aws

Leitfaden

Markieren von AWS Ressourcen

Version 1.0

Markieren von AWS Ressourcen: Leitfaden

Table of Contents

Markieren Ihrer AWS-Ressourcen

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. Beispiele für -Ressourcen sind eine Amazon Elastic Compute Cloud (Amazon EC2)-Instance, ein Amazon Simple Storage Service (Amazon S3)-Bucket oder ein Secret in AWS Secrets Manager.

> **Important**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Wir verwenden Tags, um Ihnen Fakturierungs- und Verwaltungsservices zur Verfügung zu stellen. Tags sind nicht für private oder vertrauliche Daten gedacht.

Mit Tags können Sie Ressourcen verwalten, identifizieren, organisieren, suchen und filtern. Sie können Tags erstellen, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren.

Jedes Tag besteht aus zwei Teilen:

- einem Tag-Schlüssel (z. B. `CostCenter`, `Environment` oder `Project`). Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.
- Einem Tag-Wert (z. B. `111122223333` oder `Production`). Wie bei Tag-Schlüsseln wird auch bei Tag-Werten zwischen Groß- und Kleinschreibung unterschieden.

Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren.

So fügen Sie Ihren Ressourcen Tags hinzu AWS

Es gibt drei Möglichkeiten, Ihren Ressourcen Tags hinzuzufügenAWS:

- AWS-Service API-Operation – Die Tagging-API-Operationen, die direkt unterstützt AWS-Servicewerden. Informationen dazu, welche Tagging-Funktionen die einzelnen AWS-Service bieten, finden Sie in der Dokumentation des Services im AWS Dokumentationsindex .

- Tag-Editor-Konsole – Einige Services unterstützen auch das Tagging mit der AWS Tag-Editor-Konsole.
- Resource Groups Tagging API – Die meisten -Services unterstützen auch Tagging mit der AWS Resource Groups Tagging API.

Sie können Ressourcen für alle Services mit anfallenden Kosten in AWS markieren. Für die folgenden Services empfiehlt AWS eine neuere Alternative AWS-Services, die Markierungen unterstützt, um den Anwendungsfällen der Kunden besser gerecht zu werden.

Amazon Cloud Directory	Amazon CloudSearch	Amazon Cognito Sync
AWS Data Pipeline	Amazon Elastic Transcoder	Amazon Machine Learning
AWS OpsWorks Stacks	Amazon S3 Glacier Direct	Amazon SimpleDB
Amazon WorkSpaces Application Manager	AWS DeepLens	

Bewährte Methoden

Befolgen Sie beim Erstellen einer Tagging-Strategie für AWS-Ressourcen die folgenden bewährten Methoden:

- Fügen Sie keine personenbezogenen Daten (Personally Identifiable Information, PII) oder andere vertrauliche Informationen in Tags hinzu. Tags sind für viele AWS-Dienste zugänglich, einschließlich der Abrechnung. Tags sind nicht für private oder vertrauliche Daten gedacht.
- Verwenden Sie für Tags ein standardisiertes Format, bei dem die Groß-/Kleinschreibung beachtet wird, und wenden Sie es konsistent für alle Ressourcentypen an.
- Verwenden Sie Tag-Richtlinien, die mehrere Zwecke unterstützen, wie die Verwaltung der Ressourcenzugriffskontrolle, Kostenverfolgung, Automatisierung und Organisation.
- Verwenden Sie automatisierte Tools zur Verwaltung von Ressourcen-Tags. Der Tag-Editor und die Tagging-API von Resource Groups ermöglichen die programmgesteuerte Steuerung von Tags und erleichtern so die automatische Verwaltung, Suche und Filterung von Tags und Ressourcen.
- Verwenden Sie eher zu viele als zu wenige Tags.

- Denken Sie daran, dass es einfach ist, Tags zu ändern, um sich ändernden Geschäftsanforderungen gerecht zu werden, aber bedenken Sie die Folgen zukünftiger Änderungen. Wenn Sie beispielsweise Zugriffssteuerungs-Tags ändern, müssen Sie auch die Richtlinien aktualisieren, die auf diese Tags verweisen, und den Zugriff auf Ihre Ressourcen steuern.
- Sie können Tagging-Standards, die Ihr Unternehmen einführen möchte, automatisch durchsetzen, indem Sie mit AWS Organizations Tag-Richtlinien erstellen und bereitstellen. Mithilfe von Tag-Richtlinien können Sie Tagging-Regeln angeben und gültige Schlüsselnamen sowie die für jeden Schlüssel gültigen Werte festlegen. Außerdem ist eine reine Überwachung möglich, bei der Sie bestehende Tags beurteilen und bereinigen können. Wenn die Tags den ausgewählten Standards entsprechen, können Sie die Durchsetzung der Tag-Richtlinien aktivieren, um zu verhindern, das Tags erstellt werden, die nicht regelkonform sind. Weitere Informationen finden Sie unter Tag-Richtlinien im AWS Organizations-Benutzerhandbuch.

Tagging-Kategorien

Unternehmen, die Tags sehr effektiv verwenden, erstellen in der Regel geschäftsrelevante Tag-Gruppierungen, um ihre Ressourcen anhand technischer, geschäftlicher und sicherheitsrelevanter Dimensionen zu organisieren. Unternehmen, die automatisierte Prozesse für die Verwaltung ihrer Infrastruktur nutzen, verwenden auch zusätzliche, automatisierungsspezifische Tags.

Technische Tags	Tags für die Automatisierung	Business-Tags	Sicherheits-Tags
• Name – Identifizieren einzelner Ressourcen • Anwendungs-ID – Identifizieren von Ressourcen, die mit einer bestimmten Anwendung verknüpft sind • Anwendungsrolle – Beschreibung	• Datum/Uhrzeit – Identifizieren des Datums oder der Uhrzeit, zu dem/der eine Ressource gestartet, gestoppt, gelöscht oder rotiert werden soll • Opt-In/Opt-out – Angabe, ob eine Ressource in eine automatis	• Projekt – Identifizieren von Projekten, die von der Ressource unterstützt werden • Eigentümer – Identifizieren der für die Ressource verantwortlichen Person	• Vertraulichkeit – Eine Kennung für die spezifische Datenvertraulichkeitsebene, die eine Ressource unterstützt • Compliance – Ein Bezeichner für Workloads, die bestimmte Compliance-

Technische Tags	Tags für die Automatisierung	Business-Tags	Sicherheits-Tags
der Funktion einer bestimmte n Ressource (z. B. Webserver, Message Broker, Datenbank) • Cluster – Identifiz ieren von Ressourcenfarmen, die eine gemeinsam e Konfiguration verwenden und eine bestimmte Funktion für eine Anwendung ausführen • Umgebung – Unterscheiden zwischen Entwicklu ngs-, Test- und Produktionsressour cen • Version – Unterscheiden zwischen Versionen von Ressourcen oder Anwendungen	ierte Aktivität wie Starten, Beenden oder Ändern von Instances einbezogen werden soll • Sicherheit – Festlegen von Anforderungen wie Verschlüsselung oder Aktivieren von Amazon-VPC-Flussprotokollen; Identifizieren von Routentabellen oder Sicherhei tsgruppen, die eine zusätzliche Prüfung erfordern	• Kostenstelle/ Geschäftseinheit – Identifizieren der Kostenstelle oder Geschäftseinheit, die einer Ressource zugeordnet ist, in der Regel für die Kostenzuordnung und -verfolgung • Kunde – Identifiz ieren eines bestimmten Clients, für den eine bestimmte Gruppe von Ressourcen da ist	Anforderungen erfüllen müssen

Beschränkungen und Anforderungen für die Benennung von Tags

Für Tags gelten die folgenden grundlegenden Benennungs- und Verwendungsanforderungen:

- Eine Ressource kann bis zu 50 Tags besitzen, die von Benutzern erstellt wurden.

- Tags, die vom System erstellt wurden und mit `aws:` beginnen, sind für AWS reserviert und werden nicht auf dieses Limit angerechnet. Tags, die mit dem einem `aws:`-Präfix beginnen, können nicht bearbeitet oder gelöscht werden.
- Jeder Tag (Markierung) muss für jede Ressource eindeutig sein. Jeder Tag (Markierung) kann nur einen Wert haben.
- Der Tag-Schlüssel muss eine Länge zwischen 1 und 128 Unicode-Zeichen in UTF-8 aufweisen.
- Der Tag-Wert muss eine Länge zwischen 0 und 256 Unicode-Zeichen in UTF-8 aufweisen.
- Zulässige Zeichen können je nach AWS-Service variieren. Informationen darüber, welche Zeichen Sie zum Taggen von Ressourcen in einem bestimmten AWS-Service verwenden können, finden Sie in der entsprechenden Dokumentation. Im Allgemeinen sind die zulässigen Zeichen Buchstaben, Ziffern und Leerzeichen, die in UTF-8 darstellbar sind, sowie die folgenden Zeichen: _ . : / = + - @.
- Bei Tag-Schlüsseln und -Werten muss die Groß- und Kleinschreibung beachtet werden. Eine bewährte Methode besteht darin, sich für eine einheitliche Schreibweise der Tag-Benennungen zu entscheiden und diese Strategie für alle Ressourcentypen umzusetzen. Entscheiden Sie sich beispielsweise für `Costcenter`, `costcenter` oder `CostCenter` und verwenden Sie diese Konvention für alle Tags. Vermeiden Sie die Verwendung von ähnlichen Tags mit uneinheitlicher Fallunterscheidung.

Häufig verwendete Tagging-Strategien

Anhand der folgenden Markierungs-Strategien können Sie AWS-Ressourcen leichter finden und verwalten.

Inhalt

Tags zur Ressourcenorganisation

Tags sind eine gute Möglichkeit, AWS-Ressourcen in der AWS Management Console zu organisieren. Sie können Tags so konfigurieren, dass sie mit Ressourcen angezeigt werden, und Sie

können nach Tags suchen und filtern. Mit dem AWS Resource Groups-Service können Sie Gruppen von AWS-Ressourcen basierend auf einem oder mehreren Tags oder Teilen von Tags erstellen. Sie können auch Gruppen auf der Grundlage ihres Vorkommens in einem AWS CloudFormation-Batch erstellen. Mit Ressourcengruppen und dem Tag-Editor können Sie Daten für Anwendungen konsolidieren und anzeigen, die aus mehreren Services, Ressourcen und Regionen bestehen.

Tags für die Kostenzuordnung

AWS Cost Explorer und detaillierte Abrechnungsberichte ermöglichen die Aufschlüsselung der AWS-Kosten nach Tags. In der Regel verwenden Sie Business-Tags wie Kostenstelle/Geschäftseinheit, Kunde oder Projekt, um AWS-Kosten herkömmlichen Kostenkategorien zuzuordnen. Ein Kostenzuordnungsbericht kann jedoch jedes beliebige Tag enthalten. So können Sie Ihre Kosten auch technischen oder Sicherheitspositionen, beispielsweise spezifischen Anwendungen, Umgebungen oder Compliance-Programmen zuordnen. Im Folgenden finden Sie ein Beispiel für einen Bericht zur Teilkostenzuweisung.

Total Cost	user:Owner	user:Stack	user:Cost Center	user:Application
0.95	DbAdmin	Test	80432	Widget2
0.01	DbAdmin	Test	80432	Widget2
3.84	DbAdmin	Prod	80432	Widget2
6.00	DbAdmin	Test	78925	Widget1
234.63	SysEng	Prod	78925	Widget1
0.73	DbAdmin	Test	78925	Widget1
0.00	DbAdmin	Prod	80432	Portal
2.47	DbAdmin	Prod	78925	Portal

Für manche Services können Sie ein AWS-generiertes `createdBy`-Tag für Kostenzuordnungszwecke verwenden, um Ressourcen zu berücksichtigen, die andernfalls nicht kategorisiert werden könnten. Das `createdBy`-Tag ist nur für unterstützte AWS-Services und Ressourcen verfügbar. Sein Wert enthält Daten, die bestimmten API- oder Konsolenereignissen zugeordnet sind. Weitere Informationen finden Sie unter Von AWS generierte Kostenzuordnungs-Tags im AWS Billing and Cost Management-Benutzerhandbuch.

Tags für die Automatisierung

Ressourcen- oder servicespezifische Tags werden häufig verwendet, um Ressourcen während der Automatisierungsaktivitäten zu filtern. Automatisierungs-Tags werden verwendet, um automatisierte Aufgaben zu aktivieren oder abzulehnen oder bestimmte Versionen von Ressourcen zu identifizieren, die archiviert, aktualisiert oder gelöscht werden sollen. Beispielsweise können Sie automatisierte `start`- oder `stop`-Skripts ausführen, die Entwicklungsumgebungen außerhalb der Geschäftszeiten

deaktivieren, um die Kosten zu senken. In diesem Szenario sind Amazon Elastic Compute Cloud (Amazon EC2)-Instance-Tags eine einfache Möglichkeit, Instances zu identifizieren, um diese Aktion abzulehnen. Bei Skripten, die veraltete, oder fortlaufende Amazon-EBS-Snapshots finden out-of-dateund löschen, können Snapshot-Tags eine zusätzliche Dimension von Suchkriterien hinzufügen.

