aws

User Guide

AWS Resource Groups

AWS Resource Groups: User Guide

Table of Contents

Ressourcengruppen 1
Was sind Ressourcengruppen? 1
Anwendungsfälle für Ressourcengruppen 3
AWS Resource Groupsund Berechtigungen 4
AWS Resource Groups-Ressourcen 4
Wie funktioniert Tagging 4
Erste Schritte 5
Voraussetzungen 6
Benutzergruppen erstellen 13
Arten von Ressourcengruppenabfragen 13
Erstellen Sie eine tagbasierte Abfrage und erstellen Sie eine Gruppe 18
Erstellen Sie eineAWS CloudFormation stapelbasierte Gruppe 21
Aktualisieren von Gruppen 23
Tag-basierte Abfragegruppen aktualisieren 24
Eine AWS CloudFormation stapelbasierte Gruppe aktualisieren 27
Überwachung von Ressourcengruppen auf Änderungen 30
Aktivieren von Gruppenlebenszyklusereignissen 32
Erstellen einer Regel für Gruppenlebenszyklusereignisse 34
Deaktivierung von Gruppen-Lifecycle-Ereignissen 38
Struktur und Syntax von Ereignissen 40
Löschen von Gruppen 52
AWS-Services, die mit AWS Resource Groups funktionieren 53
Dienstkonfigurationen 57
Zugriff 58
Syntax und Struktur 58
Konfigurationstypen und Parameter 59
Unterstützte Ressourcentypen 77
Amazon API Gateway 79
IAM Access Analyzer 80
AWS Amplify 80
AWS App Mesh 80
Amazon AppStream 81
AWS AppSync 81
AWS Backup 82

AWS Batch 82
AWS Billing Conductor 83
Amazon Braket 83
AWS Certificate Manager 84
AWS Certificate Manager Private Zertifizierungsstelle 84
AWS Cloud9 84
AWS CloudFormation 85
Amazon CloudFront 85
AWS CloudTrail 86
Amazon CloudWatch 86
Amazon CloudWatch -Protokolle 87
Amazon CloudWatch Synthetics 87
AWS CodeArtifact 87
AWS CodeBuild 88
AWS CodeCommit 88
AWS CodeDeploy 89
Amazon CodeGuru Reviewer 89
Amazon CodeGuru Profiler 90
AWS CodePipeline 90
AWS CodeConnections 91
Amazon Cognito 91
Amazon Comprehend 91
AWS Config 92
Amazon Connect Wisdom 92
AWS Datenaustausch 93
AWS Data Pipeline 93
AWS DataSync 94
AWS Database Migration Service 94
Amazon DynamoDB 95
Amazon EMR 95
Amazon-EMR-Container 95
Amazon EMR Serverless 96
Amazon ElastiCache 96
AWS Elastic Beanstalk 97
Amazon Elastic Compute Cloud (Amazon EC2) 97
Amazon Elastic Container Registry 102

Amazon Elastic Container Service 103
Amazon Elastic File System 103
Amazon Elastic Inference 104
Amazon Elastic Kubernetes Service (Amazon EKS) 104
Elastic Load Balancing 104
Amazon OpenSearch Service 105
Amazon CloudWatch -Ereignisse 106
Amazon EventBridge Schemata 106
Amazon FSx 107
Amazon Forecast 107
Amazon Fraud Detector 108
Amazon GameLift 109
AWS Global Accelerator 109
AWS Glue 110
AWS Glue DataBrew 110
AWS Ground Station 111
Amazon GuardDuty 111
Amazon Interactive Video Service 112
AWS Identity and Access Management 112
EC2 Image Builder 113
Amazon Inspector 114
AWS IoT 114
AWS IoT Analytics 115
AWS IoT Events 116
AWS IoT FleetWise 116
AWS IoT Greengrass 117
AWS-IoT-SiteWise-Konsole 117
AWS Key Management Service 118
Amazon Keyspaces (für Apache Cassandra) 118
Amazon Kinesis 119
Amazon Managed Service für Apache Flink 119
Amazon Data Firehose 120
AWS Lambda 120
Amazon MQ 121
Amazon Macie 121
Amazon Managed Streaming für Apache Kafka 122

AWS Elemental MediaConnect 122
AWS Elemental MediaPackage 123
AWS Network Manager 123
Amazon OpenSearch Service OpenSearch 124
AWS OpsWorks 124
AWS Organizations 125
Amazon Pinpoint 125
Amazon-Pinpoint-SMS- und -Sprachnachrichten-API 126
Amazon Quantum Ledger Database (Amazon QLDB) 126
Amazon Redshift 126
Amazon Relational Database Service (Amazon RDS) 128
AWS Resource Access Manager 129
AWS Resource Groups 129
AWS Robomaker 130
Amazon Route 53 130
Amazon Route 53 Resolver 131
Amazon S3 Glacier 132
Amazon SageMaker 132
AWS Secrets Manager 134
AWS Service Catalog 134
AWS Service Catalog AppRegistry 135
Service Quotas 135
Amazon Simple Email Service 136
Amazon Simple Notification Service 136
Amazon Simple Queue Service 137
Amazon Simple Storage Service (Amazon S3) 137
AWS Step Functions 138
Storage Gateway 138
AWS Systems Manager 139
AWS Systems Manager für SAP 139
Amazon Timestream 140
AWS Transfer Family 140
AWS WAF 141
Amazon WorkSpaces 141
AWS X-Ray 141
Veraltete Ressourcentypen 142

AWS CloudFormation-Ressourcen 143
Resource Groups undAWS CloudFormation Vorlagen 143
Weitere Informationen zu AWS CloudFormation 143
Sicherheit 144
Datenschutz 145
Datenverschlüsselung 146
Richtlinie für den Datenverkehr zwischen Netzwerken 146
Identity and Access Management 146
Zielgruppe 147
Authentifizierung mit Identitäten 148
Verwalten des Zugriffs mit Richtlinien 151
Funktionsweise von Resource Groups mit IAM 154
Von AWS verwaltete Richtlinien 159
Verwenden von serviceverknüpften Rollen 162
Beispiele für identitätsbasierte Richtlinien 165
Fehlerbehebung 169
Protokollierung und Überwachung 172
CloudTrail Integration 172
Compliance-Validierung 175
Ausfallsicherheit 176
Sicherheit der Infrastruktur 177
Bewährte Methoden für die Gewährleistung der Sicherheit 177
Service Quotas 179
Referenz 180
Service-Kontingente für Ressourcengruppen 180
Von AWS verwaltete Richtlinien zur Nutzung mit AWS Resource Groups 180
Dokumentverlauf 182
Frühere Aktualisierungen 193
AWS-Glossar 194
..... cxcv

Was sind Ressourcengruppen?

Sie können Ressourcengruppen verwenden, um Ihre AWS Ressourcen zu organisieren. AWS Resource Groupsist der Dienst, mit dem Sie Aufgaben für eine große Anzahl von Ressourcen gleichzeitig verwalten und automatisieren können. In diesem Handbuch wird beschrieben, wie Sie Ressourcengruppen in AWS Resource Groups erstellen und verwalten. Die Aufgaben, die Sie für eine Ressource ausführen können, variieren je nach dem AWS Dienst, den Sie verwenden. Eine Liste der unterstützten Dienste AWS Resource Groups und eine kurze Beschreibung dessen, was Sie mit den einzelnen Diensten mit einer Ressourcengruppe tun können, finden Sie unterAWS-Services, die mit AWS Resource Groups funktionieren.

Sie können über jeden der folgenden Einstiegspunkte auf Resource Groups zugreifen.

- Wählen Sie AWS Management Consolein der oberen Navigationsleiste Dienste aus. Wählen Sie dann unter Management & Governance die Option Resource Groups & Tag Editor aus.

  Direkter Link: AWS Resource GroupsKonsole
- Mithilfe der Resource Groups API, in AWS CLI Befehlen oder AWS SDK-Programmiersprachen. Weitere Informationen finden Sie in der AWS Resource GroupsAPI-Referenz.

So arbeiten Sie mit Ressourcengruppen auf der Startseite der AWS Management Console

1. Melden Sie sich an der AWS Management Console an.
2. Wählen Sie in der Navigationsleiste Services aus.
3. Wählen Sie unter Management & Governance die Option Resource Groups & Tag Editor aus.
4. Wählen Sie im Navigationsbereich auf der linken Seite Gespeicherte Resource Groups aus, um mit einer vorhandenen Gruppe zu arbeiten, oder Gruppe erstellen, um eine neue Gruppe zu erstellen.

Was sind Ressourcengruppen?

In AWS ist eine Ressource eine Entität, mit der Sie arbeiten können. Beispiele hierfür sind eine Amazon EC2 EC2-Instance, ein AWS CloudFormation Stack oder ein Amazon S3 S3-Bucket. Wenn Sie mit mehreren Ressourcen arbeiten, kann es nützlich sein, sie als Gruppe zu verwalten, anstatt für jede Aufgabe von einem AWS-Service zu einem anderen zu wechseln. Wenn Sie große Zahlen

verwandter Ressourcen verwalten, z. B. EC2-Instances, die eine Anwendungsebene bilden, müssen Sie wahrscheinlich für diese Ressourcen gleichzeitig Massenaktionen ausführen. Beispiele für Massenaktionen sind:

- Anwenden von Updates oder Sicherheits-Patches.
- Aktualisieren von Anwendungen.
- Öffnen oder Schließen von Ports für den Netzwerkdatenverkehr.
- Sammeln von spezifischen Protokoll- und Überwachungsdaten aus Ihrer Instance-Flotte.

Eine Ressourcengruppe ist eine Sammlung von AWS Ressourcen, die sich alle in derselben AWS-Region Gruppe befinden und die den in der Gruppenabfrage angegebenen Kriterien entsprechen. In Resource Groups gibt es zwei Arten von Abfragen, mit denen Sie eine Gruppe erstellen können. Beide Abfragetypen enthalten Ressourcen, die im Format `AWS::service::resource` angegeben werden.

- Tag-basiert

  Die Mitgliedschaft einer tagbasierten Ressourcengruppe basiert auf einer Abfrage, die eine Liste von Ressourcentypen und Tags angibt. Tags sind Schlüssel, die helfen, Ressourcen in Ihrer Organisation zu identifizieren und zu sortieren. Optional können Tags Werte für Schlüssel enthalten.

  > **Important**
  >
  > Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Wir verwenden Tags, um Ihnen Abrechnungs- und Verwaltungsdienste bereitzustellen. Tags sind nicht für private oder vertrauliche Daten gedacht.

- AWS CloudFormation-Stack-basiert

  Die Mitgliedschaft einer AWS CloudFormation stackbasierten Ressourcengruppe basiert auf einer Abfrage, die einen AWS CloudFormation Stack in Ihrem Konto in der aktuellen Region angibt. Sie können optional Ressourcentypen innerhalb des Stacks auswählen, die Sie in der Gruppe haben möchten. Sie können nur einen AWS CloudFormation-Stack als Basis für Ihre Abfrage verwenden.

Mit Diensten verknüpfte Ressourcengruppen

Einige AWS-Services definieren Ressourcengruppen, die Sie nur mithilfe der Konsole und der APIs dieses Dienstes erstellen und verwalten können. Sie haben nur begrenzte Möglichkeiten, diese Gruppen in der Resource Groups Groups-Konsole zu verwenden. Weitere Informationen finden Sie unter Dienstkonfigurationen für Ressourcengruppen im AWS Resource GroupsAPI-Referenzhandbuch.

Ressourcengruppen können verschachtelt sein; eine Ressourcengruppe kann vorhandene Ressourcengruppen in derselben Region enthalten.

Anwendungsfälle für Ressourcengruppen

Standardmäßig ist die AWS Management Console nach AWS-Service organisiert. Mit Resource Groups können Sie jedoch eine benutzerdefinierte Konsole erstellen, die Informationen auf der Grundlage von Kriterien organisiert und konsolidiert, die in Tags oder den Ressourcen in einem AWS CloudFormation Stapel angegeben sind. Die folgende Liste beschreibt einige Fälle, in denen die Ressourcengruppierung Ihnen helfen kann, Ihre Ressourcen zu organisieren.

- Eine Anwendung mit verschiedenen Phasen wie Entwicklung, Staging und Produktion.
- Projekte, die von mehreren Abteilungen oder Personen verwaltet werden.
- Eine Reihe von AWS-Ressourcen, die Sie gemeinsam für ein gemeinsames Projekt verwenden oder die Sie als Gruppe verwalten oder überwachen möchten.
- Eine Gruppe von Ressourcen, die zu Anwendungen gehören, die auf einer bestimmten Plattform ausgeführt werden, z. B. Android oder iOS.

Angenommen, Sie entwickeln eine Webanwendung und verwalten separate Gruppen von Ressourcen für Ihre Alpha-, Beta- und Veröffentlichungsphase. Jede Version läuft auf Amazon EC2 mit einem Amazon Elastic Block Store-Speichervolume. Sie verwenden Elastic Load Balancing für die Verwaltung des Datenverkehrs und Route 53 für die Verwaltung Ihrer Domain. Ohne Resource Groups müssen Sie möglicherweise auf mehrere Konsolen zugreifen, nur um den Status Ihrer Dienste zu überprüfen oder die Einstellungen für eine Version Ihrer Anwendung zu ändern.

Mit Resource Groups verwenden Sie eine einzige Seite, um Ihre Ressourcen anzuzeigen und zu verwalten. Nehmen wir beispielsweise an, Sie verwenden das Tool, um eine Ressourcengruppe für jede Version — Alpha, Beta und Release — Ihrer Anwendung zu erstellen. Um Ihre Ressourcen für die Alpha-Version Ihrer Anwendung zu überprüfen, öffnen Sie die Ressourcengruppe. Anschließend zeigen Sie die konsolidierten Informationen auf der Ressourcengruppen-Seite an. Um eine bestimmte

Ressource zu ändern, wählen Sie die Links der betreffenden Ressource auf der Ressourcengruppen-Seite aus, um auf die Servicekonsole mit den benötigten Einstellungen zuzugreifen.

AWS Resource Groupsund Berechtigungen

Die Funktionsberechtigungen für Resource Groups liegen auf Kontoebene. Solange IAM-Prinzipale wie Rollen und Benutzer, die Ihr Konto gemeinsam nutzen, über die richtigen IAM-Berechtigungen verfügen, können sie mit von Ihnen erstellten Ressourcengruppen arbeiten.

Tags sind Eigenschaften einer Ressource. Daher werden Tags für Ihr gesamtes Konto freigegeben. Benutzer in einer Abteilung oder spezialisierten Gruppe können ein gemeinsames Vokabular (Tags) nutzen, um Ressourcengruppen zu erstellen, die für ihre Rollen und Verantwortlichkeiten sinnvoll sind. Ein gemeinsamer Pool von Tags bedeutet auch, dass sich Benutzer keine Sorgen über fehlende oder miteinander in Konflikt stehende Tag-Informationen machen müssen, wenn sie eine Ressourcengruppe gemeinsam nutzen.

AWS Resource Groups-Ressourcen

In Resource Groups ist die einzige verfügbare Ressource eine Gruppe. Gruppen sind eindeutige Amazon-Ressourcennamen (ARN) zugeordnet. Weitere Informationen über ARNs finden Sie unter Amazon-Ressourcennamen (ARN) und AWS-Service-Namespaces im Allgemeine Amazon Web Services-Referenz.

Ressourcentyp	ARN-Format
Resource Group (Ressourcengruppe)	`arn:aws:resource-groups:` *`region`*`:`*`account`*`:group/`*`group-name`*

Wie funktioniert Tagging

Tags sind Schlüssel-Wert-Paare, die als Metadaten Ihre AWS-Ressourcen organisieren. Bei den meisten AWS Ressourcen haben Sie die Möglichkeit, beim Erstellen der Ressource Tags hinzuzufügen, unabhängig davon, ob es sich um eine Amazon EC2 EC2-Instance, einen Amazon S3 S3-Bucket oder eine andere Ressource handelt. Sie können jedoch auch mittels des Tag Editor

Tags gleichzeitig zu mehreren unterstützten Ressourcen hinzufügen. Sie erstellen eine Abfrage für Ressourcen verschiedener Typen und fügen anschließend den Ressourcen in den Suchergebnissen Tags hinzu oder entfernen oder ersetzen Tags. Abfragen weisen Tags den Operator `AND` zu, sodass alle Ressourcen, die mit den angegebenen Ressourcentypen und allen angegebenen Tags übereinstimmen, von der Abfrage zurückgegeben werden.

> **Important**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Wir verwenden Tags, um Ihnen Abrechnungs- und Verwaltungsdienste anzubieten. Tags sind nicht für private oder vertrauliche Daten gedacht.

Weitere Informationen zum Tagging finden Sie im Tag-Editor-Benutzerhandbuch. Sie können unterstützte Ressourcen mithilfe des Tag Editor und einige zusätzliche Ressourcen mithilfe der Tagging-Funktionalität in der Service-Konsole, in der Sie die betreffende Ressource erstellen und verwalten, mit Tags markieren.

Erste Schritte mit AWS Resource Groups

In AWS ist eine Ressource eine Entität, mit der Sie arbeiten können. Beispiele sind eine Amazon EC2 EC2-Instance, ein Amazon S3 S3-Bucket oder eine Amazon Route 53-gehostete Zone. Wenn Sie mit mehreren Ressourcen arbeiten, kann es nützlich sein, sie als Gruppe zu verwalten, anstatt für jede Aufgabe von einem AWS-Service zu einem anderen zu wechseln.

In diesem Abschnitt erhalten Sie Informationen zu den ersten Schritten mit AWS Resource Groups. Zunächst organisieren Sie AWS-Ressourcen, indem Sie sie in Tag Editor mit Tags markieren. Anschließend erstellen Sie in Resource Groups Abfragen mit den Ressourcentypen, die in einer Gruppe enthalten sein sollen, und den Tags, die Sie auf Ressourcen angewendet haben.

Nachdem Sie Ressourcengruppen in Ressourcengruppen erstellt haben, verwenden SieAWS Systems Manager-Tools wie die Automatisierung, um Verwaltungsaufgaben in Ihren Ressourcengruppen zu vereinfachen.

Weitere Informationen zu den ersten Schritten mitAWS Systems ManagerFunktionen und Tools finden Sie unterAWS Systems Manager-Benutzerhandbuchaus.

Themen

- Voraussetzungen für die Arbeit mit AWS Resource Groups

Voraussetzungen für die Arbeit mit AWS Resource Groups

Bevor Sie mit Ressourcengruppen arbeiten, müssen Sie überprüfen, ob Sie über ein aktives AWS -Konto mit vorhandenen Ressourcen und entsprechenden Berechtigungen für das Markieren von Ressourcen und Gruppen mit Tags verfügen.

Registrieren für AWS

Wenn Sie kein haben AWS-Konto, führen Sie die folgenden Schritte aus, um eines zu erstellen.

So registrieren Sie sich für ein AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
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 ein registrieren AWS-Konto, Root-Benutzer des AWS-Kontos wird ein 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.

Erstellen von -Ressourcen

Sie können eine leere Ressourcengruppe erstellen, können aber keine Aufgaben für Ressourcengruppenmitglieder ausführen, bis sich Ressourcen in der Gruppe befinden. Weitere Informationen zu den unterstützten Ressourcentypen finden Sie unter Ressourcentypen, die Sie mit AWS Resource Groups und Tag Editor verwenden können.

Berechtigungen einrichten

Um Ressourcengruppen und Tag Editor vollständig nutzen zu können, benötigen Sie möglicherweise zusätzliche Berechtigungen für das Markieren von Ressourcen oder die Anzeige der Tag-Schlüssel und -Werte einer Ressource. Diese Berechtigungen gehören folgenden Kategorien an:

- Berechtigungen für einzelne Services, sodass Sie Ressourcen aus diesen Services mit einem Tag markieren und in Ressourcengruppen einfügen können.

- Berechtigungen, die für die Verwendung der Tag-Editor-Konsole erforderlich sind
- Berechtigungen, die für die Verwendung der AWS Resource Groups Konsole und der API erforderlich sind.

Wenn Sie Administrator sind, können Sie Ihren Benutzern Berechtigungen erteilen, indem Sie Richtlinien über den AWS Identity and Access Management (IAM)-Service erstellen. Sie erstellen zunächst Ihre Prinzipale, z. B. IAM-Rollen oder -Benutzer, oder verknüpfen externe Identitäten mit Ihrer AWS Umgebung mithilfe eines Services wie AWS IAM Identity Center. Anschließend wenden Sie Richtlinien mit den Berechtigungen an, die Ihre Benutzer benötigen. Informationen zum Erstellen und Anfügen von IAM-Richtlinien finden Sie unter Arbeiten mit Richtlinien.

Berechtigungen für einzelne Services

> **Important**
>
> In diesem Abschnitt werden Berechtigungen beschrieben, die Sie benötigen, wenn Sie Ressourcen aus anderen Servicekonsolen und APIs mit Tags markieren und diese Ressourcen zu Ressourcengruppen hinzufügen möchten.

Wie in Was sind Ressourcengruppen? beschrieben, stellt jede Ressourcengruppe eine Sammlung von Ressourcen mit angegebenen Typen dar, denen mindestens ein Tag-Schlüssel oder -Wert gemeinsam ist. Um Tags zu einer Ressource hinzuzufügen, benötigen Sie die erforderlichen Berechtigungen für den Service, zu dem die Ressource gehört. Um beispielsweise Amazon EC2-Instances zu markieren, muss Ihr über Berechtigungen für die Tagging-Aktionen in der API dieses Services verfügen, z. B. über die im Amazon EC2-Benutzerhandbuch aufgeführten.

Um die Ressourcengruppenfunktion vollständig nutzen zu können, benötigen Sie weitere Berechtigungen, die Ihnen den Zugriff auf die Konsole eines Service und die Interaktion mit den dort vorhandenen Ressourcen ermöglichen. Beispiele für solche Richtlinien für Amazon EC2 finden Sie unter Beispielrichtlinien für die Arbeit in der Amazon EC2-Konsole im Amazon EC2-Benutzerhandbuch für Linux-Instances.

Erforderliche Berechtigungen für Ressourcengruppen und Tag-Editor

Um Resource Groups und Tag Editor verwenden zu können, müssen der Richtlinienanweisung eines Benutzers in IAM die folgenden Berechtigungen hinzugefügt werden. Sie können entweder von

AWSverwaltete Richtlinien hinzufügen, die up-to-date von verwaltet und verwaltet werden AWS, oder Sie können Ihre eigene benutzerdefinierte Richtlinie erstellen und verwalten.

Verwenden von AWS verwalteten Richtlinien für Ressourcengruppen und Tag-Editor-Berechtigungen

AWS Resource Groups und Tag Editor unterstützen die folgenden AWS verwalteten Richtlinien, mit denen Sie Ihren Benutzern einen vordefinierten Satz von Berechtigungen bereitstellen können. Sie können diese verwalteten Richtlinien jedem Benutzer, jeder Rolle oder Gruppe anfügen, genau wie jede andere Richtlinie, die Sie erstellen.

ResourceGroupsandTagEditorReadOnlyAccess

Diese Richtlinie gewährt der angehängten IAM-Rolle oder dem angehängten Benutzer die Berechtigung, die schreibgeschützten Operationen sowohl für Ressourcengruppen als auch für den Tag-Editor aufzurufen. Um die Tags einer Ressource zu lesen, müssen Sie auch über eine separate Richtlinie über Berechtigungen für diese Ressource verfügen (siehe den folgenden wichtigen Hinweis).

ResourceGroupsandTagEditorFullAccess

Diese Richtlinie gewährt der angehängten IAM-Rolle oder dem angehängten Benutzer die Berechtigung, jede -Ressource-Groups-Operation und die Lese- und Schreib-Tag-Operationen im Tag Editor aufzurufen. Um die Tags einer Ressource zu lesen oder zu schreiben, müssen Sie auch über eine separate Richtlinie über Berechtigungen für diese Ressource verfügen (siehe den folgenden wichtigen Hinweis).

Important

Die beiden vorherigen Richtlinien erteilen die Berechtigung zum Aufrufen der Operationen Resource Groups und Tag Editor und zum Verwenden dieser Konsolen. Für Resource-Groups-Operationen sind diese Richtlinien ausreichend und gewähren alle Berechtigungen, die für die Arbeit mit beliebigen Ressourcen in der Resource-Groups-Konsole erforderlich sind.
Für Tagging-Operationen und die Tag-Editor-Konsole sind die Berechtigungen jedoch detaillierter. Sie müssen nicht nur über Berechtigungen verfügen, um die Operation aufzurufen, sondern auch über die entsprechenden Berechtigungen für die spezifische Ressource, auf deren Tags Sie zugreifen möchten. Um diesen Zugriff auf die Tags zu gewähren, müssen Sie auch eine der folgenden Richtlinien anfügen:

- Die von AWSverwaltete Richtlinie ReadOnlyAccess gewährt Berechtigungen für die schreibgeschützten Operationen für die Ressourcen jedes Services. hält diese Richtlinie AWS automatisch mit neuen AWS Services auf dem neuesten Stand, sobald sie verfügbar sind.
- Viele -Services bieten servicespezifische AWSschreibgeschützte, von verwaltete Richtlinien, mit denen Sie den Zugriff auf die von diesem Service bereitgestellten Ressourcen beschränken können. Amazon EC2 stellt beispielsweise AmazonEC2ReadOnlyAccess bereit.
- Sie können Ihre eigene Richtlinie erstellen, die nur Zugriff auf die sehr spezifischen schreibgeschützten Operationen für die wenigen Services und Ressourcen gewährt, auf die Ihre Benutzer zugreifen sollen. Diese Richtlinie verwendet entweder eine „Zulassungsliste“-Strategie oder eine Sperrlisten-Strategie.

  Eine Zulassungslistenstrategie nutzt die Tatsache, dass der Zugriff standardmäßig verweigert wird, bis Sie ihn explizit in einer Richtlinie zulassen. Sie können also eine Richtlinie wie das folgende Beispiel verwenden:

  ```
  {
      "Version": "2012-10-17",
      "Statement": [
          {
              "Effect": "Allow",
              "Action": [ "resource-groups:*" ],
              "Resource": "arn:aws:resource-groups:*:123456789012:group/*"
          }
      ]
  }
  ```

  Alternativ können Sie eine „Verweigerungsliste“-Strategie verwenden, die den Zugriff auf alle Ressourcen ermöglicht, mit Ausnahme derjenigen, die Sie explizit blockieren.

  ```
  {
      "Version": "2012-10-17",
      "Statement": [
          {
              "Effect": "Deny",
               "Action": [ "resource-groups:*" ],
              "Resource": "arn:aws:resource-groups:*:123456789012:group/*"
          }
  ```

```
    ]
}
```

Manuelles Hinzufügen von Berechtigungen für Ressourcengruppen und Tag Editor

- `resource-groups:*` (Diese Berechtigung erlaubt alle Resource Groups-Aktionen. Wenn Sie stattdessen Aktionen einschränken möchten, die einem Benutzer zur Verfügung stehen, können Sie das Sternchen durch eine bestimmte Resource-Groups-Aktion oder durch eine durch Komma getrennte Liste von Aktionen ersetzen)
- `cloudformation:DescribeStacks`
- `cloudformation:ListStackResources`
- `tag:GetResources`
- `tag:TagResources`
- `tag:UntagResources`
- `tag:getTagKeys`
- `tag:getTagValues`
- `resource-explorer:*`

> **Note**
>
> Die `-resource-groups:SearchResources`Berechtigung ermöglicht es dem Tag-Editor, Ressourcen aufzulisten, wenn Sie Ihre Suche mithilfe von Tag-Schlüsseln oder -Werten filtern.
> Die `-resource-explorer:ListResources`Berechtigung ermöglicht es dem Tag-Editor, Ressourcen aufzulisten, wenn Sie Ressourcen suchen, ohne Such-Tags zu definieren.

Um Resource Groups und Tag Editor in der Konsole zu verwenden, benötigen Sie auch die Berechtigung zum Ausführen der `resource-groups:ListGroupResources` Aktion. Diese Berechtigung ist erforderlich, um verfügbare Ressourcentypen in der aktuellen Region aufzulisten. Die Verwendung von Richtlinienbedingungen mit `resource-groups:ListGroupResources` wird derzeit nicht unterstützt.

Erteilen von Berechtigungen für die Verwendung von AWS Resource Groups und Tag Editor

Gehen Sie wie folgt vor, um einem Benutzer eine Richtlinie für die Verwendung von AWS Resource Groups und Tag Editor hinzuzufügen.

1. Öffnen Sie die IAM-Konsole.
2. Klicken Sie im Navigationsbereich auf Users (Benutzer).
3. Suchen Sie den Benutzer, dem Sie Berechtigungen erteilen möchten, AWS Resource Groups und Tag-Editor-Berechtigungen. Wählen Sie den Namen des Benutzers aus, um die Seite „Eigenschaften“ für den Benutzer zu öffnen.
4. Wählen Sie Add permissions (Berechtigungen hinzufügen).
5. Wählen Sie Vorhandene Richtlinien direkt zuordnen.
6. Wählen Sie Richtlinie erstellen aus.
7. Fügen Sie auf der Registerkarte JSON die folgende Richtlinienanweisung ein.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "resource-groups:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "tag:GetResources",
        "tag:TagResources",
        "tag:UntagResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-explorer:*"
      ],
      "Resource": "*"
    }
  ]
}
```

> **Note**
>
> Diese Beispielrichtlinienanweisung gewährt Berechtigungen nur für AWS Resource Groups - und Tag-Editor-Aktionen. Sie erlaubt keinen Zugriff auf AWS Systems Manager Aufgaben in der - AWS Resource Groups Konsole. Diese Richtlinie gewährt Ihnen beispielsweise keine Berechtigungen zur Verwendung von Systems Manager Automation-Befehlen. Um Systems Manager-Aufgaben für Ressourcengruppen auszuführen, müssen Ihrer Richtlinie Systems Manager-Berechtigungen angefügt sein (z. B. `ssm:*`). Weitere Informationen zum Gewähren des Zugriffs auf Systems Manager finden Sie unter Konfigurieren des Zugriffs auf Systems Manager im AWS Systems Manager -Benutzerhandbuch.

8. Wählen Sie Richtlinie prüfen.
9. Geben Sie einen Namen und eine Beschreibung für die neue Richtlinie ein (z. B. `AWSResourceGroupsQueryAPIAccess`).
10. Wählen Sie Richtlinie erstellen aus.
11. Nachdem die Richtlinie nun in IAM gespeichert ist, können Sie sie an andere Benutzer anfügen. Weitere Informationen zum Hinzufügen einer Richtlinie zu einem Benutzer finden Sie unter Hinzufügen von Berechtigungen durch direktes Anfügen von Richtlinien an den Benutzer im IAM-Benutzerhandbuch.

Weitere Informationen über AWS Resource Groups Autorisierung und Zugriffskontrolle

Resource Groups unterstützt Folgendes.

- Aktionsbasierte Richtlinien. Sie können beispielsweise eine Richtlinie erstellen, die es Benutzern ermöglicht, -ListGroupsOperationen auszuführen, aber keine anderen.
- Berechtigungen auf Ressourcenebene. Resource Groups unterstützt die Verwendung von ARNs, um einzelne Ressourcen in der Richtlinie anzugeben.
- Autorisierung auf der Basis von Tags. Resource Groups unterstützt die Verwendung von Ressourcen-Tags in der Bedingung einer Richtlinie. Sie können beispielsweise eine Richtlinie erstellen, die Benutzern von Resource Groups vollen Zugriff auf eine Gruppe gewährt, die Sie markiert haben.
- Temporäre Anmeldeinformationen. Benutzer können eine Rolle mit einer Richtlinie übernehmen, die - AWS Resource Groups Operationen zulässt.

Resource Groups unterstützt keine ressourcenbasierten Richtlinien.

Resource Groups verwendet keine serviceverknüpften Rollen.

Weitere Informationen zur Integration von Ressourcengruppen und Tag Editor in AWS Identity and Access Management (IAM) finden Sie in den folgenden Themen im AWS Identity and Access Management -Benutzerhandbuch.

- AWS -Services, die mit IAM funktionieren
- Aktionen, Ressourcen und Bedingungsschlüssel für AWS Resource Groups
- Steuern des Zugriffs mithilfe von Richtlinien

Erstellen von abfragebasierten Gruppen inAWS Resource Groups

Themen

- Arten von Ressourcengruppenabfragen
- Erstellen Sie eine tagbasierte Abfrage und erstellen Sie eine Gruppe
- Erstellen Sie eineAWS CloudFormation stapelbasierte Gruppe

Arten von Ressourcengruppenabfragen

InAWS Resource Groups ist eine Abfrage die Grundlage einer abfragebasierten Gruppe. Sie können Ressourcengruppen auf der Basis von zwei Abfragetypen erstellen.

Tag-basiert

Tag-basierte Abfragen umfassen Listen von Ressourcentypen, die im folgenden Format angegeben sind`AWS::`*`service`*`::`*`resource`*, sowie Tags. Tags sind Schlüssel, die helfen, Ressourcen in Ihrer Organisation zu identifizieren und zu sortieren. Optional können Tags Werte für Schlüssel enthalten.

In einer Tag-basierten Abfrage geben Sie auch die Tags an, die den Ressourcen gemeinsam sind, die Mitglieder der Gruppe werden sollen. Wenn Sie beispielsweise eine Ressourcengruppe erstellen möchten, die alle Amazon EC2-Instances und Amazon S3 S3-Buckets enthält, die Sie zum Ausführen der Testphase einer Anwendung verwenden, und Sie Instances und Buckets haben, die auf diese Weise gekennzeichnet sind, wählen Sie die`AWS::S3::Bucket`

RessourcentypenAWS::EC2::Instance und aus der Dropdownliste aus und geben Sie dann den Tag-Schlüssel**Stage** mit einem Tag-Wert von an**Test**.

Die Syntax desResourceQuery Parameters einer tagbasierten Ressourcengruppe enthält die folgenden Elemente:

- Type

  Dieses Element gibt an, welche Art von Abfrage diese Ressourcengruppe definiert. Um eine tagbasierte Ressourcengruppe zu erstellen, geben Sie den WertTAG_FILTERS_1_0 wie folgt an:

  ```
  "Type": "TAG_FILTERS_1_0"
  ```

- Query

  Dieses Element definiert die tatsächliche Abfrage, die für den Abgleich mit Ressourcen verwendet wird. Sie enthält eine Zeichenfolgenderweise als JSON-Struktur.

  - ResourceTypeFilters

    Dieses Element begrenzt die Ergebnisse auf die Ressourcennamen, die dem Filter entsprechen. Sie können die folgenden Werte angeben:

    - "AWS::AllSupported"— um anzugeben, dass die Ergebnisse Ressourcen jedes Typs enthalten können, die der Abfrage entsprechen und die derzeit vom Resource Groups Groups-Dienst unterstützt werden.
    - "AWS::*service-id*::*resource-type*— eine durch Kommas getrennte Liste von Spezifikationszeichenfolgen für Ressourcentypen mit diesem Format:, z."AWS::EC2::Instance" B.

  - TagFilters

    Dieses Element gibt Schlüssel/Wert-Zeichenfolgenpaare an, die mit den an Ihre Ressourcen angehängten Tags verglichen werden. Diejenigen mit einem Tag-Schlüssel und einem Wert, die dem Filter entsprechen, sind in der Gruppe enthalten. Jeder Filter besteht aus diesen Elementen:

    - "Key"— eine Zeichenfolge mit einem Schlüsselnamen. Nur Ressourcen, die über Tags mit einem zulässigen Schlüsselnamen verfügen, entsprechen dem Filter und sind Mitglieder der Gruppe.

- `"Values"`— eine Zeichenfolge mit einer durch Kommas getrennten Liste von Werten für den angegebenen Schlüssel. Nur Ressourcen mit einem zulässigen Tag-Schlüssel und einem Wert, der mit einem in dieser Liste mit einem in dieser Liste mit einem in der Liste mit einem und in der Liste mit einem in der Liste mit einem in der Liste

All diese JSON-Elemente müssen zu einer einzeiligen Zeichenkettendarstellung der JSON-Struktur kombiniert werden. Stellen Sie sich zum Beispiel eine`Query` mit der folgenden Beispiel-JSON-Struktur vor. Diese Abfrage soll nur Amazon EC2 EC2-Instances abgleichen, die das Tag „Stage“ mit dem Wert „Test“ haben.

