio, per specificare tutte le operazioni che iniziano con la parola `Describe`, includi la seguente operazione.

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

Per un elenco delle azioni di Resource Explorer, vedere Azioni definite daEsploratore di risorse AWS nel AWSService Authorization Reference.

Risorse

Gli amministratori possono utilizzare le policy AWS JSON per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo Amazon Resource Name (ARN). È possibile eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, noto come autorizzazioni a livello di risorsa.

Per le operazioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Vista

Il tipo di risorsa principale di Resource Explorer è la vista.

La risorsa di visualizzazione Resource Explorer ha il seguente formato ARN.

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

Il formato ARN di Resource Explorer è mostrato nell'esempio seguente.

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

> **Note**
>
> L'ARN di una vista include un identificatore univoco alla fine per garantire che ogni vista sia unica. Questo aiuta a garantire che una policy IAM che garantiva l'accesso a una vecchia vista eliminata non possa essere utilizzata per concedere accidentalmente l'accesso a una nuova vista che ha lo stesso nome della vecchia vista. Ogni nuova vista riceve un nuovo ID univoco alla fine per garantire che gli ARN non vengano mai riutilizzati.

Per ulteriori informazioni sul formato degli ARN, consulta Amazon Resource Name (ARN).

Utilizzi le policy basate sull'identità IAM assegnate ai responsabili IAM e specifichi la vista come`Resource`. In questo modo è possibile concedere l'accesso alla ricerca tramite una vista a un set di principi e l'accesso tramite una visualizzazione completamente diversa a un diverso insieme di principi.

Ad esempio, per concedere l'autorizzazione a una singola vista indicata`ProductionResourcesView` in una dichiarazione di policy IAM, ottieni prima il nome della risorsa Amazon (ARN) della vista. È possibile utilizzare la pagina Visualizzazioni della console per visualizzare i dettagli di una vista o richiamare l'`ListViews`operazione per recuperare l'ARN completo della vista desiderata. Quindi, includilo in una dichiarazione politica, come quella mostrata nell'esempio seguente che concede il permesso di modificare la definizione di una sola vista.

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

Per consentire le azioni su tutte le viste che appartengono a un account specifico, utilizza il carattere jolly (*) nella parte pertinente dell'ARN. L'esempio seguente concede l'autorizzazione di ricerca a tutte le visualizzazioni in un accountRegione AWS ands specificato.

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

Alcune azioni di Resource Explorer`CreateView`, ad esempio, non vengono eseguite su una risorsa specifica, perché, come nell'esempio seguente, la risorsa non esiste ancora. In questi casi, è necessario utilizzare il carattere jolly (*) per l'intera ARN della risorsa.

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

Se si specifica un percorso che termina con un carattere jolly, è possibile limitare l'`CreateView`operazione alla creazione di viste con solo il percorso approvato. Il seguente esempio di policy mostra come consentire al committente di creare viste solo nel percorso`view/ProductionViews/`.

```
"Effect": "Allow",
```

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

Indice

Un altro tipo di risorsa che è possibile utilizzare per controllare l'accesso alla funzionalità di Resource Explorer è l'indice.

Il modo principale in cui interagisci con l'indice è attivare Resource Explorer in unRegione AWS creando un indice in quella regione. Dopodiché, fai quasi tutto il resto interagendo con la vista.

Una cosa che puoi fare con l'indice è controllare chi può creare viste in ogni regione.

> **Note**
>
> Dopo aver creato una vista, IAM autorizza tutte le altre azioni di visualizzazione solo sull'ARN della vista e non sull'indice.

L'indice ha un ARN a cui puoi fare riferimento in una politica di autorizzazione. Un indice di Resource Explorer ARN ha il formato seguente.

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

Vedere il seguente esempio di un indice ARN di Resource Explorer.

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

Alcune azioni di Resource Explorer controllano l'autenticazione rispetto a più tipi di risorse. Ad esempio, l'CreateViewoperazione effettua l'autorizzazione sia in base all'ARN dell'indice che all'ARN della vista così come sarà dopo la creazione di Resource Explorer. Per concedere agli amministratori il permesso di gestire il servizio Resource Explorer, è possibile utilizzarlo per`"Resource": "*"` autorizzare azioni per qualsiasi risorsa, indice o visualizzazione.

In alternativa, puoi limitare un committente a poter lavorare solo con risorse di Resource Explorer specificate. Ad esempio, per limitare le azioni alle sole risorse di Resource Explorer in una regione

specificata, puoi includere un modello ARN che corrisponda sia all'indice che alla vista, ma richiami solo una singola regione. Nell'esempio seguente, l'ARN corrisponde a entrambi gli indici o le viste solo nella`us-west-2` regione dell'account specificato. Specifica la regione nel terzo campo dell'ARN, ma utilizza un carattere jolly (*) nel campo finale per corrispondere a qualsiasi tipo di risorsa.

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

Per ulteriori informazioni, vedere Risorse definite daEsploratore di risorse AWS nel AWSService Authorization Reference. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta Operazioni definite da Esploratore di risorse AWS.

Chiavi di condizione

Resource Explorer non fornisce chiavi di condizione specifiche del servizio, ma supporta l'utilizzo di alcune chiavi di condizione globali. Per visualizzare tutte le chiavi di condizione globali di AWS, consulta Chiavi di contesto delle condizioni globali di AWS nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è attiva. L'elemento `Condition` è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND` logica. Se specifichi più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione `OR` logica. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche per il servizio. Per visualizzare tutte le chiavi di condizione globali di AWS, consulta Chiavi di contesto delle condizioni globali di AWS nella Guida per l'utente di IAM.

Per visualizzare un elenco delle chiavi di condizione che è possibile utilizzare con Resource Explorer, consulta Condition KeysEsploratore di risorse AWS nella AWSService Authorization Reference. Per informazioni su operazioni e risorse con cui è possibile utilizzare una chiave di condizione, consulta Operazioni definite daEsploratore di risorse AWS.

Esempi

Per visualizzare esempi di policy basate su identità di Resource Explorer, consultareEsempi di policy di Esploratore di risorse AWS basate su identità.

Autorizzazione basata su tag Resource Explorer

È possibile collegare dei tag alle viste di Resource Explorer o passare dei tag in una richiesta a Resource Explorer. Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `resource-explorer-2:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* o `aws:TagKeys`. Per ulteriori informazioni sull'assegnazione di tag alle risorse di Resource Explorer, consultareAggiunta di tag alle visualizzazioni. Per utilizzare l'autorizzazione basata su tag in Resource Explorer, vedereUtilizzo dell'autorizzazione basata sui tag per controllare l'accesso alle visualizzazioni.

Ruoli IAM di Resource Explorer

Un ruolo IAM è un responsabile all'interno dell'aziendaAccount AWS che dispone di autorizzazioni specifiche.

Utilizzo di credenziali temporanee con Resource Explorer

È possibile utilizzare credenziali temporanee per effettuare l'accesso con la federazione, assumere un ruolo IAM o un ruolo multi-account. Si ottengono credenziali di sicurezza temporanee chiamando operazioni APIAWS Security Token Service (AWS STS) come AssumeRoleo GetFederationToken.

Resource Explorer supporta l'uso di credenziali temporanee.

Ruoli collegati ai servizi

I Ruoli collegati ai servizi consentono agli Servizi AWS di accedere a risorse in altri servizi per completare un'operazione a tuo nome. I ruoli collegati ai servizi sono visualizzati nell'account IAM e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non può modificarle.

Resource Explorer utilizza ruoli collegati ai servizi per eseguire il proprio lavoro. Per informazioni dettagliate sui ruoli collegati ai servizi di Resource Explorer, consultareUtilizzo di ruoli collegati ai servizi per Resource Explorer.

Esempi di policy di Esploratore di risorse AWS basate su identità

Per impostazione predefinita, i responsabiliAWS Identity and Access Management (IAM), ad esempio ruoli, gruppi e utenti, non dispongono dell'autorizzazione per creare o modificare risorse Resource Explorer. Inoltre, non possono eseguire attività utilizzandoAWS Management Console,AWS Command Line Interface (AWS CLI) oAWS l'API. Un amministratore IAM deve creare policy IAM che concedono ai responsabili l'autorizzazione per eseguire operazioni API specifiche sulle risorse specificate di cui hanno bisogno. Quindi, l'amministratore deve assegnare queste policy ai responsabili IAM che richiedono tali autorizzazioni.

Per fornire l'accesso, aggiungi autorizzazioni ai tuoi utenti, gruppi o ruoli:

- Utenti e gruppi in AWS IAM Identity Center:

  Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center.
- Utenti gestiti in IAM tramite un provider di identità:

  Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina Creating a role for a third-party identity provider (federation) (Creazione di un ruolo per un provider di identità di terze parti [federazione]) nella Guida per l'utente di IAM.
- Utenti IAM:
  - Crea un ruolo che l'utente possa assumere. Per istruzioni, consulta la pagina Creating a role for an IAM user (Creazione di un ruolo per un utente IAM) nella Guida per l'utente di IAM.
  - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente di IAM.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy nella scheda JSON nella Guida per l'utente IAM.

Argomenti

- Best practice delle policy

- Utilizzo della console Resource Explorer
- Concessione dell'accesso a una visualizzazione basata su tag
- Concedere l'accesso per creare una vista basata sui tag
- Consentire ai responsabili di visualizzare le loro autorizzazioni

Best practice delle policy

Le policy basate su identità determinano se qualcuno può creare, accedere o eliminare risorse Resource Explorer nell'account. Queste operazioni possono comportare costi aggiuntivi per il proprio Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e suggerimenti:

- Nozioni di base sulle policy gestite da AWS e passaggio alle autorizzazioni con privilegio minimo: per le informazioni di base su come concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy gestite da AWS che concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente di AWS specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni di processo nella Guida per l'utente di IAM.
- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi inoltre utilizzare le condizioni per concedere l'accesso alle operazioni di servizio, ma solo se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer fornisce oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori

informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente di IAM.

- Richiesta dell'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o utenti root nel tuo Account AWS, attiva MFA per una maggiore sicurezza. Per richiedere l'AMF quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console Resource Explorer

Per eseguire ricerche nellaEsploratore di risorse AWS console, è necessario che i responsabili dispongano di un set di autorizzazioni minimo. Se non crei una policy basata su identità con le autorizzazioni minime richieste, la console Resource Explorer non funziona nel modo previsto per i responsabili dell'account.

È possibile utilizzare la policyAWS gestita denominata`AWSResourceExplorerReadOnlyAccess` per concedere la possibilità di utilizzare la console Resource Explorer per effettuare ricerche utilizzando qualsiasi visualizzazione dell'account. Per concedere le autorizzazioni per la ricerca con una sola visualizzazioneConcessione dell'accesso alle visualizzazioni di Resource Explorer per la ricerca, vedere e gli esempi nelle due sezioni seguenti.

Non sono necessarie le autorizzazioni minime della console per i principali che effettuano chiamate solo alla AWS CLI o all'API AWS. Puoi invece scegliere di concedere l'accesso solo alle azioni che corrispondono alle operazioni API che i responsabili devono eseguire.