Tags für die Zugriffskontrolle

IAM-Richtlinien unterstützen Tag-basierte Bedingungen, sodass Sie IAM-Berechtigungen basierend auf bestimmten Tags oder Tag-Werten einschränken können. Beispielsweise können IAM-Benutzer- oder -Rollenberechtigungen Bedingungen umfassen, um basierend auf ihren Tags EC2-API-Aufrufe auf bestimmte Umgebungen (wie Entwicklung, Test oder Produktion) zu beschränken. Dieselbe Strategie kann verwendet werden, um API-Aufrufe auf bestimmte Amazon Virtual Private Cloud (Amazon VPC)-Netzwerke zu beschränken. Die Unterstützung von Tag-basierten IAM-Berechtigungen auf Ressourcenebene ist servicespezifisch. Wenn Sie tagbasierte Bedingungen für die Zugriffskontrolle verwenden, müssen Sie festlegen und einschränken, wer die Tags ändern kann. Weitere Informationen zur Verwendung von Tags zur Kontrolle des API-Zugriffs auf AWS-Ressourcen finden Sie unter AWS-Services, die mit IAM funktionieren im IAM-Benutzerhandbuch.

Tagging-Governance

Eine effektive Tagging-Strategie verwendet standardisierte Tags und wendet diese konsistent und programmgesteuert über AWS-Ressourcen hinweg an. Sie können sowohl reaktive als auch proaktive Konzepte zur Steuerung von Tags in Ihrer AWS-Umgebung verwenden.

- Die Reaktive Governance dient dazu, Ressourcen zu finden, die nicht ordnungsgemäß mit Tools wie der API für das Ressourcengruppen-Tagging, AWS-Config-Regeln und benutzerdefinierten Skripten gekennzeichnet sind. Um Ressourcen manuell zu suchen, können Sie Tag-Editor und detaillierte Abrechnungsberichte verwenden.
- Proaktive Governance nutzt Tools wie AWS CloudFormation, Service Catalog, Tag-Richtlinien in AWS Organizations oder IAM-Berechtigungen auf Ressourcenebene, um sicherzustellen, dass standardisierte Tags bei der Ressourcenerstellung einheitlich angewendet werden.

  Beispielsweise können Sie die AWS CloudFormation-Eigenschaft `Resource Tags` verwenden, um Tags auf Ressourcentypen anzuwenden. In Service Catalog können Sie Portfolio- und Produkt-Tags hinzufügen, die beim Start eines Produkts automatisch kombiniert und angewendet werden. Zu den strengeren Formen der proaktiven Governance gehören automatisierte Aufgaben. Sie können beispielsweise die API für das Ressourcengruppen-Tagging verwenden, um die Tags

einer AWS-Umgebung zu durchsuchen oder Skripts ausführen, um falsch markierte Ressourcen in Quarantäne zu verschieben oder zu löschen.

Weitere Informationen

Diese Seite enthält allgemeine Informationen zum Tagging von AWS-Ressourcen. Weitere Informationen zum Taggen von Ressourcen in einem bestimmten AWS-Service finden Sie in der entsprechenden Dokumentation. Im Folgenden finden Sie auch gute Informationsquellen zum Tagging:

- Weitere Informationen über AWS Resource Groups Tagging API finden Sie unter API-Referenz der Ressourcengruppen-Markierung.
- Informationen zum Tag-Editor finden Sie unter Tag-Editor in diesem Handbuch.
- Informationen zu den jeweils AWS-Service bereitgestellten Tagging-Funktionen finden Sie in der Dokumentation des Services im AWS Dokumentationsindex .
- Informationen über die Verwendung von Tags in IAM-Richtlinien, um zu kontrollieren, wer Ihre AWS-Ressourcen anzeigen und mit ihnen interagieren kann, finden Sie unter Steuerung des Zugriffs auf und für IAM-Benutzer und IAM-Rollen mithilfe von Tags im IAM-Benutzerhandbuch.

Verwendung von Tag Editor

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. Beispiele für -Ressourcen sind eine Amazon Elastic Compute Cloud (Amazon EC2)-Instance, ein Amazon Simple Storage Service (Amazon S3)-Bucket oder ein Secret in AWS Secrets Manager. 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 Fakturierungs- und Verwaltungsservices zur Verfügung zu stellen. Tags sind nicht für private oder vertrauliche Daten gedacht.

Verwenden Sie den Tag-Editor, um Tags mehreren Ressourcen gleichzeitig hinzuzufügen oder zu bearbeiten oder zu löschen. Mit Tag Editor können Sie nach den Ressourcen suchen, die Sie mit Tags markieren möchten, und dann die Tags für die Ressourcen in Ihren Suchergebnissen verwalten.

So starten Sie den Tag Editor:

1. Melden Sie sich an der AWS Management Console an.
2. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie Services aus. Wählen Sie dann unter Management und Governance die Option Ressourcengruppen und Tag-Editor aus. Wählen Sie im Navigationsbereich auf der linken Seite Tag Editor aus.
   - Verwenden Sie den direkten Link: AWS Tag-Editor-Konsole .

Nicht alle Ressourcen können mit Tags markiert werden. Informationen darüber, welche Ressourcen der Tag-Editor unterstützt, finden Sie in der Spalte Tag-Editor-Tagging unter Unterstützte Ressourcentypen im AWS Resource Groups -Benutzerhandbuch. Wenn ein Ressourcentyp, den

Sie markieren möchten, nicht unterstützt wird, teilen Sie dies AWS mit, indem Sie Feedback in der unteren linken Ecke des Konsolenfensters auswählen.

Informationen zu den Berechtigungen und Rollen, die für das Markieren von Ressourcen mit Tags erforderlich sind, finden Sie unter Berechtigungen einrichten.

Themen

Tags und attributbasierte Zugriffskontrolle

Tags können ein wichtiger Teil Ihrer AWS Zugriffskontrollstrategie sein. Informationen zur Verwendung von Tags als Attribute in einer attributbasierten Zugriffssteuerungsstrategie (ABAC) finden Sie unter Steuern des Zugriffs auf AWS Ressourcen mithilfe von Tags und Steuern des Zugriffs auf und für IAM-Benutzer und -Rollen mithilfe von Tags, beide im IAM-Benutzerhandbuch.

Es gibt ein umfassendes Tutorial, das zeigt, wie Sie mithilfe von Tags im IAM-Tutorial Zugriff auf verschiedene Projekte und Gruppen gewähren: Definieren Sie Berechtigungen für den Zugriff auf AWS Ressourcen basierend auf Tags im AWS Identity and Access Management -Benutzerhandbuch.

Wenn Sie einen SAML-basierten Identitätsanbieter (IdP) für die einmalige Anmeldung verwenden, können Sie den angenommenen Rollen Tags anfügen, die Zugriff auf Ihre Benutzer gewähren. Weitere Informationen finden Sie im IAM-Tutorial: Verwenden von SAML-Sitzungs-Tags für ABAC im AWS Identity and Access Management -Benutzerhandbuch.

Bewährte Methoden für Tag-Namen

Dies sind einige bewährte Methoden und Namenskonventionen, die Sie mit Ihren Tags verwenden sollten.

Bei Schlüsselnamen für Tags muss die GroßAWS- und Kleinschreibung beachtet werden. Stellen Sie daher sicher, dass sie konsistent verwendet werden. Beispielsweise `costcenter` sind die Tag-Schlüssel `CostCenter` und unterschiedlich. Ein Tag-Schlüssel kann als Kostenzuordnungs-Tag für Finanzanalysen und Berichte konfiguriert werden, und der andere Tag-Schlüssel ist möglicherweise nicht für dieselbe Verwendung konfiguriert.

Eine Reihe von Tags wird von vordefiniert AWS oder automatisch von verschiedenen erstelltAWS-Services. Viele AWS generierte Tags verwenden Schlüsselnamen, die alle Kleinbuchstaben enthalten, wobei Bindestriche Wörter im Namen trennen, und Präfixe gefolgt von Doppelpunkten, um den Quellservice für das Tag zu identifizieren. Sehen Sie sich zum Beispiel Folgendes an:

- `aws:ec2spot:fleet-request-id` ist ein Tag, das die Amazon EC2-Spot-Instance-Anforderung identifiziert, die die Instance gestartet hat.
- `aws:cloudformation:stack-name` ist ein Tag, das den AWS CloudFormationStack identifiziert, der die Ressource erstellt hat.
- `elasticbeanstalk:environment-name` ist ein Tag, das die Anwendung identifiziert, die die Ressource erstellt hat.

Erwägen Sie, Ihre Tags mit den folgenden Regeln zu benennen:

- Verwenden Sie für die Wörter nur Kleinbuchstaben.
- Verwenden Sie Bindestriche, um Wörter zu trennen.
- Verwenden Sie ein Präfix gefolgt von einem Doppelpunkt, um den Namen der Organisation oder den abgekürzten Namen zu identifizieren.

Für ein fiktives Unternehmen mit dem Namen könnten AnyCompanySie beispielsweise Tags wie folgt definieren:

- `anycompany:cost-center` , um den internen Cost-Center-Code zu identifizieren.
- `anycompany:environment-type` um festzustellen, ob es sich bei der Umgebung um Entwicklungs-, Test- oder Produktionsumgebungen handelt.

- `anycompany:application-id` , um die Anwendung zu identifizieren, für die die Ressource erstellt wurde.

Das -Präfix stellt sicher, dass Tags gemäß Ihrer Organisation eindeutig erkennbar sind und nicht von AWS oder einem Tool eines Drittanbieters, das Sie möglicherweise verwenden. Die Verwendung von Kleinbuchstaben mit Bindestrichen für Trennzeichen vermeidet Verwirrung bei der Großschreibung eines Tag-Namens. Zum Beispiel ist es einfacher, sich `anycompany:project-id` zu merken als `ANYCOMPANY:ProjectID`, `anycompany:projectID` oder`Anycompany:ProjectId`.

Erste Schritte mit dem Tag-Editor

Der Tag-Editor ist eine Möglichkeit, Ihre -Ressourcen zu markieren. In den folgenden Abschnitten erfahren Sie, welche Voraussetzungen Sie erfüllen müssen, um sie zu verwenden.

Voraussetzungen für die Arbeit mit dem Tag Editor

Bevor Sie mit der Markierung Ihrer Ressourcen beginnen, stellen Sie sicher, dass Sie über eine aktive AWS-Konto mit vorhandenen Ressourcen und über die entsprechenden Rechte verfügen, um Ressourcen zu markieren und Gruppen zu erstellen.

Themen

Registrieren für ein AWS-Konto

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.

AWS sendet Ihnen eine Bestätigungs-E-Mail, nachdem der Registrierungsprozess abgeschlossen ist. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen eines Administratorbenutzers

Nachdem Sie sich für ein registriert haben AWS-Konto, sichern Sie Ihr Root-Benutzer des AWS-Kontos, aktivieren Sie AWS IAM Identity Centerund erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Ihrer Root-Benutzer des AWS-Kontos

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

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

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

Erstellen eines Administratorbenutzers

1. Aktivieren Sie das IAM Identity Center.

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

Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Konfigurieren des Benutzerzugriffs mit dem Standard IAM-Identity-Center-Verzeichnis- im AWS IAM Identity Center -Benutzerhandbuch.

Anmelden als Administratorbenutzer

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

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

Erstellen von -Ressourcen

Sie müssen über Ressourcen in Ihrem verfügen AWS-Konto , um sie zu markieren. Weitere Informationen zu den unterstützten Ressourcentypen finden Sie in der Spalte Tag-Editor-Markierung unter Unterstützte Ressourcentypen im AWS Resource Groups -Benutzerhandbuch.

Berechtigungen einrichten

Um den Tag-Editor in vollem Umfang nutzen zu können, benötigen Sie möglicherweise zusätzliche Berechtigungen, um Ressourcen zu markieren oder die Tag-Schlüssel und -Werte einer Ressource anzuzeigen. Diese Berechtigungen sind in den folgenden Kategorien unterteilt:

- 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.

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 IAM-Rollen, -Benutzer oder -Gruppen und wenden dann die Richtlinien mit den erforderlichen Berechtigungen an. 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 erforderlich sind, wenn Sie Ressourcen von anderen AWS Servicekonsolen und APIs markieren möchten.

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, müssen Sie über Berechtigungen für die Tagging-Operationen in der API dieses Services verfügen, z. B. die Amazon EC2CreateTagsOperation.

Erforderliche Berechtigungen für die Verwendung der Tag-Editor-Konsole

Um die Tag-Editor-Konsole zum Auflisten und Markieren von Ressourcen zu verwenden, müssen der Richtlinienanweisung eines Benutzers in IAM die folgenden Berechtigungen hinzugefügt werden. Sie können entweder AWS verwaltete Richtlinien hinzufügen, die von verwaltet und auf dem neuesten Stand gehalten werden AWS, oder Sie können Ihre eigene benutzerdefinierte Richtlinie erstellen und verwalten.