```
{
    "ResourceTypeFilters": [ "AWS::EC2::Instance" ],
    "TagFilters": [
        {
            "Key": "Stage",
            "Values": [ "Test" ]
        }
    ]
}
```

Dieser JSON kann als die folgende einzeilige Zeichenfolge dargestellt und als Wert des`Query` Elements verwendet werden. Da der Wert einer JSON-Struktur eine Zeichenfolge in doppelten Anführungszeichen sein muss, müssen Sie alle eingebetteten doppelten Anführungszeichen oder Schrägstriche maskieren, indem Sie jedem Zeichen einen umgekehrten Schrägstrich voranstellen, wie hier gezeigt:

```
"Query":"{\"ResourceTypeFilters\":[\"AWS::AllSupported\"],\"TagFilters\":[{\"Key\":
\"Stage\",\"Values\":[\"Test\"]}]}"
```

Die vollständige`ResourceQuery` Zeichenfolge wird dann wie hier gezeigt als CLI-Befehlsparameter dargestellt:

```
--resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters\":
[\"AWS::AllSupported\"],\"TagFilters\":[{\"Key\":\"Stage\",\"Values\":[\"Test
\"]}]}"}'
```

AWS CloudFormationstapelbasiert

In einer AWS CloudFormation-Stack-basierten Abfrage wählen Sie einen AWS CloudFormation-Stack in Ihrem Konto in der aktuellen Region und anschließend die Ressourcentypen im Stack

aus, die in der Gruppe enthalten sein sollen. Sie können nur einen AWS CloudFormation-Stack als Basis für Ihre Abfrage verwenden.

> **Note**
>
> EinAWS CloudFormation Stapel kann andereAWS CloudFormation „untergeordnete“ Stapel enthalten. Eine Ressourcengruppe, die auf einem „übergeordneten“ Stapel basiert, erhält jedoch nicht alle Ressourcen der untergeordneten Stapel als Gruppenmitglieder. Ressourcengruppen fügt die untergeordneten Stapel der Ressourcengruppe des übergeordneten Stacks als einzelne Gruppenmitglieder hinzu und erweitert sie nicht.

Resource Groups unterstützt Abfragen, die aufAWS CloudFormation Stacks basieren, die einen der folgenden Status haben.

- `CREATE_COMPLETE`
- `CREATE_IN_PROGRESS`
- `DELETE_FAILED`
- `DELETE_IN_PROGRESS`
- `REVIEW_IN_PROGRESS`

> **Important**
>
> Nur Ressourcen, die direkt als Teil des Stacks in der Abfrage erstellt wurden, sind in der Ressourcengruppe enthalten. Ressourcen, die später von Mitgliedern desAWS CloudFormation Stacks erstellt wurden, werden nicht zu Mitgliedern der Gruppe. Wenn beispielsweise eine Gruppe mit auto-scaling vonAWS CloudFormation als Teil des Stacks erstellt wird, ist diese auto-scaling skalierende Gruppe ein Mitglied der Gruppe. Eine Amazon EC2 EC2-Instance, die von dieser Autoscaling-Gruppe im Rahmen ihres Vorgangs erstellt wurde, ist jedoch kein Mitglied derAWS CloudFormation stapelbasierten Ressourcengruppe.

Wenn Sie eine Gruppe auf der Grundlage einesAWS CloudFormation Stacks erstellen und der Status des Stacks in einen Status wechselt, der nicht mehr als Grundlage für eine Gruppenabfrage unterstützt wird, z. B.`DELETE_COMPLETE`, die Ressourcengruppe ist immer noch vorhanden, hat aber keine Mitgliedsressourcen.

Nachdem Sie eine Ressourcengruppe erstellt haben, können Sie Aufgaben für die Ressourcen in der Gruppe ausführen.

Die Syntax des`ResourceQuery` Parameters einer CloudFormation stapelbasierten Ressourcengruppe enthält die folgenden Elemente:

- `Type`

  Dieses Element gibt an, welche Art von Abfrage diese Ressourcengruppe definiert.

  Um eineAWS CloudFormation stapelbasierte Ressourcengruppe zu erstellen, geben Sie den Wert`CLOUDFORMATION_STACK_1_0` wie folgt an:

  ```
  "Type": "CLOUDFORMATION_STACK_1_0"
  ```

- `Query`

  Dieses Element definiert die tatsächliche Abfrage, die für den Abgleich mit Ressourcen verwendet wird. Sie enthält eine Zeichenfolgenderweise als JSON-Struktur.

  - `ResourceTypeFilters`

    Dieses Element begrenzt die Ergebnisse auf die Ressourcennamen, die dem Filter entsprechen. Sie können die folgenden Werte angeben:

    - `"AWS::AllSupported"`— um anzugeben, dass die Ergebnisse Ressourcen jedes Typs enthalten können, die der Abfrage entsprechen.
    - `"AWS::`*`service-id`*`::`*`resource-type`*— eine durch Kommas getrennte Liste von Spezifikationszeichenfolgen für Ressourcentypen mit diesem Format:, z.`"AWS::EC2::Instance"` B.

  - `StackIdentifier`

    Dieses Element gibt den Amazon-Ressourcennamen (ARN) desAWS CloudFormation Stacks an, dessen Ressourcen Sie in die Gruppe aufnehmen möchten.

All diese JSON-Elemente müssen zu einer einzeiligen Zeichenkettendarstellung der JSON-Struktur kombiniert werden. Stellen Sie sich zum Beispiel eine`Query` mit der folgenden Beispiel-JSON-Struktur vor. Diese Abfrage soll nur Amazon S3 S3-Buckets abgleichen, die Teil des angegebenenAWS CloudFormation Stacks sind.

```
{
    "ResourceTypeFilters": [ "AWS::S3::Bucket" ],
    "StackIdentifier": "arn:aws:cloudformation:us-
west-2:123456789012:stack/MyCloudFormationStackName/fb0d5000-aba8-00e8-
aa9e-50d5cEXAMPLE"
}
```

Dieser JSON kann als die folgende einzeilige Zeichenfolge dargestellt und als Wert des`Query` Elements verwendet werden. Da der Wert einer JSON-Struktur eine Zeichenfolge in doppelten Anführungszeichen sein muss, müssen Sie alle eingebetteten doppelten Anführungszeichen oder Schrägstriche maskieren, indem Sie jedem Zeichen einen umgekehrten Schrägstrich voranstellen, wie hier gezeigt:

```
"Query":"{\"ResourceTypeFilters\":[\"AWS::S3::Bucket\"],\"StackIdentifier\":
\"arn:aws:cloudformation:us-west-2:123456789012:stack\/MyCloudFormationStackName\/
fb0d5000-aba8-00e8-aa9e-50d5cEXAMPLE\"
```

Die vollständige`ResourceQuery` Zeichenfolge wird dann wie hier gezeigt als CLI-Befehlsparameter dargestellt:

```
--resource-query '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"ResourceTypeFilters
\":[\"AWS::S3::Bucket\"],\"StackIdentifier\":\"arn:aws:cloudformation:us-
west-2:123456789012:stack\/MyCloudFormationStackName\/fb0d5000-aba8-00e8-
aa9e-50d5cEXAMPLE\"}'
```

Erstellen Sie eine tagbasierte Abfrage und erstellen Sie eine Gruppe

Die folgenden Verfahren zeigen Ihnen, wie Sie eine tagbasierte Abfrage erstellen und damit eine Ressourcengruppe erstellen.

Console

1. Melden Sie sich an der AWS Resource Groups-Konsole an.
2. Wählen Sie im Navigationsbereich die Option Ressourcergruppen.
3. Wählen Sie auf der Seite Abfragebasierte Gruppe erstellen unter Gruppentyp den Tag-basierten Gruppentyp aus.
4. Wählen Sie unter Gruppierungskriterien die Ressourcentypen aus, die Sie in Ihrer Ressourcengruppe haben möchten. Sie können maximal 20 Ressourcentypen in einer

Abfrage verwenden. Wählen Sie für diese Komplettlösung AWS::EC2::Instanceund AWS::S3::Bucket.

5. Geben Sie weiterhin unter Gruppierungskriterien für Tags einen Tag-Schlüssel oder ein Tag-Schlüssel-Wert-Paar an, um die passenden Ressourcen auf diejenigen zu beschränken, die mit Ihren angegebenen Werten markiert sind. Wählen Sie Add (Hinzufügen) aus oder drücken Sie die Eingabetaste, wenn Ihr Tag fertig gestellt wurde. In diesem Beispiel filtern Sie nach Ressourcen mit dem Tag-Schlüssel Stage (Phase). Der Tag-Wert ist optional, engt jedoch die Ergebnisse der Abfrage weiter ein. Sie können mehrere Werte für einen Tag-Schlüssel hinzufügen, indem Sie einen`OR` Operator zwischen den Tag-Werten hinzufügen. Um weitere Tags hinzuzufügen, wählen Sie Add (Hinzufügen) aus. Abfragen weisen Tags den Operator `AND` zu, sodass alle Ressourcen, die mit den angegebenen Ressourcentypen und allen angegebenen Tags übereinstimmen, von der Abfrage zurückgegeben werden.
6. Wählen Sie weiterhin unter Gruppierungskriterien die Option Vorschau der Gruppenressourcen aus, um die Liste der EC2-Instances und S3-Buckets in Ihrem Konto anzuzeigen, die dem oder den angegebenen Tag-Schlüsseln entsprechen.
7. Nachdem Sie die gewünschten Ergebnisse erhalten haben, erstellen Sie eine Gruppe, die auf dieser Abfrage basiert.

    a. Geben Sie unter Gruppendetails für Gruppenname einen Namen für Ihre Ressourcengruppe ein.

    Ein Ressourcengruppenname darf höchstens 128 Zeichen einschließlich Buchstaben, Zahlen, Bindestrichen, Punkten und Unterstrichen enthalten. Der Name darf nicht mit `AWS` oder `aws` beginnen. Diese Namen sind reserviert. Der Name einer Ressourcergruppen muss im und in der aktuellen Region in Ihrem Konto im und in der der in Ihrem Konto im und in der der der

    b. (Optional) Geben Sie in Group description (Gruppenbeschreibung) eine Beschreibung Ihrer Gruppe ein.

    c. (Optional) Fügen Sie in Group tags (Gruppen-Tags) Tag-Schlüssel-Wert-Paare hinzu, die nur für die Ressourcengruppe und nicht für die Mitgliedsressourcen in der Gruppe gelten.

    Gruppen-Tags sind nützlich, wenn Sie diese Gruppe zum Mitglied einer größeren Gruppe machen möchten. Da zum Erstellen einer Gruppe mindestens ein Tag-Schlüssel angegeben werden muss, müssen Sie in Group tags (Gruppen-Tags) mindestens einen Tag-Schlüssel zu Gruppen hinzufügen, die Sie in größere Gruppen verschachteln möchten.

8. Wenn Sie fertig sind, wählen Sie Gruppe erstellen.

AWS CLI & AWS SDKs

Eine Tag-basierte Gruppe basiert auf einer Abfrage des Typs `TAG_FILTERS_1_0`.

1. Geben Sie in einer AWS CLI-Sitzung Folgendes ein und drücken Sie anschließend die Eingabetaste. Ersetzen Sie die Werte für Gruppenname, Beschreibung, Ressourcensparend, Tag-Schlüssel und Tag-Werte durch eigene Werte. Beschreibungen dürfen maximal 512 Zeichen enthalten, einschließlich Buchstaben, Zahlen, Bindestrichen, Unterstrichen, Satzzeichen und Leerzeichenn. Sie können maximal 20 Ressourcentypen in einer Abfrage verwenden. Ein Ressourcengruppenname darf höchstens 128 Zeichen einschließlich Buchstaben, Zahlen, Bindestrichen, Punkten und Unterstrichen enthalten. Der Name darf nicht mit `AWS` oder `aws` beginnen. Diese Namen sind reserviert. Ein Ressourcengruppenname muss in Ihrem Konto eindeutig sein.

   Es ist mindestens ein Wert für `ResourceTypeFilters` erforderlich. Um alle Ressourcentypen anzugeben, verwenden Sie `AWS::AllSupported` als Wert für `ResourceTypeFilters`.

```
$ aws resource-groups create-group \
    --name resource-group-name \
    --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
\":[\"resource_type1\",\"resource_type2\"],\"TagFilters\":[{\"Key\":\"Key1\",
\"Values\":[\"Value1\",\"Value2\"]},{\"Key\":\"Key2\",\"Values\":[\"Value1\",
\"Value2\"]}]}"}'
```

   Nachfolgend finden Sie einen Beispielbefehl.

```
$ aws resource-groups create-group \
    --name my-resource-group \
    --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
\":[\"AWS::EC2::Instance\"],\"TagFilters\":[{\"Key\":\"Stage\",\"Values\":
[\"Test\"]}]}"}'
```

   Mit dem folgenden Befehl werden alle unterstützten Ressourcentypen eingeschlossen.

```
$ aws resource-groups create-group \
    --name my-resource-group \
```

```
    --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
\":[\"AWS::AllSupported\"],\"TagFilters\":[{\"Key\":\"Stage\",\"Values\":[\"Test
\"]}]}"}'
```

2. Die Antwort auf den Befehl gibt Folgendes zurück.

   - Eine vollständige Beschreibung der von Ihnen erstellten Gruppe.
   - Die von Ihnen zum Erstellen der Gruppe verwendete Ressourcenabfrage.
   - Die der Gruppe zugeordneten Tags.

Erstellen Sie eineAWS CloudFormation stapelbasierte Gruppe

Die folgenden Verfahren zeigen Ihnen, wie Sie eine stapelbasierte Abfrage erstellen und damit eine Ressourcengruppe erstellen.

Console

1. Melden Sie sich an der AWS Resource Groups-Konsole an.
2. Wählen Sie im Navigationsbereich die Option Ressourcergruppen.
3. Wählen Sie unter Abfragebasierte Gruppe erstellen unter Gruppentyp den CloudFormation stapelbasierten Gruppentyp aus.
4. Wählen Sie den Stack aus, den Sie als Grundlage Ihrer Gruppe verwenden möchten. Eine Ressourcengruppe kann nur auf einem einzelnen Stack basieren. Um die Liste der Stacks zu filtern, beginnen Sie mit der Eingabe des Namens des Stacks. Nur Stacks mit unterstützten Statusarten werden in der Liste angezeigt.
5. Wählen Sie die Ressourcentypen im Stack aus, die in der Gruppe enthalten sein sollen. Behalten Sie für diese Anleitung die Standardeinstellung bei, All supported resource types (Alle unterstützten Ressourcentypen). Weitere Informationen dazu, welche Ressourcentypen unterstützt werden und in der Gruppe enthalten sein können, finden Sie unter Ressourcentypen, die Sie mit AWS Resource Groups und Tag Editor verwenden können.
6. Wählen Sie View group resources (Gruppenressourcen anzeigen) aus, um die Liste der Ressourcen im AWS CloudFormation-Stack zurückzugeben, die mit den von Ihnen ausgewählten Ressourcentypen übereinstimmen.
7. Nachdem Sie die gewünschten Ergebnisse erhalten haben, erstellen Sie eine Gruppe, die auf dieser Abfrage basiert.

a. Geben Sie unter Gruppendetails für Gruppenname einen Namen für Ihre Ressourcengruppe ein.

   Ein Ressourcengruppenname darf höchstens 128 Zeichen einschließlich Buchstaben, Zahlen, Bindestrichen, Punkten und Unterstrichen enthalten. Der Name darf nicht mit `AWS` oder `aws` beginnen. Diese Namen sind reserviert. Der Name einer Ressourcergruppen muss im und in der aktuellen Region in Ihrem Konto im und in der der in Ihrem Konto im und in der der der

b. (Optional) Geben Sie in Group description (Gruppenbeschreibung) eine Beschreibung Ihrer Gruppe ein.

c. (Optional) Fügen Sie in Group tags (Gruppen-Tags) Tag-Schlüssel-Wert-Paare hinzu, die nur für die Ressourcengruppe und nicht für die Mitgliedsressourcen in der Gruppe gelten.

   Gruppen-Tags sind nützlich, wenn Sie diese Gruppe zum Mitglied einer größeren Gruppe machen möchten. Da zum Erstellen einer Gruppe mindestens ein Tag-Schlüssel angegeben werden muss, müssen Sie in Group tags (Gruppen-Tags) mindestens einen Tag-Schlüssel zu Gruppen hinzufügen, die Sie in größere Gruppen verschachteln möchten.

8. Wenn Sie fertig sind, wählen Sie Gruppe erstellen.

AWS CLI & AWS SDKs

Eine AWS CloudFormation-Stack-basierte Gruppe basiert auf einer Abfrage des Typs `CLOUDFORMATION_STACK_1_0`.

1. Führen Sie den folgenden Befehl aus und ersetzen Sie die Werte für Gruppenname, Beschreibung, Stack-ID und Ressourcentypen durch Ihre eigenen. Beschreibungen dürfen maximal 512 Zeichen enthalten, einschließlich Buchstaben, Zahlen, Bindestrichen, Unterstrichen, Satzzeichen und Leerzeichenn.

   Wenn Sie keine Ressourcentypen angeben, schließt Resource Groups alle unterstützten Ressourcentypen in den Stapel ein. Sie können maximal 20 Ressourcentypen in einer Abfrage verwenden. Ein Ressourcengruppenname darf höchstens 128 Zeichen einschließlich Buchstaben, Zahlen, Bindestrichen, Punkten und Unterstrichen enthalten. Der Name darf nicht mit `AWS` oder `aws` beginnen. Diese Namen sind reserviert. Ein Ressourcengruppenname muss in Ihrem Konto eindeutig sein.

Der *stack_identifier* ist der Stack-ARN wie im Beispielbefehl gezeigt.

```
$ aws resource-groups create-group \
    --name group_name \
    --description "description" \
    --resource-query
 '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"StackIdentifier\":
\"stack_identifier\",\"ResourceTypeFilters\":[\"resource_type1\",
\"resource_type2\"]}"}'
```

Nachfolgend finden Sie einen Beispielbefehl.

```
$ aws resource-groups create-group \
    --name My-CFN-stack-group \
    --description "My first CloudFormation stack-based group" \
    --resource-query
 '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"StackIdentifier\":
\"arn:aws:cloudformation:us-west-2:123456789012:stack\/AWStestuseraccount\/
fb0d5000-aba8-00e8-aa9e-50d5cEXAMPLE\",\"ResourceTypeFilters\":
[\"AWS::EC2::Instance\",\"AWS::S3::Bucket\"]}"}'
```

2. Die Antwort auf den Befehl gibt Folgendes zurück.

   - Eine vollständige Beschreibung der von Ihnen erstellten Gruppe.
   - Die von Ihnen zum Erstellen der Gruppe verwendete Ressourcenabfrage.

Gruppen aktualisieren in AWS Resource Groups

Um eine tagbasierte Ressourcengruppe in Resource Groups zu aktualisieren, können Sie die Abfrage und die Tags bearbeiten, die die Grundlage Ihrer Gruppe bilden. Sie können nur durch Anwenden von Änderungen auf die Abfrage oder die Tags Ressourcen zu Ihrer Gruppe hinzufügen oder aus Ihrer Gruppe entfernen. Sie können keine spezifischen Ressourcen auswählen, um sie zu Ihrer Gruppe hinzuzufügen oder aus Ihrer Gruppe zu entfernen. Der beste Weg, eine bestimmte Ressource zu einer Gruppe hinzuzufügen oder daraus zu entfernen, besteht darin, die Tags der Ressource zu bearbeiten. Stellen Sie dann sicher, dass Ihre Ressourcengruppen-Tag-Abfrage das Tag entweder enthält oder weglässt, je nachdem, ob Sie die Ressource in Ihrer Gruppe haben möchten.

Um eine AWS CloudFormation stapelbasierte Ressourcengruppe zu aktualisieren, können Sie einen anderen Stapel auswählen. Sie können dem Stapel, die Sie der Gruppe angehören möchten, auch Ressourcentypen hinzufügen oder daraus entfernen. Um die Ressourcen zu ändern, die im Stack verfügbar sind, aktualisieren Sie die AWS CloudFormation-Vorlage, um den Stack zu erstellen, und aktualisieren anschließend den Stack in AWS CloudFormation. Weitere Informationen zum Aktualisieren eines AWS CloudFormation AWS CloudFormationStacks finden Sie unter Stapelaktualisierungen im AWS CloudFormationBenutzerhandbuch.

In der AWS CLI können Sie Gruppen über zwei Befehle aktualisieren.

- `update-group` zur Aktualisierung der Beschreibung einer Gruppe.
- `update-group-query` zur Aktualisierung der Ressourcenabfrage und der Tags, die die Mitgliedsressourcen der Gruppe festlegen.

In der Konsole können Sie eine AWS CloudFormation stapelbasierte Gruppe nicht in eine tagbasierte Abfragegruppe ändern oder umgekehrt. Sie können dies mithilfe der Resource Groups API tun, unter anderem in derAWS CLI.

Tag-basierte Abfragegruppen aktualisieren

Console

Sie aktualisieren eine Tag-basierte Gruppe, indem Sie die Ressourcentypen oder Tags in der Abfrage ändern, auf der die Gruppe basiert. Sie können auch die Beschreibung der Gruppe hinzufügen oder ändern.

1. Melden Sie sich an der AWS Resource Groups-Konsole an.
2. Wählen Sie im Navigationsbereich unter Gespeicherte Resource Groups den Namen der Gruppe aus, und klicken Sie dann auf Bearbeiten.

> **Note**
>
> Sie können nur Ressourcengruppen deren Eigentümer Sie Sie Sie sind. In der Spalte Besitzer wird die Kontoinhaberschaft für jede Ressourcengruppe angezeigt. Alle Gruppen mit einem anderen Kontoinhaber als dem, bei dem Sie angemeldet sind, wurden erstelltAWS License Manager. Weitere Informationen finden Sie

unter Hostressourcengruppen AWS License Manager im License Manager Benutzerhandbuch.

3. Fügen Sie auf der Seite Gruppe bearbeiten unter Gruppierungskriterien Ressourcentypen hinzu oder entfernen Sie sie. Sie können maximal 20 Ressourcentypen in einer Abfrage verwenden. Um einen Ressourcentyp zu entfernen, wählen Sie das X auf der Beschriftung des Ressourcentyps aus. Wählen Sie View group resources (Gruppenressourcen anzeigen) aus, um zu sehen, wie sich die Änderungen auf die Ressourcenmitglieder Ihrer Gruppe auswirken. In dieser Anleitung wird der Ressourcentyp AWS::RDS::DBInstance zur Abfrage hinzugefügt.
4. Bearbeiten Sie die Tags immer noch unter Gruppierungskriterien nach Bedarf. In diesem Beispiel wird nach Ressourcen mit dem Tag-Schlüssel Stage (Phase) und dem Tag-Wert Test (Test) gefiltert. Der Tag-Wert ist optional, engt jedoch die Ergebnisse der Abfrage weiter ein. Um ein Tag zu entfernen, wählen Sie X auf der Beschriftung des Tags aus.
5. Im Bereich Additional information (Zusätzliche Informationen) können Sie die Beschreibung der Gruppe bearbeiten. Sie können den Namen einer Gruppe nicht mehr bearbeiten, nachdem die Gruppe erstellt wurde.
6. (Optional) Sie können unter Tag-Gruppen Tags hinzufügen oder entfernen. Gruppen-Tags sind Metadaten für Ihre Ressourcengruppe. Sie haben keine Auswirkungen auf Mitgliedsressourcen. Um die Ressourcen zu ändern, die von der Abfrage der Ressourcengruppe zurückgegeben werden, bearbeiten Sie die Tags unter Gruppierungskriterien.

   Gruppen-Tags sind nützlich, wenn Sie diese Gruppe zum Mitglied einer größeren Gruppe machen möchten. Die Angabe mindestens eines Tag-Schlüssels ist erforderlich, um eine Gruppe zu erstellen. Stellen Sie daher sicher, dass Sie Gruppen, die Sie in größeren Gruppen unterteilen möchten, mindestens einen Tag-Schlüssel unter Gruppentags hinzufügen.
7. Wählen Sie Vorschau der Gruppenressourcen aus, um die aktualisierte Liste der EC2-Instances, S3-Buckets und Amazon RDS-Datenbank-Instances in Ihrem Konto abzurufen, die den angegebenen Tag-Schlüsseln entsprechen. Wenn die erwarteten Ressourcen nicht in der Liste enthalten sind, prüfen Sie, ob die Ressourcen mit den Tags markiert sind, die Sie in Grouping criteria (Gruppierungskriterien) angegeben haben.
8. Klicken Sie auf Save changes (Änderungen speichern), wenn Sie fertig sind.

AWS CLI & AWS SDKs

Sie aktualisieren die Abfrage einer Gruppe und die Beschreibung einer Ressourcengruppe in der AWS CLI mit zwei verschiedenen Befehlen. Die Namen vorhandener Gruppen können nicht bearbeitet werden. In der AWS CLI können Sie eine tagbasierte Gruppe in eine CloudFormation stapelbasierte Gruppe ändern oder umgekehrt.

1. Wenn Sie die Beschreibung Ihrer Gruppe nicht ändern möchten, überspringen Sie diesen Schritt und fahren mit dem nächsten Schritt fort. Geben Sie in einer AWS CLI-Sitzung Folgendes ein und drücken Sie anschließend die Eingabetaste. Ersetzen Sie die Werte für den Gruppennamen und die Beschreibung durch eigene Werte.

   ```
   $ aws resource-groups update-group \
       --group-name resource-group-name \
       --description "description_text"
   ```

   Nachfolgend finden Sie einen Beispielbefehl.

   ```
   $ aws resource-groups update-group \
       --group-name my-resource-group \
       --description "EC2 instances, S3 buckets, and RDS DBs that we are using for
    the test stage."
   ```

   Der Befehl gibt eine vollständige und aktualisierte Beschreibung der Gruppe zurück.

2. Geben Sie den folgenden Befehl ein, um die Abfrage und die Tags einer Gruppe zu aktualisieren. Ersetzen Sie die Werte für Gruppennamen, Ressourcentypen, Tag-Schlüssel und Tag-Werte durch Ihre eigenen. Drücken Sie dann die Eingabetaste. Sie können maximal 20 Ressourcentypen in einer Abfrage verwenden.

   ```
   $ aws resource-groups update-group-query \
       --group-name resource-group-name \
       --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
   \":[\"resource_type1\",\"resource_type2\"],\"TagFilters\":[{\"Key\":\"Key1\",
   \"Values\":[\"Value1\",\"Value2\"]},{\"Key\":\"Key2\",\"Values\":[\"Value1\",
   \"Value2\"]}]}"}'
   ```

   Nachfolgend finden Sie einen Beispielbefehl.

   ```
   $ aws resource-groups update-group-query \
   ```

```
    --group-name my-resource-group \
    --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
\":[\"AWS::EC2::Instance\",\"AWS::S3::Bucket\",\"AWS::RDS::DBInstance\"],
\"TagFilters\":[{\"Key\":\"Stage\",\"Values\":[\"Test\"]}]}"}'
```

Der Befehl gibt als Ergebnis die aktualisierte Abfrage zurück.

Eine AWS CloudFormation stapelbasierte Gruppe aktualisieren

Console

In der können Sie eine AWS CloudFormation stapelbasierte Gruppe nicht in eine tagbasierte Gruppe ändern. AWS Management Console Sie können jedoch den Stack ändern, auf dem die Gruppe basiert, oder die Stack-Ressourcentypen ändern, die Sie in die Gruppe aufnehmen möchten. Sie können auch die Beschreibung der Gruppe hinzufügen oder ändern.

1. Melden Sie sich an der AWS Resource Groups-Konsole an.
2. Wählen Sie im Navigationsbereich unter Gespeicherte Ressourcengruppen den Namen der Gruppe aus, und klicken Sie dann auf Bearbeiten.
3.
> **Note**
>
> Sie können nur Ressourcengruppen deren Eigentümer Sie Sie Sie sind. In der Spalte Besitzer wird die Kontoinhaberschaft für jede Ressourcengruppe angezeigt. Alle Gruppen mit einem anderen Kontoinhaber als dem, bei dem Sie angemeldet sind, wurden erstelltAWS License Manager. Weitere Informationen finden Sie unter Hostressourcengruppen AWS License Manager im License Manager Benutzerhandbuch.

4. Um auf der Seite Gruppe bearbeiten unter Gruppierungskriterien den Stapel zu ändern, auf dem Ihre Gruppe basiert, wählen Sie den Stapel aus der Dropdownliste aus. Eine Ressourcengruppe kann nur auf einem einzelnen Stack basieren. Um die Liste der Stacks zu filtern, beginnen Sie mit der Eingabe des Namens des Stacks. Nur Stacks mit unterstützten Statusarten werden in der Liste angezeigt. Die Liste der unterstützten Statusarten finden Sie unter Erstellen von abfragebasierten Gruppen inAWS Resource Groups in diesem Handbuch.
5. Fügen Sie Ressourcentypen hinzu oder entfernen Sie Ressourcentypen. Nur im Stack verfügbare Ressourcentypen werden in der Dropdown-Liste angezeigt. Der Standardwert ist All supported resource types (Alle unterstützten Ressourcentypen). Sie können maximal

20 Ressourcentypen in einer Abfrage verwenden. Um einen Ressourcentyp zu entfernen, wählen Sie das X auf der Beschriftung des Ressourcentyps aus. Weitere Informationen dazu, welche Ressourcentypen unterstützt werden und in der Gruppe enthalten sein können, finden Sie unter Ressourcentypen, die Sie mit AWS Resource Groups und Tag Editor verwenden können.

6. Wählen Sie Gruppenressourcen in der Vorschau anzeigen, um die Liste der Ressourcen im AWS CloudFormation Stapel abzurufen, die Ihren ausgewählten Ressourcentypen entsprechen.
7. Im Bereich Additional information (Zusätzliche Informationen) können Sie die Beschreibung der Gruppe bearbeiten. Sie können den Namen einer Gruppe nicht mehr bearbeiten, nachdem die Gruppe erstellt wurde.
8. Fügen Sie in Group tags (Gruppen-Tags) Tags hinzu oder entfernen Sie Tags. Gruppen-Tags sind Metadaten für Ihre Ressourcengruppe. Sie haben keine Auswirkungen auf Mitgliedsressourcen. Um die Ressourcen zu ändern, die von der Abfrage der Ressourcengruppe zurückgegeben werden, bearbeiten Sie die Tags in Grouping criteria (Gruppierungskriterien).

   Gruppen-Tags sind nützlich, wenn Sie diese Gruppe zum Mitglied einer größeren Gruppe machen möchten. Die Angabe mindestens eines Tag-Schlüssels ist erforderlich, um eine Gruppe zu erstellen. Stellen Sie daher sicher, dass Sie Gruppen, die Sie in größeren Gruppen unterteilen möchten, mindestens einen Tag-Schlüssel unter Gruppentags hinzufügen.
9. Klicken Sie auf Save changes (Änderungen speichern), wenn Sie fertig sind.

AWS CLI & AWS SDKs

Sie aktualisieren die Abfrage einer Gruppe und die Beschreibung einer Ressourcengruppe in der AWS CLI mit zwei verschiedenen Befehlen. Die Namen vorhandener Gruppen können nicht bearbeitet werden. In der AWS CLI können Sie eine tagbasierte Gruppe in eine CloudFormation stapelbasierte Gruppe ändern oder umgekehrt.

1. Wenn Sie die Beschreibung Ihrer Gruppe nicht ändern möchten, überspringen Sie diesen Schritt und fahren mit dem nächsten Schritt fort. Führen Sie den folgenden Befehl aus und ersetzen Sie die Werte für den Gruppennamen und die Beschreibung durch Ihre eigenen.