Concessione dell'accesso a una visualizzazione basata su tag

In questo esempio, desideri concedere l'accesso a una visualizzazione Resource Explorer nell'account.Account AWS Per fare ciò, assegni le policy basate sull'identità IAM ai responsabili che desideri poter cercare in Resource Explorer. Il seguente esempio di policy IAM concede l'accesso a qualsiasi richiesta in cui il`Search-Group` tag allegato al committente chiamante corrisponde esattamente al valore dello stesso tag allegato alla vista utilizzata nella richiesta.

```
{
    "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}"}
            }
        }
    ]
}
```

Puoi assegnare questa policy ai responsabili IAM nel tuo account. Se un utente principale con il tag`Search-Group=A` tenta di effettuare una ricerca utilizzando una vista Resource Explorer, anche la vista deve essere contrassegnata`Search-Group=A`. In caso contrario, al preside viene negato l'accesso. La chiave di tag di condizione `Search-Group` corrisponde a `Search-group` e `search-group` perché i nomi delle chiavi di condizione non effettuano la distinzione tra maiuscole e minuscole. Per ulteriori informazioni, consulta Elementi delle policy JSON IAM: Condition nella Guida per l'utente IAM.

> **Important**
>
> Per visualizzare le risorse nei risultati di ricerca unificati inAWS Management Console, i responsabili devono disporre`Search` delle autorizzazioni`GetView` e per la visualizzazione predefinita della visualizzazioneRegione AWS che contiene l'indice aggregatore. Il modo più semplice per concedere tali autorizzazioni consiste nel lasciare l'autorizzazione predefinita basata sulle risorse che è stata allegata alla visualizzazione quando hai attivato Resource Explorer utilizzando la configurazione rapida o avanzata.
>
> In questo scenario, potresti prendere in considerazione l'impostazione della visualizzazione predefinita per filtrare le risorse sensibili e quindi l'impostazione di visualizzazioni aggiuntive a cui concedere l'accesso basato su tag, come descritto nell'esempio precedente.

Concedere l'accesso per creare una vista basata sui tag

In questo esempio, si desidera consentire solo ai principali con lo stesso tag dell'indice di poter creare visualizzazioni nell'oggettoRegione AWS che contiene l'indice. A tale scopo, crea autorizzazioni basate sull'identità per consentire ai responsabili di effettuare ricerche con le viste.

Ora puoi concedere le autorizzazioni per creare una visualizzazione. È possibile aggiungere le dichiarazioni in questo esempio alla stessa politica di autorizzazione utilizzata per concedere`Search` le autorizzazioni ai responsabili appropriati. Le azioni sono consentite o negate in base ai tag associati ai principali che chiamano le operazioni e l'indice a cui deve essere associata la vista. Il seguente esempio di policy IAM nega qualsiasi richiesta di creazione di una vista quando il valore del`Allow-Create-View` tag associato al principale del chiamante non corrisponde esattamente al valore dello stesso tag allegato all'indice nella Regione in cui è stata creata la vista.

```
{
    "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}"}
            }
        }
    ]
}
```

Consentire ai responsabili di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono allegate alla relativa identità utente. La policy include le autorizzazioni per completare questa operazione sulla console o a livello di programmazione utilizzando la AWS CLI o l'API AWS.

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

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

Esempi di politiche di controllo dei servizi per AWS Organizations e Resource Explorer

Esploratore di risorse AWS supporta le politiche di controllo dei servizi (SCP). Le SCP sono policy che collegano agli elementi di un'organizzazione per gestire le autorizzazioni all'interno di tale organizzazione. Un SCP si applica a tutti i membri di un'organizzazione Account AWS in base all'elemento a cui si collega l'SCP. Le SCP offrono un controllo centralizzato sulle autorizzazioni massime disponibili per tutti gli account dell'organizzazione. Possono aiutarvi a garantire che rispettiate le Account AWS linee guida per il controllo degli accessi della vostra organizzazione. Per ulteriori informazioni, consultare Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .

Prerequisiti

Per utilizzare le SCP, effettua innanzitutto le seguenti operazioni:

- Abilitazione di tutte le caratteristiche nell'organizzazione. Per ulteriori informazioni, consulta la sezione Abilitazione di tutte le caratteristiche nell'organizzazione nella Guida per l'utente di AWS Organizations .
- Abilita l'utilizzo delle SCP all'interno dell'organizzazione. Per ulteriori informazioni, consulta Abilitazione e disabilitazione dei tipi di policy nella Guida per l'utente di AWS Organizations .
- Crea le SCP di cui hai bisogno. Per ulteriori informazioni sulla creazione di SCP, consulta Creazione e aggiornamento di SCP nella Guida per l'AWS Organizations utente.