Verwenden von AWS verwalteten Richtlinien für Tag-Editor-Berechtigungen

Tag Editor unterstützt die folgenden AWS verwalteten Richtlinien, mit denen Sie Ihren Benutzern einen vordefinierten Satz von Berechtigungen bereitstellen können. Sie können diese verwalteten Richtlinien an jede Rolle, jeden Benutzer oder jede Gruppe anfügen, genau wie jede andere von Ihnen erstellte Richtlinie.

ResourceGroupsandTagEditorReadOnlyAccess

Diese Richtlinie gewährt der angehängten IAM-Rolle oder dem angehängten Benutzer die Berechtigung, die schreibgeschützten Operationen sowohl für als auch für den AWS Resource Groups Tag-Editor aufzurufen. Um die Tags einer Ressource zu lesen, müssen Sie auch über eine separate Richtlinie über Berechtigungen für diese Ressource verfügen. Weitere Informationen finden Sie im 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. Weitere Informationen finden Sie im folgenden wichtigen Hinweis.

Important

Die beiden vorherigen Richtlinien erteilen die Berechtigung zum Aufrufen der Tag-Editor-Operationen und zum Verwenden der Tag-Editor-Konsole. Sie müssen jedoch auch über Berechtigungen verfügen, um nicht nur 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 AWS verwaltete Richtlinie ReadOnlyAccess gewährt Berechtigungen für die schreibgeschützten Operationen für die Ressourcen jedes Services. hält diese Richtlinie AWS automatisch mit neuen auf dem neuesten Stand AWS-Services , sobald sie verfügbar sind.
- Viele -Services bieten servicespezifische schreibgeschützte AWS verwaltete Richtlinien, mit denen Sie den Zugriff auf die von diesem Service bereitgestellten Ressourcen beschränken können. Amazon EC2 stellt beispielsweise bereitAmazonEC2ReadOnlyAccess.
- Sie können Ihre eigene Richtlinie erstellen, die nur Zugriff auf die spezifischen schreibgeschützten Operationen für die wenigen Services und Ressourcen gewährt, auf die Ihre Benutzer zugreifen sollen. Diese Richtlinie verwendet entweder eine Zulassungslistenstrategie oder eine Sperrlistenstrategie.

  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": [ "tag:*" ],
            "Resource": "<ARNs of resources to allow tagging>"
        }
    ]
```

```
}
```

Alternativ können Sie eine Verweigerungslistenstrategie verwenden, die den Zugriff auf alle Ressourcen ermöglicht, mit Ausnahme derjenigen, die Sie explizit blockieren. Dies erfordert eine separate Richtlinie, die für die relevanten Benutzer gilt, die den Zugriff erlauben. Die folgende Beispielrichtlinie verweigert dann den Zugriff auf die spezifischen Ressourcen, die durch den Amazon-Ressourcennamen (ARN) aufgelistet werden.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
             "Action": [ "tag:*" ],
            "Resource": "<ARNs of resources to disallow tagging>"
        }
    ]
}
```

Manuelles Hinzufügen von Tag-Editor-Berechtigungen

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

> **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.

Erteilen von Berechtigungen für die Verwendung des Tag Editors

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

1. Öffnen Sie die IAM-Konsole zur Seite Rollen.
2. Suchen Sie die Rolle, der Sie Tag-Editor-Berechtigungen erteilen möchten. Wählen Sie den Namen der Rolle aus, um die Seite Zusammenfassung der Rolle zu öffnen.
3. Wählen Sie auf der Registerkarte Permissions die Option Add permissions.
4. Wählen Sie Vorhandene Richtlinien direkt zuordnen.
5. Wählen Sie Richtlinie erstellen aus.
6. Fügen Sie auf der Registerkarte JSON die folgende Richtlinienanweisung ein.

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

```
  ]
}
```

> **Note**
>
> Diese Beispielrichtlinienanweisung gewährt Berechtigungen, um nur Tag-Editor-Aktionen auszuführen.

7. Wählen Sie Next: Tags (Weiter: Tags) und danach Next: Review (Weiter: Prüfen) aus.
8. Geben Sie einen Namen und eine Beschreibung für die neue Richtlinie ein. Beispiel: **`AWSTaggingAccess`**
9. Wählen Sie Richtlinie erstellen aus.

Nachdem die Richtlinie nun in IAM gespeichert ist, können Sie sie an andere Prinzipale wie Rollen, Gruppen oder Benutzer anfügen. Weitere Informationen zum Hinzufügen einer Richtlinie zu einem Prinzipal finden Sie unter Hinzufügen und Entfernen von IAM-Identitätsberechtigungen im IAM-Benutzerhandbuch.

Autorisierung und Zugriffskontrolle basierend auf Tags

AWS-Services unterstützt Folgendes:

- Aktionsbasierte Richtlinien – Sie können beispielsweise eine Richtlinie erstellen, die es Benutzern ermöglicht, - `GetTagKeys` oder -`GetTagValues`Operationen auszuführen, aber keine anderen.
- Berechtigungen auf Ressourcenebene in -Richtlinien – Viele -Services unterstützen die Verwendung von ARNs, um einzelne Ressourcen in der Richtlinie anzugeben.
- Autorisierung auf der Basis von Tags – Viele -Services unterstützen die Verwendung von Ressourcen-Tags in der Bedingung einer Richtlinie. Sie können beispielsweise eine Richtlinie erstellen, die Benutzern vollen Zugriff auf eine Gruppe gewährt, die dasselbe Tag wie die Benutzer hat. Weitere Informationen finden Sie unter Was ist ABAC für AWS? im AWS Identity and Access Management -Benutzerhandbuch.
- Temporäre Anmeldeinformationen – Benutzer können eine Rolle mit einer Richtlinie übernehmen, die Tag-Editor-Operationen zulässt.

Der Tag-Editor verwendet keine serviceverknüpften Rollen.

Weitere Informationen zur Integration von 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 Tag Editor
- Steuern des Zugriffs auf AWS Ressourcen mithilfe von Richtlinien

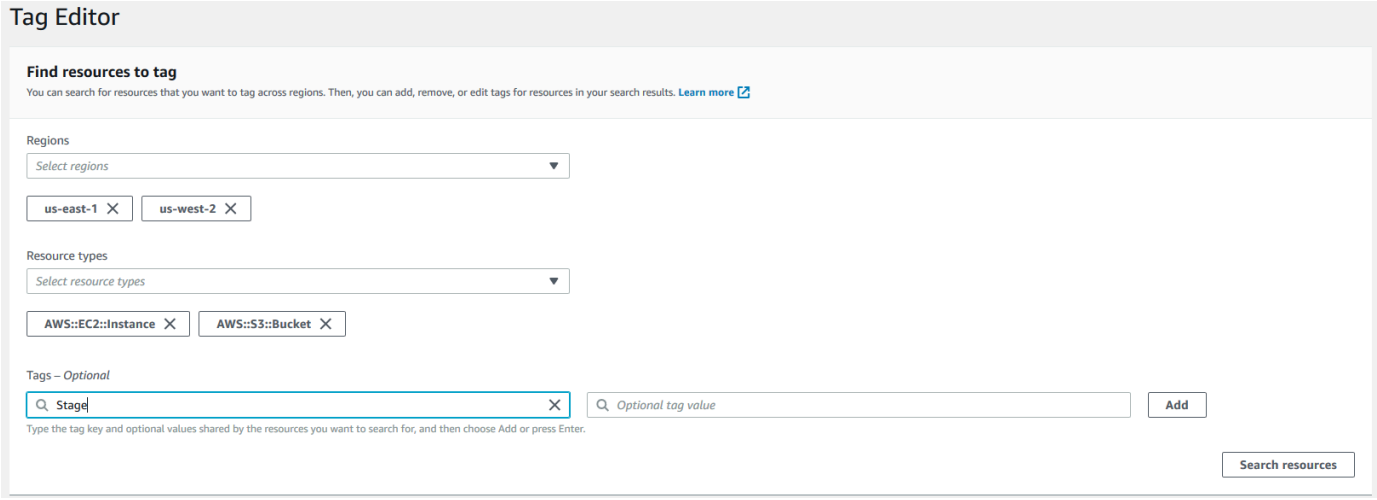
Suchen nach zu markierenden Ressourcen

Mit dem Tag-Editor erstellen Sie eine Abfrage, um Ressourcen in einer oder mehreren zu findenAWS-Regionen, die für das Tagging verfügbar sind. Sie können bis zu 20 verschiedene Ressourcentypen auswählen oder eine Abfrage auf All resource types (Alle Ressourcentypen) erstellen. Ihre Abfrage kann Ressourcen enthalten, die bereits Tags besitzen, oder Ressourcen, die keine Tags besitzen. Weitere Informationen finden Sie in der Spalte Tagging des Tag-Editors unter Unterstützte Ressourcentypen im AWS Resource Groups -Benutzerhandbuch.

Nachdem Sie die Ressourcen gefunden haben, die markiert werden sollen, können Sie in Tag Editor Tags hinzufügen, anzeigen, bearbeiten oder löschen.

So suchen Sie Ressourcen, die markiert werden sollen

1. Öffnen Sie die Tag-Editor-Konsole .
2. (Optional) Wählen Sie die aus, AWS-Regionen in der nach zu markierenden Ressourcen gesucht werden soll. Standardmäßig wird Ihre aktuelle Region verwendet. Wählen Sie für dieses Verfahren us-east-1 und us-west-2 aus.
3. Wählen Sie mindestens einen Ressourcentyp aus der Dropdown-Liste Ressourcentypen aus. Sie können Tags für bis zu 20 verschiedene Ressourcentypen gleichzeitig hinzufügen oder bearbeiten oder All resource types (Alle Ressourcentypen) auswählen. Wählen Sie für dieses Verfahren AWS::EC2::Instance und ausAWS::S3::Bucket.



4. (Optional) Geben Sie in die Felder Tags einen Tag-Schlüssel oder ein Tag-Schlüssel-Wert-Paar ein, um die Ressourcen im aktuellen AWS-Region auf diejenigen zu beschränken, die mit Ihren angegebenen Werten gekennzeichnet sind. Wenn Sie einen Tag-Schlüssel eingeben, werden übereinstimmende Tag-Schlüssel in der aktuellen Region in einer Liste unten angezeigt. Sie können einen Tag-Schlüssel aus der Liste auswählen. Tag Editor vervollständigt den Tag-Schlüssel für Sie automatisch, wenn Sie genügend Zeichen eingeben, die mit einem vorhandenen Schlüssel übereinstimmen. 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, schränkt jedoch die Ergebnisse der Abfrage weiter ein. Um weitere Tags hinzuzufügen, wählen Sie Add (Hinzufügen) aus. Abfragen weisen Tags einen `AND` Operator zu, sodass nur Ressourcen, die sowohl dem angegebenen Ressourcentyp als auch allen angegebenen Tags entsprechen, von der Abfrage zurückgegeben werden.

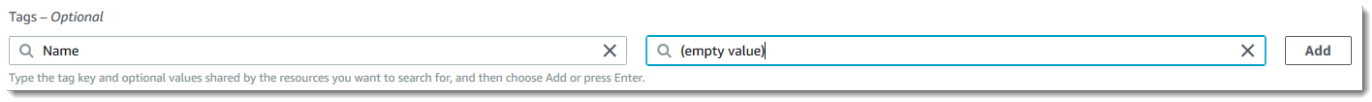
   > **Note**
   >
   > Die Tag-Editor-Konsole unterstützt derzeit keine Platzhalter.

   Um Ressourcen mit mehreren Werten für einen Tag-Schlüssel zu suchen, fügen Sie ein anderes Tag mit demselben Schlüssel zur Abfrage hinzu, geben jedoch einen anderen Wert an. Die Ergebnisse umfassen alle Ressourcen, die mit demselben Tag-Schlüssel markiert sind und einen der ausgewählten Werte haben. Bei der Suche wird die Groß-/Kleinschreibung beachtet.

