User Guide

AWS Ressourcen Explorer

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Ressourcen Explorer: User Guide

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Ressourcen-Explorer ... 1
Erstmaliger Benutzer ... 2
Funktionen von Resource Explorer ... 2
Unterstützte Regionen ... 3
Zugehörige Services ... 6
Preisgestaltung ... 7
Erste Schritte ... 8
Zugreifen auf den Resource Explorer ... 8
Begriffe und Konzepte ... 10
Resource Explorer-Administrator ... 12
Resource Explorer-Benutzer ... 13
Index ... 14
Anzeigen ... 15
Ressource ... 17
Vereinheitlichte Suche in der AWS Management Console ... 18
Suche mit mehreren Konten ... 19
Voraussetzungen ... 19
Melden Sie sich an für ein AWS-Konto ... 19
Erstellen eines Benutzers mit Administratorzugriff ... 20
Resource Explorer einrichten ... 21
Quick Setup ... 22
Erweiterte Einstellungen ... 24
Identifizieren Sie den Resource Explorer-Status in AWS-Regionen ... 30
Überprüfen des Resource Explorer-Status in einer Region ... 30
Eine Region einschalten ... 32
Erstellen Sie einen Resource Explorer-Index in einer Region ... 33
Über Opt-in-Regionen ... 36
Verhalten beim Abmelden ... 36
Aktivierung der regionsübergreifenden Suche ... 37
Über den Aggregator-Index ... 37
Aggregatorindex erstellen ... 39
Herabstufung des Aggregatorindex ... 41
Die Suche mit mehreren Konten aktivieren ... 44
Voraussetzungen ... 44

Aktivieren Sie die Suche mit mehreren Konten ... 45
Schnelle Einrichtung für mehrere Konten ... 45
Auswirkung von Kontoaktionen auf die Suche mit mehreren Konten ... 46
Resource Explorer ist deaktiviert ... 46
Das Mitgliedskonto wurde aus einer Organisation entfernt ... 46
Das Konto ist gesperrt ... 47
Das Konto ist geschlossen ... 47
Abmeldung vom Konto ... 48
Unterstützung der einheitlichen Suche auf der Konsole ... 49
Bereitstellung in einer Organisation ... 50
Voraussetzungen ... 50
Die Stack-Sets für Resource Explorer erstellen ... 51
Beispielvorlagen AWS CloudFormation ... 52
Resource Explorer ausschalten ... 56
Resource Explorer in einem Fall ausschalten AWS-Region ... 56
Alles ausschalten AWS-Regionen ... 58
Ansichten verwalten ... 62
Standardansichten ... 64
Erstellen von Ansichten ... 65
Zugriff zu Ansichten ... 70
Mit Tag-basierter Autorisierung ... 71
Eine Standardansicht einrichten ... 73
Ansichten taggen ... 74
Hinzufügen von Markern zu Ihren Ansichten hinzu ... 75
Steuern von Berechtigungen mit Tags ... 76
Verweisen auf Stichwörter in einer ABAC-Richtlinie ... 76
Ansichten teilen ... 77
Richtlinie für Berechtigungen, mit denen die Ansicht geteilt werden soll AWS-Konten ... 79
Ansichten löschen ... 80
Auf der Suche nach Ressourcen ... 82
Exportieren Sie Suchergebnisse in eine CSV-Datei ... 85
Unterstützte Ressourcentypen ... 87
Unterstützte Dienste und Ressourcentypen ... 88
APIAmazon-Gateway ... 91
AWS App Runner ... 91
Amazon AppStream 2.0 ... 91

AWS AppSync ... 91
Amazon Athena ... 92
AWS Backup ... 92
AWS Batch ... 92
AWS CloudFormation ... 92
Amazon CloudFront ... 92
AWS CloudTrail ... 93
Amazon CloudWatch ... 93
Amazon CloudWatch offenbar ... 93
CloudWatch Amazon-Protokolle ... 93
AWS CodeArtifact ... 93
AWS CodeBuild ... 93
AWS CodeCommit ... 94
Amazon CodeGuru Profiler ... 94
AWS CodePipeline ... 94
AWS CodeConnections ... 94
Amazon Cognito ... 94
Amazon Connect ... 94
Amazon Connect Wisdom ... 94
Amazon Detective ... 95
Amazon-DynamoDB ... 95
EC2Image Builder ... 95
Amazon ECR Public ... 95
AWS Elastic Beanstalk ... 95
Amazon ElastiCache ... 95
Amazon Elastic Compute Cloud (AmazonEC2) ... 96
Amazon Elastic Container Registry ... 98
Amazon Elastic Container Service ... 98
Amazon Elastic File System ... 98
Elastic Load Balancing ... 98
AWS Elemental MediaPackage ... 99
AWS Elemental MediaTailor ... 99
Amazon EMR Serverlos ... 99
Amazon EventBridge ... 99
AWS Fault Injection Service ... 99
Amazon Forecast ... 99

Amazon Fraud Detector 100
Amazon GameLift 100
AWS Global Accelerator 100
AWS Glue 100
AWS Glue DataBrew 100
AWS Identity and Access Management 101
Amazon Interactive Video Service 101
AWS IoT 101
AWS IoT Analytics 102
AWS IoT Events 102
AWS IoT Greengrass Version 1 102
AWS IoT SiteWise 102
AWS IoT TwinMaker 102
AWS Key Management Service 102
Amazon Kinesis 103
Amazon Data Firehose 103
Amazon Kinesis Video Streams 103
AWS Lambda 103
Amazon Lex 103
Amazon Location Service 103
Amazon Lookout für Metrics 103
Amazon Lookout für Vision 104
Amazon Managed Service für Apache Flink 104
Amazon Managed Service für Prometheus 104
Amazon Managed Service für Prometheus 104
Amazon Managed Streaming für Apache Kafka 104
AWS Migration Hub Refactor Spaces 104
AWS Network Firewall 105
AWS Network Manager 105
OpenSearch Amazon-Dienst 105
AWS Panorama 105
Amazon Personalize 105
AWS Private Certificate Authority 105
Amazon QLDB 105
Amazon-Redshift 106
Amazon Rekognition 106

Amazon Relational Database Service (AmazonRDS) ... 106
AWS Resilience Hub ... 107
AWS Resource Groups ... 107
AWS Ressourcen Explorer ... 107
Amazon Route 53 ... 107
Amazon Route 53 Recovery-Bereitschaft ... 107
Amazon Route 53 Resolver ... 107
Amazon SageMaker ... 108
AWS Secrets Manager ... 108
AWS Service Catalog ... 108
Amazon Simple Notification Service ... 108
Amazon Simple Queue Service ... 108
Amazon-Simple-Storage-Service (Amazon-S3) ... 108
AWS Step Functions ... 108
AWS Systems Manager ... 109
AWS Verified Access ... 109
AWS Wavelength ... 109
Programmgesteuerter Zugriff auf die Liste der unterstützten Ressourcentypen ... 109
Ressourcentypen, die als andere Typen erscheinen ... 110
Syntax der Suchabfrage ... 112
So funktionieren Abfragen im Resource Explorer ... 112
Syntax der Abfragezeichenfolge ... 112
Grundlagen ... 113
Filter ... 113
Operatoren filtern ... 118
Beispielabfragen ... 122
Ressourcen ohne Tags ... 122
Markieren von Ressourcen ... 123
Übersicht fehlender Tags ... 123
Ungültige Tags ... 123
Teilmenge von Regionen ... 124
Globale Ressourcen ... 124
Mehrere Filter ... 125
Verwendung von Anführungszeichen für Begriffe mit mehreren Wörtern ... 125
AWS CloudFormationMitglieder stapeln ... 126
Unified search ... 127

Es wird überprüft, ob die einheitliche Suche aktiviert ist ... 128
Unified Search aktivieren ... 128
Arbeiten mit CloudFormation ... 129
Resource Explorer und CloudFormation Vorlagen ... 129
Weitere Informationen zu AWS CloudFormation ... 132
Verwenden von Amazon Q Entwickler für Chat-Anwendungen ... 133
AWS -Ressourcenfragen ... 133
Voraussetzungen ... 133
Häufig gestellte Ressourcenfragen ... 134
Sicherheit ... 135
IAMRichtlinien aktualisieren auf IPv6 ... 136
Kunden, die vom Upgrade von IPv4 auf betroffen sind IPv6 ... 136
Was istIPv6? ... 136
Aktualisierung einer Richtlinie für IAM IPv6 ... 137
Stellen Sie sicher, dass Ihr Kunde Folgendes unterstützt IPv6 ... 138
Identity and Access Management ... 140
Zielgruppe ... 140
Authentifizierung mit Identitäten ... 141
Verwalten des Zugriffs mit Richtlinien ... 144
Resource Explorer und IAM ... 147
Beispiele für identitätsbasierte Richtlinien ... 155
Beispiel-SCPs ... 161
AWS verwaltete Richtlinien ... 162
Verwenden von serviceverknüpften Rollen ... 181
Problembehandlung bei Berechtigungen ... 183
Datenschutz ... 185
Verschlüsselung im Ruhezustand ... 186
Verschlüsselung während der Übertragung ... 186
Compliance-Validierung ... 186
Ausfallsicherheit ... 187
Sicherheit der Infrastruktur ... 188
Überwachung ... 189
CloudTrail protokolle ... 189
Informationen zum Resource Explorer in CloudTrail ... 190
Grundlagen zu -Protokolldateieinträgen ... 191
Fehlerbehebung ... 201

Allgemeine Probleme 201
In einem Link zum Resource Explorer fehlt derAWS-Region 201
Vereinheitlichte CloudTrail Suchfehler 202
Probleme bei der 203
Ich erhalte eine Meldung, dass der Zugriff verweigert wird, wenn ich eine Anfrage an den Resource Explorer stelle 204
Ich erhalte eine Meldung, dass der Zugriff verweigert wird, wenn ich eine Anfrage mit temporären Sicherheitsanmeldeinformationen erstelle 205
Probleme mit der Suche 205
Warum fehlen einige Ressourcen in meinen Resource Explorer-Suchergebnissen? 206
Warum werden meine Ressourcen nicht in den vereinheitlichten Suchergebnissen in der Konsole angezeigt? 208
Warum führt die einheitliche Suche in der Konsole und im Resource Explorer manchmal zu unterschiedlichen Ergebnissen? 208
Welche Berechtigungen benötige ich, um nach Ressourcen suchen zu können? 209
Kontingente 211
Arbeitet mit AWS SDKs 212
Dokumentverlauf 214
..... ccxx

Was ist AWS Ressourcen Explorer?

AWS Ressourcen Explorer ist ein Dienst zum Suchen und Entdecken von Ressourcen. Mit Resource Explorer können Sie Ihre Ressourcen wie Amazon Elastic Compute Cloud-Instances, Amazon Kinesis Kinesis-Streams oder Amazon DynamoDB-Tabellen mithilfe einer Internet-Suchmaschine erkunden. Sie können mithilfe von Ressourcenmetadaten wie Namen, Tags und nach Ihren Ressourcen suchen. IDs Resource Explorer funktioniert AWS-Regionen in Ihrem Konto, um Ihre regionsübergreifenden Workloads zu vereinfachen.

Resource Explorer bietet schnelle Antworten auf Ihre Suchanfragen mithilfe von Indizes, die vom Dienst erstellt und verwaltet werden. AWS Ressourcen Explorer Resource Explorer verwendet eine Vielzahl von Datenquellen, um Informationen zu Ressourcen in Ihrem AWS-Konto zu sammeln. Resource Explorer speichert diese Informationen in den Indizes, damit Resource Explorer sie durchsuchen kann.

> **Wir möchten Ihr Feedback zu dieser Dokumentation**
>
> Unser Ziel ist es, Ihnen zu helfen, alles aus Resource Explorer herauszuholen, was Sie können. Wenn Ihnen dieser Leitfaden dabei hilft, lassen Sie es uns wissen. Wenn der Leitfaden Ihnen nicht hilft, möchten wir von Ihnen hören, damit wir das Problem lösen können. Verwenden Sie den Feedback-Link, der sich in der oberen rechten Ecke jeder Seite befindet. Dadurch werden Ihre Kommentare direkt an die Autoren dieses Handbuchs gesendet.
> Wir überprüfen jede Einreichung und suchen nach Möglichkeiten, die Dokumentation zu verbessern. Vielen Dank im Voraus für Ihre Hilfe!

Themen

- Verwenden Sie Resource Explorer zum ersten Mal?
- Funktionen von Resource Explorer
- Von Resource Explorer unterstützte Regionen
- Verwandt AWS-Services
- Preisgestaltung

Verwenden Sie Resource Explorer zum ersten Mal?

Wenn Sie Resource Explorer zum ersten Mal verwenden, empfehlen wir Ihnen, zunächst die folgenden Themen im Abschnitt Erste Schritte zu lesen:

- Begriffe und Konzepte für Resource Explorer
- Resource Explorer mithilfe von Quick Setup einrichten

Funktionen von Resource Explorer

Resource Explorer bietet die folgenden Funktionen:

- Benutzer können in ihren Regionen AWS-Region oder in ihren Regionen nach Ressourcen suchen AWS-Konto.
- Benutzer können Stichwörter, Suchoperatoren und Attribute wie Tags verwenden, um die Suchergebnisse so zu filtern, dass nur passende Ressourcen angezeigt werden.
- Wenn Benutzer eine Ressource in den Suchergebnissen finden, können sie sofort zur systemeigenen Konsole der Ressource wechseln, um mit dieser Ressource zu arbeiten.
- Administratoren können Ansichten erstellen, die definieren, welche Ressourcen in den Suchergebnissen verfügbar sind. Administratoren können je nach ihren Aufgaben unterschiedliche Ansichten für verschiedene Benutzergruppen erstellen und nur Benutzern Berechtigungen für Ansichten gewähren, die sie benötigen.
- Resource Explorer ist, wie viele andere auch AWS-Services, letztendlich konsistent. Resource Explorer erreicht eine hohe Verfügbarkeit, indem Daten auf mehreren Servern in Amazon-Rechenzentren auf der ganzen Welt repliziert werden. Wenn eine Anforderung zur Änderung von Daten erfolgreich ist, wird die Änderung übernommen und sicher gespeichert. Dann muss die Änderung jedoch in Resource Explorer repliziert werden, was einige Zeit dauern kann. Dazu gehört beispielsweise, dass Resource Explorer eine Ressource in einer Region findet und diese in die Region repliziert, die den Aggregatorindex für das Konto enthält.

Von Resource Explorer unterstützte Regionen

Name der Region	Region	Endpunkt	Protocol (Protokoll)	
USA Ost (Ohio)	us-east-2	resource-explorer-2.us-east-2.amazonaws.com resource-explorer-2-fips.us-east-2.amazonaws.com resource-explorer-2-fips.us-east-2.api.aws	HTTPS HTTPS HTTPS	
USA Ost (Nord-Virginia)	us-east-1	resource-explorer-2.us-east-1.amazonaws.com resource-explorer-2-fips.us-east-1.amazonaws.com resource-explorer-2-fips.us-east-1.api.aws	HTTPS HTTPS HTTPS	
USA West (Nordkalifornien)	us-west-1	resource-explorer-2.us-west-1.amazonaws.com resource-explorer-2-fips.us-west-1.amazonaws.com resource-explorer-2-fips.us-west-1.api.aws	HTTPS HTTPS HTTPS	
USA West (Oregon)	us-west-2	resource-explorer-2.us-west-2.amazonaws.com resource-explorer-2-fips.us-west-2.amazonaws.com resource-explorer-2-fips.us-west-2.api.aws	HTTPS HTTPS HTTPS	
Afrika (Kapstadt)	af-south-1	resource-explorer-2.af-south-1.amazonaws.com	HTTPS	
Asien-Pazifik	ap-east-1	resource-explorer-2.ap-east-1.amazonaws.com	HTTPS	

Name der Region	Region	Endpunkt	Protocol (Protokoll)
(Hongkong)			
Asien-Pazifik (Hyderabad)	ap-south-2	resource-explorer-2.ap-south-2.amazonaws.com	HTTPS
Asien-Pazifik (Jakarta)	ap-southeast-3	resource-explorer-2.ap-southeast-3.amazonaws.com	HTTPS
Asien-Pazifik (Melbourne)	ap-southeast-4	resource-explorer-2.ap-southeast-4.amazonaws.com	HTTPS
Asien-Pazifik (Mumbai)	ap-south-1	resource-explorer-2.ap-south-1.amazonaws.com	HTTPS
Asien-Pazifik (Osaka)	ap-northeast-3	resource-explorer-2.ap-northeast-3.amazonaws.com	HTTPS
Asien-Pazifik (Seoul)	ap-northeast-2	resource-explorer-2.ap-northeast-2.amazonaws.com	HTTPS
Asien-Pazifik (Singapur)	ap-southeast-1	resource-explorer-2.ap-southeast-1.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Asien-Pazifik (Sydney)	ap-southeast-2	resource-explorer-2.ap-southeast-2.amazonaws.com	HTTPS
Asien-Pazifik (Tokio)	ap-northeast-1	resource-explorer-2.ap-northeast-1.amazonaws.com	HTTPS
Kanada (Zentral)	ca-central-1	resource-explorer-2.ca-central-1.amazonaws.com resource-explorer-2-fips.ca-central-1.amazonaws.com resource-explorer-2-fips.ca-central-1.api.aws	HTTPS HTTPS HTTPS
Kanada West (Calgary)	ca-west-1	resource-explorer-2.ca-west-1.amazonaws.com resource-explorer-2-fips.ca-west-1.amazonaws.com resource-explorer-2-fips.ca-west-1.api.aws	HTTPS HTTPS HTTPS
Europa (Frankfurt)	eu-central-1	resource-explorer-2.eu-central-1.amazonaws.com	HTTPS
Europa (Irland)	eu-west-1	resource-explorer-2.eu-west-1.amazonaws.com	HTTPS
Europa (London)	eu-west-2	resource-explorer-2.eu-west-2.amazonaws.com	HTTPS
Europa (Mailand)	eu-south-1	resource-explorer-2.eu-south-1.amazonaws.com	HTTPS

Name der Region	Region	Endpunkt	Protocol (Protokoll)
Europa (Paris)	eu-west-3	resource-explorer-2.eu-west-3.amazonaws.com	HTTPS
Europa (Spanien)	eu-south-2	resource-explorer-2.eu-south-2.amazonaws.com	HTTPS
Europa (Stockholm)	eu-north-1	resource-explorer-2.eu-north-1.amazonaws.com	HTTPS
Europa (Zürich)	eu-central-2	resource-explorer-2.eu-central-2.amazonaws.com	HTTPS
Israel (Tel Aviv)	il-central-1	resource-explorer-2.il-central-1.amazonaws.com	HTTPS
Naher Osten (Bahrain)	me-south-1	resource-explorer-2.me-south-1.amazonaws.com	HTTPS
Naher Osten (UAE)	me-central-1	resource-explorer-2.me-central-1.amazonaws.com	HTTPS
Südamerika (São Paulo)	sa-east-1	resource-explorer-2.sa-east-1.amazonaws.com	HTTPS

Verwandt AWS-Services

Im Folgenden sind die anderen aufgeführt AWS-Services , deren Hauptzweck darin besteht, Sie bei der Verwaltung Ihrer AWS Ressourcen zu unterstützen:

AWS Resource Access Manager (AWS RAM)

Teilen Sie die Ressourcen in einem AWS-Konto System mit anderen AWS-Konten. Wenn Ihr Konto von verwaltet wird AWS Organizations, können Sie AWS RAM damit Ressourcen für die Konten in einer Organisationseinheit oder für alle Konten in der Organisation gemeinsam nutzen. Die gemeinsam genutzten Ressourcen funktionieren für Benutzer in diesen Konten genauso, als ob sie im lokalen Konto erstellt würden.

AWS Resource Groups

Erstellen Sie Gruppen für Ihre AWS Ressourcen. Anschließend können Sie jede Gruppe als Einheit verwenden und verwalten, anstatt jede Ressource einzeln referenzieren zu müssen. Ihre Gruppen können aus Ressourcen bestehen, die Teil desselben AWS CloudFormation Stacks sind oder mit denselben Tags gekennzeichnet sind. Einige Ressourcentypen unterstützen auch die Anwendung einer Konfiguration auf eine Ressourcengruppe, die sich auf alle relevanten Ressourcen in dieser Gruppe auswirkt.

Der Tag-Editor und der AWS Resource Groups Tagging API

Tags sind vom Kunden definierte Metadaten, die Sie an Ihre Ressourcen anhängen können. Sie können Ihre Ressourcen für Zwecke wie Kostenzuweisung und attributbasierte Zugriffskontrolle kategorisieren.

Preisgestaltung

Für die Suche nach Ressourcen mithilfe von Ressourcen fallen keine Gebühren an AWS Ressourcen Explorer, einschließlich der Erstellung von Ansichten, der Aktivierung von Regionen oder der Suche nach Ressourcen. Bei der Erstellung Ihres Ressourceninventars ruft Resource Explorer in Ihrem Namen APIs auf, was zu Gebühren führen kann. Wenn Sie mit den Ressourcen interagieren, die Sie in Ihren Suchergebnissen finden, können Nutzungsgebühren anfallen, die je nach Ressourcentyp und deren Art variieren AWS-Service. Weitere Informationen darüber, wie die normale Nutzung eines bestimmten Ressourcentyps in AWS Rechnung gestellt wird, finden Sie in der Dokumentation des jeweiligen Ressourcentyps.

Erste Schritte mit Resource Explorer

Verwenden Sie die Themen in diesem Abschnitt, um sich ein grundlegendes Verständnis der Konzepte und Begriffe zu verschaffen, die von verwendet werden AWS Ressourcen Explorer. Erfahren Sie mehr über die Voraussetzungen, die Sie erfüllen müssen, um Resource Explorer erfolgreich zu verwenden, und wie Sie Resource Explorer in Ihrem aktivieren AWS-Konto.

Zugreifen auf den Resource Explorer

Sie können auf folgende Weise mit Resource Explorer interagieren:

Resource Explorer-Konsole

Resource Explorer bietet eine webbasierte Benutzeroberfläche, die Resource Explorer-Konsole. Wenn Sie sich für eine registriert haben AWS-Konto, können Sie auf die Resource Explorer-Konsole zugreifen, indem Sie sich bei der Resource Explorer-Konsole anmelden AWS Management Consoleund auf der Startseite der Konsole Resource Explorer auswählen.

Sie können in Ihrem Browser auch direkt zur Resource Explorer-Dashboardseite oder zur Ressourcensuchseite navigieren. Wenn Sie noch nicht angemeldet sind, werden Sie aufgefordert, dies zu tun, bevor die Konsole angezeigt wird.

> **Note**
>
> Die Resource Explorer-Konsole ist eine globale Konsole, was bedeutet, dass Sie keine auswählen müssen, in der Sie arbeiten AWS-Region möchten. Wenn Sie jedoch Resource Explorer verwenden, um einen Index oder eine Ansicht zu erstellen, müssen Sie angeben, in welcher Region der Index oder die Ansicht gespeichert ist. Wenn Sie den Ressourcen-Explorer für die Suche verwenden, können Sie eine beliebige Ansicht auswählen, auf die Sie Zugriff haben. Die Ergebnisse stammen automatisch aus der Region, die der ausgewählten Ansicht zugeordnet ist. Wenn die Ansicht aus der Region stammt, die den Aggregatorindex enthält, enthalten die Ergebnisse Ressourcen aus allen Regionen, in denen Sie Resource Explorer-Indizes erstellt haben.

AWS Management Console vereinheitlichte Suche

Oben auf jeder Seite in der befindet AWS Management Console sich eine Suchleiste. Sie können Resource Explorer so konfigurieren, dass er an der einheitlichen Suche teilnimmt. Anschließend können Ihre Benutzer die Resource Explorer-Suchanfragesyntax im einheitlichen Suchtextfeld verwenden und in diesen Suchergebnissen passende Ressourcen sehen. Wenn Sie diese Funktion aktivieren, können Benutzer von jeder beliebigen Konsole aus nach Ressourcen suchen, AWS-Service ohne zuerst zur Resource Explorer-Konsole wechseln zu müssen.

> **Important**
>
> Bei der einheitlichen Suche wird immer die Standardansicht in der Ansicht verwendet AWS-Region , die den Aggregatorindex enthält.

Resource Explorer-Befehle in den AWS CLI und Tools für Windows PowerShell

Die Tools AWS CLI und Tools für PowerShell bieten direkten Zugriff auf die öffentlichen API Vorgänge im Resource Explorer. Diese Tools funktionieren unter Windows, MacOS und Linux. Weitere Informationen zu den ersten Schritten finden Sie im AWS Command Line Interface Benutzerhandbuch oder im AWS Tools for Windows PowerShell Benutzerhandbuch. Weitere Informationen zu den Befehlen für Resource Explorer finden Sie in der AWS CLI Befehlsreferenz oder der AWS Tools for Windows PowerShell Cmdlet-Referenz.

Resource Explorer-Operationen im AWS SDKs

AWS stellt API Befehle für eine Vielzahl von Programmiersprachen bereit. Weitere Informationen zu den ersten Schritten finden Sie unter Verwenden AWS Ressourcen Explorer mit einem AWS SDK.

Abfrage API

Wenn Sie keine der unterstützten Programmiersprachen verwenden, API erhalten Sie mit der Resource HTTPS Explorer-Abfrage programmgesteuerten Zugriff auf Resource Explorer. Mit dem Resource Explorer API können Sie HTTPS Anfragen direkt an den Service richten. Wenn Sie den Resource Explorer verwendenAPI, müssen Sie Code angeben, mit dem Sie Ihre Anfragen mit Ihren AWS Anmeldeinformationen digital signieren können. Weitere Informationen finden Sie in der AWS Ressourcen Explorer APIReferenz.

Begriffe und Konzepte für Resource Explorer

AWS Ressourcen Explorer ist ein Dienst zur Suche und Entdeckung von Ressourcen. Mit Resource Explorer können Sie Ihre Ressourcen mithilfe einer Internet-Suchmaschine erkunden. Sie können nach Ihren Ressourcen wie Amazon Elastic Compute Cloud-Instances, Amazon Kinesis Kinesis-Streams oder Amazon DynamoDB-Tabellen suchen, indem Sie Ressourcenmetadaten wie Namen, Tags und IDs verwenden. Resource Explorer funktioniert AWS-Regionen in Ihrem Konto, um Ihre regionsübergreifenden Workloads zu vereinfachen.

Resource Explorer bietet schnelle Antworten auf Ihre Suchanfragen mithilfe von Indizes, die vom Dienst erstellt und verwaltet werden. AWS Ressourcen Explorer Resource Explorer verwendet eine Vielzahl von Datenquellen, um Informationen zu Ressourcen in Ihrem AWS-Konto zu sammeln. Resource Explorer speichert diese Informationen in den Indizes, damit Resource Explorer sie durchsuchen kann.

Sie sollten die folgenden Konzepte verstehen, um die Verwaltung und Konfiguration AWS Ressourcen Explorer für Ihre Benutzer erfolgreich durchführen zu können.

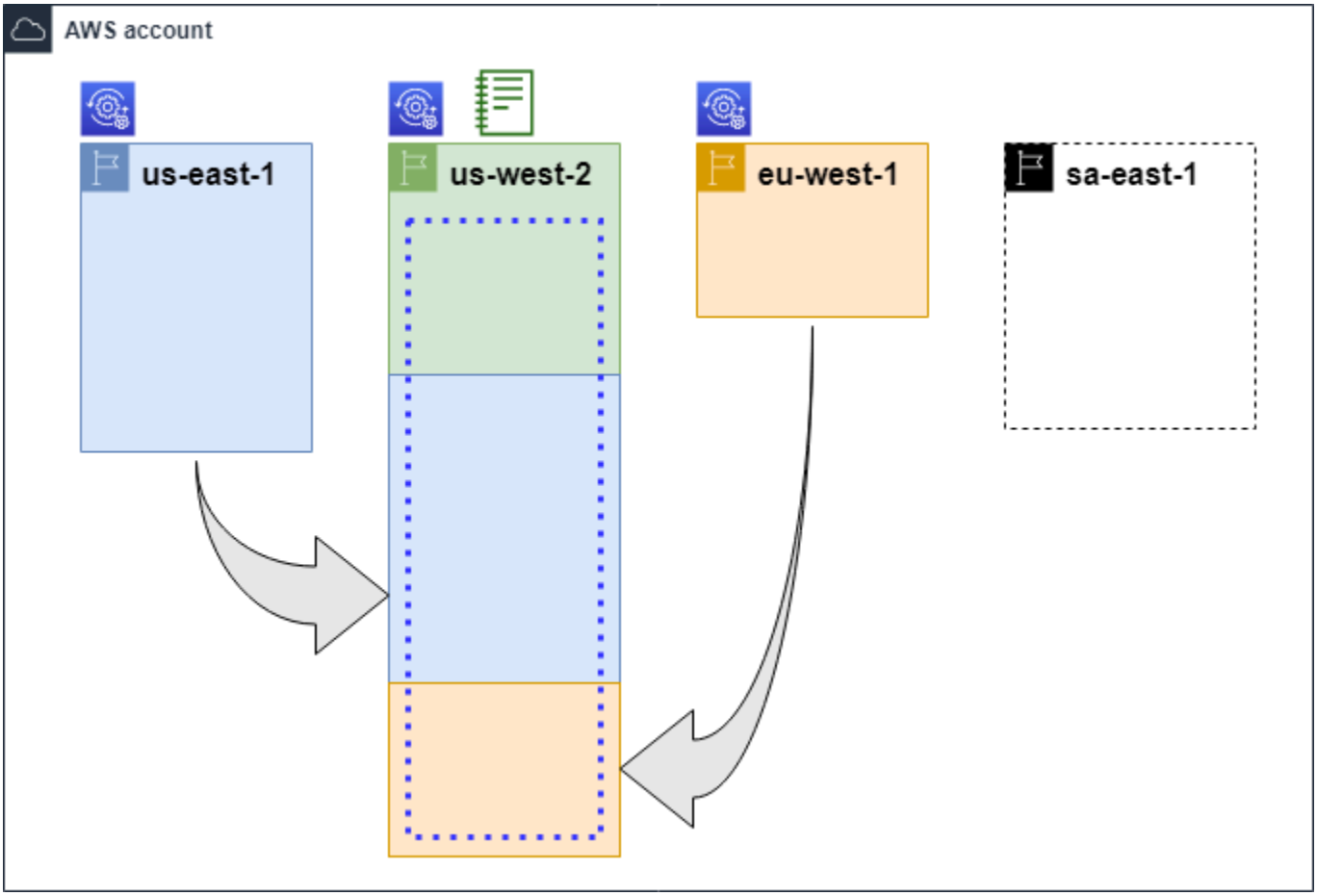
Konzepte

- Resource Explorer-Administrator
- Resource Explorer-Benutzer
- Index
- Anzeigen
- Ressource
- Vereinheitlichte Suche in der AWS Management Console
- Suche mit mehreren Konten

Das folgende Diagramm zeigt drei, AWS-Regionen in denen der Administrator Resource Explorer aktiviert hat, und eine Region, die der Administrator nicht aktiviert hat. Die Region, in der der Resource Explorer nicht aktiviert ist, hat keinen Index. Daher können ihre Ressourcen nicht mit Resource Explorer-Abfragen durchsucht werden.

In diesem Beispielszenario hat der Administrator die Region USA West (Oregon) (`us-west-2`) ausgewählt, um den Aggregatorindex für das Konto zu enthalten. Alle Regionen, die Sie aktivieren, replizieren ihre lokalen Indizes in die Region mit dem Aggregatorindex.

Die von Resource Explorer erstellte Standardansicht hat keine Filter. Daher können die Ergebnisse einer Suche mit dieser Ansicht Ressourcen jeden Typs in allen Regionen des Kontos enthalten, in dem der Ressourcen-Explorer aktiviert ist.



Legende	
	Der Resource Explorer ist in dieser Region aktiviert AWS-Region und Informationen über die Ressourcen der Region werden in einem lokalen Index in dieser Region gespeiche rt. Der lokale Index jeder Region wird ebenfalls in die Region repliziert (durch die Pfeile gekennzeichnet), die den Aggregatorindex enthält.
	Der Index darin AWS-Region ist so konfiguriert, dass er der Aggregatorindex für das Konto ist. Resource Explorer repliziert die in den lokalen Indizes aller anderen Regionen, in denen Resource Explorer aktiviert ist, gesammelten Ressourceninformationen in den Aggregatorindex in dieser Region. In dieser Region durchgeführte Suchanfragen können Ergebnisse aus allen Regionen des Kontos enthalten.

Die von Quick Setup erstellte Standardansicht umfasst alle RessourcenAWS-Regionen.

Resource Explorer-Administrator

Ein Resource Explorer-Administrator ist ein AWS Identity and Access Management (IAM-) Principal, der berechtigt ist, Resource Explorer und seine Einstellungen in der AWS-Konto Organisation sein. Der Resource Explorer-Administrator kann die folgenden Funktionen konfigurieren:

- Aktivieren Sie den Resource Explorer für einzelne Personen AWS-Regionen in den, AWS-Konto indem Sie Indizes in diesen Regionen erstellen. Auf diese Weise kann Resource Explorer Ressourcen ermitteln und den Index mit Informationen zu diesen Ressourcen füllen, sodass Benutzer nach Ressourcen in dieser Region suchen können.
- Aktualisieren Sie den Indextyp in einemAWS-Region, um ihn zum Aggregatorindex für seine zu machen. AWS-Konto Der Aggregatorindex in dieser Region empfängt replizierte Kopien der Ressourceninformationen aus allen anderen Regionen des Kontos, in dem Resource Explorer aktiviert ist.
- Erstellen Sie Ansichten, die die Teilmenge der indizierten Informationen definieren, die Benutzer im Resource Explorer suchen und entdecken können.
- Der Resource Explorer-Administrator ist zwar nicht Teil der Resource Explorer-Aktionen, muss aber auch in der Lage sein, den Prinzipalen im Konto Suchberechtigungen zu gewähren. Der Administrator kann Prinzipalen diese Berechtigungen gewähren, indem er die entsprechenden Berechtigungen zu vorhandenen IAM-Berechtigungsrichtlinien hinzufügt oder indem er die verwaltete Richtlinie „Nur AWS Lesen“ von Resource Explorer verwendet.

  Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

  - Benutzer und Gruppen in AWS IAM Identity Center:

    Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center-Benutzerhandbuch.
  - Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

    Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch.
  - IAM-Benutzer:

- Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer im IAM-Benutzerhandbuch.
- (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Der Administrator verfügt in der Regel über alle Resource Explorer-Berechtigungen (`resource-explorer-2:*`) für alle Resource Explorer-Ressourcen, einschließlich der Indizes und Ansichten. Diese Berechtigungen können mithilfe der AWSverwalteten Resource Explorer-Richtlinie für vollen Zugriff erteilt werden.

Resource Explorer-Benutzer

Ein Resource Explorer-Benutzer ist ein IAM-Prinzipal, der berechtigt ist, eine oder mehrere der folgenden Aufgaben auszuführen:

- Führen Sie eine Suche nach Ressourcen durch, indem Sie eine Ansicht verwenden, um den Resource Explorer abzufragen. Ein Resource Explorer-Benutzer möchte AWS Ressourcen suchen und finden und verwendet dafür in der Regel die Resource Explorer-Konsole oder die Resource `Search` Explorer-Operationen, die von den AWS SDKs oder dem AWS CLI bereitgestellt werden.

  Eine Rolle oder ein Benutzer kann mithilfe von IAM die Zugriffsberechtigung für die Suche mit einer von zwei Methoden abrufen:

  - Der Resource Explorer AWS hat nur Lesezugriff auf die verwaltete Richtlinie für die IAM-Rolle, die Gruppe oder den Benutzer.
  - Eine IAM-Berechtigungsrichtlinie mit einer Erklärung, die die folgenden Mindestberechtigungen für die IAM-Rolle, -Gruppe oder den Benutzer enthält.

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

- Obwohl dies in der Regel als Administratoraufgabe betrachtet wird, können Sie die Fähigkeit, Ansichten zu definieren, an vertrauenswürdige Benutzer delegieren. Zu diesem Zweck kann

der Administrator in einer IAM-Berechtigungsrichtlinie, die den entsprechenden Rollen, Gruppen oder Benutzern zugewiesen ist, die Erlaubnis zum Aufrufen des `resource-explorer-2:CreateView` Vorgangs erteilen. Wenn für die Ansicht bestimmte Berechtigungen erforderlich sind, müssen Vorkehrungen für das Hinzufügen oder Ändern der IAM-Richtlinien für die entsprechenden Benutzer getroffen werden.

Informationen zur Suche nach Ressourcen mithilfe des Resource Explorers finden Sie unterVerwendenAWS Ressourcen Explorerum nach Ressourcen zu suchen.

Index

Ein Index ist die vom Resource Explorer verwaltete Sammlung von Informationen über alle AWS Ressourcen AWS-Region in einer Ihrer RessourcenAWS-Konto. Resource Explorer verwaltet in jeder Region, in der Sie den Ressourcen-Explorer aktivieren, einen Index. Resource Explorer aktualisiert den Index automatisch, wenn Sie Ressourcen in Ihrem erstellen und löschenAWS-Konto. Im vorherigen Diagramm stellen die Felder unter den AWS-Region Namen die Resource Explorer-Indizes dar, die in den einzelnen AWS-Region Indizes verwaltet werden. Der Index in einer Region ist die Informationsquelle für alle Ansichten, die in dieser Region erstellt wurden. Benutzer können den Index nicht direkt abfragen. Stattdessen müssen sie immer eine Ansicht verwenden.

Es gibt zwei Arten von Indizes:

Lokaler Index

In jedem AWS-RegionIndex, in dem Sie den Resource Explorer aktivieren, gibt es einen lokalen Index. Ein lokaler Index enthält nur Informationen zu den Ressourcen in derselben Region.

Aggregator-Index

Der Resource Explorer-Administrator kann den Index in einem AWS-Region auch als Aggregatorindex für festlegen. AWS-Konto Der Aggregatorindex empfängt und speichert eine Kopie des Indexes für jede andere Region, in der Resource Explorer im Konto aktiviert ist. Der Aggregatorindex empfängt und speichert auch Informationen über die Ressourcen in seiner eigenen Region. Im vorherigen Diagramm `us-west-2` enthält die Region den Aggregatorindex für das Konto. Der Hauptgrund für die Festlegung eines Aggregatorindex für das Konto besteht darin, dass Sie Ansichten erstellen können, die Ressourcen aus allen Regionen des Kontos enthalten können. In einem kann es nur einen Aggregatorindex geben. AWS-Konto

Wenn Sie den Resource Explorer einschalten, können Sie angeben, AWS-Region welcher den Aggregatorindex enthalten soll. Sie können den für den Aggregator AWS-Region

verwendeten Index auch später ändern. Hinweise dazu, wie Sie einen lokalen Index heraufstufen, sodass er zum Aggregatorindex für ihn wirdAWS-Konto, finden Sie unter. Aktivierung der regionsübergreifenden Suche durch Erstellen eines Aggregatorindexes

Ein Index ist eine Ressource mit einem Amazon-Ressourcennamen (ARN). Sie können diesen ARN jedoch nur in Berechtigungsrichtlinien verwenden, um Zugriff auf Operationen zu gewähren, die direkt mit dem Index interagieren. Mit diesen Vorgängen können Sie Ansichten erstellen und diese als Standard in einer Region festlegen, den Resource Explorer in einer Region ein- oder ausschalten und einen Aggregatorindex für das Konto erstellen. Der ARN eines Indexes sieht dem folgenden Beispiel ähnlich:

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

Anzeigen

Eine Ansicht ist der Mechanismus, der verwendet wird, um die in einem Index aufgelisteten Ressourcen abzufragen. Die Ansicht definiert, welche Informationen im Index sichtbar und für Such- und Entdeckungszwecke verfügbar sind. Ein Benutzer fragt den Resource Explorer-Index niemals direkt ab. Stattdessen müssen Abfragen immer eine Ansicht durchlaufen, sodass der Ersteller der Ansicht einschränken kann, welche Ressourcen der Benutzer in den Suchergebnissen sehen kann.