Policy di controllo dei servizi di esempio

L'esempio seguente mostra come utilizzare il controllo degli accessi basato sugli attributi (ABAC) per controllare l'accesso alle operazioni amministrative di Resource Explorer. Questa policy di esempio nega l'accesso a tutte le operazioni di Resource Explorer tranne le due autorizzazioni necessarie per la ricerca `resource-explorer-2:Search` e`resource-explorer-2:GetView`, a meno che il principale IAM che effettua la richiesta non sia taggato. `ResourceExplorerAdmin=TRUE` Per una discussione più completa sull'uso di ABAC con Resource Explorer, vedere. Utilizzo dell'autorizzazione basata sui tag per controllare l'accesso alle visualizzazioni

```
{
  "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 politiche gestite per Esploratore di risorse AWS

Una politica AWS gestita è una politica autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWSnella Guida per l'utente di IAM.

Politiche AWS gestite generali che includono le autorizzazioni di Resource Explorer

- AdministratorAccess— Garantisce l'accesso completo alle risorse Servizi AWS e alle risorse.
- ReadOnlyAccesso: consente l'accesso in sola lettura alle risorse e alle risorse. Servizi AWS
- ViewOnlyAccesso: concede le autorizzazioni per la visualizzazione di risorse e metadati di base per. Servizi AWS

> **Note**
>
> Le `Get*` autorizzazioni di Resource Explorer incluse nella `ViewOnlyAccess` policy funzionano come `List` le autorizzazioni, sebbene restituiscano solo un singolo valore, poiché una regione può contenere solo un indice e una visualizzazione predefinita.

AWS politiche gestite per Resource Explorer

- AWSResourceExplorerFullAccess
- AWSResourceExplorerReadOnlyAccess
- AWSResourceExplorerServiceRolePolicy

AWS politica gestita: AWSResourceExplorerFullAccess

Puoi assegnare la `AWSResourceExplorerFullAccess` policy alle tue identità IAM.

Questa policy concede autorizzazioni che consentono il pieno controllo amministrativo del servizio Resource Explorer. Puoi eseguire tutte le attività relative all'attivazione e alla gestione di Resource Explorer Regioni AWS nel tuo account.

Dettagli dell'autorizzazione

Questa politica include le autorizzazioni che consentono tutte le azioni di Resource Explorer, tra cui l'attivazione e la disattivazione di Resource Explorer Regioni AWS, la creazione o l'eliminazione di un indice di aggregazione per l'account, la creazione, l'aggiornamento e l'eliminazione di viste e la ricerca. Questa politica include anche le autorizzazioni che non fanno parte di Resource Explorer:

- `ec2:DescribeRegions`— consente a Resource Explorer di accedere ai dettagli sulle regioni del tuo account.
- `ram:ListResources`— consente a Resource Explorer di elencare le condivisioni di risorse di cui fanno parte le risorse.
- `ram:GetResourceShares`— consente a Resource Explorer di identificare i dettagli sulle condivisioni di risorse che possiedi o che sono condivise con te.
- `iam:CreateServiceLinkedRole`— consente a Resource Explorer di creare il ruolo collegato al servizio richiesto quando si attiva Resource Explorer creando il primo indice.

- `organizations:DescribeOrganization`— consente a Resource Explorer di accedere alle informazioni sull'organizzazione.

Per visualizzare la versione più recente di questa policy AWS gestita, consulta `AWSResourceExplorerFullAccess` la AWS Managed Policy Reference Guide.

AWS politica gestita: AWSResourceExplorerReadOnlyAccess

Puoi assegnare la `AWSResourceExplorerReadOnlyAccess` policy alle tue identità IAM.

Questa policy concede autorizzazioni di sola lettura che consentono agli utenti di accedere alla ricerca di base per scoprire le proprie risorse.

Dettagli dell'autorizzazione

Questa politica include autorizzazioni che consentono agli utenti di eseguire Resource Explorer `Get*` e `Search` operazioni per visualizzare informazioni sui componenti e sulle impostazioni di configurazione di Resource Explorer, ma non consente agli utenti di modificarle. `List*` Gli utenti possono anche effettuare ricerche. Questa politica include anche due autorizzazioni che non fanno parte di Resource Explorer:

- `ec2:DescribeRegions`— consente a Resource Explorer di accedere ai dettagli sulle regioni del tuo account.
- `ram:ListResources`— consente a Resource Explorer di elencare le condivisioni di risorse di cui fanno parte le risorse.
- `ram:GetResourceShares`— consente a Resource Explorer di identificare i dettagli sulle condivisioni di risorse che possiedi o che sono condivise con te.
- `organizations:DescribeOrganization`— consente a Resource Explorer di accedere alle informazioni sull'organizzazione.

Per visualizzare la versione più recente di questa policy AWS gestita, consulta `AWSResourceExplorerReadOnlyAccess` la AWS Managed Policy Reference Guide.

AWS politica gestita: AWSResourceExplorerServiceRolePolicy

Non puoi collegarti personalmente `AWSResourceExplorerServiceRolePolicy` a nessuna entità IAM. Questa policy può essere associata solo a un ruolo collegato al servizio che consente a

Resource Explorer di eseguire azioni per tuo conto. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Resource Explorer.

Questa politica concede le autorizzazioni necessarie a Resource Explorer per recuperare informazioni sulle risorse dell'utente. Resource Explorer popola gli indici che mantiene in ogni indice registrato. Regione AWS

Per vedere la versione più recente di questa policy AWS gestita, consulta `AWSResourceExplorerServiceRolePolicy` nella console IAM.

AWS politica gestita: AWSResourceExplorerOrganizationsAccess

Puoi assegnarle `AWSResourceExplorerOrganizationsAccess` alle tue identità IAM.

Questa politica concede autorizzazioni amministrative a Resource Explorer e concede autorizzazioni di sola lettura ad altri per supportare questo accesso. Servizi AWS L' AWS Organizations amministratore necessita di queste autorizzazioni per configurare e gestire la ricerca su più account nella console.

Dettagli dell'autorizzazione

Questa politica include le autorizzazioni che consentono agli amministratori di configurare la ricerca su più account per l'organizzazione:

- `ec2:DescribeRegions`— Consente a Resource Explorer di accedere ai dettagli sulle regioni del tuo account.
- `ram:ListResources`— Consente a Resource Explorer di elencare le condivisioni di risorse di cui fanno parte le risorse.
- `ram:GetResourceShares`— Consente a Resource Explorer di identificare i dettagli sulle condivisioni di risorse che possiedi o che sono condivise con te.
- `organizations:ListAccounts`— Consente a Resource Explorer di identificare gli account all'interno di un'organizzazione.
- `organizations:ListRoots`— Consente a Resource Explorer di identificare gli account root all'interno di un'organizzazione.
- `organizations:ListOrganizationalUnitsForParent`— Consente a Resource Explorer di identificare le unità organizzative (OU) in un'unità organizzativa principale o radice.
- `organizations:ListAccountsForParent`— Consente a Resource Explorer di identificare gli account di un'organizzazione contenuti nella radice o nell'unità organizzativa di destinazione specificata.

- `organizations:ListDelegatedAdministrators`— Consente a Resource Explorer di identificare gli AWS account designati come amministratori delegati in questa organizzazione.
- `organizations:ListAWSServiceAccessForOrganization`— Consente a Resource Explorer di identificare un elenco di Servizi AWS quelli abilitati all'integrazione con l'organizzazione.
- `organizations:DescribeOrganization`— Consente a Resource Explorer di recuperare informazioni sull'organizzazione a cui appartiene l'account dell'utente.
- `organizations:EnableAWSServiceAccess`— Consente a Resource Explorer di abilitare l'integrazione di un Servizio AWS (il servizio specificato da`ServicePrincipal`) con AWS Organizations.
- `organizations:DisableAWSServiceAccess`— Consente a Resource Explorer di disabilitare l'integrazione di un Servizio AWS (il servizio specificato da ServicePrincipal) con AWS Organizations.
- `organizations:RegisterDelegatedAdministrator`— Consente a Resource Explorer di consentire all'account membro specificato di amministrare le funzionalità dell'organizzazione del AWS servizio specificato.
- `organizations:DeregisterDelegatedAdministrator`— Consente a Resource Explorer di rimuovere il membro specificato Account AWS come amministratore delegato del membro specificato. Servizio AWS
- `iam:GetRole`— Consente a Resource Explorer di recuperare informazioni sul ruolo specificato, inclusi il percorso del ruolo, il GUID, l'ARN e la politica di fiducia del ruolo che concede l'autorizzazione ad assumere il ruolo.
- `iam:CreateServiceLinkedRole`— Consente a Resource Explorer di creare il ruolo collegato al servizio richiesto quando si attiva Resource Explorer creando il primo indice.

Per visualizzare la versione più recente di questa policy AWS gestita, consulta `AWSResourceExplorerOrganizationsAccess` nella console IAM.

Resource Explorer aggiorna le policy AWS gestite

Visualizza i dettagli sugli aggiornamenti alle politiche AWS gestite per Resource Explorer da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei documenti di Resource Explorer.

Modifica	Descrizione	Data
AWSResourceExplorerServiceRolePolicy- Autorizzazioni politiche aggiornate per visualizzare tipi di risorse aggiuntivi	Resource Explorer ha aggiunto le autorizzazioni alla politica relativa ai ruoli collegati al servizio AWSResourceExplorerServiceRolePolicy che consente a Resource Explorer di visualizzare tipi di risorse aggiuntivi: • apprunner:ListVpcConnectors • backup:ListReportPlans • emr-serverless:ListApplications • events:ListEventBuses • geo:ListPlaceIndexes • geo:ListTrackers • greengrass:ListComponents • greengrass:ListComponentVersions • iot:ListRoleAliases • iottwinmaker:ListComponentTypes • iottwinmaker:ListEntities • iottwinmaker:ListScenes	12 dicembre 2023

Modifica	Descrizione	Data
	• `kafka:ListConfigurations` • `kms:ListKeys` • `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`	
Nuove policy gestite da	Resource Explorer ha aggiunto la seguente AWS politica gestita: • AWSResourceExplorerOrganizationsAccess	14 novembre 2023

Modifica	Descrizione	Data
Policy gestite da aggiornate	Resource Explorer ha aggiornato le seguenti politiche AWS gestite per supportare la ricerca su più account: • AWSResourceExplorerFullAccess • AWSResourceExplorerReadOnlyAccess	14 novembre 2023
AWSResourceExplorerServiceRolePolicy— Politica aggiornata per supportare la ricerca su più account con Organizations	Resource Explorer ha aggiunto le autorizzazioni alla politica dei ruoli collegati al servizio AWSResourceExplorerServiceRolePolicy che consente a Resource Explorer di supportare la ricerca su più account con Organizations: • `organizations:ListAWSServiceAccessForOrganization` • `organizations:DescribeAccount` • `organizations:DescribeOrganization` • `organizations:ListAccounts` • `organizations:ListDelegatedAdministrators`	14 novembre 2023

Modifica	Descrizione	Data
AWSResourceExplorerServiceRolePolicy— Politica aggiornata per supportare tipi di risorse aggiuntivi	Resource Explorer ha aggiunto le autorizzazioni alla politica relativa ai ruoli collegati al servizio AWSResourceExplorerServiceRolePolicy che consente al servizio di indicizzare i seguenti tipi di risorse: • access analyzer: analyzer • acmpca: autorità di certificazione • amplify:app • amplify:ambiente di backend • amplify:branch • amplify:associazione di domini • amplifyuibuilder:componente • amplifyuibuilder: tema • integrazioni di app: integrazione di eventi • apprunner: servizio • appstream: appblock • appstream:applicazione • appstream: flotta • appstream: generatore di immagini • appstream: stack • appsync: graphqlapi	17 ottobre 2023

Modifica	Descrizione	Data
	• spazio dei nomi aps:ruleg roupsnamespace • aps:workspace • apigateway: restapi • apigateway: distribuzione • athena: catalogo dati • athena: gruppo di lavoro • scalabilità automatic a: gruppo di scalabilità automatica • backup: piano di backup • batch: ambiente di calcolo • batch: job queue • batch: politica di pianifica zione • formazione in cloud: pila • cloudformation: stackset • cloudfront: configurazione di crittografia a livello di campo • cloudfront: profilo di crittogra fia a livello di campo • cloudfront: controllo dell'accesso all'origine • cloudtrail: trail • codeartifact:domain • codeartifact:repository • codecommit: repository • codeguru profiler: gruppo di profilazione • connessioni codestar: connessione	

Modifica	Descrizione	Data
	• databrew: set di dati • databrew: ricetta • databrew: set di regole • investigativo: grafico • servizi di directory: directory • ec2: gateway portante • ec2: endpoint di accesso verificato • ec2: gruppo di accesso verificato • ec2: istanza di accesso verificata • ec2: fornitore di fiducia di accesso verificato • ecr: repository • elasticache: gruppo di sicurezza della cache • elasticfilesystem: punto di accesso • eventi:regola • evidentemente: esperimento • evidentemente: caratteri stica • evidentemente: lancio • evidentemente: progetto • finspace: ambiente • tubo antincendio: flusso di distribuzione • faultinjectionsimulator: modello di esperimento	

Modifica	Descrizione	Data
	• previsione: gruppo di set di dati • previsione: set di dati • rilevatore di frodi: rilevatore • rilevatore di frodi: tipo di entità • rilevatore di frodi: tipo di evento • rilevatore di frodi: etichetta • frauddetector:risultato • rilevatore di frodi: variabile • gamelift:alias • acceleratore globale: acceleratore • globalaccelerator:gruppo di endpoint • acceleratore globale: ascoltatore • glue:database • colla: lavoro • colla: tabella • colla: grilletto • erba verde: gruppo • healthlake: fhir datastore • sono: dispositivo mfa virtuale • imagebuilder/build version • imagebuilder: componente • imagebuilder: ricetta del contenitore	

Modifica	Descrizione	Data
	• imagebuilder: configura zione della distribuzione • imagebuilder: versione imagebuild • imagebuilder:imagepipeline • imagebuilder: imagerecipe • generatore di immagini: immagine • imagebuilder: configura zione dell'infrastruttura • iot: autorizzatore • iot: modello di lavoro • iot: azione di mitigazione • iot: modello di provisioning • iot:profilo di sicurezza • iot: cosa • iot: destinazione della regola dell'argomento • iotanalytics: canale • iotanalytics: set di dati • iotanalytics: datastore • iotanalytics:pipeline • iotevents: modello di allarme • iotevents: modello di rilevatore • ioteventi:input • iotsitewise: modello di asset • iotsitewise: risorsa • iotsitewise: gateway	

Modifica	Descrizione	Data
	• iottwinmaker:spazio di lavoro • iv: canale • ivs: streamkey • kafka: cluster • kinesisvideo: streaming • lambda: alias • lambda: versione a strati • lambda: livello • lookoutmetrics: alert • lookoutvision: progetto • pacchetto multimediale: canale • pacchetto multimediale: originendpoint • mediatailor: configurazione di riproduzione • memorydb:acl • memorydb: cluster • memorydb: gruppo di parametri • memorydb: utente • targeting mobile: app • targeting mobile: segmento • targeting:modello • firewall di rete: politica firewall • firewall di rete: firewall • gestore di rete: rete globale • gestore di rete: dispositivo	

Modifica	Descrizione	Data
	• gestore di rete: link • gestore di rete: allegato • gestore di rete: rete principal e • panorama: pacchetto • qldb: journalkinesisstre amforledger • qldb: libro mastro • rds: distribuzione bluegreen • refactorspaces: applicazione • refactorspaces: ambiente • refactorspaces:percorso • refactorspaces: servizio • ricognizione:progetto • resiliencehub: app • resiliencehub: politica di resilienza • gruppi di risorse: gruppo • route 53: gruppo di ripristino • route 53: set di risorse • route53: dominio firewall • route 53: gruppo di regole del firewall • route 53: resolverendpoint • route 53: resolverrule • sagemaker: modello • sagemaker: istanza per notebook • firmatario: profilo di firma	

Modifica	Descrizione	Data
	• ssm incidenti: piano di risposta • ssm: inserimento nell'inventario • ssm: sincronizzazione dei dati delle risorse • stati: attività • timestream:database • saggezza:assistente • saggezza: associazione assistente • saggezza: base di conoscenza	

Modifica	Descrizione	Data
AWSResourceExplorerServiceRolePolicy— Politica aggiornata per supportare tipi di risorse aggiuntivi	Resource Explorer ha aggiunto le autorizzazioni alla politica relativa ai ruoli collegati al servizio `AWSResourceExplorerServiceRolePolicy` che consente al servizio di indicizzare i seguenti tipi di risorse: • codebuild:progetto • codepipeline: pipeline • cognito: pool di identità • cognito: pool di utenti • ecr: repository • efs: filesystem • elasticbeanstalk: applicazione • elasticbeanstalk: versione dell'applicazione • elasticbeanstalk: ambiente • iot:politica • iot: regola tematica • step functions: statemachine • s3: secchio	1° agosto 2023

Modifica	Descrizione	Data
AWSResourceExplorerServiceRolePolicy— Politica aggiornata per supportare tipi di risorse aggiuntivi	Resource Explorer ha aggiunto le autorizzazioni alla politica relativa ai ruoli collegati al servizio `AWSResourceExplorerServiceRolePolicy` che consente al servizio di indicizzare i seguenti tipi di risorse: • elasticache: cluster • elasticache: gruppo di replica globale • elasticache: gruppo di parametri • elasticache: gruppo di replica • elasticache: istanza riservata • elasticache: istantanea • elasticache: gruppo di sottorete • elasticache: utente • elasticache: gruppo di utenti • lambda: code-signing-config • lambda: mappatura delle sorgenti degli eventi • sqs: coda	7 marzo 2023

Modifica	Descrizione	Data
Nuove policy gestite	Resource Explorer ha aggiunto le seguenti AWS politiche gestite: • AWSResourceExplorerFullAccess • AWSResourceExplorerReadOnlyAccess • AWSResourceExplorerServiceRolePolicy	7 novembre 2022
Resource Explorer ha iniziato a tenere traccia	Resource Explorer ha iniziato a tenere traccia delle modifiche relative alle politiche AWS gestite.	7 novembre 2022

Utilizzo di ruoli collegati ai servizi per Resource Explorer

Esploratore di risorse AWS utilizza ruoli collegati al servizio AWS Identity and Access Management(IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente a Resource Explorer. I ruoli collegati ai servizi sono predefiniti da Resource Explorer e includono tutte le autorizzazioni richieste dal servizio per chiamare altri utenti per tuo conto. Servizi AWS

Un ruolo collegato al servizio semplifica la configurazione di Resource Explorer perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Resource Explorer definisce le autorizzazioni dei suoi ruoli collegati ai servizi e, se non diversamente definito, solo Resource Explorer può assumerne i ruoli. Le autorizzazioni definite includono sia la politica di fiducia che la politica di autorizzazione e tale politica di autorizzazione non può essere assegnata a nessun'altra entità IAM.

Per informazioni sugli altri servizi che supportano i ruoli orientati ai servizi, consulta la pagina Servizi AWS supportati da IAM nella Guida per l'utente IAM. Qui, cerca i servizi con Sì nella colonna Ruoli collegati ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni di ruolo collegate ai servizi per Resource Explorer

Resource Explorer utilizza il ruolo collegato al servizio denominato. `AWSServiceRoleForResourceExplorer` Questo ruolo concede al servizio Resource Explorer le autorizzazioni per visualizzare risorse ed AWS CloudTrail eventi dell'utente per conto dell'utente Account AWS e per indicizzare tali risorse per supportare la ricerca.

Il ruolo `AWSServiceRoleForResourceExplorer` collegato al servizio affida il ruolo solo al servizio con il seguente responsabile del servizio:

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

La politica di autorizzazione dei ruoli denominata AWSResourceExplorerServiceRolePolicy consente l'accesso in sola lettura a Resource Explorer per recuperare i nomi e le proprietà delle risorse supportate. AWS Per visualizzare i servizi e le risorse supportati da Resource Explorer, vedi Tipi di risorse che puoi cercare con Resource Explorer. Per l'elenco completo di tutte le azioni che questo ruolo può eseguire, puoi visualizzare la `AWSResourceExplorerServiceRolePolicy` policy nella console IAM.

Un principale è un'entità IAM come un utente, un gruppo o un ruolo. Se consenti a Resource Explorer di creare automaticamente il ruolo collegato al servizio quando crea l'indice nella prima regione dell'account, il responsabile che esegue l'attività necessita solo delle autorizzazioni necessarie per creare l'indice Resource Explorer. Per creare manualmente il ruolo collegato al servizio utilizzando IAM, il responsabile che esegue l'attività deve disporre dell'autorizzazione per creare un ruolo collegato al servizio. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato al servizio per Resource Explorer

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando attivi Resource Explorer in o esegui AWS Management Console il primo CreateIndexRegione AWSnel tuo account utilizzando AWS CLI o un'AWSAPI, Resource Explorer crea automaticamente il ruolo collegato al servizio.

Se elimini questo ruolo collegato al servizio e poi devi crearlo di nuovo, puoi utilizzare la stessa procedura per ricreare il ruolo nel tuo account. Quando ti trovi RegisterResourceExplorernella prima regione del tuo account, Resource Explorer crea nuovamente il ruolo collegato al servizio per te.

Modifica di un ruolo collegato al servizio per Resource Explorer

Resource Explorer non consente di modificare il ruolo collegato al `AWSServiceRoleForResourceExplorer` servizio. Dopo aver creato un ruolo collegato al servizio, non puoi modificarne il nome, perché potrebbero farvi riferimento diverse entità. Puoi tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio per Resource Explorer

Puoi utilizzare la console IAMAWS CLI, o l'AWSAPI per eliminare manualmente il ruolo collegato al servizio. A tale scopo, devi prima rimuovere gli indici di Resource Explorer da ogni Regione AWS elemento del tuo account e poi eliminare manualmente il ruolo collegato al servizio.

> **Note**
>
> Se il servizio Resource Explorer utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione non riesce. In tal caso, assicurati che tutti gli indici di tutte le regioni vengano eliminati, quindi attendi qualche minuto e riprova l'operazione.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM, la AWS CLI o l'API AWS per eliminare il ruolo collegato ai servizi `AWSServiceRoleForResourceExplorer`. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi di Resource Explorer

Resource Explorer supporta l'utilizzo di ruoli collegati al servizio in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta gli Servizio AWSendpoint in. Riferimenti generali di Amazon Web Services

Risoluzione dei problemiEsploratore di risorse AWS delle autorizzazioni

Utilizza le informazioni seguenti per diagnosticare e risolvere i problemi comuni che possono verificarsi durante l'utilizzo diAWS Identity and Access Management Resuzione uzione uzione

Argomenti

- Non sono autorizzato/a eseguire un'operazione in Resource Explorer
- Voglio consentire a persone esterneAccount AWS al mio risorse Resource Explorer

Non sono autorizzato/a eseguire un'operazione in Resource Explorer

Se la AWS Management Console indica che non sei autorizzato a eseguire un'operazione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è la persona che ti ha fornito le credenziali utilizzate per eseguire questa operazione.

Ad esempio, l'errore seguente si verifica quando qualcuno assume il ruolo IAM`MyExampleRole` cerca di utilizzare la console per visualizzare i dettagli relativi a una vista ma non dispone di`resource-explorer-2:GetView` autorizzazioni.