   Lassen Sie die Felder Tags leer, um alle Ressourcen des angegebenen Typs im ausgewählten zu findenAWS-Regionen. Diese Abfrage gibt Ressourcen mit beliebigen Tags zurück und enthält

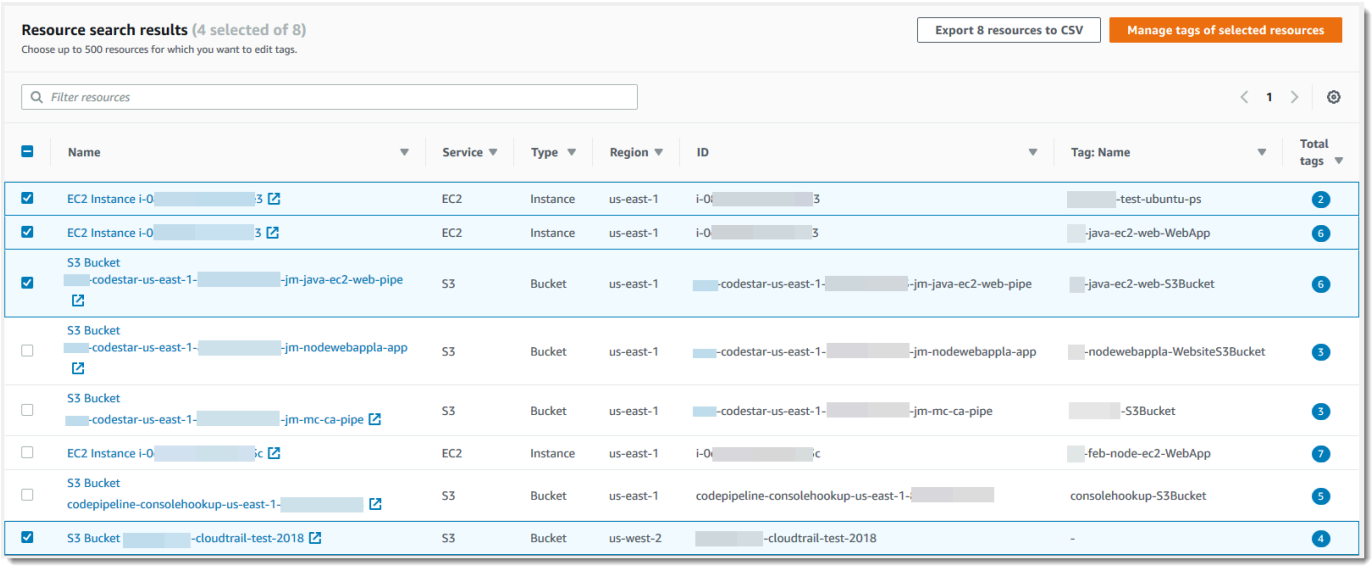
auch Ressourcen, die keine Tags besitzen. Um ein Tag aus Ihrer Abfrage zu entfernen, wählen Sie X auf der Beschriftung des Tags aus.

Um Ressourcen zu finden, die ein Tag, aber einen leeren Wert haben, wählen Sie (leerer Wert), wie unten gezeigt, wenn sich Ihr Cursor im Feld Tag-Wert befindet.



> **Note**
>
> Bevor Sie Ressourcen mit den angegebenen Tags finden können, müssen diese auf mindestens eine Ressource des angegebenen Typs im aktuellen angewendet worden seinAWS-Region.

5. Wenn Ihre Abfrage bereit ist, wählen Sie Search resources (Ressourcen durchsuchen) aus. Die Ergebnisse werden als Tabelle im Bereich Ressourcensuchergebnisse angezeigt.



Um eine große Zahl von Ressourcen zu filtern, geben Sie in Filter resources (Ressourcen filtern) einen beliebigen Filtertext ein, z. B. den Teil des Namens einer Ressource.

> **Note**
>
> Sie können Teilzeichenfolgen verwenden, um Ihre Ergebnisse zu filtern.

6. (Optional) Um die Spalten zu konfigurieren, die der Tag-Editor in Ihren Ressourcensuchergebnissen anzeigt, wählen Sie das Zahnradsymbol Präferenzen  in den Ressourcensuchergebnissen aus.

   Klicken Sie auf der Seite Preferences (Einstellungen) auf die Anzahl der Zeilen, die in Ihren Suchergebnissen angezeigt werden sollen. Wenn Sie den gesamten Text in der Tabelle sehen möchten, aktivieren Sie das Kontrollkästchen Zeilen umbrechen.

   Aktivieren Sie Spalten, die Tag Editor in Ihren Ergebnissen anzeigen soll. Sie können für jedes Tag, das in Ihren Suchergebnissen vorkommt, eine Spalte oder eine ausgewählte Teilmenge Ihrer Suchergebnisse anzeigen. Sie können dies jederzeit tun, nachdem Sie die zu markierenden Ressourcen gefunden haben. Um eine Spalte zu aktivieren, wählen Sie das Schaltersymbol neben dem Tag und ändern Sie es von aus  in auf  .

   Wählen Sie nach dem Konfigurieren der sichtbaren Spalten und der Anzahl der angezeigten Zeilen Confirm (Bestätigen) aus.

Anzeigen und Bearbeiten von Tags für eine ausgewählte Ressource

Der Tag-Editor zeigt Ihnen die vorhandenen Tags für ausgewählte Ressourcen an, die sich in den Ergebnissen Ihrer Abfrage Ressourcen zum Markieren suchen befinden.

Wenn Sie Tag-Spalten wie im vorherigen Abschnitt beschrieben aktiviert haben, können Sie den aktuellen Wert dieses Tags für jede Ressource in den Suchergebnissen sehen.

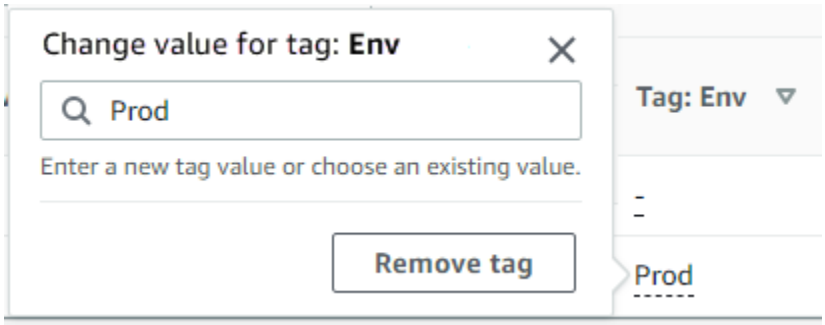
> **Note**
>
> In diesem Thema wird erläutert, wie Sie das Tag für eine einzelne Ressource bearbeiten. Sie können Tags auch für mehrere ausgewählte Ressourcen gleichzeitig bearbeiten. Weitere Informationen finden Sie unter Verwalten von Tags mit dem Tag Editor.

So bearbeiten Sie Tags inline in der Tabelle der Suchergebnisse

1. Wählen Sie den Wert für das Tag für die Ressource aus, die Sie bearbeiten möchten.

   > **Note**
   >
   > - Wenn die ausgewählte Ressource derzeit kein Tag mit dem ausgewählten Schlüssel hat, wird der Wert als (nicht markiert) angezeigt.
   > - Wenn die ausgewählte Ressource ein Tag mit dem ausgewählten Schlüssel, aber ohne Wert hat, wird der Wert als „–“ angezeigt.

   Im folgenden Beispiel wurde die Spalte für das Tag Env und mit dem aktuellen Wert Prod ausgewählt.

2. Sie können einen neuen Wert eingeben oder einen der Werte auswählen, die bereits in anderen Ressourcen mit diesem Tag vorhanden sind. Sie können das Tag auch aus dieser Ressource löschen, indem Sie Tag entfernen auswählen.

So zeigen Sie alle Tags für eine einzelne Ressource an

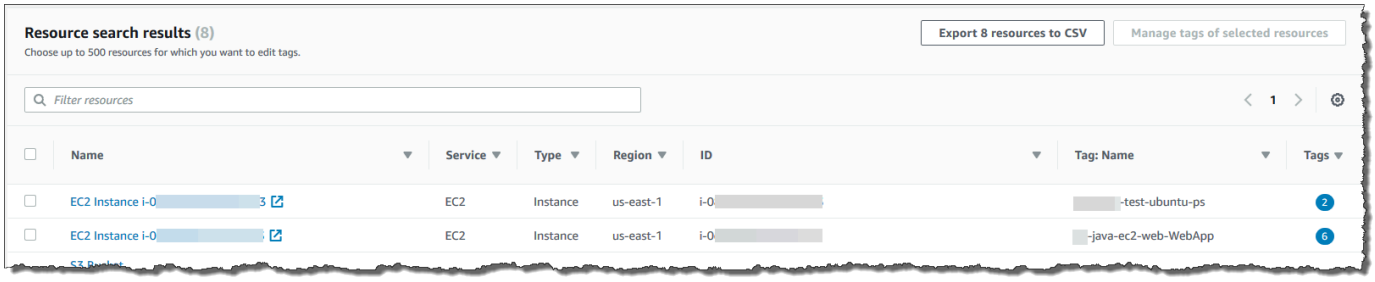
1. Wählen Sie in den Ergebnissen Ihrer Abfrage Ressourcen zum Markieren suchen die Zahl in der Spalte Tags für jede Ressource aus, für die Sie vorhandene Tags anzeigen möchten. Ressourcen mit einem Bindestrich in der Spalte Tags (Tags) besitzen keine vorhandenen Tags.
2. Sie zeigen vorhandene Tags in Resource tags (Ressourcen-Tags) an. Sie können dieses Fenster auch öffnen, indem Sie Tags ausgewählter Ressourcen verwalten auswählen, wenn Sie Tags auf der Seite Tags verwalten ändern oder entfernen.

> **Note**
>
> Wenn Ihnen ein Tag, das Sie vor kurzem auf eine Ressource angewendet haben, nicht angezeigt wird, versuchen Sie, das Browser-Fenster zu aktualisieren.

Exportieren von Ergebnissen in CSV-Datei

Sie können die Ergebnisse einer Suche nach Ressourcen exportieren, um Abfragen in eine CSV-Datei (durch Kommas getrennte Werte) zu markieren. Die CSV-Datei enthält die Ressourcennamen, Services, Region, Ressourcen-IDs, die Gesamtzahl der Tags und eine Spalte für jeden eindeutigen Tag-Schlüssel in der Sammlung. Die CSV-Datei kann Ihnen helfen, eine Tagging-Strategie für Ressourcen in Ihrer Organisation zu entwickeln oder festzustellen, wo es Überschneidungen oder Inkonsistenzen beim Markieren zwischen Ressourcen gibt.

1. Wählen Sie in den Ergebnissen Ihrer Abfrage Find resources to tag (Ressourcen suchen, die markiert werden sollen) Export resources to CSV (Ressourcen zu CSV exportieren) aus.



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

Ähnliche Informationen

- Verwenden von Kostenzuordnungs-Tags im AWS Billing-Benutzerhandbuch

Verwalten von Tags mit dem Tag Editor

Nachdem Sie Ressourcen gefunden haben, die Sie markieren möchten, können Sie die Tags für einige oder alle Ihrer Suchergebnisse hinzufügen, entfernen und bearbeiten. Der Tag-Editor zeigt

Ihnen alle Tags an, die an -Ressourcen angefügt sind. Es zeigt Ihnen auch, ob diese Tags im Tag Editor, über die Servicekonsole der Ressource oder mithilfe der API hinzugefügt wurden.

> **Important**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Wir verwenden Tags, um Ihnen Fakturierungs- und Verwaltungsservices zur Verfügung zu stellen. Tags sind nicht für private oder vertrauliche Daten gedacht.

> **Andere Möglichkeiten zur Verwaltung Ihrer Tags**
>
> In diesem Thema wird das Markieren von Ressourcen mithilfe des Tag-Editors im behandeltAWS Management Console. Sie können die Tags auf Ihren AWS Ressourcen jedoch auch mithilfe der folgenden Tools verwalten:
>
> - Sie können - oder -Skriptbefehle an Ihrer Shell-Eingabeaufforderung eingeben, indem Sie die `resourcegroupstaggingapi` Befehle in der AWS Command Line Interface (AWS CLI) verwenden.
> - Sie können PowerShellSkripts mithilfe der AWS Resource Groups Tagging-API in der erstellen und ausführenAWS Tools for PowerShell Core.
> - Sie können Programme mit jedem der verfügbaren AWS SDKs erstellen und ausführen, indem Sie die Ressourcengruppen-Tagging-APIs verwenden, z. B. die Tagging-APIs für Python oder die Tagging-APIs für Java .

Wenn Sie vorhandene Tags hinzufügen, entfernen oder bearbeiten, ändern Sie Tags nur für die Ressourcen, die Sie in den Ergebnissen Ihrer Abfrage Nach Ressourcen zum Markieren suchen auswählen. Sie können bis zu 500 Ressourcen auswählen, um ihre Tags zu verwalten.