Wenn Sie eine Ansicht erstellen, geben Sie Filter an, die einschränken, welche Ressourcen in den Suchergebnissen enthalten sind. Sie könnten sich beispielsweise dafür entscheiden, nur Ressourcen einiger bestimmter Ressourcentypen einzubeziehen, die von denjenigen verwendet werden, denen Sie Zugriff auf diese Ansicht gewähren. Ergebnisse von Abfragen, die Benutzer mit einer Ansicht durchführen, werden immer automatisch gefiltert, sodass nur die Ressourcen berücksichtigt werden, die den Kriterien der Ansicht entsprechen.

Um Zugriff auf die Verwendung einer Ansicht zu gewähren, können Sie das Zuweisen von Berechtigungen mithilfe einer der folgenden Methoden verwenden.

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center-Benutzerhandbuch.
- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch.

- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erteilen Sie Ihren Rollen, Gruppen oder Benutzern die Berechtigung, die `resource-explorer-2:Search` Operationen `resource-explorer-2:GetView` und für eine Ansicht aufzurufen, die durch ihren Amazon-Ressourcennamen (ARN) identifiziert wird. Alternativ können Sie die AWSverwaltete Richtlinie „Nur Lesen“ von Resource Explorer für alle Prinzipale verwenden, die die Ansicht für die Suche verwenden müssen. Sie können mehrere Ansichten mit unterschiedlichen Filtern und Bereichen erstellen und somit unterschiedliche Teilmengen Ihrer Ressourceninformationen zurückgeben. Anschließend können Sie Benutzern, die die in den Ergebnissen dieser Ansicht enthaltenen Informationen sehen müssen, Berechtigungen für jede Ansicht gewähren.

Um mit Resource Explorer suchen zu können, muss jeder Benutzer über die Berechtigung verfügen, mindestens eine Ansicht zu verwenden. Sie können im Resource Explorer keine Suche durchführen, ohne eine Ansicht zu verwenden.

Ansichten werden pro Region gespeichert. Eine Ansicht kann in dieser AWS-Region Ansicht nur auf den Resource Explorer-Index zugreifen. Um auf kontoweite Suchergebnisse zuzugreifen, müssen Sie eine Ansicht in der Region verwenden, die den Aggregatorindex für das Konto enthält. Die Option Schnelleinrichtung erstellt eine Standardansicht AWS-Region mit dem Aggregatorindex und mit Filtern, die alle vom Konto AWS-Regionen verwendeten Ressourcen einbeziehen.

Informationen zum Erstellen von Ansichten finden Sie unterResource Explorer-Ansichten verwalten, um Zugriff auf die Suche zu gewähren. Hinweise zur Verwendung von Ansichten in einer Abfrage finden Sie unterVerwendenAWS Ressourcen Explorerum nach Ressourcen zu suchen.

Jede Ansicht hat einen Amazon-Ressourcennamen (ARN), auf den Sie in den Berechtigungsrichtlinien verweisen können, um Zugriff auf einzelne Ansichten zu gewähren. Sie können den ARN einer Ansicht auch als Parameter an jede API oder AWS CLI Operation übergeben, die mit einer Ansicht interagiert. Der ARN einer Ansicht sieht dem folgenden Beispiel ähnlich.

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

> **Note**
>
> Jeder View-ARN enthält am AWS Ende eine generierte UUID. Dadurch wird sichergestellt, dass Benutzer, die möglicherweise Zugriff auf Ansichten mit einem bestimmten Namen hatten, der gelöscht wurde, nicht automatisch auf eine neue Ansicht zugreifen können, die mit demselben Namen erstellt wurde.

Ressource

Eine Ressource ist eine EntitätAWS, mit der Sie arbeiten können. Ressourcen werden erstelltAWS-Services, indem Sie die Funktionen des Dienstes nutzen. Beispiele hierfür sind eine Amazon EC2 EC2-Instance, ein Amazon S3 S3-Bucket oder ein AWS CloudFormation Stack. Einige Ressourcentypen können Kundendaten enthalten. Alle Ressourcentypen verfügen über Attribute oder Metadaten zur Beschreibung der Ressource, einschließlich eines Namens, einer Beschreibung und des Amazon-Ressourcennamens (ARN), den Sie verwenden, um eine Ressource eindeutig zu referenzieren. Die meisten Ressourcentypen unterstützen auch Tags. Bei Tags handelt es sich um benutzerdefinierte Metadaten, die Sie Ihren Ressourcen für eine Vielzahl von Zwecken hinzufügen können, z. B. für die Kostenzuweisung in Ihrer Abrechnung, für die Sicherheitsautorisierung mithilfe einer attributebasierten Zugriffskontrolle oder zur Unterstützung Ihrer anderen Kategorisierungsanforderungen.

Der Hauptzweck von Resource Explorer besteht darin, Ihnen zu helfen, die Ressourcen zu finden, die in Ihrem vorhanden sind. AWS-Konto Resource Explorer verwendet eine Vielzahl von Techniken, um all Ihre Ressourcen zu finden und Informationen darüber in einem Index zu platzieren. Anschließend können Sie den Index über alle Ansichten abfragen, die Ihnen Ihr Administrator zur Verfügung stellt.

> **Important**
>
> Resource Explorer schließt bewusst die Ressourcentypen aus, deren Aufnahme Kundendaten preisgeben würde. Die folgenden Ressourcentypen werden vom Resource Explorer nicht indexiert und werden daher nie in den Suchergebnissen zurückgegeben.
>
> - Amazon S3 S3-Objekte, die in einem Bucket enthalten sind
> - Amazon DynamoDB-Tabellenelemente

- DynamoDB-Attributwerte

Vereinheitlichte Suche in der AWS Management Console

Oben in jedem befindet sich eine SuchleisteAWS-Service, mit der Sie nach einer Vielzahl AWS verwandter Dinge suchen können. AWS Management Console Sie können nach Diensten und Funktionen suchen und erhalten Links direkt zu der entsprechenden Seite in der Konsole dieses Dienstes. Sie können auch nach Dokumentation und Blogartikeln suchen, die sich auf Ihren Suchbegriff beziehen.

Nachdem Sie den Resource Explorer aktiviert und einen Aggregatorindex und eine Standardansicht erstellt haben, kann die vereinheitlichte Suche auch die Ressourcen Ihres Kontos in die Suchergebnisse einbeziehen. Die einheitliche Suche verwendet automatisch die Standardansicht in derAWS-Region, die den Aggregatorindex für das Konto enthält. Auf diese Weise können Sie von jeder Seite im aus nach einer Ressource suchenAWS Management Console, ohne zuerst den Resource Explorer öffnen zu müssen. Wenn Sie einen lokalen Index nicht zum Aggregatorindex für das Konto heraufstufen oder wenn Sie keine Standardansicht in der Aggregator-Index-Region erstellen, bezieht die vereinheitlichte Suche keine Ressourcen in die Suchergebnisse ein. Außerdem muss jeder Principal, der eine Suche durchführt, über die Berechtigung verfügen, die Standardansicht in der Region zu verwenden, die den Aggregatorindex enthält, oder die vereinheitlichte Suche nimmt keine Ressourcen in ihren Suchergebnissen auf.

> **Important**
>
> Bei der einheitlichen Suche wird am Ende des ersten Schlüsselworts in der Zeichenfolge automatisch ein Platzhalterzeichen (*) eingefügt. Das bedeutet, dass vereinheitlichte Suchergebnisse Ressourcen enthalten, die mit einer beliebigen Zeichenfolge übereinstimmen, die mit dem angegebenen Schlüsselwort beginnt.
> Bei der Suche, die im Textfeld Abfrage auf der Seite Ressourcensuche in der Resource Explorer-Konsole ausgeführt wird, wird nicht automatisch ein Platzhalterzeichen angehängt. Sie können nach einem beliebigen Begriff * manuell ein Wort in die Suchzeichenfolge einfügen.

Weitere Informationen zur vereinheitlichten Suche und ihrer Integration mit Resource Explorer finden Sie unterMithilfe der vereinheitlichten Suche in der AWS Management Console.

Suche mit mehreren Konten

Mit der Suche nach mehreren Konten können Sie Ressourcen über und AWS-Regionen mit einer einzigen Stichwortsuche suchen AWS Organizations und entdecken.

Weitere Informationen zur Suche mit mehreren Konten und deren Aktivierung für Resource Explorer finden Sie unter. Suche mit mehreren Konten aktivieren

Voraussetzungen für die Verwendung von Resource Explorer

Führen Sie vor der ersten Verwendung AWS Ressourcen Explorer die folgenden Aufgaben nach Bedarf aus.

Aufgaben

- Melden Sie sich an für ein AWS-Konto
- Erstellen eines Benutzers mit Administratorzugriff

Melden Sie sich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu https://aws.amazon.com/gehst und Mein Konto auswählst.

Erstellen eines Benutzers mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für Ihren Root-Benutzer.

   Anweisungen finden Sie im Benutzerhandbuch unter Aktivieren eines virtuellen MFA Geräts für Ihren AWS-Konto IAM Root-Benutzer (Konsole).

Erstellen eines Benutzers mit Administratorzugriff

1. Aktivieren Sie IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.
2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis im AWS IAM Identity Center Benutzerhandbuch.

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM Identity Center-Benutzer anzumelden, verwenden Sie die Anmeldung, URL die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM Identity Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Zugangsportal.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

   Anweisungen hierzu finden Sie unter Berechtigungssatz erstellen im AWS IAM Identity Center Benutzerhandbuch.

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Eine genaue Anleitung finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center Benutzerhandbuch.

Resource Explorer einrichten und konfigurieren

Bevor Sie mit der Einrichtung und Konfiguration beginnen AWS Ressourcen Explorer, stellen Sie zunächst sicher, dass Sie die Voraussetzungen erfüllen. Melden Sie sich danach als eine IAM Rolle oder ein Benutzer an, der über die erforderlichen Berechtigungen verfügt, um die Resource Explorer-Vorgänge für das folgende Verfahren auszuführen.

Sie können dieses Einrichtungs- und Konfigurationsverfahren verwenden, um Resource Explorer für bestehende Konten und für alle neuen Konten, die Ihrer Organisation hinzugefügt wurden, einzurichten.

Es gibt zwei Möglichkeiten, Resource Explorer einzurichten:

- Schnelleinrichtung
- Erweiterte Einrichtung

> **Important**
>
> Wenn Sie den Resource Explorer mit einer Option einrichten, die AWS-Regionen„Alle“ lautet, werden nur die Optionen aktiviert AWS-Regionen , die vorhanden sind und die AWS-Kontozum Zeitpunkt der Ausführung des Vorgangs aktiviert sind. Der Resource Explorer wird nicht automatisch aktiviert AWS-Regionen , wenn er in future AWS hinzugefügt wird. Wenn eine neue Region AWS eingeführt wird, können Sie den Resource Explorer in der Region

manuell aktivieren, wenn er auf der Seite „Einstellungen“ der Resource Explorer-Konsole angezeigt wird, oder indem Sie den CreateIndexVorgang aufrufen.

> **Note**
>
> Durch die Einrichtung des Resource Explorers können Sie auch die Möglichkeit aktivieren, mithilfe der einheitlichen Suchleiste auf der nach Ressourcen zu suchen AWS Management Console. Damit Benutzer Ressourcen in den vereinheitlichten Suchergebnissen sehen können, müssen Sie Resource Explorer mit einem regionsübergreifenden Aggregatorindex und einer Standardansicht konfigurieren. Einzelheiten finden Sie in den folgenden Verfahren. Sie müssen außerdem sicherstellen, dass Ihre suchenden Benutzer berechtigt sind, die Standardansicht in der Ansicht zu verwenden AWS-Region , die den Aggregatorindex enthält. Weitere Informationen finden Sie unter Mithilfe der vereinheitlichten Suche in der AWS Management Console.

Resource Explorer mithilfe von Quick Setup einrichten

Wenn Sie die Option „Schnelle Einrichtung“ wählen, führt Resource Explorer folgende Aktionen aus:

- Erstellt AWS-Region in jedem von Ihnen einen Index AWS-Konto.
- Aktualisiert den Index in der Region, die Sie als Aggregatorindex für das Konto angeben.
- Erstellt eine Standardansicht in der Aggregator-Index-Region. Diese Ansicht hat keine Filter und gibt daher alle im Index gefundenen Ressourcen zurück.

Mindestberechtigungen

Um die Schritte im folgenden Verfahren ausführen zu können, benötigen Sie die folgenden Berechtigungen:

- Aktion: `resource-explorer-2:*` — Ressource: keine spezifische Ressource (`*`)
- Aktion: `iam:CreateServiceLinkedRole` — Ressource: keine spezifische Ressource (`*`)

AWS Management Console

So richten Sie Resource Explorer mit Quick Setup ein

1. Öffnen Sie die AWS Ressourcen Explorer Konsole unterhttps://console.aws.amazon.com/resource-explorer.
2. Wählen Sie Resource Explorer einschalten.
3. Wählen Sie auf der Seite „Resource Explorer aktivieren“ die Option Schnellinstallation aus.
4. Wählen AWS-Region Sie aus, welchen Aggregatorindex Sie enthalten möchten. Sie sollten die Region auswählen, die für den geografischen Standort Ihrer Benutzer geeignet ist.
5. Wählen Sie unten auf der Seite die Option Resource Explorer einschalten aus.
6. Auf der Fortschrittsseite können Sie jeden Schritt verfolgen, AWS-Region während Resource Explorer seinen Index erstellt. Auf der Seite wird der Status der Erstellung des Aggregator-Indexes und der Erstellung der Standardansicht angezeigt.

Nachdem sich gezeigt hat, dass alle Schritte erfolgreich abgeschlossen wurden, können Sie und Ihre Benutzer zur Seite für die Ressourcensuche navigieren und mit der Suche nach Ressourcen beginnen.

> **Note**
>
> Getaggte Ressourcen, die sich lokal im Index befinden, werden innerhalb weniger Minuten in den Suchergebnissen angezeigt. Es dauert in der Regel weniger als zwei Stunden, bis Ressourcen ohne Tags angezeigt werden. Bei starker Nachfrage kann es jedoch auch länger dauern. Es kann auch bis zu einer Stunde dauern, bis die erste Replikation aller vorhandenen lokalen Indizes zu einem neuen Aggregatorindex abgeschlossen ist.

Nächste Schritte: Bevor Ihre Benutzer mit der soeben erstellten Standardansicht suchen können, müssen Sie ihnen die entsprechenden Suchberechtigungen erteilen. Weitere Informationen finden Sie unter Zugriff auf Resource Explorer-Ansichten für die Suche gewähren.

AWS CLI

Das Einrichten des AWS CLI Resource Explorers in Ihrem mithilfe AWS-Konto von entspricht definitionsgemäß der Einrichtungsoption „Erweitert“. Dies liegt daran, dass die Resource CLI Explorer-Operationen keinen der Schritte automatisch für Sie ausführen, wie dies bei der

Resource Explorer-Konsole der Fall ist. Auf der AWS CLI Registerkarte Resource Explorer mit den erweiterten Einstellungen einrichten auf der können Sie sehen, welche Befehle der Verwendung der Konsole entsprechen.

Resource Explorer mit den erweiterten Einstellungen einrichten

Wenn Sie die Option Erweiterte Einrichtung wählen, können Sie Folgendes tun:

- Wählen Sie den aus, AWS-Regionen in dem der Resource Explorer aktiviert werden soll.
- Wählen Sie aus, ob eine Region mit einem Aggregatorindex konfiguriert werden soll. Wenn Sie dies tun, geben Sie die an, in der es platziert werden AWS-Region soll. Mit diesem Index können Sie Ansichten erstellen, die Ressourcen aus allen Regionen des Kontos enthalten können. Weitere Informationen finden Sie unter Aktivieren der regionsübergreifenden Suche durch Erstellen eines Aggregatorindexes.
- Wählen Sie aus, ob Sie eine Standardansicht erstellen möchten. In dieser Ansicht können Sie in den Regionen, in denen Sie den AWS Ressourcen-Explorer aktivieren, automatisch nach Ressourcen suchen. Sie müssen sicherstellen, dass alle Prinzipale, die die Standardansicht für die Suche im Resource Explorer verwenden müssen, über Berechtigungen für die Ansicht verfügen. Weitere Informationen finden Sie unter Zugriff auf Resource Explorer-Ansichten für die Suche gewähren.

> **Note**
>
> Sie können Resource Explorer so konfigurieren, dass Ihre Ressourcen in die Suchergebnisse aufgenommen werden, die über die einheitliche Suchfunktion auf der AWS Management Console angezeigt werden. Um diese Funktion zu aktivieren, müssen Sie Resource Explorer mit einem Aggregatorindex und einer Standardansicht konfigurieren, mit der alle Rollen und Benutzer suchen können. Mit der Option „Schnellinstallation“ werden sowohl der Aggregatorindex als auch die Standardansicht erstellt. Auf diese Weise empfehlen wir, den Resource Explorer zu aktivieren.

Mindestberechtigungen

Um die Schritte im folgenden Verfahren ausführen zu können, benötigen Sie die folgenden Berechtigungen:

- Aktion: `resource-explorer-2:*` — Ressource: keine spezifische Ressource (`*`)
- Aktion: `iam:CreateServiceLinkedRole` — Ressource: keine spezifische Ressource (`*`)

AWS Management Console

So aktivieren Sie den Resource Explorer mit den erweiterten Einstellungen

1. Öffnen Sie die AWS Ressourcen Explorer Konsole unterhttps://console.aws.amazon.com/resource-explorer.
2. Wählen Sie Resource Explorer einschalten.
3. Wählen Sie auf der Seite „Resource Explorer aktivieren“ die Option Erweiterte Einstellungen aus.
4. Wählen Sie im AWS-RegionenFeld unter Regionen aus, ob Sie den Ressourcen-Explorer in allen AWS-Regionen oder nur in bestimmten Regionen aktivieren möchten.

   Wenn Sie Resource Explorer nur in den AWS-Regionen in diesem Konto angegebenen Bereichen aktivieren wählen, wählen Sie jede Region aus, deren Ressourcen Sie in die Suchergebnisse aufnehmen möchten.
5. Wählen Sie für Aggregator-Index aus, ob Sie einen Aggregator-Index erstellen möchten. Wenn Sie sich dafür entscheiden, einen Aggregatorindex zu erstellen, AWS-Regionen replizieren alle anderen ihre Indizes in diese Region. Auf diese Weise können Benutzer in allen ausgewählten Regionen in der nach Ressourcen suchen. AWS-Konto Wählen Sie den aus AWS-Region , der den Aggregatorindex enthält. Wir empfehlen, dass Sie die Region angeben, in der Ihre Benutzer die meiste Zeit verbringen, oder zumindest, wo Sie davon ausgehen, dass sie die meisten ihrer Ressourcensuchen durchführen werden.
6. Wählen Sie im Feld Standardansicht unter Ansichtserstellung aus, ob eine Standardansicht erstellt werden soll. Diese Option ist nur verfügbar, wenn Sie sich dafür entschieden haben, einen Aggregatorindex zu erstellen. Wenn Sie sich dafür entscheiden, eine Standardansicht zu erstellen, platziert Resource Explorer diese Ansicht in derselben Ansicht AWS-Region wie den Aggregatorindex. Auf diese Weise kann die Standardansicht Ergebnisse von allen Objekten enthalten, AWS-Regionen in denen Sie Resource Explorer registriert haben. Immer wenn ein Benutzer eine Suche in einer Region mit einer Standardansicht durchführt und keine Ansicht explizit angibt, verwendet die Suche die Standardansicht für diese Region.

> **Note**
>
> Bevor Ihre Benutzer mit einer Ansicht suchen können, müssen Sie ihnen die Erlaubnis erteilen, diese Ansicht zu verwenden. Weitere Informationen finden Sie unter Zugriff auf Resource Explorer-Ansichten für die Suche gewähren.

7. Wählen Sie „Resource Explorer aktivieren“.

> **Note**
>
> Getaggte Ressourcen, die sich lokal im Index befinden, werden innerhalb weniger Minuten in den Suchergebnissen angezeigt. Es dauert in der Regel weniger als zwei Stunden, bis Ressourcen ohne Tags angezeigt werden. Bei starker Nachfrage kann es jedoch auch länger dauern. Es kann auch bis zu einer Stunde dauern, bis die erste Replikation aller vorhandenen lokalen Indizes zu einem neuen Aggregatorindex abgeschlossen ist.

AWS CLI

So richten Sie Resource Explorer mit den erweiterten Einstellungen ein

Die Resource Explorer-Konsole führt auf der Grundlage der von Ihnen getroffenen Entscheidungen viele API Betriebsaufrufen in Ihrem Namen durch. Die folgenden AWS CLI Beispielbefehle veranschaulichen, wie Sie dieselben grundlegenden Verfahren auch außerhalb der Konsole mithilfe von ausführen können AWS CLI.

Example Schritt 1: Aktivieren Sie den Resource Explorer, indem Sie Indizes im gewünschten Ordner erstellen AWS-Regionen

Führen Sie den folgenden Befehl in jedem aus, AWS-Region in dem Sie den Resource Explorer aktivieren möchten. Der folgende Beispielbefehl aktiviert den Resource Explorer in dem AWS-Region , was die Standardeinstellung für den ist 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 Schritt 2: Aktualisieren Sie den Index in einem so AWS-Region , dass er der Aggregatorindex für das Konto ist

Führen Sie den folgenden Befehl in dem aus, AWS-Region in dem Resource Explorer den lokalen Index auf den Aggregatorindex für das Konto aktualisieren soll. Der folgende Beispielbefehl aktualisiert den Aggregatorindex im Osten der USA (Nord-Virginia) (`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 Schritt 3: Erstellen Sie eine Ansicht in der AWS-Region , die den Aggregatorindex enthält

Führen Sie den folgenden Befehl in dem aus, AWS-Region in dem Sie den Aggregatorindex erstellt haben. Mit dem folgenden Beispielbefehl wird eine Ansicht erstellt, die mit der Ansicht identisch ist, die beim Setup der Resource Explorer-Konsole erstellt wurde. Diese neue Ansicht umfasst Tags, die der Ressource als Teil der indizierten Informationen zugeordnet sind, und unterstützt die Suche nach Ressourcen anhand eines Tag-Schlüssels oder -werts.

```
$ 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 Schritt 4: Legen Sie Ihre neue Ansicht als Standardansicht für AWS-Region

Im folgenden Beispiel wird die Ansicht, die Sie im vorherigen Schritt erstellt haben, als Standard für die Region festgelegt. Sie müssen den folgenden Befehl in derselben Datei ausführen, AWS-Region in der Sie die Standardansicht erstellt haben.

```
$ 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"
}
```

Bevor Ihre Benutzer mit einer Ansicht suchen können, müssen Sie ihnen Berechtigungen zur Verwendung dieser Ansicht erteilen. Weitere Informationen finden Sie unter Zugriff auf Resource Explorer-Ansichten für die Suche gewähren.

Nachdem Sie diese Befehle ausgeführt haben, wird Resource Explorer in den angegebenen Regionen in Ihrem ausgeführt AWS-Konto. Resource Explorer erstellt und verwaltet in jeder Region einen Index mit Details zu den Ressourcen, die sich dort befinden. Resource Explorer repliziert jeden der einzelnen Regionsindizes in den Aggregatorindex in der angegebenen Region. Diese Region enthält auch eine Ansicht, die es jeder IAM Rolle oder jedem Benutzer im Konto ermöglicht, in allen indizierten Regionen nach Ressourcen zu suchen.

> **Note**
>
> Getaggte Ressourcen, die sich lokal im Index befinden, werden innerhalb weniger Minuten in den Suchergebnissen angezeigt. Es dauert in der Regel weniger als zwei Stunden, bis Ressourcen ohne Tags angezeigt werden. Bei starker Nachfrage kann es jedoch auch

länger dauern. Es kann auch bis zu einer Stunde dauern, bis die erste Replikation aller vorhandenen lokalen Indizes zu einem neuen Aggregatorindex abgeschlossen ist.

Identifizieren Sie, welche Resource Explorer aktiviert AWS-Regionen haben

Sie können herausfinden, welche AWS Ressourcen Explorer aktiviert AWS-Regionen sind, indem Sie überprüfen, ob die Region einen Index für Resource Explorer enthält. Gehen Sie wie auf dieser Seite beschrieben vor, um zu sehen, welche Regionen über einen Index verfügen.

> **Important**
>
> Benutzer können nur in den Regionen nach Ressourcen suchen, in denen der Resource Explorer aktiviert ist. Sie können auch einen Aggregatorindex in einer Region erstellen, um die Suche nach Ressourcen in all Ihren Regionen zu unterstützen. Resource Explorer repliziert Ressourceninformationen mit dem Aggregatorindex aus allen anderen Regionen, die einen Resource Explorer-Index enthalten, in die Region. Benutzer können Resource Explorer nicht verwenden, um Ressourcen in Regionen zu finden, die keinen Index haben.

Überprüfen des Resource Explorer-Status in einer Region

Sie können überprüfen, welche Regionen Indizes für den Resource Explorer haben AWS Management Console, indem Sie den, die Befehle in der AWS Command Line Interface (AWS CLI) verwenden oder API Operationen in einer AWS SDK verwenden.

AWS Management Console

Um zu überprüfen, welche Regionen Indizes für den Resource Explorer haben

1. Öffnen Sie die Seite „Einstellungen“ in der Resource Explorer-Konsole.
2. Die Liste im Abschnitt Indizes enthält nur die Regionen, die einen Resource Explorer-Index enthalten. Der Wert in der Spalte Typ gibt an, ob es sich bei dem Index um einen lokalen Index für die entsprechende Region oder um den Aggregatorindex für handelt. AWS-Konto
3. Um zu sehen, welche Regionen keinen Resource Explorer enthalten, wählen Sie Indizes erstellen. Wenn eine Region nicht vorhanden ist, enthält die Region keinen Resource Explorer.

AWS CLI

Um zu überprüfen, welche Regionen Indizes für Resource Explorer haben

Führen Sie den folgenden Befehl aus, um zu sehen, welche Indizes für Resource Explorer AWS-Regionen haben.

```
$ 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"
        }
    ]
}
```

Den Resource Explorer in einem einschalten AWS-Region , um Ihre Ressourcen zu indizieren

Bei der ersten Aktivierung AWS Ressourcen Explorer in Ihrem AWS-Konto haben Sie Indizes für den Dienst in einem oder mehreren AWS-Regionen erstellt. Wenn Sie die Option Quick Setup verwendet haben, hat Resource Explorer automatisch Indizes in allen AWS-Regionen , die in Ihrem aktiviert sind, erstellt. AWS-Konto Der Resource Explorer-Dienst hat außerdem den Index in der angegebenen Region zum Aggregatorindex für das Konto heraufgestuft. Wenn Sie die Option Erweiterte Konfiguration verwendet haben, haben Sie die Regionen angegeben, in denen Indizes erstellt werden sollen.

Themen

- Erstellen Sie einen Resource Explorer-Index in einer Region
- Überlegungen zu AWS Opt-in-Regionen

Wenn Sie Resource Explorer in einem aktivieren AWS-Region, führt der Dienst die folgenden Aktionen aus:

- Wenn Sie Resource Explorer in der ersten Region in einer starten AWS-Konto, erstellt Resource Explorer eine dienstverknüpfte Rolle in dem genannten `AWSServiceRoleForResourceExplorer` Konto. Diese Rolle gewährt Resource Explorer die Erlaubnis, die Ressourcen in Ihrem Konto mithilfe von Diensten wie und dem Tagging-Dienst zu ermitteln AWS CloudTrail und zu indizieren. Die dienstbezogene Rolle wird erst erstellt, wenn Sie die erste Rolle AWS-Region im Konto registrieren. Resource Explorer verwendet dieselbe dienstbezogene Rolle für alle zusätzlichen Regionen, die Sie später hinzufügen.
- Resource Explorer erstellt einen Index in der angegebenen Region, um die Details zu den Ressourcen dieser Region zu speichern.
- Resource Explorer beginnt mit der Suche nach den Ressourcen in der angegebenen Region und fügt die Informationen, die er über sie findet, dem Index dieser Region hinzu.
- Wenn Ihr Konto bereits einen Aggregatorindex in einer anderen Region enthält, beginnt Resource Explorer damit, die Informationen aus dem Index der neuen Region in den Aggregatorindex zu replizieren, um die regionsübergreifende Suche zu unterstützen.

Wenn diese Schritte abgeschlossen sind, stehen den Benutzern Informationen zu Ihren Ressourcen zur Verfügung. Sie können mithilfe einer der Ansichten suchen, die entweder in derselben Region oder in der Region definiert sind, die den Aggregatorindex enthält.

Erstellen Sie einen Resource Explorer-Index in einer Region

Sie können einen Resource Explorer-Index in einem zusätzlichen AWS-Region Verzeichnis erstellen AWS Management Console, indem Sie den, mithilfe von Befehlen in AWS Command Line Interface (AWS CLI) oder mithilfe von API Operationen in einem AWS SDK. Sie können nur einen Index in einer Region erstellen.

Mindestberechtigungen

Um die Schritte im folgenden Verfahren ausführen zu können, benötigen Sie die folgenden Berechtigungen:

- Aktion: `resource-explorer-2:*` — Ressource: keine spezifische Ressource (`*`)
- Aktion: `iam:CreateServiceLinkedRole` — Ressource: keine spezifische Ressource (`*`)

AWS Management Console

Um einen Resource Explorer-Index in einem zu erstellen AWS-Region

1. Auf der Seite mit den Resource Explorer-Einstellungen.
2. Wählen Sie im Abschnitt Indizes die Option Indizes erstellen aus.
3. Aktivieren Sie auf der Seite Indizes erstellen die Kontrollkästchen neben dem, AWS-Regionen in dem Sie einen Index erstellen möchten, um das Durchsuchen der Ressourcen dieser Region zu unterstützen. Nicht verfügbare Kontrollkästchen weisen auf Regionen hin, die bereits einen Resource Explorer-Index enthalten.
4. (Optional) Im Abschnitt Tags können Sie Tag-Schlüssel- und Wertepaare für den Index angeben.
5. Wählen Sie Indizes erstellen aus.

   Resource Explorer zeigt oben auf der Seite ein grünes Banner an, um auf Erfolg hinzuweisen, oder ein rotes Banner, wenn beim Erstellen eines Indexes in einer oder mehreren der ausgewählten Regionen ein Fehler auftritt.

> **Note**
>
> Getaggte Ressourcen, die sich lokal im Index befinden, werden innerhalb weniger Minuten in den Suchergebnissen angezeigt. Es dauert in der Regel weniger als zwei Stunden, bis Ressourcen ohne Tags angezeigt werden. Bei starker Nachfrage kann es jedoch länger dauern. Es kann auch bis zu einer Stunde dauern, bis die erste Replikation aller vorhandenen lokalen Indizes zu einem neuen Aggregatorindex abgeschlossen ist.

Nächster Schritt — Wenn Sie bereits einen Aggregatorindex erstellt haben, beginnen die neuen Regionen automatisch, ihre Indexinformationen in den Aggregatorindex zu replizieren. Wenn Ihre Benutzer dort ihre gesamte Suche durchführen, werden die Ressourcen in der neuen Region in diesen Suchergebnissen angezeigt, und Sie sind fertig.

Wenn Sie jedoch möchten, dass Benutzer nur in der neu indizierten Region nach Ressourcen suchen können, müssen Sie auch eine Ansicht für Benutzer in dieser Region erstellen und Ihren Benutzern Berechtigungen für diese Ansicht gewähren. Anweisungen zum Erstellen einer Ansicht finden Sie unterResource Explorer-Ansichten verwalten, um Zugriff auf die Suche zu gewähren.

AWS CLI

So erstellen Sie einen Resource Explorer-Index in einem AWS-Region

Führen Sie den folgenden Befehl für jeden aus, AWS-Region in dem Sie einen Index erstellen möchten, um das Durchsuchen der Ressourcen dieser Region zu unterstützen. Mit dem folgenden Beispielbefehl wird Resource Explorer im Osten der USA (Nord-Virginia) registriert (`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"
}
```

Wiederholen Sie diesen Befehl für jede Region, in der Sie den Resource Explorer aktivieren möchten, und ersetzen Sie den Parameter durch den entsprechenden Regionalcode. `--region`

Da Resource Explorer einen Teil der Indexerstellung als asynchrone Aufgaben im Hintergrund ausführt, kann die Antwort lauten`CREATING`, dass die Hintergrundprozesse noch nicht abgeschlossen sind.

> **Note**
>
> Markierte Ressourcen, die sich lokal im Index befinden, werden innerhalb weniger Minuten in den Suchergebnissen angezeigt. Es dauert in der Regel weniger als zwei Stunden, bis Ressourcen ohne Tags angezeigt werden. Bei starker Nachfrage kann es jedoch länger dauern. Es kann auch bis zu einer Stunde dauern, bis die erste Replikation aller vorhandenen lokalen Indizes zu einem neuen Aggregatorindex abgeschlossen ist.

Sie können den endgültigen Abschluss überprüfen, indem Sie den folgenden Befehl ausführen und den `ACTIVE` Status überprüfen.

```
$ 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"
}
```

Nächster Schritt — Wenn Sie bereits einen Aggregatorindex erstellt haben, beginnen die neuen Regionen automatisch, ihre Indexinformationen in den Aggregatorindex zu replizieren. Wenn Ihre Benutzer dort ihre gesamte Suche durchführen, werden die Ressourcen in der neuen Region in diesen Suchergebnissen angezeigt, und Sie sind fertig.

Wenn Sie jedoch möchten, dass Benutzer nur in der neu indizierten Region nach Ressourcen suchen können, müssen Sie auch eine Ansicht für Benutzer in dieser Region erstellen und Ihren Benutzern Berechtigungen für diese Ansicht gewähren. Anweisungen zum Erstellen einer Ansicht finden Sie unterResource Explorer-Ansichten verwalten, um Zugriff auf die Suche zu gewähren.

Überlegungen zu AWS Opt-in-Regionen

Für Opt-in-Regionen gelten höhere Sicherheitsanforderungen als für kommerzielle Regionen, was die gemeinsame Nutzung von IAM Daten über Konten in Opt-in-Regionen betrifft. Alle über den IAM Dienst verwalteten Daten gelten als Identitätsdaten.

Sie können Opt-in-Regionen über die AWS Ressourcen Explorer Konsole aktivieren. Weitere Informationen finden Sie unter Den Resource Explorer aktivieren AWS-Region , um Ihre Ressourcen zu indizieren.

Verhalten beim Abmelden

Beachten Sie die folgenden Verhaltensweisen, bevor Sie sich von einer Opt-in-Region abmelden:

> **Important**
>
> Bevor Sie sich von einer Region mit einem Aggregatorindex abmelden, empfehlen wir Ihnen, den Aggregatorindex zu löschen oder ihn zu einem lokalen Index herabzustufen. Resource Explorer unterstützt einen Aggregatorindex für alle Regionen innerhalb der Partition.

- Ihr Index wird nicht gelöscht, er ist nur deaktiviert. Wenn Sie sich später erneut anmelden, werden Ihre Einstellungen zurückgesetzt.
- IAMdeaktiviert IAM den Zugriff auf Ressourcen in der Region.
- Resource Explorer deaktiviert den Index für die Region, für die Sie sich abgemeldet haben, und beendet die Datenaufnahme. Der `ListIndexes` API Regionsindex wird nicht mehr angezeigt.
- Wenn sich Ihr Aggregatorindex in einer anderen Region befindet, stoppt Resource Explorer die Datenreplikation aus der Region, für die Sie sich entschieden haben, und bereinigt die Daten innerhalb von 24 Stunden.
- Wenn Sie Ihre Aggregator-Index-Region deaktivieren, müssen Sie sich erneut anmelden, um den Index zu löschen oder herabzustufen.
- Wenn Sie sich erneut für die Region anmelden, aktiviert Resource Explorer den Index erneut und beginnt mit der Datenaufnahme.
- Es dauert etwa 24 Stunden, bis alle Änderungen am Status einer Opt-in-Region wirksam werden.

Aktivierung der regionsübergreifenden Suche durch Erstellen eines Aggregatorindexes

Wenn die regionsübergreifende Suche aktiviert ist, können Sie in allen Regionen Ihrer AWS-Konto Region nach Ressourcen suchen.

Themen

- Über den Aggregator-Index
- Einen lokalen Index zum Aggregatorindex für das Konto heraufstufen
- Den Aggregatorindex auf einen lokalen Index herabstufen

Über den Aggregator-Index

AWS Ressourcen Explorer speichert die gesammelten Informationen über die Ressourcen in einem lokalen Index, AWS-Region den Resource Explorer in dieser Region erstellt und verwaltet. Nehmen wir beispielsweise an, dass Sie eine EC2 Amazon-Instance in der Region USA West (Oregon) haben. Resource Explorer speichert die Details zu dieser Ressource im lokalen Index in der Region USA West (Oregon).

Um die Suche nach Ressourcen AWS-Regionen in Ihrem gesamten Konto zu unterstützen, können Sie den lokalen Index in einer Region in den Aggregatorindex für Ihr Konto umwandeln.