```
$ aws resource-groups update-group \
    --group-name "resource-group-name" \
```

```
    --description "description_text"
```

Nachfolgend finden Sie einen Beispielbefehl.

```
$ aws resource-groups update-group \
    --group-name "My-CFN-stack-group" \
    --description "EC2 instances, S3 buckets, and RDS DBs that we are using for
 the test stage."
```

Der Befehl gibt eine vollständige und aktualisierte Beschreibung der Gruppe zurück.

2. Führen Sie den folgenden Befehl aus, um die Abfrage und Tags einer Gruppe zu aktualisieren. Ersetzen Sie die Werte für Gruppennamen, Stack-ID und Ressourcentypen durch Ihre eigenen. Um Ressourcentypen hinzuzufügen, geben Sie die vollständige Liste der Ressourcentypen im Befehl an, nicht nur die Ressourcentypen, die Sie hinzufügen. Sie können maximal 20 Ressourcentypen in einer Abfrage verwenden.

   Der *stack_identifier* ist der Stack-ARN wie im Beispielbefehl gezeigt.

```
$ aws resource-groups update-group-query \
    --group-name resource-group-name \
    --description "description" \
    --resource-query
 '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"StackIdentifier\":
\"stack_identifier\",\"ResourceTypeFilters\":[\"resource_type1\",
\"resource_type2\"]}"}'
```

Nachfolgend finden Sie einen Beispielbefehl.

```
$ aws resource-groups update-group-query \
    --group-name "my-resource-group" \
    --description "Updated CloudFormation stack-based group" \
    --resource-query
 '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"StackIdentifier\":
\"arn:aws:cloudformation:us-west-2:810000000000:stack\/AWStestuseraccount
\/fb0d5000-aba8-00e8-aa9e-50d5cEXAMPLE\",\"ResourceTypeFilters\":
[\"AWS::EC2::Instance\",\"AWS::S3::Bucket\"]}"}'
```

Der Befehl gibt als Ergebnis die aktualisierte Abfrage zurück.

Ereignisse im Gruppenlebenszyklus: Überwachung von Ressourcengruppen auf Änderungen

Nachdem Sie Ihre Ressourcen in Gruppen organisiert haben, können Sie diese Gruppen auf Änderungen hin überwachen, die Ihnen als Ereignisse auffallen.AWS Resource Groups Sie können eine Benachrichtigung über ein Gruppenereignis als Signal erhalten, um Maßnahmen zu ergreifen. Sie könnten beispielsweise eine Benachrichtigung konfigurieren, die gesendet wird, wenn sich die Mitgliedschaft einer Gruppe ändert. Sie könnten ein Ereignis beim Hinzufügen eines neuen Gruppenmitglieds verwenden, um eine Lambda-Funktion auszulösen, die die Änderung programmgesteuert überprüft, um sicherzustellen, dass neue Gruppenmitglieder die von Ihrer Organisation festgelegten Compliance-Anforderungen erfüllen. Eine solche Lambda-Funktion könnte eine automatische Korrektur für alle neuen Gruppenmitglieder durchführen, die diese Anforderungen nicht erfüllen. Ein Ereignis, das durch die Entfernung eines Gruppenmitglieds verursacht wird, kann eine Lambda-Funktion auslösen, die alle erforderlichen Bereinigungen durchführt, z. B. das Löschen verknüpfter Ressourcen.

Indem Sie Gruppen-Lifecycle-Ereignisse für Ihre Ressourcengruppen aktivieren, ermöglichen Sie, dass Ereignisse im Zusammenhang mit Änderungen an Ihren Gruppen von Amazon erfasst EventBridge und allen verschiedenen EventBridge unterstützten Zieldiensten zur Verfügung gestellt werden. Sie können diese Zieldienste dann so konfigurieren, dass sie automatisch alle Maßnahmen ergreifen, die Ihr Szenario erfordert. Zu diesen Zielen gehören Amazon Simple Notification Service (Amazon SNS), Amazon Simple Queue Service (Amazon SQS), Amazon Simple Queue Service (Amazon SQS) und verfügbarAWS Lambda.AWS Mit Diensten wie Lambda können Ihre Ereignisse programmatische Reaktionen auslösen, die Code verwenden, um die von Ihnen benötigten Aktionen auszuführen. Eine Liste derAWS Services, mit denen Sie Targeting durchführen können EventBridge, finden Sie unter EventBridge Amazon-Ziele im EventBridge Amazon-Benutzerhandbuch.

Wenn Sie Gruppen-Lebenszyklusereignisse aktivieren, werden die folgenden ElementeAWS Resource Groups erstellt:

- EineAWS Identity and Access Management (IAM) serviceverknüpfte Rolle, die berechtigt ist, Ihre Ressourcen auf Änderungen an ihren Tags und IhreAWS CloudFormation Stacks auf Änderungen an den Ressourcen, die Teil eines Stacks sind, zu überwachen.
- Eine von Resource Groups verwaltete EventBridge Regel, die die Details aller Tag- oder Stack-Änderungen an Ihren Ressourcen erfasst. EventBridge verwendet diese Regel, um Resource Groups über diese Änderungen zu informieren. Anschließend generiert Resource Groups

Mitgliedschaftsereignisse, an die EventBridge Sie Ihre benutzerdefinierten Regeln zur Verarbeitung senden können.

Die dienstverknüpfte Rolle kann nur vom Resource Groups Groups-Dienst übernommen werden. Weitere Informationen zu der serviceverknüverknüverknüverknüverknüverknüverknüruppe erstellen, finden Sie unterVerwenden von serviceverknüpften Rollen für Resource Groups.

Wenn diese Funktion aktiviert ist, generiert Resource Groups ein Ereignis, wenn Sie eine der folgenden Änderungen an einer Ressourcengruppe vornehmen:

- Erstellen Sie
- Aktualisieren Sie die Abfrage, die die Mitgliedschaft einer abfragebasierten Ressourcengruppe definiert.
- Aktualisieren Sie die Konfiguration einer dienstverknüpften Ressourcengruppe.
- Aktualisieren Sie die Beschreibung einer Ressourcengruppe.
- Löschen Sie eine Ressourcengruppe.
- Ändern Sie die Mitgliedschaft einer Ressourcengruppe, indem Sie der Gruppe eine Ressource hinzufügen oder daraus entfernen. Eine Änderung der Mitgliedschaft kann auch erfolgen, wenn sich die Tags ändern oder wenn sich einAWS CloudFormation Stapel ändert.

Important

- Um Gruppenereignisse erfolgreich zu empfangen und darauf zu reagieren, müssen Sie Änderungen sowohl an den Resource Groups als auch an EventBridge. Sie können die Änderungen in beliebiger Reihenfolge durchführen, aber Gruppenereignisse werden erst dann für EventBridge Ziele veröffentlicht, wenn Sie Änderungen an beiden Diensten vorgenommen haben.

- Die Änderungen an der Ressourcengruppe beinhalten keine Änderungen an Tags, die der Ressourcengruppe selbst zugeordnet sind. Um Ereignisse auf der Grundlage von Tag-Änderungen an Ihren Gruppen zu generieren, müssen Sie eine EventBridge Regel verwenden, die die`aws.tag` Quelle anstelle der`aws.resource-groups` Quelle verwendet. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch unter Tag-Änderungsereignisse aufAWS Ressourcen.

Themen

- Aktivieren von Gruppenlebenszyklusereignissen in Resource Groups
- Erstellen einer - EventBridge Regel zum Erfassen von Gruppenlebenszyklusereignissen und zum Veröffentlichen von Benachrichtigungen
- Deaktivierung von Gruppen-Lifecycle-Ereignissen
- Struktur und Syntax von Resource-Groups-Lebenszyklusereignissen

Aktivieren von Gruppenlebenszyklusereignissen in Resource Groups

Um Benachrichtigungen über Lebenszyklusänderungen an Ihren Ressourcengruppen zu erhalten, können Sie die Option Ereignisse im Gruppenlebenszyklus aktivieren. Resource Groups bietet dann Informationen über die Änderungen Ihrer Gruppen an Amazon EventBridge. In können Sie die Änderungen anhand von Regeln EventBridge, die Sie im EventBridge Service definieren, bewerten und darauf reagieren.

> **Mindestberechtigungen**
>
> Um Gruppenlebenszyklusereignisse in Ihrem zu aktivierenAWS-Konto, müssen Sie sich als AWS Identity and Access Management (IAM-) Principal mit den folgenden Berechtigungen anmelden:
>
> - `resource-groups:UpdateAccountSettings`
> - `iam:CreateServiceLinkedRole`
> - `events:PutRule`
> - `events:PutTargets`
> - `events:DescribeRule`
> - `events:ListTargetsByRule`
> - `cloudformation:DescribeStacks`
> - `cloudformation:ListStackResources`
> - `tag:GetResources`

Wenn Sie Gruppenlebenszyklusereignisse zum ersten Mal in einer aktivierenAWS-Konto, erstellt Resource Groups eine dienstverknüpfte Rolle mit dem Namen `AWSServiceRoleForResourceGroups`. Diese verwaltete Rolle hat die Berechtigung, eine

verwaltete EventBridge Regel für Resource Groups zu verwenden. Die Regel überwacht die mit Ihren Ressourcen verknüpften Tags und die AWS CloudFormation Stapel in Ihrem Konto auf Änderungen. Resource Groups veröffentlicht diese Änderungen dann am Standard-Event-Bus in Amazon EventBridge. Der Service erstellt auch eine EventBridge verwaltete Regel mit dem Namen`Managed.ResourceGroups.TagChangeEvents`. Diese Regel erfasst die Details der Tag-Änderungen Ihrer Ressourcen. Auf diese Weise können Resource Groups Mitgliedschaftsereignisse generieren, an die sie EventBridge senden können, damit Ihre benutzerdefinierten Regeln verarbeitet werden können. Ihre EventBridge Regeln können dann auf Ereignisse reagieren, indem sie Benachrichtigungen an die konfigurierten Ziele der Regeln senden.

Nachdem Sie diese Schritte abgeschlossen haben, sollten Regeln, die nach diesen Ereignissen suchen, in wenigen Minuten damit beginnen, sie zu empfangen.

Sie können Gruppenlebenszyklusereignisse entweder mithilfe von AWS Management Console oder mithilfe eines Befehls aus der AWS CLI oder einer der SDK-APIs aktivieren.

AWS Management Console

So aktivieren Sie Gruppenlebenszyklusereignisse in der Resource Groups Groups-Konsole

1. Öffnen Sie die Seite „Einstellungen“ in der Ressourcengruppen-Konsole.
2. Wählen Sie im Abschnitt Ereignisse im Gruppenlebenszyklus den Schalter neben Benachrichtigungen sind ausgeschaltet.
3. Wählen Sie im Bestätigungsdialogfeld die Option Benachrichtigungen aktivieren aus.

   Der Funktionsschalter zeigt an, dass Benachrichtigungen aktiviert sind.

Damit ist der erste Teil des Prozesses abgeschlossen. Nachdem Sie die Ereignisbenachrichtigungen aktiviert haben, können Sie in Amazon Regeln erstellen EventBridge, die die Ereignisse erfassen und sie AWS-Services zur Verarbeitung an bestimmte Personen senden.

AWS CLI

Um Ereignisse im Gruppenlebenszyklus mithilfe der SDKs AWS CLI oder der AWS SDKs zu aktivieren

Das folgende Beispiel zeigt, wie Sie mithilfe von Gruppenlebenszyklusereignisse in Resource Groups aktivieren können. AWS CLI Geben Sie den Befehl mit dem Dienstprinzipalparameter

genau wie in der Abbildung gezeigt ein. Die Ausgabe zeigt sowohl den aktuellen Status als auch den gewünschten Status des Features.

```
$ aws resource-groups update-account-settings \
    --group-lifecycle-events-desired-status ACTIVE
{
    "AccountSettings": {
        "GroupLifecycleEventsDesiredStatus": "ACTIVE",
        "GroupLifecycleEventsStatus": "IN_PROGRESS"
    }
}
```

Sie können überprüfen, ob die Funktion aktiviert ist, indem Sie den folgenden Beispielbefehl ausführen. Wenn beide Statusfelder denselben Wert anzeigen, ist der Vorgang abgeschlossen.

```
$ aws resource-groups get-account-settings
{
    "AccountSettings": {
        "GroupLifecycleEventsDesiredStatus": "ACTIVE",
        "GroupLifecycleEventsStatus": "ACTIVE"
    }
}
```

Weitere Informationen finden Sie in den folgenden Ressourcen:

- AWS CLI— AWS-Ressourcengruppen update-account-settings und AWS-Ressourcengruppen get-account-settings
- UpdateAccountSettingsAPI — und GetAccountSettings

Erstellen einer - EventBridge Regel zum Erfassen von Gruppenlebenszyklusereignissen und zum Veröffentlichen von Benachrichtigungen

Sie können Gruppenlebenszyklusereignisse für Ihre Ressourcengruppen in aktivierenAWS Resource Groups, um Ereignisse in Amazon zu veröffentlichen EventBridge. Anschließend können Sie Regeln erstellen EventBridge, die auf diese Ereignisse reagieren, indem Sie sie AWS-Services zur weiteren Verarbeitung an andere senden.

AWS CLI

Der Prozess zum Erstellen einer Regel in EventBridge , die Ereignisse erfasst und an den gewünschten Zielservice sendet, verwendet zwei separate CLI-Befehle:

1. Erstellen Sie die EventBridge Regel, um die gewünschten Ereignisse zu erfassen
2. Anfügen eines Ziels, das die Ereignisse verarbeiten kann, an die EventBridge Regel

Schritt 1: Erstellen der EventBridge Regel zur Erfassung der Ereignisse

Mit dem folgenden AWS CLI `put-rule` Beispielbefehl wird eine EventBridge Regel erstellt, die all eLebenszyklusereignisänderungen für Ressourcengruppen erfasst.

```
$ aws events put-rule \
    --name "CatchAllResourceGroupEvents" \
    --event-pattern '{"source":["aws.resource-groups"]}'
{
    "RuleArn": "arn:aws:events:us-east-1:123456789012:rule/
CatchAllResourceGroupEvents"
}
```

Die Ausgabe enthält den Amazon-Ressourcennamen (ARN) der neuen Regel.

> **Note**
>
> Parameterwerte, die Zeichenfolgen in Anführungszeichen enthalten, haben je nach verwendetem Betriebssystem und Shell unterschiedliche Formatierungsregeln. Für die Beispiele in diesem Handbuch zeigen wir Befehle, die auf einer Linux-BASH-Shell funktionieren. Anweisungen zum Formatieren von Zeichenfolgen mit eingebetteten Anführungszeichen für andere Betriebssysteme, z. B. die Windows-Eingabeaufforderung, finden Sie unter Verwenden von Anführungszeichen in Zeichenfolgen im AWS Command Line Interface -Benutzerhandbuch.
> Wenn Parameterzeichenfolgen komplexer werden, kann es einfacher und weniger fehleranfällig sein, einen Parameterwert aus einer Textdatei zu akzeptieren, anstatt ihn direkt in die Befehlszeile einzugeben.

Das folgende Ereignismuster beschränkt die Ereignisse auf diejenigen, die sich auf die angegebene Gruppe beziehen, die durch ihren ARN identifiziert wird. Dieses Ereignismuster

ist eine komplexe JSON-Zeichenfolge, die viel weniger lesbar ist, wenn sie in eine einzeilige, ordnungsgemäß mit Escape-Zeichen versehene JSON-Zeichenfolge komprimiert wird. Sie können sie stattdessen in einer Datei speichern.

Speichern Sie die JSON-Zeichenfolge des Ereignismusters in einer Datei. Im folgenden Codebeispiel lautet die Datei `eventpattern.txt`.

```
{
    "source": [ "aws.resource-groups" ],
    "detail": {
        "group": {
            "arn": [ "my-resource-group-arn" ]
        }
    }
}
```

Führen Sie dann den folgenden Befehl aus, um die Regel zu erstellen und das benutzerdefinierte Ereignismuster aus der Datei abzurufen.

```
$ aws events put-rule \
    --name "CatchResourceGroupEventsForMyGroup" \
    --event-pattern file://eventpattern.txt
{
    "RuleArn": "arn:aws:events:us-east-1:123456789012:rule/
CatchResourceGroupEventsForMyGroup"
}
```

Um andere Arten von Resource-Groups-Ereignissen zu erfassen, ersetzen Sie die `--event-pattern` Zeichenfolge durch Filter wie die im Abschnitt Beispiel für EventBridge benutzerdefinierte Ereignismuster für verschiedene Anwendungsfälle.

Schritt 2: Anfügen eines Ziels, das die Ereignisse verarbeiten kann, an die EventBridge Regel

Da Sie nun über eine Regel verfügen, die die für Sie interessanten Ereignisse erfasst, können Sie ein oder mehrere Ziele anfügen, um eine Art der Verarbeitung der Ereignisse durchzuführen.

Der folgende AWS CLI `put-targets` Befehl fügt ein Amazon Simple Notification Service (Amazon SNS)-Thema mit dem Namen `my-sns-topic` an die Regel an, die Sie im vorherigen Beispiel erstellt haben. Alle Subscriber des Themas erhalten eine Benachrichtigung, wenn eine Änderung an der in der Regel angegebenen Gruppe auftritt.

```
$ aws events put-targets \
    --rule CatchResourceGroupEventsForMyGroup \
    --targets Id=1,Arn=arn:aws:sns:us-east-1:123456789012:my-sns-topic
{
    "FailedEntryCount": 0,
    "FailedEntries": []
}
```

Zu diesem Zeitpunkt werden alle Gruppenänderungen, die dem Ereignismuster in Ihrer Regel entsprechen, automatisch an das konfigurierte Ziel oder die konfigurierten Ziele gesendet. Wenn es sich bei dem Ziel wie im vorherigen Beispiel um ein Amazon SNS-Thema handelt, erhalten alle Abonnenten des Themas eine Nachricht, die das Ereignis enthält, wie unter beschriebenStruktur und Syntax von Resource-Groups-Lebenszyklusereignissen.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- AWS CLI – aws events put-rule und aws events put-targets
- API – PutRule und PutTargets

Erstellen einer Regel, um nur bestimmte Gruppenlebenszyklus-Ereignistypen zu erfassen

Sie können eine Regel mit einem benutzerdefinierten Ereignismuster erstellen, das nur die Ereignisse erfasst, an denen Sie interessiert sind. Ausführliche Informationen zum Filtern eingehender Ereignisse mithilfe eines benutzerdefinierten Ereignismusters finden Sie unter Amazon- EventBridge Ereignisse im Amazon- EventBridge Benutzerhandbuch.

Angenommen, Sie möchten, dass eine Regel nur die Ressourcengruppen-Benachrichtigungen verarbeitet, die die Erstellung einer neuen Ressourcengruppe angeben. Sie könnten ein benutzerdefiniertes Ereignismuster ähnlich dem folgenden Beispiel verwenden.

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group State Change" ],
    "detail": {
        "state-change": "create"
    }
}
```

Dieser Filter erfasst nur die Ereignisse, die genau diese Werte in den angegebenen Feldern haben. Eine vollständige Liste der Felder, die Sie abgleichen können, finden Sie unter Struktur und Syntax von Resource-Groups-Lebenszyklusereignissen.

Deaktivierung von Gruppen-Lifecycle-Ereignissen

Sie können Gruppen-Lifecycle-Ereignisse deaktivieren, um zuAWS Resource Groups verhindern, dass Ereignisse an Amazon gesendet EventBridge werden. Sie können dies tun, indem Sie entweder verwendenAWS Management Console oder einen Befehl vonAWS CLI oder einer der SDK-APIs verwenden.

> **Note**
>
> Durch das Deaktivieren von Gruppen-Lebenszyklusereignissen wird die EventBridge Regel „Verwaltete Resource Groups“ gelöscht, die verwendet wird, um Ihre Ressourcen-Tags undAWS CloudFormation -Stapel auf Änderungen zu überprüfen. Resource Groups können diese Änderungen nicht mehr weitergeben EventBridge. Alle Regeln, die Sie definiert haben und EventBridge die nach Ereignissen von Resource Groups suchen, empfangen keine zu verarbeitenden Ereignisse mehr. Wenn Sie beabsichtigen, Gruppen-Lifecycle-Ereignisse in future wieder zu aktivieren, können Sie Ihre Regeln deaktivieren. Wenn Sie diese Regeln nicht verwenden möchten, können Sie sie löschen). Weitere Informationen finden Sie unter Deaktivierung oder Löschen einer EventBridge Regel im EventBridge Amazon-Benutzerhandbuch.
> Durch das Deaktivieren von Gruppen-Lebenszyklusereignissen wird die dienstverknüpfte Rolle nicht gelöscht. Sie können die servicegebundene Rolle mit IAM löschen). Wenn Sie später die Gruppen-Lifecycle-Ereignisse erneut aktivieren müssen und die serviceverknüpfte Rolle nicht vorhanden ist, wird sie von Resource Groups automatisch neu erstellt.

> **Mindestberechtigungen**
>
> Um Gruppen-Lifecycle-Ereignisse in Ihrem aktuellen Konto zu deaktivierenAWS-Konto, müssen Sie sich alsAWS Identity and Access Management (IAM-) Principal mit den folgenden Berechtigungen anmelden:
>
> - `resource-groups:UpdateAccountSettings`
> - `events:DeleteRule`
> - `events:RemoveTargets`

- `events:DescribeRule`
- `events:ListTargetsByRule`

AWS Management Console

Um Benachrichtigungen über Gruppen-Lifecycle-Ereignisse zu deaktivieren, EventBridge

1. Öffnen Sie die Seite „Einstellungen“ in der Resource Groups Groups-Konsole.
2. Wählen Sie im Abschnitt Gruppen-Lebenszyklusereignisse den Schalter neben Benachrichtigungen sind aktiviert.
3. Wählen Sie im Bestätigungsdialogfeld die Option De).

   Der Funktionsschalter wird angezeigt: Ereignisbenachrichtigungen sind deaktiviert.

Zu diesem Zeitpunkt sendet Resource Groups keine Ereignisse mehr an den EventBridge Standardereignisbus und alle Regeln, die Sie haben, erhalten keine Gruppenbenachrichtigungsereignisse mehr zur Verarbeitung. Sie können diese Regeln optional löschen, um die Bereinigung abzuschließen.

AWS CLI

Um Benachrichtigungen über Gruppen-Lifecycle-Ereignisse zu deaktivieren, EventBridge

Das folgende Beispiel zeigt, wie Sie das verwenden,AWS CLI um Gruppen-Lebenszyklusereignisse in Resource Groups zu deaktivieren.

```
$ aws resource-groups update-account-settings \
    ----group-lifecycle-events-desired-status INACTIVE
{
    "AccountSettings": {
        "GroupLifecycleEventsDesiredStatus": "INACTIVE",
        "GroupLifecycleEventsStatus": "INACTIVE"
    }
}
```

Weitere Informationen finden Sie in den folgenden Ressourcen:

- AWS CLI— AWS-Ressourcengruppen update-account-settings und AWS-Ressourcengruppen get-account-settings
- API — UpdateAccountSettingsund GetAccountSettings

Struktur und Syntax von Resource-Groups-Lebenszyklusereignissen

Die Lebenszyklusereignisse für AWS Resource Groups haben die Form von JSON-Objektzeichenfolgen im folgenden allgemeinen Format.

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group ... Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/MyGroupName"
    ],
    "detail": {
        ...
    }
}
```

Einzelheiten zu den Feldern, die allen Amazon- EventBridge Ereignissen gemeinsam sind, finden Sie unter Amazon- EventBridge Ereignisse im Amazon- EventBridge Benutzerhandbuch. Details, die spezifisch für Resource Groups sind, werden in der folgenden Tabelle erläutert.

Feldname	Typ	Beschreibung
`detail-type`	String	Für Resource Groups ist das `detail-type` Feld immer einer der folgenden Werte: • `ResourceGroups Group State Change` – Stellt Änderungen am Gesamtgruppenstatus und seinen Eigenschaften dar.

Feldname	Typ	Beschreibung
		• `ResourceGroups Group Membership Change` – Stellt Änderungen an der Gruppenmitgliedschaft dar.
`source`	String	Für Ressourcengruppen ist dieser Wert immer `"aws.resource-groups"` .
`resources`	Ein Array von Amazon-Ressourcennamen (ARNs)	Dieses Feld enthält immer den Amazon-Ressourcennamen (ARN) der Gruppe mit der Änderung, die dieses Ereignis ausgelöst hat. Dieses Feld kann auch die ARNs aller Ressourcen enthalten, die der Gruppe hinzugefügt oder daraus entfernt wurden, falls zutreffend.
`detail`	JSON-Objektzeichenfolge	Dies ist die Nutzlast des Ereignisses. Der Inhalt des `detail` Felds variiert je nach Wert des `detail-type` . Weitere Informationen finden Sie im nächsten Abschnitt.

Struktur des **`detail`** Felds

Das `detail` Feld enthält alle servicespezifischen Details zu einer bestimmten Änderung für Ressourcengruppen. Das `detail` Feld kann eine von zwei Formen annehmen, eine Änderung des Gruppenstatus oder eine Änderung der Mitgliedschaft, basierend auf dem Wert des im vorherigen Abschnitt beschriebenen `detail-type` Felds.

> **Important**
>
> Ressourcengruppen in diesen Ereignissen werden durch eine Kombination aus dem ARN der Gruppe und einem `"unique-id"` Feld identifiziert, das eine UUID enthält. Indem Sie eine UUID als Teil der Identität einer Ressourcengruppe einschließen, können Sie zwischen einer gelöschten Gruppe und einer anderen Gruppe unterscheiden, die später mit demselben Namen erstellt wird. Wir empfehlen Ihnen, eine Verkettung des ARN und der eindeutigen ID

als Schlüssel für die Gruppe in Ihren Programmen zu behandeln, die mit diesen Ereignissen interagieren.

Änderung des Gruppenstatus

`"detail-type": "ResourceGroups Group State Change"`

Dieser `detail-type` Wert gibt an, dass sich der Status der Gruppe selbst, einschließlich ihrer Metadaten, geändert hat. Diese Änderung tritt auf, wenn eine Gruppe erstellt, aktualisiert oder gelöscht wird, wie im `"change"` Feld innerhalb der angegeben`detail`.

Zu den Informationen, die im `details` Abschnitt enthalten sind, wenn dies angegeben `detail-type` ist, gehören die in der folgenden Tabelle beschriebenen Felder.

Feldname	Typ	Beschreibung
`event-sequence`	Double	Eine monoton steigende Zahl, die die Ereignisfolge für eine bestimmte Gruppe angibt. Die Nummer wird zurückgesetzt, wenn Sie die Gruppe löschen und eine andere Gruppe mit demselben Namen erstellen.
`group`	`Group` JSON-Objekt	Das Gruppenobjekt, das dem Ereignis anhand seines ARN, seines Namens und seiner eindeutigen ID zugeordnet ist.
`state-change`	String	Der Typ der Zustandsänderung, die stattgefunden hat. Kann einer der folgenden Werte sein: • `create` • `update` • `delete`
`old-state`	`GroupState` JSON-Objekt	Der Status der Gruppe vor der Änderung. Das -Objekt enthält nur die Werte der Eigenschaften, die sich geändert haben.

Feldname	Typ	Beschreibung
`new-state`	`GroupState` JSON-Objekt	Der Status der Gruppe nach der Änderung. Das -Objekt enthält nur die Werte der Eigenschaften, die sich geändert haben.

Das `group` JSON-Objekt enthält die in der folgenden Tabelle beschriebenen Elemente.

Feldname	Typ	Beschreibung
`arn`	String	Der ARN der Gruppe.
`name`	String	Der Anzeigename der Gruppe.
`unique-id`	GUID	Ein eindeutiger GUID-Wert, der zwischen einer Gruppe, die gelöscht wurde, und einer anderen Gruppe unterscheidet, die später mit demselben Namen und ARN erstellt wurde. Verwenden Sie die Verkettung von ARN und diesem Wert als eindeutigen Schlüssel für die Gruppe, wenn Sie diese Ereignisse in Ihrem Code verwenden.

Die `GroupState` JSON-Objekte enthalten die in der folgenden Tabelle beschriebenen Elemente.

Feldname	Typ	Beschreibung
`description`	String	Die vom Kunden bereitgestellte Beschreibung der Ressourcengruppe.
`resource-query`	`ResourceQuery` JSON-Objekt	Eine JSON-Darstellung der Abfrage, die die Mitglieder der Gruppe definiert. Dieses Feld ist nur für Gruppen vorhanden, die auf einer Abfrage basieren. Die Syntax dieses Felds wird durch den ResourceQuery API-Datentyp definiert. Beispiele hierfür finden Sie in den Beispielen für das Erstellen und Aktualisieren von Ereignissen.

Feldname	Typ	Beschreibung
`group-configuration`	`Configuration` JSON-Objekt	Eine JSON-Darstellung von Konfigurationsparametern, die einer serviceverknüpften Gruppe zugeordnet sind. Weitere Informationen finden Sie unter Servicekonfigurationen für Ressourcengruppen in der APIAWS Resource Groups-Referenz zu .

Jedes der folgenden Codebeispiele veranschaulicht den Inhalt des `detail` Feldes für jeden `state-change` Typ.

Erstellen

`"state-change": "create"`

Das Ereignis zeigt an, dass eine neue Gruppe erstellt wurde. Das Ereignis enthält alle Gruppenmetadateneigenschaften, die während der Erstellung der Gruppe festgelegt wurden. Auf dieses Ereignis folgt in der Regel eines von mehreren Gruppenmitgliedschaftsereignissen, es sei denn, die Gruppe ist leer. Eigenschaften mit einem Nullwert werden nicht im Ereignistext angezeigt.

Das folgende Beispielereignis gibt eine neu erstellte Ressourcengruppe mit dem Namen an`my-service-group`. In diesem Beispiel verwendet die Gruppe eine Tag-basierte Abfrage, die nur Amazon Elastic Compute Cloud (Amazon EC2)-Instances entspricht, die das Tag haben`"project"="my-service"`.

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group State Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-group"
    ],
    "detail": {
        "event-sequence": 1.0,
        "state-change": "create",
```

```
        "group": {
            "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-
group",
            "name": "my-service-group",
            "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceea"
        },
        "new-state": {
            "resource-query": {
                "type": "TAG_FILTERS_1_0",
                "query": "{
                    \"ResourceTypeFilters\": [\"AWS::EC2::Instance\"],
                    \"TagFilters\": [{\"Key\":\"project\", \"Values\":[\"my-service\"}]
                }"
            }
        }
    }
}
```

Aktualisierung

`"state-change": "update"`

Das Ereignis zeigt an, dass eine vorhandene Gruppe auf irgendeine Weise geändert wurde. Das Ereignis enthält nur die Eigenschaften, die sich gegenüber dem vorherigen Status geändert haben. Eigenschaften, die nicht geändert wurden, werden nicht im Ereignistext angezeigt.