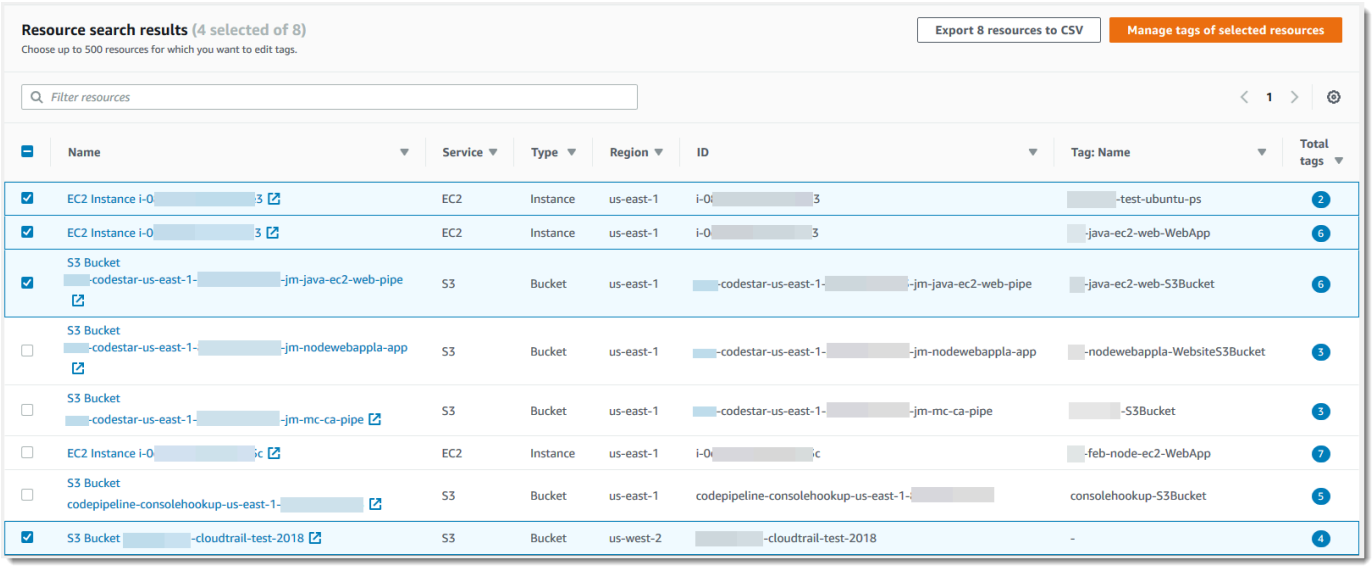
Themen

Hinzufügen von Tags zu ausgewählten Ressourcen

Sie können mit Tag Editor Tags zu ausgewählten Ressourcen hinzufügen, die in den Ergebnissen Ihrer Abfrage Find resources to tag (Ressourcen suchen, die markiert werden sollen) enthalten sind.

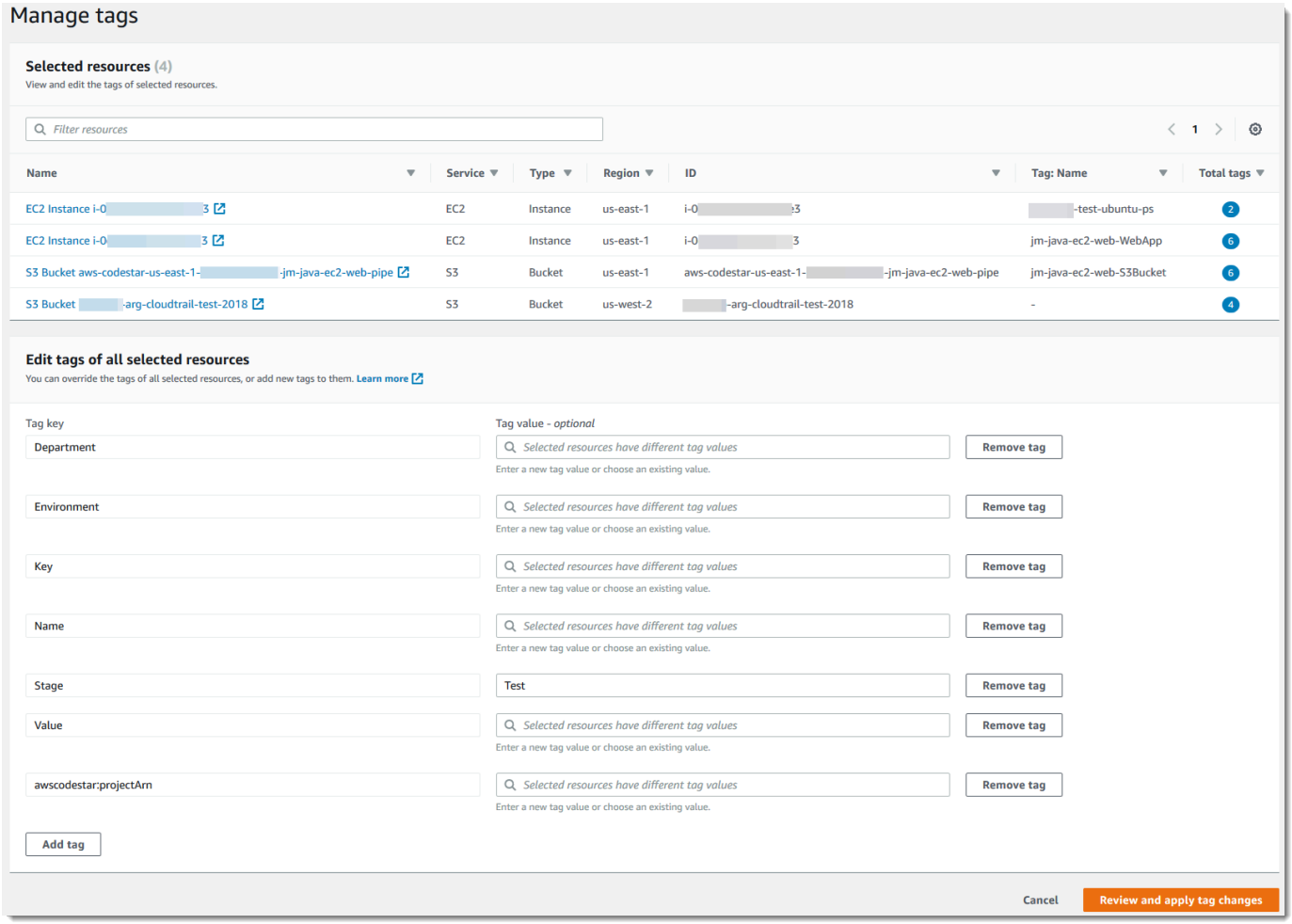
> **Note**
>
> In diesem Thema wird beschrieben, wie Sie die Tags für mehrere Ressourcen massenweise bearbeiten. Sie können auch die Tag-Werte für eine einzelne Ressource bearbeiten. Weitere Informationen finden Sie unter Anzeigen und Bearbeiten von Tags für eine ausgewählte Ressource.

1. Öffnen Sie die Tag-Editor-Konsole und senden Sie eine Abfrage, die mehrere Ressourcen zurückgibt, die Sie markieren möchten.
2. Aktivieren Sie in der Ergebnistabelle Ihrer Abfrage Nach zu markierenden Ressourcen suchen die Kontrollkästchen neben den Ressourcen, denen Sie Tags hinzufügen möchten. Geben Sie unter Filterressourcen oben in der Tabelle eine Textzeichenfolge ein, um nach einem Teil des Namens, der ID, der Tag-Schlüssel oder der Tag-Werte einer Ressource zu filtern. Beachten Sie in der Spalte Tags (Tags), dass auf die Ressourcen in den Ergebnissen bereits Tags angewendet wurden. Im folgenden Beispiel hat die erste EC2-Instance in der Liste bereits zwei Tags.

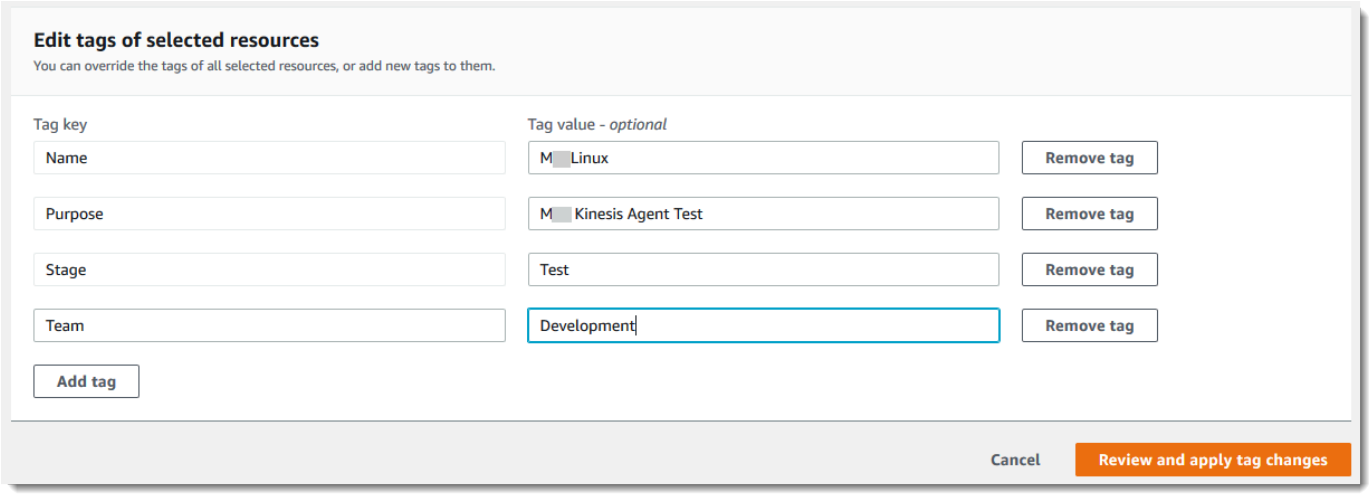


3. Aktivieren Sie das Kontrollkästchen für eine oder mehrere Ressourcen und wählen Sie dann Tags der ausgewählten Ressourcen verwalten aus.

4. Zeigen Sie auf der unten gezeigten Seite Tags verwalten die Tags auf den von Ihnen ausgewählten Ressourcen an. Obwohl Ihre ursprüngliche Abfrage mehr Ressourcen zurückgegeben hat, fügen Sie Tags nur zu den Ressourcen hinzu, die Sie in Schritt 1 ausgewählt haben. Wählen Sie Add tag.



5. Geben Sie einen Tag-Schlüssel und einen optionalen Tag-Wert ein. Für dieses Verfahren fügen Sie den Tag-Schlüssel **`Team`** und den Tag-Wert hinzu**`Development`**.



> **Note**
>
> Eine Ressource kann bis zu 50 Tags besitzen, die von Benutzern auf sie angewendet wurden. Möglicherweise können Sie einer Ressource keine neuen Tags hinzufügen, wenn Sie sich 50 vom Benutzer angewendeten Tags nähern. Von AWS generierte Tags gelten nicht für das Limit von 50 Tags. Tag-Schlüssel müssen darüber hinaus innerhalb der von Ihnen ausgewählten Ressourcen eindeutig sein. Sie können kein neues Tag mit einem Schlüssel hinzufügen, der einem Tag-Schlüssel entspricht, der bereits in den von Ihnen ausgewählten Ressourcen vorhanden ist.

6. Wenn Sie mit dem Hinzufügen von Tags fertig sind, wählen Sie Änderungen überprüfen und anwenden aus.
7. Wenn Sie die Änderungen akzeptieren, wählen Sie Apply changes to all selected (Änderungen auf gesamte Auswahl anwenden) aus.
8. Abhängig von der Anzahl der ausgewählten Ressourcen kann das Anwenden neuer Tags einige Minuten dauern. Verlassen Sie die Seite nicht und öffnen Sie keine andere Seite auf derselben Browser-Registerkarte. Wenn die Änderungen erfolgreich waren, wird oben auf der Seite ein grünes Erfolgs-Banner angezeigt. Warten Sie auf die Anzeige des Banners für Erfolg oder Misserfolg, bevor Sie fortfahren.

   Wenn Tag-Änderungen an einigen oder allen Ressourcen nicht erfolgreich waren, finden Sie weitere Informationen unter Fehlerbehebung bei Tag-Änderungen. Nachdem Sie die erfolglosen Tag-Änderungen behoben haben (z. B. unzureichende Berechtigungen), können Sie die Tag-Änderungen für Ressourcen wiederholen, für die Tag-Änderungen fehlgeschlagen sind.

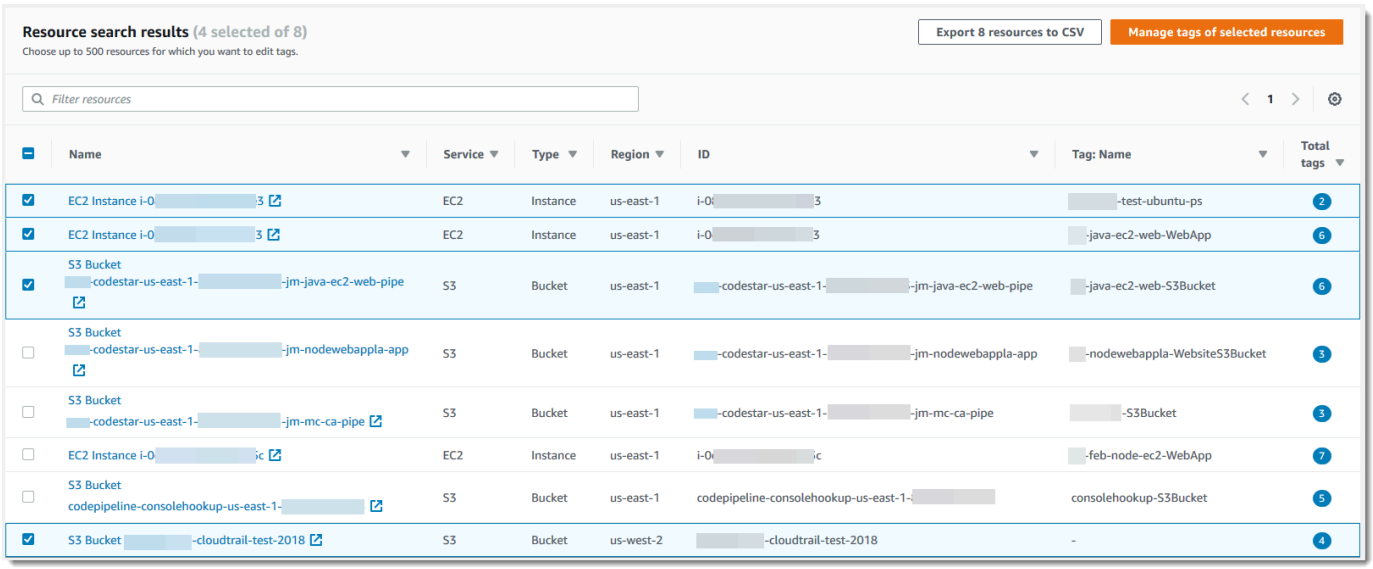
Weitere Informationen finden Sie unter the section called “Wiederholen fehlgeschlagener Tag-Änderungen”.