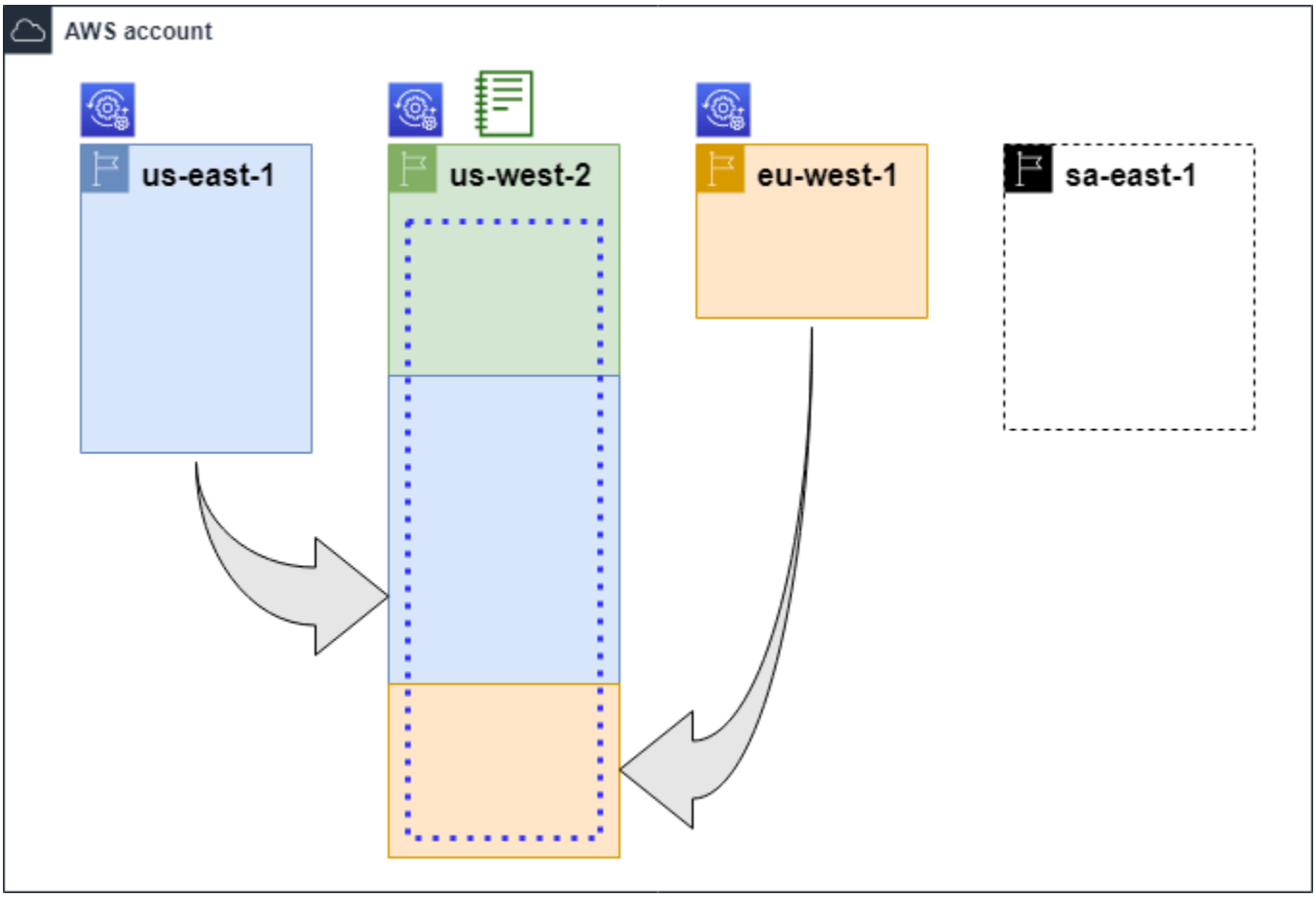
Der Aggregatorindex enthält eine replizierte Kopie des lokalen Indexes in allen anderen Regionen, in denen Sie Resource Explorer aktiviert haben. Auf diese Weise können Sie Ansichten in der Region erstellen, die den Aggregatorindex enthält, deren Ergebnisse Ressourcen aus allen AWS-Regionen Konten enthalten können.

Das folgende Diagramm zeigt ein Beispiel dafür, wie der Aggregatorindex funktioniert. In diesem AWS-Konto Beispiel geht der Administrator wie folgt vor:

- Aktiviert den Resource Explorer in drei Bereichen AWS-Regionen (`us-east-1`us-west-2, und`eu-west-1`), indem Indizes in diesen Regionen erstellt werden. Jede Region enthält ihren eigenen lokalen Index.
- Entscheidet sich, keinen Index in der `sa-east-1` Region zu erstellen. Benutzer können in dieser Region keine Suchen durchführen`sa-east-1`, und in den Suchergebnissen werden keine Ressourcen aus dieser Region angezeigt.

- Erstellt den Aggregatorindex für das Konto in der `us-west-2` Region. Dadurch repliziert Resource Explorer Informationen aus den lokalen Indizes in allen anderen Regionen, in denen Resource Explorer aktiviert ist, auf den Aggregatorindex. Dadurch können Suchvorgänge in `us-west-2` Ressourcen aus allen drei Regionen durchgeführt werden, in denen der Resource Explorer aktiviert ist.

Diese Konfiguration bedeutet, dass ein Benutzer regionsübergreifende Suchen nur in der Region durchführen kann`us-west-2`, die den Aggregatorindex enthält. Nur Ansichten aus dieser Region können Ergebnisse aus allen Regionen des Kontos zurückgeben.



Legende	
	Der Resource Explorer ist dabei aktiviert AWS-Region, und seine Ressourcen werden in einem Index in dieser Region katalogisiert. Der Index dieser Region wird auch in den Index repliziert (angezeigt durch die Pfeile) AWS-Region , der den Aggregatorindex enthält.

	Dieser AWS-Region enthält den Aggregatorindex. Resource Explorer repliziert die in allen anderen Ländern gesammelten Ressourceninformationen AWS-Regionen in diese Region.
	Die von Quick Setup erstellte Standardansicht umfasst alle Ressourcen. AWS-Regionen

Einen lokalen Index zum Aggregatorindex für das Konto heraufstufen

Sie habenAWS-Region bei der ersten Einrichtung die Möglichkeit, einen Aggregatorindex in einem zu erstellenAWS Ressourcen Explorer. Weitere Informationen finden Sie unter Resource Explorer einrichten und konfigurieren. Bei diesem Verfahren geht es darum, einen der lokalen Indizes zum Aggregatorindex für das Konto hochzustufen, falls Sie dies bei der ersten Einrichtung nicht getan haben.

> **Important**
>
> - Sie können nur einen Aggregatorindex in einem habenAWS-Konto. Wenn das Konto bereits über einen Aggregatorindex verfügt, müssen Sie es zunächst entweder auf einen lokalen Index herabstufen oder löschen.
> - Nachdem Sie gelöscht oder geändert haben, welche Region den Aggregatorindex enthält, müssen Sie 24 Stunden warten, bevor Sie einen anderen Index zum Aggregatorindex heraufstufen können.

AWS Management Console

Um einen lokalen Index zum Aggregatorindex für das Konto zu machen

1. Öffnen Sie die Seite mit den Resource Explorer-Einstellungen.
2. Aktivieren Sie im Abschnitt Indizes das Kontrollkästchen neben dem Index, den Sie heraufstufen möchten, und wählen Sie dann Indextyp ändern.
3. Wählen Sie im Dialogfeld „Indextyp ändern für < Regionsname“ die Option „Aggregatorindex“ und dann „Änderungen speichern“.

AWS CLI

Um einen lokalen Index zum Aggregatorindex für das Konto zu machen

Der folgende Beispielbefehl aktualisiert den Index im angegebenen FormatAWS-Region von Typ`LOCAL` zu Typ`AGGREGATOR`. Sie müssen die Operation von der aufrufenAWS-Region, die den Aggregatorindex enthalten soll.

```
$ 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"
}
```

Der Vorgang funktioniert asynchron und beginnt mit`State` set to`UPDATING`. Um zu überprüfen, ob der Vorgang abgeschlossen wurde, können Sie den folgenden Befehl ausführen und`ACTIVE` im`State` Antwortfeld nach dem Wert suchen. Sie müssen diesen Befehl in der Region ausführen, die den Index enthält, den Sie überprüfen möchten.

```
$ 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"
}
```

Den Aggregatorindex auf einen lokalen Index herabstufen

Sie können einen Aggregatorindex zu einem lokalen Index herabstufen, z. B. wenn Sie den Aggregatorindex in einen anderen verschieben möchten. AWS-Region

Wenn Sie einen Aggregatorindex zu einem lokalen Index herabstufen, beendet Resource Explorer die Replikation der Indizes aus anderen. AWS-Regionen Außerdem wird eine asynchrone Hintergrundaufgabe gestartet, um alle replizierten Informationen aus anderen Regionen zu löschen. Bis diese asynchrone Aufgabe abgeschlossen ist, können einige regionsübergreifende Ergebnisse weiterhin in den Suchergebnissen angezeigt werden.

Hinweise

- Nachdem Sie einen Aggregatorindex herabgestuft haben, müssen Sie 24 Stunden warten, bevor Sie entweder denselben Index oder den Index in einer anderen Region zum neuen Aggregatorindex für das Konto heraufstufen können.
- Nach dem Herabstufen eines Aggregatorindexes kann es bis zu 36 Stunden dauern, bis die Hintergrundprozesse abgeschlossen sind und alle Ressourceninformationen aus anderen Regionen aus den Ergebnissen der in dieser Region durchgeführten Suchanfragen verschwinden.
- Wenn Sie ein Mitgliedskonto in einer unternehmensweiten Ansicht herabstufen, wird das Mitglied möglicherweise aus der Suche nach mehreren Konten entfernt.

Sie können den Status der Hintergrundaufgabe überprüfen, indem Sie sich die Liste der Indizes auf der Seite Einstellungen ansehen oder den Vorgang verwenden. GetIndex Wenn die asynchronen Aufgaben abgeschlossen sind, ändert sich das `Status` Feld aus dem Index von `UPDATING` zu. `ACTIVE` Zu diesem Zeitpunkt werden nur Ergebnisse aus der lokalen Region in den Abfrageergebnissen angezeigt.

AWS Management Console

Um einen Aggregatorindex zu einem lokalen Index herabzustufen

1. Öffnen Sie die Seite mit den Resource Explorer-Einstellungen.

2. Aktivieren Sie im Abschnitt Indizes das Kontrollkästchen neben der Region, die den Aggregatorindex enthält, den Sie zu einem lokalen Index herabstufen möchten, und wählen Sie dann Indextyp ändern aus.
3. Wählen Sie im Dialogfeld Indextyp ändern für **<** Regionsname **>** die Option Lokaler Index und dann Änderungen speichern aus.

AWS CLI

Um einen Aggregatorindex zu einem lokalen Index herabzustufen

Im folgenden Beispiel wird der angegebene Aggregatorindex zu einem lokalen Index herabgestuft. Sie müssen die Operation in dem aufrufenAWS-Region, der derzeit den Aggregatorindex enthält.

```
$ 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"
}
```

Der Vorgang funktioniert asynchron und beginnt mit `State` set to. `UPDATING` Um zu überprüfen, ob der Vorgang abgeschlossen wurde, können Sie den folgenden Befehl ausführen und `ACTIVE` im `State` Antwortfeld nach dem Wert suchen. Sie müssen diesen Befehl in der Region ausführen, die den Index enthält, den Sie überprüfen möchten.

```
$ 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"
}
```

Suche mit mehreren Konten aktivieren

Mit der Suche nach mehreren Konten können Sie in allen Konten mit aktiven Indizes in Ihrer AWS Organizations oder Ihrer Organisationseinheit (OU) nach Ressourcen suchen.

Themen

- Voraussetzungen
- Aktivieren Sie die Suche mit mehreren Konten
- Schnelle Einrichtung für mehrere Konten
- Auswirkung von Kontoaktionen auf die Suche nach mehreren Konten in Resource Explorer

Voraussetzungen

Gehen Sie wie folgt vor, um die Suche mit mehreren Konten für Ihre Organisation zu aktivieren:

- Stellen Sie bei Regionen mit Opt-in-Option sicher, dass Ihr Verwaltungskonto auch aktiviert ist, wenn Sie die Suche mit mehreren Konten aktivieren.
- Erstellen Sie einen Administratorbenutzer.
- Erstellen Sie eine mit dem Dienst verknüpfte Rolle im Administratorkonto mit. `aws iam create-service-linked-role --aws-service-name resource-explorer-2.amazonaws.com`
- Aktivieren Sie den vertrauenswürdigen Zugriff in AWS Organizations. Dies ermöglicht eine vollständige Integration mit Resource Explorer, um Ressourcen für alle Konten in Ihrer Organisation aufzulisten.
- Weisen Sie einen delegierten Administrator zu (empfohlen). Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter Delegierter Administrator für AWS Dienste, die mit Organizations funktionieren.
  - Resource Explorer unterstützt nur einen delegierten Administrator, der ähnliche Aktionen wie das Verwaltungskonto ausführt.
  - Wenn Sie den delegierten Administrator für Ihre Organisation entfernen oder ändern, werden alle in diesem Konto erstellten Ansichten mit mehreren Konten entfernt.

Aktivieren Sie die Suche mit mehreren Konten

Um Ressourcen in den Konten Ihrer Organisation zu suchen und zu finden, müssen Sie die folgenden Schritte ausführen:

1. Aktivieren Sie es AWS Ressourcen Explorer in einem oder mehreren Konten in Ihrem AWS Organizations.
2. Registrieren Sie eine Region, die den Aggregatorindex enthalten soll.
3. Wählen Sie eine Region aus, in der Sie einen Aggregatorindex erstellen möchten. Diese Region muss in Ihrer AWS Organizations Region einheitlich sein.
4. Erstellen Sie eine Resource Explorer-Ansicht, die auf Sie AWS Organizations oder Ihre Organisationseinheit zugeschnitten ist. Erstellen Sie diese Ansicht in der Aggregator-Region aus dem vorherigen Schritt.
5. Teilen Sie die Ansicht mit Konten in Ihrer gesamten Organisation.

Schnelle Einrichtung für mehrere Konten

Mit der Schnellinstallation können Sie Resource Explorer für mehrere Konten in Ihrer Organisation aktivieren.

> **Note**
>
> Bei diesem Vorgang werden keine Ressourcen im Verwaltungskonto bereitgestellt. Wenn Sie das Verwaltungskonto verwenden und Indizes im Konto haben möchten, müssen Sie diese manuell mit dem Resource Explorer-Onboarding-Flow hinzufügen.

1. Navigieren Sie in der Systems Manager Manager-Konsole zu Quick Setup for Resource Explorer.
2. Wählen Sie Ihre Aggregator-Index-Region aus. Auf diese Weise können Sie nach Ressourcen suchen, die sich in allen Regionen der ausgewählten Zielkonten befinden. Wenn für eines der ausgewählten Zielkonten bereits ein Aggregatorindex in einer anderen Region konfiguriert ist, wird der bestehende Aggregatorindex automatisch durch diese neue Region ersetzt.
3. Wählen Sie Ihre Kontoziele aus. Sie können Resource Explorer für Ihre gesamte Organisation oder für bestimmte Organisationseinheiten aktivieren (OUs).

> **Note**
>
> Sie können maximal 50.000 AWS CloudFormation Stacks gleichzeitig bereitstellen. Wenn Sie eine große Organisation haben, die sich über mehrere Regionen erstreckt, sollten Sie die Bereitstellung auf OU-Ebene in kleineren Batches durchführen.

4. Lesen Sie sich die Zusammenfassung der Bestätigungen durch, bevor Sie Create wählen.

Auswirkung von Kontoaktionen auf die Suche nach mehreren Konten in Resource Explorer

> **Note**
>
> Das Entfernen von Konten und Ressourcen aus den Suchergebnissen mit mehreren Konten dauert bis zu 24 Stunden.

Kontoaktionen haben die folgenden Auswirkungen auf die Suche AWS Ressourcen Explorer mit mehreren Konten.

Resource Explorer ist deaktiviert

Wenn Sie den Ressourcen-Explorer für ein Konto deaktivieren, ist er nur für das Konto deaktiviert AWS-Region , das bei der Deaktivierung ausgewählt wurde.

Sie müssen Resource Explorer in jeder Region, in der er aktiviert ist, separat deaktivieren.

Nach 24 Stunden werden Ressourcen aus diesem Konto nicht in den Suchergebnissen angezeigt.

Andere Resource Explorer-Daten und -Einstellungen werden nicht entfernt.

Das Mitgliedskonto wurde aus einer Organisation entfernt

Wenn ein Mitgliedskonto aus einer Organisation entfernt wird, verliert das Resource Explorer-Administratorkonto die Berechtigungen zum Anzeigen von Ressourcen im Mitgliedskonto.

Wenn es sich bei dem entfernten Konto um ein Administrator- oder delegiertes Administratorkonto handelt, werden alle Ansichten mit mehreren Konten, die zuvor von diesen Konten erstellt wurden, ebenfalls entfernt.

Resource Explorer wird weiterhin in beiden Konten ausgeführt.

Die Ergebnisse der Ressourcensuche enthalten keine Ressourcen aus diesem Konto mehr.

Das Konto ist gesperrt

Wenn ein Konto gesperrt wird AWS, verliert das Konto die Berechtigungen zum Anzeigen von Ressourcen im Resource Explorer. Das Administratorkonto für ein gesperrtes Konto kann die vorhandenen Ressourcen einsehen.

Bei einem Unternehmenskonto kann der Status des Mitgliedskontos auch in Konto gesperrt geändert werden. Dies ist der Fall, wenn das Konto gleichzeitig gesperrt wird, während das Administratorkonto versucht, das Konto zu aktivieren. Das Administratorkonto für ein gesperrtes Konto kann die Ressourcen für dieses Konto nicht anzeigen.

Andernfalls hat der Status „Gesperrt“ keinen Einfluss auf den Status des Mitgliedskontos.

Nach 90 Tagen wird das Konto entweder deaktiviert oder reaktiviert. Wenn das Konto reaktiviert wird, werden seine Resource Explorer-Berechtigungen wiederhergestellt. Wenn das Mitgliedskonto den Status Konto gesperrt hat, muss das Administratorkonto das Konto manuell aktivieren.

Das Konto ist geschlossen

Wenn ein AWS Konto geschlossen wird, reagiert Resource Explorer wie folgt auf die Schließung:

- Resource Explorer bewahrt die Ressourcen für das Konto für einen Zeitraum von 90 Tagen ab dem Datum des Inkrafttretens der Kontoschließung auf. Am Ende des 90-Tage-Zeitraums löscht Resource Explorer dauerhaft alle Ressourcen für das Konto.
- Um Ressourcen für mehr als 90 Tage aufzubewahren, können Sie eine benutzerdefinierte Aktion mit einer EventBridge Regel verwenden, um die Ressourcen in einem Amazon S3 S3-Bucket zu speichern. Solange Resource Explorer die Ressourcen aufbewahrt, stellt Resource Explorer die Ressourcen für das Konto wieder her, wenn Sie das geschlossene Konto erneut öffnen.
- Wenn es sich bei dem Konto um ein Resource Explorer-Administratorkonto handelt, wird es als Administrator entfernt und alle Mitgliedskonten werden entfernt. Wenn es sich bei dem Konto um ein Mitgliedskonto handelt, wird es getrennt und als Mitglied aus dem Resource Explorer-Administratorkonto entfernt.

- Weitere Informationen finden Sie unter Schließen eines Kontos.

Abmeldung vom Konto

Wenn sich ein Konto von einer Region abmeldet, werden Ihnen deren Ressourcen weiterhin bis zu 24 Stunden in den Suchergebnissen angezeigt.

Nach 24 Stunden werden Ressourcen aus diesem Konto nicht mehr in den Suchergebnissen angezeigt. Weitere Informationen finden Sie unter Verhalten beim Abmelden.

Unterstützung der einheitlichen Suche in der AWS Management Console

Das AWS Management Console hat oben auf jeder Konsolenseite eine Suchleiste. Dies bietet ein einheitliches Sucherlebnis für alle AWS-Services. Einheitliche Suchergebnisse können unter anderem Folgendes beinhalten:

- AWS-Service und bieten Konsolenseiten.
- AWS Dokumentationsseiten.
- AWS Blog- und Knowledge-Base-Artikel
- Ressourcen in Ihren Konten — wenn Sie die folgenden Schritte befolgen.

Um die Ressourcen Ihres Kontos in Ihren vereinheitlichten Suchergebnissen zu sehen, müssen Sie die folgenden Schritte ausführen. Sie können dies bei der Ersteinrichtung von tun AWS Ressourcen Explorer. Alles passiert automatisch, wenn Sie die Option Quick Setup verwenden.

- Sie müssen einen Aggregatorindex in einem AWS-Region für den AWS-Konto erstellen.
- Sie müssen eine Standardansicht in der erstellen AWS-Region , die den Aggregatorindex enthält.
- Sie müssen allen Principals, die in der vereinheitlichten Suchleiste nach Ressourcen suchen müssen, die Berechtigung erteilen, mit dieser Standardansicht zu suchen.

Bei der einheitlichen Suche wird immer die Standardansicht in der Ansicht verwendet AWS-Region , die den Aggregatorindex enthält, um alle Suchen durchzuführen.

Bereitstellen von Resource Explorer für die Konten in einer Organisation

Mithilfe AWS CloudFormation StackSets von können Sie alle in einer Organisation verwalteten Konten definieren und diese für alle Konten bereitstellen, die in einer Organisation verwaltet werden AWS Organizations. Wenn Sie ein Stack-Set definieren, geben Sie AWS Ressourcen an, die Sie für alle von Ihnen angegebenen Zielkonten AWS-Regionen und für alle von Ihnen angegebenen Zielkonten erstellen möchten. Wenn alle Konten Teil derselben Organisation sind, können Sie die Vorteile der AWS CloudFormation Integration mit Organizations nutzen und diese Dienste die kontoübergreifende Rollenerstellung übernehmen lassen. Sie können die automatische Bereitstellung in einer Organisation aktivieren, wodurch Stack-Instances automatisch für neue Konten bereitgestellt werden, die Sie möglicherweise in future der Zielorganisation oder einer Organisationseinheit (OU) hinzufügen. Wenn Sie ein Konto aus der Organisation entfernen, AWS CloudFormation werden automatisch alle Ressourcen gelöscht, die als Teil einer Organisations-Stack-Instanz bereitgestellt wurden. Weitere Informationen zu StackSets finden Sie unter Arbeiten mit AWS CloudFormation StackSets im AWS CloudFormation Benutzerhandbuch.

Sie können AWS CloudFormation StackSets es verwenden, um alle Konten AWS Ressourcen Explorer in Ihrer Organisation zu aktivieren und zu konfigurieren, Indizes in jeder aktivierten Region zu erstellen und Ansichten dort zu erstellen, wo Sie sie benötigen.

> **Important**
>
> Wenn Sie versuchen, einen Aggregatorindex in einer Region einzurichten, müssen Sie sicherstellen, dass für das Konto kein Aggregatorindex in anderen Regionen vorhanden ist. Nachdem Sie einen Aggregatorindex zu einem lokalen Index herabgestuft haben, müssen Sie 24 Stunden warten, bevor Sie einen anderen Index zum neuen Aggregatorindex für das Konto heraufstufen können.

Voraussetzungen

Um Resource Explorer für die Konten in Ihrer Organisation bereitzustellen, müssen Sie oder der Administrator Ihrer Organisation zunächst die folgenden Schritte ausführen, um Stacks mit vom Dienst verwalteten Berechtigungen zu aktivieren: AWS CloudFormation StackSets

1. In der Organisation müssen alle Funktionen aktiviert sein. Wenn in der Organisation nur Funktionen für die konsolidierte Abrechnung aktiviert sind, können Sie kein Stack-Set mit vom Service verwalteten Berechtigungen erstellen.
2. Aktivieren Sie den vertrauenswürdigen Zugriff zwischen AWS CloudFormation und Organizations. Dadurch wird die AWS CloudFormation Berechtigung erteilt, die benötigten Rollen im Verwaltungskonto der Organisation zu erstellen, und die Mitgliedskonten AWS CloudFormation stellen Resource Explorer-Indizes und -Ansichten bereit.

Jetzt können Sie Stack-Sets mit vom Service verwalteten Berechtigungen erstellen.

> **Important**
>
> Sie müssen die Stack-Sets im Verwaltungskonto der Organisation erstellen. AWS CloudFormation ist ein regionaler Dienst, sodass Sie die von Ihnen erstellten Stack-Sets nur in der Region anzeigen und verwalten können, in der Sie sie ursprünglich erstellt haben.

Die Stack-Sets für Resource Explorer erstellen

Um Resource Explorer vollständig bereitstellen zu können, müssen Sie zwei Stack-Sets bereitstellen.

- Das erste Stack-Set erstellt den Aggregatorindex und die Standardansicht, mit der Benutzer in allen Regionen des Kontos nach Ressourcen suchen können.

  Stellen Sie dieses Stack-Set nur für die einzelne Region bereit, in der Sie den Aggregatorindex erstellen möchten.
- Das zweite Stack-Set erstellt einen lokalen Index und eine Standardansicht. Der lokale Index repliziert seinen Inhalt in den Aggregatorindex.

  Stellen Sie dieses Stack-Set für jede aktivierte Region im Konto bereit, mit Ausnahme der Region, die den Aggregatorindex enthält. Wählen Sie keine Regionen aus, die in den Konten, für die Sie den Stack bereitstellen, nicht aktiviert sind. Wenn Sie dies tun, schlägt die Bereitstellung fehl.

Beispielvorlagen für jede dieser Vorlagen finden Sie im folgenden Abschnitt. step-by-stepAnweisungen zum Erstellen eines Stack-Sets mithilfe dieser Vorlagen finden Sie im AWS CloudFormation Benutzerhandbuch unter Erstellen eines Stack-Sets mit vom Service verwalteten Berechtigungen.

Nachdem Sie diese Stack-Sets in Ihrer Organisation bereitgestellt haben, hat jedes Konto innerhalb des von Ihnen ausgewählten Bereichs, Organisation oder Organisationseinheit, einen Aggregatorindex in der angegebenen Region und lokale Indizes in jeder anderen Region.

Beispielvorlagen AWS CloudFormation

Die folgende Beispielvorlage erstellt den Aggregatorindex des Kontos und eine Standardansicht, mit der in allen Regionen des Kontos, in dem Sie einen Index bereitstellen, nach Ressourcen gesucht werden kann.

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"
                }
            }
        }
    }
}
```

Die folgende Beispielvorlage erstellt einen lokalen Index in jeder aktivierten Region in allen Konten außer dem Konto mit dem Aggregatorindex. Außerdem wird eine Standardansicht erstellt, in der Benutzer nur in dieser Region nach Ressourcen suchen können. Benutzer müssen mit einer Ansicht in der Aggregator-Region suchen, um in allen Regionen nach Ressourcen suchen zu können.

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"
                }
            }
        }
    }
}
```

Resource Explorer ausschalten

Wenn Sie in einer bestimmten Region nicht mehr nach Ressourcen suchen müssen AWS-Region, können Sie die Option nur AWS Ressourcen Explorer in dieser Region deaktivieren, indem Sie den Index löschen, oder Sie können den Ressourcen-Explorer in allen Bereichen löschen AWS-Regionen. Wenn Sie dies tun, stoppt Resource Explorer die Suche nach neuen oder aktualisierten Ressourcen in dieser Region. Wenn Ihr Konto einen Aggregatorindex enthält, wird die Replikation aus dem gelöschten Index beendet, und die Informationen aus dem gelöschten Index werden aus dem Aggregatorindex entfernt und erscheinen nicht mehr in den Suchergebnissen. Es kann bis zu 24 Stunden dauern, bis alle Ressourcen aus dem gelöschten Index aus den Suchergebnissen in der Region mit dem Aggregatorindex verschwinden.

> **Note**
>
> Wenn Sie die erste registrieren AWS-Region, erstellt Resource Explorer eine dienstverknüpfte Rolle (SLR) mit `AWSServiceRoleForResourceExplorer` dem AWS-Konto Namen. Resource Explorer löscht dies nicht SLR automatisch. Nachdem Sie den Resource Explorer-Index in jeder Region des Kontos gelöscht haben, können Sie die IAM Konsole verwenden, um den zu löschen, SLR falls Sie Resource Explorer in future nicht mehr verwenden werden. Wenn Sie die Rolle löschen und dann den Resource Explorer in mindestens einer Rolle erneut aktivieren möchten AWS-Region, erstellt Resource Explorer die mit dem Dienst verknüpfte Rolle automatisch neu.

Resource Explorer in einem Fall ausschalten AWS-Region

Sie können den Ressourcen-Explorer in einem deaktivieren, AWS-Region indem Sie den AWS Management Console, mithilfe von Befehlen in der AWS Command Line Interface (AWS CLI) oder mithilfe von API Operationen in einem AWS SDK.

Wenn Sie den Ressourcen-Explorer für ein Mitgliedskonto deaktivieren und das Mitglied in einer organisationsweiten Ansicht angezeigt wird, wird es aus den Suchergebnissen für mehrere Konten entfernt.

Wenn Sie die Suche nach Ressourcen in einer oder mehreren der Ressourcen AWS-Regionen in Ihrem Konto nicht mehr unterstützen möchten, führen Sie die Schritte im folgenden Verfahren aus.

> **Note**
>
> Wenn es sich bei dem Index, den Sie löschen, um den Aggregatorindex für handelt AWS-Konto, müssen Sie 24 Stunden warten, bevor Sie einen anderen lokalen Index zum Aggregatorindex für das Konto heraufstufen können. Benutzer können mit Resource Explorer keine kontoweiten Suchen durchführen, bis ein anderer Aggregatorindex konfiguriert ist.

AWS Management Console

Um den Resource Explorer-Index in einem zu löschen AWS-Region

1. Öffnen Sie die Seite mit den Resource Explorer-Einstellungen.
2. Aktivieren Sie im Abschnitt Indizes die Kontrollkästchen neben den Indizes, die AWS-Regionen Sie löschen möchten, und wählen Sie dann Löschen aus.
3. Stellen Sie auf der Seite Indizes löschen sicher, dass Sie nur Indizes ausgewählt haben, die Sie löschen möchten. Geben Sie **`delete`** in das Textfeld Bestätigen etwas ein, und wählen Sie dann Indizes löschen aus.

   Resource Explorer zeigt oben auf der Seite ein grünes Banner an, um den Erfolg anzuzeigen, oder ein rotes Banner, wenn in einer oder mehreren der ausgewählten Regionen ein Fehler auftritt.

AWS CLI

Um den Resource Explorer-Index in einem zu löschen AWS-Region

Wenn Sie die Suche nach Ressourcen in einer oder mehreren der Ressourcen AWS-Regionen in Ihrem Konto nicht mehr unterstützen möchten, führen Sie die folgenden Befehle aus.

Führen Sie den folgenden Befehl für jede Region mit den Indizes aus, die Sie löschen möchten. Sie müssen den Befehl in der Region mit dem Index ausführen, den Sie löschen möchten. Der folgende Beispielbefehl löscht den Resource Explorer-Index in den USA West (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"
}
```

Da Resource Explorer einen Teil der Löscharbeiten als asynchrone Aufgaben im Hintergrund ausführt, könnte die Antwort darauf hindeuten, dass es sich um einen Vorgang handelt. `DELETING` Dieser Status weist darauf hin, dass die Hintergrundprozesse noch nicht abgeschlossen sind. Sie können überprüfen, ob der Vorgang endgültig abgeschlossen ist, indem Sie den folgenden Befehl ausführen und prüfen, ob der `State` Befehl geändert `DELETED` werden soll.

```
$ 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"
}
```

Resource Explorer insgesamt ausschalten AWS-Regionen

Wenn Sie ihn AWS Ressourcen Explorer vollständig ausschalten möchten, gehen Sie wie folgt vor.

> **Note**
>
> Resource Explorer erstellt eine dienstverknüpfte Rolle mit dem Namen AWSServiceRoleForResourceExplorer des Kontos, wenn Sie im ersten Abschnitt einen Index AWS-Region für ein Konto erstellen. Resource Explorer löscht diese dienstverknüpfte Rolle nicht automatisch. Nachdem Sie den Resource Explorer-Index in jeder Region gelöscht haben, können Sie die IAM Konsole verwenden, um die Rolle zu löschen, wenn Sie sicher sind, dass Sie Resource Explorer in future nicht mehr verwenden werden. Wenn Sie die Rolle

löschen und anschließend Resource Explorer in mindestens einer Rolle starten möchten AWS-Region, erstellt Resource Explorer die mit dem Dienst verknüpfte Rolle neu.

Sie können den Resource Explorer mithilfe von AWS Management Console, mithilfe von Befehlen in AWS Command Line Interface (AWS CLI) oder mithilfe von API Operationen in einem deaktivieren. AWS SDK

AWS Management Console

Wenn Sie die Suche nach Ressourcen AWS-Region in Ihrem System nicht mehr unterstützen möchten AWS-Konto, führen Sie die Schritte im folgenden Verfahren aus.

Um den Resource Explorer für alle auszuschalten AWS-Regionen

1. Öffnen Sie die Seite mit den Resource Explorer-Einstellungen.
2. Aktivieren Sie im Abschnitt Indizes die Kontrollkästchen neben „Alle registrierten AWS-Regionen“ und wählen Sie dann „Löschen“.

   > **Tip**
   >
   > Sie können das Kästchen in der Tabellenkopfzeile neben Index aktivieren, um die Kästchen für alle Regionen in einem einzigen Schritt zu aktivieren.

3. Vergewissern Sie sich auf der Seite Indizes löschen, dass Sie alle Indizes löschen möchten. Geben Sie **`delete`** in das Textfeld Bestätigen einen Text ein und wählen Sie dann Indizes löschen aus.

   Resource Explorer zeigt oben auf der Seite ein grünes Banner an, um den Erfolg anzuzeigen, oder ein rotes Banner, wenn in einer oder mehreren der ausgewählten Regionen ein Fehler auftritt.

AWS CLI

Um den Resource Explorer für alle auszuschalten AWS-Regionen

Wenn Sie die Suche nach Ressourcen AWS-Regionen in allen Bereichen Ihres Kontos nicht mehr unterstützen möchten, führen Sie den folgenden Befehl aus, um alle Indizes in allen Indizes zu finden, AWS-Region in denen Sie zuvor den Ressourcen-Explorer aktiviert haben. ARN

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

Führen Sie für jede Antwort den folgenden Befehl aus, um den Resource Explorer-Index in dieser Region zu löschen.

```
$ 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"
}
```

Wiederholen Sie den vorherigen Befehl in jeder weiteren Region.

Da Resource Explorer einen Teil der Bereinigung als asynchrone Aufgaben im Hintergrund ausführt, könnte die Antwort darauf hindeuten, dass es sich um einen Vorgang handelt. `DELETING` Dieser Status weist darauf hin, dass die Hintergrundprozesse noch nicht abgeschlossen sind. Sie können den endgültigen Abschluss überprüfen, indem Sie den folgenden Befehl ausführen und prüfen, ob der Status geändert `DELETED` werden soll.