Das folgende Beispielereignis zeigt an, dass die tagbasierte Abfrage in der Ressourcengruppe des vorherigen Beispiels so geändert wurde, dass sie auch Amazon EC2-Volume-Ressourcen in die Gruppe einschließt.

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group State Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-group"
    ],
    "detail": {
        "event-sequence": 3.0,
```

```
        "state-change": "update",
        "group": {
            "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-
group",
            "name": "my-service",
            "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceea"
        },
        "new-state": {
            "resource-query": {
                "type": "TAG_FILTERS_1_0",
                "query": "{
                    \"ResourceTypeFilters\": [\"AWS::EC2::Instance\",
 \"AWS::EC2::Volume\"],
                    \"TagFilters\": [{\"Key\":\"project\", \"Values\":[\"my-service\"}]
                }"
            }
        },
        "old-state": {
            "resource-query": {
                "type": "TAG_FILTERS_1_0",
                "query": "{
                    \"ResourceTypeFilters\": [\"AWS::EC2::Instance\"],
                    \"TagFilters\": [{\"Key\":\"Project\", \"Values\":[\"my-service\"}]
                }"
            }
        }
    }
}
```

Löschen

`"state-change": "delete"`

Das Ereignis zeigt an, dass eine vorhandene Gruppe gelöscht wurde. Das Detailfeld enthält keine Metadaten über die Gruppe, mit Ausnahme ihrer Identifizierung. Das `event-sequence` Feld wird nach diesem Ereignis zurückgesetzt, so wie es ist, per Definition das letzte Ereignis für dieses `arn` und `unique-id`.

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group State Change",
    "source": "aws.resource-groups",
```

```
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/my-service"
    ],
    "detail": {
        "event-sequence": 4.0,
        "state-change": "delete",
        "group": {
            "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service",
            "name": "my-service",
            "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceea"
        }
    }
}
```

Änderung der Gruppenmitgliedschaft

`"detail-type": "ResourceGroups Group Membership Change"`

Dieser `detail-type` Wert gibt an, dass die Mitgliedschaft der Gruppe durch eine Ressource geändert wurde, die der Gruppe hinzugefügt oder daraus entfernt wird. Wenn dies angegeben `detail-type` ist, enthält das `resources` Feld der obersten Ebene den ARN der Gruppe, deren Mitgliedschaft geändert wurde, und die ARNs aller Ressourcen, die der Gruppe hinzugefügt oder daraus entfernt wurden.

Zu den Informationen, die im `details` Abschnitt enthalten sind, wenn dies angegeben `detail-type` ist, gehören die in der folgenden Tabelle beschriebenen Felder.

Feldname	Typ	Beschreibung
`event-sequence`	Double	Eine monoton steigende Zahl, die die Abfolge von Ereignissen für eine bestimmte Gruppe angibt. Die Zahl wird zurückgesetzt, wenn die Gruppe gelöscht wird und sich ihre eindeutige ID ändert.
`group`	`Group` JSON-Objekt	Identifiziert das mit dem Ereignis verknüpfte Gruppenobjekt anhand seines ARN, seines Namens und seiner eindeutigen ID.

Feldname	Typ	Beschreibung
`resources`	Array von `ResourceChange` JSON-Objekten	Ein Array von Ressourcen, deren Gruppenmitgliedschaft sich geändert hat. Dieses `ResourceChange` Objekt enthält die folgenden Felder für jede Ressource: • `membership-change` – Der Wert ist entweder `"add"` oder `"remove"`. • `arn` – Der ARN der Ressource, die hinzugefügt oder entfernt wurde. • `resource-type` – Der Typ der hinzugefügten oder entfernten Ressource.

Das folgende Codebeispiel veranschaulicht den Inhalt des Ereignisses für einen typischen Mitgliedschaftsänderungstyp. Dieses Beispiel zeigt eine Ressource, die der Gruppe hinzugefügt wird, und eine Ressource, die aus der Gruppe entfernt wird.

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group Membership Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/my-service",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1111",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-efef2222"
    ],
    "detail": {
        "event-sequence": 2.0,
        "group": {
            "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service",
            "name": "my-service",
            "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceea"
        },
        "resources": [
```

```
            {
                "membership-change": "add",
                "arn": "arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1111",
                "resource-type": "AWS::EC2::Instance"
            },
            {
                "membership-change": "remove",
                "arn": "arn:aws:ec2:us-east-1:123456789012:instance/i-efef2222",
                "resource-type": "AWS::EC2::Instance"
            }
        ]
    }
}
```

Beispiel für EventBridge benutzerdefinierte Ereignismuster für verschiedene Anwendungsfälle

Das folgende Beispiel für EventBridge benutzerdefinierte Ereignismuster filtert die von Ressourcengruppen generierten Ereignisse nur nach Ereignissen, die für eine bestimmte Ereignisregel und ein bestimmtes Ziel relevant sind.

Wenn in den folgenden Codebeispielen eine bestimmte Gruppe oder Ressource benötigt wird, ersetzen Sie jeden *`Platzhalter für Benutzereingaben`* durch Ihre eigenen Informationen.

Alle Ressourcengruppen-Ereignisse

```
{
    "source": [ "aws.resource-groups" ]
}
```

Ereignisse zur Änderung des Gruppenstatus oder der Mitgliedschaft

Das folgende Codebeispiel gilt für alle Änderungen des Gruppenstatus.

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group State Change " ]
}
```

Das folgende Codebeispiel gilt für alle Änderungen der Gruppenmitgliedschaft.

```
{
```

```
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change" ]
}
```

Ereignisse für eine bestimmte Gruppe

```
{
    "source": [ "aws.resource-groups" ],
    "detail": {
        "group": {
            "arn": [ "my-group-arn" ]
        }
    }
}
```

Im vorherigen Beispiel werden Änderungen an der angegebenen Gruppe erfasst. Im folgenden Beispiel werden die gleichen Aktionen ausgeführt und Änderungen erfasst, wenn die Gruppe eine Mitgliedsressource einer anderen Gruppe ist.

```
{
    "source": [ "aws.resource-groups" ],
    "resources": [ "my-group-arn" ]
}
```

Ereignisse für eine bestimmte Ressource

Sie können nur Änderungsereignisse für Gruppenmitgliedschaften für bestimmte Mitgliedsressourcen filtern.

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change " ],
    "resources": [ "arn:aws:ec2:us-east-1:123456789012:instance/i-b188560f" ]
}
```

Ereignisse für einen bestimmten Ressourcentyp

Sie können den Präfixabgleich mit ARNs verwenden, um Ereignisse für einen bestimmten Ressourcentyp abzugleichen.

```
{
```

```
    "source": [ "aws.resource-groups" ],
    "resources": [
        { "prefix": "arn:aws:ec2:us-east-1:123456789012:instance" }
    ]
}
```

Alternativ können Sie den exakten Abgleich verwenden, indem Sie `resource-type` Kennungen verwenden, die möglicherweise für mehr als einen Typ präzise übereinstimmen. Im Gegensatz zum vorherigen Beispiel gleicht das folgende Beispiel nur Änderungsereignisse der Gruppenmitgliedschaft ab, da Änderungsereignisse des Gruppenstatus kein `resources` Feld in ihrem `detail` Feld enthalten.

```
{
    "source": [ "aws.resource-groups" ],
    "detail": {
        "resources": {
                "resource-type": [ "AWS::EC2::Instance", "AWS::EC2::Volume" ]
         }
    }
}
```

Alle Ereignisse zum Entfernen von Ressourcen

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change" ],
    "detail": {
        "resources": {
                "membership-change": [ "remove" ]
        }
    }
}
```

Alle Ereignisse zum Entfernen von Ressourcen für eine bestimmte Ressource

```
 {
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change" ],
    "detail": {
        "resources": {
                "membership-change": [ "remove" ],
```

```
                "arn": [ "arn:aws:ec2:us-east-1:123456789012:instance/i-b188560f" ]
        }
    }
}
```

Sie können das `resources`Array der obersten Ebene, das im ersten Beispiel in diesem Abschnitt verwendet wurde, nicht für diese Art der Ereignisfilterung verwenden. Das liegt daran, dass es sich bei einer Ressource im `resources` Element der obersten Ebene möglicherweise um eine Ressource handelt, die einer Gruppe hinzugefügt wird, und das Ereignis weiterhin übereinstimmen würde. Mit anderen Worten, das folgende Codebeispiel kann unerwartete Ereignisse zurückgeben. Verwenden Sie stattdessen die im vorherigen Beispiel gezeigte Syntax.

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change" ],
    "resources": [ "arn:aws:ec2:us-east-1:123456789012:instance/i-b188560f" ],
    "detail": {
        "resources": {
                "membership-change": [ "remove" ]
        }
     }
}
```

Löschen von Ressourcengruppen von AWS Resource Groups

Sie können die AWS Resource GroupsKonsole oder die verwendenAWS CLI, um Ressourcengruppen aus zu löschenAWS Resource Groups. Durch das Löschen einer Ressourcengruppe werden die Ressourcen, die Mitglied der Gruppe sind, oder Tags für Mitgliedsressourcen nicht gelöscht. Gelöscht werden ausschließlich die Gruppenstruktur und alle Tags auf Gruppenebene.

Console

So löschen Sie Gruppe aus

1. Melden Sie sich an der AWS Resource Groups-Konsole an.
2. Wählen Sie im Navigationsbereich die Option Gespeicherte Resource Groups aus.
3. Wählen Sie den Namen der Gruppe aus, die Sie löschen möchten, und wählen Sie dann Details anzeigen.

4. Wählen Sie auf der Gruppe auf der Gruppe in der Gruppe oben rechts Löschen.
5. Wenn Sie zum Bestätigen des Löschvorgangs aufgefordert werden, wählen Sie Delete (Löschen) aus.

AWS CLI & AWS SDKs

So löschen Sie Gruppe aus

1. Führen Sie den folgenden Befehl aus und ersetzen Sie *resource_group_name durch den Namen* Ihrer Gruppe.

```
$ aws resource-groups delete-group \
    --group-name resource_group_name
```

2. Wenn Sie zur Bestätigung des Löschvorgangs aufgefordert werden, geben Sie `yes` ein und drücken anschließend die Eingabetaste.

AWS-Services, die mit AWS Resource Groups funktionieren

Sie können die folgenden AWS Dienste mit nutzenAWS Resource Groups.

AWS-Service	Verwendung mit Resource Groups
AWS CloudFormation— Erstellen Sie Ressourcengruppen in AWS CloudFormation mithilfe einer Stack-Vorlage.	Stellen Sie AWS Ressourcen bereit und organisieren Sie sie gleichzeitig. Organisieren Sie Ressourcen nach Schlagwörtern. Organisie ren Sie Ressourcen aus einem anderen Stapel. Sammeln Sie mithilfe von Amazon Einblicke in Ihre AWS Ressourcen in Ressourcengruppen CloudWatch oder ergreifen Sie mithilfe von Amazon operative MaßnahmenAWS Systems Manager. Weitere Informationen finden Sie in der Referenz zu den ResourceGroups Ressource ntypen im AWS CloudFormationBenutzerhandb uch.

AWS-Service	Verwendung mit Resource Groups
CloudTrail— Erfassen Sie alle Aktionen der Ressourcengruppe mithilfe vonAWS CloudTrail.	Erfassen Sie Informationen über Aktionen, die in Ihren Ressourcengruppen ausgeführt wurden, einschließlich Informationen darüber, wer die Aktion ausgeführt hat (IAM-Principal, z. B. eine Rolle, ein Benutzer oder einAWS-Service), wann die Aktion ausgeführt wurde, wo die Aktion stattgefunden hat (die Quell-IP-Adresse) und mehr. Diese Aufzeichnungen können dann zur Analyse oder zur Auslösung von Folgemaßnahmen verwendet werden. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail-Ereignisverlauf.
Amazon CloudWatch — gestatten Ihnen, Ihre AWS -Ressourcen und der in ausgeführten Anwendungen zu verwendenAWS.	Konzentrieren Sie Ihre Ansicht, um Metriken und Alups aus einer einzigen Resource ups ups ups ups ups ups ups ups ups ups ups ups Weitere Informationen finden Sie im CloudWatchAmazon-Benutzerhandbuch unter Konzentrieren Sie sich auf Metriken und Alarme in einer Ressourcengruppe.
Amazon CloudWatch Application Insights — Erkennen Sie häufig auftretende Probleme mit Ihren .NET- und SQL Server-basierten Anwendungen.	Überwachung Ihrer .NET- und pro Resource. Weitere Informationen finden Sie unter Unterstützte Anwendungskomponenten im CloudWatchAmazon-Benutzerhandbuch.
Amazon DynamoDB-Tabellengruppen — Organisieren Sie Ihre DynamoDB-Tabellen in logischen Gruppierungen, damit Sie Ihre Ressourcen einfacher verwalten können.	Erstellen, bearbeiten und löschen Sie Gruppen von DynamoDB-Tabellen über das DynamoDB-Aktionsmenü. Weitere Informationen finden Sie im Amazon DynamoDB Developer Guide.

AWS-Service	Verwendung mit Resource Groups
Amazon EC2 Dedicated Hosts: Sie zahlen für Ihre vorhandenen Lizenzen pro Socket, pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro pro VM-Software.	Führen Sie Amazon EC2 EC2-Instances in Host-Ressourcengruppen ein, um Ihre Nutzung von Dedicated Hosts zu maximieren. Weitere Informationen finden Sie unter Arbeiten mit Dedicated Hosts.
Amazon EC2 EC2-Kapazitätsreservierungen — Reservieren Sie Kapazität für Ihre Amazon EC2 EC2-Instances, die Sie dann nutzen können, wenn Sie sie benötigen. Sie können Attribute für die Kapazitätsreservierung angeben, sodass sie nur mit Amazon EC2 EC2-Insta nces funktioniert, die mit passenden Attributen gestartet werden.	Starten Sie Ihre Amazon EC2 EC2-Instances in Ressourcengruppen, die eine oder mehrere Kapazitätsreservierungen enthalten. Wenn die Gruppe keine Kapazitätsreservierung mit passenden Attributen und verfügbarer Kapazität für eine angeforderte Instance hat, wird die Instance als On-Demand-Instance ausgeführt. Wenn Sie der Zielgruppe später eine übereinstimmende Kapazitätsreservierung hinzufügen, wird die Instance automatisch mit der reservierten Kapazität abgeglichen und in diese verschoben. Weitere Informationen finden Sie unter Arbeiten mit Kapazitätsreservierungsgruppen.
AWS License Manager— Rationalisieren Sie den Prozess der Übertragung von Lizenzen von Softwareanbietern in die Cloud.	Konfigurieren Sie eine Host-Ressourcengru ppe, damit License Manager Ihre Dedicated Hosts verwalten kann. Weitere Informationen finden Sie unter Hostressourcengruppen in License Manager.

AWS-Service	Verwendung mit Resource Groups
AWSResilience Hub — Bereiten Sie Ihre Anwendungen vor und schützen Sie sie vor Störungen.	Entdecken Sie Ihre Anwendungen, die mithilfe von Resource Groups definiert wurden. Weitere Informationen finden Sie im AWSNews Blog unter Messen und verbessern Sie die Widerstandsfähigkeit Ihrer Anwendung mit AWS Resilience Hub.
AWS Resource Access Manager— Teilen Sie bestimmte AWS Ressourcen, die Sie besitzen, mit anderen Konten.	Teilen Sie Host-Ressourcengruppen mithilfe vonAWS RAM. Weitere Informationen finden Sie unter Gemeinsam nutzbare Ressourcen im AWS RAMBenutzerhandbuch.
AWS Service Catalog AppRegistry— Definieren und verwalten Sie Ihre Anwendungen und deren Metadaten.	Wenn Sie eine Anwendung in erstellen AppRegistry, erstellt dieser Dienst automatisch eine Ressourcengruppe für diese Anwendung . Die Anwendungsressourcengruppe ist eine Sammlung aller Ressourcen in Ihrer Anwendung. Der Dienst erstellt außerdem eine AWS CloudFormation stapelbasierte Ressourcengruppe für jeden Stapel, der der Anwendung zugeordnet ist. Weitere Informationen finden Sie AppRegistry im AWS Service CatalogAdministratorhandbuch unter Verwenden.

AWS-Service	Verwendung mit Resource Groups
AWS Systems Manager— Ermöglichen Sie die Sichtbarkeit und Kontrolle Ihrer AWS Ressourcen.	Sammeln Sie betriebliche Erkenntnisse und führen Sie Massenaktionen an Ihren Anwendungen durch, die auf Ressource ngruppen basieren. In der AWS Systems Manager Konsole werden auf der Seite „Benutzerdefinierte Anwendungen von Applicati on Manager“ automatisch Betriebsdaten für Anwendungen importiert und angezeigt, die auf Ressourcengruppen basieren. anhand der Informationen in Application Manager, um zu ermitteln, welche Ressourcen in einer Anwendung kompatibel sind und welche Ressourcen eine Aktion erfordern. Weitere Informationen finden Sie im AWS Systems ManagerBenutzerhandbuch unter Arbeiten mit Anwendungen in Application Manager.
Amazon VPC Analyzer — identifiziert unbeabsichtigten Netzwerkzugriff auf Ihre Ressourcen auf. AWS	Sie können die Quellen und Ziele für Ihre Netzwerkzugriffsanforderungen angeben, indem SieAWS Resource Groups. Auf diese Weise können Sie den Netzwerkzugriff in Ihrer gesamten AWS Umgebung steuern, unabhängi g davon, wie Sie Ihr Netzwerk konfigurieren. Weitere Informationen finden Sie unter Verwenden von Resource Groups mit Netzwerkzugangsbereichen.

Dienstkonfigurationen für Ressourcengruppen

Mit Ressourcengruppen können Sie Sammlungen Ihrer AWS Ressourcen als Einheit verwalten. Einige AWS Dienste unterstützen dies, indem sie die angeforderten Operationen für alle Mitglieder der Gruppe ausführen. Solche Dienste können die Einstellungen, die auf Gruppenmitglieder

angewendet werden sollen, als Konfiguration in Form einer JSON-Datenstruktur speichern, die an die Gruppe angehängt ist.

In diesem Thema werden die verfügbaren Konfigurationseinstellungen für unterstützte AWS Dienste beschrieben.

Themen

- Wie greife ich auf die Dienstkonfiguration zu, die einer Ressourcengruppe zugeordnet ist
- JSON-Syntax einer Dienstkonfiguration
- Unterstützte Konfigurationstypen und Parameter

Wie greife ich auf die Dienstkonfiguration zu, die einer Ressourcengruppe zugeordnet ist

Dienste, die mit Diensten verknüpfte Gruppen unterstützen, legen die Konfiguration in der Regel für Sie fest, wenn Sie die von diesem Dienst bereitgestellten Tools verwenden, z. B. die Verwaltungskonsole dieses Dienstes oder dessen AWS CLI und AWS SDK-Operationen. Einige Dienste verwalten ihre mit Diensten verknüpften Gruppen vollständig, und Sie können sie in keiner Weise ändern, es sei denn, die Konsole oder die Befehle, die vom jeweiligen Dienst bereitgestellt werden, erlauben dies. AWS In einigen Fällen können Sie jedoch mit der Dienstkonfiguration interagieren, indem Sie die folgenden API-Operationen in den AWS SDKs oder deren Äquivalenten verwenden: AWS CLI

- Sie können Ihre eigene Konfiguration an eine Gruppe anhängen, wenn Sie die Gruppe mithilfe der Operation erstellen. CreateGroup
- Sie können die aktuelle Konfiguration ändern, die einer Gruppe zugeordnet ist, indem Sie den PutGroupConfigurationVorgang verwenden.
- Sie können die aktuelle Konfiguration einer Ressourcengruppe anzeigen, indem Sie den GetGroupConfigurationVorgang aufrufen.

JSON-Syntax einer Dienstkonfiguration

Eine Ressourcengruppe kann eine Konfiguration enthalten, die dienstspezifische Einstellungen definiert, die für die Ressourcen gelten, die Mitglieder dieser Gruppe sind.

Eine Konfiguration wird als JSON-Objekt ausgedrückt. Auf der obersten Ebene besteht eine Konfiguration aus einer Reihe von Gruppenkonfigurationselementen. Jedes Gruppenkonfigurationselement enthält zwei Elemente: ein Element `Type` für die Konfiguration und eine Reihe von Elementen, die durch diesen Typ `Parameters` definiert sind. Jeder Parameter enthält ein `Name` und ein Array aus einem oder mehreren`Values`. Das folgende Beispiel mit *`Platzhaltern`* zeigt die grundlegende Syntax für eine Konfiguration für einen einzelnen Beispielressourcentyp. Dieses Beispiel zeigt einen Typ mit zwei Parametern und jeden Parameter mit zwei Werten. Die tatsächlich gültigen Typen, Parameter und Werte werden im nächsten Abschnitt behandelt.

```
{
    "Configuration": [
        {
            "Type": "configuration-type",
            "Parameters": [
                {
                    "Name": "parameter1-name",
                    "Values": [
                        "value1",
                        "value2"
                    ]
                },
                {
                    "Name": "parameter2-name",
                    "Values": [
                        "value3",
                        "value4"
                    ]
                }
            ]
        }
    ]
}
```

Unterstützte Konfigurationstypen und Parameter

Resource Groups unterstützt die Verwendung der folgenden Konfigurationstypen. Jeder Konfigurationstyp hat eine Reihe von Parametern, die für diesen Typ gültig sind.

Themen

- AWS::ResourceGroups::Generic

- AWS::AppRegistry::Application
- AWS::CloudFormation::Stack
- AWS::EC2::CapacityReservationPool
- AWS::EC2::HostManagement
- AWS::NetworkFirewall::RuleGroup

`AWS::ResourceGroups::Generic`

Dieser Konfigurationstyp spezifiziert Einstellungen, die Mitgliedschaftsanforderungen für die Ressourcengruppe durchsetzen, anstatt das Verhalten eines bestimmten Ressourcentyps für einen AWS Dienst zu konfigurieren. Dieser Konfigurationstyp wird automatisch von den dienstverknüpften Gruppen hinzugefügt, die ihn benötigen, z. B. die `AWS::EC2::HostManagment` Typen `AWS::EC2::CapacityReservationPool` und.

Folgendes gilt für `Parameters` die `AWS::ResourceGroups::Generic` serviceverknüpfte Gruppe. `Type`

- **`allowed-resource-types`**

  Dieser Parameter gibt an, dass die Ressourcengruppe nur aus Ressourcen des oder der angegebenen Typen bestehen kann.

  Datentyp der Werte: Zeichenfolge

  Zulässige Werte:

  - `AWS::EC2::Host`— A `Configuration` mit diesem Parameter und Wert ist erforderlich, wenn die Dienstkonfiguration auch den Typ A `Configuration` enthält`AWS::EC2::HostManagement`. Dadurch wird sichergestellt, dass die `HostManagement` Gruppe nur Amazon EC2 EC2-Dedicated Hosts enthalten kann.
  - `AWS::EC2::CapacityReservation`— A `Configuration` mit diesem Parameter und Wert ist erforderlich, wenn die Servicekonfiguration auch ein `Configuration` Element vom Typ `AWS::EC2::CapacityReservationPool` enthält. Dadurch wird sichergestellt, dass eine `CapacityReservation` Gruppe nur Amazon EC2 EC2-Kapazitätsreservierungskapazität enthalten kann.

  Erforderlich: Bedingt, basierend auf anderen `Configuration` Elementen, die der Ressourcengruppe zugeordnet sind. Zulässige Werte finden Sie im vorherigen Eintrag.

Das folgende Beispiel beschränkt Gruppenmitglieder auf Amazon EC2 EC2-Host-Instances.

```
{
    "Configuration": [
        {
            "Type": "AWS::ResourceGroups::Generic",
            "Parameters": [
                {
                    "Name": "allowed-resource-types",
                    "Values": ["AWS::EC2::Host"]
                }
            ]
        }
    ]
}
```

- **`deletion-protection`**

  Dieser Parameter gibt an, dass die Ressourcengruppe nur gelöscht werden kann, wenn sie keine Mitglieder enthält. Weitere Informationen finden Sie unter Löschen einer Host-Ressourcengruppe im License Manager Manager-Benutzerhandbuch

  Datentyp der Werte: Array aus Zeichenketten

  Zulässige Werte: Der einzig zulässige Wert ist `[ "UNLESS_EMPTY" ]` (der Wert muss in Großbuchstaben geschrieben werden).

  Erforderlich: Bedingt, basierend auf anderen `Configuration` Elementen, die an die Ressourcengruppe angehängt sind. Dieser Parameter ist nur erforderlich, wenn die Ressourcengruppe auch ein anderes `Configuration` Element mit dem Wert `Type` of enthält`AWS::EC2::HostManagement`.

  Im folgenden Beispiel wird der Löschschutz für die Gruppe aktiviert, sofern die Gruppe keine Mitglieder hat.

```
{
    "Configuration": [
        {
            "Type": "AWS::ResourceGroups::Generic",
            "Parameters": [
                {
```

```
                    "Name": "deletion-protection",
                    "Values": [ "UNLESS_EMPTY" ]
                }
            ]
        }
    ]
}
```

AWS::AppRegistry::Application

Dieser `Configuration` Typ gibt an, dass die Ressourcengruppe eine Anwendung darstellt, die von erstellt wurdeAWS Service Catalog AppRegistry.

Ressourcengruppen dieses Typs werden vollständig vom AppRegistry Dienst verwaltet und können von Benutzern nur mithilfe der von bereitgestellten Tools erstellt, aktualisiert oder gelöscht werden AppRegistry.

> **Note**
>
> Da Ressourcengruppen dieses Typs automatisch vom Benutzer erstellt und verwaltet AWS und nicht von diesem verwaltet werden, werden diese Ressourcengruppen nicht auf Ihr Kontingentlimit für die maximale Anzahl von Ressourcengruppen angerechnet, die Sie in Ihrem erstellen können AWS-Konto.

Weitere Informationen finden Sie unter Verwenden AppRegistry im Service Catalog-Benutzerhandbuch.

Wenn eine dienstverknüpfte Ressourcengruppe dieses Typs AppRegistry erstellt wird, wird auch automatisch eine separate, zusätzliche AWS CloudFormationdienstverknüpfte Gruppe für jeden AWS CloudFormation Stapel erstellt, der der Anwendung zugeordnet ist.

AppRegistry benennt die von ihr erstellten serviceverknüpften Gruppen dieses Typs automatisch mit dem Präfix, `AWS_AppRegistry_Application-` gefolgt vom Namen der Anwendung: `AWS_AppRegistry_Application-`*`MyAppName`*

Die folgenden Parameter werden für den Typ der `AWS::AppRegistry::Application` dienstverknüpften Gruppe unterstützt.

- **`Name`**

Dieser Parameter gibt den Anzeigenamen der Anwendung an, der vom Benutzer bei der Erstellung in AppRegistry zugewiesen wurde.

Datentyp der Werte: Zeichenfolge

Zulässige Werte: jede vom AppRegistry Dienst zugelassene Textzeichenfolge für einen Anwendungsnamen.

Required: Yes

- **`Arn`**

  Dieser Parameter gibt den Amazon Resource Name (ARN) -Pfad der Anwendung an, der von zugewiesen wurde AppRegistry.

  Datentyp der Werte: Zeichenfolge

  Zulässige Werte: ein gültiger ARN.

  Required: Yes

> **Note**
>
> Um eines dieser Elemente zu ändern, müssen Sie die Anwendung mithilfe der AppRegistry Konsole oder des AWS SDK und der AWS CLI Operationen dieses Dienstes ändern.

Diese Anwendungsressourcengruppe schließt automatisch die Ressourcengruppen als Gruppenmitglieder ein, die für die AWS CloudFormation Stacks erstellt wurden, die der AppRegistry Anwendung zugeordnet sind. Sie können den ListGroupResourcesVorgang verwenden, um diese untergeordneten Gruppen anzuzeigen.

Das folgende Beispiel zeigt, wie der Konfigurationsabschnitt einer mit einem `AWS::AppRegistry::Application` Dienst verknüpften Gruppe aussieht.

```
{
    "Configuration": [
        {
            "Type": "AWS::AppRegistry::Application",
```

```
            "Parameters":[
                {
                    "Name": "Name",
                    "Values": [
                        "MyApplication"
                    ]
                },
                {
                    "Name": "Arn",
                    "Values": [
                        "arn:aws:servicecatalog:us-east-1:123456789012:/
applications/<application-id>"
                    ]
                }
            ]
        }
    ]
}
```

AWS::CloudFormation::Stack

Dieser `Configuration` Typ gibt an, dass die Gruppe einen AWS CloudFormation Stack darstellt und dass ihre Mitglieder die AWS Ressourcen sind, die von diesem Stack erzeugt werden.

Ressourcengruppen dieses Typs werden automatisch für Sie erstellt, wenn Sie dem AppRegistry Service einen AWS CloudFormation Stack zuordnen. Sie können diese Gruppen nur mithilfe der von bereitgestellten Tools erstellen, aktualisieren oder löschen AppRegistry.

AppRegistry benennt die mit Diensten verknüpften Gruppen dieses Typs, die er erstellt, automatisch mit dem Präfix, `AWS_CloudFormation_Stack-` gefolgt vom Namen des Stacks: `AWS_CloudFormation_Stack-`*`MyStackName`*

> **Note**
>
> Da Ressourcengruppen dieses Typs automatisch vom Benutzer erstellt und verwaltet AWS und nicht von diesem verwaltet werden, werden diese Ressourcengruppen nicht auf Ihr Kontingentlimit für die maximale Anzahl von Ressourcengruppen angerechnet, die Sie in Ihrem AWS-Konto erstellen können.

Weitere Informationen finden Sie unter Verwenden AppRegistry im Service Catalog-Benutzerhandbuch.

AppRegistry erstellt automatisch eine dienstbezogene Ressourcengruppe dieses Typs für jeden AWS CloudFormation Stapel, den Sie der AppRegistry Anwendung zuordnen. Diese Ressourcengruppen werden zu untergeordneten Mitgliedern der übergeordneten Ressourcengruppe für die AppRegistry Anwendung.

Die Mitglieder dieser AWS CloudFormation Ressourcengruppe sind die AWS Ressourcen, die als Teil des Stacks erstellt wurden.

Die folgenden Parameter werden für den Typ der `AWS::CloudFormation::Stack` serviceverknüpften Gruppe unterstützt.

- **`Name`**

  Dieser Parameter gibt den Anzeigenamen des AWS CloudFormation Stacks an, der vom Benutzer bei der Erstellung des Stacks zugewiesen wurde.

  Datentyp der Werte: Zeichenfolge

  Zulässige Werte: jede vom AWS CloudFormation Dienst zugelassene Textzeichenfolge für einen Stacknamen.

  Required: Yes

- **`Arn`**

  Dieser Parameter gibt den Amazon Resource Name (ARN) -Pfad des AWS CloudFormation Stacks an, der an die Anwendung in angehängt ist AppRegistry.

  Datentyp der Werte: Zeichenfolge

  Zulässige Werte: ein gültiger ARN.

  Required: Yes

> **Note**
>
> Um eines dieser Elemente zu ändern, müssen Sie die Anwendung mithilfe der AppRegistry Konsole oder eines gleichwertigen AWS SDK und der entsprechenden AWS CLI Operationen ändern.

Das folgende Beispiel zeigt, wie der Konfigurationsabschnitt einer mit einem `AWS::CloudFormation::Stack` Dienst verknüpften Gruppe aussieht.

```
{
    "Configuration": [
        {
            "Type": "AWS::CloudFormation::Stack",
            "Parameters":[
                {
                    "Name": "Name",
                    "Values": [
                        "MyStack"
                    ]
                },
                {
                    "Name": "Arn",
                    "Values": [
                        "arn:aws:cloudformation:us-
east-1:123456789012:stack/MyStack/<stack-id>"
                    ]
                }
            ]
        }
    ]
}
```

`AWS::EC2::CapacityReservationPool`

Dieser `Configuration` Typ gibt an, dass die Ressourcengruppe einen gemeinsamen Kapazitätspool darstellt, der von den Mitgliedern der Gruppe bereitgestellt wird. Die Mitglieder dieser Ressourcengruppe müssen Amazon EC2 EC2-Kapazitätsreservierungen sein. Eine Ressourcengruppe kann sowohl Kapazitätsreservierungen enthalten, die Sie in Ihrem Konto besitzen, als auch Kapazitätsreservierungen, die mithilfe AWS Resource Access Manager von anderen Konten mit Ihnen geteilt wurden. Auf diese Weise können Sie eine Amazon EC2 EC2-Instance starten,

indem Sie diese Ressourcengruppe als Wert für den Kapazitätsreservierungsparameter verwenden. Wenn Sie dies tun, verwendet die Instance die verfügbare reservierte Kapazität in der Gruppe. Wenn die Ressourcengruppe keine verfügbare Kapazität hat, wird die Instance als eigenständige On-Demand-Instance außerhalb des Pools gestartet. Weitere Informationen finden Sie unter Arbeiten mit Kapazitätsreservierungsgruppen im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

Wenn Sie eine serviceverknüpfte Ressourcengruppe mit einem `Configuration` Element dieses Typs konfigurieren, müssen Sie auch separate `Configuration` Elemente mit den folgenden Werten angeben:

- Ein `AWS::ResourceGroups::Generic` Typ mit einem Parameter:
  - Der Parameter `allowed-resource-types` und ein einzelner Wert von`AWS::EC2::CapacityReservation`. Dadurch wird sichergestellt, dass nur Amazon EC2 EC2-Kapazitätsreservierungen Mitglieder der Ressourcengruppe sein können.

Das `AWS::EC2::CapacityReservationPool` Element in einer Gruppenkonfiguration unterstützt keine Parameter.

Das folgende Beispiel zeigt, wie der `Configuration` Abschnitt einer solchen Gruppe aussieht.