```
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
```

In questo caso, la persona che utilizza il ruolo deve chiedere all'amministratore di aggiornare le politiche di autorizzazione del ruolo per consentire l'accesso alla vista utilizzando l'`resource-explorer-2:GetView`azione.

Voglio consentire a persone esterneAccount AWS al mio risorse Resource Explorer

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Resource Explorer supporta queste funzionalitàFunzionamento di Resource Explorer con IAM.
- Per informazioni su come garantire l'accesso alle risorse negli Account AWS che possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS in tuo possesso nella Guida per l'utente di IAM.
- Per informazioni su come fornire l'accesso alle risorse ad Account AWS di terze parti, consulta Fornire l'accesso agli Account AWS di proprietà di terze parti nella Guida per l'utente di IAM.

- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consultare Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Protezione dei dati in Esploratore di risorse AWS

Il modello di responsabilità condivisa di AWSsi applica alla protezione dei dati in Esploratore di risorse AWS. Come descritto in questo modello, AWSè responsabile della protezione dell'infrastruttura globale che esegue tutto l'Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. Inoltre, sei responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS che utilizzi. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS.

Per garantire la protezione dei dati, ti suggeriamo di proteggere le credenziali Account AWS e di configurare singoli utenti con AWS IAM Identity Center o AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Utilizza SSL/TLS per comunicare con le risorse AWS. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail.
- Utilizza le soluzioni di crittografia AWS, insieme a tutti i controlli di sicurezza predefiniti in Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se necessiti di moduli crittografici convalidati FIPS 140-2 quando accedi ad AWSattraverso un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Resource Explorer o altro Servizi AWS utilizzando la console, l'API o AWS gli SDK. AWS CLI I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Crittografia dei dati a riposo

I dati archiviati da Resource Explorer includono l'elenco indicizzato delle risorse e degli ARN associati utilizzati dal cliente e le visualizzazioni per accedervi.

Questi dati vengono crittografati quando sono inattivi utilizzando AWS Key Management Service(AWS KMS) chiavi di crittografia simmetriche che implementano l'Advanced Encryption Standard (AES) in Galois Counter Mode (GCM) con chiavi a 256 bit (AES-256-GCM).

Crittografia in transito

Le richieste dei clienti e tutti i dati associati vengono crittografati in transito utilizzando Transport Later Security (TLS) 1.2 o versione successiva. Tutti gli endpoint Resource Explorer supportano HTTPS per la crittografia dei dati in transito. Per un elenco degli endpoint del servizio Resource Explorer, consulta Esploratore di risorse AWSendpoint e quote in. Riferimenti generali di AWS

Convalida della conformità per Esploratore di risorse AWS

Per sapere se un programma Servizio AWS rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Ambito per programma di conformità. Per informazioni generali, consulta Programmi di conformità AWS.

È possibile scaricare i report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact Guida AWS Artifact per l'utente.

La responsabilità di conformità quando si utilizza Resource Explorer è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWSfornisce le seguenti risorse per contribuire alla conformità:

- Security and Compliance Quick Start Guides (Guide Quick Start Sicurezza e compliance): queste guide alla distribuzione illustrano considerazioni relative all'architettura e forniscono procedure per la distribuzione di ambienti di base incentrati sulla sicurezza e sulla conformità su AWS.

- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

  > **Note**
  >
  > Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- Risorse per la conformità AWS: una raccolta di cartelle di lavoro e guide suddivise per settore e area geografica.
- Valutazione delle risorse con le regole nella Guida per gli sviluppatori di AWS Config: AWS Config valuta il livello di conformità delle configurazioni delle risorse con pratiche interne, linee guida e regolamenti industriali.
- AWS Security Hub: Questo servizio AWS fornisce una visione completa dello stato di sicurezza all'interno di AWS che consente di verificare la conformità con gli standard e le best practice di sicurezza del settore.

Resilienza in Esploratore di risorse AWS

L'infrastrutturaAWS globale di è basata su è basataRegioni AWS su zone di disponibilità. Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, connesse tramite reti altamente ridondanti, a bassa latenza e throughput elevato. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le Zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili, rispetto alle infrastrutture a data center singolo o multiplo.

Per ulteriori informazioni sulle Regioni AWS e le zone di disponibilità, consulta Infrastruttura globale di AWS.

Sicurezza dell'infrastruttura in Esploratore di risorse AWS

Come servizio gestito, Esploratore di risorse AWS è protetto dalla sicurezza di rete globale AWS. Per informazioni sui servizi di sicurezza AWS e su come AWS protegge l'infrastruttura, consulta la pagina Sicurezza del cloud AWS. Per progettare l'ambiente AWS utilizzando le best practice per la sicurezza dell'infrastruttura, consulta la pagina Protezione dell'infrastruttura nel Pilastro della sicurezza di AWS Well-Architected Framework.

Tu usiAWSchiamate API pubblicate per accedere a Resource Explorer tramite la rete. I clienti devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa, è possibile utilizzare AWS Security Token Service (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

Per ulteriori informazioni suAWSprocedure globali di sicurezza della rete, vedereAmazon Web Services: panoramica dei processi di sicurezzawhite paper.

Monitoraggio di Esploratore di risorse AWS

Il monitoraggio è importante per garantire l'affidabilità, la disponibilità e le prestazioni diEsploratore di risorse AWS e delle altreAWS soluzioni. AWSfornisce i seguenti strumenti di monitoraggio per controllare Resource Explorer, segnalare un problema e intervenire automaticamente quando necessario:

- AWS CloudTrail acquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo Account AWS e fornisce i file di log a un bucket Simple Storage Service (Amazon S3) specificato. Puoi identificare quali utenti e account hanno richiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute. Per ulteriori informazioni, consulta Registrazione di chiamate API Esploratore di risorse AWS con AWS CloudTrail e la Guida per l'utente di AWS CloudTrail.

Registrazione di chiamate API Esploratore di risorse AWS con AWS CloudTrail

Esploratore di risorse AWSè integrato conAWS CloudTrail, un servizio che offre un record delle operazioni eseguite da un utente, un ruolo o unServizio AWS in Resource Explorer. CloudTrail acquisisce tutte chiamate API per Resource Explorer come eventi. Le chiamate acquisite includono le chiamate dalla console Resource Explorer e le chiamate di codice alle operazioni delle API Resource Explor

Se crei un percorso, puoi abilitare la distribuzione continua di CloudTrail eventi in un bucket Amazon S3, inclusi gli eventi per Resource Explorer. Un percorso è una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 specificato. Se non configuri un trail, è comunque possibile visualizzare gli eventi più recenti nella console di CloudTrail in Event history (Cronologia eventi). Le informazioni raccolte da permettono CloudTrail di determinare la richiesta effettuata a Resource Explorer, l'indirizzo IP da cui è partita la richiesta, l'autore della richiesta, il momento in cui è stata eseguita e altri dettagli.

Per ulteriori informazioni CloudTrail, consulta la Guida perAWS CloudTrail l'utente.

Informazioni su Resource Explorer in CloudTrail

CloudTrail è abilitato sul tuo alAccount AWS momento della sua creazione. Quando si verifica un'attività in Resource Explorer, questa viene registrata in un CloudTrail evento insieme ad

altriServizio AWS eventi nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nell'Account AWS. Per ulteriori informazioni, consulta Visualizzazione di eventi mediante la cronologia CloudTrail eventi.

> **Important**
>
> Puoi trovare tutti gli eventi di Resource Explorer cercando Event source = resource-explorer-2.amazonaws.com

Per una registrazione continua degli eventi nella tuaAccount AWS, inclusi gli eventi per Resource Explorer, crea un trail. Un trail consente di CloudTrail distribuire i file di log in un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il percorso registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, è possibile configurare altriServizi AWS per analizzare con maggiore dettaglio e usare i dati raccolti nei CloudTrail log. Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utenteAWS CloudTrail:

- Creazione di un trail per il tuo Account AWS
- AWSintegrazioni di servizi con CloudTrail Logs
- Configurazione Amazon SNS per CloudTrail
- Ricezione di CloudTrail log da più regioni
- Ricezione di CloudTrail log da più account

Tutte le operazioni Clouroot vengono registrate CloudTrail e sono documentate nella documentazione di riferimento delleEsploratore di risorse AWS API. Ad esempio, le chiamate a`CreateIndex`e`DeleteIndex`, e`UpdateIndex` le azioni generano voci nei file di CloudTrail registro.

Ogni evento o voce di log contiene informazioni che consentono di determinare chi ha effettuato la richiesta.

- Account AWSCutente root root root root root
- Credenziali di sicurezza temporanee fornite da un ruolo AWS Identity and Access Management (IAM) o un utente federato.
- Credenziali di sicurezza a lungo termine fornite da un utente IAM.
- Un altro servizio AWS.

> **Important**
>
> Per motivi di sicurezza`TagsFilters`, tutti i`QueryString` valori e i valori vengono eliminati dalle voci del CloudTrail percorso.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Informazioni sulle voci del log di Resource Explorer Explorer

Un trail è una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di log possono contenere una o più voci di log. Un evento rappresenta una singola richiesta da un'origine e include informazioni sull'operazione richiesta, data e ora dell'operazione, parametri della richiesta e così via. CloudTrail i file di log non sono una traccia stack ordinata delle chiamate API pubbliche e di conseguenza non appaiono in base a un ordine specifico.

Argomenti

- CreateIndex
- DeleteIndex
- UpdateIndexType
- Cerca
- CreateView
- DeleteView
- DisassociateDefaultView

CreateIndex

L'esempio seguente mostra una voce di CloudTrail log che illustra l'`CreateIndex`operazione.

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

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

DeleteIndex

L'esempio seguente mostra una voce CloudTrail lunga che illustra l'`DeleteIndex`operazione.

> **Note**
>
> Questa azione elimina anche in modo asincrono tutte le visualizzazioni dell'account in quella regione, il che si traduce in un`DeleteView` evento per ogni vista eliminata.


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

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

UpdateIndexType

L'esempio seguente mostra una voce di CloudTrail registro che dimostra l'`UpdateIndexType`azione per promuovere un indice da tipo`LOCAL` a`AGGREGATOR`.

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

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


Cerca

L'esempio seguente mostra una voce di CloudTrail log che illustra l'`Search`operazione.

> **Note**
>
> Per motivi di sicurezza, tutti i`Tag` riferimenti e`QueryString` i parametri vengono oscurati nelle voci del CloudTrail percorso.`Filters`

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

CreateView

L'esempio seguente mostra una voce di CloudTrail log che illustra l'`CreateView`operazione.


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

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

DeleteView

L'esempio seguente mostra una voce di CloudTrail registro che dimostra l'evento che può verificarsi quando l'`DeleteView`azione viene avviata automaticamente a causa di un'`DeleteIndex`operazione nella stessaRegione AWS.

> **Note**
>
> Se la vista eliminata è la vista predefinita per la regione, questa azione dissocia anche la vista in modo asincrono come predefinita. Questo produce un`DisassociateDefaultView` evento.

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

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


DisassociateDefaultView

L'esempio seguente mostra una voce di CloudTrail registro che dimostra l'evento che può verificarsi quando l'`DisassociateDefaultView`azione viene avviata automaticamente a causa di un'`DeleteView`operazione nella vista predefinita corrente.