```
$ 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"
```

```
}
```

Resource Explorer-Ansichten verwalten, um Zugriff auf die Suche zu gewähren

Ansichten sind der Schlüssel zur Suche nach Ihren Ressourcen. Jeder AWS Ressourcen Explorer Suchvorgang muss eine Ansicht verwenden. Ansichten sind die Methode, mit der der Administrator den Zugriff auf die Informationen über Ressourcen in Ihrem steuern kann AWS-Konto.

Auf eine Ansicht können nur Prinzipale (IAMRollen oder Benutzer) zugreifen, die berechtigt sind, diese Ansicht zu verwenden. Um mit Resource Explorer erfolgreich zu suchen, muss ein Principal `Allow` Zugriff auf die `resource-explorer-2:Search` Operationen `resource-explorer-2:GetView` und in den Ansichten haben. ARN

Ansichten enthalten integrierte Filter, mit denen der Administrator die Ergebnisse auf interessante Elemente beschränken kann. Sie können beispielsweise eine Ansicht erstellen, die nur Ressourcen enthält, die sich auf ein bestimmtes Projekt beziehen. Benutzer, die keine Informationen zu anderen Projekten benötigen, können diese Ansicht verwenden, um nur die Ressourcen zu sehen, die für sie von Interesse sind.

Eine Ansicht ist eine regionale Ressource. Die Ansicht wird in einer bestimmten Region erstellt und gespeichert AWS-Region und gibt in ihren Ergebnissen nur Informationen aus dem Index in dieser Region zurück. Um Ergebnisse aus allen Regionen des Kontos einzubeziehen, muss sich die Ansicht in der Region befinden, die den Aggregatorindex enthält. Diese Region enthält ein Replikat der Indizes aus allen anderen Regionen im Konto.

Jede Ansicht besteht aus mehreren Schlüsselelementen:

Berechtigungen für die Suche

Mithilfe von AWS Standardberechtigungsrichtlinien können Sie steuern, wer die einzelnen Ansichten verwenden kann. Dies wird durch identitätsbasierte Berechtigungsrichtlinien gewährleistet, die den Prinzipalen zugeordnet sind und Ihnen eine genaue Kontrolle darüber geben, wer die in den einzelnen Ansichten bereitgestellten Informationen sehen kann. Sie können beispielsweise Zugriff auf die `Production-resources` Ansicht gewähren, sodass nur die Techniker suchen können, die für Ihre Produktionsdienste zuständig sind. Anschließend können Sie verschiedene Berechtigungen für die `Pre-production-resources` Ansicht gewähren, sodass Ihre Entwickler nach Ressourcen aus der Vorproduktion suchen können.

Wenn Sie die AWS verwaltete Richtlinie verwenden, die `AWSResourceExplorerReadOnlyAccess` zusammen mit Ihren Hauptbenutzern benannt ist, erhalten diese die Möglichkeit, mithilfe einer beliebigen Ansicht im Konto zu suchen.

Alternativ können Sie Ihre eigene Berechtigungsrichtlinie erstellen und die folgenden Berechtigungen nur für bestimmte Ansichten gewähren:

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

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.

- Benutzer, IAM die über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verband) im IAMBenutzerhandbuch.

- IAMBenutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Eine Rolle für einen IAM Benutzer erstellen im IAMBenutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Folgen Sie den Anweisungen unter Hinzufügen von Berechtigungen für einen Benutzer (Konsole) im IAMBenutzerhandbuch.

Weitere Informationen zu Berechtigungen im Zusammenhang mit Ansichten finden Sie unterZugriff auf Resource Explorer-Ansichten für die Suche gewähren.

Die Suche filtern

Eine Ansicht dient als virtuelles Fenster, durch das der Benutzer die Ressourcen im Konto sehen kann. Sie können mehrere Ansichten erstellen, von denen jede eine andere Ansicht des Gesamtbilds bietet. Sie können beispielsweise eine Ansicht erstellen, in der nur nach Ressourcen gesucht werden kann, die mit Ihrer Vorproduktionsumgebung verknüpft sind und anhand von Tags identifiziert wurden, die Ihren Ressourcen zugeordnet sind. Dann könnten Sie eine separate Ansicht erstellen, mit der Sie nur nach Ressourcen in Ihrer Produktionsumgebung suchen können, und zwar auf der Grundlage verschiedener Werte in den Tags. Wenn Sie mehrere Ansichten mit

unterschiedlichen `FilterString` Werten konfigurieren, müssen Sie diese Abfrageparameter nicht bei jeder Suche erneut eingeben.

In Ansichten können Sie auch angeben, welche optionalen Informationen zu den Ressourcen in die Ergebnisse aufgenommen werden sollen. Die Standardliste der Felder ist immer in den Ergebnissen enthalten. Zusätzlich zur Standardliste können Sie festlegen, dass die Ansicht auch alle mit der Ressource verknüpften Tags .

Umfang der Suche

- Regionsbereich — Wenn Sie in einem AWS-Region mit dem Resource Explorer suchen, können die Ergebnisse nur Ressourcen enthalten, die in dieser Region indexiert sind. In den meisten Regionen ist der Index beschriftet`LOCAL`, weil er nur Informationen über Ressourcen innerhalb dieser Region enthält. Bei Suchanfragen in diesen Regionen können nur diese Ressourcen zurückgegeben werden.
- Kontobereich — Sie können einen lokalen Index zum Aggregatorindex für das Konto heraufstufen. Wenn Sie dies tun, replizieren alle anderen Regionen, in denen Resource Explorer aktiviert ist, ihre Indexinformationen in die Region mit dem Aggregatorindex. Wenn Sie in dieser Region suchen, enthalten diese Ergebnisse Ressourcen aus allen Regionen des Kontos. Wenn Sie die Option Quick Setup verwenden, um den Server zu konfigurieren, erstellt Resource Explorer automatisch einen Aggregatorindex in der von Ihnen angegebenen Region. Außerdem erstellt die Option Quick Setup eine Standardansicht in dieser Region, um die Suche nach allen Ressourcen im Konto in allen Regionen zu unterstützen.

Standardansichten

Wenn ein Benutzer versucht zu suchen, ohne explizit eine Ansicht anzugeben, verwendet Resource Explorer die dafür definierte Standardansicht AWS-Region.

Wenn für diese Region keine Standardansicht existiert und der Benutzer keine zu verwendende Ansicht angegeben hat, schlägt die Suche fehl und generiert eine Ausnahme.

Resource Explorer erstellt automatisch eine Standardansicht wie folgt:

- Wenn Sie den Resource Explorer mit dem aktivieren AWS Management Console und die Option Quick Setup wählen, müssen Sie angeben, welche Region den Aggregatorindex für das Konto enthält. Resource Explorer erstellt automatisch eine Standardansicht in der angegebenen Aggregatorindex-Region.

- Wenn Sie Resource Explorer mit dem registrieren AWS Management Console und die Option Erweiterte Konfiguration wählen, können Sie optional den Aggregatorindex für das Konto in einer bestimmten Region erstellen. Wenn Sie dies tun, erstellt Resource Explorer automatisch eine Standardansicht in der Aggregator-Index-Region.
- Wenn Sie Resource Explorer mithilfe der Konsole registrieren und sich dafür entscheiden, keine Aggregator-Index-Region zu registrieren, erstellt Resource Explorer eine Standardansicht für den lokalen Index in jeder Region.
- Wenn Sie Resource Explorer mithilfe der API Operationen AWS CLI oder registrieren, erstellt Resource Explorer nicht automatisch eine Standardansicht. Stattdessen müssen Sie die Standardansicht für jede Region, von der aus Sie erwarten, dass Benutzer suchen, manuell konfigurieren.

Resource Explorer-Ansichten für die Suche erstellen

Bei allen Suchen muss eine Ansicht verwendet werden. Eine Ansicht definiert Filter, die bestimmen, welche Ressourcen von Abfragen zurückgegeben werden können, die die Ansicht verwenden. Ansichten steuern auch, wer nach Ressourcen suchen kann.

Eine Ansicht wird in einem AWS-Region gespeichert und gibt nur Suchergebnisse aus dem Index dieser Region zurück. Wenn die Region den Aggregatorindex enthält, gibt die Ansicht Suchergebnisse aus dem Index in jeder Region im Konto zurück.

Mithilfe von Ansichten für mehrere Konten können Sie in Konten in Ihrer gesamten Organisation nach Ressourcen suchen. Für jedes Konto, das Sie durchsuchen möchten, sind Indizes erforderlich. Nur das Verwaltungskonto oder ein delegierter Administrator für die Organisation kann eine Ansicht mit mehreren Konten erstellen.

AWS Ressourcen Explorer kann bei der Ersteinrichtung eine Standardansicht für Sie erstellen, wenn Sie die entsprechenden Optionen entweder in der Schnellinstallation für Resource Explorer in der Systems Manager Manager-Konsole oder in der erweiterten Konfiguration ausgewählt haben. Zu einem späteren Zeitpunkt können Sie zusätzliche Ansichten mit unterschiedlichen Filtern für unterschiedliche Benutzergruppen erstellen.

Sie können eine Ansicht mithilfe von AWS Management Console oder erstellen, indem Sie AWS CLI Befehle oder entsprechende API Operationen in einem ausführen AWS SDK.

Mindestberechtigungen

Um dieses Verfahren ausführen zu können, benötigen Sie die folgenden Berechtigungen:

- Aktion: `resource-explorer-2:CreateView`

  Ressource: Dies kann `*` die Erstellung einer Ansicht in einem beliebigen Bereich AWS-Region des Kontos ermöglichen.

AWS Management Console

Um eine Ansicht zu erstellen

1. Öffnen Sie die Seite „Ansichten“ der Resource Explorer-Konsole und wählen Sie Ansicht erstellen.
2. Geben Sie auf der Seite Ansicht erstellen unter Name einen Namen für die Ansicht ein.

   Der Name darf nicht mehr als 64 Zeichen lang sein und kann Buchstaben, Zahlen und den Bindestrich (-) enthalten. Der Name muss innerhalb seines AWS-Region Namens eindeutig sein.
3. Wählen Sie die Ansicht aus, AWS-Region in der Sie die Ansicht erstellen möchten. Um eine Ansicht zu erstellen, die Ressourcen aus allen Regionen des Kontos zurückgibt, wählen Sie die Ansicht aus, AWS-Region die den Aggregatorindex enthält.
4. (Optional) Wählen Sie unter Umfang aus, ob Ihre Suche Ressourcen mit mehreren Konten oder nur Ressourcen aus Ihrem Konto zurückgibt. Der Bereich auf Kontoebene ist die Standardeinstellung.

   Nur das Verwaltungskonto oder der delegierte Administrator kann die Option zum Erstellen einer Ansicht mit mehreren Konten sehen.
5. Wählen Sie aus, ob die Ergebnisse gefiltert werden sollen.

   - Alle Ressourcen einbeziehen

     Es sind keine Abfragefilter enthalten. Alle Ressourcen im Index, die der Ansicht zugeordnet sind, können in Suchergebnissen zurückgegeben werden.
   - Schließt nur Ressourcen ein, die einem bestimmten Filter entsprechen

     Aktiviert das Kontrollkästchen Ressourcenfilter, in dem Sie Filternamen und Operatoren auswählen können. Eine Erläuterung der einzelnen verfügbaren Filternamen und Operatoren finden Sie unterFilter.
   - Wählen Sie die optionalen Ressourcenattribute aus, die in die Ergebnisse dieser Ansicht aufgenommen werden sollen. Aktivieren Sie das Kontrollkästchen neben Tags, damit

Benutzer anhand ihrer Tag-Schlüsselnamen und -werte nach Ressourcen suchen können. Wenn Sie keine Tags in die Ansicht aufnehmen, können Benutzer keine Suchanfragen stellen, bei denen Tagschlüssel und -werte verwendet werden, um die Ergebnisse weiter zu filtern.

- Optional können Sie der Ansicht Tags hinzufügen. Erweitern Sie das Feld Tags und geben Sie bis zu 50 Tag-Schlüssel/Wert-Paare ein. Sie können Tags zur Kategorisierung von Ressourcen oder als Teil einer auf Attributen basierenden Sicherheitsberechtigungsstrategie für die Zugriffskontrolle () verwenden. ABAC Weitere Informationen finden Sie unter Hinzufügen von Markern zu Ansichten zu Ansichten hinzu.
- Wählen Sie Ansicht erstellen.

Die Konsole kehrt zur Suchseite zurück, auf der Sie Ihre neue Ansicht verwenden können, um eine Suche durchzuführen.

Nächster Schritt: Erteilen Sie den Hauptbenutzern in Ihrem Konto die Berechtigungen, mit Ihrer neuen Ansicht zu suchen. Weitere Informationen finden Sie unter Zugriff auf Resource Explorer-Ansichten für die Suche gewähren

AWS CLI

Um eine Ansicht zu erstellen

Führen Sie den folgenden Befehl aus, um eine Ansicht in der angegebenen Ansicht zu erstellen AWS-Region. Das folgende Beispiel erstellt eine Ansicht, die nur Ressourcen zurückgibt, die sich auf den EC2 Amazon-Service beziehen und mit einem `Stage` Schlüssel und dem Wert gekennzeichnet sind`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"
    }
}
```

Um eine Ansicht auf Organisationsebene zu erstellen

Im folgenden Beispiel wird eine Ansicht erstellt, in der Ressourcen aus Ihrer gesamten Organisation angezeigt werden. Dies muss über das Verwaltungskonto der Organisation oder über ein delegiertes Administratorkonto ausgeführt werden.

1. Führen Sie den `aws organizations describe-organization` Befehl aus, um Ihre Organisation ARN abzurufen.
2. Führen Sie den folgenden Befehl aus, um eine Ansicht für die angegebene Organisation zu erstellen.

```
$ 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"
    }
}
```

Um eine Ansicht auf der Ebene einer Organisationseinheit zu erstellen

Im folgenden Beispiel wird eine Ansicht erstellt, die Ressourcen von allen Mitgliedern dieser Organisationseinheit zurückgibt. Diese Ansicht verhält sich ähnlich wie eine Ansicht auf Organisationsebene. Dies muss über das Verwaltungskonto der Organisation oder ein delegiertes Administratorkonto ausgeführt werden.

1. Führen Sie den `aws organizations describe-organizational-unit` Befehl aus, um Ihre Organisation ARN abzurufen.
2. Führen Sie den folgenden Befehl aus, um eine Ansicht für die angegebene Organisationseinheit zu erstellen.

```
$ 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"
    }
}
```

Nächster Schritt: Erteilen Sie den Hauptbenutzern in Ihrem Konto die Berechtigungen, mit Ihrer neuen Ansicht zu suchen. Weitere Informationen finden Sie unter Zugriff auf Resource Explorer-Ansichten für die Suche gewähren

Zugriff auf Resource Explorer-Ansichten für die Suche gewähren

Bevor Benutzer mit einer neuen AnsichtAWS Ressourcen Explorer Verwenden Sie dazu eine identitätsbasierte Berechtigungsrichtlinie für dieAWS Identity and Access Management (IAM) - Prinzipale, die mit der Ansicht suchen müssen.

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center-Benutzerhandbuch.
- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Sie haben die Wahl zwischen den folgenden Methoden:

- Verwenden Sie eine bestehendeAWS verwaltete Richtlinie. Resource Explorer bietet mehrere vordefinierteAWS verwaltete Richtlinien für Ihre Verwendung. Einzelheiten zu allen verfügbarenAWS verwalteten Richtlinien finden Sie unterAWS verwaltete Richtlinien für AWS Ressourcen Explorer.

  Sie könnten die`AWSResourceExplorerReadOnlyAccess` Richtlinie beispielsweise verwenden, um Suchberechtigungen für alle Ansichten im Konto zu gewähren.
- Erstellen Sie Ihre eigene Berechtigungsrichtlinie und weisen Sie sie den Schulleitern zu. Wenn Sie Ihre eigene Richtlinie erstellen, können Sie den Zugriff auf eine einzelne Ansicht oder eine Teilmenge der verfügbaren Ansichten einschränken, indem Sie den Amazon-Ressourcennamen (ARN) jeder Ansicht im`Resource` Element der Richtlinienerklärung angeben. Sie können

beispielsweise die folgende Beispielrichtlinie verwenden, um diesem Principal die Möglichkeit zu geben, nur mit dieser einen Ansicht zu suchen.

```
{
    "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
        }
    ]
}
```

Verwenden Sie die IAM-Konsole, um die Berechtigungsrichtlinien zu erstellen und sie mit den Prinzipalen zu verwenden, die diese Berechtigungen benötigen. Weitere Informationen zu IAM-Berechtigungsrichtlinien finden Sie in den folgenden Themen:

- Richtlinien und Berechtigungen in IAM
- Hinzufügen und Entfernen von IAM-Identitätsberechtigungen
- Grundlegendes zu Richtlinien

Mit Tag-basierter Autorisierung

Wenn Sie mehrere Ansichten mit Filtern erstellen möchten, die nur Ergebnisse mit bestimmten Ressourcen zurückgeben, möchten Sie möglicherweise auch den Zugriff auf diese Ansichten auf die Hauptbenutzer beschränken, die diese Ressourcen sehen müssen. Sie können diese Art von Sicherheit für die Ansichten in Ihrem Konto bereitstellen, indem Sie eine Strategie zur attributbasierten Zugriffskontrolle (ABAC) verwenden. Die von ABAC verwendeten Attribute sind die Tags, die sowohl den Principalen, die versuchen, Operationen auszuführen, als auch den Ressourcen, auf die sie zugreifen möchten, zugeordnet sind.AWS

ABAC verwendet standardmäßige IAM-Berechtigungsrichtlinien, die den Principals beigefügt sind. Die Richtlinien verwenden`Condition` Elemente in den Richtlinienerklärungen, um den Zugriff nur

dann zu ermöglichen, wenn sowohl die an den anfragenden Principal angehängten Tags als auch die an die betroffene Ressource angehängten Tags den Anforderungen der Richtlinie entsprechen.

Sie könnten beispielsweise allenAWS Ressourcen, die die Produktionsanwendung Ihres Unternehmens unterstützen, ein Tag`"Environment" = "Production"` zuordnen. Um sicherzustellen, dass nur Prinzipale, die für den Zugriff auf die Produktionsumgebung autorisiert sind, diese Ressourcen sehen können, erstellen Sie eine Resource Explorer-Ansicht, die dieses Tag als Filter verwendet. Um dann den Zugriff auf die Ansicht nur auf die entsprechenden Prinzipale zu beschränken, gewähren Sie Berechtigungen mithilfe einer Richtlinie, die eine ähnliche Bedingung wie die folgenden Beispielelemente hat.

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

`Condition`Im vorherigen Beispiel wird festgelegt, dass die Anforderung nur zulässig ist, wenn das`Environment` Tag, das an den die Anfrage stellenden Principal angehängt ist, mit dem`Environment` Tag übereinstimmt, das an die in der Anfrage angegebene Ressource angehängt ist. Wenn diese beiden Tags nicht genau übereinstimmen oder wenn eines der Tags fehlt, lehnt der Resource Explorer die Anfrage ab.

> **Important**
>
> Um ABAC erfolgreich für den sicheren Zugriff auf Ihre Ressourcen zu verwenden, müssen Sie den Zugriff zunächst auf die Möglichkeit beschränken, die an Ihre Prinzipale und Ressourcen angehängten Tags hinzuzufügen oder zu ändern. Wenn ein Benutzer die mit einemAWS Principal oder einer Ressource verknüpften Tags hinzufügen oder ändern kann, kann dieser Benutzer die durch diese Tags gesteuerten Berechtigungen beeinflussen.
> In einer sicheren ABAC-Umgebung sind nur zugelassene Sicherheitsadministratoren berechtigt, die an Prinzipale angehängten Tags hinzuzufügen oder zu ändern, und nur Sicherheitsadministratoren und Ressourcenbesitzer können die an Ressourcen angehängten Tags hinzufügen oder ändern.

Weitere Informationen über die erfolgreiche Implementierung einer ABAC-Strategie finden Sie in den folgenden Themen im IAM-Benutzerhandbuch:

- IAM-Tutorial: Definieren von BerechtigungenAWS
- Steuern SteuerungAWS von Tags

Nachdem Sie die erforderliche ABAC-Infrastruktur eingerichtet haben, können Sie mit start using tags festlegen, wer mithilfe der Resource Explorer-Ansichten in Ihrem Konto suchen darf. Ein Beispiel für das Prinzip von Berechtigungen finden Sie in den folgenden Beispielberechtigungsrichtlinien:

- Gewähren des Zugriffs auf eine Ansicht anhand von Stichwörtern
- Zugriff gewähren, um eine Ansicht auf der Grundlage von Tags zu erstellen

Festlegen einer Standardansicht in einemAWS-Region

InAWS Ressourcen Explorer, Sie können viele Ansichten in einer definierenAWS-Region, wobei jede Ansicht unterschiedliche Suchanforderungen erfüllt. Wir empfehlen, in jeder Region eine Ansicht als Standardansicht für diese Region festzulegen.

Resource Explorer verwendet die Standardansicht, wenn ein Benutzer eine Suche durchführt, und gibt nicht explizit an, welche Ansicht verwendet werden soll. Die einheitliche Suchleiste oben auf jederAWS Management Console Seite verwendet außerdem automatisch die Standardansicht in der Region, die den Aggregatorindex enthält, um Ressourcen zu finden, die der Suchanfrage des Benutzers entsprechen.

Sie können nur eine Ansicht, die in der Region vorhanden ist, als Standardansicht für diese Region auswählen. Wenn eine andere Region über eine Ansicht verfügt, die Sie verwenden möchten, müssen Sie zunächst eine Kopie dieser Ansicht in der Region erstellen, in der Sie sie zur Standardansicht machen möchten.

> **Tip**
>
> Es gibt keinen Vorgang zum Kopieren der Ansicht. Sie müssen eine Ansicht in der Zielregion erstellen und dann die Einstellungen von der vorhandenen Ansicht in die neue Ansicht kopieren.

Sie können eine Ansicht als Standard für ihre Region angeben, indem Sie dieAWS Management ConsoleAWS CLI Befehle oder die entsprechenden API-Operationen in einemAWS SDK ausführen.

AWS Management Console

Legen Sie eine Standardansicht fest wie folgt

1. Wählen Sie auf der Seite „Resource Explorer-Ansichten“ die Optionsschaltfläche neben der Ansicht aus, die Sie als Standard für ihre Region festlegen möchten.
2. Wählen Sie „Aktionen“ und dann „Als Standard festlegen“.

AWS CLI

Legen Sie eine Standardansicht fest wie folgt

Führen Sie den folgenden Befehl aus, um die angegebene Ansicht als Standard für ihre Region festzulegen. Im folgenden Beispiel wird die angegebene Ansicht als Standard für alle in der Region us-east-1 durchgeführten Suchen festgelegt. Diese Ansicht muss in der Region vorhanden sein, in der Sie den Befehl ausführen.

```
$ 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"
}
```

Hinzufügen von Markern zu Ansichten zu Ansichten hinzu

Sie können Markern zu Ihren Ansichten hinzufügen, um zu kategorisieren. Tags sind vom Kunden bereitgestellte Metadaten, die die Form einer Schlüsselnamenzeichenfolge und einer zugehörigen optionalen Wertzeichenfolge haben. Allgemeine Informationen zum Taggen vonAWS Ressourcen finden Sie unter Taggen vonAWS Ressourcen in der Allgemeine Amazon Web Services-Referenz.

Hinzufügen von Markern zu Ihren Ansichten hinzu

Sie können Ihren Resource Explorer-Ansichten Tags hinzufügen, indem Sie dieAWS Management Console oder verwenden, indem SieAWS CLI Befehle oder entsprechende API-Operationen in einemAWS SDK ausführen.

AWS Management Console

Hinzufügen von Markern zu einer Ansicht Markern hinzu hinzu hinzu hinzu

1. Öffnen Sie die Seite mit den Ansichten des Resource Explorers und wählen Sie den Namen der Ansicht aus, die Sie taggen möchten, um die Detailseite anzuzeigen.
2. Wählen Sie unter Tags die Option Manage tags (Tags verwalten) aus.
3. Um ein Tag hinzuzufügen, wählen Sie, um ein Tag hinzuzufügen, und geben Sie dann einen Tag-Schlüsselnamen und einen optionalen Wert ein.

   > **Note**
   >
   > Sie können ein Tag auch löschen, indem Sie das X neben dem Tag auswählen.

   Sie können einer Ressource bis zu 50 benutzerdefinierte Tags anfügen. Alle Tags, die automatisch von erstellt und verwaltet werden, werdenAWS nicht auf dieses Kontingent angerechnet.
4. Wenn Sie mit allen Tag-Änderungen fertig sind, wählen Sie Änderungen speichern.

AWS CLI

Hinzufügen von Markern zu einer Ansicht Markern hinzu hinzu hinzu hinzu

Führen Sie den folgenden Befehl aus, um einer Ansicht Markern hinzuzufügen. Im folgenden Beispiel werden der angegebenen Ansicht Tags mit dem Schlüsselnamen`environment` und`production` dem Wert hinzugefügt.

```
$ 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
```

Der vorherige Befehl erzeugt keine Ausgabe, wenn er erfolgreich ist.

> **Note**
>
> Verwenden Sie den`untag-resource` Befehl, um ein vorhandenes Tag aus einer Ansicht zu entfernen.

Steuern von Berechtigungen mit Tags

Eine wichtige Anwendung von Markern ist die -Unterstützung für Attribute-Based Access Control (ABAC, attributbasierte Zugriffssteuerung). ABAC kann Ihnen dabei helfen, die Rechteverwaltung zu vereinfachen, indem Sie Ressourcen taggen können. Anschließend erteilen Sie Benutzern die Berechtigung für Ressourcen, die auf eine bestimmte Art gekennzeichnet sind.

Betrachten Sie beispielsweise folgendes Szenario. Für eine aufgerufene`ViewA` Ansicht hängst du das Tag an`environment=prod` (Schlüsselname=Wert). Ein andererViewB könnte markiert sein`environment=beta`. Sie kennzeichnen Ihre Rollen und Benutzer mit denselben Tags und Werten, je nachdem, auf welche Umgebung jede Rolle oder jeder Benutzer zugreifen können soll.

Anschließend könnten Sie Ihren IAM-Rollen, -Gruppen und -Benutzern eineAWS Identity and Access Management (IAM-) Berechtigungsrichtlinie zuweisen. Die Richtlinie gewährt nur dann die Berechtigung, auf eine Ansicht zuzugreifen und sie zu durchsuchen, wenn die Rolle oder der Benutzer, der die Suchanfrage stellt, über ein`environment` Tag mit demselben Wert wie das`environment` Tag verfügt, das an die Ansicht angehängt ist.

Der Vorteil dieses Ansatzes besteht darin, dass er dynamisch ist und Sie keine Liste darüber führen müssen, wer Zugriff auf welche Ressourcen hat. Stattdessen stellen Sie sicher, dass alle Ressourcen (Ihre Ansichten) und Principals (IAM-Rollen und Benutzer) ordnungsgemäß gekennzeichnet sind. Anschließend werden die Berechtigungen automatisch aktualisiert, ohne dass Sie die Richtlinien ändern müssen.

Verweisen auf Stichwörter in einer ABAC-Richtlinie

Nachdem Ihre Ansichten mit Tags versehen wurden, können Sie diese Tags verwenden, um den Zugriff auf diese Ansichten dynamisch zu steuern. Die folgende Beispielrichtlinie geht davon aus, dass sowohl Ihre IAM-Prinzipale als auch Ihre Views mit dem Tag-Schlüssel`environment` und einem bestimmten Wert gekennzeichnet sind. Wenn das erledigt ist, können Sie die folgende

Beispielrichtlinie Ihren Principals anfügen hinzu. Ihre Rollen und Benutzer können dann alle Ansichten`Search` verwenden, die mit einem`environment` Tag-Wert gekennzeichnet sind, der exakt dem`environment` Tag entspricht, der dem Principal zugeordnet ist.

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

Wenn sowohl der Principal als auch die Ansicht das`environment` Tag haben, die Werte jedoch nicht übereinstimmen, oder wenn bei einem der beiden das`environment` Tag fehlt, lehnt Resource Explorer die Suchanfrage ab.

Weitere Informationen zur Verwendung von ABAC zur sicheren Gewährung des Zugriffs auf Ihre Ressourcen finden Sie unter Wofür ist ABACAWS?

Resource Explorer-Ansichten teilen

Ansichten in verwenden AWS Ressourcen Explorer hauptsächlich ressourcenbasierte Richtlinien, um Zugriff zu gewähren. Ähnlich wie die Amazon S3 S3-Bucket-Richtlinien sind diese Richtlinien an die Ansicht angehängt und geben an, wer die Ansicht verwenden kann. Dies steht im Gegensatz zu AWS Identity and Access Management (IAM) identitätsbasierten Richtlinien. Eine IAM identitätsbasierte Richtlinie wird einer Rolle, Gruppe oder einem Benutzer zugewiesen und legt fest, auf welche Aktionen und Ressourcen diese Rolle, Gruppe oder dieser Benutzer zugreifen kann. Sie können beide Richtlinientypen mit Resource Explorer-Ansichten wie folgt verwenden:

- Verwenden Sie innerhalb des Verwaltungskontos oder des delegierten Administratorkontos, dem die Ressource gehört, einen der beiden Richtlinientypen, um Zugriff zu gewähren, vorausgesetzt, dass keine andere Richtlinie diesem Prinzipal ausdrücklich den Zugriff auf die Ansicht verweigert.
- Für alle Konten müssen Sie beide Richtlinientypen verwenden. Die ressourcenbasierte Richtlinie, die der Ansicht im Sharing-Konto beigefügt ist, aktiviert das Teilen mit einem anderen Nutzerkonto. Diese Richtlinie gewährt jedoch keinen Zugriff auf einzelne Benutzer oder Rollen im Nutzerkonto. Der Administrator des Benutzerkontos muss den gewünschten Rollen und Benutzern des Benutzerkontos außerdem eine identitätsbasierte Richtlinie zuweisen. Diese Richtlinie gewährt Zugriff auf den Amazon-Ressourcennamen (ARN) der Ansicht.

Um Ansichten mit anderen Konten zu teilen, müssen Sie AWS Resource Access Manager (AWS RAM) verwenden. AWS RAM kümmert sich für Sie um die Komplexität ressourcenbasierter Richtlinien. Bevor Sie Inhalte teilen können, müssen Sie die folgenden Aufgaben ausführen:

- Aktivieren Sie die Suche mit mehreren Konten.
- Stellen Sie sicher, dass Ihre ressourcenbasierte Richtlinie oder die IAM identitätsbasierte Richtlinie, die Sie zum Teilen und Aufheben der Freigabe von Ansichten verwenden, die Berechtigungen und enthält. `resource-explorer-2:GetResourcePolicy` `resource-explorer-2:PutResourcePolicy` `resource-explorer-2:DeleteResourcePolicy`

Um eine Ansicht teilen zu können, müssen Sie das Verwaltungskonto der Organisation oder ein delegierter Administrator sein. Sie geben die Konten oder Identitäten an, mit denen Sie die Ressource gemeinsam nutzen möchten. AWS RAM unterstützt Resource Explorer-Ansichten vollständig. AWS RAM verwendet Richtlinien, die den in den folgenden Abschnitten beschriebenen ähneln und auf den Typen der Prinzipale basieren, für die Sie die gemeinsame Nutzung auswählen. Anweisungen zur gemeinsamen Nutzung von Ressourcen finden Sie im AWS Resource Access Manager Benutzerhandbuch unter AWS Ressourcen teilen.

Administratoren und delegierte Administratoren können drei Arten von Ansichten erstellen und gemeinsam nutzen: Ansicht des Organisationsumfangs, Bereichsansichten der Organisationseinheit (OU) und Bereichsansichten auf Kontoebene. Sie können Daten mit Organisationen oder Konten teilen. OUs Wenn Konten der Organisation beitreten oder sie verlassen, AWS RAM wird die geteilte Ansicht automatisch gewährt oder widerrufen.

Richtlinie für Berechtigungen, mit denen die Ansicht geteilt werden soll AWS-Konten

Die folgende Beispielrichtlinie zeigt, wie Sie den Prinzipalen eine Ansicht auf zwei verschiedene AWS-Konten Arten zur Verfügung stellen können:

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

Der Administrator für jedes der angegebenen Konten muss nun angeben, welche Rollen und Benutzer auf die Ansicht zugreifen können, indem er identitätsbasierte Berechtigungsrichtlinien an die Rollen, Gruppen und Benutzer anhängt. Die Administratoren der Konten 111122223333 oder 444455556666 können die folgende Beispielrichtlinie erstellen. Anschließend können sie die Richtlinie Rollen, Gruppen und Benutzern in diesen Konten zuweisen, denen erlaubt werden soll, mithilfe der Ansicht zu suchen, die vom ursprünglichen Konto aus geteilt wurde.

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

Sie können diese IAM identitätsbasierten Richtlinien als Teil einer attributebasierten Zugriffskontrolle () Sicherheitsstrategie verwenden. ABAC In diesem Paradigma stellen Sie sicher, dass alle Ihre Ressourcen und alle Ihre Identitäten markiert sind. Anschließend geben Sie in Ihren Richtlinien an, welche Tag-Schlüssel und Werte zwischen der Identität und der Ressource übereinstimmen müssen, damit der Zugriff zulässig ist. Informationen zum Taggen der Aufrufe in Ihrem Konto finden Sie unterHinzufügen von Markern zu Ansichten zu Ansichten hinzu. Weitere Informationen zur attributbasierten Zugriffskontrolle finden Sie unter Wofür? ABAC AWS und Steuern des Zugriffs auf AWS Ressourcen mithilfe von Tags, beide im IAM Benutzerhandbuch.

Löschen von Ansichten im Resource Explorer

Wenn Sie eineAWS Ressourcen Explorer Ansicht nicht mehr benötigen, können Sie sie löschen. Sie können Ansichten löschen, indem Sie dieAWS Management ConsoleAWS CLI Befehle oder die entsprechenden API-Operationen in einemAWS SDK ausführen.

> **Note**
>
> Sie können keine Ansicht löschen, die derzeit als Standardansicht für ihre Ansicht festgelegt istAWS-Region. Um die Ansicht zu löschen, müssen Sie die Ansicht als Standard entfernen. Dazu können Sie den DisassociateDefaultViewAPI-Vorgang in dieser Region ausführen.

Mindestberechtigungen

Um dieses Verfahren auszuführen, müssen Sie über die folgenden Berechtigungen verfügen:

- Aktion: `resource-explorer-2:DeleteView`

  Ressource: Der ARN der zu löschenden Ansicht

AWS Management Console

Um eine Ansicht zu löschen

1. Wählen Sie auf der Seite „Ansichten“ der Resource Explorer-Konsole die Optionsschaltfläche neben der Ansicht, die Sie löschen möchten.
2. Wählen Sie Actions (Aktionen) und anschließend Delete (Löschen).
3. Geben Sie im Bestätigungsdialogfeld den Namen der Ansicht den Namen der Ansicht ein und wählen Sie dann Löschen aus.

AWS CLI

Um eine Ansicht zu löschen

Führen Sie den folgenden Befehl durch, um die Ansicht mit dem angegebenen Amazon-Ressourcennamen (ARN) zu löschen.

```
$ 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"
}
```

VerwendenAWS Ressourcen Explorerum nach Ressourcen zu suchen

Der Hauptzweck der AktivierungAWS Ressourcen Explorerin deinemAWS-Kontodient dazu, Ihren Benutzern die Suche nach Ressourcen im Konto zu ermöglichen. Benutze dieAWS Management Consoleoder derAWS Command Line Interface(AWS CLI), um mit Resource Explorer nach Ressourcen zu suchen.

Im Folgenden sind einige der Hauptmerkmale der Resource Explorer-Suche aufgeführt.

- Jede Suche muss eine Ansicht verwenden.

  Die Ansicht wird von Resource Explorer verwendet, um zu ermitteln, wer berechtigt ist, welche Ressourcen zu sehen. Um eine Ansicht in einem Resource Explorer-Suchvorgang zu verwenden, muss der Benutzer über`Allow`auf der`resource-explorer-2:Search`Operation für die angegebene Ansicht. Diese Erlaubnis stammt von einemidentitätsbasierte Genehmigungsrichtliniedem Schulleiter beigefügt, der die Anfrage stellt.

  Die Ansicht kann einen Filter enthalten, der einschränkt, welche Ressourcen in die Ergebnisse aufgenommen werden können. Indem Sie verschiedene Ansichten erstellen, die Filter verwenden, und indem Sie verschiedenen Prinzipalen Zugriff auf verschiedene Ansichten gewähren, können Sie eine Umgebung konfigurieren, in der jede Benutzergruppe nur die für sie relevanten Ressourcen einsehen kann.

  Weitere Informationen zu Ansichten finden Sie unterResource Explorer-Ansichten verwalten, um Zugriff auf die Suche zu gewähren.
- Resource Explorer verwendet asynchrone Hintergrundprozesse, um seine Indizes zu verwalten.

  Es kann einige Zeit dauern, bis Resource Explorer bei seinen Indexierungsprozessen neu erstellte oder geänderte Ressourcen erkennt und sie dem lokalen Index hinzufügt. Es kann zusätzliche Zeit in Anspruch nehmen, bis Resource Explorer Änderungen in den lokalen Indizes auf den Aggregatorindex repliziert hat.

  Das Gleiche gilt für Ressourcen, die Sie löschen. Nach dem Löschen einer Ressource kann es einige Zeit dauern, bis diese Löschung vom Indexierungsprozess erkannt wird und die Informationen dieser Ressource aus dem lokalen Index entfernt werden. Resource Explorer

benötigt zusätzliche Zeit, um diese Löschung aus dem lokalen Index in den Aggregatorindex des Kontos zu replizieren.

Das Hinzufügen, Ändern und Löschen Ihrer Ressourcen kann bis zu 36 Stunden dauern, bis Resource Explorer diese Änderungen in den Suchergebnissen in allen Regionen anzeigt, in denen Sie den Resource Explorer aktiviert haben.

- Eine Suche im Resource Explorer erfolgt in einemAWS-Region.

  Jede Region, in der Sie den Resource Explorer aktivieren, enthält nur einen Index der in dieser Region gespeicherten Ressourcen. Ansichten sind auch Regionen zugeordnet und können nur die Ressourcen zurückgeben, die im Index dieser Region zu finden sind. Die einzige Ausnahme bildet der Aggregatorindex, der eine replizierte Kopie aller lokalen Indizes erhält, um die Suche in allen Regionen des Kontos zu unterstützen.

- Für die regionsübergreifende Suche ist ein Aggregatorindex für das Konto erforderlich.

  Damit Benutzer überall nach Ressourcen suchen könnenAWS-Regionen, muss der Administrator eine Region benennen, die den Aggregatorindex für das Konto enthält. Eine Kopie jedes lokalen Indexes wird automatisch in den Aggregatorindex repliziert.

  Aus diesem Grund können nur Ansichten im Aggregatorindex Region Ergebnisse zurückgeben, die Ressourcen aus allenAWS-Regionenauf dem Konto.

- Eine Abfrage besteht aus einer beliebigen Anzahl von Freitextschlüsselwörtern und Filtern.

  Freiformschlüsselwörter werden in der Abfrage mithilfe logischer**OR**Betreiber. Filter, die von Resource Explorer definierte Filternamen verwendenwerden in der Abfrage mithilfe von logischen**AND**Betreiber. Betrachten Sie die folgende Beispielabfrage.

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

  Dies wird vom Resource Explorer wie folgt ausgewertet.

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

  Diese Abfrage erfordert, dass es sich bei den passenden Ressourcen um Amazon EC2-Ressourcen in der Region USA West (Oregon) handelt und mindestens eines der Schlüsselwörter enthalten (testen,Instanz) auf irgendeine Weise angehängt, z. B. im Namen, in der Beschreibung oder in den Tags.

> **Note**
>
> Wegen des Impliziten`AND`, können Sie erfolgreich nur einen Filter für ein Attribut verwenden, dem nur ein Wert mit der Ressource verknüpft sein kann. Eine Ressource kann beispielsweise nur Teil einer Ressource seinAWS-Region. Daher gibt die folgende Abfrage keine Ergebnisse zurück.
>
> ```
> region:us-east-1 region:us-west-1
> ```
>
> Diese Einschränkung tutnichtauf die Filter für Attribute anwenden, die mehrere Werte gleichzeitig haben können, wie`tag:`,`tag.key:`, und`tag.value:`.

- Eine Suche kann nur die ersten 1.000 Ergebnisse liefern.

  Diese Anforderung beinhaltet eine Suche mit einer leeren Abfragezeichenfolge, die allen Ressourcen entspricht. Um Ressourcen zu sehen, die über 1.000 liegen, die von einer leeren Abfragezeichenfolge zurückgegeben wurden, müssen Sie Abfragen verwenden, um die passenden Ergebnisse auf die Ergebnisse zu beschränken, die Sie sehen möchten, und die Anzahl der Treffer auf weniger als 1.000 beschränken.

- Es gibt ein Kontingent pro Konto für die Anzahl der Suchvorgänge, die Sie ausführen können.

  Kontingente begrenzen, wie viele Abfragen Sie pro Sekunde stellen können, und wie viele Abfragen Sie jeden Monat stellen können. Spezifische Kontingentzahlen finden Sie unterKontingente für Resource Explorer.

AWS Management Console

So suchen Sie mit Resource Explorer nach Ressourcen

1. Auf derSuche nach RessourcenSeite, wählen Sie zunächst die Ansicht aus, die Sie verwenden möchten. Sie können nur aus den Ansichten wählen, für die Sie über Zugriffsberechtigungen verfügen.
2. FürAnfrage, geben Sie die Suchbegriffe ein undFilterdie die Ressourcen identifizieren, die Sie sehen möchten. Hinweise zu allen verfügbaren Syntaxoptionen finden Sie unterSyntaxreferenz für Suchabfragen für Resource Explorer.
3. DrückenEingebenum Ihre Anfrage einzureichen.

Resource Explorer zeigt alle Ergebnisse an, die sowohl den`Filter`definiert in der Ansicht und derAnfragedie du bereitstellst. Die Ergebnisse sind nach Relevanz sortiert, wobei die Ressourcen, die mehr Ihrer Abfragebegriffe entsprechen, in der Liste weiter oben angezeigt werden, während Ressourcen, die weniger Begriffen entsprechen, weiter unten in der Liste angezeigt werden.

4. Wählen Sie die ID einer Ressource, um zur nativen Konsole dieses Ressourcentyps zu navigieren, wo Sie mit der Ressource auf alle von diesem Dienst unterstützten Arten interagieren können.

AWS CLI

So suchen Sie mit Resource Explorer nach Ressourcen

Führen Sie den folgenden Befehl aus, um mithilfe der angegebenen Ansicht nach Ressourcen zu suchen. Diese Ansicht muss in der Region existieren, in der Sie die Operation durchführen. Im folgenden Beispiel wird nach Amazon EC2-Instances gesucht, die gekennzeichnet sind`env=production`im Osten der USA (Ohio) (us-east-2). Für Informationen zu allen verfügbaren Syntaxoptionen für`query-string`Parameter, siehe[Syntaxreferenz für Suchabfragen für Resource Explorer](#).