```
{
    "Configuration": [
        {
            "Type": "AWS::EC2::CapacityReservationPool"
        },
        {
            "Type": "AWS::ResourceGroups::Generic",
            "Parameters": [
                {
                    "Name": "allowed-resource-types",
                    "Values": [ "AWS::EC2::CapacityReservation" ]
                }
            ]
        }
    ]
}
```

AWS::EC2::HostManagement

Diese ID gibt Einstellungen für die Amazon EC2 EC2-Hostverwaltung anAWS License Manager, die für die Mitglieder der Gruppe durchgesetzt werden. Weitere Informationen finden Sie unter Host-Ressourcengruppen in. AWS License Manager

Wenn Sie eine mit einem Dienst verknüpfte Ressourcengruppe mit einem `Configuration` Element dieses Typs konfigurieren, müssen Sie auch separate `Configuration` Elemente mit den folgenden Werten angeben:

- Ein `AWS::ResourceGroups::Generic` Typ mit einem Parameter von `allowed-resource-types` und einem einzelnen Wert von`AWS::EC2::Host`. Dadurch wird sichergestellt, dass nur Amazon EC2 EC2-Dedicated Hosts Mitglieder der Gruppe sein können.
- Ein `AWS::ResourceGroups::Generic` Typ mit einem Parameter von `deletion-protection` und einem einzelnen Wert von`UNLESS_EMPTY`. Dadurch wird sichergestellt, dass die Gruppe nur gelöscht werden kann, wenn die Gruppe leer ist.

Die folgenden Parameter werden für den Typ der `AWS::EC2::HostManagement` serviceverknüpften Gruppe unterstützt.

- **`auto-allocate-host`**

  Dieser Parameter gibt an, ob Instances auf einem bestimmten dedizierten Host oder auf einem beliebigen verfügbaren Host mit einer passenden Konfiguration gestartet werden. Weitere Informationen finden Sie unter Understanding Auto Placement and Affinity im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

  Datentyp der Werte: Boolean

  Zulässige Werte: „true“ oder „false“ (muss in Kleinbuchstaben geschrieben werden).

  Required: No

```
{
    "Configuration": [
        {
            "Type": "AWS::EC2::HostManagement",
            "Parameters": [
                {
                    "Name": "auto-allocate-host",
```

```
                    "Values": [ "true" ]
                }
            ]
        },
        {
            "Type": "AWS::ResourceGroups::Generic",
            "Parameters": [
                {
                    "Name": "allowed-resource-types",
                    "Values": [ "AWS::EC2::Host" ]
                },
                {
                    "Name": "deletion-protection",
                    "Values": [ "UNLESS_EMPTY" ]
                }
            ]
        }
    ]
}
```

- **`auto-release-host`**

  Dieser Parameter gibt an, ob ein dedizierter Host in der Gruppe automatisch freigegeben wird, nachdem seine letzte laufende Instance beendet wurde. Weitere Informationen finden Sie unter Releasing Dedicated Hosts im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

  Datentyp der Werte: Boolean

  Zulässige Werte: „true“ oder „false“ (muss in Kleinbuchstaben geschrieben werden).

  Required: No

```
{
    "Configuration": [
        {
            "Type": "AWS::EC2::HostManagement",
            "Parameters": [
                {
                    "Name": "auto-release-host",
                    "Values": [ "false" ]
                }
            ]
        },
```

```
        {
            "Type": "AWS::ResourceGroups::Generic",
            "Parameters": [
                {
                    "Name": "allowed-resource-types",
                    "Values": [ "AWS::EC2::Host" ]
                },
                {
                    "Name": "deletion-protection",
                    "Values": [ "UNLESS_EMPTY" ]
                }
            ]
        }
    ]
}
```

- **`allowed-host-families`**

  Dieser Parameter gibt an, welche Instanztypfamilien von Instanzen verwendet werden können, die Mitglieder dieser Gruppe sind.

  Datentyp der Werte: Ein Array von Zeichenketten.

  Zulässige Werte: Bei jedem Wert muss es sich um eine gültige Familienkennung des Amazon EC2 EC2-Instance-Typs handeln`C4`, z. B.`M5`,`P3dn`, oder`R5d`.

  Required: No

  Das folgende Beispielkonfigurationselement gibt an, dass gestartete Instances nur Mitglieder der Instance-Typfamilien C5 oder M5 sein können.

```
{
    "Configuration": [
        {
            "Type": "AWS::EC2::HostManagement",
            "Parameters": [
                {
                    "Name": "allowed-host-families",
                    "Values": ["c5", "m5"]
                }
            ]
        },
        {
```

```
            "Type": "AWS::ResourceGroups::Generic",
            "Parameters": [
                {
                    "Name": "allowed-resource-types",
                    "Values": ["AWS::EC2::Host"]
                },
                {
                    "Name": "deletion-protection",
                    "Values": ["UNLESS_EMPTY"]
                }
            ]
        }
    ]
}
```

- **`allowed-host-based-license-configurations`**

  Dieser Parameter gibt die Amazon Resource Name (ARN) -Pfade einer oder mehrerer Core-/Socket-basierter Lizenzkonfigurationen an, die Sie auf Mitglieder der Gruppe anwenden möchten.

  Datentyp der Werte: Ein Array von ARNs.

  Zulässige Werte: Jeder Wert muss ein gültiger License Manager Manager-Konfigurations-ARN sein.

  Erforderlich: Bedingt. Sie müssen entweder diesen Parameter oder`any-host-based-license-configuration`, aber nicht beide angeben. Sie schließen sich gegenseitig aus.

  Das folgende Beispielkonfigurationselement gibt an, dass Gruppenmitglieder die beiden angegebenen License Manager Manager-Konfigurationen verwenden können.

```
{
    "Configuration": [
        {
            "Type": "AWS::EC2::HostManagement",
            "Parameters": [
                {
                    "Name": "allowed-host-based-license-configurations",
                    "Values": [
                        "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-6eb6586f508a786a2ba41EXAMPLE1111",
                        "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-8a786a26f50ba416eb658EXAMPLE2222"
```

```
                    ]
                }
            ]
        },
        {
            "Type": "AWS::ResourceGroups::Generic",
            "Parameters": [
                {
                    "Name": "allowed-resource-types",
                    "Values": [ "AWS::EC2::Host" ]
                },
                {
                    "Name": "deletion-protection",
                    "Values": [ "UNLESS_EMPTY" ]
                }
            ]
        }
    ]
}
```

- **`any-host-based-license-configuration`**

  Dieser Parameter gibt an, dass Sie Ihrer Gruppe keine bestimmte Lizenzkonfiguration zuordnen möchten. In diesem Fall stehen alle Core-/Socket-basierten Lizenzkonfigurationen Ihren Mitgliedern Ihrer Host-Ressourcengruppe zur Verfügung. Verwenden Sie diese Einstellung, wenn Sie über eine unbegrenzte Anzahl von Lizenzen verfügen und die Hostauslastung optimieren möchten.

  Datentyp der Werte: Boolean

  Zulässige Werte: „true“ oder „false“ (muss in Kleinbuchstaben geschrieben werden).

  Erforderlich: Bedingt. Sie müssen entweder diesen Parameter oder`allowed-host-based-license-configurations`, aber nicht beide angeben. Sie schließen sich gegenseitig aus.

  Das folgende Beispielkonfigurationselement gibt an, dass Gruppenmitglieder jede Core-/Socket-basierte Lizenzkonfiguration verwenden können.

```
{
    "Configuration": [
        {
            "Type": "AWS::EC2::HostManagement",
            "Parameters": [
                {
```

```
                    "Name": "any-host-based-license-configuration",
                    "Values": ["true"]
                }
            ]
        },
        {
            "Type": "AWS::ResourceGroups::Generic",
            "Parameters": [
                {
                    "Name": "allowed-resource-types",
                    "Values": ["AWS::EC2::Host"]
                },
                {
                    "Name": "deletion-protection",
                    "Values": ["UNLESS_EMPTY"]
                }
            ]
        }
    ]
}
```

Das folgende Beispiel zeigt, wie alle Hostverwaltungseinstellungen in einer einzigen Konfiguration zusammengefasst werden können.

```
{
    "Configuration": [
        {
            "Type": "AWS::EC2::HostManagement",
            "Parameters": [
                {
                    "Name": "auto-allocate-host",
                    "Values": ["true"]
                },
                {
                    "Name": "auto-release-host",
                    "Values": ["false"]
                },
                {
                    "Name": "allowed-host-families",
                    "Values": ["c5", "m5"]
                },
                {
```

```
                    "Name": "allowed-host-based-license-configurations",
                    "Values": [
                        "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-6eb6586f508a786a2ba41EXAMPLE1111",
                        "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-8a786a26f50ba416eb658EXAMPLE2222"
                    ]
                }
            ]
        },
        {
            "Type": "AWS::ResourceGroups::Generic",
            "Parameters": [
                {
                    "Name": "allowed-resource-types",
                    "Values": ["AWS::EC2::Host"]
                },
                {
                    "Name": "deletion-protection",
                    "Values": ["UNLESS_EMPTY"]
                }
            ]
        }
    ]
}
```

`AWS::NetworkFirewall::RuleGroup`

Diese Kennung gibt Einstellungen für AWS Network Firewall Regelgruppen an, die für die Mitglieder der Gruppe durchgesetzt werden. Firewalladministratoren können den ARN einer Ressourcengruppe dieses Typs angeben, um die IP-Adressen der Gruppenmitglieder automatisch für eine Firewallregel aufzulösen, anstatt jede Adresse manuell auflisten zu müssen. Weitere Informationen finden Sie unter Tag-basierte Ressourcengruppen verwenden in AWS Network Firewall.

Sie können Ressourcengruppen dieses Konfigurationstyps mithilfe der Netzwerk-Firewall-Konsole oder durch Ausführen eines AWS CLI Befehls oder AWS SDK-Vorgangs erstellen.

Für Ressourcengruppen dieses Konfigurationstyps gelten die folgenden Einschränkungen:

- Die Mitglieder der Gruppe bestehen nur aus Ressourcen der Typen, die von der Network Firewall unterstützt werden.

- Die Gruppe muss eine tagbasierte Abfrage enthalten, um die Gruppenmitgliedschaft zu verwalten. Alle Ressourcen unterstützter Typen mit Tags, die der Abfrage entsprechen, sind automatisch Mitglieder der Gruppe.
- Für diesen Konfigurationstyp werden keine `Parameters` unterstützt.
- Um eine Ressourcengruppe dieses Konfigurationstyps zu löschen, kann keine Netzwerk-Firewall-Regelgruppe darauf verweisen.

Das folgende Beispiel veranschaulicht die `ResourceQuery` Abschnitte `Configuration` und für eine Gruppe dieses Typs.

```
{
    "Configuration": [
        {
            "Type": "AWS::NetworkFirewall::RuleGroup",
            "Parameters": []
        }
    ],
    "ResourceQuery": {
        "Query": "{\"ResourceTypeFilters\":[\"AWS::EC2::Instance\"],\"TagFilters\":
[{\"Key\":\"environment\",\"Values\":[\"production\"]}]}",
        "Type": "TAG_FILTERS_1_0"
    }
}
```

Der folgende AWS CLI Beispielbefehl erstellt eine Ressourcengruppe mit der vorherigen Konfiguration und Abfrage.