```
{
    "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"
}
```

Creazione di risorse Resource Explorer con CloudFormation

Esploratore di risorse AWSè integrato conAWS CloudFormation, un servizio che consente di modellare e configurare le AWS risorse. Questa integrazione consente di dedicare meno tempo alla creazione e alla gestione delle risorse e dell'infrastruttura. Puoi creare un modello che descrive tutte le risorse AWS desiderate e CloudFormation si occuperà del provisioning e della configurazione di queste risorse per tuo conto. Esempi di risorse includono indici, viste o l'assegnazione di una vista predefinita per un. Regione AWS

Quando usiCloudFormation, puoi riutilizzare il modello per configurare le risorse di Resource Explorer in modo coerente e continuo. Descrivi le risorse una volta, quindi esegui il provisioning delle stesse risorse più volte in più Regioni Account AWS e.

Utilizzo AWS CloudFormation per distribuire Resource Explorer su AWS Organizations

Puoi utilizzarlo AWS CloudFormation StackSets per distribuire Resource Explorer su tutti gli account della tua organizzazione. Quando aggiungi o crei account membri nella tua organizzazione, StackSets puoi configurare automaticamente gli indici in ciascuno di essiRegione AWS, incluso un indice aggregatore dove lo specifichi, per ogni nuovo account membro. Per istruzioni, consulta Distribuzione di Resource Explorer agli account di un'organizzazione.

Resource Explorer e CloudFormation modelli

Per eseguire il provisioning e la configurazione delle risorse per Resource Explorer e per i servizi correlati, devi conoscere AWS CloudFormationi modelli. I modelli sono file di testo formattati in JSON o YAML. Questi modelli descrivono le risorse di cui intendi effettuare il provisioning negli stack CloudFormation. Se non hai familiarità con JSON o YAML, puoi usare AWS CloudFormation Designer per iniziare a utilizzare i modelli CloudFormation. Per ulteriori informazioni, consulta Che cos'è AWS CloudFormation Designer? nella Guida per l'utente di AWS CloudFormation.

Resource Explorer supporta la creazione dei seguenti tipi di risorse inCloudFormation:

- Indice: crea un indice in una regione e attiva Resource Explorer in quella regione. È possibile specificare che l'indice sia locale o l'indice aggregatore per. Account AWS Per ulteriori informazioni, consultare Attivazione di Resource Explorer in unRegione AWS per indicizzare le risorse e Attivazione della ricerca tra aree geografiche creando un indice di aggregazione.
- Visualizza: crea una vista che determina quali risultati possono apparire quando un utente esegue una ricerca. Ogni operazione di ricerca deve specificare una vista. Devi concedere agli utenti

l'autorizzazione per usando le visualizzazioni alle quali desideri che accedano. Per ulteriori informazioni, consulta Gestione delle visualizzazioni di Resource Explorer per fornire l'accesso alla ricerca.

> **Note**
>
> È necessario creare un indice in una regione prima di poter creare una vista in quella stessa regione. Se create un indice e lo visualizzate come parte dello stesso stack, utilizzate l'`DependsOn`attributo sulla vista, come mostrato nel seguente modello di esempio, per assicurarvi che l'indice venga creato per primo.

- DefaultViewAssociation— Assegna la visualizzazione specificata come predefinita nella relativa regione. Quando un utente non specifica esplicitamente la vista da utilizzare per un'operazione di ricerca, Resource Explorer tenta di utilizzare la visualizzazione predefinita associata alla regione in cui l'utente esegue la ricerca. Per ulteriori informazioni, consulta Impostazione di una visualizzazione predefinita in unRegione AWS.

L'esempio seguente illustra come è possibile creare un indice e una vista nella stessa regione e impostare la visualizzazione come predefinita per la regione.

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"
                }
            }
```

```
        }
    }
}
```

Per ulteriori informazioni, inclusi esempi di modelli JSON e YAML per gli indici e le viste di Resource Explorer, consulta Riferimento ai tipi di risorse ResourceExplorer nella Guida per l'utente di. AWS CloudFormation

Ulteriori informazioni su AWS CloudFormation

Per ulteriori informazioni su CloudFormation, consulta le seguenti risorse:

- AWS CloudFormation
- Guida per l'utente di AWS CloudFormation
- Guida per l'utente dell'interfaccia a riga di comando di AWS CloudFormation

Risoluzione dei problemi di Resour

Se si verificano problemi durante l'utilizzo di Resource Explorer, consulta gli argomenti in questa sezione. Vedi anche Risoluzione dei problemi Esploratore di risorse AWS delle autorizzazioni nella sezione Sicurezza di questa guida.

Argomenti

- Problemi generali (questa pagina)
- Risoluzione dei problemi di installazione e configurazione di Resource Explorer
- Risoluzione dei problemi di ricerca di Resource Explor

Problemi generali

Argomenti

- Ho ricevuto un collegamento a Resource Explorer ma quando lo apro, la console mostra solo un errore.
- Perché la ricerca unificata nella console causa errori di «accesso negato» nei miei CloudTrail registri?

Ho ricevuto un collegamento a Resource Explorer ma quando lo apro, la console mostra solo un errore.

Alcuni strumenti di terze parti producono link a pagine in Resource Explorer. In alcuni casi, questi URL non includono il parametro che indirizza la console a uno specificoRegione AWS. Se apri un collegamento di questo tipo, alla console di Resource Explorer non viene detto quale regione utilizzare e per impostazione predefinita utilizza l'ultima regione a cui l'utente ha effettuato l'accesso. Se l'utente non dispone delle autorizzazioni per accedere a Resource Explorer in quella regione, la console tenta di utilizzare la regione Stati Uniti orientali (Virginia settentrionale`us-east-1`) () o Stati Uniti occidentali (Oregon) (`us-west-2`) se la console non riesce a raggiungerla`us-east-1`.

Se l'utente non dispone dell'autorizzazione per accedere all'indice in nessuna di queste regioni, la console Resource Explorer restituisce un errore.

Puoi prevenire questo problema assicurandoti che tutti gli utenti dispongano delle seguenti autorizzazioni:

- `ListIndexes`— nessuna risorsa specifica; uso*.
- `GetIndex`per l'ARN di ogni indice creato nell'account. Per evitare di dover ripetere i criteri di autorizzazione se si elimina e si ricrea un indice, si consiglia di utilizzarlo*.

La politica minima per raggiungere questo obiettivo potrebbe essere simile a questo esempio:

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

In alternativa, potresti prendere in considerazione l'idea di allegare l'autorizzazioneAWS gestitaAWSResourceExplorerReadOnlyAccess a tutti gli utenti che devono utilizzare Resource Explorer. Ciò garantisce le autorizzazioni necessarie, oltre alle autorizzazioni necessarie per visualizzare le viste disponibili nella Regione ed effettuare ricerche utilizzando tali visualizzazioni.

Perché la ricerca unificata nella console causa errori di «accesso negato» nei miei CloudTrail registri?