Bearbeiten von Tags ausgewählter Ressourcen

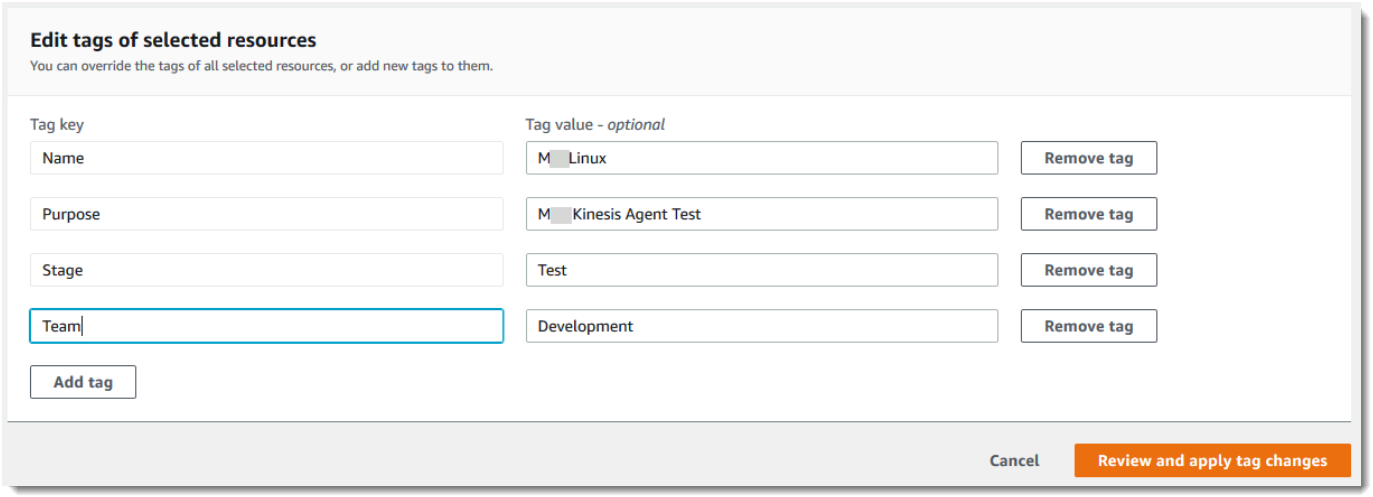
Sie können im Tag Editor vorhandene Tag-Werte für ausgewählte Ressourcen ändern, die in den Ergebnissen Ihrer AbfrageFind resources to tag (Ressourcen suchen, die markiert werden sollen) enthalten sind. Durch das Bearbeiten eines Tags wird der Tag-Wert für alle ausgewählten Ressourcen geändert, die denselben Schlüssel besitzen. Sie können einen Tag-Schlüssel nicht umbenennen, aber Sie können ein Tag löschen und ein Tag mit einem neuen Namen erstellen, um den ursprünglichen Tag-Schlüssel zu ersetzen. Hierdurch werden alle Tags mit diesem Schlüssel für die ausgewählten Ressourcen gelöscht.

> **Important**
>
> Speichern Sie keine personenbezogenen Daten (PII) oder andere vertrauliche Informationen in Tags. Wir verwenden Tags, um Ihnen Fakturierungs- und Verwaltungsservices zur Verfügung zu stellen. Tags sind nicht für private oder vertrauliche Daten gedacht.

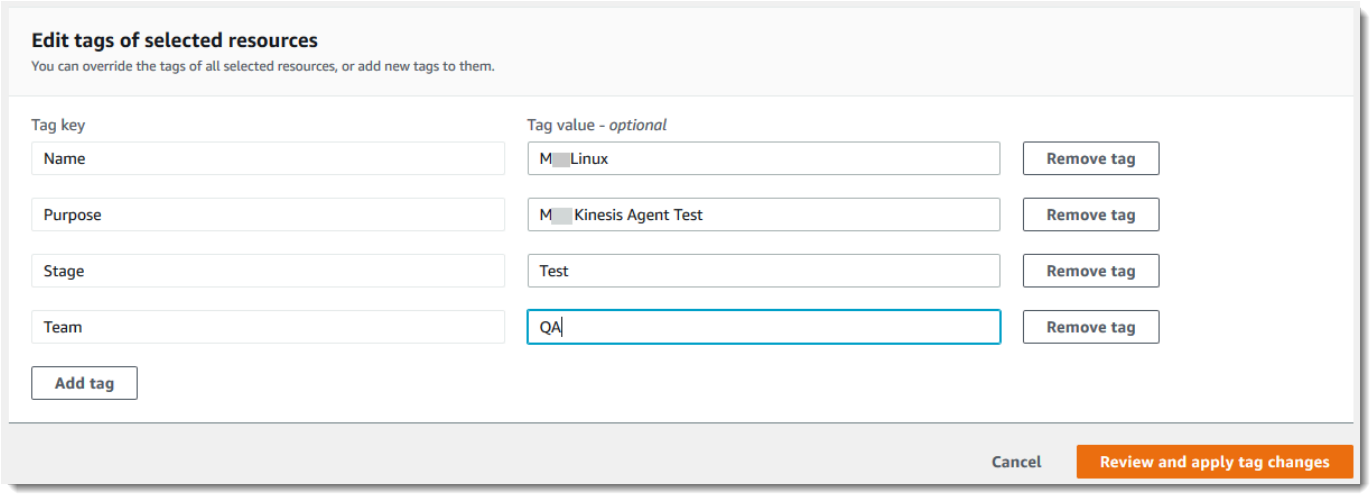
1. Aktivieren Sie in den Ergebnissen Ihrer Abfrage Find resources to tag (Ressourcen suchen, die markiert werden sollen)die Kontrollkästchen neben den Ressourcen, für die Sie vorhandene Tags ändern möchten. Geben Sie eine Textzeichenfolge in Filter resources (Ressourcen filtern) ein, um nach einem Teil des Namens oder nach der ID einer Ressource zu filtern. Beachten Sie in der Spalte Tags (Tags), dass auf die Ressourcen in den Ergebnissen bereits Tags angewendet wurden. Im folgenden Beispiel besitzt die erste ausgewählte EC2-Instance bereits über zwei Tags.



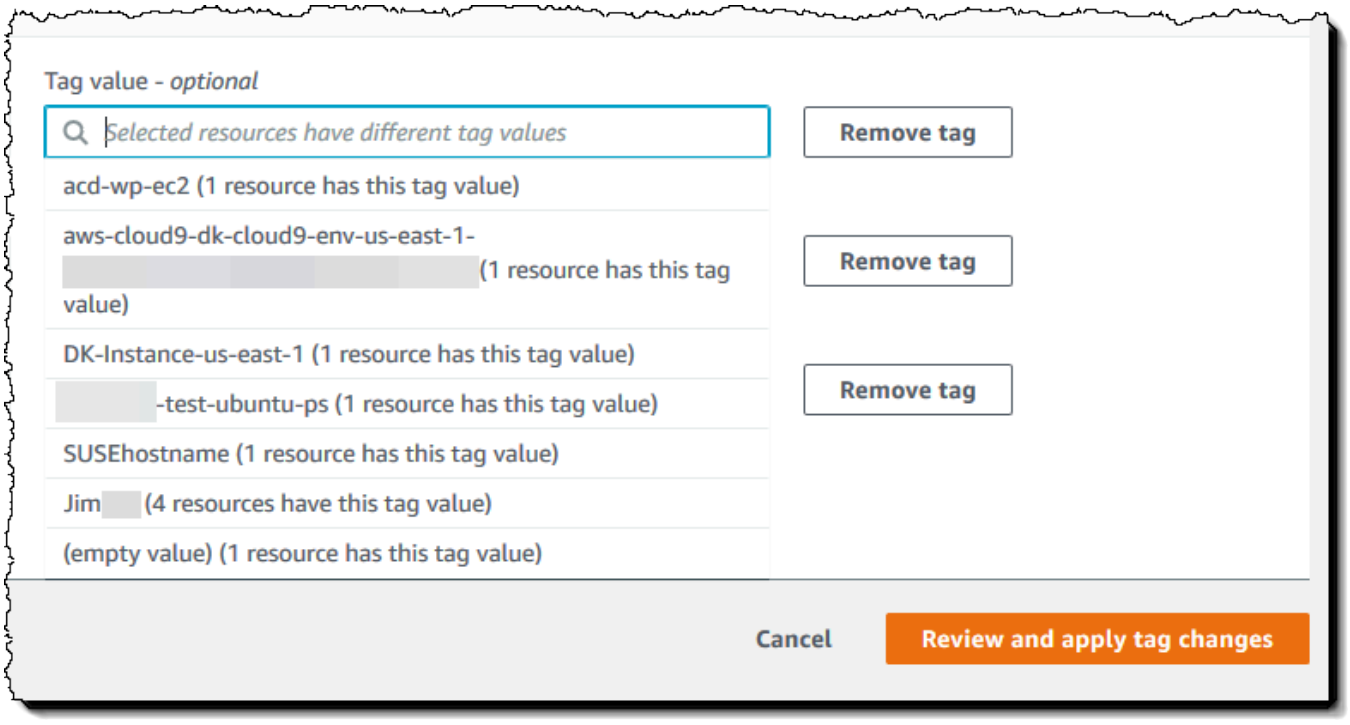
2. Wählen Sie Manage tags of the selected resources (Tags der ausgewählten Ressourcen verwalten) aus.
3. Zeigen Sie auf der Seite Manage Tags (Tags verwalten in Edit tags of selected resources (Tags ausgewählter Ressourcen bearbeiten) die Tags für die von Ihnen ausgewählte Ressource an. Obwohl Ihre ursprüngliche Abfrage möglicherweise mehr Ressourcen zurückgegeben hat, ändern Sie Tags nur für die Ressourcen, die Sie in Schritt 1 ausgewählt haben.



4. Fügen Sie Tag-Werte hinzu und ändern oder löschen Sie Tag-Werte. Vorhandene Tags müssen einen Tag-Schlüssel besitzen. Tag-Werte sind jedoch optional. In diesem Verfahren ändern wir den Wert des -**`Team`**Tags in **`QA`**.



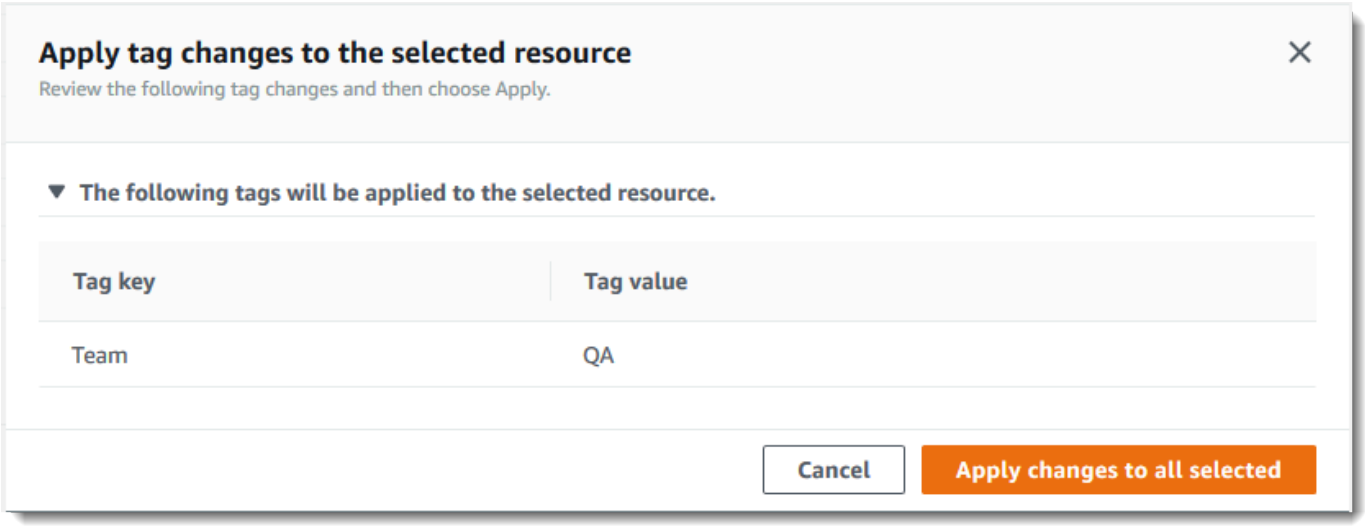
Wenn Ressourcen in Ihrer Auswahl unterschiedliche Werte für denselben Schlüssel haben, werden Ausgewählte Ressourcen mit unterschiedlichen Tag-Werten im Feld Tag-Wert angezeigt. In diesem Fall wird durch das Platzieren des Cursors im Feld eine Dropdown-Liste aller verfügbaren Werte für diesen Tag-Schlüssel in den von Ihnen ausgewählten Ressourcen geöffnet.