```
$ aws resource-groups create-group \
    --name test-group \
    --resource-query '{"Type": "TAG_FILTERS_1_0", "Query": "{\"ResourceTypeFilters\":
 [\"AWS::EC2::Instance\"], \"TagFilters\": [{\"Key\": \"environment\", \"Values\":
 [\"production\"]}]}"}' \
    --configuration '[{"Type": "AWS::NetworkFirewall::RuleGroup", "Parameters": []}]'
{
    "Group":{
        "GroupArn":"arn:aws:resource-groups:us-west-2:123456789012:group/test-group",
        "Name":"test-group",
        "OwnerId":"123456789012"
    },
    "Configuration": [
```

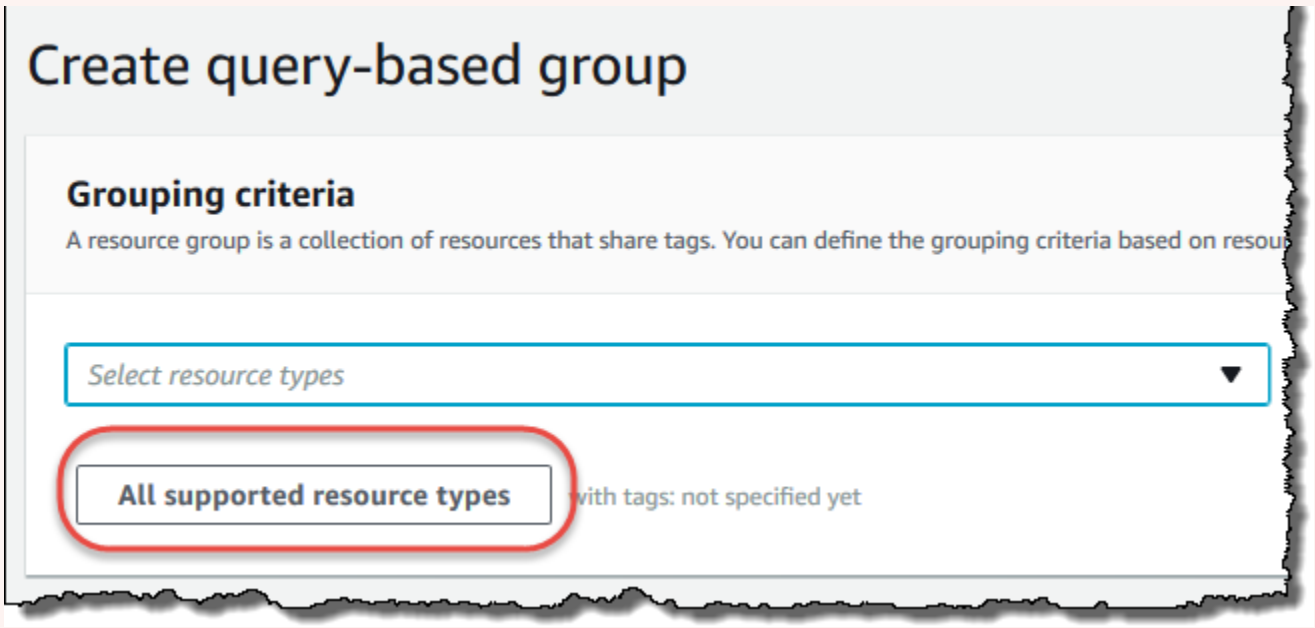
```
        {
            "Type": "AWS::NetworkFirewall::RuleGroup",
            "Parameters": []
        }
    ],
    "ResourceQuery": {
        "Query": "{\"ResourceTypeFilters\":[\"AWS::EC2::Instance\"],\"TagFilters\":
[{\"Key\":\"environment\",\"Values\":[\"production\"]}]}",
        "Type": "TAG_FILTERS_1_0"
    }
}
```

Ressourcentypen, die Sie mit AWS Resource Groups und Tag Editor verwenden können

Sie können die AWS Management Console oder die verwenden AWS CLI , um Ressourcengruppen zu erstellen und dann über diese Gruppen mit den Mitgliedsressourcen zu interagieren. Sie können Tags zu vielen AWS Ressourcen hinzufügen und diese Tags dann verwenden, um die Gruppenmitgliedschaft zu verwalten. In diesem Thema werden die AWS Ressourcentypen beschrieben, die Sie mithilfe von in Ressourcengruppen aufnehmen können AWS Resource Groups, sowie die Ressourcentypen, die Sie mithilfe des Tag-Editors markieren können.

Important

Eine Ressourcengruppe, die auf einer Abfrage für Alle unterstützten Ressourcentypen basiert, kann im Laufe der Zeit automatisch Mitglieder hinzufügen, da neue Ressourcen von Ressourcengruppen unterstützt werden. Wenn Sie Automatisierungen oder andere Massenaufgaben für eine vorhandene Ressourcengruppe basierend auf Alle unterstützten Ressourcentypen ausführen, beachten Sie, dass die Aktionen möglicherweise auf vielen mehr Ressourcen ausgeführt werden, als beim ersten Erstellen der Gruppe in der Gruppe waren. Dies kann auch bedeuten, dass Automatisierungen oder Aufgaben, die Sie für andere Ressourcen erstellt haben, auf möglicherweise unbeabsichtigte Ressourcen oder Ressourcen angewendet werden, auf denen die Aufgaben nicht erfolgreich abgeschlossen werden können. In diesen Fällen können Sie einen Ressourcentypfilter hinzufügen, um anzugeben, dass nur Ressourcen der angegebenen Typen Teil der Gruppe sein können.



In den folgenden Tabellen wird aufgeführt, welche Ressourcentypen für das Tagging im Tag Editor, für die Mitgliedschaft in abfragebasierten Tag-Gruppen und für die Mitgliedschaft in AWS CloudFormation Stack-basierten Gruppen unterstützt werden.

Spaltendefinitionen

- Markierung des Tag-Editors – Sie können Ressourcen dieses Typs mithilfe der Konsole des Tag-Editors markieren. Andernfalls müssen Sie entweder die AWS Resource Groups Tagging API oder die Tagging-Services verwenden, die nativ vom Eigentümerdienst dieser Ressource unterstützt werden.
- Tag-basierte Gruppen – Sie können Ressourcen dieses Typs in Ressourcengruppen aufnehmen, deren Mitgliedschaft durch die Tags bestimmt wird, die den Ressourcen zugeordnet sind. Die Gruppe gibt Tag-Schlüsselnamen und -werte an, und alle Ressourcen mit übereinstimmenden Tags sind automatisch Teil der Gruppe
- AWS CloudFormation Stack-basierte Gruppen – Sie können Ressourcen dieses Typs in Ressourcengruppen aufnehmen, deren Mitgliedschaft aus den Ressourcen besteht, die als Teil eines CloudFormation Stacks erstellt wurden. Die Gruppe gibt den ARN des Stacks an, und alle seine Ressourcen sind automatisch Mitglieder der Gruppe.

> **Note**
>
> Das Hinzufügen von Tags zu einem AWS CloudFormation Stack führt zu einer Aktualisierung des Stacks.

Eine Liste der Ressourcentypen, die veraltet sind und von Resource Groups nicht mehr unterstützt werden, finden Sie im Abschnitt Veraltete Ressourcentypen am Ende dieses Themas.

Amazon API Gateway

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::ApiGateway::Account`	✗ Nein	✗ Nein	✓ Ja
`AWS::ApiGateway::ApiKey`	✗ Nein	✓ Ja	✓ Ja
`AWS::ApiGateway::ClientCertificate`	✗ Nein	✓ Ja	✗ Nein
`AWS::ApiGateway::DomainName`	✗ Nein	✗ Nein	✓ Ja
`AWS::ApiGateway::RestApi`	✗ Nein	✓ Ja	✓ Ja
`AWS::ApiGateway::Stage`	✗ Nein	✓ Ja	✗ Nein
`AWS::ApiGateway::UsagePlan`	✗ Nein	✓ Ja	✓ Ja

IAM Access Analyzer

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::AccessAnalyzer::Analyzer`	✗ Nein	✓ Ja	✗ Nein

AWS Amplify

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Amplify::App`	✗ Nein	✓ Ja	✗ Nein

AWS App Mesh

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::AppMesh::Mesh`	✗ Nein	✓ Ja	✗ Nein

Amazon AppStream

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::AppStream::AppBlock`	✗ Nein	✓ Ja	✗ Nein
`AWS::AppStream::Application`	✗ Nein	✓ Ja	✗ Nein
`AWS::AppStream::Fleet`	✓ Ja	✓ Ja	✓ Ja
`AWS::AppStream::ImageBuilder`	✓ Ja	✓ Ja	✓ Ja
`AWS::AppStream::Stack`	✓ Ja	✓ Ja	✓ Ja

AWS AppSync

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::AppSync::DataSource`	✗ Nein	✗ Nein	✓ Ja
`AWS::AppSync::GraphQLApi`	✗ Nein	✗ Nein	✓ Ja

AWS Backup

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Backup::BackupPlan`	✗ Nein	✓ Ja	✗ Nein
`AWS::Backup::BackupVault`	✗ Nein	✓ Ja	✗ Nein
`AWS::Backup::ReportPlan`	✗ Nein	✓ Ja	✗ Nein

AWS Batch

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Batch::ComputeEnvironment`	✗ Nein	✓ Ja	✗ Nein
`AWS::Batch::JobQueue`	✗ Nein	✓ Ja	✗ Nein
`AWS::Batch::SchedulingPolicy`	✗ Nein	✓ Ja	✗ Nein

AWS Billing Conductor

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::BillingConductor::BillingGroup`	✗ Nein	✓ Ja	✓ Ja
`AWS::BillingConductor::CustomLineItem`	✗ Nein	✓ Ja	✓ Ja
`AWS::BillingConductor::PricingPlan`	✗ Nein	✓ Ja	✓ Ja
`AWS::BillingConductor::PricingRule`	✗ Nein	✓ Ja	✓ Ja

Amazon Braket

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Braket::Job`	✗ Nein	✓ Ja	✗ Nein
`AWS::Braket::QuantumTask`	✓ Ja	✓ Ja	✗ Nein

AWS Certificate Manager

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::CertificateManager::Certificate`	✓ Ja	✓ Ja	✓ Ja

AWS Certificate Manager Private Zertifizierungsstelle

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::ACMPCA::CertificateAuthority`	✗ Nein	✓ Ja	✗ Nein

AWS Cloud9

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Cloud9::Environment`	✓ Ja	✓ Ja	✗ Nein

AWS CloudFormation

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::CloudFormation::Stack`	✓ Ja	✓ Ja	✓ Ja

Amazon CloudFront

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::CloudFront::Distribution`	Bol Ja1	Ja2	Bol Ja2
`AWS::CloudFront::StreamingDistribution`	Ja1	Bol Ja2	Bol Ja2

1 Dies ist eine Ressource für einen globalen Service, der in der Region USA Ost (Nord-Virginia) gehostet wird. Um den Tag-Editor zum Erstellen oder Ändern von Tags für diesen Ressourcentyp zu verwenden, müssen Sie `us-east-1` in der Liste Regionen auswählen unter Zu markierende Ressourcen finden in der Tag-Editor-Konsole einfügen.

2 Dies ist eine Ressource für einen globalen Service, der in der Region USA Ost (Nord-Virginia) gehostet wird. Da Ressourcengruppen für jede Region separat verwaltet werden, müssen Sie Ihre AWS Management Console auf die umstellen AWS-Region , die die Ressourcen enthält, die Sie in die Gruppe aufnehmen möchten. Um eine Ressourcengruppe AWS Management Console zu

erstellen, die eine globale -Ressource enthält, müssen Sie Ihre mit der Regionsauswahl in der oberen rechten Ecke der für USA Ost (Nord-Virginia) us-east-1 konfigurieren AWS Management Console.

AWS CloudTrail

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::CloudTrail::Channel`	✗ Nein	✓ Ja	✗ Nein
`AWS::CloudTrail::EventDataStore`	✗ Nein	✓ Ja	✗ Nein
`AWS::CloudTrail::Trail`	✓ Ja	✓ Ja	✓ Ja

Amazon CloudWatch

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::CloudWatch::Alarm`	✓ Ja	✓ Ja	✓ Ja
`AWS::CloudWatch::Dashboard`	✗ Nein	✗ Nein	✓ Ja
`AWS::CloudWatch::InsightRule`	✗ Nein	✓ Ja	✗ Nein
`AWS::CloudWatch::MetricStream`	✗ Nein	✓ Ja	✗ Nein
`AWS::CloudWatch::ServiceLevelObjective`	✗ Nein	✓ Ja	✗ Nein

Amazon CloudWatch -Protokolle

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Logs::Destination`	✗ Nein	✓ Ja	✗ Nein
`AWS::Logs::LogGroup`	✗ Nein	✓ Ja	✓ Ja

Amazon CloudWatch Synthetics

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Synthetics::Canary`	✗ Nein	✓ Ja	✓ Ja

AWS CodeArtifact

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::CodeArtifact::Domain`	✓ Ja	✓ Ja	✓ Ja

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::CodeArtifact::Repository`	✓ Ja	✓ Ja	✓ Ja

AWS CodeBuild

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::CodeBuild::Project`	✓ Ja	✓ Ja	X Nein

AWS CodeCommit

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::CodeCommit::Repository`	✓ Ja	✓ Ja	X Nein

AWS CodeDeploy

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::CodeDeploy::Application`	✗ Nein	✓ Ja	✓ Ja
`AWS::CodeDeploy::DeploymentConfig`	✗ Nein	✗ Nein	✓ Ja

Amazon CodeGuru Reviewer

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::CodeGuruReviewer::RepositoryAssociation`	✓ Ja	✓ Ja	✓ Ja

Amazon CodeGuru Profiler

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::CodeGuruProfiler::ProfilingGroup`	✗ Nein	✓ Ja	✗ Nein

AWS CodePipeline

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::CodePipeline::CustomActionType`	✗ Nein	✓ Ja	✗ Nein
`AWS::CodePipeline::Pipeline`	✓ Ja	✓ Ja	✓ Ja
`AWS::CodePipeline::Webhook`	✓ Ja	✓ Ja	✓ Ja

AWS CodeConnections

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::CodeStarConnections::Connection`	✗ Nein	✓ Ja	✗ Nein

Amazon Cognito

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Cognito::IdentityPool`	✓ Ja	✓ Ja	✓ Ja
`AWS::Cognito::UserPool`	✓ Ja	✓ Ja	✓ Ja

Amazon Comprehend

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Comprehend::DocumentClassifier`	✓ Ja	✓ Ja	✗ Nein

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Comprehend::EntityRecognizer`	✓ Ja	✓ Ja	✗ Nein

AWS Config

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Config::ConfigRule`	✓ Ja	✓ Ja	✗ Nein

Amazon Connect Wisdom

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Wisdom::Assistant`	✗ Nein	✓ Ja	✓ Ja
`AWS::Wisdom::AssistantAssociation`	✗ Nein	✓ Ja	✓ Ja
`AWS::Wisdom::Content`	✗ Nein	✓ Ja	✗ Nein

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Wisdom::KnowledgeBase`	✗ Nein	✓ Ja	✓ Ja
`AWS::Wisdom::Session`	✗ Nein	✓ Ja	✗ Nein

AWS Datenaustausch

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::DataExchange::DataSet`	✓ Ja	✓ Ja	✗ Nein
`AWS::DataExchange::Revision`	✗ Nein	✓ Ja	✗ Nein

AWS Data Pipeline

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::DataPipeline::Pipeline`	✓ Ja	✓ Ja	✓ Ja

AWS DataSync

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::DataSync::Task`	✗ Nein	✓ Ja	✗ Nein

AWS Database Migration Service

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::DMS::Certificate`	✓ Ja	✓ Ja	✗ Nein
`AWS::DMS::Endpoint`	✓ Ja	✓ Ja	✓ Ja
`AWS::DMS::EventSubscription`	✓ Ja	✓ Ja	✗ Nein
`AWS::DMS::ReplicationInstance`	✓ Ja	✓ Ja	✓ Ja
`AWS::DMS::ReplicationSubnetGroup`	✓ Ja	✓ Ja	✗ Nein
`AWS::DMS::ReplicationTask`	✓ Ja	✓ Ja	✗ Nein

Amazon DynamoDB

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::DynamoDB::Table`	✓ Ja	✓ Ja	✓ Ja

Amazon EMR

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::EMR::Cluster`	✓ Ja	✓ Ja	✓ Ja

Amazon-EMR-Container

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::EMRContainers::JobRun`	✗ Nein	✓ Ja	✗ Nein
`AWS::EMRContainers::VirtualCluster`	✓ Ja	✓ Ja	✓ Ja

Amazon EMR Serverless

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::EMRServerless::Application`	✗ Nein	✓ Ja	✓ Ja
`AWS::EMRServerless::JobRun`	✗ Nein	✓ Ja	✗ Nein

Amazon ElastiCache

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::ElastiCache::CacheCluster`	✓ Ja	✓ Ja	✓ Ja
`AWS::ElastiCache::ParameterGroup`	✗ Nein	✓ Ja	✗ Nein
`AWS::ElastiCache::SecurityGroup`	✗ Nein	✓ Ja	✗ Nein
`AWS::ElastiCache::Snapshot`	✓ Ja	✓ Ja	✗ Nein
`AWS::ElastiCache::SubnetGroup`	✗ Nein	✓ Ja	✗ Nein
`AWS::ElastiCache::User`	✗ Nein	✓ Ja	✗ Nein
`AWS::ElastiCache::UserGroup`	✗ Nein	✓ Ja	✗ Nein

AWS Elastic Beanstalk

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::ElasticBeanstalk::Application`	✓ Ja	✓ Ja	✗ Nein
`AWS::ElasticBeanstalk::ApplicationVersion`	✗ Nein	✓ Ja	✗ Nein
`AWS::ElasticBeanstalk::ConfigurationTemplate`	✗ Nein	✓ Ja	✗ Nein
`AWS::ElasticBeanstalk::Environment`	✗ Nein	✓ Ja	✗ Nein

Amazon Elastic Compute Cloud (Amazon EC2)

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::EC2::CapacityReservation`	✗ Nein	✓ Ja	✗ Nein
`AWS::EC2::CapacityReservationFleet`	✗ Nein	✓ Ja	✗ Nein
`AWS::EC2::CarrierGateway`	✗ Nein	✓ Ja	✗ Nein
`AWS::EC2::ClientVpnEndpoint`	✗ Nein	✓ Ja	✗ Nein
`AWS::EC2::CoipPool`	✗ Nein	✓ Ja	✗ Nein

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
AWS::EC2::CustomerGateway	✓ Ja	✓ Ja	✓ Ja
AWS::EC2::DHCPOptions	✓ Ja	✓ Ja	✓ Ja
AWS::EC2::EC2Fleet	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::EgressOnlyInternetGateway	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::EIP	✓ Ja	✓ Ja	✗ Nein
AWS::EC2::ExportImageTask	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::ExportInstanceTask	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::FlowLog	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::FpgaImage	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::Host	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::HostReservation	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::Image	✓ Ja	✓ Ja	✗ Nein
AWS::EC2::ImportImageTask	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::ImportSnapshotTask	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::Instance	✓ Ja	✓ Ja	✓ Ja
AWS::EC2::InstanceEventWindow	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::InternetGateway	✓ Ja	✓ Ja	✓ Ja

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
AWS::EC2::IPv4Pool	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::IPv6Pool	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::KeyPair	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::LaunchTemplate	✗ Nein	✓ Ja	✓ Ja
AWS::EC2::LocalGateway	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::LocalGatewayRouteTable	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::LocalGatewayRouteTableVirtualInterfaceGroupAssociation	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::LocalGatewayRouteTableVPCAssociation	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::LocalGatewayVirtualInterface	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::LocalGatewayVirtualInterfaceGroup	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::NatGateway	✓ Ja	✓ Ja	✓ Ja
AWS::EC2::NetworkAcl	✓ Ja	✓ Ja	✓ Ja
AWS::EC2::NetworkInsightsAccessScope	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::NetworkInsightsAccessScopeAnalysis	✗ Nein	✓ Ja	✗ Nein

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
AWS::EC2::NetworkInsightsAnalysis	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::NetworkInsightsPath	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::NetworkInterface	✓ Ja	✓ Ja	✓ Ja
AWS::EC2::PlacementGroup	✗ Nein	✓ Ja	✓ Ja
AWS::EC2::PrefixList	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::ReplaceRootVolumeTask	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::ReservedInstance	✓ Ja	✓ Ja	✗ Nein
AWS::EC2::RouteTable	✓ Ja	✓ Ja	✓ Ja
AWS::EC2::SecurityGroup	✓ Ja	✓ Ja	✓ Ja
AWS::EC2::Snapshot	✓ Ja	✓ Ja	✗ Nein
AWS::EC2::SpotFleet	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::SpotInstanceRequest	✓ Ja	✓ Ja	✗ Nein
AWS::EC2::Subnet	✓ Ja	✓ Ja	✓ Ja
AWS::EC2::SubnetCidrReservation	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::TrafficMirrorFilter	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::TrafficMirrorSession	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::TrafficMirrorTarget	✗ Nein	✓ Ja	✗ Nein

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
AWS::EC2::TransitGateway	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::TransitGatewayAttachment	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::TransitGatewayConnectPeer	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::TransitGatewayMulticastDomain	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::TransitGatewayPolicyTable	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::TransitGatewayRouteTable	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::TransitGatewayRouteTableAnnouncement	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::VerifiedAccessEndpoint	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::VerifiedAccessGroup	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::VerifiedAccessInstance	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::VerifiedAccessTrustProvider	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::Volume	✓ Ja	✓ Ja	✓ Ja
AWS::EC2::VPC	✓ Ja	✓ Ja	✓ Ja
AWS::EC2::VPCEndpoint	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::VPCEndpointConnection	✗ Nein	✓ Ja	✗ Nein
AWS::EC2::VPCEndpointService	✗ Nein	✓ Ja	✗ Nein

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::EC2::VPCEndpointServicePermissions`	✗ Nein	✓ Ja	✗ Nein
`AWS::EC2::VPCPeeringConnection`	✗ Nein	✓ Ja	✓ Ja
`AWS::EC2::VPNConnection`	✓ Ja	✓ Ja	✓ Ja
`AWS::EC2::VPNGateway`	✓ Ja	✓ Ja	✓ Ja

Amazon Elastic Container Registry

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::ECR::Repository`	✗ Nein	✓ Ja	✗ Nein

Amazon Elastic Container Service

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::ECS::CapacityProvider`	✗ Nein	✓ Ja	✗ Nein
`AWS::ECS::Cluster`	✓ Ja	✓ Ja	✗ Nein
`AWS::ECS::ContainerInstance`	✗ Nein	✓ Ja	✗ Nein
`AWS::ECS::Service`	✗ Nein	✓ Ja	✗ Nein
`AWS::ECS::Task`	✗ Nein	✓ Ja	✗ Nein
`AWS::ECS::TaskDefinition`	✓ Ja	✓ Ja	✗ Nein
`AWS::ECS::TaskSet`	✗ Nein	✓ Ja	✗ Nein

Amazon Elastic File System

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::EFS::FileSystem`	✓ Ja	✓ Ja	✓ Ja

Amazon Elastic Inference

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::ElasticInference::ElasticInferenceAccelerator`	✓ Ja	✓ Ja	✗ Nein

Amazon Elastic Kubernetes Service (Amazon EKS)

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::EKS::Cluster`	✓ Ja	✓ Ja	✓ Ja

Elastic Load Balancing

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::ElasticLoadBalancing::LoadBalancer`	✓ Ja	✓ Ja	✓ Ja

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::ElasticLoadBalancingV2::Listener`	✗ Nein	✓ Ja	✓ Ja
`AWS::ElasticLoadBalancingV2::ListenerRule`	✗ Nein	✓ Ja	✓ Ja
`AWS::ElasticLoadBalancingV2::LoadBalancer`	✓ Ja	✓ Ja	✓ Ja
`AWS::ElasticLoadBalancingV2::TargetGroup`	✓ Ja	✓ Ja	✓ Ja

Amazon OpenSearch Service

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Elasticsearch::Domain`	✓ Ja	✓ Ja	✓ Ja

Amazon CloudWatch -Ereignisse

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Events::EventBus`	✗ Nein	✓ Ja	✗ Nein
`AWS::Events::Rule`	✓ Ja	✓ Ja	✓ Ja

> **Note**
>
> Regeln in benutzerdefinierten Event Buses werden im Tag Editor nicht unterstützt.

Amazon EventBridge Schemata

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::EventSchemas::Discoverer`	✗ Nein	✓ Ja	✗ Nein
`AWS::EventSchemas::Registry`	✗ Nein	✓ Ja	✗ Nein
`AWS::EventSchemas::Schema`	✗ Nein	✓ Ja	✗ Nein

Amazon FSx

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::FSx::FileSystem`	✓ Ja	✓ Ja	✗ Nein

Amazon Forecast

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Forecast::Dataset`	✓ Ja	✓ Ja	✗ Nein
`AWS::Forecast::DatasetGroup`	✓ Ja	✓ Ja	✗ Nein
`AWS::Forecast::DatasetImportJob`	✓ Ja	✓ Ja	✗ Nein
`AWS::Forecast::Forecast`	✓ Ja	✓ Ja	✗ Nein
`AWS::Forecast::ForecastExportJob`	✓ Ja	✓ Ja	✗ Nein
`AWS::Forecast::Predictor`	✓ Ja	✓ Ja	✗ Nein
`AWS::Forecast::PredictorBacktestExportJob`	✓ Ja	✓ Ja	✗ Nein

Amazon Fraud Detector

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::FraudDetector::Detector`	✓ Ja	✓ Ja	× Nein
`AWS::FraudDetector::DetectorVersion`	× Nein	✓ Ja	× Nein
`AWS::FraudDetector::EntityType`	✓ Ja	✓ Ja	× Nein
`AWS::FraudDetector::EventType`	✓ Ja	✓ Ja	× Nein
`AWS::FraudDetector::ExternalModel`	✓ Ja	✓ Ja	× Nein
`AWS::FraudDetector::Label`	✓ Ja	✓ Ja	× Nein
`AWS::FraudDetector::Model`	✓ Ja	✓ Ja	× Nein
`AWS::FraudDetector::ModelVersion`	× Nein	✓ Ja	× Nein
`AWS::FraudDetector::Outcome`	✓ Ja	✓ Ja	× Nein
`AWS::FraudDetector::Rule`	× Nein	✓ Ja	× Nein
`AWS::FraudDetector::Variable`	✓ Ja	✓ Ja	× Nein

Amazon GameLift

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::GameLift::Alias`	✗ Nein	✓ Ja	✗ Nein
`AWS::GameLift::GameSessionQueue`	✗ Nein	✓ Ja	✗ Nein
`AWS::GameLift::MatchmakingConfiguration`	✗ Nein	✓ Ja	✗ Nein
`AWS::GameLift::MatchmakingRuleSet`	✗ Nein	✓ Ja	✗ Nein

AWS Global Accelerator

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::GlobalAccelerator::Accelerator`	✗ Nein	✓ Ja	✗ Nein

AWS Glue

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Glue::Crawler`	✓ Ja	✓ Ja	✗ Nein
`AWS::Glue::Database`	✗ Nein	✓ Ja	✓ Ja
`AWS::Glue::Job`	✓ Ja	✓ Ja	✗ Nein
`AWS::Glue::Trigger`	✓ Ja	✓ Ja	✗ Nein
`AWS::Glue::Workflow`	✗ Nein	✓ Ja	✗ Nein

AWS Glue DataBrew

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::DataBrew::Dataset`	✓ Ja	✓ Ja	✓ Ja
`AWS::DataBrew::Job`	✓ Ja	✓ Ja	✓ Ja
`AWS::DataBrew::Project`	✓ Ja	✓ Ja	✓ Ja
`AWS::DataBrew::Recipe`	✓ Ja	✓ Ja	✓ Ja
`AWS::DataBrew::Schedule`	✓ Ja	✓ Ja	✓ Ja

AWS Ground Station

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::GroundStation::Config`	✗ Nein	✓ Ja	✗ Nein

Amazon GuardDuty

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::GuardDuty::Detector`	✗ Nein	✓ Ja	✓ Ja
`AWS::GuardDuty::Filter`	✗ Nein	✓ Ja	✗ Nein
`AWS::GuardDuty::IPSet`	✗ Nein	✓ Ja	✗ Nein
`AWS::GuardDuty::ThreatIntelSet`	✗ Nein	✓ Ja	✗ Nein

Amazon Interactive Video Service

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::IVS::Channel`	✗ Nein	✓ Ja	✗ Nein
`AWS::IVS::RecordingConfiguration`	✗ Nein	✓ Ja	✗ Nein
`AWS::IVS::StreamKey`	✗ Nein	✓ Ja	✗ Nein

AWS Identity and Access Management

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::IAM::InstanceProfile`	Bol Ja1	Bol Ja2	✗ Nein
`AWS::IAM::ManagedPolicy`	Bol Ja1	Ja2	✗ Nein
`AWS::IAM::OpenIDConnectProvider`	Bol Ja1	Ja2	✗ Nein
`AWS::IAM::Role`	✗ Nein	✗ Nein	Ja2
`AWS::IAM::SAMLProvider`	Bol Ja1	Ja2	✗ Nein
`AWS::IAM::ServerCertificate`	Bol Ja1	Bol Ja2	✗ Nein
`AWS::IAM::VirtualMFADevice`	Bol Ja1	Bol Ja2	✗ Nein

1 Dies ist eine Ressource für einen globalen Service, der in der Region USA Ost (Nord-Virginia) gehostet wird. Um den Tag-Editor zum Erstellen oder Ändern von Tags für diesen Ressourcentyp zu verwenden, müssen Sie `us-east-1` in der Liste Regionen auswählen unter Zu markierende Ressourcen finden in der Tag-Editor-Konsole einfügen.

2 Dies ist eine Ressource für einen globalen Service, der in der Region USA Ost (Nord-Virginia) gehostet wird. Da Ressourcengruppen für jede Region separat verwaltet werden, müssen Sie Ihre AWS Management Console auf die umstellen AWS-Region , die die Ressourcen enthält, die Sie in die Gruppe aufnehmen möchten. Um eine Ressourcengruppe AWS Management Console zu erstellen, die eine globale -Ressource enthält, müssen Sie Ihre für USA Ost (Nord-Virginia) us-east-1 konfigurieren, indem Sie die Regionsauswahl in der oberen rechten Ecke der verwenden AWS Management Console.

EC2 Image Builder

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::ImageBuilder::Component`	✗ Nein	✓ Ja	✗ Nein
`AWS::ImageBuilder::ContainerRecipe`	✗ Nein	✓ Ja	✗ Nein
`AWS::ImageBuilder::DistributionConfiguration`	✗ Nein	✓ Ja	✗ Nein
`AWS::ImageBuilder::Image`	✗ Nein	✓ Ja	✗ Nein
`AWS::ImageBuilder::ImagePipeline`	✗ Nein	✓ Ja	✗ Nein
`AWS::ImageBuilder::ImageRecipe`	✗ Nein	✓ Ja	✗ Nein
`AWS::ImageBuilder::InfrastructureConfiguration`	✗ Nein	✓ Ja	✗ Nein

Amazon Inspector

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Inspector::AssessmentTemplate`	✗ Nein	✓ Ja	✓ Ja

AWS IoT

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::IoT::Authorizer`	✗ Nein	✓ Ja	✗ Nein
`AWS::IoT::CustomMetric`	✗ Nein	✓ Ja	✗ Nein
`AWS::IoT::Dimension`	✗ Nein	✓ Ja	✗ Nein
`AWS::IoT::JobTemplate`	✗ Nein	✓ Ja	✗ Nein
`AWS::IoT::MitigationAction`	✗ Nein	✓ Ja	✗ Nein
`AWS::IoT::Policy`	✗ Nein	✓ Ja	✗ Nein
`AWS::IoT::RoleAlias`	✗ Nein	✓ Ja	✗ Nein
`AWS::IoT::ScheduledAudit`	✗ Nein	✓ Ja	✗ Nein
`AWS::IoT::SecurityProfile`	✗ Nein	✓ Ja	✗ Nein

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::IoT::TopicRule`	✗ Nein	✓ Ja	✓ Ja

AWS IoT Analytics

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::IoTAnalytics::Channel`	✗ Nein	✓ Ja	✗ Nein
`AWS::IoTAnalytics::Dataset`	✓ Ja	✓ Ja	✗ Nein
`AWS::IoTAnalytics::Datastore`	✗ Nein	✓ Ja	✗ Nein
`AWS::IoTAnalytics::Pipeline`	✗ Nein	✓ Ja	✗ Nein

AWS IoT Events

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::IoTEvents::DetectorModel`	✓ Ja	✓ Ja	✓ Ja
`AWS::IoTEvents::Input`	✓ Ja	✓ Ja	✓ Ja

AWS IoT FleetWise

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::IoTFleetWise::Campaign`	✗ Nein	✓ Ja	✓ Ja
`AWS::IoTFleetWise::DecoderManifest`	✗ Nein	✓ Ja	✓ Ja
`AWS::IoTFleetWise::Fleet`	✗ Nein	✓ Ja	✓ Ja
`AWS::IoTFleetWise::ModelManifest`	✗ Nein	✓ Ja	✓ Ja
`AWS::IoTFleetWise::SignalCatalog`	✗ Nein	✓ Ja	✓ Ja
`AWS::IoTFleetWise::Vehicle`	✗ Nein	✓ Ja	✓ Ja

AWS IoT Greengrass

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Greengrass::ConnectorDefinition`	✓ Ja	✓ Ja	✗ Nein
`AWS::Greengrass::CoreDefinition`	✓ Ja	✓ Ja	✗ Nein
`AWS::Greengrass::DeviceDefinition`	✓ Ja	✓ Ja	✗ Nein
`AWS::Greengrass::FunctionDefinition`	✓ Ja	✓ Ja	✗ Nein
`AWS::Greengrass::Group`	✓ Ja	✓ Ja	✗ Nein
`AWS::Greengrass::LoggerDefinition`	✓ Ja	✓ Ja	✗ Nein
`AWS::Greengrass::ResourceDefinition`	✓ Ja	✓ Ja	✗ Nein
`AWS::Greengrass::SubscriptionDefinition`	✓ Ja	✓ Ja	✗ Nein

AWS-IoT-SiteWise-Konsole

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::IoTSiteWise::Asset`	✗ Nein	✓ Ja	✗ Nein

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::IoTSiteWise::AssetModel`	✗ Nein	✓ Ja	✗ Nein
`AWS::IoTSiteWise::Gateway`	✗ Nein	✓ Ja	✗ Nein

AWS Key Management Service

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::KMS::Alias`	✗ Nein	✗ Nein	✓ Ja
`AWS::KMS::Key`	✓ Ja	✓ Ja	✓ Ja

Amazon Keyspaces (für Apache Cassandra)

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Cassandra::Keyspace`	✗ Nein	✓ Ja	✓ Ja

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Cassandra::Table`	✗ Nein	✓ Ja	✗ Nein

Amazon Kinesis

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Kinesis::Stream`	✓ Ja	✓ Ja	✓ Ja

Amazon Managed Service für Apache Flink

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::KinesisAnalytics::Application`	✓ Ja	✓ Ja	✓ Ja
`AWS::KinesisAnalyticsV2::Application`	✗ Nein	✗ Nein	✓ Ja

Amazon Data Firehose

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::KinesisFirehose::DeliveryStream`	✗ Nein	✓ Ja	✓ Ja

AWS Lambda

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Lambda::Alias`	✗ Nein	✗ Nein	✓ Ja
`AWS::Lambda::EventSourceMapping`	✗ Nein	✗ Nein	✓ Ja
`AWS::Lambda::Function`	✓ Ja	✓ Ja	✓ Ja
`AWS::Lambda::LayerVersion`	✗ Nein	✗ Nein	✓ Ja
`AWS::Lambda::Version`	✗ Nein	✗ Nein	✓ Ja

Amazon MQ

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::AmazonMQ::Broker`	✓ Ja	✓ Ja	✗ Nein
`AWS::AmazonMQ::Configuration`	✓ Ja	✓ Ja	✗ Nein

Amazon Macie

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Macie::ClassificationJob`	✓ Ja	✓ Ja	✗ Nein
`AWS::Macie::CustomDataIdentifier`	✓ Ja	✓ Ja	✓ Ja
`AWS::Macie::FindingsFilter`	✓ Ja	✓ Ja	✓ Ja
`AWS::Macie::Member`	✓ Ja	✓ Ja	✗ Nein

Amazon Managed Streaming für Apache Kafka

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Kafka::Cluster`	✓ Ja	✓ Ja	✗ Nein

AWS Elemental MediaConnect

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::MediaConnect::Flow`	✗ Nein	✓ Ja	✗ Nein
`AWS::MediaConnect::FlowEntitlement`	✗ Nein	✓ Ja	✗ Nein
`AWS::MediaConnect::FlowOutput`	✗ Nein	✓ Ja	✗ Nein
`AWS::MediaConnect::FlowSource`	✗ Nein	✓ Ja	✗ Nein

AWS Elemental MediaPackage

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::MediaPackage::Channel`	✗ Nein	✓ Ja	✗ Nein
`AWS::MediaPackage::PackagingConfiguration`	✗ Nein	✓ Ja	✗ Nein
`AWS::MediaPackage::PackagingGroup`	✗ Nein	✓ Ja	✗ Nein

AWS Network Manager

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::NetworkManager::CoreNetwork`	✗ Nein	✓ Ja	✗ Nein
`AWS::NetworkManager::Device`	✗ Nein	✓ Ja	✗ Nein
`AWS::NetworkManager::GlobalNetwork`	✗ Nein	✓ Ja	✗ Nein
`AWS::NetworkManager::Link`	✗ Nein	✓ Ja	✗ Nein
`AWS::NetworkManager::Site`	✗ Nein	✓ Ja	✗ Nein
`AWS::NetworkManager::VpcAttachment`	✗ Nein	✓ Ja	✗ Nein

Amazon OpenSearch Service OpenSearch

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::OpenSearchService::Domain`	✓ Ja	✓ Ja	✓ Ja

AWS OpsWorks

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::OpsWorks::Instance`	✗ Nein	✓ Ja	✓ Ja
`AWS::OpsWorks::Layer`	✗ Nein	✓ Ja	✓ Ja
`AWS::OpsWorks::Stack`	✗ Nein	✓ Ja	✓ Ja

AWS Organizations

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Organizations::Account`	✓ Ja	✓ Ja	✗ Nein
`AWS::Organizations::OrganizationalUnit`	✗ Nein	✓ Ja	✗ Nein
`AWS::Organizations::Policy`	✗ Nein	✓ Ja	✗ Nein
`AWS::Organizations::Root`	✓ Ja	✓ Ja	✗ Nein

Amazon Pinpoint

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Pinpoint::App`	✗ Nein	✓ Ja	✓ Ja
`AWS::Pinpoint::EmailTemplate`	✗ Nein	✓ Ja	✓ Ja
`AWS::Pinpoint::PushTemplate`	✗ Nein	✓ Ja	✓ Ja
`AWS::Pinpoint::SmsTemplate`	✗ Nein	✓ Ja	✓ Ja
`AWS::Pinpoint::VoiceTemplate`	✗ Nein	✓ Ja	✗ Nein

Amazon-Pinpoint-SMS- und -Sprachnachrichten-API

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::PinpointSMSVoiceV2::Pool`	✗ Nein	✓ Ja	✗ Nein

Amazon Quantum Ledger Database (Amazon QLDB)

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::QLDB::Ledger`	✓ Ja	✓ Ja	✓ Ja
`AWS::QLDB::Stream`	✗ Nein	✓ Ja	✓ Ja

Amazon Redshift

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Redshift::Cluster`	✓ Ja	✓ Ja	✓ Ja

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
AWS::Redshift::ClusterParameterGroup	✓ Ja	✓ Ja	✓ Ja
AWS::Redshift::ClusterSecurityGroup	✗ Nein	✓ Ja	✓ Ja
AWS::Redshift::ClusterSubnetGroup	✓ Ja	✓ Ja	✓ Ja
AWS::Redshift::DBGroup	✗ Nein	✓ Ja	✗ Nein
AWS::Redshift::DBName	✗ Nein	✓ Ja	✗ Nein
AWS::Redshift::DBUser	✗ Nein	✓ Ja	✗ Nein
AWS::Redshift::EventSubscription	✗ Nein	✓ Ja	✗ Nein
AWS::Redshift::HSMClientCertificate	✓ Ja	✓ Ja	✗ Nein
AWS::Redshift::HSMConfiguration	✗ Nein	✓ Ja	✗ Nein
AWS::Redshift::Namespace	✗ Nein	✓ Ja	✗ Nein
AWS::Redshift::Snapshot	✗ Nein	✓ Ja	✗ Nein
AWS::Redshift::SnapshotCopyGrant	✗ Nein	✓ Ja	✗ Nein
AWS::Redshift::SnapshotSchedule	✗ Nein	✓ Ja	✗ Nein
AWS::Redshift::UsageLimit	✗ Nein	✓ Ja	✗ Nein

Amazon Relational Database Service (Amazon RDS)

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
AWS::RDS::CustomDBEngineVersion	✗ Nein	✓ Ja	✗ Nein
AWS::RDS::DBCluster	✓ Ja	✓ Ja	✓ Ja
AWS::RDS::DBClusterEndpoint	✗ Nein	✓ Ja	✗ Nein
AWS::RDS::DBClusterParameterGroup	✓ Ja	✓ Ja	✓ Ja
AWS::RDS::DBClusterSnapshot	✓ Ja	✓ Ja	✗ Nein
AWS::RDS::DBInstance	✓ Ja	✓ Ja	✓ Ja
AWS::RDS::DBParameterGroup	✓ Ja	✓ Ja	✓ Ja
AWS::RDS::DBProxy	✗ Nein	✓ Ja	✗ Nein
AWS::RDS::DBProxyEndpoint	✗ Nein	✓ Ja	✗ Nein
AWS::RDS::DBProxyTargetGroup	✗ Nein	✓ Ja	✗ Nein
AWS::RDS::DBSecurityGroup	✓ Ja	✓ Ja	✓ Ja
AWS::RDS::DBSnapshot	✓ Ja	✓ Ja	✗ Nein
AWS::RDS::DBSubnetGroup	✓ Ja	✓ Ja	✓ Ja
AWS::RDS::Deployment	✗ Nein	✓ Ja	✗ Nein
AWS::RDS::EventSubscription	✓ Ja	✓ Ja	✗ Nein
AWS::RDS::OptionGroup	✓ Ja	✓ Ja	✗ Nein

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::RDS::ReservedDBInstance`	✓ Ja	✓ Ja	✗ Nein

AWS Resource Access Manager

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::RAM::ResourceShare`	✓ Ja	✓ Ja	✗ Nein

AWS Resource Groups

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::ResourceGroups::Group`	✓ Ja	✓ Ja	✓ Ja

AWS Robomaker

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::RoboMaker::DeploymentJob`	✗ Nein	✓ Ja	✗ Nein
`AWS::RoboMaker::Fleet`	✗ Nein	✓ Ja	✗ Nein
`AWS::RoboMaker::Robot`	✗ Nein	✓ Ja	✗ Nein
`AWS::RoboMaker::RobotApplication`	✓ Ja	✓ Ja	✗ Nein
`AWS::RoboMaker::SimulationApplication`	✓ Ja	✓ Ja	✗ Nein
`AWS::RoboMaker::SimulationJob`	✓ Ja	✓ Ja	✗ Nein

Amazon Route 53

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Route53::Domain`	Bol Ja1	Bol Ja2	✗ Nein
`AWS::Route53::HealthCheck`	Bol Ja1	Ja2	Bol Ja2
`AWS::Route53::HostedZone`	Bol Ja1	Bol Ja2	Ja2

1 Dies ist eine Ressource für einen globalen Service, der in der Region USA Ost (Nord-Virginia) gehostet wird. Um den Tag-Editor zum Erstellen oder Ändern von Tags für diesen Ressourcentyp zu verwenden, müssen Sie `us-east-1` in der Liste Regionen auswählen unter Zu markierende Ressourcen finden in der Tag-Editor-Konsole einfügen.

2 Dies ist eine Ressource für einen globalen Service, der in der Region USA Ost (Nord-Virginia) gehostet wird. Da Ressourcengruppen für jede Region separat verwaltet werden, müssen Sie Ihre AWS Management Console auf die umstellen AWS-Region , die die Ressourcen enthält, die Sie in die Gruppe aufnehmen möchten. Um eine Ressourcengruppe AWS Management Console zu erstellen, die eine globale -Ressource enthält, müssen Sie Ihre mit der Regionsauswahl in der oberen rechten Ecke der für USA Ost (Nord-Virginia) us-east-1 konfigurieren AWS Management Console.

Amazon Route 53 Resolver

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Route53Resolver::FirewallDomainList`	✗ Nein	Bol Ja2	✗ Nein
`AWS::Route53Resolver::FirewallRuleGroup`	✗ Nein	Bol Ja2	✗ Nein
`AWS::Route53Resolver::ResolverEndpoint`	Bol Ja1	Bol Ja2	✗ Nein
`AWS::Route53Resolver::ResolverQueryLoggingConfig`	✗ Nein	Bol Ja2	✗ Nein
`AWS::Route53Resolver::ResolverRule`	Bol Ja1	Ja2	✗ Nein

1 Dies ist eine Ressource für einen globalen Service, der in der Region USA Ost (Nord-Virginia) gehostet wird. Um den Tag-Editor zum Erstellen oder Ändern von Tags für diesen Ressourcentyp

zu verwenden, müssen Sie `us-east-1` in der Liste Regionen auswählen unter Zu markierende Ressourcen finden in der Tag-Editor-Konsole einfügen.

2 Dies ist eine Ressource für einen globalen Service, der in der Region USA Ost (Nord-Virginia) gehostet wird. Da Ressourcengruppen für jede Region separat verwaltet werden, müssen Sie Ihre AWS Management Console auf die umstellen AWS-Region , die die Ressourcen enthält, die Sie in die Gruppe aufnehmen möchten. Um eine Ressourcengruppe AWS Management Console zu erstellen, die eine globale -Ressource enthält, müssen Sie Ihre mit der Regionsauswahl in der oberen rechten Ecke der für USA Ost (Nord-Virginia) us-east-1 konfigurieren AWS Management Console.

Amazon S3 Glacier

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Glacier::Vault`	✓ Ja	✓ Ja	✗ Nein

Amazon SageMaker

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::SageMaker::AppImageConfig`	✗ Nein	✓ Ja	✗ Nein
`AWS::SageMaker::CodeRepository`	✗ Nein	✓ Ja	✗ Nein
`AWS::SageMaker::Endpoint`	✗ Nein	✓ Ja	✓ Ja

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
AWS::SageMaker::EndpointConfig	✗ Nein	✓ Ja	✓ Ja
AWS::SageMaker::HyperParameterTuningJob	✗ Nein	✓ Ja	✗ Nein
AWS::SageMaker::Image	✗ Nein	✓ Ja	✗ Nein
AWS::SageMaker::LabelingJob	✗ Nein	✓ Ja	✗ Nein
AWS::SageMaker::Model	✗ Nein	✓ Ja	✓ Ja
AWS::SageMaker::ModelPackageGroup	✗ Nein	✓ Ja	✓ Ja
AWS::SageMaker::NotebookInstance	✓ Ja	✓ Ja	✓ Ja
AWS::SageMaker::Pipeline	✗ Nein	✓ Ja	✗ Nein
AWS::SageMaker::Project	✗ Nein	✓ Ja	✓ Ja
AWS::SageMaker::TrainingJob	✗ Nein	✓ Ja	✗ Nein
AWS::SageMaker::TransformJob	✗ Nein	✓ Ja	✗ Nein
AWS::SageMaker::Workteam	✗ Nein	✓ Ja	✗ Nein

AWS Secrets Manager

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::SecretsManager::Secret`	✓ Ja	✓ Ja	✓ Ja

AWS Service Catalog

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::ServiceCatalog::CloudFormationProduct`	× Nein	✓ Ja	✓ Ja
`AWS::ServiceCatalog::Portfolio`	× Nein	✓ Ja	✓ Ja

AWS Service Catalog AppRegistry

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::ServiceCatalogAppRegistry::Application`	✗ Nein	✓ Ja	✗ Nein
`AWS::ServiceCatalogAppRegistry::AttributeGroup`	✗ Nein	✓ Ja	✗ Nein

Service Quotas

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::ServiceQuotas::Quota`	✗ Nein	✓ Ja	✗ Nein

Amazon Simple Email Service

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::SES::ConfigurationSet`	✓ Ja	✓ Ja	✓ Ja
`AWS::SES::ContactList`	✓ Ja	✓ Ja	✓ Ja
`AWS::SES::DedicatedIpPool`	✓ Ja	✓ Ja	✗ Nein
`AWS::SES::Identity`	✓ Ja	✓ Ja	✗ Nein

Amazon Simple Notification Service

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::SNS::Topic`	✓ Ja	✓ Ja	✓ Ja

Amazon Simple Queue Service

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::SQS::Queue`	✓ Ja	✓ Ja	✓ Ja

Amazon Simple Storage Service (Amazon S3)

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::S3::Bucket`	✓ Ja	✓ Ja	✓ Ja
`AWS::S3::Job`	X Nein	✓ Ja	X Nein
`AWS::S3::StorageLens`	X Nein	✓ Ja	X Nein

AWS Step Functions

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::StepFunctions::Activity`	✓ Ja	✓ Ja	✓ Ja
`AWS::StepFunctions::StateMachine`	✓ Ja	✓ Ja	✓ Ja

Storage Gateway

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::StorageGateway::Gateway`	✓ Ja	✓ Ja	X Nein
`AWS::StorageGateway::Volume`	X Nein	✓ Ja	X Nein

AWS Systems Manager

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::SSM::Association`	✗ Nein	✓ Ja	✗ Nein
`AWS::SSM::AutomationExecution`	✗ Nein	✓ Ja	✗ Nein
`AWS::SSM::Document`	✗ Nein	✓ Ja	✓ Ja
`AWS::SSM::MaintenanceWindow`	✗ Nein	✓ Ja	✗ Nein
`AWS::SSM::ManagedInstance`	✗ Nein	✓ Ja	✗ Nein
`AWS::SSM::OpsItem`	✗ Nein	✓ Ja	✗ Nein
`AWS::SSM::OpsMetadata`	✗ Nein	✓ Ja	✗ Nein
`AWS::SSM::Parameter`	✓ Ja	✓ Ja	✓ Ja
`AWS::SSM::PatchBaseline`	✗ Nein	✓ Ja	✓ Ja

AWS Systems Manager für SAP

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::SystemsManagerSAP::Application`	✗ Nein	✓ Ja	✓ Ja

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::SystemsManagerSAP::Database`	✗ Nein	✓ Ja	✗ Nein

Amazon Timestream

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Timestream::ScheduledQuery`	✗ Nein	✓ Ja	✓ Ja

AWS Transfer Family

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::Transfer::Certificate`	✗ Nein	✓ Ja	✗ Nein
`AWS::Transfer::Connector`	✗ Nein	✓ Ja	✗ Nein
`AWS::Transfer::Workflow`	✗ Nein	✓ Ja	✗ Nein

AWS WAF

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::WAF::Rule`	✗ Nein	✓ Ja	✗ Nein
`AWS::WAF::WebACL`	✗ Nein	✓ Ja	✗ Nein

Amazon WorkSpaces

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::WorkSpaces::Workspace`	✓ Ja	✓ Ja	✓ Ja

AWS X-Ray

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::XRay::Group`	✗ Nein	✓ Ja	✗ Nein

Ressourcen	Markierung des Tag-Editors	Tag-basierte Gruppen	AWS CloudFormation Stack-basierte Gruppen
`AWS::XRay::SamplingRule`	✗ Nein	✓ Ja	✗ Nein

Veraltete Ressourcentypen

Die folgenden Ressourcentypen werden für die angegebene Funktionalität nicht mehr unterstützt.

Service	Ressourcentyp	Support-Änderung	Date (Datum)
AWS RoboMaker	`AWS::RoboMaker::Robot`	Wird vom Tag-Editor nicht mehr unterstützt.	2. Mai 2022
AWS RoboMaker	`AWS::RoboMaker::Fleet`	Wird vom Tag-Editor nicht mehr unterstützt.	2. Mai 2022
AWS RoboMaker	`AWS::RoboMaker::DeploymentJob`	Wird vom Tag-Editor nicht mehr unterstützt.	2. Mai 2022

Ressourcengruppen erstellen mitAWS CloudFormation

AWS Resource Groups ist in AWS CloudFormation integriert, ein Service, der Ihnen hilft, Ihre AWS-Ressourcen zu modellieren und einzurichten, damit Sie weniger Zeit mit der Erstellung und Verwaltung Ihrer Ressourcen und Infrastruktur verbringen können. Sie erstellen eine Vorlage, in der alle gewünschtenAWS -Ressourcen (z. B. Ressourcentruppen) beschrieben werden. übernimmtAWS CloudFormation dann die Bereitstellung und Konfiguration dieser Ressourcen für Sie.

Wenn Sie verwendenAWS CloudFormation, können Sie Ihre Vorlage wiederverwenden, um Ihre Ressourcentkonsistent und wiederholt einzurichten. Beschreiben Sie Ihre Ressourcentyp einmal und stellen Sie dann die gleichen Ressourcentyp in mehrerenAWS-Konten -Konten und -Regionen immer wieder bereit.

Resource Groups undAWS CloudFormation Vorlagen

Um Ressourcen für Resource Groups und verwandte Dienstleistungen bereitzustellen und zu konfigurieren, müssen Sie AWS CloudFormation-Vorlagen kennen und verstehen. Vorlagen sind formatierte Textdateien in JSON oder YAML. Diese Vorlagen beschreiben die Ressourcen, die Sie in Ihren AWS 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 AWS CloudFormation-Vorlagen erleichtert. Weitere Informationen finden Sie unter Was ist AWS CloudFormation-Designer? im AWS CloudFormation-Benutzerhandbuch.

Resource Groups unterstützt das Erstellen von Ressourcengruppen inAWS CloudFormation. Weitere Informationen, einschließlich Beispiele für JSON- und YAML-Vorlagen für Ressourcentyp, finden Sie in der Referenz zumAWS Resource Groups Ressourcentyp im AWS CloudFormation-Benutzerhandbuch.

Weitere Informationen zu AWS CloudFormation

Weitere Informationen zu AWS CloudFormation finden Sie in den folgenden Ressourcen.

- AWS CloudFormation
- AWS CloudFormation-Benutzerhandbuch
- AWS CloudFormation API Referenz
- AWS CloudFormation-Benutzerhandbuch für die Befehlszeilenschnittstelle

Sicherheit in AWS Resource Groups

Die Sicherheit in der Cloud hat AWS höchste Priorität. Als AWS-Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die zur Erfüllung der Anforderungen von Organisationen entwickelt wurden, für die Sicherheit eine kritische Bedeutung hat.

Sicherheit gilt zwischen AWS und Ihnen eine geteilte Verantwortung. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud – AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS-Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS-Compliance-Programme regelmäßig. Weitere Informationen zu den Compliance-Programmen für AWS Resource Groups finden Sie unter Durch das Compliance-Programm abgedeckte AWS-Services.
- Sicherheit in der Cloud – Ihr Verantwortungsumfang wird durch den AWS-Service bestimmt, den 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 erläuterte, wie das Modell der geteilten Verantwortung bei der Verwendung von Resource Groups zum Tragen kommt. Die folgenden Themen veranschaulichen, wie Sie Resource Groups zur Erfüllung Ihrer Sicherheits- und Compliance-Ziele konfigurieren können. Sie erfahren außerdem, wie Sie andere verwendenAWS-Services, die Ihnen helfen, Ihre -Ressourcen zu überwachen und zu schützen.

Themen

- Datenschutz in AWS Resource Groups
- Identity and Access Management für AWS Resource Groups
- Protokollieren und Überwachen in Resource Groups
- Konformitätsprüfung für Resource Groups
- Ausfallsicherheit in Resource Groups
- Infrastruktursicherheit in Ressourcengruppen
- Bewährte Methoden für Resource Groups

Datenschutz in AWS Resource Groups

Das Modell der geteilten Verantwortung von AWS gilt für den Datenschutz in AWS Resource Groups. Wie in diesem Modell beschrieben, ist AWS verantwortlich für den Schutz der globalen Infrastruktur, in der die gesamte AWS Cloud ausgeführt wird. 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 unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS-Modell der geteilten Verantwortung und in der DSGVO im AWS-Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, AWS-Konto-Anmeldeinformationen zu schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einzurichten. 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 die Multi-Faktor Authentifizierung (MFA).
- Verwenden Sie SSL/TLS für die Kommunikation mit AWS-Ressourcen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit AWS CloudTrail ein.
- Verwenden Sie AWS-Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen in 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 für den Zugriff auf AWS über eine Befehlszeilenschnittstelle oder über eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

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 Groups oder anderen AWS-Services über die KonsoleAWS CLI, API oder AWS SDKs arbeiten. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Datenverschlüsselung

AWS Resource GroupsHat im Vergleich zu anderen AWS Diensten nur eine minimale Angriffsfläche, da es keine Möglichkeit bietet, AWS Ressourcen zu ändern, hinzuzufügen oder zu löschen, es sei denn, es handelt sich um Gruppen. Resource Groups sammelt die folgenden dienstspezifischen Informationen von Ihnen.

- Gruppennamen (nicht verschlüsselt, nicht privat)
- Gruppenbeschreibungen (nicht verschlüsselt, aber privat)
- Mitgliederressourcen in Gruppen (diese werden in Protokollen gespeichert, die nicht verschlüsselt sind)

Verschlüsselung im Ruhezustand

Es gibt keine zusätzlichen Möglichkeiten, Dienst- oder Netzwerkverkehr zu isolieren, die für Resource Groups spezifisch sind. Verwenden Sie gegebenenfalls eine AWS -spezifische Isolierung. Sie können die Resource Groups API und die Konsole in einer VPC verwenden, um den Datenschutz und die Infrastruktursicherheit zu maximieren.

Verschlüsselung während der Übertragung

AWS Resource GroupsDaten werden bei der Übertragung in die interne Datenbank des Dienstes zur Sicherung verschlüsselt. Dies ist nicht vom Benutzer konfigurierbar.

Schlüsselverwaltung

AWS Resource Groupsist derzeit nicht in integriert AWS Key Management Service und unterstützt es nichtAWS KMS keys.

Richtlinie für den Datenverkehr zwischen Netzwerken

AWS Resource Groupsverwendet HTTPS für alle Übertragungen zwischen Resource Groups Groups-Benutzern undAWS. Resource Groups verwendet Transport Layer Security (TLS) 1.2, unterstützt aber auch TLS 1.0 und 1.1.

Identity and Access Management für AWS Resource Groups

AWS Identity and Access Management (IAM) ist ein AWS-Service, mit dem ein Administrator den Zugriff auf AWS-Ressourcen sicher steuern kann. IAM-Administratoren kontrollieren, wer

authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), Ressourcen von Resource Groups zu verwenden. IAM ist ein AWS-Service, den Sie ohne zusätzliche Kosten verwenden können.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- Funktionsweise von Resource Groups mit IAM
- AWS Von verwaltete Richtlinien für AWS Resource Groups
- Verwenden von serviceverknüpften Rollen für Resource Groups
- AWS Resource GroupsBeispiele für identitätsbasierte -Richtlinien
- Fehlerbehebung für AWS Resource Groups-Identität und -Zugriff

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in Resource Groups ausführen.

Dienstbenutzer — Wenn Sie den Resource Groups Groups-Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. Da Sie für Ihre Arbeit mehr Ressourcengruppen-Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Wenn Sie in Resource Groups nicht auf eine Funktion zugreifen können, finden Sie weitere Informationen unterFehlerbehebung für AWS Resource Groups-Identität und -Zugriff.

Dienstadministrator — Wenn Sie in Ihrem Unternehmen für Resource Groups-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Resource Groups. Es ist Ihre Aufgabe, zu bestimmen, auf welche Resource Groups, Funktionen und Ressourcen Ihre Servicebenutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit Resource Groups verwenden kann, finden Sie unterFunktionsweise von Resource Groups mit IAM.

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

Authentifizierung mit Identitäten

Die Authentifizierung ist die Art und Weise, wie Sie sich mit Ihren Anmeldeinformationen bei AWS anmelden. Die Authentifizierung (Anmeldung bei AWS) muss als Root-Benutzer des AWS-Kontos, als IAM-Benutzer oder durch Übernahme einer IAM-Rolle erfolgen.

Sie können sich bei AWS als Verbundidentität mit Anmeldeinformationen anmelden, die über eine Identitätsquelle bereitgestellt werden. Benutzer von AWS IAM Identity Center. (IAM Identity Center), die Single-Sign-on-Authentifizierung Ihres Unternehmens und Anmeldeinformationen für Google oder Facebook sind Beispiele für Verbundidentitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie auf AWS mithilfe des Verbunds zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich bei der AWS Management Console oder beim AWS-Zugriffsportal anmelden. Weitere Informationen zum Anmelden bei AWS finden Sie unter Anmelden bei Ihrem AWS-Konto im Benutzerhandbuch von AWS-Anmeldung.

Bei programmgesteuerten Zugriff auf AWS bietet AWS ein Software Development Kit (SDK) und eine Command Line Interface (CLI, Befehlszeilenschnittstelle) zum kryptographischen Signieren Ihrer Anfragen mit Ihren Anmeldeinformationen. Wenn Sie keine AWS-Tools verwenden, müssen Sie Anforderungen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode zum eigenen Signieren von Anforderungen finden Sie unter Signieren von AWS-API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS empfiehlt beispielsweise die Verwendung von Multi-Factor Authentication (MFA), um die Sicherheit Ihres Kontos zu verbessern. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center-Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

AWS-Konto-Stammbenutzer

Wenn Sie ein AWS-Konto neu erstellen, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services und Ressourcen des Kontos hat. Diese Identität wird als AWS-

Konto-Root-Benutzer bezeichnet. Für den Zugriff auf den Root-Benutzer müssen Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, die zur Erstellung des Kontos verwendet wurden. 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 unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität in Ihrem AWS-Konto mit bestimmten Berechtigungen für eine einzelne Person oder eine einzelne Anwendung. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe 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 einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten 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 Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM roles (IAM-Rollen)

Eine IAM-Rolle ist eine Identität in Ihrem AWS-Konto mit spezifischen Berechtigungen. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der AWS Management Console übernehmen, indem Sie Rollen wechseln. Sie können eine Rolle annehmen, indem Sie eine AWS CLI oder AWS-API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wenn eine Verbundidentität authentifiziert wird, wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, 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 andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontenübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. In einigen AWS-Services können Sie jedoch eine Richtlinie direkt an eine Ressource anfügen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff – Einige AWS-Services verwenden Features in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon EC2 aus oder speichert Objekte in Amazon S3. Ein Service kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward access sessions (FAS) – Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle zum Ausführen von Aktionen in AWS verwenden, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen AWS-Service aufruft, in Kombination mit der Anforderung an den AWS-Service, Anforderungen an nachgelagerte Services zu stellen. FAS-Anforderungen werden nur dann gestellt, wenn ein Service eine Anforderung erhält, die Interaktionen mit anderen AWS-Services oder Ressourcen erfordert, um abgeschlossen werden zu können. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Forward Access Sessions (FAS).

- Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
- Serviceverknüpfte Rolle – Eine serviceverknüpfte Rolle ist ein Typ von Servicerolle, die mit einem AWS-Service verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem AWS-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.

- Anwendungen in Amazon EC2 – Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und AWS CLI- oder AWS-API-Anforderungen durchführen. Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Erstellen Sie ein Instance-Profil, das an die Instance angefügt ist, um eine AWS-Rolle einer EC2-Instance zuzuweisen und die Rolle für sämtliche Anwendungen der Instance bereitzustellen. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Für die Zugriffssteuerung in AWS erstellen Sie Richtlinien und weisen diese den AWS-Identitäten oder -Ressourcen zu. Eine Richtlinie ist ein Objekt in AWS, das, wenn es einer Identität oder Ressource zugeordnet wird, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anforderung stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

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

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole` -Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Benutzerinformationen über die AWS Management Console, die AWS CLI oder die AWS -API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

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 AWS-Konto anfügen können. Verwaltete Richtlinien umfassen von AWS verwaltete und von Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon 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. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS-Services umfassen.

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

Zugriffskontrolllisten (ACLs)

Zugriffskontrolllisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3, AWS WAF und Amazon VPC sind Beispiele für Services, die ACLs unterstützen. Weitere Informationen“ zu ACLs finden Sie unter Zugriffskontrollliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

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

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen 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. Ein ausdrückliches Ablehnen in einer dieser Richtlinien setzt das Zulassen außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Service-Kontrollrichtlinien (SCPs) – SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OE) in AWS Organizations angeben. AWS Organizations ist ein Service für die Gruppierung und zentrale Verwaltung mehrerer AWS-Konten Ihres Unternehmens. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. SCPs schränken Berechtigungen für Entitäten in Mitgliedskonten einschließlich des jeweiligen Root-Benutzer des AWS-Kontos ein. Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs 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 unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen dazu, wie AWS die Zulässigkeit einer Anforderung ermittelt, wenn mehrere Richtlinientypen beteiligt sind, finden Sie unter Logik für die Richtlinienauswertung im IAM-Benutzerhandbuch.

Funktionsweise von Resource Groups mit IAM

Bevor Sie IAM zum Verwalten des Zugriffs auf Resource Groups verwenden, sollten Sie verstehen, welche IAM-Funktionen für die Verwendung mit Resource Groups verfügbar sind. Einen Überblick über das Zusammenwirken von Resource Groups und anderenAWS -Services mit IAM finden Sie unter AWS-Services, die mit IAM funktionieren im IAM-Benutzerhandbuch.

Themen

- Identitätsbasierte Richtlinien
- Ressourcenbasierte Richtlinien
- Tagbasierte Autorisierung
- Resource Groups — IAM-Rollen

Identitätsbasierte Richtlinien

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Resource Groups unterstützt bestimmte Aktionen, Ressourcen und Bedingungsschlüssel. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Aktionen

Administratoren können mit AWS-JSON-Richtlinien festlegen, welche Personen zum Zugriff auf welche Ressourcen berechtigt sind. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie die zugehörige AWS-API-Operation. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. 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 in Resource Groups verwenden vor der Aktion das folgende Präfix:`resource-groups:` Tag-Editor-Aktionen werden vollständig in der Konsole ausgeführt, haben jedoch das Präfix`resource-explorer` in den Protokolleinträgen.

Um jemandem beispielsweise die Berechtigung zum Erstellen einer Resource Groups mithilfe der Resource`CreateGroup` Groups-API-Operation zu erteilen, fügen Sie die`resource-groups:CreateGroup` Aktion in seine Richtlinie ein. Richtlinienanweisungen müssen entweder ein `Action`- oder ein `NotAction`-Element enthalten. Resource Groups definiert eine eigene Gruppe von Aktionen, die Sie mit diesem Service durchführen können.

Um mehrere Resource Groups und Tagbasierte Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie folgendermaßen durch Kommas:

```
"Action": [
      "resource-groups:action1",
      "resource-groups:action2",
      "resource-explorer:action3"
```

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `List` beginnen, einschließlich der folgenden Aktion:

```
"Action": "resource-groups:List*"
```

Eine Liste der Ressourcen-Aktionen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel fürAWS Resource Groups im IAM-Benutzerhandbuch.

Ressourcen

Administratoren können mit AWS-JSON-Richtlinien festlegen, welche Personen zum Zugriff auf welche Ressourcen berechtigt sind. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein `Resource`- oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. 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": "*"
```

Die einzige Ressource für Resource Groups ist eine Gruppe. Die Gruppenressource hat einen ARN im folgenden Format:

```
arn:${Partition}:resource-groups:${Region}:${Account}:group/${GroupName}
```

Weitere Informationen zum Format von ARNs finden Sie unter Amazon-Ressourcennamen (ARNs) und AWS-Service-Namespaces.

Um beispielsweise die`my-test-group` Ressourcengruppe in Ihrer Anweisung anzugeben, verwenden Sie den folgenden ARN:

```
"Resource": "arn:aws:resource-groups:us-east-1:123456789012:group/my-test-group"
```

Um alle Gruppen anzugeben, die zu einem bestimmten Konto gehören, verwenden Sie den Platzhalter (*):

```
"Resource": "arn:aws:resource-groups:us-east-1:123456789012:group/*"
```

Einige Ressourcen-Aktionen, z. B. zum Erstellen von Ressourcen, können auf bestimmten Ressourcen nicht ausgeführt werden. In diesen Fällen müssen Sie den Platzhalter (*) verwenden.

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

Einige Ressourcen-API-Aktionen können mehrere Ressourcen umfassen. `DeleteGroup`Löscht beispielsweise Gruppen, sodass ein aufrufender Principal über die Berechtigungen zum Löschen einer bestimmten Gruppe oder aller Gruppen verfügen muss. Um mehrere Ressourcen in einer einzigen Anweisung anzugeben, trennen Sie die ARNs durch Kommata voneinander.

```
"Resource": [
  "resource1",
  "resource2"
]
```

Eine Liste der Ressourcentypen und ihrer ARNs sowie Informationen zu den Aktionen, mit denen Sie den ARN jeder Ressource angeben können, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel fürAWS Resource Groups das IAM-Benutzerhandbuch.

Bedingungsschlüssel

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. 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, wertet AWS die Bedingung mittels 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. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und servicespezifische Bedingungsschlüssel. Eine Liste aller globalen AWS-Bedingungsschlüssel finden Sie unter Globale AWS-Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Resource Groups definiert einen eigenen Satz von Bedingungsschlüsseln und unterstützt auch einige globale Bedingungsschlüssel. Eine Liste aller globalen AWS-Bedingungsschlüssel finden Sie unter Globale AWS-Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Eine Liste der Bedingungsschlüssel für Resource Groups und Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel fürAWS Resource Groups

Beispiele

Beispiele für identitätsbasierte Richtlinien für Resource Groups finden Sie unterAWS Resource GroupsBeispiele für identitätsbasierte -Richtlinien.

Ressourcenbasierte Richtlinien

Resource Groups unterstützt keine ressourcenbasierten Richtlinien.

Tagbasierte Autorisierung

Sie können Tags an Gruppen in Resource Groups anhängen oder Tags in einer Anforderung an Resource Groups übergeben. Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder `aws:TagKeys`Bedingung verwenden. Sie können einer Gruppe Tags zuweisen, wenn Sie die Gruppe erstellen oder aktualisieren. Weitere Informationen zum Taggen einer Gruppe in Resource Groups finden Sie unterErstellen von abfragebasierten Gruppen inAWS Resource Groups undGruppen aktualisieren in AWS Resource Groups in diesem Handbuch.

Ein Beispiel für eine identitätsbasierte Richtlinie zur Einschränkung des Zugriffs auf eine Ressource auf der Grundlage der Markierungen dieser Ressource finden Sie unter Tagbasierend auf Tags.

Resource Groups — IAM-Rollen

Eine IAM-Rolle ist eine Entität in Ihrem AWS-Konto mit spezifischen Berechtigungen. Resource Groups besitzt und verwendet keine Servicerollen.

Verwenden temporärer Anmeldeinformationen mit Resource Groups

In Resource Groups können Sie temporäre Anmeldeinformationen verwenden, um sich über einen Verbund anzumelden, eine IAM-Rolle anzunehmen oder eine kontenübergreifende Rolle anzunehmen. Temporäre Sicherheitsanmeldeinformationen erhalten Sie durch Aufrufen vonAWS STS -API-Vorgängen wie AssumeRoleoder GetFederationToken.

Serviceverknüpfte Rollen

Serviceverknüpfte Rollen erlauben AWS-Services den Zugriff auf Ressourcen in anderen Services, um eine Aktion in Ihrem Auftrag auszuführen.

Resource Groups haben keine serviceverknüpften Rollen und verwenden sie auch nicht.

Servicerollen

Diese Funktion ermöglicht einem Service das Annehmen einer Servicerolle in Ihrem Namen.

Resource Groups besitzt und verwendet keine Servicerollen.

AWS Von verwaltete Richtlinien für AWS Resource Groups

Eine von AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von AWS erstellt und verwaltet wird. Von AWS verwaltete Richtlinien stellen Berechtigungen für viele häufige Anwendungsfälle bereit, damit Sie beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS-verwaltete Richtlinien möglicherweise nicht die geringsten Berechtigungen für Ihre spezifischen Anwendungsfälle 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.

Die Berechtigungen, die in den von AWS verwalteten Richtlinien definiert sind, können nicht geändert werden. Wenn AWS Berechtigungen aktualisiert, die in einer von AWS verwalteten Richtlinie definiert werden, wirkt sich das Update auf alle Prinzipalidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWSaktualisiert am wahrscheinlichsten eine von AWS verwaltete Richtlinie, wenn ein neuer AWS-Service gestartet wird oder neue API-Operationen für bestehende Services verfügbar werden.

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

AWS-verwaltete Richtlinien für Ressourcengruppen

- ResourceGroupsServiceRolePolicy

AWS verwaltete Richtlinie: ResourceGroupsServiceRolePolicy

Du kannst nicht anhängen`ResourceGroupsServiceRolePolicy`an alle IAM-Entitäten selbst. Diese Richtlinie kann nur mit einer dienstverknüpften Rolle verknüpft werden, die es Ressourcengruppen ermöglicht, Aktionen in Ihrem Namen durchzuführen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Resource Groups.

Diese Richtlinie gewährt Ressourcengruppen die erforderlichen Berechtigungen, um Informationen über die Ressourcen in Ihren Ressourcengruppen und alleAWS CloudFormationStapel, zu denen diese Ressourcen gehören. Auf diese Weise können Ressourcengruppen generiert werdenCloudWatchEreignisse für die Funktion Gruppen-Lifecycle-Ereignisse.

Um die neueste Version davon zu sehenAWSverwaltete Richtlinie, siehe`ResourceGroupsServiceRolePolicy`in der IAM-Konsole.

AWSverwaltete Richtlinie: ResourceGroupsandTagEditorFullAccess

Wenn Sie einer prinzipiellen Entität eine Richtlinie zuordnen, erteilen Sie der Entität die in der Richtlinie definierten Berechtigungen.AWSMit verwalteten Richtlinien können Sie Benutzern, Gruppen und Rollen leichter die entsprechenden Berechtigungen zuweisen, als wenn Sie die Richtlinien selbst schreiben müssten.

Diese Richtlinie gewährt die Berechtigungen, die für den vollen Zugriff auf Ressourcengruppen und die Tag-Editor-Funktionen erforderlich sind.

Um die neueste Version davon zu sehenAWSverwaltete Richtlinie, siehe`ResourceGroupsandTagEditorFullAccess`in der IAM-Konsole.

Weitere Informationen zu dieser Richtlinie finden Sie unter ResourceGroupsandTagEditorFullAccessin derAWSReferenzleitfaden für verwaltete Richtlinien.

AWSverwaltete Richtlinie: ResourceGroupsandTagEditorReadOnlyZugriff

Wenn Sie einer prinzipiellen Entität eine Richtlinie zuordnen, erteilen Sie der Entität die in der Richtlinie definierten Berechtigungen.AWSMit verwalteten Richtlinien können Sie Benutzern, Gruppen und Rollen leichter die entsprechenden Berechtigungen zuweisen, als wenn Sie die Richtlinien selbst schreiben müssten.

Diese Richtlinie gewährt die Berechtigungen, die für den schreibgeschützten Zugriff auf Ressourcengruppen und die Tag-Editor-Funktionalität erforderlich sind.

Um die neueste Version davon zu sehenAWSverwaltete Richtlinie, siehe`ResourceGroupsandTagEditorReadOnlyAccess`in der IAM-Konsole.

Weitere Informationen zu dieser Richtlinie finden Sie unter ResourceGroupsandTagEditorReadOnlyZugriffin derAWSReferenzleitfaden für verwaltete Richtlinien.

Aktualisierungen der Ressourcengruppen fürAWSverwaltete Richtlinien

Details zu Updates für anzeigenAWSverwaltete Richtlinien für Ressourcengruppen, seit dieser Dienst damit begonnen hat, diese Änderungen zu verfolgen. Um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf derRessourcengruppen DokumentenverlaufSeite.

Änderung	Beschreibung	Datum
Aktualisierung der Richtlinie —ResourceGroupsandTagEditorFullAccess	Resource Groups haben eine Richtlinie aktualisiert und enthält nun weitereAWS CloudFormationberechtigungen.	10. August 2023
Aktualisierung der Richtlinie —ResourceGroupsandTagEditorReadOnlyAccess	Resource Groups haben eine Richtlinie aktualisiert und enthält nun weitereAWS CloudFormationberechtigungen.	10. August 2023
Neue Richtlinie —ResourceGroupsServiceRolePolicy	Resource Groups hat eine neue Richtlinie hinzugefügt, um ihre dienstbezogene Rolle zu unterstützen.	17. November 2022
Ressourcengruppen haben begonnen, Änderungen zu verfolgen	Ressourcengruppen haben begonnen, Änderungen für ihreAWSverwaltete Richtlinien.	17. November 2022

Verwenden von serviceverknüpften Rollen für Resource Groups

AWS Resource Groups verwendet serviceverknüpfte Rollen von AWS Identity and Access Management (IAM). Eine serviceverknüpfte Rolle ist ein spezieller Typ einer IAM-Rolle, die direkt mit Resource Groups verknüpft ist. Serviceverknüpfte Rollen werden von Resource Groups vordefiniert und schließen alle Berechtigungen ein, die der Service zum Aufrufen anderer Rollen inAWS-Services Ihrem Namen erfordert.

Eine serviceverknüpfte Rolle vereinfacht das Einrichten von Resource Groups, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Resource Groups definieren die Berechtigungen seiner serviceverknüpften Rollen und legt für jede Konfiguration Vertrauensrichtlinien fest. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter AWS-Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Yes (Ja) in der Spalte Service-linked roles (Serviceverknüpfte Rollen) angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer servicegebundenen Rolle für diesen Service anzuzeigen.

Berechtigungen von serviceverknüpften Rollen für Resource Groups

Resource Groups verwendet die folgende serviceverknüpfte Rolle zur Unterstützung von Gruppen-Lebenszyklusereignissen. Wählen Sie den Link auf dem Rollennamen, um die Rolle in der IAM-Konsole anzuzeigen, nachdem Sie sie erstellt haben.

- `AWSServiceRoleForResourceGroups`

Resource Groups verwendet die Berechtigungen in dieser Rolle, um diejenigen abzufragenAWS-Services, denen Ihre Ressourcen gehören, um die Gruppenmitgliedschaft zu klären und die Gruppe zu behalten up-to-date. Es ermöglicht Resource Groups, servicebezogene Ereignisse an den EventBridge Amazon-Service zu senden.

Die`AWSServiceRoleForResourceGroups` Rolle vertraut nur dem folgenden Service, um die Rolle zu übernehmen:

- `resourcegroups.amazonaws.com`

Die der Rolle zugewiesenen Berechtigungen stammen aus der folgendenAWS verwalteten Richtlinie. Wählen den Link im Richtliniennamen, um die Richtlinie in der IAM-Konsole zu sehen.

- AWS Von verwaltete Richtlinien für AWS Resource Groups

Erstellen der serviceverknüpften Rolle für Resource Groups

> **Important**
>
> Diese serviceverknüpfte Rolle kann in Ihrem Konto erscheinen, wenn Sie eine Aktion in einem anderen Dienst abgeschlossen haben, der die von dieser Rolle unterstützten Funktionen erfordert. Weitere Informationen finden Sie unter In meinem wird eine neue Rolle angezeigtAWS-Konto.

Um die serviceverknüpfte Rolle zu erstellen, aktivieren der Funktion Gruppen-Lebenszyklusereignisse.

Bearbeiten einer serviceverknüpften Rolle für Resource Groups

In Resource Groups können die AWSServiceRoleForResourceGroups serviceverknüpften Rolle nicht bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach der Erstellung einer serviceverknüpften Rolle nicht bearbeitet werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Resource Groups

Sie können die serviceverknüpften Rolle erst löschen, nachdem Sie die Funktion „Gruppen-Lebenszyklussereignisse“ deaktiviert haben.

> **Important**
>
> - AWSverhindert, dass Sie die serviceverknüpfte Rolle entfernen, bis Sie die Funktion für Gruppen-Lebenszyklusereignisse, mit der sie erstellt wurde, zum ersten Mal deaktiviert haben.
> - Wir empfehlen, dass Sie die dienstverknüpfte Rolle nicht löschen, solange Sie über Ressourcengruppen in Ihrer Rolle verfügenAWS-Konto. Der Resource Groups Groups-Dienst kann nicht mit anderen interagierenAWS-Services, um Ihre Gruppen zu verwalten, wenn Sie diese Rolle löschen.

Manuelles Löschen der -serviceverknüpften Rolle

Verwenden Sie die IAM-Konsole, AWS CLI- oder AWS-API, um die AWSServiceRoleForResourceGroups serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Console

So löschen Sie die serviceverknüpfte Rolle Resource Groups

1. Öffnen Sie die IAM-Konsole, um die Seite Rollen zu öffnen.
2. Suchen Sie die benannte AWSServiceRoleForResourceGroups Rolle und aktivieren Sie das Kontrollkästchen neben der Rolle.
3. Wählen Sie Löschen.
4. Bestätigen Sie Ihre Absicht, die Rolle zu löschen, indem Sie den Namen der Rolle in das Feld eingeben und dann Löschen wählen.

Die Rolle wird aus der Liste der Rollen in der IAM-Konsole gelöscht.

AWS CLI

So löschen Sie die serviceverknüpfte Rolle Resource Groups

Geben Sie zum Löschen der Rolle den folgenden Befehl mit den Parametern genau der jeweiligen Konfiguration ein. Ersetzen keinen der Werte.

```
$ aws iam delete-service-linked-role \
    --role-name AWSServiceRoleForResourceGroups
{
    "DeletionTaskId": "task/aws-service-role/resource-groups.amazonaws.com/
AWSServiceRoleForResourceGroups/34e58943-e9a5-4220-9856-fc565EXAMPLE"
}
```

Der Befehl gibt eine Aufgaben-ID zurück. Das eigentliche Löschen der Rolle erfolgt asynchron. Sie können den Status der Löschen der Rolle überprüfen, indem Sie an den folgendenAWS CLI Befehl übergeben.

```
$ aws iam get-service-linked-role-deletion-status \
    --deletion-task-id "task/aws-service-role/resource-groups.amazonaws.com/
AWSServiceRoleForResourceGroups/34e58943-e9a5-4220-9856-fc565EXAMPLE"
{
```

```
    "Status": "SUCCEEDED"
}
```

Unterstützte Regionen für Resource Groups serviceverknüpften Rollen

Resource Groups unterstützt die Verwendung von serviceverknüpften Rollen in allen Umgebungen, inAWS-Regionen denen der Service verfügbar ist. Weitere Informationen finden Sie unter AWSRegionen und Endpunkte.

AWS Resource GroupsBeispiele für identitätsbasierte -Richtlinien

IAM-Prinzipale wie Rollen und -Benutzer besitzen keine Berechtigungen zum Erstellen oder Ändern von Resource Groups Groups-Ressourcen. Sie können auch keine Aufgaben ausführen, die die AWS Management Console-, AWS CLI- oder AWS-API benutzen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die den -Benutzern die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Der Administrator muss diese Richtlinien anschließend den -Benutzern anfügen, die diese Berechtigungen benötigen.

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 Groups Groups-Konsole und der API
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer
- Tagbasierend auf Tags

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Resource Groups Group-Ressourcen in Ihrem Konto erstellen, aufrufen 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.
- Multi-Faktor-Authentifizierung (MFA) — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Stammbenutzer in Ihrem Konto erfordertAWS-Konto, 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 Groups Groups-Konsole und der API

Um auf die KonsoleAWS Resource Groups und die API des and Tag Editors zugreifen zu können, müssen Sie über einen Mindestsatz von Berechtigungen verfügen. Diese Berechtigungen müssen Ihnen das Auflisten und der Ressourcen von Resource Groups in IhremAWS Konto gestatten. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktionieren die Konsole- und API-Befehle nicht wie vorgesehen für Prinzipale (IAM-Rollen oder -Benutzer) mit dieser Richtlinie.

Um sicherzustellen, dass diese Entitäten dennoch Resource Groups verwenden können, fügen Sie den Entitäten die folgende Richtlinie (oder eine Richtlinie, die die in der folgenden Richtlinie ist) an die Entitäten an. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "resource-groups:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "tag:GetResources",
        "tag:TagResources",
        "tag:UntagResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-explorer:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

Weitere Informationen zum Zugriff auf Resource Groups finden Sie unterErteilen von Berechtigungen für die Verwendung von AWS Resource Groups und Tag Editor in dieser Anleitung.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

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": "*"
        }
    ]
}
```

Tagbasierend auf Tags

Sie können Bedingungen in Ihrer identitätsbasierten Richtlinie verwenden, um den Zugriff auf Ressourcen von Resource Groups zu steuern. In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen können, die das Anzeigen einer Ressource erlaubt, in diesem Beispiel einer Ressourcengruppe. Die Erlaubnis wird jedoch nur erteilt, wenn das Gruppen-Tag den gleichen Wert`project` hat wie das`project` Tag, das an den aufrufenden Principal angehängt ist.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "resource-groups:ListGroups",
            "Resource": "arn:aws:resource-groups::region:account_ID:group/group_name"
        },
        {
            "Effect": "Allow",
            "Action": "resource-groups:ListGroups",
            "Resource": "arn:aws:resource-groups::region:account_ID:group/group_name",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/project": "${aws:PrincipalTag/
project}"}
            }
        }
    ]
}
```

Sie können diese Richtlinie den -Tags in Ihrem Konto zuweisen. Wenn ein Principal mit dem Tag-Schlüssel`project` und dem Tag-Wert`alpha` versucht, eine Ressourcengruppe anzuzeigen, muss die Gruppe ebenfalls mit einem Tag versehen werden`project=alpha`. Andernfalls wird dem Benutzer der Zugriff verweigert. Der Tag-Schlüssel `project` der Bedingung stimmt sowohl mit `Project` als auch mit `project` überein, da die Namen von Bedingungsschlüsseln nicht zwischen Groß- und Kleinschreibung unterscheiden. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

Fehlerbehebung für AWS Resource Groups-Identität und -Zugriff

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die beim Arbeiten mit Resource Groups und IAM auftreten können.