Ricerca unificata inAWS Management Console consente ai principali di cercare da qualsiasi pagina delAWS Management Console. I risultati possono includere risorse dell'account del committente se Resource Explorer è attivato e configurato per supportare la ricerca unificata. Ogni volta che inizi a digitare nella barra di ricerca unificata, la ricerca unificata tenta di richiamare`resource-explorer-2:ListIndexes` l'operazione per verificare se può includere risorse dell'account dell'utente nei risultati.

La ricerca unificata utilizza le autorizzazioni dell'utente attualmente connesso per eseguire questo controllo. Se l'utente non dispone dell'autorizzazione alle chiamate`resource-explorer-2:ListIndexes` concessa in una politica di autorizzazione allegataAWS Identity and

Access Management (IAM), il controllo ha esito negativo. Tale errore viene aggiunto come`Access denied` voce nei CloudTrail registri.

Questa voce di CloudTrail registro presenta le caratteristiche seguenti:

- Fonte dell'evento:`resource-explorer-2.amazonaws.com`
- Nome dell'evento:`ListIndexes`
- Codice di errore:`403` (accesso negato)

Le seguenti politicheAWS gestite includono l'autorizzazione alle chiamate`resource-explorer-2:ListIndexes`. Se assegni una di queste norme al committente o qualsiasi altra politica che includa questa autorizzazione, questo errore non si verifica:

- AWSResourceExplorerReadOnlyAccess
- AWSResourceExplorerFullAccess
- ReadOnlyAccess
- ViewOnlyAccess

Risoluzione dei problemi di installazione e configurazione di Resource Explorer

Utilizza le informazioni contenute in questa pagina per diagnosticare e risolvere i problemi che possono verificarsi durante l'installazione o la configurazione inizialeEsploratore di risorse AWS.

Argomenti

- Messaggio accesso rifiutato quando effettua una richiesta a Resource Explorer
- Visualizzo un messaggio di accesso negato quando effettuo una richiesta con credenziali di sicurezza provvisorie.

Messaggio accesso rifiutato quando effettua una richiesta a Resource Explorer

- Verificare di disporre delle autorizzazioni per chiamare l'operazione e le risorse richieste. Un amministratore può concedere le autorizzazioni assegnando una politica di autorizzazioneAWS

Identity and Access Management (IAM) al responsabile IAM, ad esempio un ruolo, un gruppo o un utente.

Per fornire l'accesso, aggiungi autorizzazioni ai tuoi utenti, gruppi o ruoli:

- Utenti e gruppi in AWS IAM Identity Center:

  Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina Create a permission set (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center.

- Utenti gestiti in IAM tramite un provider di identità:

  Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina Creating a role for a third-party identity provider (federation) (Creazione di un ruolo per un provider di identità di terze parti [federazione]) nella Guida per l'utente di IAM.

- Utenti IAM:
  - Crea un ruolo che l'utente possa assumere. Per istruzioni, consulta la pagina Creating a role for an IAM user (Creazione di un ruolo per un utente IAM) nella Guida per l'utente di IAM.
  - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina Aggiunta di autorizzazioni a un utente (console) nella Guida per l'utente di IAM.

La politica deve consentire quanto richiesto`Action` sul sito a`Resource` cui si desidera accedere.

Se le dichiarazioni politiche che concedono tali autorizzazioni includono condizioni, ad esempio time-of-day restrizioni relative all'indirizzo IP, è necessario soddisfare tali requisiti anche quando si invia la richiesta. Per informazioni sulla visualizzazione o sulla modifica delle policy per un utente di IAM, consulta Gestione delle policy per l'utente di IAM.

- Se firmi manualmente le richieste API (senza utilizzare gli AWSSDK), verifica di aver firmato la richiesta correttamente.

Visualizzo un messaggio di accesso negato quando effettuo una richiesta con credenziali di sicurezza provvisorie.

- Verifica che l'utente di IAM utilizzato per effettuare la richiesta disponga delle autorizzazioni corrette. Le autorizzazioni per le credenziali di sicurezza temporanee sono derivate da un principio definito in IAM, quindi le autorizzazioni sono limitate a quelle concesse al committente. Per Scopri come vengono determinate le autorizzazioni per le credenziali di sicurezza temporanee, consulta

Controllo delle autorizzazioni per le credenziali di sicurezza provvisorie nella Guida per l'utente di IAM.

- Verificare che le richieste vengano firmate correttamente e che il formato della richiesta sia valido. Per i dettagli, consulta la documentazione del toolkit per l'SDK scelto o Utilizzo di credenziali temporanee conAWS risorse nella Guida per l'utente IAM.
- Verifica che le credenziali di sicurezza provvisorie non siano scadute. Per ulteriori informazioni, consulta Richiesta di credenziali di sicurezza temporanee nella Guida per l'utente IAM.

Risoluzione dei problemi di ricerca di Resource Explor

Usa le informazioni qui per aiutarti a diagnosticare e correggere gli errori più comuni che possono verificarsi durante la ricerca di risorse utilizzando Resource Explorer.

Argomenti

- Perché mancano alcune risorse nei risultati di ricerca di Resource Explorer?
- Perché le mie risorse non vengono visualizzate nei risultati di ricerca unificati della console?
- Perché la ricerca unificata nella console e in Resource Explorer a volte dà risultati diversi?
- Di quali autorizzazioni ho bisogno per poter cercare risorse?

Perché mancano alcune risorse nei risultati di ricerca di Resource Explorer?

L'elenco seguente fornisce i motivi per cui alcune risorse potrebbero non essere visualizzate nei risultati di ricerca come previsto:

L'indicizzazione iniziale non è completa

> Dopo aver attivato Resource Explorer per la prima volta in unRegione AWS, il completamento dell'indicizzazione e della replica nell'indice di aggregazione può richiedere fino a 36 ore. Riprova la ricerca più tardi.

La risorsa è nuova

> Potrebbero essere necessari alcuni minuti prima che una nuova risorsa venga scoperta da Resource Explorer e aggiunta all'indice locale. Riprova tra qualche minuto.

Le informazioni su una nuova risorsa in una regione non sono ancora state propagate all'indice dell'aggregatore

Può essere necessario del tempo prima che i dettagli su una nuova risorsa scoperta in una regione vengano indicizzati nella regione corrispondente e quindi replicati nell'indice di aggregazione dell'account. La nuova risorsa può essere visualizzata nei risultati di ricerca interregionali solo dopo il completamento della replica. Riprova la ricerca più tardi.

La regione in cui è presente la risorsa non ha Resource Explorer attivato

L'amministratore determina in quale ambiente Regioni AWS può operare il Resource Explorer. La pagina Impostazioni mostra in quali regioni è attivo Resource Explorer e in quali aree è presente un indice. Se la regione con la risorsa non è attiva, chiedi all'amministratore di attivare Resource Explorer in quella regione.

La risorsa esiste in un'altra regione e la regione cercata non contiene l'indice dell'aggregatore

Puoi cercare risorse in tutte le regioni dell'account solo utilizzando una visualizzazione nella regione che contiene l'indice dell'aggregatore. Le ricerche in qualsiasi altra regione restituiscono risorse solo dalla regione in cui viene eseguita la ricerca.

I filtri sulla visualizzazione escludono quella risorsa

Ogni vista può includere filtri nella configurazione che limitano i risultati che possono essere inclusi nei risultati di ricerca creati con quella vista. Assicurati che la risorsa che stai cercando corrisponda ai filtri nella visualizzazione che stai utilizzando per la ricerca. Per ulteriori informazioni sui filtri, consultaFiltri. Per ulteriori informazioni sulle visualizzazioni, vedereInformazioni sulle visualizzazioni Resource Explorer.

Il tipo di risorsa non è supportato da Resource Explorer

Alcuni tipi di risorse non sono supportati da Resource Explorer. Per ulteriori informazioni, consulta Tipi di risorse che puoi cercare con Resource Explorer.

Gli indici o le viste non sono configurati nella regione della console

Se gli indici o le viste non sono configurati nelle regioni previste dalla console che utilizza il widget, non vedrai i risultati previsti. Per ulteriori informazioni, consulta Attivazione della ricerca tra aree geografiche creando un indice di aggregazione e Informazioni sulle visualizzazioni Resource Explorer.

Le tue visualizzazioni non includono tag

I tag sono richiesti dal widget Resource Explorer. Se le tue visualizzazioni non includono tag, le risorse non verranno incluse nei risultati. Per ulteriori informazioni, consulta Aggiunta di tag alle visualizzazioni.

La ricerca utilizza la sintassi della query di ricerca errata

La ricerca in Resource Explorer è esclusiva di questo servizio. Senza la sintassi corretta, non troverai le risorse che ti aspetti. Per ulteriori informazioni, consulta Riferimento alla sintassi delle query di ricerca per Resource Explorer.

Di recente hai taggato le tue risorse

Dopo aver taggato una risorsa, c'è un ritardo di 30 secondi prima che la risorsa venga visualizzata nei risultati di ricerca.

Il tipo di risorsa non supporta i filtri per tag

Se i filtri di tag non sono supportati dal tipo di risorsa, non verranno visualizzati nel widget Resource Explorer. I tipi di risorse che non supportano i filtri di tag sono:

- `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`

Perché le mie risorse non vengono visualizzate nei risultati di ricerca unificati della console?

I risultati di ricerca unificati sono disponibili nella barra di ricerca nella parte superiore di ogni pagina. AWS Management Console Tuttavia, la ricerca può restituire risorse che corrispondono alla query nei risultati di ricerca solo dopo aver completato le seguenti opzioni di configurazione:

- Deve esserci un indice di aggregazione in una delle regioni dell'account.
- Nella Regione deve essere presente una vista predefinita che contenga l'indice dell'aggregatore.
- Tutti i principali (ruoli e utenti IAM) devono disporre dell'autorizzazione per effettuare ricerche utilizzando quella visualizzazione predefinita.

Perché la ricerca unificata nella console e in Resource Explorer a volte dà risultati diversi?

I risultati di ricerca unificati sono disponibili nella barra di ricerca nella parte superiore di ogni AWS Management Console pagina. Quando si utilizza la ricerca unificata, il processo di ricerca unificata inserisce automaticamente un carattere jolly (*) alla fine del primo termine digitato nella stringa di query. Questo carattere jolly non è visibile nella casella di ricerca unificata, ma influisce sui risultati.

> **Important**
>
> La ricerca unificata inserisce automaticamente un operatore di caratteri jolly (*) alla fine della prima parola chiave della stringa. Ciò significa che i risultati della ricerca unificata includono risorse che corrispondono a qualsiasi stringa che inizia con la parola chiave specificata. La ricerca eseguita dalla casella di testo Query nella pagina di ricerca delle risorse della console Resource Explorer non aggiunge automaticamente un carattere jolly. È possibile inserire * manualmente un dopo qualsiasi termine nella stringa di ricerca.

Di quali autorizzazioni ho bisogno per poter cercare risorse?

Per eseguire la ricerca, è necessario disporre dell'autorizzazione per eseguire entrambe le operazioni seguenti su una visualizzazione che si trova nella regione in cui si chiama l'operazione:

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

Ciò può essere fatto aggiungendo un'istruzione simile all'esempio seguente a una policy assegnata al responsabile IAM.

```
        {
            "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"
        }
```

Puoi sostituire l'Amazon Resource Number (ARN) di una vista specifica con un ARN che include un carattere jolly (*) per concedere l'autorizzazione a tutte le viste corrispondenti.