Wenn Ressourcen in Ihrer Auswahl den von Ihnen gewünschten Tag-Wert besitzen, wird der Tag-Wert hervorgehoben, während Sie diesen eingeben. Wenn Ressourcen in Ihrer Auswahl beispielsweise bereits den Tag-Wert **QA** besitzen, wird der Wert hervorgehoben , während Sie **Q**

eingeben. Die Werte in der Dropdown-Liste tragen dazu bei, Tag-Werte ressourcenübergreifend konsistent zu halten. Der Tag-Wert wird für alle ausgewählten Ressourcen geändert. In diesem Beispiel wird der Tag-Wert in **`QA`** für alle ausgewählten Ressourcen mit dem Tag-Schlüssel **`Team`** geändert. Für ausgewählte Ressourcen, die das **`Team`** Tag nicht haben, **`QA`** wird das **`Team`** Tag mit dem Wert hinzugefügt.

5. Wenn Sie mit dem Ändern von Tags fertig sind, wählen Sie Änderungen überprüfen und anwenden aus.
6. Wenn Sie die Änderungen akzeptieren, wählen Sie Apply changes to all selected (Änderungen auf gesamte Auswahl anwenden) aus.



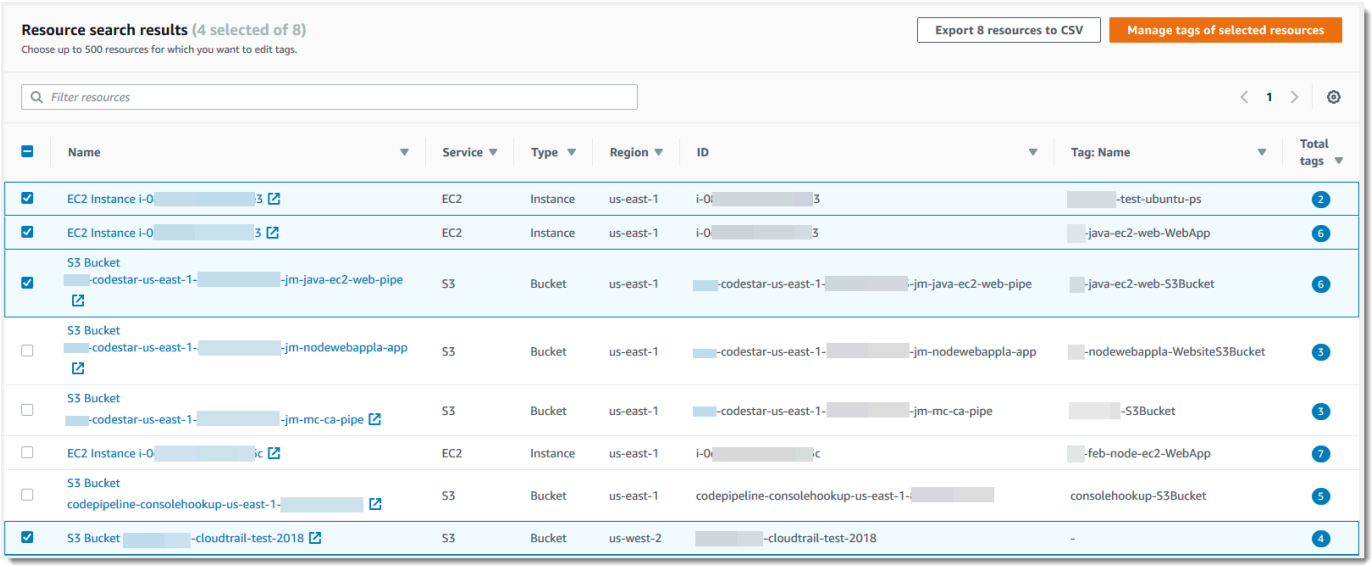
7. Abhängig von der Anzahl der von Ihnen ausgewählten Ressourcen, kann das Bearbeiten der Tags einige Minuten in Anspruch nehmen. Verlassen Sie die Seite nicht und öffnen Sie keine andere Seite auf derselben Browser-Registerkarte. Wenn die Änderungen erfolgreich waren, wird oben auf der Seite ein grünes Erfolgs-Banner angezeigt. Warten Sie auf die Anzeige des Banners für Erfolg oder Misserfolg, bevor Sie fortfahren.

   Wenn Tag-Änderungen an einigen oder allen Ressourcen nicht erfolgreich waren, finden Sie weitere Informationen unter Fehlerbehebung bei Tag-Änderungen. Nachdem Sie die Ursachen für erfolglose Tag-Änderungen behoben haben (z. B. unzureichende Berechtigungen), können Sie Tag-Änderungen für Ressourcen wiederholen, für die Tag-Änderungen fehlgeschlagen sind. Weitere Informationen finden Sie unter the section called “Wiederholen fehlgeschlagener Tag-Änderungen”.

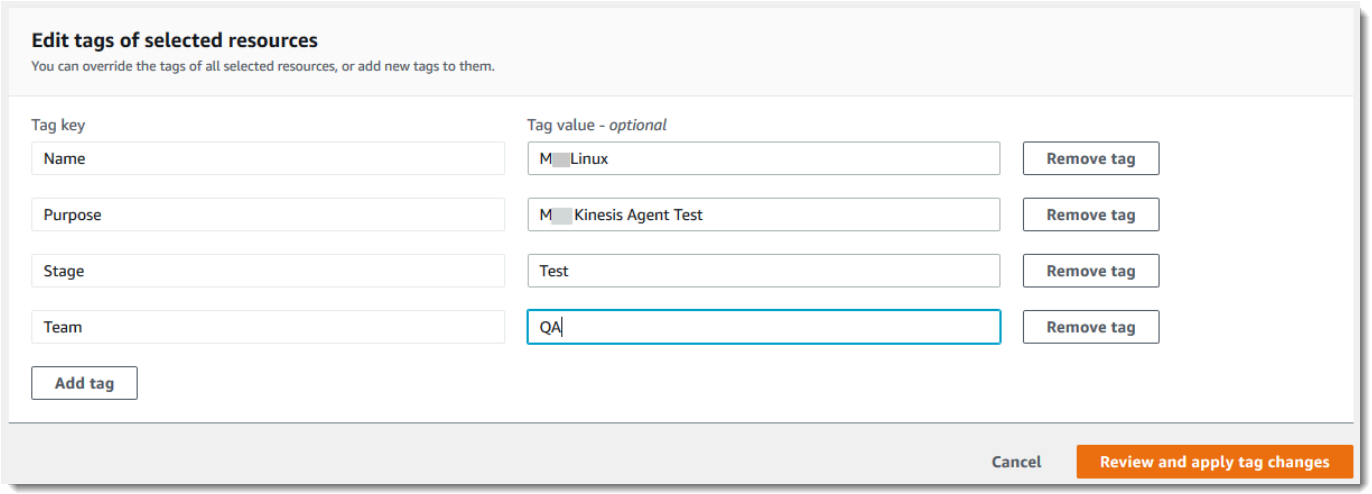
Entfernen von Tags aus ausgewählten Ressourcen

Sie können im Tag Editor Tags aus ausgewählten Ressourcen entfernen, die in den Ergebnissen Ihrer AbfrageFind resources to tag (Ressourcen suchen, die markiert werden sollen) enthalten sind. Durch das Entfernen eines Tags wird das Tag aus allen ausgewählten Ressourcen gelöscht, die dieses Tag besitzen. Da Sie Tag-Schlüssel nicht bearbeiten können, können Sie Tags entfernen und sie durch neue Tags ersetzen, wenn Sie einen Tag-Schlüssel bearbeiten müssen. Hierdurch werden alle Tags mit diesem Schlüssel für die ausgewählten Ressourcen gelöscht.

1. Aktivieren Sie in den Ergebnissen Ihrer Abfrage Find resources to tag (Ressourcen suchen, die markiert werden sollen) die Kontrollkästchen neben den Ressourcen, aus denen Sie Tags entfernen möchten. Geben Sie eine Textzeichenfolge in Filter resources (Ressourcen filtern) ein, um nach einem Teil des Namens oder nach der ID einer Ressource zu filtern.

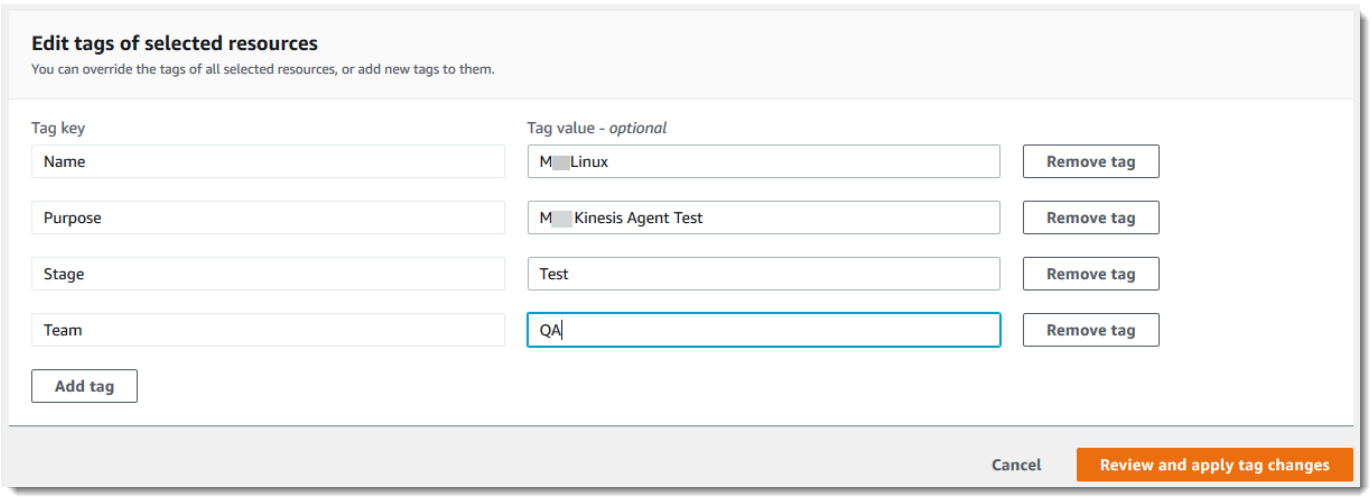


2. Wählen Sie Manage tags of the selected resources (Tags der ausgewählten Ressourcen verwalten) aus.
3. Zeigen Sie auf der Seite Manage Tags (Tags verwalten in Edit tags of selected resources (Tags ausgewählter Ressourcen bearbeiten) die Tags für die von Ihnen ausgewählten Ressourcen an. Obwohl Ihre ursprüngliche Abfrage möglicherweise mehr Ressourcen zurückgegeben hat, ändern Sie Tags nur für die Ressourcen, die Sie in Schritt 1 ausgewählt haben.



4. Wählen Sie Remove tag (Tag entfernen) neben allen Tags aus, die Sie löschen möchten. In diesem Verfahren entfernen wir das -**`Team`**Tag.

> **Note**
>
> Durch Auswählen von Remove tag (Tag entfernen) wird ein Tag aus allen ausgewählten Ressourcen entfernt, die das Tag besitzen. Im gezeigten Beispiel wird das Tag **`Team`** aus allen ausgewählten Ressourcen entfernt, die das Tag **`Team`** zurzeit besitzen, unabhängig vom Tag-Wert.



5. Wählen Sie Review and apply changes (Änderungen prüfen und anwenden) aus.
6. Wählen Sie auf der Bestätigungsseite Apply changes to all selected (Änderungen auf gesamte Auswahl anwenden) aus.

7. Abhängig von der Anzahl der von Ihnen ausgewählten Ressourcen, kann das Entfernen von Tags einige Minuten in Anspruch nehmen. Verlassen Sie die Seite nicht und öffnen Sie keine andere Seite auf derselben Browser-Registerkarte. Wenn die Änderungen erfolgreich waren, wird oben auf der Seite ein grünes Erfolgs-Banner angezeigt. Warten Sie auf die Anzeige des Banners für Erfolg oder Misserfolg, bevor Sie fortfahren.