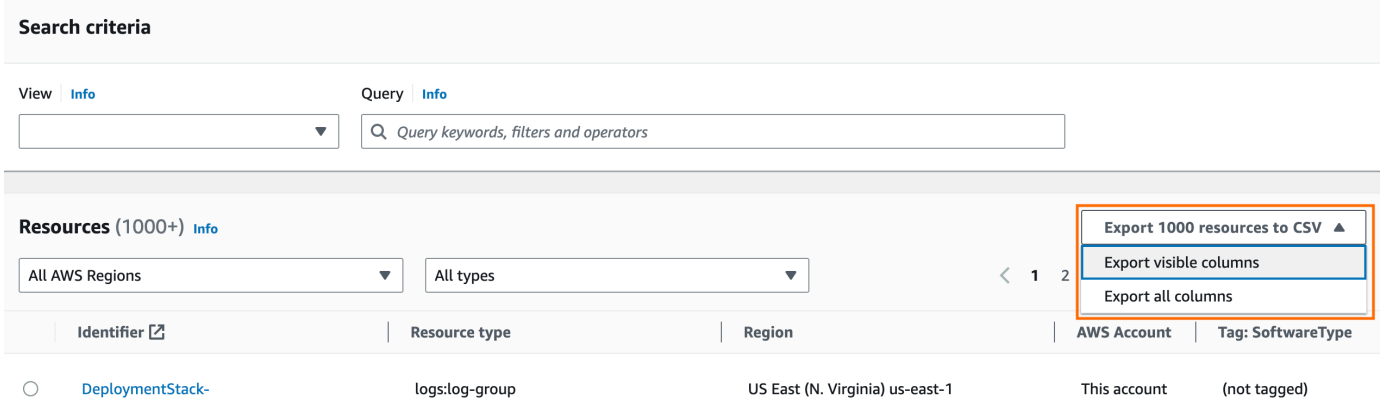
```
$ aws resource-explorer-2 search \
    --region us-east-1 \
    --query-string "resourcetype:AWS::EC2::Instance tag:env=production"
    --view-arn arn:aws:resource-explorer-2:us-east-2:123456789012:view/My-Resources-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

Exportieren Sie Suchergebnisse in eine CSV-Datei

Sie können die Ergebnisse eines exportierenSuche nach RessourcenAbfrage in eine Datei mit kommagetrennten Werten (.csv). Die CSV-Datei enthält die Kennung, den Ressourcentyp, die Region,AWS-Konto, die Gesamtzahl der Tags und eine Spalte für jeden eindeutigen Tag-Schlüssel in der Sammlung. Die CSV-Datei kann Ihnen bei der Konfiguration IhrerAWSRessourcen in Ihrer Organisation oder stellen Sie fest, wo es Überschneidungen oder Inkonsistenzen bei der Ressourcenkennzeichnung gibt.

1. In den Ergebnissen IhresSuche nach Ressourcenabfragen, wählenRessourcen nach CSV exportieren.

Sie können wählen, ob Sie Ihre Ergebnisse nur mit den Spalten exportieren möchten, die Sie aktuell sehen, oder mit allen verfügbaren Spalten exportieren möchten.



2. Wenn Sie von Ihrem Browser dazu aufgefordert werden, wählen Sie, ob Sie die CSV-Datei öffnen oder an einem geeigneten Ort speichern möchten.

Ressourcentypen, nach denen Sie mit Resource Explorer suchen können

Resource Explorer unterstützt Ressourcentypen in zahlreichen AWS Diensten.

Themen

- Unterstützte Dienste und Ressourcentypen
- Programmgesteuerter Zugriff auf die Liste der unterstützten Ressourcentypen
- Ressourcentypen, die als andere Typen erscheinen

Einige Ressourcentypen werden durch Amazon-Ressourcennamen (ARN) -Zeichenketten identifiziert, die ein gemeinsames Format wie ein anderer Ressourcentyp haben. In diesem Fall kann Resource Explorer solche Ressourcen als diesen anderen Ressourcentyp melden. Eine Liste der Ressourcentypen, die von diesem Problem betroffen sind, finden Sie unterRessourcentypen, die als andere Typen erscheinen.

Derzeit können Tags, die an Ressourcen AWS Identity and Access Management (IAM) angehängt sind, z. B. Rollen oder Benutzer, nicht für die Suche verwendet werden.

Wenn Sie verschlüsselten Zugriff auf einige Ihrer Ressourcen haben, kann Resource Explorer sie nicht ermitteln. Sie werden diese Ressourcen nicht in Ihren Suchergebnissen sehen.

In den folgenden Tabellen sind die Ressourcentypen aufgeführt, die für die Suche unterstützt werden AWS Ressourcen Explorer.

> **Note**
>
> Seit dem 9. Juli 2024 unterstützt Resource Explorer die folgenden Ressourcentypen nicht mehr:
>
> - Amazon Elastic Container Service — `ecs:task`
> - AWS Systems Manager — `ssm:automation-execution`
> - AWS Systems Manager — `ssm:patchbaseline`

Sie können diese Ressourcentypen weiterhin in ihren eigenen Diensten verwenden, sie sind jedoch nicht mehr indexiert oder können im Resource Explorer nicht mehr durchsucht werden.

Unterstützte Dienste und Ressourcentypen

Unterstützt AWS-Services

- APIAmazon-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 offenbar
- CloudWatch Amazon-Protokolle
- AWS CodeArtifact
- AWS CodeBuild
- AWS CodeCommit
- Amazon CodeGuru Profiler
- AWS CodePipeline
- AWS CodeConnections
- Amazon Cognito
- Amazon Connect
- Amazon Connect Wisdom

- Amazon Detective
- Amazon-DynamoDB
- EC2Image Builder
- Amazon ECR Public
- AWS Elastic Beanstalk
- Amazon ElastiCache
- Amazon Elastic Compute Cloud (AmazonEC2)
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- Amazon Elastic File System
- Elastic Load Balancing
- AWS Elemental MediaPackage
- AWS Elemental MediaTailor
- Amazon EMR Serverlos
- Amazon EventBridge
- AWS Fault Injection Service
- Amazon Forecast
- Amazon Fraud Detector
- Amazon GameLift
- AWS Global Accelerator
- AWS Glue
- AWS Glue DataBrew
- AWS Identity and Access Management
- Amazon Interactive Video Service
- AWS IoT
- AWS IoT Analytics
- AWS IoT Events
- AWS IoT Greengrass Version 1
- AWS IoT SiteWise

- AWS IoT TwinMaker
- AWS Key Management Service
- Amazon Kinesis
- Amazon Data Firehose
- Amazon Kinesis Video Streams
- AWS Lambda
- Amazon Lex
- Amazon Location Service
- Amazon Lookout für Metrics
- Amazon Lookout für Vision
- Amazon Managed Service für Apache Flink
- Amazon Managed Service für Prometheus
- Amazon Managed Service für Prometheus
- Amazon Managed Streaming für Apache Kafka
- AWS Migration Hub Refactor Spaces
- AWS Network Firewall
- AWS Network Manager
- OpenSearch Amazon-Dienst
- AWS Panorama
- Amazon Personalize
- AWS Private Certificate Authority
- Amazon QLDB
- Amazon-Redshift
- Amazon Rekognition
- Amazon Relational Database Service (AmazonRDS)
- AWS Resilience Hub
- AWS Resource Groups
- AWS Ressourcen Explorer
- Amazon Route 53

- Amazon Route 53 Recovery-Bereitschaft
- 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
- AWS Verified Access
- AWS Wavelength

APIAmazon-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 offenbar

- `evidently:project/experiment`
- `evidently:project/feature`
- `evidently:project/launch`

CloudWatch Amazon-Protokolle

- `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`

EC2Image Builder

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

Amazon ECR Public

- `ecrpublic:repository`

AWS Elastic Beanstalk

- `elasticbeanstalk:application`
- `elasticbeanstalk:applicationversion`
- `elasticbeanstalk:configurationtemplate`
- `elasticbeanstalk:environment`

Amazon ElastiCache

- `elasticache:cluster`
- `elasticache:globalreplicationgroup`

- `elasticache:parametergroup`
- `elasticache:replicationgroup`
- `elasticache:reserved-instance`
- `elasticache:snapshot`
- `elasticache:subnetgroup`
- `elasticache:user`
- `elasticache:usergroup`

Amazon Elastic Compute Cloud (AmazonEC2)

- `ec2:capacity-reservation`
- `ec2:capacity-reservation-fleet`
- `ec2:client-vpn-endpoint`
- `ec2:customer-gateway`
- `ec2:dedicated-host`
- `ec2:dhcp-options`
- `ec2:egress-only-internet-gateway`
- `ec2:elastic-gpu`
- `ec2:elastic-ip`
- `ec2:fleet`
- `ec2:fpga-image`
- `ec2:host-reservation`
- `ec2:image`
- `ec2:instance`
- `ec2:instance-event-window`
- `ec2:internet-gateway`
- `ec2:ipam`
- `ec2:ipam-pool`
- `ec2:ipam-scope`
- `ec2:ipv4pool-ec2`

- ec2:key-pair
- ec2:launch-template
- ec2:natgateway
- ec2:network-acl
- ec2:network-insights-access-scope
- ec2:network-insights-access-scope-analysis
- ec2:network-insights-analysis
- ec2:network-insights-path
- ec2:network-interface
- ec2:placement-group
- ec2:prefix-list
- ec2:reserved-instances
- ec2:route-table
- ec2:security-group
- ec2:security-group-rule
- ec2:snapshot
- ec2:spot-fleet-request
- ec2:spot-instances-request
- ec2:subnet
- ec2:subnet-cidr-reservation
- ec2:traffic-mirror-filter
- ec2:traffic-mirror-filter-rule
- ec2:traffic-mirror-session
- ec2:traffic-mirror-target
- ec2:transit-gateway
- ec2:transit-gateway-attachment
- ec2:transit-gateway-connect-peer
- ec2:transit-gateway-multicast-domain
- ec2:transit-gateway-policy-table
- ec2:transit-gateway-route-table

- `ec2:transitgatewayroutetableannouncement`
- `ec2:volume`
- `ec2:vpc`
- `ec2:vpc-endpoint`
- `ec2:vpc-flow-log`
- `ec2:vpc-peering-connection`
- `ec2:vpn-connection`
- `ec2:vpn-gateway`

Amazon Elastic Container Registry

- `ecr:repository`

Amazon Elastic Container Service

- `ecs:cluster`
- `ecs:container-instance`
- `ecs:service`
- `ecs:task-definition`
- `ecs:task-set`

Amazon Elastic File System

- `efs:filesystem`
- `efs:accesspoint`

Elastic Load Balancing

- `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 Serverlos

- `emr-serverless:applications`

Amazon EventBridge

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

AWS Fault Injection Service

- `fis:experimenttemplate`

Amazon Forecast

- `forcast:dataset`

- `forcast:dataset-group`

Amazon Fraud Detector

- `frauddetector:detector`
- `frauddetector:entity-type`
- `frauddetector:event-type`
- `frauddetector:label`
- `frauddetector:outcome`
- `frauddetector:variable`

Amazon GameLift

- `gamelift:alias`

AWS Global Accelerator

- `globalaccelerator:accelerator`
- `globalaccelerator:accelerator/listener`
- `globalaccelerator:accelerator/listener/endpoint-group`

AWS Glue

- `glue:database`
- `glue:job`
- `glue:table`
- `glue:trigger`

AWS Glue DataBrew

- `databrew:dataset`
- `databrew:recipe`

- `databrew:ruleset`

AWS Identity and Access Management

- `iam:group`
- `iam:instance-profile`
- `iam:oidc-provider`
- `iam:policy`
- `iam:role`
- `iam:saml-provider`
- `iam:server-certificate`
- `iam:user`
- `iam:virtualmfadevice`

Amazon Interactive Video Service

- `ivs:channel`
- `ivs:streamkey`

AWS IoT

- `iot:authorizer`
- `iot:jobtemplate`
- `iot:mitigationaction`
- `iot:policy`
- `iot:provisioningtemplate`
- `iot:rolealias`
- `iot:securityprofile`
- `iot:thing`
- `iot:topicrule`

AWS IoT Analytics

- `iotanalytics:channel`
- `iotanalytics:dataset`
- `iotanalytics:datastore`
- `iotanalytics:pipeline`

AWS IoT Events

- `iotevents:alarmModel`
- `iotevents:detectorModel`
- `iotevents:input`

AWS IoT Greengrass Version 1

- `greengrass:components`
- `greengrass:groups`

AWS IoT SiteWise

- `iotsitewise:asset`
- `iotsitewise:assetmodel`
- `iotsitewise:gateway`

AWS IoT TwinMaker

- `iottwinmaker:workspace`
- `iottwinmaker:workspace/component-type`
- `iottwinmaker:workspace/entity`

AWS Key Management Service

- `kms:key`

Amazon Kinesis

- `kinesis:stream`

Amazon Data Firehose

- `kinesisfirehose:deliverystream`

Amazon Kinesis Video Streams

- `kinesisvideo:stream`

AWS Lambda

- `lambda:code-signing-config`
- `lambda:event-source-mapping`
- `lambda:function`

Amazon Lex

- `lex:bot`

Amazon Location Service

- `geo:place-index`
- `geo:tracker`

Amazon Lookout für Metrics

- `lookoutmetrics:Alert`

Amazon Lookout für Vision

- `lookoutvision:project`

Amazon Managed Service für Apache Flink

- `kinesisanalytics:application`

Amazon Managed Service für Prometheus

- `aps:rulegroupsnamespace`
- `aps:workspace`

Amazon Managed Service für Prometheus

- `memorydb:cluster`
- `memorydb:parametergroup`
- `memorydb:user`

Amazon Managed Streaming für 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 Amazon-Dienst

- `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 (AmazonRDS)

- `rds:auto-backup`
- `rds:cev`
- `rds:cluster`
- `rds:cluster-endpoint`
- `rds:cluster-pg`
- `rds:cluster-snapshot`
- `rds:db`
- `rds:db-proxy`
- `rds:db-proxy-endpoint`
- `rds:deployment`
- `rds:es`
- `rds:global-cluster`
- `rds:og`
- `rds:pg`

- `rds:ri`
- `rds:secgrp`
- `rds:snapshot`
- `rds:subgrp`

AWS Resilience Hub

- `resiliencehub:resiliencypolicy`

AWS Resource Groups

- `resourcegroups:group`

AWS Ressourcen Explorer

- `resource-explorer-2:index`
- `resource-explorer-2:view`

Amazon Route 53

- `route53:healthcheck`
- `route53:hostedzone`

Amazon Route 53 Recovery-Bereitschaft

- `route53-recover-readiness:recovery-group`
- `route53-recover-readiness:resource-set`

Amazon Route 53 Resolver

- `route53resolver:firewalldomainlist`
- `route53resolver:firewallrulegroup`
- `route53resolver:resolverendpoint`

- `route53resolver:resolverrule`

Amazon SageMaker

- `sagemaker:model`
- `sagemaker:notebookinstance`

AWS Secrets Manager

- `secretsmanager:secret`

AWS Service Catalog

- `servicecatalog:applications`
- `servicecatalog:attribute-groups`

Amazon Simple Notification Service

- `sns:topic`

Amazon Simple Queue Service

- `sqs:queue`

Amazon-Simple-Storage-Service (Amazon-S3)

- `s3:accesspoint`
- `s3:bucket`
- `s3:storage-lens`

AWS Step Functions

- `states:statemachine`

- `stepfunctions:activity`

AWS Systems Manager

- `ssm:association`
- `ssm:document`
- `ssm:maintenancewindow`
- `ssm:managed-instance`
- `ssm:parameter`
- `ssm:resourcedatasync`
- `ssm:windowtarget`
- `ssm:windowtask`

AWS Verified Access

- `ec2:verifiedaccessendpoint`
- `ec2:verifiedaccessgroup`
- `ec2:verifiedaccessinstance`
- `ec2:verifiedaccesstrustprovider`

AWS Wavelength

- `ec2:carriergateway`

Programmgesteuerter Zugriff auf die Liste der unterstützten Ressourcentypen

Um über den Code auf die Liste der unterstützten Ressourcentypen zuzugreifen, können Sie den ListSupportedResourceTypesVorgang von einem beliebigen Code aus aufrufen. AWS SDK

Sie können beispielsweise den Befehl list-supported-resource-types AWS Command Line Interface (AWS CLI) ausführen, wie im folgenden Beispiel gezeigt.

```
$ 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 ...
```

Ressourcentypen, die als andere Typen erscheinen

Einige Ressourcentypen werden durch Amazon-Ressourcennamen (ARN) -Zeichenketten identifiziert, die ein gemeinsames Format wie ein anderer Ressourcentyp haben. In diesem Fall kann Resource Explorer solche Ressourcen als diesen anderen Ressourcentyp melden. Dies wirkt sich auf die Ressourcentypen in der folgenden Tabelle aus.

Tatsächlicher Ressourcentyp	Als Ressourcentyp gemeldet

`ec2:securitygroupegress`
 	
`ec2:securitygroupingress`
	`ec2:security-group-rule`

`elasticloadbalancingv2:load balancer`	`elasticloadbalancing:loadba lancer`

`docdb:dbcluster`
 	
`neptune:dbcluster`
 	
`rds:dbcluster`
	`rds:cluster`

`docdb:dbclusterparametergroup`	`rds:cluster-pg`

Tatsächlicher Ressourcentyp	Als Ressourcentyp gemeldet
`neptune:dbclusterparametergroup` `rds:dbclusterparametergroup`	

`docdb:clustersnapshot`
`neptune:dbclustersnapshot`
`rds:clustersnapshot`
	`rds:cluster-snapshot`

`docdb:dbinstance`
`neptune:dbinstance`
`rds:dbinstance`
	`rds:db`

`docdb:eventsubscription`
`neptune:eventsubscription`
`rds:eventsubscription`
	`rds:es`

`docdb:globalcluster` `rds:globalcluster`	`rds:global-cluster`
`neptune:dbparametergroup` `rds:dbparametergroup`	`rds:pg`

`docdb:dbsubnetgroup`
`neptune:dbsubnetgroup`
`rds:dbsubnetgroup`
	`rds:subgrp`

Syntaxreferenz für Suchabfragen für Resource Explorer

AWS Ressourcen Explorer hilft Ihnen dabei, einzelne AWS Ressourcen in Ihrem zu finden AWS-Konten. Damit Sie genau die Ressourcen finden können, nach denen Sie suchen, akzeptiert Resource Explorer Suchabfragezeichenfolgen, die die in diesem Thema beschriebene Syntax unterstützen. Beispielabfragen, die demonstrieren, wie die hier beschriebenen Funktionen verwendet werden, finden Sie unterBeispiel für Resource Explorer-Suchanfragen.

> **Note**
>
> Derzeit werden Tags, die an AWS Identity and Access Management (IAM) -Ressourcen wie Rollen oder Benutzer angehängt sind, nicht indexiert.

So funktionieren Abfragen im Resource Explorer

Suchanfragen verwenden immer eine Ansicht. Wenn Sie keine explizit angeben, verwendet Resource Explorer die Ansicht, die als Standardansicht für die Ansicht vorgesehen ist AWS-Region , in der Sie gerade arbeiten.

Ansichten bestimmen, welche Ressourcen für Sie zum Abfragen verfügbar sind. Sie können verschiedene Ansichten erstellen, die jeweils einen anderen Satz von Ressourcen zurückgeben.

Sie könnten beispielsweise eine Ansicht erstellen, die nur die Ressourcen enthält, die mit dem Schlüssel `Environment` und dem Wert gekennzeichnet sind`Production`. Dann könnten Sie festlegen, dass nur Benutzern Zugriff auf diese Ansicht gewährt wird, die diese Ressourcen aus geschäftlichen Gründen aufrufen möchten. Verschiedene Benutzer, die diese Ressourcen einsehen müssen, könnten auf eine separate Ansicht zugreifen, die die Ressourcen `Alpha` oder die `Beta` Umgebung enthält. Informationen darüber, wie Sie steuern können, wer Zugriff auf welche Ansichten erhält, finden Sie unterZugriff auf Resource Explorer-Ansichten für die Suche gewähren.

Syntax der Abfragezeichenfolge

Dieser Abschnitt enthält Informationen zu grundlegenden Aspekten der Abfragesyntax, zu Filtern und Filteroperatoren.

Grundlagen

Im Grunde genommen `QueryString` handelt es sich bei a um eine Reihe von frei formulierten Textschlüsselwörtern, die implizit durch einen logischen **`OR`** Operator verknüpft werden. Trennen Sie jedes Schlüsselwort von den anderen, indem Sie ein Leerzeichen verwenden, wie im folgenden Beispiel gezeigt:

```
ec2 billing test gamma
```

Resource Explorer bewertet diese Liste von Schlüsselwörtern dahingehend, dass sie Folgendes bedeuten:

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

Resource Explorer sortiert die Ergebnisse nach Relevanz und gibt Ressourcen, die einer größeren Anzahl von Suchbegriffen entsprechen, eine höhere Priorität. Ressourcen, die einem oder mehreren der Begriffe nicht entsprechen, werden nicht von den Ergebnissen ausgeschlossen. Resource Explorer betrachtet sie jedoch als weniger relevant und verschiebt sie in den Suchergebnissen weiter nach unten.

Wenn Sie eine leere Zeichenfolge für den `QueryString` Parameter angeben, gibt Ihre Abfrage die ersten 1.000 Ressourcen zurück, die in der für den Vorgang verwendeten Ansicht verfügbar sind. Die maximale Anzahl von Ressourcen, die von einer Abfrage zurückgegeben werden können, ist 1.000.

> **Note**
>
> AWS behält sich das Recht vor, die Abgleichslogik und die Relevanzalgorithmen für die Bewertung von frei formulierten Textschlüsselwörtern zu aktualisieren, damit wir unseren Kunden die relevantesten Ergebnisse liefern können. Daher können sich die Ergebnisse, die für dieselben Abfragen mit frei formulierten Textschlüsselwörtern zurückgegeben werden, im Laufe der Zeit ändern. Wenn Sie deterministischere Ergebnisse benötigen, empfehlen wir die Verwendung von Filtern. Die Logik des Filterabgleichs ändert sich im Laufe der Zeit nicht.

Filter

Sie können die Ergebnisse Ihrer Abfrage strenger einschränken, indem Sie Filter einbeziehen. Im Gegensatz zu Textschlüsselwörtern werden Filter in der Abfrage mit dem ANDOperator ausgewertet. Stellen Sie sich beispielsweise die folgende Abfrage vor, die aus zwei frei formbaren Schlüsselwörtern und zwei Filtern besteht:

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

Diese Abfrage wird wie folgt ausgewertet:

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

Filter werden immer mit ANDlogischen Operatoren ausgewertet. Wenn eine Ressource nicht mit dem Filter übereinstimmt, ist diese Ressource nicht in den Ergebnissen enthalten. Die Ergebnisse der Beispielabfrage beinhalten alle Ressourcen, die mit Amazon verknüpft sind EC2 und sich im Westen der USA (Oregon) befinden AWS-Region und denen mindestens eines der Schlüsselwörter in irgendeiner Weise zugeordnet ist.

> **Note**
>
> Aufgrund der impliziten Angabe `AND` können Sie erfolgreich nur einen Filter für ein Attribut verwenden, für das nur ein Wert mit der Ressource verknüpft werden kann. Eine Ressource kann beispielsweise nur Teil einer AWS-Region Ressource sein. Daher gibt die folgende Abfrage keine Ergebnisse zurück.
>
> ```
> region:us-east-1 region:us-west-1
> ```
>
> Diese Einschränkung gilt nicht für Filter für Attribute, die mehrere Werte gleichzeitig haben können, wie `tag:tag.key:`, und`tag.value:`.

In der folgenden Tabelle sind die verfügbaren Filternamen aufgeführt, die Sie in einer Resource Explorer-Suchabfrage verwenden können.

Name des Filters	Beschreibung und Beispiel
`accountid:`	AWS-Konto Derjenige, dem die Ressource gehört. Resource Explorer bezieht in die Ergebnisse nur die Ressourcen ein, die dem angegebenen Konto gehören. `accountid:123456789012`
`application:`	Mit diesem Filter können Sie nach Ressourcen mit einem `awsApplication` Tagschlüssel und einem Ressourcengruppenwert suchen. Sie können nach

Name des Filters	Beschreibung und Beispiel

	dem Namen der Anwendung oder der Ressourcengruppe der Anwendung suchenARN.
	
	`application:MyApplicationName`
	
	`application:arn:aws:resource-groups: us-east-1 :123456789012:group/MyApplicationName/123456789abced`
	
	`arn:aws:resource-groups: us-east-1 :123456789012:group/MyApplicationName/123456789abced`
	
	Note
	Um diesen Filter verwenden zu können, muss Ihre Ansicht Zugriff auf Tagging-Daten haben.

`id:`	Die Kennung einer einzelnen Ressource, ausgedrückt als Amazon-Ressourcenname (ARN). `id:arn:aws:license-manager: us-east-1 :123456789012:license-configuration:lic-ecbd5574fd92cb0d312baea26EXAMPLE`

Name des Filters	Beschreibung und Beispiel
`region:`	Der AWS-Region Ort, an dem sich die Ressource befindet. Resource Explorer bezieht in die Ergebnisse nur die Ressourcen ein, die sich in der angegeben en AWS-Region Datenbank befinden. `region:us-east-1` **Note** Wenn Sie nur den Regionalcode eingeben (ohne Filter, z. B.`us-east-1`), werden nicht dieselben Ergebnisse zurückgegeben wie`region:us-east-1` . Dieses Ergebnis ist darauf zurückzuf ühren, dass der Regionalcode als Freitextschlüsselwort, bei dem es sich nicht um einen Filter handelt, in seine einzelnen Teile zerlegt wird. `us-east-1` Wird beispielsweise als `useast`, und 1 gesucht. Diese Aufschlüsselung in Komponenten erfolgt nicht, wenn Sie das `region:` Präfix verwenden.
`region:global`	Ein Sonderfall für den `region:` Filter, mit dem Sie nach Ressourcen suchen können, die keiner Einzelperson zugeordnet sind, AWS-Region sondern als global gelten. `region:global` **Note** Wenn Sie nur das Schlüsselwort eingeben, werden `global` nicht dieselben Ergebnisse zurückgegeben`region:global` , da das wörtliche Wort „global“ nicht mit globalen Ressourcen verknüpft ist. Wenn Sie `global` als Schlüsselwort eingeben, werden nur die Ressourcen zurückgegeben, denen diese Literalzeichenfolge der Ressource zugeordnet ist.

Name des Filters	Beschreibung und Beispiel
`resourcetype:`	Der Ressourcentyp in *`service`*`:`*`type`* Notation. Resource Explorer bezieht nur die Ressourcen des angegebenen Typs in die Ergebnisse ein. `resourcetype:ec2:instance`
`resourcetype.supports:`	Mit diesem Filter können Sie nach Ressourcen suchen, die Tags unterstützen. `tags`ist der einzige unterstützte Wert. Resource Explorer bezieht in die Ergebnisse nur die Ressourcen ein, die mit Tags versehen werden können. `resourcetype.supports:tags`
`service:`	Die AWS-Service , die dem Typ der Ressource zugeordnet ist. Resource Explorer berücksichtigt in den Ergebnissen nur die Ressourcen, die vom angegebenen Dienst erstellt und verwaltet werden. `service:ec2`
`tag:`	Ein Tag-Schlüssel/Wert-Paar, ausgedrückt als. `<key>=<value>` Resource Explorer bezieht in die Ergebnisse nur die Ressourcen ein, die über ein Tag verfügen, das sowohl einen passenden Schlüssel als auch den angegebenen Wert enthält. `tag:environment=production`
`tag:all`	Ein Sonderfall des `tag:` Filters, mit dem Sie nach Ressourcen suchen können, denen ein oder mehrere benutzerdefinierte Tags zugeordnet sind, auch wenn der Ressourcentyp im Resource Explorer nicht unterstützt wird. **Note** Ressourcen mit vom AWS Dienst erstellten Tags werden weiterhin in den Ergebnissen für diesen Filter angezeigt.

Name des Filters	Beschreibung und Beispiel
`tag:none`	Ein Sonderfall des `tag:` Filters, mit dem Sie nach Ressourcen suchen können, denen keine vom Benutzer erstellten Tags zugeordnet sind. **Note** Ressourcen mit vom AWS Dienst erstellten Tags werden weiterhin in den Ergebnissen für diesen Filter angezeigt.
`tag.key:`	Ein Tag-Schlüssel. Resource Explorer bezieht in die Ergebnisse nur die Ressourcen ein, die über ein Tag mit einem passenden Schlüssel verfügen, unabhängig vom Wert. `tag.key:environment`
`tag.value:`	Ein Tag-Wert. Resource Explorer bezieht unabhängig vom Schlüsselnamen nur die Ressourcen in die Ergebnisse ein, die über ein Tag mit einem passenden Wert verfügen. `tag.value:production`

Operatoren filtern

Sie können Ihre Schlüsselwörter und Filter ändern, indem Sie einen der in der folgenden Tabelle aufgeführten Operatoren als Teil der Zeichenfolge hinzufügen.

Operator	Beschreibung und Beispiel

`"multiple word phrase"`
 	
or
 	
`"hyphenated-phrase "`
	Setzen Sie einen aus mehreren Wörtern bestehenden Satz, der als einzelnes Schlüsselwort behandelt werden soll, in doppelte Anführungszeichen (`"  "`). Der Ressourcen-Explorer enthält nur die Ressourcen, die dem gesamten Ausdruck entsprechen, also alle Wörter zusammen und in der angegebenen Reihenfolge.
	
	Wenn Sie die doppelten Anführungszeichen nicht verwenden, teilt Resource Explorer den Ausdruck durch Leerzeichen oder Bindestriche in seine

Operator	Beschreibung und Beispiel

	Bestandteile auf und schließt Ressourcen ein, die den einzelnen Komponenten entsprechen, auch wenn sie nicht zusammen oder in einer anderen Reihenfol ge vorkommen. Alles hinter dem Operator sollte in Anführungszeichen stehen.
	
	`"This matches only resources with the whole sentence."`
	
	`This matches resources with any of the words.`
	
	`"us-east-1"` — entspricht nur Ressourcen, die genau dieser Region zugeordnet sind.
	
	`us-east-1` — entspricht allen Ressourcen, die „uns“, „Ost“ oder „1“ enthalten .
	
	`-tag:"environment=production"`

`keyword``*`	Platzhalterübereinstimmung mit Präfixen. Sie können ein Platzhalterzeichen (ein Sternchen`*`) nur am Ende der Zeichenfolge platzieren. Resource Explorer bezieht in die Ergebnisse nur die Ressourcen ein, deren Werte mit dem Präfixtext vor dem beginnen. `*` Das folgende Beispiel entspricht allen AWS-Regionen , die mit beginnen`us-east`. `region:us-east*` **Important** Bei der einheitlichen Suche wird am Ende des ersten Schlüsselworts in der Zeichenfolge automatisch ein Platzhalterzeichen (`*`) eingefügt. Das bedeutet, dass vereinheitlichte Suchergebnisse Ressourcen enthalten , die mit einer beliebigen Zeichenfolge übereinstimmen, die mit dem angegebenen Schlüsselwort beginnt. Bei der Suche, die im Textfeld Abfrage auf der Seite Ressourcensuche in der Resource Explorer-Konsole ausgeführt wird, wird nicht automatis ch ein Platzhalterzeichen angehängt. Sie können nach einem beliebige n Begriff `*` manuell ein Wort in die Suchzeichenfolge einfügen.

Operator	Beschreibung und Beispiel

`-keyword`	`Not`Betreiber. Sie können einen Bindestrich (`-`) an den Anfang des Schlüssel worts setzen oder einen Filter verwenden, um die Suchergebnisse umzukehre n. Resource Explorer schließt alle Ressourcen aus den Ergebnissen aus, die dem Schlüsselwort oder Filter entsprechen, der diesem Operator folgt. Das folgende Beispiel führt dazu, dass alle Ressourcen, die mit dem EC2 Amazon-Service verknüpft sind, von den Ergebnissen ausgeschlossen werden.
	
	`-service:ec2`
	
	Important
	Wenn Sie den AWS CLI `search` Befehl verwenden und Ihr `--query-string` Parameterwert den `-` Operator als erstes Zeichen hat, müssen Sie den Parameternamen durch ein Gleichheitszeichen (=) anstelle des üblichen Leerzeichens von seinem Wert trennen. Wenn Sie das Leerzeichen verwenden, CLI interpretiert das die Zeichenfolge falsch. Die folgende Abfrage schlägt beispielsweise fehl.
	
	`aws resource-explorer-2 search --query-string "-tag:none region:us-east-1"`
	
	Die folgende korrigierte Abfragezeichenfolge, bei der ein Leerzeichen = ersetzt wird, funktioniert erwartungsgemäß.
	
	`aws resource-explorer-2 search --query-string =""-tag:none region:us-east-1"`
	
	Wenn Sie die Reihenfolge der Filter in der Abfragezeichenfolge ändern, sodass das `-` nicht das erste Zeichen im Parameterwert ist, können Sie das Standard-Leerzeichen verwenden. Die folgende Abfrageze ichenfolge funktioniert.
	
	`aws resource-explorer-2 search --query-string "region:us-east-1 -tag:none"`

Operator	Beschreibung und Beispiel

`\<special character>`	Sie können Sonderzeichen maskieren, die exakt wie abgebildet enthalten und nicht interpretiert werden müssen. Wenn Ihr Text eines der Sonderzeichen (`* " - : =` \) enthält, müssen Sie diesem Zeichen einen umgekehrten Schrägstrich (\) voranstellen, um sicherzustellen, dass das Zeichen wörtlich genommen wird. Das folgende Beispiel zeigt, wie Sie ein Freitextschlüsselwort verwenden, das den Bindestrich () `-` enthält. `"my-key-word"`
	
	Um zu verhindern, dass Resource Explorer den Ausdruck an den Bindestri chen in drei separate Schlüsselwörter aufteilt, können Sie außerdem den gesamten Ausdruck in doppelte Anführungszeichen setzen.
	
	`"my\-key\-word"`
	
	Um einen buchstäblichen umgekehrten Schrägstrich einzufügen, fügen Sie zwei umgekehrte Schrägstriche hintereinander ein. Der erste umgekehrte Schrägstrich wird als Escape interpretiert und der zweite umgekehrte Schrägstr ich ist das einzufügende Literalzeichen.
	
	`"some_text\\some_more_text"`

> **Note**
>
> Wenn die Ansicht die mit den Ressourcen verknüpften Tags enthält, löst der `Search` Vorgang keine Validierungsfehler für Suchzeichenfolgen aus, da ein ungültiger Filter auch als Freitextsuche interpretiert werden könnte. Obwohl er wie ein Filter `cat:blue` aussieht, kann Resource Explorer ihn beispielsweise nicht als einen Filter analysieren, da er `cat:` keiner der gültigen, definierten Filter ist. Stattdessen interpretiert Resource Explorer die gesamte Zeichenfolge als formlose Suchzeichenfolge, sodass sie mit Dingen wie einem Tag-Schlüsselnamen oder einem Teil eines Suchbegriffs übereinstimmt. ARN
> Der Vorgang löst einen Validierungsfehler aus, wenn eine der folgenden Bedingungen zutrifft:
>
> - Die Ansicht enthält keine Informationen zu Tags
> - Die Suchabfrage verwendet explizit einen Tagfilter (`tag.key:`,`tag.value:`, oder`tag:`)

Beispiel für Resource Explorer-Suchanfragen

Die folgenden Beispiele zeigen die Syntax für gängige Abfragetypen, die Sie in verwenden könnenAWS Ressourcen Explorer.

> **Important**
>
> Wenn Sie denAWS CLI`search` Befehl verwenden und Ihr`--query-string` Parameterwert den`-` Operator als erstes Zeichen enthält, müssen Sie den Parameternamen von seinem Wert durch ein Gleichheitszeichen (=) anstelle des üblichen Leerzeichens trennen. Wenn Sie das Leerzeichen verwenden, interpretiert die CLI die Zeichenfolge falsch. Beispielsweise schlägt die folgende Abfrage fehl.
>
> ```
> aws resource-explorer-2 search --query-string "-tag:none region:us-east-1"
> ```
>
> Die folgende korrigierte Abfrage, bei der das Leerzeichen= ersetzt wurde, funktioniert wie erwartet.
>
> ```
> aws resource-explorer-2 search --query-string="-tag:none region:us-east-1"
> ```
>
> Wenn Sie die Reihenfolge der Filter in der Abfragezeichenfolge ändern, sodass das`-` nicht das erste Zeichen im Parameterwert ist, können Sie das Standard-Leerzeichen verwenden. Die folgende Abfrage funktioniert.
>
> ```
> aws resource-explorer-2 search --query-string "region:us-east-1 -tag:none"
> ```

Suche nach Ressourcen ohne Tags

Wenn Sie die attributbasierte Zugriffskontrolle (ABAC) in Ihrem Konto verwenden, eine kostenbasierte Zuweisung verwenden oder eine tagbasierte Automatisierung für Ihre Ressourcen durchführen möchten, müssen Sie wissen, bei welchen Ressourcen in Ihrem Konto möglicherweise Tags fehlen. Die folgende Beispielabfrage verwendet das Filter-Tag für Sonderfälle: none, um alle Ressourcen zurückzugeben, denen benutzergenerierte Tags fehlen.

Der`tag:none` Filter gilt nur für Tags, die vom Benutzer erstellt wurden. Tags, die von generiert und verwaltetAWS werden, sind von diesem Filter ausgenommen und erscheinen weiterhin in den Ergebnissen.

```
tag:none
```

Um auch alleAWS erstellten System-Tags auszuschließen, fügen Sie einen zweiten Filter hinzu, wie im folgenden Beispiel gezeigt. Das erste Element in der Abfragezeichenfolge dupliziert das vorherige Beispiel, indem es alle vom Benutzer erstellten Tags herausfiltert. AWSerstellte System-Tags beginnen immer mit den Buchstaben`aws`. Daher können Sie den logischen NOT-Operator (-) mit dem Filter tag.key verwenden, um auch alle Ressourcen auszuschließen, die ein Tag mit einem Schlüsselnamen haben, der mit beginnt`aws`.

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

Suche nach markierten Ressourcen

Um alle Ressourcen zu finden, die ein beliebiges Tag haben, können Sie den logischen NOT-Operator (-) mit dem Sonderfall-Tag: none wie folgt filtern.

```
-tag:none
```

Suchen Sie nach Ressourcen, denen ein bestimmtes Tag fehlt

Auch im Zusammenhang mit ABAC möchten Sie vielleicht nach allen Ressourcen suchen, die kein Tag mit einem bestimmten Schlüssel haben. Im folgenden Beispiel wird der logische NOT-Operator verwendet,`-` um alle Ressourcen zurückzugeben, denen ein Tag mit dem Schlüsselnamen fehlt`Department`.

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

Suchen Sie nach Ressourcen mit ungültigen Tag-Werten

Aus Compliance-Gründen sollten Sie möglicherweise nach allen Ressourcen suchen, bei denen Tag-Werte für wichtige Tags fehlen oder falsch geschrieben wurden. Das folgende Beispiel gibt alle Ressourcen zurück, die ein Tag mit dem Schlüsselnamen haben`environment`. Die Abfrage

filtert jedoch jede Ressource heraus, die einen der gültigen Werte hat`prodinteg`, oder`dev`. Alle Ergebnisse dieser Abfrage haben einen anderen Wert, den Sie untersuchen und korrigieren sollten.

> **Important**
>
> Bei der Suche im Resource Explorer wird nicht zwischen Groß- und Kleinschreibung unterschieden und es kann nicht zwischen Schlüsselnamen und Werten unterschieden werden, die sich nur dadurch unterscheiden, wie sie groß geschrieben werden. Die Werte im folgenden Beispiel stimmen beispielsweise mit`PROD`,`prodPrOd`, oder einer beliebigen Variante überein. In einigen Anwendungen wird bei der Verwendung von Tags jedoch zwischen Groß- und Kleinschreibung unterschieden. Wir empfehlen, dass Sie für Ihr Unternehmen eine Standardstrategie zur Großschreibung festlegen, z. B. nur Namen und Werte für Tag-Schlüsselnamen und -werte in Kleinbuchstaben zu verwenden. Ein konsistenter Ansatz kann dazu beitragen, Verwirrung zu vermeiden, die entstehen kann, wenn Tags verwendet werden, die sich nur dadurch unterscheiden, wie sie groß geschrieben werden.

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

Suchen Sie nach Ressourcen in einer Teilmenge vonAWS-Regionen

Verwenden Sie den `'*'` Platzhalteroperator, um alle Regionen in einem bestimmten Gebiet der Welt abzugleichen. Das folgende Beispiel gibt alle Ressourcen zurück, die sich in Regionen in Europa (EU) befinden.