Themen

- Ich bin nicht autorisiert, eine Aktion in Resource Groups auszuführen
- Ich bin nicht zur Ausführung von iam autorisiert:PassRole
- Ich möchte Personen außerhalb meinesAWS -Kontos Zugriff auf meine Resource Groups erteilen

Ich bin nicht autorisiert, eine Aktion in Resource Groups auszuführen

Wenn die AWS Management Console Ihnen mitteilt, dass Sie nicht zur Ausführung einer Aktion autorisiert sind, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator ist die Person, die Ihnen Ihre Anmeldeinformationen bereitgestellt hat.

Der folgende Beispielfehler tritt auf, wenn der -Benutzer`mateojackson` versucht, die Konsole zum Anzeigen von Details zu einer Gruppe zu verwenden, jedoch nicht über`resource-groups:ListGroups` -Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
 perform: resource-groups:ListGroups on resource: arn:aws:resource-groups::us-
west-2:123456789012:group/my-test-group
```

In diesem Fall bittet Mateo seinen Administrator um die Aktualisierung seiner Richtlinien, um unter Verwendung der Aktion `my-test-group` auf die Ressource `resource-groups:ListGroups` zugreifen zu können.

Ich bin nicht zur Ausführung von iam autorisiert:PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zur Ausführung der`iam:PassRole` Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Resource Groups übergeben können.

Einige AWS-Services erlauben die Übergabe einer vorhandenen Rolle an diesen Service, sodass keine neue Servicerolle oder serviceverknüpfte Rolle erstellt werden muss. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Service.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen`marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Resource Groups auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenden Sie sich an Ihren AWS-Administrator, falls Sie weitere Unterstützung benötigen. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen odzur Verfügung gestellt.

Ich möchte Personen außerhalb meinesAWS -Kontos Zugriff auf meine Resource Groups erteilen

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 Services, 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 dazu, ob Resource Groups diese Funktionen unterstützt, finden Sie unterFunktionsweise von Resource Groups mit IAM.
- Informationen zum Gewähren des Zugriffs auf Ihre Ressourcen für alle Ihre AWS-Konten finden Sie unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen Ihrer AWS-Konto im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie AWS-Konten-Drittanbieter Zugriff auf Ihre Ressourcen bereitstellen, finden Sie unter Gewähren des Zugriffs auf AWS-Konten von externen Benutzern im IAM-Benutzerhandbuch.
- 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 kontenübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

Protokollieren und Überwachen in Resource Groups

AlleAWS Resource Groups Aktionen sind angemeldetAWS CloudTrail.

Protokollierung von AWS Resource Groups-API-Aufrufen mit AWS CloudTrail

AWS Resource Groupsund Tag Editor sind in integriertAWS CloudTrail, einen Service, der eine Aufzeichnung der Aktionen eines Benutzers, einer Rolle oder einesAWS -Services in Resource Groups oder im Tag Editor bereitstellt. CloudTrail erfasst alle API-Aufrufe für Resource Groups als Ereignisse, einschließlich Aufrufen aus der Resource Groups- oder Tag Editor-Konsole und von Code-Aufrufen an die Resource Groups Group-APIs. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket, einschließlich Ereignissen für Resource Groups aktivieren. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail -Konsole trotzdem in Event history (Ereignisverlauf) anzeigen. Mit den von CloudTrail gesammelten Informationen können Sie die an Resource Groups gestellte Anfrage, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen.

Weitere Informationen CloudTrail finden Sie im AWS CloudTrailBenutzerhandbuch.

Informationen zu Resource Groups in CloudTrail

CloudTrail wird beim Erstellen IhresAWS -Kontos für Sie aktiviert. Wenn Aktivität in Resource Groups oder in der Tag Editor-Konsole auftritt, wird diese Aktivität in einem CloudTrail Ereignis zusammen mit anderenAWS -Service-Ereignissen im Ereignisverlauf aufgezeichnet. Sie können die neusten Ereignisse in Ihr AWS-Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail -Ereignisverlauf.

Erstellen Sie für eine fortlaufende Aufzeichnung der Ereignisse in IhremAWS -Konto, darunter Ereignisse für Resource Groups, einen Trail. Ein Trail ermöglicht CloudTrail die Bereitstellung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser standardmäßig für alle 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 AWS-Services konfigurieren, um die in den CloudTrail-Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie unter:

- Übersicht zum Erstellen eines Trails

- Von CloudTrail unterstützte Services und Integrationen
- Konfigurieren von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien aus mehreren Konten

Alle Aktionen von Resource Groups werden von der -API-Referenz protokolliert CloudTrail und sind in dieser AWS Resource Groups-API-Referenz dokumentiert. Aktionen in Resource Groups CloudTrail werden als Ereignisse mit dem API-Endpunkt`resource-groups.amazonaws.com` als Quelle angezeigt. Beispielsweise generieren Aufrufe der`UpdateGroupQuery` Aktionen`CreateGroup`, `GetGroup`, und und Einträge in den CloudTrail Protokolldateien. Tag-Editor-Aktionen in der Konsole werden von CloudTrail protokolliert und als Ereignisse mit dem internen API-Endpunkt`resource-explorer` als Quelle angezeigt.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Gibt an, ob die Anfrage mit Root- oder IAM-Benutzer-Anmeldeinformationen ausgeführt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen verbundenen Benutzer gesendet wurde.
- Gibt an, ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen hierzu finden Sie unter dem CloudTrail-Element `userIdentity`.

Grundlagen zu -Protokolldateieinträgen für Resource Groups

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 nicht in einer bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen CloudTrail -Protokolleintrag, der die Aktion demonstriert`CreateGroup`.

```
{"eventVersion":"1.05",
"userIdentity":{
    "type":"AssumedRole",
```

```
    "principalId":"ID number:AWSResourceGroupsUser",
    "arn":"arn:aws:sts::831000000000:assumed-role/Admin/AWSResourceGroupsUser",
    "accountId":"831000000000","accessKeyId":"ID number",
    "sessionContext":{
        "attributes":{
            "mfaAuthenticated":"false",
            "creationDate":"2018-06-05T22:03:47Z"
            },
        "sessionIssuer":{
            "type":"Role",
            "principalId":"ID number",
            "arn":"arn:aws:iam::831000000000:role/Admin",
            "accountId":"831000000000",
            "userName":"Admin"
            }
        }
    },
"eventTime":"2018-06-05T22:18:23Z",
"eventSource":"resource-groups.amazonaws.com",
"eventName":"CreateGroup",
"awsRegion":"us-west-2",
"sourceIPAddress":"100.25.190.51",
"userAgent":"console.amazonaws.com",
"requestParameters":{
    "Description": "EC2 instances that we are using for application staging.",
    "Name": "Staging",
    "ResourceQuery": {
      "Query": "string",
      "Type": "TAG_FILTERS_1_0"
      },
    "Tags": {
      "Key":"Phase",
      "Value":"Stage"
      }
    },
"responseElements":{
    "Group": {
      "Description":"EC2 instances that we are using for application staging.",
      "groupArn":"arn:aws:resource-groups:us-west-2:831000000000:group/Staging",
      "Name":"Staging"
     },
    "resourceQuery": {
      "Query":"string",
      "Type":"TAG_FILTERS_1_0"
```

```
    }
   },
"requestID":"de7z64z9-d394-12ug-8081-7zz0386fbcb6",
"eventID":"8z7z18dz-6z90-47bz-87cf-e8346428zzz3",
"eventType":"AwsApiCall",
"recipientAccountId":"831000000000"
}
```

Konformitätsprüfung für Resource Groups

Informationen darüber, ob ein AWS-Service in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter AWS-Services in Geltungsbereich nach Compliance-Programm. Wählen Sie das Compliance-Programm, das Sie interessiert. Allgemeine Informationen finden Sie unter AWS-Compliance-Programme.

Sie können Auditberichte von Drittanbietern unter AWS Artifact herunterladen. Weitere Informationen finden Sie unter Berichte herunterladen in AWS Artifact.

Ihre Compliance-Verantwortung bei der Verwendung von AWS-Services ist von der Sensibilität Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften abhängig. AWS stellt die folgenden Ressourcen zur Unterstützung der Compliance bereit:

- Kurzanleitungen für Sicherheit und Compliance – In diesen Bereitstellungsleitfäden werden Überlegungen zur Architektur erörtert und Schritte zum Bereitstellen von Basisumgebungen auf AWS zur Verfügung gestellt, die auf Sicherheit und Compliance ausgerichtet sind.
- Erstellung einer Architektur mit HIPAA-konformer Sicherheit und Compliance in Amazon Web Services – In diesem Whitepaper wird beschrieben, wie Unternehmen mithilfe von AWS HIPAA-berechtigte Anwendungen erstellen können.

  > **Note**
  >
  > Nicht alle AWS-Services sind HIPAA-berechtigt. 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.
- AWS-Compliance-Leitfäden für Kunden – Verstehen Sie das Modell der geteilten Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten

Methoden zum Schutz von AWS-Services zusammengefasst und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.

- Auswertung von Ressourcen mit Regeln im AWS ConfigEntwicklerhandbuch – Der AWS Config-Service bewertet, wie gut Ihre Ressourcenkonfigurationen mit internen Praktiken, Branchenrichtlinien und Vorschriften übereinstimmen.
- AWS Security Hub – Dieser AWS-Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus innerhalb von AWS. Security Hub verwendet Sicherheitskontrollen, um Ihre AWS-Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- AWS Audit Manager – Dieser AWS-Service hilft Ihnen, Ihre AWS-Nutzung kontinuierlich zu überprüfen, um den Umgang mit Risiken und die Compliance von Branchenstandards zu vereinfachen.

Ausfallsicherheit in Resource Groups

AWS Resource Groupsführt automatisierte Backups für interne Serviceressourcen durch. Diese Backups sind nicht vom Benutzer konfigurierbar. Sicherungen werden sowohl im Ruhezustand als auch während der Übertragung verschlüsselt. Resource Groups speichert Kundendaten in Amazon DynamoDB.

Die globale AWS-Infrastruktur ist um AWS-Regionen und Availability Zones herum aufgebaut. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die mit einem Netzwerk mit geringer Latenz, hohem Durchsatz und hoher Redundanz verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Selbst ein vollständiger Verlust von Benutzerressourcengruppen würde nicht zu einem Verlust von Kundendaten führen, da die meisten Kundendaten überAWSAvailability Zones (AZs). Wenn Sie Gruppen versehentlich löschen, wenden Sie sich anAWS Supportzentrumaus.

Weitere Informationen über AWS-Regionen und Availability Zones finden Sie unter Globale AWS-Infrastruktur.

Infrastruktursicherheit in Ressourcengruppen

Es gibt keine zusätzlichen Möglichkeiten, den von Ressourcengruppen bereitgestellten Dienst- oder Netzwerkverkehr zu isolieren. Verwenden Sie gegebenenfalls AWS -specific isolation. Sie können die Resource Groups API und die Konsole in einer VPC verwenden, um die Datenschutz- und Infrastruktursicherheit zu maximieren.

Als verwalteter Dienst AWS Resource Groups ist er durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS-Sicherheitsdiensten und wie AWS die Infrastruktur schützt, finden Sie unter AWSCloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS-Umgebung anhand der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz im Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Ressourcengruppen zuzugreifen. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Resource Groups unterstützt keine ressourcenbasierten Richtlinien.

Bewährte Methoden für Resource Groups

Die folgenden bewährten Methoden sind allgemeine Richtlinien und keine vollständige Sicherheitslösung. Da diese bewährten Methoden für Ihre Umgebung möglicherweise nicht angemessen oder ausreichend sind, sollten Sie sie als hilfreiche Überlegungen und nicht als bindend ansehen.

- Verwenden Sie das Prinzip der geringsten Rechte, um Gruppen Zugriff zu gewähren. Resource Groups unterstützt auch Berechtigungen auf Ressourcenebene. Gewähren Sie bestimmten Gruppen nur dann Zugriff, wenn dies für bestimmte Benutzer erforderlich ist. Vermeiden Sie die

Verwendung von Sternchen in Richtlinienerklärungen, die allen Benutzern oder allen Gruppen Berechtigungen zuweisen. Weitere Informationen zu Least Privilege finden Sie unter Grant Least Privilege im IAM-Benutzerhandbuch.

- Halten Sie private Informationen von öffentlichen Bereichen fern. Der Name einer Gruppe wird als Dienstmetadaten behandelt. Gruppennamen sind nicht verschlüsselt. Geben Sie keine vertraulichen Informationen in Gruppennamen ein. Gruppenbeschreibungen sind privat.

  Geben Sie keine privaten oder vertraulichen Informationen in Tag-Schlüsseln oder Tag-Werten ein.
- Verwenden Sie bei Bedarf eine Autorisierung, die auf Tagging basiert. Resource Groups unterstützt die Autorisierung auf Basis von Tags. Sie können Gruppen taggen und dann die an Ihre IAM-Prinzipale angehängten Richtlinien wie Benutzer und Rollen aktualisieren, um deren Zugriffsebene auf der Grundlage der Tags festzulegen, die auf eine Gruppe angewendet werden. Weitere Informationen zur Verwendung der Autorisierung auf der Grundlage von Tags finden Sie im IAM-Benutzerhandbuch unter Steuern des Zugriffs aufAWS Ressourcen mithilfe von Ressourcen-Tags.

  VieleAWS Services unterstützen die Autorisierung auf Basis von Tags für ihre Ressourcen. Beachten Sie, dass die tagbasierte Autorisierung möglicherweise für Mitgliederressourcen in einer Gruppe konfiguriert ist. Wenn der Zugriff auf die Ressourcen einer Gruppe durch Tags eingeschränkt ist, können nicht autorisierte Benutzer oder Gruppen möglicherweise keine Aktionen oder Automatisierungen für diese Ressourcen ausführen. Wenn beispielsweise eine Amazon EC2 EC2-Instance in einer Ihrer Gruppen mit einem Tag-Schlüssel von`Confidentiality` und einem Tag-Wert von gekennzeichnet ist und Sie nicht berechtigt sind`High`, Befehle für markierte Ressourcen auszuführen`Confidentiality:High`, schlagen Aktionen oder Automatisierungen, die Sie auf der EC2-Instance ausführen, fehl, selbst wenn Aktionen für andere Ressourcen in der Ressourcengruppe erfolgreich sind. Weitere Informationen darüber, welche Dienste die tagbasierte Autorisierung für ihre Ressourcen unterstützen, finden Sie im IAM-Benutzerhandbuch unterAWS Services That Work with IAM.

  Weitere Informationen zur Entwicklung einer Tagging-Strategie für IhreAWS Ressourcen finden Sie unter AWSTagging-Strategien.

Service-Kontingente für Ressourcengruppen

In der folgenden Tabelle werden die Grenzwerte innerhalb von AWS Resource Groups (Ressourcengruppen) beschrieben. Sie können eine Erhöhung einiger dieser Limits beantragen. Um eine Erhöhung des Limits zu beantragen, rufen Sie die Service Quotas-Konsole auf. Informationen zu Limits, die geändert werden können, finden Sie unter Service Quotas.

> **Note**
>
> Die folgenden Definitionen gelten für die Beschreibung in den folgenden Kontingenten:
>
> - Ressourcengruppe – Eine Sammlung von AWS Ressourcen, die sich alle im selben befinden AWS-Regionund den in der Abfrage der Gruppe angegebenen Kriterien entsprechen.

Ressource	Standardlimit
Maximale Anzahl von Ressourcengruppen pro AWS-Konto und AWS-Region	100

AWS Resource Groups-Referenz

In den Themen in diesem Abschnitt finden Sie Referenzinformationen zu verschiedenen Aspekten von. AWS Resource Groups

Service-Kontingente für Ressourcengruppen

Name	Standard	Anpas	Beschreibung
Ressourcengruppen pro Konto	Jede unterstützte Region: 100	Yes (Ja)	Die maximale Anzahl der Ressourcengruppen, die Sie in diesem Konto erstellen können. Eine Ressourcengruppe ist eine Sammlung von AWS-Ressourcen, die bestimmten Kriterien entsprechen.

> **Note**
>
> Sie können Änderungen an Kontingenten, die als anpassbar gekennzeichnet sind, über die AWS Resource GroupsSeite in der Servicekontingenten-Konsole anfordern.

Von AWS verwaltete Richtlinien zur Nutzung mit AWS Resource Groups

AWS-verwaltete IAM-Berechtigungsrichtlinien ermöglichen es Ihnen, den IAM-Prinzipalen, wie Rollen und Benutzern, in Ihrem Konto vorkonfigurierte Berechtigungen zu gewähren. AWSverwaltete Richtlinien werden getestet und entsprechen den Empfehlungen bewährter Verfahren, sodass Sie sie zuverlässig in den Szenarien verwenden können, für die sie definiert wurden. Da neue Ressourcentypen als Mitglieder von Ressourcengruppen unterstützt werden und neue Ressourcentypen Tagging unterstützen, AWS werden diese Richtlinien automatisch aktualisiert, um sie zu unterstützen. Es sind keine Schritte erforderlich.

In der folgenden Tabelle sind die AWS -verwalteten IAM-Berechtigungsrichtlinien aufgeführt, mit denen Sie Berechtigungen erteilen können. AWS Resource Groups

Richtlinienname und ARN	Beschreibung
AWSResourceGroupsReadOnlyAccess `arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess`	Gewährt schreibgeschützten Zugriff auf die AWS Resource Groups Managementkonsole. Es beinhaltet die Berechtigung, die Details einer Ressource, einschließlich der Liste der angehängten Tags, anzuzeigen. Diese Richtlinie gewährt keine Erlaubnis, Änderungen an Ressourcengruppen oder Tags vorzunehmen.
ResourceGroupsandTagEditorReadOnlyAccess `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess`	Gewährt schreibgeschützten Zugriff auf die AWS Resource Groups Managementkonsole, einschließlich des Tag-Editors. Es beinhaltet die Berechtigung, die Details einer Ressource, einschließlich ihrer Tags, anzuzeigen. Sie können den Tag-Editor verwenden, um Ressourcen anzuzeigen, die Tag-Abfragen entsprechen. Diese Richtlinie gewährt keine Erlaubnis, Änderungen an Ressourcengruppen oder Tags vorzunehmen.
ResourceGroupsandTagEditorFullAccess `arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess`	Gewährt vollen Administratorzugriff auf die AWS Resource Groups Managementkonsole. Es umfasst Berechtigungen zum Anzeigen, Erstellen und Ändern von Ressourcengruppen. Es umfasst auch Berechtigungen zum Anzeigen, Festlegen und Ändern von Tags für alle Ressourcen, die vom Tag Editor unterstützt werden.

Dokumentverlauf für AWS Resource Groups

Änderung	Beschreibung	Datum
AktualisiertAWSverwaltete Richtlinien ResourceGroupsandTagEditorFullAccess und ResourceGroupsandTagEditorReadOnlyZugriff	Ressourcengruppen haben zwei aktualisiertAWSverwaltete Richtlinien zum Hinzufügen zusätzlicherAWS CloudFormationBerechtigungen.	10. August 2023
Servicekontingente für Ressourcengruppen	Mithilfe von Servicekontingenten können Sie jetzt die Kontingentlimits für Ressourcengruppen einsehen.	29. Juni 2023
Aktualisierung der bewährten IAM-Praktiken	Aktualisierter Leitfaden, angepasst an die bewährten IAM-Methoden. Weitere Informationen finden Sie unter Bewährte IAM-Methoden.	3. Januar 2023
Die Informationen zum Tag-Editor wurden in ein eigenes Handbuch verschoben	Die Dokumentation für den Tag Editor wurde aus diesem Handbuch entfernt und in das neue Tag Editor-Benutzerhandbuch verschoben.	13. Dezember 2022
Ressourcengruppen können jetzt Ressourcen von Amazon Keyspaces (für Apache Cassandra) enthalten	AWS Resource Groupsunterstützt jetzt die Aufnahme von Ressourcen für Amazon Keyspaces (für Apache Cassandra) in eine Ressourcengruppe.	20. Oktober 2022
Veraltete Verwendung von Ressourcentypen	Die folgenden Ressourcentypen werden vom Tag	17. Mai 2022

	Editor nicht mehr unterstützt:`AWS::RoboMaker::Robot` ,`AWS::RoboMaker::Fleet` , und`AWS::RoboMaker::DeploymentJob` .	
neuAWSverwaltete Richtlinie - ResourceGroupsServiceRolePolicy	Resource Groups hat eine neue hinzugefügtAWSverwaltete Richtlinie inAWS Identity and Access Management(IAM), um die servicebezogene Rolle des Dienstes zu unterstützen.	12. Januar 2022
Ereignisse im Lebenszyklus gruppieren	Ressourcengruppen können jetzt Ereignisse in Amazon generierenCloudWatchEreignisse, die Sie benachrichtigen, wenn Änderungen an Ihren Ressourcengruppen vorgenommen werden.	12. Januar 2022
Ressourcengruppen können jetzt von Amazon VPC Network Access Analyzer verwendet werden, um unerwünschten Netzwerkverkehr zu IhremAWSRessourcen.	Du kannst benutzenAWS Resource Groupsum die Quellen und Ziele für Ihre Netzwerkzugriffsanforderungen anzugeben.	3. Dezember 2021
Unterstützung für Ressourcen von hinzugefügtAWSZentrum für Resilienz	AWS Resource Groupsunterstützt jetzt das Einbinden von Ressourcen fürAWSResilience Hub in einer Ressourcengruppe.	18. November 2021

Unterstützung für Ressourcen von Amazon Pinpoint hinzugefügt	AWS Resource Groupsunt erstützt jetzt die Aufnahme von Ressourcen für Amazon Pinpoint in eine Ressourcengruppe.	11. November 2021
Unterstützung für Ressourcengruppen hinzugefügt, die konfiguriert und verwaltet werden vonAppRegistry	AWS Resource Groupsunt erstützt jetzt Ressourcengruppen, die Dienstkonfigurationen für Ressourcen in Anwendungen enthalten, die Sie mithilfe vonAWS Service Catalog AppRegistry. Weitere Informationen finden Sie unterDienstkonfigurationeninderAWS Resource GroupsAPI-Referenz.	15. September 2021
Unterstützung für Ressourcen von Amazon hinzugefügtOpenSearchBedienung	AWS Resource Groupsunt erstützt jetzt das Einbinden von Ressourcen für AmazonOpenSearchDienst in einer Ressourcengruppe.	11. August 2021
Unterstützung für Ressourcen von hinzugefügtAWSKlammer	AWS Resource Groupsunt erstützt jetzt das Einbinden von Ressourcen fürAWSKlammer in einer Ressourcengruppe.	30. Juni 2021
Unterstützung für Ressourcen von Amazon EMR Containers hinzugefügt	AWS Resource Groupsunt erstützt jetzt die Aufnahme von Ressourcen für Amazon EMR-Container in eine Ressourcengruppe.	27. April 2021

Unterstützung für zusätzliche Ressourcen hinzugefügtAWSDienstleistungen	AWS Resource Groupsunterstützt jetzt die Aufnahme von Ressourcen für die folgenden Dienste in eine Ressourcengruppe: AmazonCodeGuruReviewer, Amazon Elastic Inference, Amazon Forecast, Amazon Fraud Detector und Servicekontingente.	25. Februar 2021
Kapitel über Sicherheit und Compliance hinzugefügt.	Erläutert, wie Resource Groups Ihre Informationen schützt und die gesetzlichen Standards einhält.	30. Juli 2020

Unterstützung für Ressourcengruppen hinzugefügt, die konfiguriert sind fürAWSDienstleistungen	Sie können jetzt Ressourcengruppen erstellen, die mit einem verknüpft sindAWSDienst und die konfigurieren, wie der Dienst mit den Ressourcen interagieren kann, die sich in der Gruppe befinden. In dieser ersten Version der Funktion können Sie eine Ressourcengruppe erstellen, die Amazon EC2-Kapazitätsreservierungen enthält, und dann Amazon EC2-Instances in der Gruppe starten. Wenn in einer oder mehreren Reservierungen der Gruppe Kapazität vorhanden ist, die Ihrer Instance entspricht, verwendet diese Instance die Reservierung. Wenn die Instance keinen verfügbaren Reservierungen in der Gruppe entspricht, wird sie als On-Demand-Instance gestartet. Weitere Informationen finden Sie unterArbeiten mit Kapazitätsreservierungsgruppenin derAmazon EC2-Benutzerhandbuch für Linux-Instances.	29. Juli 2020
Unterstützung hinzugefügt fürAWS IoT GreengrassRessourcen.	Weitere Ressourcentypen werden jetzt unterstützt vonAWS Resource Groupsund Tag-Editor.	25. März 2020

Betriebsdaten anzeigen fürAWS Resource Groups	In derAWS Systems ManagerKonsole, dieAWS Resource GroupsDie Seite zeigt Betriebsdaten für eine ausgewählte Gruppe auf vier Tabs an:Einzelheiten,Konfiguration,CloudTrail,OpsItems. Diese Registerkarten sind nicht verfügbar, wenn eine Gruppe in der Resource Group-Konsole angezeigt wird. Mithilfe der Informationen auf diesen Registerkarten können Sie ermitteln, welche Ressourcen in einer Gruppe konform sind und für welche Ressourcen Handlungsbedarf besteht. Wenn Sie Maßnahmen für eine Ressource ergreifen müssen, können Sie Systems Manager-Automatisierungs-Runbooks verwenden, um allgemeine Aufgaben zur Wartung und Problembehandlung durchzuführen. Weitere Informationen finden Sie unterBetriebsdaten anzeigen fürAWS Resource Groupsin derAWS Systems ManagerBenutzerleitfaden.	16. März 2020

Überprüfen Sie, ob die Tag-Richtlinien eingehalten werden	Nachdem Sie Tag-Richtlinien erstellt und an Konten angehängt haben, verwenden SieAWS Organizations, können Sie in den Konten Ihrer Organisation nach nicht konformen Tags auf Ressourcen suchen.	26. November 2019
Unterstützung für mehr Ressourcentypen	Weitere Ressourcentypen werden jetzt unterstützt vonAWS Resource Groupsund Tag-Editor.	4. Oktober 2019
Neue Ressourcentypen, unterstützt vonAWS Resource Groups	Weitere Ressourcentypen werden jetzt unterstützt vonAWS Resource Groups, insbesondere für Gruppen, die auf einemAWS CloudFormationstapeln.	5. August 2019
Neue Ressourcentypen, unterstützt vonAWS Resource Groups	Amazon API-Gateway-REST-APIs, AmazonCloudWatchEreignisse, Ereignisse und Amazon SNS-Themen sind jetzt unterstützte Ressourcentypen inAWS Resource Groups.	27. Juni 2019
Der Tag Editor unterstützt jetzt die Suche nach Ressourcen ohne Tags	Sie können jetzt im Tag Editor nach Ressourcen suchen, denen keine Tag-Werte für einen bestimmten Tag-Schlüssel zugewiesen wurden.	18. Juni 2019

Neue Ressourcentypen, unterstützt vonAWS Resource Groupsund Tag-Editor	Über 50 neue Ressource ntypen wurden hinzugefü gtAWS Resource Groupsund Tag-Editor-Unterstützung.	6. Juni 2019
AWS Resource Groupsund die Tag Editor-Konsole wechselt ausAWS Systems ManagerKo nsole	DerAWS Resource Groupsund die Tag Editor-Konsole ist jetzt unabhängig von der Systems Manager-Konsole. Sie können zwar immer noch Hinweise auf die findenAWS Resource GroupsKonsole In der linken Navigationsleiste von Systems Manager können Sie die Resource Groups und Tag Editor-Konsole direkt über das Drop-down-Menü oben links imAWS Management Console.	5. Juni 2019
Neue Funktionen zur Autorisie rung und Zugriffskontrolle für Ressourcengruppen	Resource Groups unterstützen jetzt auf Aktionen basierend e Richtlinien, Berechtig ungen auf Ressourcenebene und Autorisierung auf der Grundlage von Tags.	24. Mai 2019
Ältere, veraltete Tools für Ressourcengruppen und Tag Editor sind nicht mehr verfügbar	Erwähnungen älterer, klassischer oder veralteter Ressourcengruppen und des Tag-Editors wurden entfernt. Diese Tools sind nicht mehr verfügbar inAWS. BenutzenA WS Resource Groupsund stattdessen Tag Editor.	14. Mai 2019

Der Tag Editor unterstützt jetzt das Taggen von Ressourcen in mehreren Regionen	Mit Tag Editor können Sie jetzt Ressourcen-Tags in mehreren Regionen suchen und verwalten, wobei den Ressourcenabfragen Ihre aktuelle Region standardmäßig hinzugefügt wird.	2. Mai 2019
Der Tag Editor unterstützt jetzt den Export von Abfrageergebnissen in eine CSV-Datei	Sie können die Ergebnisse einer Abfrage auf der Seite Ressourcen für Tag suchen in eine CSV-formatierte Datei exportieren. In den Tag Editor-Abfrageergebnissen wird eine neue Spalte „Region“ angezeigt. Mit Tag Editor können Sie jetzt nach Ressourcen suchen, die für einen bestimmten Tag-Schlüssel leere Werte besitzen. Tag-Schlüsselwerte werden automatisch ausgefüllt, wenn Sie einen Wert eingeben, der für die vorhandenen Schlüssel eindeutig ist.	2. April 2019

Der Tag Editor unterstützt jetzt das Hinzufügen aller Ressourcentypen zu einer Abfrage	Sie können Tags auf bis zu 20 einzelne Ressourcentypen in einer einzigen Operation anwenden. Sie können auch All resource types (Alle Ressourcentypen) auswählen , um alle Ressourcentypen in einer Region abzufragen. Autovervollständigungs wurde hinzugefügt, um die Tag-Schlüssel- Feld eine Abfrage, um die konsistente Tag-Schlüssel zwischen Ressourcen aktiviere n. Wenn Tag-Änderungen für einige Ressourcen fehlschla gen, können Sie Tag-Änder ungen nur für die Ressourcen wiederholen, für die die Tag-Änderungen fehlgeschlagen sind.	19. März 2019
Der Tag Editor unterstützt jetzt mehrere Ressourcentypen bei einer Suche	Sie können Tags auf bis zu 20 Ressourcentypen in einer einzigen Operation anwenden. Sie können auch die Spalten auswählen, die Ihnen in den Suchergebnissen angezeigt werden, einschließlich Spalten für jeden eindeutigen Tag-Schlüssel in Ihren Suchergebnissen oder in bestimmten Ressourcen in den Ergebnissen.	26. Februar 2019

Dokumentation für den neuen Tag-Editor hinzugefügt	Im Abschnitt „Arbeiten mit Tag Editor“ wird beschrieben, wie Sie die neue AWS Tag Editor-Konsole verwenden.	13. Februar 2019
Neue Ressourcentypen werden für Gruppen in Ressourcengruppen unterstützt	Neue Ressourcentypen wurden hinzugefügt, die jetzt in Ressourcengruppen unterstützt werden.	4. Februar 2019
Verbesserte Benutzererfahrung beim Hinzufügen von Tags zu tagbasierten Resource Groups-Abfragen	Es wurden kleinere Änderungen in der Benutzeroberfläche der Konsole für das Hinzufügen von Tags in einer Tag-basierte Abfrage durchgeführt.	17. Dezember 2018
AWS CloudFormationUnterstützung für stapelbasierte Abfragen zu Ressourcengruppen hinzugefügt	Sie können Ressourcengruppen erstellen, in denen die Abfrage auf einem AWS CloudFormation-Stack basiert. Nach der Auswahl eines Stacks können Sie festlegen, welche Stack-Ressourcentypen in der Abfrage Ihrer Gruppe angezeigt werden sollen.	13. November 2018
Ressourcengruppen undCloudTrail	Resource Groups bietet jetztAWS CloudTrailUnterstützung. Sie können die Protokolle aller API-Aufrufe von Resource Groups in einsehen und mit ihnen arbeitenCloudTrail.	29. Juni 2018

- API-Version: 2017-11-27
- Letzte Aktualisierung der Dokumentation: 24. September 2019

Frühere Aktualisierungen

In der folgenden Tabelle sind wichtige Änderungen in jeder Version des AWS Resource Groups-Benutzerhandbuchs vor Juni 2018 beschrieben.

Änderung	Beschreibung	Datum
Erstversion	Erste Version der nächsten Generation von AWS Resource Groups	29. November 2017

AWS-Glossar

Die neueste AWS-Terminologie finden Sie im AWS-Glossar in der AWS-Glossar-Referenz.

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.