Se non specifichi una visualizzazione nella richiesta, Resource Explorer utilizza automaticamente la visualizzazione predefinita per la regione in cui hai effettuato la richiesta. Se non disponi delle autorizzazioni per utilizzare la visualizzazione predefinita, rivolgiti all'amministratore.

> **Note**
>
> Anche se vedi una risorsa nei risultati di una query di ricerca di Resource Explorer, hai bisogno delle autorizzazioni sulla risorsa stessa per poter interagire con quella risorsa.

Tipi di risorse che puoi cercare con Resource Explorer

Argomenti

- Servizi e tipi di risorse supportati
- Accesso programmatico all'elenco dei tipi di risorse supportati
- Tipi di risorse che appaiono come altri tipi

Nelle tabelle seguenti sono elencati i tipi di risorse supportati per la ricerca Esploratore di risorse AWS.

> **Note**
>
> - Alcuni tipi di risorse sono identificati da stringhe Amazon resource name (ARN) che condividono un formato comune con un altro tipo di risorsa. Quando ciò accade, Resource Explorer può segnalare risorse come quell'altro tipo di risorsa. Per un elenco dei tipi di risorse interessati da questo problema, vedereTipi di risorse che appaiono come altri tipi.
> - Al momento, i tag allegati alle risorse AWS Identity and Access Management (IAM), come ruoli o utenti, non possono essere utilizzati per la ricerca.
> - Se hai accesso crittografato ad alcune delle tue risorse, Resource Explorer non è in grado di rilevarle. Queste risorse non verranno visualizzate nei risultati della ricerca.

Servizi e tipi di risorse supportati

Supportati Servizi AWS

- Amazon API Gateway
- AWS App Runner
- Amazon AppStream 2.0
- AWS AppSync
- Amazon Athena
- AWS Backup
- AWS Batch

- AWS CloudFormation
- Amazon CloudFront
- AWS CloudTrail
- Amazon CloudWatch
- Amazon CloudWatch evidentemente
- CloudWatch Registri Amazon
- AWS CodeArtifact
- AWS CodeBuild
- AWS CodeCommit
- Amazon CodeGuru Profiler
- AWS CodePipeline
- AWS CodeConnections
- Amazon Cognito
- Amazon Connect
- Amazon Connect Wisdom
- Amazon Detective
- Amazon DynamoDB
- EC2 Image Builder
- Amazon ECR
- AWS Elastic Beanstalk
- Amazon ElastiCache
- Amazon Elastic Compute Cloud (Amazon EC2)
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- Amazon Elastic File System
- Sistema di bilanciamento del carico elastico
- AWS Elemental MediaPackage
- AWS Elemental MediaTailor
- Amazon EMR Serverless

- 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
- Flusso di video Amazon Kinesis
- AWS Lambda
- Amazon Lex
- Servizio di posizione Amazon
- Amazon Lookout per le metriche
- Amazon Lookout per Vision
- Servizio gestito da Amazon per Apache Flink
- Amazon Managed Service per Prometheus
- Amazon Managed Service per Prometheus
- Amazon Managed Streaming per Apache Kafka
- AWS Migration Hub Refactor Spaces

- AWS Network Firewall
- AWS Network Manager
- OpenSearch Servizio Amazon
- AWS Panorama
- Amazon Personalize
- AWS Private Certificate Authority
- Amazon QLDB
- Amazon Redshift
- Amazon Rekognition
- Amazon Relational Database Service (Amazon RDS)
- AWS Resilience Hub
- AWS Resource Groups
- Esploratore di risorse AWS
- Amazon Route 53
- Preparazione al ripristino di 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
- Accesso verificato da AWS
- AWS Wavelength

Amazon API Gateway

- `apigateway:restapis`

AWS App Runner

- apprunner:vpcconnector

Amazon AppStream 2.0

- appstream:appblock
- appstream:application
- appstream:fleet
- appstream:stack

AWS AppSync

- appsync:apis

Amazon Athena

- athena:datacatalog
- athena:workgroup

AWS Backup

- backup:backupplan

AWS Batch

- batch:computeenvironment
- batch:jobqueue
- batch:schedulingpolicy

AWS CloudFormation

- cloudformation:stack

- cloudformation:stackset

Amazon CloudFront

- cloudfront:cache-policy
- cloudfront:distribution
- cloudfront:function
- cloudfront:fieldlevelencryptionconfig
- cloudfront:fieldlevelencryptionprofile
- cloudfront:origin-access-identity
- cloudfront:originaccesscontrol
- cloudfront:origin-request-policy
- cloudfront:realtime-log-config
- cloudfront:response-headers-policy

AWS CloudTrail

- cloudtrail:trail

Amazon CloudWatch

- cloudwatch:alarm
- cloudwatch:dashboard
- cloudwatch:insight-rule
- cloudwatch:metric-stream
- evidently:project

Amazon CloudWatch evidentemente

- evidently:project/experiment
- evidently:project/feature
- evidently:project/launch

CloudWatch Registri 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

Amazon Connect Wisdom

- wisdom:assistant
- wisdom:association
- wisdom:knowledge-base

Amazon Detective

- detective:graph

Amazon DynamoDB

- dynamodb:table

EC2 Image Builder

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

Amazon ECR

- ecrpublic:repository

AWS Elastic Beanstalk

- elasticbeanstalk:application
- elasticbeanstalk:applicationversion
- elasticbeanstalk:configurationtemplate
- elasticbeanstalk:environment

Amazon ElastiCache

- elasticache:cluster
- elasticache:globalreplicationgroup
- elasticache:parametergroup
- elasticache:replicationgroup
- elasticache:reserved-instance
- elasticache:snapshot
- elasticache:subnetgroup
- elasticache:user
- elasticache:usergroup

Amazon Elastic Compute Cloud (Amazon EC2)

- ec2:capacity-reservation
- ec2:capacity-reservation-fleet
- ec2:client-vpn-endpoint
- ec2:customer-gateway
- ec2:dedicated-host
- ec2:dhcp-options
- ec2:egress-only-internet-gateway
- ec2:elastic-gpu
- ec2:elastic-ip

- ec2:fleet
- ec2:fpga-image
- ec2:host-reservation
- ec2:image
- ec2:instance
- ec2:instance-event-window
- ec2:internet-gateway
- ec2:ipam
- ec2:ipam-pool
- ec2:ipam-scope
- ec2:ipv4pool-ec2
- ec2:key-pair
- ec2:launch-template
- ec2:natgateway
- ec2:network-acl
- ec2:network-insights-access-scope
- ec2:network-insights-access-scope-analysis
- ec2:network-insights-analysis
- ec2:network-insights-path
- ec2:network-interface
- ec2:placement-group
- ec2:prefix-list
- ec2:reserved-instances
- ec2:route-table
- ec2:security-group
- ec2:security-group-rule
- ec2:snapshot
- ec2:spot-fleet-request
- ec2:spot-instances-request

- ec2:subnet
- ec2:subnet-cidr-reservation
- ec2:traffic-mirror-filter
- ec2:traffic-mirror-filter-rule
- ec2:traffic-mirror-session
- ec2:traffic-mirror-target
- ec2:transit-gateway
- ec2:transit-gateway-attachment
- ec2:transit-gateway-connect-peer
- ec2:transit-gateway-multicast-domain
- ec2:transit-gateway-policy-table
- ec2:transit-gateway-route-table
- ec2:transitgatewayroutetableannouncement
- ec2:volume
- ec2:vpc
- ec2:vpc-endpoint
- ec2:vpc-flow-log
- ec2:vpc-peering-connection
- ec2:vpn-connection
- ec2:vpn-gateway

Amazon Elastic Container Registry

- ecr:repository

Amazon Elastic Container Service

- ecs:cluster
- ecs:container-instance
- ecs:service

- ecs:task
- ecs:task-definition
- ecs:task-set

Amazon Elastic File System

- efs:filesystem
- efs:accesspoint

Sistema di bilanciamento del carico elastico

- elasticloadbalancing:listener
- elasticloadbalancing:listener-rule
- elasticloadbalancing:listener-rule/app
- elasticloadbalancing:listener/app
- elasticloadbalancing:listener/net
- elasticloadbalancing:loadbalancer
- elasticloadbalancing:loadbalancer/app
- elasticloadbalancing:loadbalancer/net
- elasticloadbalancing:targetgroup

AWS Elemental MediaPackage

- mediapackage:channel
- mediapackage:originendpoint
- mediapackage-vod:packaging-configurations
- mediapackage-vod:packaging-groups

AWS Elemental MediaTailor

- mediatailor:playbackConfiguration

Amazon EMR Serverless

- emr-serverless:applications

Amazon EventBridge

- events:event-bus
- events:rule

AWS Fault Injection Service

- fis:experimenttemplate

Amazon Forecast

- forcast:dataset
- forcast:dataset-group

Amazon Fraud Detector

- frauddetector:detector
- frauddetector:entity-type
- frauddetector:event-type
- frauddetector:label
- frauddetector:outcome
- frauddetector:variable

Amazon GameLift

- gamelift:alias

AWS Global Accelerator

- globalaccelerator:accelerator
- globalaccelerator:accelerator/listener
- globalaccelerator:accelerator/listener/endpoint-group

AWS Glue

- glue:database
- glue:job
- glue:table
- glue:trigger

AWS Glue DataBrew

- databrew:dataset
- databrew:recipe
- databrew:ruleset

AWS Identity and Access Management

- iam:group
- iam:instance-profile
- iam:oidc-provider
- iam:policy
- iam:role
- iam:saml-provider
- iam:server-certificate
- iam:user
- iam:virtualmfadevice

Amazon Interactive Video Service

- ivs:channel
- ivs:streamkey

AWS IoT

- iot:authorizer
- iot:jobtemplate
- iot:mitigationaction
- iot:policy
- iot:provisioningtemplate
- iot:rolealias
- iot:securityprofile
- iot:thing
- iot:topicrule

AWS IoT Analytics

- iotanalytics:channel
- iotanalytics:dataset
- iotanalytics:datastore
- iotanalytics:pipeline

AWS IoT Events

- iotevents:alarmModel
- iotevents:detectorModel
- iotevents:input

AWS IoT Greengrass Version 1

- greengrass:components
- greengrass:groups

AWS IoT SiteWise

- iotsitewise:asset
- iotsitewise:assetmodel
- iotsitewise:gateway

AWS IoT TwinMaker

- iottwinmaker:workspace
- iottwinmaker:workspace/component-type
- iottwinmaker:workspace/entity

AWS Key Management Service

- kms:key

Amazon Kinesis

- kinesis:stream

Amazon Data Firehose

- kinesisfirehose:deliverystream

Flusso di video Amazon Kinesis

- kinesisvideo:stream

AWS Lambda

- `lambda:code-signing-config`
- `lambda:event-source-mapping`
- `lambda:function`

Amazon Lex

- `lex:bot`

Servizio di posizione Amazon

- `geo:place-index`
- `geo:tracker`

Amazon Lookout per le metriche

- `lookoutmetrics:Alert`

Amazon Lookout per Vision

- `lookoutvision:project`

Servizio gestito da Amazon per Apache Flink

- `kinesisanalytics:application`

Amazon Managed Service per Prometheus

- `aps:rulegroupsnamespace`
- `aps:workspace`

Amazon Managed Service per Prometheus

- memorydb:cluster
- memorydb:parametergroup
- memorydb:user

Amazon Managed Streaming per 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 Servizio Amazon