```
region:eu-*
```

Suchen Sie nach globalen Ressourcen

Verwenden Sie den`global` Sonderfallwert für den`region:` Filter, um Ihre Ressourcen zu finden, die als global betrachtet werden und keiner einzelnen Region zugeordnet sind.

```
region:global
```

Suchen Sie nach Ressourcen eines bestimmten Typs, die sich in einer bestimmten Region befinden

Wenn Sie mehrere Filter verwenden, wertet Resource Explorer den Ausdruck aus, indem er die Präfixe mit impliziten logischen`AND` Operatoren kombiniert. Im folgenden Beispiel werden alle Ressourcen in der Region`AND` Asien-Pazifik (Hongkong) Amazon EC2 EC2-Instances zurückgegeben.

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

> **Note**
>
> Aufgrund des Impliziten`AND` können Sie erfolgreich nur einen Filter für ein Attribut verwenden, dem nur ein Wert zugeordnet sein kann. Beispielsweise kann eine Ressource nur Teil einer Ressource seinAWS-Region. Daher gibt die folgende Abfrage keine Ergebnisse zurück.
>
> ```
> region:us-east-1 region:us-west-1
> ```
>
> Diese Einschränkung gilt nicht für die Filter für Attribute, die mehrere Werte gleichzeitig haben können, z. B.`tag:tag.key:`, und`tag.value:`.

Suchen Sie nach Ressourcen, die einen Begriff mit mehreren Wörtern enthalten

Umgeben Sie einen Begriff mit mehreren Wörtern in doppelte Anführungszeichen (`"`), um nur Ergebnisse zurückzugeben, die den gesamten Begriff in der angegebenen Reihenfolge enthalten. Ohne doppelte Anführungszeichen gibt Resource Explorer Ressourcen zurück, die mit den einzelnen Wörtern übereinstimmen, aus denen der Begriff besteht. Die folgende Abfrage verwendet beispielsweise die doppelten Anführungszeichen, um nur Ressourcen zurückzugeben, die dem Begriff entsprechen`"west wing"`. Die Abfrage stimmt nicht mit Ressourcen in der Region`us-west-2`AWS-Region (oder einer anderen Region, die`west` in ihrem Code enthalten ist) oder mit Ressourcen, die dem Wort „Flügel“ ohne das Wort „West“ entsprechen, überein.

```
"west wing"
```

Sucht nach Ressourcen, die Teil eines bestimmten CloudFormation Stacks sind

Wenn Sie eine Ressource als Teil einesAWS CloudFormation Stacks erstellen, werden sie alle automatisch mit dem Namen des Stacks gekennzeichnet. Das folgende Beispiel gibt alle Ressourcen zurück, die als Teil des angegebenen Stacks erstellt wurden.

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

Mithilfe der vereinheitlichten Suche in der AWS Management Console

Das AWS Management Console enthält eine Suchleiste oben auf jeder AWS Konsolenseite. Mit dieser Suchleiste können Sie die AWS-Service Dokumentations- und Blogthemen durchsuchen und Sie direkt zu den Seiten der AWS Servicekonsole führen. Es kann auch die Ressourcen in Ihrem System zurückgebenAWS-Konto, wenn Sie die vereinheitlichte Suchfunktion aktivieren, indem Sie die erforderlichen Resource Explorer-Funktionen aktivieren.

Mit der vereinheitlichten Suche können Ihre Benutzer von jeder AWS-Service Konsole aus nach Ressourcen suchen, ohne zuerst zur AWS Ressourcen Explorer Konsole navigieren zu müssen.

> **Tip**
>
> Wenn Sie die vereinheitlichte Suchleiste verwenden möchten, um gezielt nach Ressourcen zu suchen, beginnen Sie Ihre Suchabfrage, indem Sie Folgendes eingeben**`/Resources`**. Dies führt dazu, dass AWS Ressourcen in den Suchergebnissen höher eingestuft werden als Ergebnisse, die keine Ressourcen darstellen.

Themen

- Es wird überprüft, ob die einheitliche Suche aktiviert ist
- Unified Search aktivieren

> **Important**
>
> Die vereinheitlichte Suche fügt automatisch einen Platzhalteroperator (`*`) am Ende des ersten Schlüsselworts in der Zeichenfolge ein. Dies bedeutet, dass vereinheitlichte Suchergebnisse Ressourcen enthalten, die mit einer beliebigen Zeichenfolge übereinstimmen, die mit dem angegebenen Schlüsselwort beginnt.
> Bei der Suche, die über das Textfeld Abfrage auf der Seite Ressourcensuche in der Resource Explorer-Konsole ausgeführt wird, wird nicht automatisch ein Platzhalterzeichen angehängt. Sie können nach jedem Begriff in die Suchzeichenfolge `*` manuell eine einfügen.

Es wird überprüft, ob die einheitliche Suche aktiviert ist

Um zu sehen, ob die vereinheitlichte Suche in Ihrem aktiviert istAWS-Konto, schauen Sie oben auf der Seite mit den Einstellungen nach. Resource Explorer zeigt dort den aktuellen Status jeder Anforderung an. Die Anforderungen für die einheitliche Suche sind Folgende:

- Sie müssen den Resource Explorer in mindestens einem Gerät aktivierenAWS-Region. Nur Ressourcen in Regionen mit Resource Explorer-Indizes können in vereinheitlichten Suchergebnissen erscheinen.
- Sie müssen einen Aggregatorindex in der Region Ihrer Wahl erstellen. In dieser Region durchgeführte Suchanfragen geben Ergebnisse aus allen registrierten Regionen im Konto zurück.
- Sie müssen eine Standardansicht in der Region erstellen, die den Aggregatorindex enthält. Alle Benutzer, die die vereinheitlichte Suche nach Ressourcen verwenden müssen, müssen über die Berechtigung verfügen, diese Standardansicht zu verwenden.
- Benutzern muss eine AWS Identity and Access Management (IAM-) Berechtigungsrichtlinie zugewiesen sein, die ihrem IAM-Prinzip die Berechtigung zur Ausführung der`resource-explorer-2:Get*`, `resource-explorer-2:List*`resource-explorer-2:Describe*, `resource-explorer-2:Search` Aktionen erteilt. Sie können diese Berechtigungen gewähren, indem Sie Ihre eigenen benutzerdefinierten IAM-Richtlinien verwenden. Diese Berechtigungen sind bereits in den folgenden AWS verwalteten Richtlinien enthalten, die Ihnen zur Verfügung stehen:
  - AWSResourceExplorerReadOnlyAccess
  - AWSResourceExplorerFullAccess

Unified Search aktivieren

Um die Aufnahme der Ressourcen Ihres Kontos in die Suchergebnisse für die vereinheitlichte Suche von einer beliebigen AWS Konsole aus zu aktivieren, müssen Sie die folgenden Schritte ausführen:

1. Aktiviere AWS Ressourcen Explorer eine oder mehrere AWS-Regionen in deinem Konto.
2. Registrieren Sie eine Region, die den Aggregatorindex enthält.
3. Erstellen Sie eine Standardansicht in der Region mit dem Aggregatorindex.

Resource Explorer-Ressourcen erstellen mit CloudFormation

AWS Ressourcen Explorerist in integriertAWS CloudFormation, ein Service, der Ihnen hilft, Ihre AWS Ressourcen zu modellieren und einzurichten. Durch diese Integration können Sie weniger Zeit mit der Erstellung und Verwaltung Ihrer Ressourcen und Infrastruktur verbringen. Sie erstellen eine Vorlage, in der alle gewünschten AWS-Ressourcen beschrieben werden. CloudFormation übernimmt dann die Bereitstellung und Konfiguration dieser Ressourcen für Sie. Zu den Ressourcen gehören beispielsweise Indizes, Ansichten oder die Zuweisung einer Standardansicht für eineAWS-Region.

Wenn Sie verwendenCloudFormation, können Sie Ihre Vorlage wiederverwenden, um Ihre Resource Explorer-Ressourcen einheitlich und wiederholt einzurichten. Sie beschreiben Ihre Ressourcen dann einmal und können die gleichen Ressourcen dann in mehreren AWS-Konten und -Regionen immer wieder bereitstellen.

Wird verwendetAWS CloudFormation, um Resource Explorer bereitzustellen für AWS Organizations

Sie können Resource Explorer verwenden AWS CloudFormationStackSets, um ihn für alle Konten in Ihrer Organisation bereitzustellen. Wenn Sie in Ihrer Organisation Mitgliedskonten hinzufügen oder erstellen, StackSets können Sie für jedes neue Mitgliedskonto automatisch Indizes für jedes neue Mitgliedskonto konfigurierenAWS-Region, einschließlich eines Aggregator-Index, den Sie angeben. Detaillierte Anweisungen finden Sie unter Bereitstellen von Resource Explorer für die Konten in einer Organisation.

Resource Explorer und CloudFormation Vorlagen

Um Ressourcen für den Resource Explorer und die damit verbundenen Dienste AWS CloudFormationbereitzustellenzusten Vorlagen sind formatierte Textdateien in JSON oder YAML. Diese Vorlagen beschreiben die Ressourcen, die Sie in Ihren CloudFormation-Stacks bereitstellen möchten. Wenn Sie noch keine Erfahrungen mit JSON oder YAML haben, können Sie AWS CloudFormation Designer verwenden, der den Einstieg in die Arbeit mit CloudFormation-Vorlagen erleichtert. Weitere Informationen finden Sie unter Was ist AWS CloudFormation-Designer? im AWS CloudFormation-Benutzerhandbuch.

Resource Explorer unterstützt das Erstellen der folgenden -Ressourcentypen inCloudFormation:

- Index — Erstellt einen Index in einer Region und aktiviert den Resource Explorer in dieser Region. Sie können angeben, dass es sich bei dem Index entweder um einen lokalen Index oder um den Aggregatorindex für handelt. AWS-Konto Weitere Informationen erhalten Sie unter Den Resource

Explorer in einem einschalten AWS-Region , um Ihre Ressourcen zu indizieren und Aktivierung der regionsübergreifenden Suche durch Erstellen eines Aggregatorindexes.

- Ansicht — Erstellt eine Ansicht, die bestimmt, welche Ergebnisse angezeigt werden können, wenn ein Benutzer eine Suche durchführt. Jeder Suchvorgang muss eine Ansicht angeben. Sie müssen Benutzern die Berechtigung zur Verwendung der Ansichten gewähren, auf die sie zugreifen sollen. Weitere Informationen finden Sie unter Resource Explorer-Ansichten verwalten, um Zugriff auf die Suche zu gewähren.

> **Note**
>
> Sie müssen einen Index in einer Region erstellen, bevor Sie eine Ansicht in derselben Region erstellen können. Wenn Sie einen Index und eine Ansicht als Teil desselben Stacks erstellen, verwenden Sie das `DependsOn` Attribut für die Ansicht, wie in der folgenden Beispielvorlage gezeigt, um sicherzustellen, dass der Index zuerst erstellt wird.

- DefaultViewAssociation— Weist die angegebene Ansicht als Standard in der zugehörigen Region zu. Wenn ein Benutzer die Ansicht, die für einen Suchvorgang verwendet werden soll, nicht explizit angibt, versucht Resource Explorer, die Standardansicht zu verwenden, die der Region zugeordnet ist, in der der Benutzer die Suche durchführt. Weitere Informationen finden Sie unter Festlegen einer Standardansicht in einemAWS-Region

Das folgende Beispiel zeigt, wie Sie einen Index und eine Ansicht in derselben Region erstellen und die Ansicht als Standard für die Region festlegen können.

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"
                }
            }
        }
    }
}
```

Weitere Informationen, einschließlich Beispiele für JSON- und YAML-Vorlagen für diese Resource Explorer-Indizes und -Ansichten, finden Sie in der Referenz zum ResourceExplorer RDSRessourcentyp im AWS CloudFormation-Benutzerhandbuch.

Weitere Informationen zu AWS CloudFormation

Weitere Informationen zu CloudFormation finden Sie in den folgenden Ressourcen.

- AWS CloudFormation
- AWS CloudFormation-Benutzerhandbuch
- AWS CloudFormation-Benutzerhandbuch für die Befehlszeilenschnittstelle

Verwenden von Amazon Q Entwickler für Chat-Anwendungen zum Suchen nach Ressourcen

Sie können Informationen zu AWS-Services und Ihren -AWSRessourcen suchen und entdecken, indem Sie Fragen in Amazon Q Entwickler für Chat-Anwendungen natürlicher Sprache stellen. Amazon Q Entwickler für Chat-Anwendungen beantwortet servicebezogene Fragen direkt in Ihren Chat-Kanälen mit relevanten AWS Dokumentations- und Support-Artikelauszügen. Amazon Q Entwickler für Chat-Anwendungen verwendet Resource Explorer, um nach Ihren ressourcenbezogenen Fragen zu suchen und Antworten zu finden.

Weitere Informationen finden Sie unter Was ist Amazon Q Entwickler für Chat-Anwendungen? im Amazon Q Entwickler für Chat-Anwendungen Administratorhandbuch für .

AWS -Ressourcenfragen

Amazon Q Entwickler für Chat-Anwendungen verwendet Resource Explorer, um Ihre Ressourcen zu suchen und zu entdecken. Amazon Q Entwickler für Chat-Anwendungen zeigt diese Suchergebnisse in einer Liste an. Diese Liste zeigt die fünf wichtigsten übereinstimmenden Ressourcen und enthält die Möglichkeit, Ergebnisse weiter nach RessourcentypAWS-Region, und Tag zu filtern.

Voraussetzungen

Um Amazon Q Entwickler für Chat-Anwendungenressourcenbezogene Fragen zu stellen, müssen Sie:

- Stellen Sie sicher, dass Sie aktive Indizes und Ansichten mit mindestens einer Standardansicht in Ihrem habenAWS-Region. Indizes und Ansichten ermöglichen es Resource Explorer, Ihre Ressourcen zu katalogisieren und abzufragen. Weitere Informationen finden Sie unter Begriffe und Konzepte für Resource Explorer.
- Fügen Sie die AWSResourceExplorerReadOnlyAccess Richtlinie Ihrer Kanalrolle oder jeder entsprechenden Benutzerrolle hinzu, abhängig vom Berechtigungsschema Ihres Kanals.
- Stellen Sie sicher, dass Ihre Kanalschutzrichtlinien AWSResourceExplorerReadOnlyAccess Berechtigungen zulassen.

Häufig gestellte Ressourcenfragen

Sie können diese Fragen direkt über Ihre Chat-Kanäle stellen. Ersetzen Sie die Wörter durch roten Text durch Ihre eigenen Informationen.

```
@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?
```

Sicherheit in AWS Ressourcen Explorer

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der übergreifenden Verantwortlichkeit beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS-Services in der läuft AWS Cloud. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für Resource Explorer gelten, finden Sie unter AWS-Services Umfang nach Compliance-ProgrammAWS-Services und .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS-Service , was Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung anwenden können AWS Ressourcen Explorer. Es zeigt Ihnen, wie Sie Resource Explorer konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere verwenden können AWS-Services , die Ihnen bei der Überwachung und Sicherung Ihrer Resource Explorer-Ressourcen helfen.

Inhalt

- IAMRichtlinien aktualisieren auf IPv6
- Identitäts- und Zugriffsmanagement für AWS Ressourcen Explorer
- Datenschutz in AWS Ressourcen Explorer
- Compliance-Validierung für AWS Ressourcen Explorer
- Ausfallsicherheit in AWS Ressourcen Explorer
- Infrastruktursicherheit in AWS Ressourcen Explorer

IAMRichtlinien aktualisieren auf IPv6

AWS Ressourcen Explorer Kunden verwenden IAM Richtlinien, um einen zulässigen Bereich von IP-Adressen festzulegen und zu verhindern, dass IP-Adressen außerhalb des konfigurierten Bereichs auf Resource Explorer zugreifen könnenAPIs.

Der Resource-Explorer-2.*region*Die Domain .api.aws, in der Resource Explorer gehostet APIs werden, wird aktualisiert, sodass sie zusätzlich unterstützt wird. IPv6 IPv4

Richtlinien zur IP-Adressfilterung, die nicht für den Umgang mit IPv6 Adressen aktualisiert wurden, können dazu führen, dass Clients den Zugriff auf die Ressourcen in der Resource Explorer-Domäne verlieren. API

Kunden, die vom Upgrade von IPv4 auf betroffen sind IPv6

Kunden, die die duale Adressierung verwenden und deren Richtlinien aws: enthalten, sourceIp sind von diesem Upgrade betroffen. Duale Adressierung bedeutet, dass das Netzwerk IPv4 sowohl IPv6 als auch unterstützt.

Wenn Sie die duale Adressierung verwenden, müssen Sie Ihre IAM Richtlinien, die derzeit mit IPv4 Formatadressen konfiguriert sind, so aktualisieren, dass sie auch IPv6 Formatadressen enthalten.

Wenn Sie Hilfe bei Zugriffsproblemen benötigen, wenden Sie sich an Support.

> **Note**
>
> Die folgenden Kunden sind von diesem Upgrade nicht betroffen:
>
> - Kunden, die nur in IPv4 Netzwerken aktiv sind.
> - Kunden, die nur in IPv6 Netzwerken aktiv sind.

Was istIPv6?

IPv6ist der IP-Standard der nächsten Generation, der irgendwann ersetzt IPv4 werden soll. Die vorherige Version verwendet ein 32-Bit-Adressierungsschema zur Unterstützung von 4,3 Milliarden Geräten. IPv4 IPv6verwendet stattdessen 128-Bit-Adressierung, um etwa 340 Billionen Billionen Billionen (oder 2 bis 128.) Geräte zu unterstützen.

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

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

Aktualisierung einer Richtlinie für IAM IPv6

IAMRichtlinien werden derzeit verwendet, um mithilfe des `aws:SourceIp` Filters einen zulässigen Bereich von IP-Adressen festzulegen.

Die duale Adressierung unterstützt IPv4 sowohl den Datenverkehr als auch IPV6 den Datenverkehr. Wenn Ihr Netzwerk die duale Adressierung verwendet, müssen Sie sicherstellen, dass alle IAM Richtlinien, die für die IP-Adressfilterung verwendet werden, aktualisiert werden, sodass sie IPv6 Adressbereiche einbeziehen.

Diese Amazon S3 S3-Bucket-Richtlinie identifiziert beispielsweise zulässige IPv4 Adressbereiche `192.0.2.0.*` und `203.0.113.0.*` im `Condition` Element.

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

Um diese Richtlinie zu aktualisieren, wird das `Condition` Element der Richtlinie aktualisiert und umfasst nun IPv6 Adressbereiche `2001:DB8:1234:5678::/64` und`2001:cdba:3257:8593::/64`.

> **Note**
>
> Geben Sie NOT REMOVE die vorhandenen IPv4 Adressen ein, da sie aus Gründen der Abwärtskompatibilität benötigt werden.

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

Weitere Informationen zur Verwaltung von Zugriffsberechtigungen mit IAM finden Sie unter Verwaltete Richtlinien und Inline-Richtlinien im AWS Identity and Access Management Benutzerhandbuch.

Stellen Sie sicher, dass Ihr Kunde Folgendes unterstützt IPv6

Kunden, die den Resource-Explorer-2 verwenden. Es wird empfohlen, den Endpunkt {region} .api.aws zu überprüfen, ob ihre Clients auf andere Endpoints zugreifen können, die bereits aktiviert sind. AWS-Service IPv6 In den folgenden Schritten wird beschrieben, wie Sie diese Endpunkte verifizieren können.

Dieses Beispiel verwendet Linux und Curl Version 8.6.0 und verwendet die Amazon Athena-Servicendpunkte, für die Endpunkte IPv6 aktiviert sind, die sich in der api.aws-Domain befinden.

> **Note**
>
> Wechseln Sie zu derselben Region AWS-Region , in der sich der Client befindet. In diesem Beispiel verwenden wir den `us-east-1` Endpunkt USA Ost (Nord-Virginia).

1. Ermitteln Sie mithilfe des folgenden curl-Befehls, ob der Endpunkt mit einer IPv6 Adresse aufgelöst wird.

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

2. Stellen Sie mithilfe IPv6 des folgenden curl-Befehls fest, ob das Client-Netzwerk eine Verbindung herstellen kann.

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

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

   Wenn eine Remote-IP identifiziert wurde und der Antwortcode nicht angegeben ist`0`, wurde mithilfe IPv6 von erfolgreich eine Netzwerkverbindung zum Endpunkt hergestellt.

Wenn die Remote-IP leer ist oder der Antwortcode leer ist`0`, ist das Client-Netzwerk oder der Netzwerkpfad zum Endpunkt IPv4 -only. Sie können diese Konfiguration mit dem folgenden curl-Befehl überprüfen.

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

remote ip: 3.210.103.49
response code: 404
```

Wenn eine Remote-IP identifiziert wurde und der Antwortcode nicht angegeben ist`0`, wurde mithilfe IPv4 von erfolgreich eine Netzwerkverbindung zum Endpunkt hergestellt. Die Remote-IP sollte eine IPv4 Adresse sein, da das Betriebssystem das für den Client gültige Protokoll auswählen sollte. Wenn es sich bei der Remote-IP nicht um eine IPv4 Adresse handelt, verwenden Sie den folgenden Befehl, um die Verwendung IPv4 von curl zu erzwingen.

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

remote ip: 35.170.237.34
```

```
response code: 404
```

Identitäts- und Zugriffsmanagement für AWS Ressourcen Explorer

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAMAdministratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Resource Explorer-Ressourcen zu verwenden. IAMist eine AWS-Service , die Sie ohne zusätzliche Kosten verwenden können.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- So funktioniert Resource Explorer mit IAM
- AWS Ressourcen ExplorerBeispiele für identitätsbasierte -Richtlinien
- Beispiel für Service-Kontrollrichtlinien für AWS Organizations und Resource Explorer
- AWS verwaltete Richtlinien für AWS Ressourcen Explorer
- Verwenden von serviceverknüpften Rollen für Resource Explorer
- Problembehandlung bei AWS Ressourcen Explorer Berechtigungen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie im Resource Explorer ausführen.

Dienstbenutzer — Wenn Sie den Resource Explorer-Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr Resource Explorer-Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie im Resource Explorer nicht auf eine Funktion zugreifen können, finden Sie weitere Informationen unterProblembehandlung bei AWS Ressourcen Explorer Berechtigungen.

Dienstadministrator — Wenn Sie in Ihrem Unternehmen für Resource Explorer-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Resource Explorer. Es ist

Ihre Aufgabe, zu bestimmen, auf welche Resource Explorer-Funktionen und Ressourcen Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anfragen an Ihren IAM Administrator senden, um die Berechtigungen Ihrer Dienstbenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die grundlegenden Konzepte von zu verstehenIAM. Weitere Informationen darüber, wie Ihr Unternehmen Resource Explorer verwenden IAM kann, finden Sie unterSo funktioniert Resource Explorer mit IAM.

IAMAdministrator — Wenn Sie ein IAM Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Resource Explorer zu verwalten. Beispiele für identitätsbasierte Resource Explorer-Richtlinien, die Sie in verwenden könnenIAM, finden Sie unter. AWS Ressourcen ExplorerBeispiele für identitätsbasierte -Richtlinien

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM Rolle übernehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAMIdentity Center-) Nutzer, die Single-Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als föderierte Identität anmelden, hat Ihr Administrator zuvor einen Identitätsverbund mithilfe von Rollen eingerichtet. IAM Wenn Sie AWS mithilfe eines Verbunds darauf zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit der Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im IAMBenutzerhandbuch unter AWS API Anfragen signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere

Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) AWS im IAM Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie im Benutzerhandbuch unter Aufgaben, für die Root-Benutzeranmeldedaten erforderlich sind. IAM

Benutzer und Gruppen

Ein IAMBenutzer ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wir empfehlen, sich nach Möglichkeit auf temporäre Anmeldeinformationen zu verlassen, anstatt IAM Benutzer mit langfristigen Anmeldeinformationen wie Passwörtern und Zugriffsschlüsseln zu erstellen. Wenn Sie jedoch spezielle Anwendungsfälle haben, für die langfristige Anmeldeinformationen von IAM Benutzern erforderlich sind, empfehlen wir, die Zugriffsschlüssel abwechselnd zu verwenden. Weitere Informationen finden Sie im Benutzerhandbuch unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, für die IAM langfristige Anmeldeinformationen erforderlich sind.

Eine IAMGruppe ist eine Identität, die eine Sammlung von IAM Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung von IAM Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Wann sollte ein IAM Benutzer (statt einer Rolle) erstellt werden? im IAMBenutzerhandbuch.

Rollen

Eine IAMRolle ist eine Identität innerhalb von Ihnen AWS-Konto , für die bestimmte Berechtigungen gelten. Sie ähnelt einem IAM Benutzer, ist jedoch keiner bestimmten Person zugeordnet. Sie können vorübergehend eine IAM Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS CLI AWS API OR-Operation aufrufen oder eine benutzerdefinierte Operation verwendenURL. Weitere Informationen zu Methoden zur Verwendung von Rollen finden Sie unter Methoden zur Übernahme einer Rolle im IAMBenutzerhandbuch.

IAMRollen mit temporären Anmeldeinformationen sind in den folgenden Situationen nützlich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle für einen externen Identitätsanbieter. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Um zu kontrollieren, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in. IAM Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM Benutzerberechtigungen — Ein IAM Benutzer oder eine Rolle kann eine IAM Rolle übernehmen, um vorübergehend verschiedene Berechtigungen für eine bestimmte Aufgabe zu übernehmen.
- Kontoübergreifender Zugriff — Sie können eine IAM Rolle verwenden, um einer Person (einem vertrauenswürdigen Principal) in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie IAMim Benutzerhandbuch unter Kontoübergreifender Ressourcenzugriff. IAM
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen. AWS-Services Wenn Sie beispielsweise einen Service aufrufen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.

- Zugriffssitzungen weiterleiten (FAS) — Wenn Sie einen IAM Benutzer oder eine Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FASverwendet die Berechtigungen des Prinzipals, der an aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen AWS-Service an nachgelagerte Dienste zu stellen. FASAnfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien beim Stellen von FAS Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
- Servicerolle — Eine Servicerolle ist eine IAMRolle, die ein Dienst übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM Administrator kann eine Servicerolle von innen heraus erstellen, ändern und löschenIAM. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen AWS-Service an eine.
- Dienstbezogene Rolle — Eine dienstverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM Administrator kann die Berechtigungen für dienstbezogene Rollen anzeigen, aber nicht bearbeiten.

- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Verwenden einer IAM Rolle zur Erteilung von Berechtigungen für Anwendungen, die auf EC2 Amazon-Instances ausgeführt werden.

Informationen darüber, ob Sie IAM Rollen oder IAM Benutzer verwenden sollten, finden Sie im Benutzerhandbuch unter Wann sollte eine IAM Rolle (anstelle eines IAM Benutzers) erstellt werden.

Verwalten des Zugriffs mit Richtlinien

Sie steuern den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder

Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in AWS Form von JSON Dokumenten gespeichert. Weitere Informationen zur Struktur und zum Inhalt von JSON Richtliniendokumenten finden Sie im IAMBenutzerhandbuch unter Überblick über JSON Richtlinien.

Administratoren können mithilfe von AWS JSON Richtlinien festlegen, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Um Benutzern die Erlaubnis zu erteilen, Aktionen mit den Ressourcen durchzuführen, die sie benötigen, kann ein IAM Administrator IAM Richtlinien erstellen. Der Administrator kann dann die IAM Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen übernehmen.

IAMRichtlinien definieren Berechtigungen für eine Aktion, unabhängig von der Methode, mit der Sie den Vorgang ausführen. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen aus dem AWS Management Console AWS CLI, dem oder dem abrufen AWS API.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind Dokumente mit JSON Berechtigungsrichtlinien, die Sie an eine Identität anhängen können, z. B. an einen IAM Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen einer identitätsbasierten Richtlinie finden Sie unter IAMRichtlinien erstellen im Benutzerhandbuch. IAM

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können. AWS-Konto Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie oder einer Inline-Richtlinie wählen können, finden Sie im IAMBenutzerhandbuch unter Auswahl zwischen verwalteten Richtlinien und Inline-Richtlinien.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM Rollenvertrauensrichtlinien und Amazon S3 S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien nicht IAM in einer ressourcenbasierten Richtlinie verwenden.

AWS Ressourcen Explorer unterstützt keine ressourcenbasierten Richtlinien.

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLsähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON Richtliniendokumentformat.

Amazon S3 und AWS WAF Amazon VPC sind Beispiele für Dienste, die Unterstützung bietenACLs. Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

AWS Ressourcen Explorer unterstützt nichtACLs.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen — Eine Berechtigungsgrenze ist eine erweiterte Funktion, mit der Sie die maximalen Berechtigungen festlegen, die eine identitätsbasierte Richtlinie einer IAM Entität (IAMBenutzer oder Rolle) gewähren kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch

Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen zu Berechtigungsgrenzen finden Sie im IAMBenutzerhandbuch unter Berechtigungsgrenzen für IAM Entitäten.

- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen AWS Organizations. AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Geräte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Sitzungsrichtlinien.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAMBenutzerhandbuch unter Bewertungslogik für Richtlinien.

So funktioniert Resource Explorer mit IAM

Bevor Sie IAM den Zugriff auf verwalten AWS Ressourcen Explorer, sollten Sie sich darüber im Klaren sein, welche IAM Funktionen mit Resource Explorer zur Verfügung stehen. Einen allgemeinen Überblick darüber, wie Resource Explorer und andere Tools AWS-Services funktionieren IAM AWS-Services , finden Sie IAM im IAMBenutzerhandbuch unter Funktionen mit Resource Explorer.

Themen

- Identitätsbasierte Richtlinien von Resource Explorer
- Autorisierung auf der Grundlage von Resource Explorer-Tags

- Rollen im Resource Explorer IAM

Wie jeder andere Browser benötigt auch Resource Explorer Berechtigungen AWS-Service, um seine Operationen für die Interaktion mit Ihren Ressourcen nutzen zu können. Für die Suche benötigen Benutzer die Berechtigung, die Details zu einer Ansicht abzurufen und mithilfe der Ansicht zu suchen. Um Indizes oder Ansichten zu erstellen oder sie oder andere Resource Explorer-Einstellungen zu ändern, benötigen Sie zusätzliche Berechtigungen.

Weisen Sie IAM identitätsbasierte Richtlinien zu, die diese Berechtigungen den entsprechenden Prinzipalen gewähren. IAM Resource Explorer bietet mehrere verwaltete Richtlinien, die allgemeine Berechtigungssätze vordefinieren. Sie können diese Ihren IAM Hauptbenutzern zuweisen.

Identitätsbasierte Richtlinien von Resource Explorer

Mit IAM identitätsbasierten Richtlinien können Sie zulässige oder verweigerte Aktionen für bestimmte Ressourcen sowie die Bedingungen angeben, unter denen diese Aktionen zugelassen oder verweigert werden. Resource Explorer unterstützt bestimmte Aktionen, Ressourcen und Bedingungsschlüssel. Weitere Informationen zu allen Elementen, die Sie in einer JSON Richtlinie verwenden, finden Sie in der Referenz zu den IAM JSON Richtlinienelementen im IAMBenutzerhandbuch.

Aktionen

Administratoren können mithilfe von AWS JSON Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das `Action` Element einer JSON Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, für die nur eine Genehmigung erforderlich ist und für die es keinen entsprechenden Vorgang gibt. API Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Richtlinienaktionen im Resource Explorer verwenden das `resource-explorer-2` Dienstpräfix vor der Aktion. Um beispielsweise jemandem die Erlaubnis zu erteilen, mithilfe einer Ansicht zu suchen,

fügen Sie beim Resource `Search` API Explorer-Vorgang die `resource-explorer-2:Search` Aktion in eine Richtlinie ein, die diesem Prinzipal zugewiesen ist. Richtlinienanweisungen müssen entweder ein – `Action`oder ein `NotAction`-Element enthalten. Resource Explorer definiert eigene Aktionen, die Aufgaben beschreiben, die Sie mit diesem Dienst ausführen können. Diese entsprechen den Resource API Explorer-Vorgängen.

Um mehrere Aktionen in einer einzelnen Anweisung anzugeben, trennen Sie sie durch Beistriche, wie im folgenden Beispiel gezeigt.

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

Sie können mehrere Aktionen mithilfe von Platzhalterzeichen (`*`) angeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Describe` beginnen, einschließlich der folgenden Aktion:

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

Eine Liste der Resource Explorer-Aktionen finden Sie unter Aktionen Definiert von AWS Ressourcen Explorer in der AWS Service Authorization Reference.

Ressourcen

Administratoren können mithilfe von AWS JSON Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das `Resource` JSON Richtlinienelement gibt das Objekt oder die Objekte an, für die die Aktion gilt. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Es hat sich bewährt, eine Ressource mit ihrem Amazon-Ressourcennamen (ARN) anzugeben. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Anzeigen

Der primäre Resource Explorer-Ressourcentyp ist die Ansicht.

Die Ressource Resource Explorer-Ansicht hat das folgende ARN Format.

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

Das Resource ARN Explorer-Format wird im folgenden Beispiel gezeigt.

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

> **Note**
>
> Das ARN Feld für eine Ansicht enthält am Ende eine eindeutige Kennung, um sicherzustellen, dass jede Ansicht einzigartig ist. Dadurch wird sichergestellt, dass eine IAM Richtlinie, die Zugriff auf eine alte, gelöschte Ansicht gewährt hat, nicht dazu verwendet werden kann, versehentlich Zugriff auf eine neue Ansicht zu gewähren, die zufällig denselben Namen wie die alte Ansicht hat. Jede neue Ansicht erhält am Ende eine neue, eindeutige ID, um sicherzustellen, dass ARNs sie niemals wiederverwendet werden.

Weitere Informationen zum Format von ARNs finden Sie unter Amazon Resource Names (ARNs).

Sie verwenden IAM identitätsbasierte Richtlinien, die den IAM Prinzipalen zugewiesen sind, und geben die Ansicht als. `Resource` Auf diese Weise können Sie einer Gruppe von Prinzipalen Suchzugriff über eine Ansicht und einer anderen Gruppe von Prinzipalen Zugriff über eine völlig andere Ansicht gewähren.

Um beispielsweise einer einzelnen Ansicht, die `ProductionResourcesView` in einer IAM Richtlinienerklärung genannt wird, die Erlaubnis zu erteilen, rufen Sie zunächst den Amazon-Ressourcennamen (ARN) der Ansicht ab. Sie können die Seite „Ansichten“ in der Konsole verwenden, um die Details einer Ansicht anzuzeigen, oder den `ListViews` Vorgang aufrufen, um die gewünschte Ansicht vollständig ARN abzurufen. Fügen Sie es dann in eine Richtlinienerklärung ein, wie im folgenden Beispiel gezeigt, die die Erlaubnis erteilt, die Definition nur einer Ansicht zu ändern.

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

Um die Aktionen für alle Ansichten zuzulassen, die zu einem bestimmten Konto gehören, verwenden Sie das Platzhalterzeichen (`*`) im entsprechenden Teil von. ARN Das folgende Beispiel gewährt Suchberechtigungen für alle Ansichten in einem angegebenen AWS-Region AND-Konto.

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

Einige Resource Explorer-Aktionen`CreateView`, z. B., werden nicht für eine bestimmte Ressource ausgeführt, weil die Ressource, wie im folgenden Beispiel, noch nicht existiert. In solchen Fällen müssen Sie das Platzhalterzeichen (`*`) für die gesamte Ressource ARN verwenden.

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

Wenn Sie einen Pfad angeben, der mit einem Platzhalterzeichen endet, können Sie den `CreateView` Vorgang darauf beschränken, Ansichten zu erstellen, die nur den genehmigten Pfad enthalten. Das folgende Beispiel für eine Richtlinie zeigt, wie Sie es dem Prinzipal ermöglichen, Ansichten nur im Pfad `view/ProductionViews/` zu erstellen.

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

Index

Ein weiterer Ressourcentyp, mit dem Sie den Zugriff auf die Resource Explorer-Funktionen steuern können, ist der Index.

Die primäre Art, mit dem Index zu interagieren, besteht darin, den Resource Explorer in einer zu aktivieren, AWS-Region indem Sie einen Index in dieser Region erstellen. Danach erledigen Sie fast alles andere, indem Sie mit der Ansicht interagieren.

Mit dem Index können Sie unter anderem steuern, wer in jeder Region Ansichten erstellen kann.

> **Note**
>
> Nachdem Sie eine Ansicht erstellt haben, werden alle anderen Ansichtsaktionen nur für die ARN Ansicht und nicht für den Index IAM autorisiert.

Der Index enthält eine ARN, auf die Sie in einer Berechtigungsrichtlinie verweisen können. Ein Resource Explorer-Index ARN hat das folgende Format.

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

Sehen Sie sich das folgende Beispiel für einen Resource Explorer-Index anARN.

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

Bei einigen Resource Explorer-Aktionen wird die Authentifizierung anhand mehrerer Ressourcentypen überprüft. Der CreateViewVorgang autorisiert beispielsweise sowohl für den Index als auch für die Ansicht, so wie es nach ARN der Erstellung durch Resource Explorer der Fall sein wird. ARN Um Administratoren die Berechtigung zur Verwaltung des Resource Explorer-Dienstes `"Resource": "*"` zu erteilen, können Sie damit Aktionen für jede Ressource, jeden Index oder jede Ansicht autorisieren.

Alternativ können Sie einen Prinzipal so einschränken, dass er nur mit bestimmten Resource Explorer-Ressourcen arbeiten kann. Um beispielsweise Aktionen nur auf Resource Explorer-Ressourcen in einer bestimmten Region zu beschränken, können Sie eine ARN Vorlage hinzufügen, die sowohl dem Index als auch der Ansicht entspricht, aber nur eine einzige Region aufruft. Im folgenden Beispiel ARN entspricht der beiden Indizes oder Ansichten nur in der `us-west-2` Region des angegebenen Kontos. Geben Sie die Region im dritten Feld von anARN, verwenden Sie jedoch im letzten Feld ein Platzhalterzeichen (*), um einem beliebigen Ressourcentyp zu entsprechen.

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

Weitere Informationen finden Sie unter Resources Defined by AWS Ressourcen Explorer in der AWS Service Authorization Reference. Informationen darüber, mit welchen Aktionen Sie die ARN einzelnen

Ressourcen spezifizieren können, finden Sie unter Definierte Aktionen von AWS Ressourcen Explorer.

Bedingungsschlüssel

Resource Explorer stellt keine dienstspezifischen Bedingungsschlüssel bereit, unterstützt aber die Verwendung einiger globaler Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAMBenutzerhandbuch.

Administratoren können mithilfe von AWS JSON Richtlinien festlegen, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen `OR` Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Sie können einem IAM Benutzer beispielsweise nur dann Zugriff auf eine Ressource gewähren, wenn sie mit seinem IAM Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter IAMRichtlinienelemente: Variablen und Tags.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontext-Schlüssel für AWS globale Bedingungen im IAMBenutzerhandbuch.

Eine Liste der Bedingungsschlüssel, die Sie mit Resource Explorer verwenden können, finden Sie unter Bedingungsschlüssel für AWS Ressourcen Explorer in der AWS Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Definierte Aktionen von AWS Ressourcen Explorer.

Beispiele

Beispiele für identitätsbasierte Richtlinien von Resource Explorer finden Sie unter. AWS Ressourcen ExplorerBeispiele für identitätsbasierte -Richtlinien

Autorisierung auf der Grundlage von Resource Explorer-Tags

Sie können Tags an Resource Explorer-Ansichten anhängen oder Tags in einer Anfrage an Resource Explorer übergeben. Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `resource-explorer-2:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden. Weitere Informationen zum Taggen von Resource Explorer-Ressourcen finden Sie unterHinzufügen von Markern zu Ansichten zu Ansichten hinzu. Informationen zur Verwendung der Tag-basierten Autorisierung im Resource Explorer finden Sie unter. Mit Tag-basierter Autorisierung

Rollen im Resource Explorer IAM

Bei einer IAMRolle handelt es sich um einen Prinzipal innerhalb von Ihnen AWS-Konto , der über bestimmte Berechtigungen verfügt.

Verwenden temporärer Anmeldeinformationen mit Resource Explorer

Sie können temporäre Anmeldeinformationen verwenden, um sich bei einem Verbund anzumelden, eine IAM Rolle zu übernehmen oder eine kontoübergreifende Rolle anzunehmen. Sie erhalten temporäre Sicherheitsanmeldedaten, indem Sie AWS Security Token Service (AWS STS) API -Operationen wie AssumeRoleoder GetFederationTokenaufrufen.

Resource Explorer unterstützt die Verwendung temporärer Anmeldeinformationen.

Service-verknüpfte Rollen

Mit Diensten verknüpfte Rollen ermöglichen AWS-Services den Zugriff auf Ressourcen in anderen Diensten, um eine Aktion in Ihrem Namen auszuführen. Mit Diensten verknüpfte Rollen werden in Ihrem IAM Konto angezeigt und gehören dem Dienst. Ein IAM Administrator kann die Berechtigungen für dienstbezogene Rollen anzeigen, aber nicht bearbeiten.

Resource Explorer verwendet dienstverknüpfte Rollen, um seine Arbeit auszuführen. Einzelheiten zu dienstbezogenen Rollen in Resource Explorer finden Sie unter. Verwenden von serviceverknüpften Rollen für Resource Explorer

AWS Ressourcen ExplorerBeispiele für identitätsbasierte -Richtlinien

AWS Identity and Access ManagementIAM-Prinzipale wie Rollen, Gruppen und Benutzer verfügen nicht über die Berechtigung zum Erstellen oder Ändern von Resource Explorer-Ressourcen. Sie können auch keine Aufgaben mit derAWS Management Console,AWS Command Line Interface (AWS CLI) oderAWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die den Prinzipals die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Anschließend muss der Administrator diese Richtlinien den IAM-Prinzipalen zuweisen, die diese Berechtigungen benötigen.

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center-Benutzerhandbuch.
- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von Richtlinien auf der JSON-Registerkarte im IAM-Benutzerhandbuch.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der Resource Explorer-Konsole
- Gewähren des Zugriffs auf eine Ansicht anhand von Stichwörtern
- Zugriff gewähren, um eine Ansicht auf der Grundlage von Tags zu erstellen

- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien können festlegen, ob jemand Resource Explorer-Ressourcen in Ihrem Konto erstellen, zugreifen oder löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS-verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen – Um Ihren Benutzern und Workloads Berechtigungen zu gewähren, verwenden Sie die AWS-verwaltete Richtlinien die Berechtigungen für viele allgemeine Anwendungsfälle gewähren. Sie sind in Ihrem AWS-Konto verfügbar. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie AWS-kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS-verwaltete Richtlinien oder AWS-verwaltete Richtlinien für Auftragsfunktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Service-Aktionen zu gewähren, wenn diese durch ein bestimmtes AWS-Service, wie beispielsweise AWS CloudFormation, verwendet werden. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als

100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.

- Bedarf einer Multi-Faktor-Authentifizierung (MFA) – Wenn Sie ein Szenario haben, das IAM-Benutzer oder Root-Benutzer in Ihrem AWS-Konto erfordert, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der Resource Explorer-Konsole

Damit Principals in derAWS Ressourcen Explorer Konsole suchen können, müssen sie über einen Mindestsatz von Berechtigungen verfügen. Wenn Sie keine identitätsbasierte Richtlinie mit den mindestens erforderlichen Berechtigungen erstellen, funktioniert die Resource Explorer-Konsole nicht wie vorgesehen für die Hauptbenutzer im Konto.

Sie können die benannteAWS verwaltete Richtlinie verwenden`AWSResourceExplorerReadOnlyAccess`, um die Möglichkeit zu gewähren, die Resource Explorer-Konsole für die Suche in einer beliebigen Ansicht im Konto zu verwenden. Informationen zum Erteilen von Suchberechtigungen für nur eine einzige Ansicht finden Sie unterZugriff auf Resource Explorer-Ansichten für die Suche gewähren und in den Beispielen in den folgenden beiden Abschnitten.

Für Prinzipale, die nur Aufrufe an die AWS CLI oder AWS-API durchführen, müssen Sie keine Mindestberechtigungen in der Konsole erteilen. Stattdessen können Sie festlegen, dass nur den Aktionen Zugriff gewährt wird, die den API-Vorgängen entsprechen, die die Prinzipale ausführen müssen.

Gewähren des Zugriffs auf eine Ansicht anhand von Stichwörtern

In diesem Beispiel möchten Sie Zugriff auf eine Resource Explorer-Ansicht inAWS-Konto Ihren beiden Hauptverwaltern des Kontos gewähren. Dazu weisen Sie den Prinzipalen, nach denen Sie im Resource Explorer suchen können möchten, identitätsbasierte IAM-Richtlinien zu. Die folgende IAM-Beispielrichtlinie gewährt Zugriff auf jede Anfrage, bei der das an den aufrufenden Principal

angehängte`Search-Group` Tag genau mit dem Wert für dasselbe Tag übereinstimmt, das an die in der Anforderung verwendete View angehängt ist.

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

Sie können diese Richtlinie den IAM-Prinzipalen in Ihrem Konto zuweisen. Wenn ein Principal mit dem Tag`Search-Group=A` versucht, in einer Resource Explorer-Ansicht zu suchen, muss die Ansicht ebenfalls mit einem Tag versehen werden`Search-Group=A`. Ist dies nicht der Fall, wird dem Principal der Zugriff verweigert. Der Tag-Schlüssel `Search-Group` der Bedingung stimmt sowohl mit `Search-group` als auch mit `search-group` überein, da die Namen von Bedingungsschlüsseln nicht zwischen Groß- und Kleinschreibung unterscheiden. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

> **Important**
>
> Um Ihre Ressourcen in vereinheitlichten Suchergebnissen in der anzuzeigenAWS Management Console, müssen die Prinzipale`GetView` sowohl über als auch über`Search` Berechtigungen für die Standardansicht in derAWS-Region Ansicht verfügen, die den Aggregatorindex enthält. Die einfachste Methode, diese Berechtigungen zu gewähren, besteht darin, die standardmäßige ressourcenbasierte Berechtigung beizubehalten, die an die Ansicht angehängt war, als Sie den Resource Explorer mithilfe der Schnelleinstellungen oder Erweitert aktiviert haben.

Für dieses Szenario könnten Sie erwägen, die Standardansicht so einzurichten, dass vertrauliche Ressourcen herausgefiltert werden, und dann zusätzliche Ansichten einzurichten, für die Sie tagbasierten Zugriff gewähren, wie im vorherigen Beispiel beschrieben.

Zugriff gewähren, um eine Ansicht auf der Grundlage von Tags zu erstellen

In diesem Beispiel möchten Sie zulassen, dass nur Prinzipale, die mit demselben Tag wie der Index gekennzeichnet sind, Ansichten in dem erstellen könnenAWS-Region, der den Index enthält. Erstellen Sie dazu identitätsbasierte Berechtigungen, damit die Prinzipale mithilfe von Ansichten suchen können.

Jetzt können Sie Berechtigungen zum Erstellen einer Ansicht gewähren. Sie können die Anweisungen in diesem Beispiel zu derselben Berechtigungsrichtlinie hinzufügen, die Sie verwenden, um den entsprechenden Prinzipalen`Search` Berechtigungen zu gewähren. Die Aktionen werden auf der Grundlage der an die Prinzipale angehängten Tags zugelassen oder verweigert, die die Operationen und den Index aufrufen, mit denen die Ansicht verknüpft werden soll. Die folgende IAM-Beispielrichtlinie lehnt jede Anforderung zur Erstellung einer Ansicht ab, wenn der Wert des an den Principal des Aufrufers angefügten`Allow-Create-View` Tags nicht genau mit dem Wert für dasselbe Tag übereinstimmt, das an den Index in der Region angehängt ist, in der die Ansicht erstellt wurde.

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

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie enthält Berechtigungen für die Ausführung dieser Aktion auf der Konsole oder für die programmgesteuerte Ausführung über die AWS CLI oder die AWS-API.

```
{
    "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": "*"
        }
    ]
}
```

Beispiel für Service-Kontrollrichtlinien für AWS Organizations und Resource Explorer

AWS Ressourcen Explorer unterstützt Service-Kontrollrichtlinien (SCPs). SCPs sind Richtlinien, die Sie an Elemente in einer Organisation anfügen, um Berechtigungen innerhalb dieser Organisation zu verwalten. Ein SCP gilt für alle AWS-Konten in einer Organisation unter dem -Element, an das Sie den SCP anfügen. SCPs bieten eine zentrale Kontrolle über die maximal verfügbaren Berechtigungen aller Konten Ihrer Organisation. Sie können Ihnen dabei helfen, sicherzustellen, dass Sie die Zugriffskontrollrichtlinien Ihrer Organisation AWS-Konten einhalten. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.

Voraussetzungen

Um SCPs zu verwenden, müssen Sie Folgendes ausführen:

- Aktivieren aller Funktionen in der Organisation. Weitere Informationen finden Sie unter Aktivieren aller Funktionen in Ihrer Organisation im AWS Organizations Benutzerhandbuch.
- Aktivieren Sie SCPs für die Verwendung in Ihrer Organisation. Weitere Informationen finden Sie unter Aktivieren und Deaktivieren von Richtlinientypen im AWS Organizations -Benutzerhandbuch.
- Erstellen Sie die SCPs, die Sie benötigen. Weitere Informationen zum Erstellen von SCPs finden Sie unter Erstellen und Aktualisieren von SCPs im AWS Organizations -Benutzerhandbuch.

Beispiel für Service-Kontrollrichtlinien

Das folgende Beispiel zeigt, wie Sie die attributbasierte Zugriffskontrolle (ABAC) verwenden können, um den Zugriff auf die administrativen Vorgänge von Resource Explorer zu steuern. Diese Beispielrichtlinie verweigert den Zugriff auf alle Resource-Explorer-Operationen mit Ausnahme der beiden Berechtigungen, die für die Suche erforderlich sind, `resource-explorer-2:Search` und , es sei denn`resource-explorer-2:GetView`, der IAM-Prinzipal, der die Anforderung stellt, ist mit gekennzeichnet`ResourceExplorerAdmin=TRUE`. Eine vollständigere Erläuterung der Verwendung von ABAC mit Resource Explorer finden Sie unter Mit Tag-basierter Autorisierung.

```
{
  "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 verwaltete Richtlinien für AWS Ressourcen Explorer

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien dienen dazu, Berechtigungen für viele gängige Anwendungsfälle bereitzustellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie für alle AWS Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das

Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

Allgemeine AWS verwaltete Richtlinien, die Resource Explorer-Berechtigungen beinhalten

- AdministratorAccess— Gewährt vollen Zugriff auf AWS-Services und Ressourcen.
- ReadOnlyZugriff — Gewährt schreibgeschützten Zugriff auf AWS-Services und Ressourcen.
- ViewOnlyZugriff — Erteilt Berechtigungen zum Anzeigen von Ressourcen und grundlegenden Metadaten für. AWS-Services

> **Note**
>
> Die in der `ViewOnlyAccess` Richtlinie enthaltenen Resource `Get*` `List` Explorer-Berechtigungen verhalten sich ähnlich wie Berechtigungen, geben jedoch nur einen einzigen Wert zurück, da eine Region nur einen Index und eine Standardansicht enthalten kann.

AWS verwaltete Richtlinien für Resource Explorer

- AWSResourceExplorerFullAccess
- AWSResourceExplorerReadOnlyAccess
- AWSResourceExplorerServiceRolePolicy

AWS verwaltete Richtlinie: AWSResourceExplorerFullAccess

Sie können die `AWSResourceExplorerFullAccess` Richtlinie Ihren IAM-Identitäten zuweisen.

Diese Richtlinie gewährt Berechtigungen, die die vollständige administrative Kontrolle über den Resource Explorer-Dienst ermöglichen. Sie können alle Aufgaben, die mit der Aktivierung und Verwaltung von Resource Explorer verbunden sind, AWS-Regionen in Ihrem Konto ausführen.

Details zu Berechtigungen

Diese Richtlinie umfasst Berechtigungen, die alle Aktionen für Resource Explorer ermöglichen, darunter das Ein- und Ausschalten des Resource Explorers in AWS-Regionen, das Erstellen oder

Löschen eines Aggregatorindexes für das Konto, das Erstellen, Aktualisieren und Löschen von Ansichten und das Suchen. Diese Richtlinie umfasst auch Berechtigungen, die nicht Teil von Resource Explorer sind:

- `ec2:DescribeRegions`— ermöglicht Resource Explorer den Zugriff auf die Details zu den Regionen in Ihrem Konto.
- `ram:ListResources`— ermöglicht Resource Explorer, die Ressourcenfreigaben aufzulisten, zu denen Ressourcen gehören.
- `ram:GetResourceShares`— ermöglicht Resource Explorer, Details zu den Ressourcenfreigaben zu ermitteln, die Ihnen gehören oder die mit Ihnen gemeinsam genutzt werden.
- `iam:CreateServiceLinkedRole`— ermöglicht Resource Explorer, die erforderliche dienstbezogene Rolle zu erstellen, wenn Sie Resource Explorer aktivieren, indem Sie den ersten Index erstellen.
- `organizations:DescribeOrganization`— ermöglicht Resource Explorer den Zugriff auf Informationen über Ihre Organisation.

Die neueste Version dieser AWS verwalteten Richtlinie finden Sie `AWSResourceExplorerFullAccess` im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AWSResourceExplorerReadOnlyAccess

Sie können die `AWSResourceExplorerReadOnlyAccess` Richtlinie Ihren IAM-Identitäten zuweisen.

Diese Richtlinie gewährt Benutzern nur Leseberechtigungen, mit denen sie ihre Ressourcen mit einfachem Suchzugriff finden können.

Details zu Berechtigungen

Diese Richtlinie umfasst Berechtigungen, die es Benutzern ermöglichen, den Resource Explorer auszuführen `Get*List*`, sowie `Search` Operationen zum Anzeigen von Informationen über Resource Explorer-Komponenten und Konfigurationseinstellungen, erlaubt Benutzern jedoch nicht, diese zu ändern. Benutzer können auch suchen. Diese Richtlinie umfasst auch zwei Berechtigungen, die nicht Teil von Resource Explorer sind:

- `ec2:DescribeRegions`— ermöglicht Resource Explorer den Zugriff auf die Details zu den Regionen in Ihrem Konto.

- `ram:ListResources`— ermöglicht Resource Explorer, die Ressourcenfreigaben aufzulisten, zu denen Ressourcen gehören.
- `ram:GetResourceShares`— ermöglicht Resource Explorer, Details zu den Ressourcenfreigaben zu ermitteln, die Ihnen gehören oder die mit Ihnen gemeinsam genutzt werden.
- `organizations:DescribeOrganization`— ermöglicht Resource Explorer den Zugriff auf Informationen über Ihre Organisation.

Die neueste Version dieser AWS verwalteten Richtlinie finden Sie `AWSResourceExplorerReadOnlyAccess` im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AWSResourceExplorerServiceRolePolicy

Sie können selbst keine Verbindungen `AWSResourceExplorerServiceRolePolicy` zu IAM-Entitäten herstellen. Diese Richtlinie kann nur einer dienstbezogenen Rolle zugewiesen werden, die es Resource Explorer ermöglicht, Aktionen in Ihrem Namen auszuführen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Resource Explorer.

Diese Richtlinie gewährt die Berechtigungen, die Resource Explorer benötigt, um Informationen über Ihre Ressourcen abzurufen. Resource Explorer füllt die Indizes, die er in jeder Registrierung verwaltet AWS-Region , auf.

Die neueste Version dieser AWS verwalteten Richtlinie finden Sie unter `AWSResourceExplorerServiceRolePolicy` In der IAM-Konsole.

AWS verwaltete Richtlinie: AWSResourceExplorerOrganizationsAccess

Sie können `AWSResourceExplorerOrganizationsAccess` Ihren IAM-Identitäten zuweisen.

Diese Richtlinie gewährt Resource Explorer Administratorberechtigungen und anderen Benutzern nur Leseberechtigungen, um diesen Zugriff AWS-Services zu unterstützen. Der AWS Organizations Administrator benötigt diese Berechtigungen, um die Suche mit mehreren Konten in der Konsole einzurichten und zu verwalten.

Details zu Berechtigungen

Diese Richtlinie umfasst Berechtigungen, die es Administratoren ermöglichen, die Suche mit mehreren Konten für die Organisation einzurichten:

- `ec2:DescribeRegions`— Ermöglicht Resource Explorer den Zugriff auf die Details zu den Regionen in Ihrem Konto.

- `ram:ListResources`— Ermöglicht Resource Explorer, die Ressourcenfreigaben aufzulisten, zu denen Ressourcen gehören.
- `ram:GetResourceShares`— Ermöglicht Resource Explorer, Details zu den Ressourcenfreigaben zu ermitteln, die Ihnen gehören oder die mit Ihnen gemeinsam genutzt werden.
- `organizations:ListAccounts`— Ermöglicht Resource Explorer, die Konten innerhalb einer Organisation zu identifizieren.
- `organizations:ListRoots`— Ermöglicht Resource Explorer, die Stammkonten innerhalb einer Organisation zu identifizieren.
- `organizations:ListOrganizationalUnitsForParent`— Ermöglicht Resource Explorer, die Organisationseinheiten (OUs) in einer übergeordneten Organisationseinheit oder einem Stamm zu identifizieren.
- `organizations:ListAccountsForParent`— Ermöglicht Resource Explorer, die Konten in einer Organisation zu identifizieren, die im angegebenen Zielstamm oder in einer Organisationseinheit enthalten sind.
- `organizations:ListDelegatedAdministrators`— Ermöglicht Resource Explorer, die AWS Konten zu identifizieren, die in dieser Organisation als delegierte Administratoren bezeichnet wurden.
- `organizations:ListAWSServiceAccessForOrganization`— Ermöglicht Resource Explorer, eine Liste mit denjenigen zu identifizieren AWS-Services , die für die Integration in Ihre Organisation aktiviert wurden.
- `organizations:DescribeOrganization`— Ermöglicht Resource Explorer, Informationen über die Organisation abzurufen, zu der das Benutzerkonto gehört.
- `organizations:EnableAWSServiceAccess`— Ermöglicht Resource Explorer, die Integration eines AWS-Service (des Dienstes, der von spezifiziert ist`ServicePrincipal`) mit zu ermöglichen AWS Organizations.
- `organizations:DisableAWSServiceAccess`— Ermöglicht Resource Explorer, die Integration eines AWS-Service (des Dienstes, der von spezifiziert ist ServicePrincipal) mit zu deaktivieren AWS Organizations.
- `organizations:RegisterDelegatedAdministrator`— Ermöglicht Resource Explorer, das angegebene Mitgliedskonto zu aktivieren, um die Funktionen des angegebenen AWS Dienstes der Organisation zu verwalten.
- `organizations:DeregisterDelegatedAdministrator`— Ermöglicht Resource Explorer, das angegebene Mitglied AWS-Konto als delegierten Administrator für den angegebenen Benutzer zu entfernen. AWS-Service

- `iam:GetRole`— Ermöglicht Resource Explorer, Informationen über die angegebene Rolle abzurufen, einschließlich des Pfads, der GUID, des ARN und der Vertrauensrichtlinie der Rolle, die die Erlaubnis erteilt, die Rolle anzunehmen.
- `iam:CreateServiceLinkedRole`— Ermöglicht Resource Explorer, die erforderliche dienstbezogene Rolle zu erstellen, wenn Sie Resource Explorer aktivieren, indem Sie den ersten Index erstellen.

Die neueste Version dieser AWS verwalteten Richtlinie finden Sie `AWSResourceExplorerOrganizationsAccess` in der IAM-Konsole.

Resource Explorer aktualisiert AWS verwaltete Richtlinien

Hier finden Sie Details zu Aktualisierungen der AWS verwalteten Richtlinien für Resource Explorer, seit dieser Dienst diese Änderungen nachverfolgt hat. Wenn Sie automatische Benachrichtigungen über Änderungen an dieser Seite erhalten möchten, abonnieren Sie den RSS-Feed auf der Seite mit dem Dokumentverlauf von Resource Explorer.

Änderung	Beschreibung	Datum
AWSResourceExplorerServiceRolePolicy- Die Richtlinienberechtigungen wurden aktualisiert, um zusätzliche Ressourcentypen anzuzeigen	Resource Explorer hat der servicebezogenen Rollenrichtlinie Berechtigungen hinzugefügt `AWSResourceExplorerServiceRolePolicy`, die es Resource Explorer ermöglichen, zusätzliche Ressourcentypen anzuzeigen: • `apprunner:ListVpcConnectors` • `backup:ListReportPlans` • `emr-serverless:ListApplications`	12. Dezember 2023

Änderung	Beschreibung	Datum
	• events:ListEventBuses • geo:ListPlaceIndexes • geo:ListTrackers • greengrass:ListComponents • greengrass:ListComponentVersions • iot:ListRoleAliases • iottwinmaker:ListComponentTypes • iottwinmaker:ListEntities • iottwinmaker:ListScenes • kafka:ListConfigurations • kms:ListKeys • kinesisanalytics:ListApplications • lex:ListBots • lex:ListBotAliases • mediapackage-vod:ListPackagingConfigurations • mediapackage-vod:ListPackagingGroups • mq:ListBrokers • personalize:ListDatasetGroups	

Änderung	Beschreibung	Datum
	• `personalize:ListDatasets` • `personalize:ListSchemas` • `route53:ListHealthChecks` • `route53:ListHostedZones` • `secretsmanager:ListSecrets`	
Neue von verwaltete Richtlinie	Resource Explorer hat die folgende AWS verwaltete Richtlinie hinzugefügt: • AWSResourceExplorerOrganizationsAccess	14. November 2023
Aktualisierte von verwaltete Richtlinien	Resource Explorer hat die folgenden AWS verwalteten Richtlinien aktualisiert, um die Suche mit mehreren Konten zu unterstützen: • AWSResourceExplorerFullAccess • AWSResourceExplorerReadOnlyAccess	14. November 2023

Änderung	Beschreibung	Datum
AWSResourceExplorerServiceRolePolicy— Aktualisierte Richtlinie zur Unterstützung der Suche mit mehreren Konten bei Organizations	Resource Explorer hat der servicebezogenen Rollenrichtlinie Berechtigungen hinzugefügt`AWSResourceExplorerServiceRolePolicy`, die es dem Resource Explorer ermöglichen, die Suche mehrerer Konten mit Organizations zu unterstützen: • `organizations:ListAWSServiceAccessForOrganization` • `organizations:DescribeAccount` • `organizations:DescribeOrganization` • `organizations:ListAccounts` • `organizations:ListDelegatedAdministrators`	14. November 2023

Änderung	Beschreibung	Datum
AWSResourceExplorerServiceRolePolicy— Die Richtlinie wurde aktualisiert, um zusätzliche Ressourcentypen zu unterstützen	Resource Explorer hat der Richtlinie für dienstbezogene Rollen Berechtigungen hinzugefügt`AWSResourceExplorerServiceRolePolicy`, die es dem Dienst ermöglichen, die folgenden Ressourcentypen zu indizieren: • AccessAnalyzer: Analyzer • acmpca: Zertifizierungsstelle • amplifizieren: App • Amplify:Backend-Umgebung • Verstärken: Zweig • amplifizieren: Domänenzuweisung • amplifyuibuilder:Komponente • amplifyuibuilder:Thema • App-Integrationen: Eventintegration • AppRunner: Service • Appstream: Appblock • Appstream: Anwendung • Appstream: Flotte • Appstream: ImageBuilder • Appstream: Stack • appsync: graphqlapi • APS:RuleGroups-Namespace	17. Oktober 2023

Änderung	Beschreibung	Datum
	• aps:workspace • apigateway:restapi • apigateway:Bereitstellung • Athena: Datenkatalog • Athena:Arbeitsgruppe • Autoscaling: Autoscaling-Gruppe • Sicherung: Sicherungsplan • Batch: Computerumgebung • Batch:Job-Warteschlange • Batch:Planungsrichtlinie • Wolkenbildung: Stapel • Wolkenbildung: Stackset • Cloudfront: Verschlüs selungskonfiguration auf Feldebene • cloudfront: Verschlüs selungsprofil auf Feldebene • Cloudfront: ursprüngliche Zugriffskontrolle • Wolkenspur: Spur • Code-Artefakt: Domäne • Codeartefact:Repository • codecommit: Repository • Codeguru Profiler: Gruppe zur Profilerstellung • Codestar-Verbindungen: Verbindung • DataBrew: Datensatz • DataBrew: Rezept	

Änderung	Beschreibung	Datum
	• DataBrew: Regelsatz • Detektiv: Graph • Verzeichnisdienste: Verzeichnis • ec2: Carrier-Gateway • ec2: verifizierter Zugriffsendpunkt • ec2: verifizierte Zugriffsgruppe • ec2: verifizierte Zugriffsinstanz • ec2: verifizierter Access-Vertrauensanbieter • ecr: Repository • Elasticache:CacheSicherheitsgruppe • elastisches Dateisystem: Zugriffspunkt • Ereignisse: Regel • offensichtlich: Experiment • offensichtlich: Merkmal • offensichtlich: starten • offensichtlich: Projekt • finspace: Umgebung • Feuerwehrschlauch: Lieferstrom • Fehlerinjektionssimulator: Versuchsvorlage • Prognose: Datensatzgruppe • Prognose: Datensatz • Betrugserkennung: Detektor	

Änderung	Beschreibung	Datum
	• Betrugserkennung: Entitätstyp • Betrugsdetektor: Ereignistyp • Betrugserkennung: Etikett • Betrugserkennung: Ergebnis • Betrugserkennung: variabel • Gamelift: Alias • globaler Beschleuniger: Beschleuniger • globaler Beschleuniger: Endpunktgruppe • globaler Beschleuniger: Zuhörer • Glue: Datenbank • kleber:job • Kleber:Tabelle • Kleber:Auslöser • grünes Gras: Gruppe • Gesundheitssee: FHIR-Datenspeicher • Ich bin: virtuelles MFA-Gerät • ImageBuilderBuildversion • imagebuilder: Komponente • ImageBuilder: Container-Rezept • ImageBuilder: Distributionskonfiguration • ImageBuilder: ImageBuild-Version • ImageBuilder: Image-Pipeline	

Änderung	Beschreibung	Datum
	• imagebuilder: Bildrezept • ImageBuilder: Bild • imagebuilder: Infrastru kturkonfiguration • IoT: Autorisierer • iot: Jobvorlage • iot: Maßnahmen zur Schadensbegrenzung • iot: Vorlage für die Bereitste llung • iot: Sicherheitsprofil • iot: Ding • iot: Ziel der TopicRule • iotanalytics: Kanal • iotanalytics: Datensatz • iot analytics: Datenspeicher • iotanalytics: Pipeline • IoT-Ereignisse: Alarmmodell • IoT-Ereignisse: Detektorm odell • IoT-Ereignisse: Eingabe • iotsite: Assetmodel • iotsitewise: Anlage • iotsitewise: Gateway • iottwinmaker: Arbeitsbereich • ivs:Kanal • ivs:Streamkey • Kafka: Cluster • Kinesis-Video: Stream • Lambda: Alias	

Änderung	Beschreibung	Datum
	• Lambda: Layerversion • Lambda:Schicht • Lookout-Metriken: Warnung • lookoutvision: Projekt • Medienpaket: Kanal • Medienpaket: Originale ndpunkt • mediatailor: Wiedergab ekonfiguration • Memory-DB: ACL • memorydb:cluster • memorydb:Parameter gruppe • memorydb:Benutzer • Mobiles Targeting: App • Mobiles Targeting: Segment • Mobiles Targeting: Vorlage • Netzwerkfirewall: Firewall-Richtlinie • Netzwerk-Firewall: Firewall • Netzwerkmanager: globales Netzwerk • Netzwerkmanager: Gerät • Netzwerkmanager: Link • Netzwerkmanager: Anlage • Netzwerkmanager: Kernnetzwerk • Panorama: Paket • qldb: Journalkinesis-Str eams für Ledger	

Änderung	Beschreibung	Datum
	• qldb: Hauptbuch • rds: blaugrünes Deployment • RefactorSpaces: Anwendung • RefactorSpaces: Umgebung • RefactorSpaces: Route • RefactorSpaces: Dienst • rekognition: Projekt • Resilience Hub: App • Resiliencehub: Resilienz politik • Ressourcengruppen: Gruppe • Route 53: Wiederher stellungsgruppe • Route 53: Ressourcensatz • Route53: Firewall-Domäne • Route53: Firewall-Regelgruppe • Route53: Resolver-Endpunkt • Route53: Resolver-Regel • Sagemaker: Modell • Sagemaker: Notebook-Instanz • Unterzeichner: Profil signieren • SSM-Vorfälle: Reaktions plan • ssm: Inventareintrag	

Änderung	Beschreibung	Datum
	• ssm: Ressourcendatensynchronisierung • Staaten: Aktivität • Zeitstrom: Datenbank • Weisheit: Assistent • Weisheit: Assistenzverein • Weisheit: Wissensbasis	

Änderung	Beschreibung	Datum
AWSResourceExplorerServiceRolePolicy— Die Richtlinie wurde aktualisiert, um zusätzliche Ressourcentypen zu unterstützen	Resource Explorer hat der Richtlinie für dienstbezogene Rollen Berechtigungen hinzugefügt`AWSResourceExplorerServiceRolePolicy`, die es dem Dienst ermöglichen, die folgenden Ressourcentypen zu indizieren: • codebuild:project • Code-Pipeline: Pipeline • Cognito: Identitätspool • Cognito: Benutzerpool • ecr: Repository • efs:Dateisystem • Elastic Beanstalk: Anwendung • Elastic Beanstalk: Anwendungsversion • Elastic Beanstalk: Umgebung • IoT: Richtlinie • iot:themenregel • Schrittfunktionen: Zustandsmaschine • s3: Eimer	1. August 2023

Änderung	Beschreibung	Datum
AWSResourceExplorerServiceRolePolicy— Die Richtlinie wurde aktualisiert, um zusätzliche Ressourcentypen zu unterstützen	Resource Explorer hat der Richtlinie für dienstbezogene Rollen Berechtigungen hinzugefügt`AWSResourceExplorerServiceRolePolicy`, die es dem Dienst ermöglichen, die folgenden Ressourcentypen zu indizieren: • Elasticache: Cluster • Elasticache: globale Replikationsgruppe • Elasticache: Parametergruppe • Elasticache: Replikationsgruppe • Elasticache:Reservierte Instanz • Elasticache:Schnappschuss • Elasticache:Subnetzgruppe • Elasticache:Benutzer • Elasticache:Benutzergruppe • Lambda: Konfiguration für Codesignatur • Lambda: Zuordnung der Ereignisquellen • sqs: Warteschlange	7. März 2023

Änderung	Beschreibung	Datum
Neue verwaltete Richtlinien	Resource Explorer hat die folgenden AWS verwalteten Richtlinien hinzugefügt: • AWSResourceExplorerFullAccess • AWSResourceExplorerReadOnlyAccess • AWSResourceExplorerServiceRolePolicy	7. November 2022
Resource Explorer hat begonnen, Änderungen zu verfolgen	Resource Explorer hat damit begonnen, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	7. November 2022

Verwenden von serviceverknüpften Rollen für Resource Explorer

AWS Ressourcen Explorer verwendet AWS Identity and Access Management (IAM) dienstbezogene Rollen. Eine dienstverknüpfte Rolle ist ein einzigartiger IAM Rollentyp, der direkt mit Resource Explorer verknüpft ist. Dienstbezogene Rollen sind von Resource Explorer vordefiniert und beinhalten alle Berechtigungen, die der Dienst benötigt, um andere Rollen in Ihrem Namen AWS-Services aufzurufen.

Eine dienstverknüpfte Rolle erleichtert die Konfiguration von Resource Explorer, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Resource Explorer definiert die Berechtigungen seiner dienstbezogenen Rollen, und sofern nicht anders definiert, kann nur Resource Explorer seine Rollen übernehmen. Die definierten Berechtigungen umfassen sowohl die Vertrauensrichtlinie als auch die Berechtigungsrichtlinie, und diese Berechtigungsrichtlinie kann keiner anderen IAM Entität zugewiesen werden.

Informationen zu anderen Diensten, die dienstbezogene Rollen unterstützen, finden Sie IAM im IAMBenutzerhandbuch unter AWS Services that work with. Suchen Sie dort in der Spalte Dienstbezogene Rollen nach den Diensten, für die Ja angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Berechtigungen für dienstbezogene Rollen für Resource Explorer

Resource Explorer verwendet die mit dem Dienst verknüpfte Rolle mit dem Namen. `AWSServiceRoleForResourceExplorer` Diese Rolle gewährt dem Resource Explorer-Dienst die Berechtigung, Ressourcen und AWS CloudTrail Ereignisse in AWS-Konto Ihrem Namen anzuzeigen und diese Ressourcen zu indizieren, um die Suche zu unterstützen.

Die mit dem Dienst `AWSServiceRoleForResourceExplorer` verknüpfte Rolle vertraut nur dem Dienst, bei dem der folgende Dienstprinzipal die Rolle übernimmt:

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

Die genannte Rollenberechtigungsrichtlinie AWSResourceExplorerServiceRolePolicy ermöglicht Resource Explorer nur Lesezugriff, um Ressourcennamen und Eigenschaften für unterstützte Ressourcen abzurufen. AWS Informationen zu den Diensten und Ressourcen, die Resource Explorer unterstützt, finden Sie unter Ressourcentypen, nach denen Sie mit Resource Explorer suchen können. Eine vollständige Liste aller Aktionen, die diese Rolle ausführen kann, finden Sie in der `AWSResourceExplorerServiceRolePolicy` Richtlinie in der IAM Konsole.

Ein Principal ist eine IAM Entität wie ein Benutzer, eine Gruppe oder eine Rolle. Wenn Sie Resource Explorer beim Erstellen des Indexes in der ersten Region des Kontos die dienstbezogene Rolle für Sie erstellen lassen, benötigt der Principal, der die Aufgabe ausführt, nur die Berechtigungen, die zum Erstellen des Resource Explorer-Indexes erforderlich sind. Um die dienstverknüpfte Rolle manuell mithilfe von zu erstellenIAM, muss der Principal, der die Aufgabe ausführt, über die Berechtigung zum Erstellen einer dienstbezogenen Rolle verfügen. Weitere Informationen finden Sie im Benutzerhandbuch unter Berechtigungen für dienstverknüpfte Rollen. IAM

Eine dienstverknüpfte Rolle für Resource Explorer erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie den Resource Explorer im aktivieren oder den AWS Management Console ersten CreateIndex AWS-Region in Ihrem Konto mit dem AWS CLI oder einem ausführen AWS API, erstellt Resource Explorer die dienstbezogene Rolle für Sie.

Wenn Sie diese serviceverknüpfte Rolle löschen und dann erneut erstellen müssen, können Sie die Rolle in Ihrem Konto mit demselben Verfahren neu anlegen. Wenn Sie sich RegisterResourceExplorerin der ersten Region Ihres Kontos befinden, erstellt Resource Explorer die dienstbezogene Rolle erneut für Sie.

Bearbeitung einer dienstbezogenen Rolle für Resource Explorer

Mit Resource Explorer können Sie die `AWSServiceRoleForResourceExplorer` dienstverknüpfte Rolle nicht bearbeiten. Nachdem Sie eine serviceverknüpfte Rolle erstellt haben, können Sie den Namen der Rolle nicht mehr ändern, da verschiedene Entitäten auf die Rolle verweisen könnten. Sie können die Beschreibung der Rolle jedoch mithilfe IAM von bearbeiten. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Bearbeiten einer dienstbezogenen Rolle.

Löschen einer dienstverknüpften Rolle für Resource Explorer

Sie können die IAM Konsole, die oder die verwenden AWS CLI, AWS API um die dienstverknüpfte Rolle manuell zu löschen. Dazu müssen Sie zuerst die Resource Explorer-Indizes aus allen Indizes AWS-Region in Ihrem Konto entfernen. Anschließend können Sie die dienstverknüpfte Rolle manuell löschen.

> **Note**
>
> Wenn der Resource Explorer-Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen fehl. Stellen Sie in diesem Fall sicher, dass alle Indizes aus allen Regionen gelöscht wurden, warten Sie dann einige Minuten und wiederholen Sie den Vorgang.

Um die mit dem Service verknüpfte Rolle manuell zu löschen, verwenden Sie IAM

Verwenden Sie die IAM Konsole, den oder AWS CLI, AWS API um die `AWSServiceRoleForResourceExplorer` dienstverknüpfte Rolle zu löschen. Weitere Informationen finden Sie im IAMBenutzerhandbuch unter Löschen einer dienstbezogenen Rolle.

Unterstützte Regionen für dienstverknüpfte Resource Explorer-Rollen

Resource Explorer unterstützt die Verwendung von dienstbezogenen Rollen in allen Regionen, in denen der Dienst verfügbar ist. Weitere Informationen finden Sie unter AWS-Service -Endpunkte in Allgemeine Amazon Web Services-Referenz.

Problembehandlung bei AWS Ressourcen Explorer Berechtigungen

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Resource Explorer und AWS Identity and Access Management (IAM) auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion im Resource Explorer auszuführen
- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Resource Explorer-Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion im Resource Explorer auszuführen

Wenn Ihnen AWS Management Console mitgeteilt wird, dass Sie nicht berechtigt sind, eine Aktion auszuführen, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator ist die Person, die Ihnen die Anmeldeinformationen zur Verfügung gestellt hat, mit denen Sie diesen Vorgang versucht haben.

Der folgende Fehler tritt beispielsweise auf, wenn jemand, der die IAM-Rolle annimmt, `MyExampleRole` versucht, die Konsole zu verwenden, um Details zu einer Ansicht anzuzeigen, aber nicht `resource-explorer-2:GetView` dazu berechtigt ist.