- es:domain

AWS Panorama

- panorama:package

Amazon Personalize

- personalize:dataset
- personalize:dataset-group
- personalize:schema

AWS Private Certificate Authority

- acmpca:certificateauthority

Amazon QLDB

- qldb:ledger
- qldb:stream

Amazon Redshift

- redshift:cluster
- redshift:eventsubscription
- redshift:parametergroup
- redshift:snapshot
- redshift:snapshotcopygrant
- redshift:snapshotschedule
- redshift:subnetgroup
- redshift:usagelimit

Amazon Rekognition

- rekognition:project

Amazon Relational Database Service (Amazon RDS)

- rds:auto-backup
- rds:cev
- rds:cluster
- rds:cluster-endpoint
- rds:cluster-pg
- rds:cluster-snapshot
- rds:db
- rds:db-proxy
- rds:db-proxy-endpoint
- rds:deployment
- rds:es
- rds:global-cluster
- rds:og
- rds:pg
- rds:ri
- rds:secgrp
- rds:snapshot
- rds:subgrp

AWS Resilience Hub

- resiliencehub:resiliencypolicy

AWS Resource Groups

- resourcegroups:group

Esploratore di risorse AWS

- resource-explorer-2:index

- resource-explorer-2:view

Amazon Route 53

- route53:healthcheck
- route53:hostedzone

Preparazione al ripristino di Amazon Route 53

- route53-recover-readiness:recovery-group
- route53-recover-readiness:resource-set

Amazon Route 53 Resolver

- route53resolver:firewalldomainlist
- route53resolver:firewallrulegroup
- route53resolver:resolverendpoint
- route53resolver:resolverrule

Amazon SageMaker

- sagemaker:model
- sagemaker:notebookinstance

AWS Secrets Manager

- secretsmanager:secret

AWS Service Catalog

- servicecatalog:applications
- servicecatalog:attribute-groups

Amazon Simple Notification Service

- sns:topic

Amazon Simple Queue Service

- sqs:queue

Amazon Simple Storage Service (Amazon S3)

- s3:accesspoint
- s3:bucket
- s3:storage-lens

AWS Step Functions

- states:statemachine
- stepfunctions:activity

AWS Systems Manager

- ssm:association
- ssm:automation-execution
- ssm:document
- ssm:maintenancewindow
- ssm:managed-instance
- ssm:parameter
- ssm:patchbaseline
- ssm:resourcedatasync
- ssm:windowtarget
- ssm:windowtask

Accesso verificato da AWS

- `ec2:verifiedaccessendpoint`
- `ec2:verifiedaccessgroup`
- `ec2:verifiedaccessinstance`
- `ec2:verifiedaccesstrustprovider`

AWS Wavelength

- `ec2:carriergateway`

Accesso programmatico all'elenco dei tipi di risorse supportati

Per accedere all'elenco dei tipi di risorse supportati dal codice, puoi richiamare l'ListSupportedResourceTypesoperazione da qualsiasi SDK. AWS

Ad esempio, è possibile eseguire il comando list-supported-resource-types AWS Command Line Interface (AWS CLI), come illustrato nell'esempio seguente.

```
$ 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 ...
```

Tipi di risorse che appaiono come altri tipi

Alcuni tipi di risorse sono identificati da stringhe Amazon resource name (ARN) che condividono un formato comune con un altro tipo di risorsa. Quando ciò accade, Resource Explorer può segnalare risorse come quell'altro tipo di risorsa. Ciò influisce sui tipi di risorse riportati nella tabella seguente.

Tipo di risorsa effettivo	Segnalato come tipo di risorsa
`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`

`docdb:eventsubscription` `neptune:eventsubscription`	`rds:es`

Tipo di risorsa effettivo	Segnalato come tipo di risorsa
`rds:eventsubscription`	
`docdb:globalcluster` `rds:globalcluster`	`rds:global-cluster`
`neptune:dbparametergroup` `rds:dbparametergroup`	`rds:pg`

`docdb:dbsubnetgroup`
`neptune:dbsubnetgroup`
`rds:dbsubnetgroup`
	`rds:subgrp`

Quote per Resource Explorer

Le tueAccount AWS quote sono predefinite per ognuna di esseServizio AWS. Salvo dove diversamente specificato, le quote si applicano a una regione specifica. Se per alcune quote è possibile richiedere aumenti, altre quote non possono essere modificate.

Per visualizzare le quote perEsploratore di risorse AWS, apri la Console Service Quotas. Nel riquadro di navigazione scegliere Servizi AWSe selezionare Resource Explorer.

Per richiedere un aumento delle quote, consultare Richiesta di aumento delle quote nella Guida per l'utente di Service Quotas. Se la quota non è ancora disponibile in Service Quotas, utilizza il modulo di incremento dei limiti.

Le quote seguenti sono le impostazioni predefinite per Resource Explorer.

Quote di valore massimo	Valore predefinito
Numero di visualizzazioni in unRegione AWS	10

Limiti tariffari per le operazioni	Valore predefinito
Numero massimo di operazioni di ricerca al secondo	5
Numero massimo di operazioni non di ricerca al secondo	3
Numero massimo di operazioni di ricerca nella regione aggregatrice per mese	10.000
Numero massimo di operazioni di ricerca nelle regioni locali al mese	500

Utilizzo Esploratore di risorse AWS con un SDK AWS

AWS I kit di sviluppo software (SDK) sono disponibili per molti linguaggi di programmazione più diffusi. Ogni SDK fornisce un'API, esempi di codice, e documentazione che facilitano agli sviluppatori la creazione di applicazioni nel loro linguaggio preferito.

Documentazione sugli SDK	Esempi di codice
AWS SDK for C++	AWS SDK for C++ esempi di codice
AWS CLI	AWS CLI esempi di codice
AWS SDK for Go	AWS SDK for Go esempi di codice
AWS SDK for Java	AWS SDK for Java esempi di codice
AWS SDK for JavaScript	AWS SDK for JavaScript esempi di codice
SDK AWS for Kotlin	SDK AWS for Kotlin esempi di codice
AWS SDK for .NET	AWS SDK for .NET esempi di codice
AWS SDK for PHP	AWS SDK for PHP esempi di codice
AWS Tools for PowerShell	Strumenti per esempi di PowerShell codice
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) esempi di codice
AWS SDK for Ruby	AWS SDK for Ruby esempi di codice
AWS SDK for Rust	AWS SDK for Rust esempi di codice
SDK AWS per SAP ABAP	SDK AWS per SAP ABAP esempi di codice
SDK AWS per Swift	SDK AWS per Swift esempi di codice

Esempio di disponibilità

Non riesci a trovare quello che ti serve? Richiedi un esempio di codice utilizzando il link Provide feedback (Fornisci un feedback) nella parte inferiore di questa pagina.

Cronologia dei documenti per la Resource Explorer User Guide

La tabella seguente descrive le versioni della documentazione per Esploratore di risorse AWS. Per ricevere notifiche sugli aggiornamenti di questa documentazione, puoi abbonarti a un feed RSS.

Modifica	Descrizione	Data
È stato aggiunto il supporto per nuovi tipi di risorse	Resource Explorer ha aggiunto il supporto per 65 nuove risorse AWS Key Management Service, Servizi AWS tra cui Amazon Route 53 e Amazon Fraud Detector.	20 febbraio 2024
Policy gestite e aggiornate	Resource Explorer ha aggiunto il supporto per visualizzare tipi di risorse aggiuntivi. La politica `AWSResourceExplorerServiceRolePolicy` AWS gestita è stata aggiornat a per concedere a Resource Explorer l'accesso per visualizzare tipi di risorse aggiuntivi.	12 dicembre 2023
È stato aggiunto un nuovo filtro di ricerca	Resource Explorer ora supporta la ricerca delle risorse per applicazione.	16 novembre 2023
È stato aggiunto il supporto per nuovi tipi di risorse	Resource Explorer ha aggiunto il supporto per 86 nuove risorse Servizi AWS tra cui AWS CloudForm	15 novembre 2023

	ation AWS Glue, e Amazon SageMaker.	
Resource Explorer supporta la ricerca su più account	Ora puoi usare Resource Explorer per cercare e scoprire risorse Account AWS all'interno della tua organizzazione o unità organizzativa. Per ulteriori informazioni, consulta Attivazione della ricerca su più account.	14 novembre 2023
Policy gestite nuove e aggiornate	Resource Explorer ha aggiunto il supporto per AWS Organizations. Le politiche AWS gestite sono state aggiunte e aggiornate per consentire a Resource Explorer l'accesso all'organizzazione, alla struttura organizzativa, agli account e agli amministratori delegati.	14 novembre 2023
È stato aggiunto il supporto per nuovi tipi di risorse	Resource Explorer ha aggiunto il supporto per AWS Organizations. Le politiche AWS gestite sono state aggiornate per concedere a Resource Explorer l'accesso all'organizzazione, alla struttura organizzativa, agli account e agli amministratori delegati.	14 novembre 2023

È stato aggiunto il supporto per nuovi tipi di risorse	Resource Explorer ora supporta 12 nuovi tipi di risorse provenienti da servizi tra cui Amazon Cognito e Amazon Elastic File System. AWS Elastic Beanstalk	18 ottobre 2023
È stato aggiunto il supporto per nuovi tipi di risorse	Resource Explorer ha aggiunto il supporto per 164 risorse. Le politiche AWS gestite che concedono a Resource Explorer l'accesso alle risorse dell'indice sono state aggiornate per includere questi nuovi tipi di risorse.	17 ottobre 2023
Resource Explorer è ora disponibile in alcune regioni opzionali	I clienti di BAH e CGK possono ora optare per Resource Explorer.	5 ottobre 2023
È stato aggiunto il supporto per nuovi tipi di risorse	Resource Explorer ha aggiunto il supporto per le risorse seguenti Servizi AWS: AWS CodeBuild AWS CodePipeline,, Amazon Cognito, Amazon Elastic Container Registry AWS Elastic Beanstalk, Amazon Elastic File System e. AWS IoT AWS Step Functions Le politiche AWS gestite che garantiscono a Resource Explorer l'accesso alle risorse dell'indice sono state aggiornate per includere questi nuovi tipi di risorse.	1° agosto 2023

Resource Explorer ora supporta l'esportazione dei risultati della ricerca in un file CSV	È ora possibile esportare i risultati della ricerca nella pagina di ricerca delle risorse in un file in formato CSV.	4 aprile 2023
Utilizzalo per cercare AWS Chatbot e scoprire le tue risorse AWS	Ora puoi usarle AWS Chatbot per cercare le tue risorse usando domande in linguaggio naturale. Per ulteriori informazioni, consulta Utilizzo AWS Chatbot per la ricerca di risorse.	30 marzo 2023
È stato aggiunto il supporto per nuovi tipi di risorse	Resource Explorer ha aggiunto il supporto per le seguenti risorse Servizi AWS: Amazon ElastiCache e Amazon Simple Queue Service (Amazon SQS). AWS Lambda Le politiche AWS gestite che garantiscono a Resource Explorer l'accesso alle risorse dell'indice sono state aggiornate per includere questi nuovi tipi di risorse.	7 marzo 2023
Aggiornamento delle best practice di IAM	Guida aggiornata per l'allinea mento alle best practice IAM. Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM.	6 dicembre 2022

Nuove politiche AWS gestite	Resource Explorer aggiunge AWSResourceExplorerFullAccess e AWSResourceExplorerServiceRolePolicy gestisce le politiche . AWSResourceExplorerReadOnlyAccess	7 novembre 2022
Versione iniziale	Versione iniziale della Guida per l'utente di Resource Explorer	7 novembre 2022

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.