```
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 diesem Fall muss die Person, die die Rolle verwendet, den Administrator bitten, die Berechtigungsrichtlinien der Rolle zu aktualisieren, um mithilfe der `resource-explorer-2:GetView` Aktion Zugriff auf die Ansicht zu gewähren.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Resource Explorer-Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Resource Explorer diese Funktionen unterstützt, finden Sie unterSo funktioniert Resource Explorer mit IAM.

- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Datenschutz in AWS Ressourcen Explorer

Das Modell der AWS gemeinsamen Verantwortung und geteilter Verantwortung gilt für den Datenschutz in AWS Ressourcen Explorer. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie im Abschnitt Datenschutz FAQ. Informationen zum Datenschutz in Europa finden Sie im AWS Shared Responsibility Model und im GDPR Blogbeitrag im AWS Security Blog.

Aus Datenschutzgründen empfehlen wir, dass Sie Ihre AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto eine Multi-Faktor-Authentifizierung (MFA).
- Verwenden SieSSL/TLS, um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Einrichtung API und Protokollierung von Benutzeraktivitäten mit AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.

- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie FIPS 140-3 validierte kryptografische Module für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine benötigenAPI, verwenden Sie einen Endpunkt. FIPS Weitere Informationen zu den verfügbaren FIPS Endpunkten finden Sie unter Federal Information Processing Standard () 140-3. FIPS

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Resource Explorer oder anderen Geräten AWS-Services über die Konsole arbeiten,API, AWS CLI oder. AWS SDKs Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie einem externen Server eine URL zur Verfügung stellen, empfehlen wir dringend, dass Sie keine Anmeldeinformationen in den angebenURL, um Ihre Anfrage an diesen Server zu überprüfen.

Verschlüsselung im Ruhezustand

Zu den vom Resource Explorer gespeicherten Daten gehören die indizierte Liste der Ressourcen und der zugehörigen RessourcenARNs, die vom Kunden verwendet werden, sowie die Ansichten, um auf sie zuzugreifen.

Diese Daten werden im Ruhezustand mithilfe von AWS Key Management Service (AWS KMS) symmetrischen Verschlüsselungsschlüsseln verschlüsselt, die den Advanced Encryption Standard (AES) im Galois Counter Mode () mit 256-Bit-Schlüsseln (-256-GCM) implementieren. AES GCM

Verschlüsselung während der Übertragung

Kundenanfragen und alle zugehörigen Daten werden bei der Übertragung mit Transport Later Security () 1.2 oder höher verschlüsselt. TLS Alle Resource Explorer-Endpunkte unterstützen HTTPS die Verschlüsselung von Daten während der Übertragung. Eine Liste der Resource Explorer-Dienstendpunkte finden Sie unter AWS Ressourcen Explorer Endpunkte und Kontingente in der. Allgemeine AWS-Referenz

Compliance-Validierung für AWS Ressourcen Explorer

Informationen darüber, ob AWS-Service ein in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie AWS-Servicesunter Umfang nach Compliance-Programmen. Allgemeine Informationen finden Sie unter AWS-Compliance-Programme.

Sie können Auditberichte von Drittanbietern unter AWS Artifact herunterladen. Weitere Informationen finden Sie unter Herunterladen von Berichten im von Berichten AWS Artifact im AWS ArtifactBenutzerhandbuch.

Ihre Verantwortung für die Einhaltung von Vorschriften bei der Verwendung von Resource Explorer hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWSstellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung von Vorschriften unterstützen:

- Schnellstartanleitungen für Sicherheit und Compliance – In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Bereitstellung von sicherheits- und konformitätsorientierten Basisumgebungen auf AWS angegeben.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

> **Note**
>
> AWS-ServicesNicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- AWS-Compliance-Ressourcen – Diese Arbeitsbücher und Leitfäden könnten für Ihre Branche und Ihren Standort relevant sein.
- Evaluieren von Ressourcen mit Regeln im AWS Config-Entwicklerhandbuch – AWS Config bewertet, wie gut Ihre Ressourcenkonfigurationen mit internen Praktiken, Branchenrichtlinien und Vorschriften übereinstimmen.
- AWS Security Hub – Dieser AWS-Dienst liefert einen umfassenden Überblick über den Sicherheitsstatus in AWS. So können Sie die Compliance mit den Sicherheitsstandards in der Branche und den bewährten Methoden abgleichen.

Ausfallsicherheit in AWS Ressourcen Explorer

Im Zentrum derAWS globalen -Infrastruktur stehen Availability Zones (AWS-RegionenVerfügbarkeitszonen, AZs). Regionen stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz und hohen Durchsätzen verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne

dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen über AWS-Regionen und Availability Zones finden Sie unter Globale AWS-Infrastruktur.

Infrastruktursicherheit in AWS Ressourcen Explorer

Als verwalteter Dienst AWS Ressourcen Explorer ist er durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API Aufrufe, um über das Netzwerk auf Resource Explorer zuzugreifen. Kunden müssen Folgendes unterstützen:

- Sicherheit auf Transportschicht (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Cipher-Suites mit perfekter Vorwärtsgeheimhaltung (PFS) wie (Ephemeral Diffie-Hellman) oder DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Darüber hinaus müssen Anfragen mithilfe einer Zugriffsschlüssel-ID und eines geheimen Zugriffsschlüssels, der einem Prinzipal zugeordnet ist, signiert werden. IAM Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Weitere Informationen zu AWS globalen Netzwerksicherheitsverfahren finden Sie im Whitepaper Amazon Web Services: Sicherheitsprozesse im Überblick.

Überwachung von AWS Ressourcen Explorer

Die Überwachung ist eine wichtige Komponente für die Wahrung der Zuverlässigkeit, Verfügbarkeit und Leistung vonAWS Ressourcen Explorer und Ihrer anderenAWS Lösungen. AWSstellt die folgenden Überwachungstools bereit, um Resource Explorer zu überwachen, zu melden, wenn etwas nicht in Ordnung ist, und gegebenenfalls automatische Aktionen durchzuführen:

- AWS CloudTrail erfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS-Konto-Kontos erfolgten, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon-S3-Bucket. Sie können die Benutzer und Konten, die AWS aufgerufen haben, identifizieren, sowie die Quell-IP-Adresse, von der diese Aufrufe stammen, und den Zeitpunkt der Aufrufe ermitteln. Weitere Informationen finden Sie im Protokollieren von AWS Ressourcen Explorer-API-Aufrufen mithilfe von AWS CloudTrail und dem AWS CloudTrail-Benutzerhandbuch.

Protokollieren von AWS Ressourcen Explorer-API-Aufrufen mithilfe von AWS CloudTrail

AWS Ressourcen Explorerist in integriertAWS CloudTrail, einem Service, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem durchgeführten AktionenAWS-Service im Resource Explorer bereitstellt. CloudTrail erfasst alle API-Aufrufe für Resource Explorer als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe über die Resource Explor-Konsole und Codeaufrufe der Resource Explor-API-Operationen.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon-S3-Bucket, einschließlich Ereignissen für Resource Explorer, aktivieren. Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. Auch wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail -Konsole in Event history (Ereignisverlauf) anzeigen. Mit den von CloudTrail gesammelten Informationen können Sie die an Resource Explorer gestellte Anfrage, die IP-Adresse, von der die Anforderung gestellt wurde, den Initiator sowie den Zeitpunkt der Anforderung und zusätzliche Details bestimmen.

Weitere Informationen CloudTrail finden Sie im AWS CloudTrailBenutzerhandbuch.

Informationen zum Resource Explorer in CloudTrail

CloudTrail wirdAWS-Konto beim Erstellen Ihres für Sie aktiviert. Wenn eine Aktivität in Resource Explorer auftritt, wird diese Aktivität in einem CloudTrail Ereignis zusammen mit anderenAWS-Service Ereignissen in Ereignisverlauf protokolliert. Sie können die neusten Ereignisse in Ihr(em) AWS-Konto anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail -Ereignisverlauf.

> **Important**
>
> Sie können alle Resource Explorer-Ereignisse finden, indem Sie nach Event source = resource-explorer-2.amazonaws.com suchen

Um die Ereignisse in IhremAWS-Konto einschließlich Ereignissen für den Resource Explorer kontinuierlich aufzuzeichnen, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Bereitstellung von Protokolldateien in einem Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon S3 Bucket bereit. Darüber hinaus können Sie andere konfigurieren,AWS-Services um die in den CloudTrail -Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie in folgenden Themen im AWS CloudTrail-Benutzerhandbuch:

- Erstellen eines Trails für AWS-Konto
- AWSServiceintegrationen mit CloudTrail Logs
- Konfigurieren von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen
- Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle -Aktionen werden von Resource Explorer protokolliert CloudTrail und sind in der AWS Ressourcen Explorer-API-Referenz dokumentiert. Beispielsweise generieren Aufrufe der`UpdateIndex` Aktionen`CreateIndex`,`DeleteIndex`, und und Einträge in den CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen, anhand derer Sie feststellen können, wer die Anfrage gestellt hat.

- AWS-KontoAnmeldeinformationen
- Temporäre Sicherheits-Anmeldeinformationen von einer AWS Identity and Access Management (IAM)-Rolle oder einem Verbundbenutzer.
- Langfristige Sicherheits-Anmeldeinformation eines IAM-Benutzers.
- Ein anderer AWS-Service.

> **Important**
>
> Aus Sicherheitsgründen werden alle`Tags` und`QueryString` -Werte aus den CloudTrail Traileinträgen redigiert.`Filters`

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Grundlagen zu -Protokolldateieinträgen

Ein Trail ist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. CloudTrail Protokolldateien können einen oder mehrere Einträge enthalten. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. CloudTrail Protokolldateien sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher in keiner bestimmten Reihenfolge.

Themen

- CreateIndex
- DeleteIndex
- UpdateIndexType
- Suche
- CreateView
- DeleteView
- DisassociateDefaultView

CreateIndex

Das folgende Beispiel zeigt einen CloudTrail -Protokolleintrag, der die`CreateIndex` Aktion demonstriert.


```
{
    "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

Das folgende Beispiel zeigt einen CloudTrail langen Eintrag, der die`DeleteIndex` Aktion demonstriert.

> **Note**
>
> Diese Aktion löscht auch asynchron alle Ansichten für das Konto in dieser Region, was zu einem`DeleteView` Ereignis für jede gelöschte Ansicht führt.

```
{
    "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

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die`UpdateIndexType` Aktion veranschaulicht, mit der ein Index vom Typ auf den Index`LOCAL` heraufgestuft wird`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"
```

```
}
```

Suche

Das folgende Beispiel zeigt einen CloudTrail -Protokolleintrag, der die`Search` Aktion demonstriert.

> **Note**
>
> Aus Sicherheitsgründen werden alle Verweise auf`TagFilters`, und`QueryString` Parameter in den CloudTrail Traileinträgen geschwärzt.

```
{
    "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

Das folgende Beispiel zeigt einen CloudTrail -Protokolleintrag, der die`CreateView` Aktion demonstriert.

```
{
    "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

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der das Ereignis veranschaulicht, das eintreten kann, wenn die`DeleteView` Aktion aufgrund eines`DeleteIndex` Vorgangs in derselben Aktion automatisch gestartet wirdAWS-Region.

> **Note**
>
> Wenn die gelöschte Ansicht die Standardansicht für die Region ist, wird die Verknüpfung der Ansicht durch diese Aktion ebenfalls asynchron als Standardansicht aufgehoben. Dadurch entsteht ein`DisassociateDefaultView` Ereignis.


```
{
    "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

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der das Ereignis veranschaulicht, das eintreten kann, wenn die`DisassociateDefaultView` Aktion aufgrund eines`DeleteView` Vorgangs in der aktuellen Standardansicht automatisch gestartet wird.

```
{
    "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"
}
```

Fehlerbehebung bei Resource Explorer

Wenn bei der Arbeit mit Resource Explorer aufgetreten ist, finden Sie Sie Sie Sie Sie die Themen in diesem Abschnitt weitere Informationen. Weitere Informationen finden Sie auchProblembehandlung bei AWS Ressourcen Explorer Berechtigungen im Abschnitt Sicherheit dieses Handbuchs.

Themen

- Allgemeine Probleme(diese Seite)
- Behebung von Setup- und Konfigurationsproblemen von Resource Explorer
- Behebung von Suchproblemen im Resource Explorer

Allgemeine Probleme

Themen

- Ich habe einen Link zum Resource Explorer erhalten, aber wenn ich ihn öffne, zeigt die Konsole nur einen Fehler an.
- Warum verursacht die vereinheitlichte Suche in der Konsole die Fehlermeldung „Zugriff verweigert“ in meinen CloudTrail Logs?

Ich habe einen Link zum Resource Explorer erhalten, aber wenn ich ihn öffne, zeigt die Konsole nur einen Fehler an.

Einige Tools von Drittanbietern erzeugen Link-URLs zu Seiten im Resource Explorer. In einigen Fällen enthalten diese URLs nicht den Parameter, der die Konsole an eine bestimmte Stelle weiterleitetAWS-Region. Wenn Sie einen solchen Link öffnen, wird der Resource Explorer-Konsole nicht mitgeteilt, welche Region verwendet werden soll, und sie verwendet standardmäßig die Region, in der sich der Benutzer zuletzt angemeldet hat. Wenn der Benutzer in dieser Region nicht über die Berechtigungen für den Zugriff auf Resource Explorer verfügt, versucht die Konsole, die Region USA Ost (Nord-Virginia) (`us-east-1`) oder USA West (Oregon) (`us-west-2`) zu verwenden, falls die Konsole keine Verbindung herstellen kann`us-east-1`.

Wenn der Benutzer keine Berechtigung hat, in einer dieser Regionen zu finden, gibt Sie die Resource Explorer-Konsole eine Fehlermeldung.

Sie können dieses Problem verhindern, indem Sie sicherstellen, dass alle Benutzer über die folgenden Berechtigungen verfügen:

- `ListIndexes`— keine spezifische Ressource; Verwendung`*`.
- `GetIndex`für den ARN der einzelnen im Konto erstellten Indizes. Um zu vermeiden, dass Sie die Berechtigungsrichtlinien wiederholen müssen, wenn Sie einen Index löschen und neu erstellen, empfehlen wir Ihnen, diese zu verwenden`*`.

Die Mindestrichtlinie, um dies zu erreichen, könnte beispielsweise wie folgt aussehen:

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

Alternativ könnten Sie erwägen, die AWSverwaltete Berechtigung allen Benutzern`AWSResourceExplorerReadOnlyAccess` zuzuweisen, die Resource Explorer verwenden müssen. Dadurch werden diese erforderlichen Berechtigungen sowie die erforderlichen Berechtigungen gewährt, um die verfügbaren Ansichten in der Region anzuzeigen und anhand dieser Ansichten zu suchen.

Warum verursacht die vereinheitlichte Suche in der Konsole die Fehlermeldung „Zugriff verweigert“ in meinen CloudTrail Logs?

AWS Management ConsoleMit der vereinheitlichten Suche in der können Prinzipale von jeder Seite in der aus suchenAWS Management Console. Die Ergebnisse können Ressourcen aus dem Konto des Prinzipals enthalten, wenn Resource Explorer aktiviert und für die Unterstützung einer einheitlichen Suche konfiguriert ist. Immer wenn Sie mit der Eingabe in die vereinheitlichte Suchleiste beginnen, versucht Unified Search, den`resource-explorer-2:ListIndexes` Vorgang aufzurufen, um zu überprüfen, ob Ressourcen aus dem Benutzerkonto in die Ergebnisse aufgenommen werden können.

Die einheitliche Suche verwendet die Berechtigungen des aktuell angemeldeten Benutzers, um diese Überprüfung durchzuführen. Wenn diesem Benutzer in einer angehängtenAWS Identity and Access Management (IAM) -Berechtigungsrichtlinie keine Berechtigung zum Anrufen`resource-explorer-2:ListIndexes` gewährt wurde, schlägt die Prüfung fehl. Dieser Fehler wird als`Access denied` Eintrag in Ihre CloudTrail Protokolle aufgenommen.

Dieser CloudTrail Logeintrag hat die folgenden Merkmale:

- Quelle des Ereignisses:`resource-explorer-2.amazonaws.com`
- Name der Veranstaltung:`ListIndexes`
- Fehlercode:`403` (Zugriff verweigert)

Die folgendenAWS verwalteten Richtlinien beinhalten die Erlaubnis zum Anrufen`resource-explorer-2:ListIndexes`. Wenn Sie eine dieser Richtlinien dem Principal oder einer anderen Richtlinie zuweisen, die diese Berechtigung beinhaltet, tritt dieser Fehler nicht auf:

- AWSResourceExplorerReadOnlyAccess
- AWSResourceExplorerFullAccess
- ReadOnlyAccess
- ViewOnlyAccess

Behebung von Setup- und Konfigurationsproblemen von Resource Explorer

Verwenden Sie die hier aufgeführten Informationen, um Probleme bei der oder oder oder oder oder oder oder oder oder oder oder oder oder oder oder oder oder oder (,)AWS Ressourcen Explorer.

Themen

- Ich erhalte eine Meldung, dass der Zugriff verweigert wird, wenn ich eine Anfrage an den Resource Explorer stelle
- Ich erhalte eine Meldung, dass der Zugriff verweigert wird, wenn ich eine Anfrage mit temporären Sicherheitsanmeldeinformationen erstelle

Ich erhalte eine Meldung, dass der Zugriff verweigert wird, wenn ich eine Anfrage an den Resource Explorer stelle

- Stellen Sie sicher, dass Sie über die Berechtigungen zum Aufder und die Sie angefordert haben, verfügen. Ein Administrator kann Berechtigungen gewähren, indem er Ihrem IAM-Prinzip eineAWS Identity and Access Management (IAM) -Berechtigungsrichtlinie zuweist, z. B. einer Rolle, Gruppe oder Benutzer.

  Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

  - Benutzer und Gruppen in AWS IAM Identity Center:

    Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center-Benutzerhandbuch.

  - Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

    Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch.

  - IAM-Benutzer:

    - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer im IAM-Benutzerhandbuch.
    - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

  Die Richtlinie muss die angeforderte`Action` Seite zulassen, auf`Resource` die Sie zugreifen möchten.

  Wenn die Richtlinienerklärungen, die diese Berechtigungen gewähren, Bedingungen enthalten, wie z. time-of-day B. IP-Adresseinschränkungen, müssen Sie diese Anforderungen auch erfüllen, wenn Sie die Anfrage senden. Informationen zum Anzeigen oder zum Ändern von Richtlinien für einen IAM-Prinzipal finden Sie unter IAM-Richtlinien im IAM-Benutzerhandbuch.

- Wenn Sie API-Anfragen manuell (ohne die AWSSDKs), stellen Sie sicher, dass Sie die Anfrage korrekt signieren haben.

Ich erhalte eine Meldung, dass der Zugriff verweigert wird, wenn ich eine Anfrage mit temporären Sicherheitsanmeldeinformationen erstelle

- Stellen Sie sicher, dass der IAM-Prinzip, das Sie zum Erstellen der Anfrage verwenden, über die entsprechenden Berechtigungen verfügt, über die entsprechenden Berechtigungen verfügt. Berechtigungen für temporäre Sicherheitsanmeldeinformationen werden von einem in IAM abgeleitet, sodass die Berechtigungen auf die Berechtigungen des entsprechenden Prinzials beschränkt sind. Weitere Informationen zum Festlegen von Berechtigungen für temporäre Sicherheitsanmeldeinformationen finden Sie unter Steuern für temporäre Sicherheitsanmeldeinformationen im IAM-Benutzerhandbuch.
- Stellen Sie sicher, dass Ihre Anfragen korrekt signiert sind und die Anfrage richtig aufgebaut ist. Einzelheiten finden Sie in der Toolkit-Dokumentation für das von Ihnen gewählte SDK oder Verwenden temporärer Anmeldeinformationen mitAWS Ressourcen im IAM-Benutzerhandbuch.
- Stellen Sie sicher, dass die temporären Sicherheitsanmeldeinformationen nicht abgelaufen sind. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Anfordern temporärer Sicherheitsanmeldeinformationen.

Behebung von Suchproblemen im Resource Explorer

Mithilfe dieser Informationen können Sie häufig auftretende Fehler diagnostizieren und beheben, die bei der Suche nach Ressourcen mithilfe des Resource Explorers auftreten können.

Themen

- Warum fehlen einige Ressourcen in meinen Resource Explorer-Suchergebnissen?
- Warum werden meine Ressourcen nicht in den vereinheitlichten Suchergebnissen in der Konsole angezeigt?
- Warum führt die einheitliche Suche in der Konsole und im Resource Explorer manchmal zu unterschiedlichen Ergebnissen?
- Welche Berechtigungen benötige ich, um nach Ressourcen suchen zu können?

Warum fehlen einige Ressourcen in meinen Resource Explorer-Suchergebnissen?

Die folgende Liste enthält Gründe, warum einige Ressourcen möglicherweise nicht wie erwartet in Ihren Suchergebnissen angezeigt werden:

Die anfängliche Indizierung ist nicht abgeschlossen

Nachdem Sie Resource Explorer in einem zum ersten Mal aktiviert haben AWS-Region, kann es bis zu 36 Stunden dauern, bis die Indizierung und Replikation in den Aggregatorindex abgeschlossen ist. Versuchen Sie Ihre Suche später erneut.

Die Ressource ist neu

Es kann einige Minuten dauern, bis eine neue Ressource vom Resource Explorer erkannt und dem lokalen Index hinzugefügt wird. Versuchen Sie es in ein paar Minuten erneut.

Informationen über eine neue Ressource in einer Region wurden noch nicht an den Aggregatorindex weitergegeben

Es kann einige Zeit dauern, bis Details zu einer neuen Ressource, die in einer Region entdeckt wurde, in ihrer eigenen Region indexiert und dann in den Aggregatorindex für das Konto repliziert werden. Die neue Ressource kann erst nach Abschluss der Replikation in regionsübergreifenden Suchergebnissen angezeigt werden. Versuchen Sie Ihre Suche später erneut.

In der Region mit der Ressource ist der Resource Explorer nicht aktiviert

Ihr Administrator legt fest AWS-Regionen , in welchem Bereich der Resource Explorer ausgeführt werden kann. Auf der Seite „Einstellungen“ wird angezeigt, in welchen Regionen der Resource Explorer aktiviert ist und welche Regionen einen Index enthalten. Wenn die Region mit Ihrer Ressource nicht aktiviert ist, bitten Sie Ihren Administrator, den Resource Explorer in dieser Region zu aktivieren.

Die Ressource ist in einer anderen Region vorhanden, und die gesuchte Region enthält den Aggregatorindex nicht

Sie können in allen Regionen des Kontos nur dann nach Ressourcen suchen, wenn Sie eine Ansicht in der Region verwenden, die den Aggregatorindex enthält. Bei Suchen in einer anderen Region werden nur Ressourcen aus der Region zurückgegeben, in der Sie die Suche durchführen.

Filter in der Ansicht schließen diese Ressource aus

Jede Ansicht kann Filter in der Konfiguration enthalten, die einschränken, welche Ergebnisse in die mit dieser Ansicht erstellten Suchergebnisse aufgenommen werden können. Stellen Sie sicher, dass die gesuchte Ressource den Filtern in der Ansicht entspricht, die Sie für die Suche verwenden. Weitere Informationen zu Filtern finden Sie unterFilter.

Der Ressourcentyp wird vom Resource Explorer nicht unterstützt

Einige Ressourcentypen werden vom Resource Explorer nicht unterstützt. Weitere Informationen finden Sie unter Ressourcentypen, nach denen Sie mit Resource Explorer suchen können.

Indizes oder Ansichten sind in der Konsolenregion nicht konfiguriert

Wenn die Indizes oder Ansichten nicht in den Regionen konfiguriert sind, die von der Konsole erwartet werden, die das Widget verwendet, werden Sie nicht die erwarteten Ergebnisse sehen. Weitere Informationen finden Sie unter Aktivierung der regionsübergreifenden Suche durch Erstellen eines Aggregatorindexes.

Ihre Ansichten enthalten keine Tags

Tags sind für das Resource Explorer-Widget erforderlich. Wenn Ihre Ansichten keine Tags enthalten, werden die Ressourcen nicht in Ihre Ergebnisse aufgenommen. Weitere Informationen finden Sie unter Hinzufügen von Markern zu Ansichten zu Ansichten hinzu.

Ihre Suche verwendet die falsche Suchabfragesyntax

Die Suche im Resource Explorer ist für diesen Dienst einzigartig. Ohne die richtige Syntax werden Sie nicht die Ressourcen finden, die Sie erwarten. Weitere Informationen finden Sie unter Syntaxreferenz für Suchabfragen für Resource Explorer.

Sie haben kürzlich Ihre Ressourcen mit Tags versehen

Nachdem Sie eine Ressource markiert haben, dauert es 30 Sekunden, bis die Ressource in Ihren Suchergebnissen angezeigt wird.

Der Ressourcentyp unterstützt keine Tag-Filter

Wenn Tagfilter vom Ressourcentyp nicht unterstützt werden, werden sie nicht im Resource Explorer-Widget angezeigt. Folgende Ressourcentypen unterstützen keine Tag-Filter:

- `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`

Warum werden meine Ressourcen nicht in den vereinheitlichten Suchergebnissen in der Konsole angezeigt?

Einheitliche Suchergebnisse sind in der Suchleiste oben auf jeder AWS Management Console Seite verfügbar. Die Suche kann jedoch erst dann Ressourcen zurückgeben, die der Abfrage in den Suchergebnissen entsprechen, wenn die folgenden Konfigurationsoptionen abgeschlossen sind:

- In einer der Regionen des Kontos muss ein Aggregatorindex vorhanden sein.
- In der Region, die den Aggregatorindex enthält, muss es eine Standardansicht geben.
- Alle Principals (IAMRollen und Benutzer) müssen über die Berechtigung verfügen, mithilfe dieser Standardansicht zu suchen.

Warum führt die einheitliche Suche in der Konsole und im Resource Explorer manchmal zu unterschiedlichen Ergebnissen?

Einheitliche Suchergebnisse sind in der Suchleiste oben auf jeder AWS Management Console Seite verfügbar. Wenn Sie die einheitliche Suche verwenden, fügt der einheitliche Suchvorgang

automatisch ein Platzhalterzeichen (*) am Ende des ersten Begriffs ein, den Sie in die Abfragezeichenfolge eingeben. Dieses Platzhalterzeichen ist im einheitlichen Suchfeld nicht sichtbar, wirkt sich jedoch auf die Ergebnisse aus.

> **Important**
>
> Bei der einheitlichen Suche wird am Ende des ersten Schlüsselworts in der Zeichenfolge automatisch ein Platzhalterzeichen (*) eingefügt. Das bedeutet, dass vereinheitlichte Suchergebnisse Ressourcen enthalten, die mit einer beliebigen Zeichenfolge übereinstimmen, die mit dem angegebenen Schlüsselwort beginnt.
> Bei der Suche, die über das Textfeld Abfrage auf der Seite Ressourcensuche in der Resource Explorer-Konsole ausgeführt wird, wird nicht automatisch ein Platzhalterzeichen angehängt. Sie können nach einem beliebigen Begriff * manuell ein Wort in die Suchzeichenfolge einfügen.

Welche Berechtigungen benötige ich, um nach Ressourcen suchen zu können?

Für die Suche benötigen Sie die Berechtigung, die beiden folgenden Operationen für eine Ansicht auszuführen, die sich in der Region befindet, in der Sie die Operation aufrufen:

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

Dies kann erreicht werden, indem Sie einer Richtlinie, die Ihrem IAM Principal zugewiesen ist, eine Anweisung hinzufügen, die dem folgenden Beispiel ähnelt.

```
        {
            "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"
        }
```

Sie können die Amazon-Ressourcennummer (ARN) einer bestimmten Ansicht durch eine ersetzenARN, die einen Platzhalter (`*`) enthält, um allen übereinstimmenden Ansichten die Erlaubnis zu erteilen.

Wenn Sie in Ihrer Anfrage keine Ansicht angeben, verwendet Resource Explorer automatisch die Standardansicht für die Region, in der Sie die Anfrage gestellt haben. Wenn Sie nicht berechtigt sind, die Standardansicht zu verwenden, wenden Sie sich an Ihren Administrator.

> **Note**
>
> Auch wenn Sie in den Ergebnissen einer Resource Explorer-Suchanfrage eine Ressource sehen, benötigen Sie Berechtigungen für die Ressource selbst, um mit dieser Ressource interagieren zu können.

Kontingente für Resource Explorer

SieAWS-Konto haben Standardkontingente für jedenAWS-Service. Wenn nicht anders angegeben, gelten Kontingente spezifisch für eine Region. Sie können Erhöhungen für einige Kontingente beantragen und andere Kontingente können nicht erhöht werden.

Um die Kontingente für anzuzeigenAWS Ressourcen Explorer, öffnen Sie die Konsole für Service Quotas. Wählen Sie im Navigationsbereich Resource Explorer aus AWS-Servicesund wählen Sie ihn aus.

Informationen zur Erhöhung eines Kontingents finden Sie unter Anfordern einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch. Wenn das Kontingent unter Service Quotas noch nicht in verfügbar ist, verwenden Sie das Formular zur Erhöhung des Service-Limits.

Die folgenden Kontingente sind die Standardwerte für Resource Explorer.

Kontingente für Höchstwerte	Standardwert
Anzahl der Views in einemAWS-Region	10

Tarifgrenzen für Operationen	Standardwert
Maximale Suchoperationen pro Sekunde	5
Maximale Anzahl von Nicht-Suchvorgängen pro Sekunde	3
Maximale Anzahl an Suchvorgängen in der Aggregatorregion pro Monat	10.000
Maximale Anzahl an Suchvorgängen in lokalen Regionen pro Monat	500

Verwenden AWS Ressourcen Explorer mit einem AWS SDK

AWS Software Development Kits (SDKs) sind für viele gängige Programmiersprachen verfügbar. Jedes SDK bietet eineAPI, Codebeispiele und Dokumentation, die es Entwicklern erleichtern, Anwendungen in ihrer bevorzugten Sprache zu erstellen.

SDKDokumentation	Codebeispiele
AWS SDK für C++	AWS SDK für C++ Codebeispiele
AWS CLI	AWS CLI Codebeispiele
AWS SDK für Go	AWS SDK für Go Codebeispiele
AWS SDK für Java	AWS SDK für Java Codebeispiele
AWS SDK für JavaScript	AWS SDK für JavaScript Codebeispiele
AWS SDK für Kotlin	AWS SDK für Kotlin Codebeispiele
AWS SDK für .NET	AWS SDK für .NET Codebeispiele
AWS SDK für PHP	AWS SDK für PHP Codebeispiele
AWS -Tools für PowerShell	Tools für PowerShell Codebeispiele
AWS SDK für Python (Boto3)	AWS SDK für Python (Boto3) Codebeispiele
AWS SDK für Ruby	AWS SDK für Ruby Codebeispiele
AWS SDK for Rust	AWS SDK for Rust Codebeispiele
AWS SDK für SAP ABAP	AWS SDK für SAP ABAP Codebeispiele
AWS SDK for Swift	AWS SDK for Swift Codebeispiele

Beispiel für die Verfügbarkeit

Sie können nicht finden, was Sie brauchen? Fordern Sie ein Codebeispiel an, indem Sie unten den Link Provide feedback (Feedback geben) auswählen.

Dokumentenverlauf für das Resource Explorer-Benutzerhandbuch

In der folgenden Tabelle werden die Dokumentationsversionen für beschrieben AWS Ressourcen Explorer. Wenn Sie über Aktualisierungen dieser Dokumentation informiert werden möchten, können Sie einen RSS Feed abonnieren.

Änderung	Beschreibung	Datum
Neuer Suchfilter hinzugefügt	Resource Explorer hat einen neuen `tag:all` Suchabfra gefilter hinzugefügt, mit dem Sie nach Ressourcen suchen können, denen ein oder mehrere benutzerdefinierte Tags angehängt sind, auch wenn der Ressourcentyp im Resource Explorer nicht unterstützt wird.	6. September 2024
Verbesserungen der Inhaltsor ganisation	Die Thementitel wurden aktualisiert und der Inhalt wurde neu organisiert, um die Lesbarkeit und Auffindbarkeit zu verbessern.	29. August 2024
Hinweis zum Upgrade der IAM Richtlinien auf IPv6	Kunden, die duale Adressier ung mit ASPEN folgenden Richtlinien verwenden, `aws:sourceIp` sind von diesem Upgrade betroffen. Duale Adressierung bedeutet, dass das Netzwerk IPv4 sowohl IPv6 als auch unterstüt zt.	15. Juli 2024

Die Unterstützung für drei Ressourcentypen wurde eingestellt	Resource Explorer hat die Unterstützung für die folgenden drei Ressource ntypen eingestellt: `ecs:tasks` `ssm:automation-execution` , und `ssm:patchbaseline` .	9. Juli 2024
Unterstützung für neue Ressourcentypen hinzugefügt	Resource Explorer hat Unterstützung für 65 neue Ressourcen hinzugefügt AWS Key Managemen t Service, AWS-Services darunter Amazon Route 53 und Amazon Fraud Detector.	20. Februar 2024
Verwaltete Richtlinie aktualisi ert	Resource Explorer hat Unterstützung für die Anzeige zusätzlicher Ressourcentypen hinzugefügt. Die `AWSResourceExplorerServiceRolePolicy` AWS verwaltet e Richtlinie wurde aktualisiert, um Resource Explorer Zugriff auf zusätzliche Ressource ntypen zu gewähren.	12. Dezember 2023
Ein neuer Suchfilter wurde hinzugefügt	Resource Explorer unterstüt zt jetzt das Durchsuchen Ihrer Ressourcen nach Anwendung en.	16. November 2023

Unterstützung für neue Ressourcentypen hinzugefügt	Resource Explorer hat Unterstützung für 86 neue Ressourcen von AWS-Services AWS CloudFormation Including AWS Glue, und Amazon hinzugefügt SageMaker.	15. November 2023
Resource Explorer unterstützt die Suche mit mehreren Konten	Sie können den Resource Explorer jetzt verwenden, um Ressourcen AWS-Konten innerhalb Ihrer Organisation oder Organisationseinheit zu suchen und zu finden. Weitere Informationen finden Sie unter Aktivieren der Suche mit mehreren Konten.	14. November 2023
Neue und aktualisierte verwaltete Richtlinien	Resource Explorer hat Unterstützung für AWS Organizations hinzugefügt. Die AWS verwalteten Richtlinien wurden hinzugefügt und aktualisiert, um Resource Explorer Zugriff auf Ihre Organisation, Organisationsstruktur, Konten und delegierte Administratoren zu gewähren.	14. November 2023

Unterstützung für neue Ressourcentypen hinzugefügt	Resource Explorer hat Unterstützung für hinzugefügt AWS Organizations. Die AWS verwalteten Richtlinien wurden aktualisiert, um Resource Explorer Zugriff auf Ihre Organisation, Organisationsstruktur, Konten und delegierte Administratoren zu gewähren.	14. November 2023
Unterstützung für neue Ressourcentypen hinzugefügt	Resource Explorer unterstützt jetzt 12 neue Ressourcentypen von Diensten wie Amazon Cognito und Amazon Elastic File System. AWS Elastic Beanstalk	18. Oktober 2023
Unterstützung für neue Ressourcentypen hinzugefügt	Resource Explorer hat Unterstützung für 164 Ressourcen hinzugefügt. Die AWS verwalteten Richtlinien, die Resource Explorer Zugriff auf Indexressourcen gewähren, wurden aktualisiert und enthalten nun auch diese neuen Ressourcentypen.	17. Oktober 2023
Resource Explorer ist jetzt in bestimmten Opt-in-Regionen verfügbar	Kunden, die Resource Explorer registriert haben BAH und CGK können sich jetzt für diesen anmelden.	05. Oktober 2023

Unterstützung für neue Ressourcentypen hinzugefügt	Resource Explorer hat Unterstützung für Ressourcen aus den folgenden Bereichen hinzugefügt AWS-Servi ces: AWS CodeBuild, AWS CodePipeline, Amazon Cognito, Amazon Elastic Container Registry, AWS Elastic Beanstalk, Amazon Elastic File System, AWS IoT, und AWS Step Functions. Die AWS verwalteten Richtlini en, die Resource Explorer Zugriff auf Indexressourcen gewähren, wurden aktualisiert und enthalten nun auch diese neuen Ressourcentypen.	1. August 2023
Resource Explorer unterstüt zt jetzt das Exportieren von Suchergebnissen in ein CSV	Sie können jetzt die Ergebniss e Ihrer Suche auf der Seite für die Ressourcensuche in eine Datei im CSV -Format exportieren.	4. April 2023
Verwenden Sie diese Amazon Q Entwickler für Chat-Anwe ndungen Option, um Ihre Ressourcen zu suchen und zu entdecken AWS	Sie können es jetzt verwenden Amazon Q Entwickler für Chat-Anwendungen , um Ihre Ressourcen mithilfe von Fragen in natürlicher Sprache zu durchsuchen. Weitere Informationen finden Sie unter Verwenden Amazon Q Entwickler für Chat-Anwe ndungen zur Suche nach Ressourcen.	30. März 2023

Unterstützung für neue Ressourcentypen hinzugefügt	Resource Explorer hat Unterstützung für Ressourcen der folgenden Anbieter hinzugefügt AWS-Services: Amazon ElastiCache und Amazon Simple Queue Service (AmazonSQS). AWS Lambda Die AWS verwalteten Richtlinien, die Resource Explorer Zugriff auf Indexressourcen gewähren, wurden aktualisiert und enthalten nun auch diese neuen Ressourcentypen.	7. März 2023
IAMAktualisierung der bewährten Verfahren	Aktualisierter Leitfaden zur Anpassung an die IAM bewährten Verfahren. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden unter IAM.	6. Dezember 2022
Neue AWS verwaltete Richtlinien	Resource Explorer fügt AWSResourceExplorerFullAccess Richtlinien AWSResourceExplorerReadOnlyAccess hinzu und AWSResourceExplorerServiceRolePolicy verwaltet sie.	7. November 2022
Erstversion	Erste Version des Resource Explorer-Benutzerhandbuchs	7. November 2022

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.