   Wenn die Tag-Änderungen für einige oder alle Ressourcen nicht erfolgreich waren, finden Sie unter Beheben von Fehlern bei Tag-Änderungen entsprechende Informationen. Nachdem Sie die Ursachen für erfolglose Tag-Änderungen behoben haben (z. B. unzureichende Berechtigungen), können Sie Tag-Änderungen für Ressourcen wiederholen, für die Tag-Änderungen fehlgeschlagen sind. Weitere Informationen finden Sie unter the section called “Wiederholen fehlgeschlagener Tag-Änderungen”.

Wiederholen fehlgeschlagener Tag-Änderungen

Wenn für mindestens eine der von Ihnen ausgewählten Ressourcen Tag-Änderungen fehlgeschlagen sind, zeigt Tag Editor unten auf der Seite ein rotes Banner an. Das Banner zeigt eine Fehlermeldung für jede Art von Fehler, die auftritt. Für jeden Fehler identifiziert das Banner die spezifischen Ressourcen, für die der Tag-Editor keine Tag-Änderungen vornehmen konnte. Nachdem Sie die Fehler überprüft und behoben haben, wählen Sie Fehlgeschlagene Tag-Änderungen für Ressourcen wiederholen, um Änderungen nur für die Ressourcen zu wiederholen, bei denen Tag-Änderungen fehlgeschlagen sind.

Ähnliche Informationen

- Verwenden von Kostenzuordnungs-Tags im AWS Billing-Benutzerhandbuch

Verwenden von Tags in IAM-Berechtigungsrichtlinien

AWS Identity and Access Management (IAM) ist die AWS-Service, mit der Sie Berechtigungsrichtlinien erstellen und verwalten, die festlegen, wer auf Ihre -AWSRessourcen zugreifen kann. Jeder Versuch, auf einen -AWSService zuzugreifen oder eine -AWSRessource zu lesen oder zu schreiben, wird durch eine IAM-Richtlinie gesteuert.

Mit diesen Richtlinien können Sie einen detaillierten Zugriff auf Ihre -Ressourcen ermöglichen. Eine der Funktionen, mit denen Sie diesen Zugriff optimieren können, ist das `Condition` Element der Richtlinie. Mit diesem Element können Sie die Bedingungen angeben, die mit der Anforderung

übereinstimmen müssen, um festzustellen, ob die Anforderung fortgesetzt werden kann. Zu den Dingen, die Sie mit dem -`Condition`Element überprüfen können, gehören die folgenden:

- Tags, die dem Benutzer oder der Rolle angefügt sind, der/die die Anforderung stellt.
- Tags, die an die Ressource angehängt sind, die das Objekt der Anforderung ist.

Tag-bezogene Bedingungsschlüssel

Die folgende Tabelle beschreibt die Bedingungsschlüssel, die Sie in einer IAM-Berechtigungsrichtlinie verwenden können, um den Zugriff basierend auf Tags zu steuern. Mit diesen Bedingungsschlüsseln können Sie Folgendes tun:

- Vergleichen Sie die Tags auf dem Prinzipal, der die -Operation aufruft.
- Vergleichen Sie die Tags, die der Operation zur Verfügung gestellt werden, als Parameter.
- Vergleichen Sie die Tags, die an die Ressource angehängt sind, auf die der Vorgang zugreifen würde.

Ausführliche Informationen zu einem Bedingungsschlüssel und dessen Verwendung finden Sie auf der Seite, die in der Spalte Name des Bedingungsschlüssels verknüpft ist.

Name des Bedingungsschlüssels	Beschreibung
aws:PrincipalTag	Vergleicht das Tag, das dem Prinzipal (IAM-Rolle oder Benutzer) angefügt ist, der die Anforderung stellt, mit dem Tag, das Sie in der Richtlinie angeben.
aws:RequestTag	Vergleicht das Tag-Schlüssel-Wert-Paar, das als Parameter an die Anforderung übergeben wurde, mit dem Tag-Schlüssel-Wert-Paar, das Sie in der Richtlinie angeben.
aws:ResourceTag	Vergleicht das Schlüssel-Wert-Paar, das der Ressource angefügt ist, mit dem Tag-Schlüssel-Wert-Paar, das Sie in der Richtlinie angeben.
aws:TagKeys	Vergleicht nur die Tag-Schlüssel in der Anforderung mit den Schlüsseln, die Sie in der Richtlinie angeben.

Beispiel für IAM-Richtlinien, die Tags verwenden

Example Beispiel 1: Benutzer zwingen, ein bestimmtes Tag anzufügen, wenn sie eine Ressource erstellen

Das folgende Beispiel für eine IAM-Berechtigungsrichtlinie zeigt, wie der Benutzer, der die Tags einer IAM-Richtlinie erstellt oder ändert, gezwungen wird, ein Tag mit dem Schlüssel einzuschließen`0wner`. Außerdem erfordert die Richtlinie, dass der Wert des Tags auf denselben Wert wie das `0wner` Tag festgelegt ist, das derzeit dem aufrufenden Prinzipal angefügt ist. Damit diese Strategie funktioniert, muss allen Prinzipalen ein -`0wner`Tag angefügt sein, und Benutzer müssen daran gehindert werden, dieses Tag zu ändern. Wenn ein Versuch erfolgt, eine Richtlinie zu erstellen oder zu ändern, ohne das -`0wner`Tag einzuschließen, stimmt die Richtlinie nicht überein und der Vorgang ist nicht zulässig.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TagCustomerManagedPolicies",
            "Effect": "Allow",
            "Action": [
                "iam:CreatePolicy",
                "iam:TagPolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:policy/*",
            "Condition": {
                "StringEquals": {"aws:RequestTag/Owner": "${aws:PrincipalTag/Owner}"}
            }
        }
    ]
}
```

Example Beispiel 2: Verwenden von Tags, um den Zugriff auf eine Ressource auf ihren „Eigentümer“ zu beschränken

Mit der folgenden Beispiel-IAM-Berechtigungsrichtlinie kann der Benutzer eine ausgeführte Amazon EC2-Instance nur anhalten, wenn der aufrufende Prinzipal mit demselben `project` Tag-Wert wie die Instance gekennzeichnet ist.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances"
      ],
      "Resource": [
        "arn:aws:iam::123456789012:instance/*"
      ],
      "Condition": {
        "StringEquals": {"aws:ResourceTag/project": "${aws:PrincipalTag/project}"}
      }
    }
  ]
}
```

Dieses Beispiel ist ein Beispiel für die attributbasierte Zugriffskontrolle (ABAC). Weitere Informationen und zusätzliche Beispiele für die Verwendung von IAM-Richtlinien zur Implementierung einer Tag-basierten Zugriffskontrollstrategie finden Sie in den folgenden Themen im AWS Identity and Access Management -Benutzerhandbuch:

- Steuern des Zugriffs auf AWS-Ressourcen mithilfe von Tags
- Steuern des Zugriffs auf und für IAM-Benutzer und -Rollen mithilfe von Tags
- IAM-Tutorial: Definieren von Berechtigungen für den Zugriff auf AWS Ressourcen basierend auf Tags – Zeigt, wie Sie mithilfe mehrerer Tags Zugriff auf verschiedene Projekte und Gruppen gewähren.

AWS Organizations Tag-Richtlinien

Eine Tag-Richtlinie ist eine Art von Richtlinie, die Sie in erstellenAWS Organizations. Sie können Tag-Richtlinien verwenden, um Tags für alle Ressourcen in den Konten Ihrer Organisation zu standardisieren. Um Tag-Richtlinien zu verwenden, empfehlen wir Ihnen, die unter Erste Schritte mit Tag-Richtlinien im AWS Organizations -Benutzerhandbuch beschriebenen Workflows zu befolgen. Wie auf dieser Seite erwähnt, umfassen die empfohlenen Workflows das Suchen und Korrigieren von nicht konformen Tags. Um diese Aufgaben auszuführen, verwenden Sie die Tag-Editor-Konsole.

Themen

Voraussetzungen und Berechtigungen

Bevor Sie die Compliance mit Tag-Richtlinien im Tag Editor bewerten können, müssen Sie die Anforderungen erfüllen und die erforderlichen Berechtigungen festlegen.

Voraussetzungen für die Bewertung der Compliance mit Tag-Richtlinien

Die Bewertung der Compliance mit Tag-Richtlinien erfordert Folgendes:

- Sie müssen zuerst die Funktion in aktivieren AWS Organizationsund Tag-Richtlinien erstellen und anfügen. Weitere Informationen finden Sie auf den folgenden Seiten im AWS Organizations - Benutzerhandbuch:
  - Voraussetzungen und Berechtigungen für die Verwaltung von Tag-Richtlinien
  - Aktivieren von Tag-Richtlinien
  - Erste Schritte mit Tag-Richtlinien
- Um nicht konforme Tags für die Ressourcen eines Kontos zu finden, benötigen Sie Anmeldeinformationen für dieses Konto und die unter aufgeführten BerechtigungenBerechtigungen zum Auswerten der Compliance für ein Konto.
- Um die unternehmensweite Compliance zu bewerten, benötigen Sie Anmeldeinformationen für das Verwaltungskonto der Organisation und die unter aufgeführten BerechtigungenBerechtigungen zur Bewertung der organisationsweiten Compliance . Sie können den Compliance-Bericht nur von der AWS-Region USA Ost (Nord-Virginia) anfordern.

Berechtigungen zum Auswerten der Compliance für ein Konto

Das Suchen nicht konformer Tags für die Ressourcen eines Kontos erfordert die folgenden Berechtigungen:

- `organizations:DescribeEffectivePolicy` – Um den Inhalt der effektiven Tag-Richtlinie für das Konto abzurufen.
- `tag:GetResources` – Zum Abrufen einer Liste von Ressourcen, die nicht der angehängten Tag-Richtlinie entsprechen.

- `tag:TagResources` – Zum Hinzufügen oder Aktualisieren von Tags. Sie benötigen auch servicespezifische Berechtigungen, um Tags zu erstellen. Um beispielsweise Ressourcen in Amazon Elastic Compute Cloud (Amazon EC2) zu markieren, benötigen Sie Berechtigungen für `ec2:CreateTags`.
- `tag:UnTagResources` – Zum Entfernen eines Tags. Sie benötigen auch servicespezifische Berechtigungen, um Tags zu entfernen. Um beispielsweise die Markierung von Ressourcen in Amazon EC2 aufzuheben, benötigen Sie Berechtigungen für `ec2:DeleteTags`.

Die folgende Beispielrichtlinie AWS Identity and Access Management (IAM) bietet Berechtigungen zum Auswerten der Tag-Compliance für ein Konto.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EvaluateAccountCompliance",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeEffectivePolicy",
                "tag:GetResources",
                "tag:TagResources",
                "tag:UnTagResources"
            ],
            "Resource": "*"
        }
    ]
}
```

Weitere Informationen zu IAM-Richtlinien und -Berechtigungen finden Sie im IAM-Benutzerhandbuch.

Berechtigungen zur Bewertung der organisationsweiten Compliance

Die Bewertung der organisationsweiten Compliance mit Tag-Richtlinien erfordert die folgenden Berechtigungen:

- `organizations:DescribeEffectivePolicy` – Um den Inhalt der Tag-Richtlinie abzurufen, die der Organisation, der Organisationseinheit (OU) oder dem Konto zugeordnet ist.
- `tag:GetComplianceSummary` – Zum Abrufen einer Zusammenfassung der nicht konformen Ressourcen in allen Konten in der Organisation.

- `tag:StartReportCreation` – Zum Exportieren der Ergebnisse der letzten Compliance-Bewertung in eine Datei. Die unternehmensweite Compliance wird alle 48 Stunden bewertet.
- `tag:DescribeReportCreation` – Um den Status der Berichtserstellung zu überprüfen.

Die folgende Beispiel-IAM-Richtlinie bietet Berechtigungen für die Bewertung der organisationsweiten Compliance.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EvaluateOrgCompliance",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeEffectivePolicy",
                "tag:GetComplianceSummary",
                "tag:StartReportCreation",
                "tag:DescribeReportCreation"
            ],
            "Resource": "*"
        }
    ]
}
```

Weitere Informationen zu IAM-Richtlinien und -Berechtigungen finden Sie im IAM-Benutzerhandbuch.

Amazon S3-Bucket-Richtlinie für die Berichtsspeicherung

Um einen organisationsweiten Compliance-Bericht zu erstellen, müssen Sie Zugriff für den Service-Prinzipal für Tag-Richtlinien auf einen Amazon Simple Storage Service (Amazon S3)-Bucket in der Region USA Ost (Nord-Virginia) zur Berichtsspeicherung gewähren. Fügen Sie dem Bucket die folgende Bucket-Richtlinie an und ersetzen Sie jeden *`Platzhalter`* durch Ihre eigenen Informationen:

- Ihr S3-Bucket-Name
- ID-Nummer der Organisation
- Konto-ID-Nummer des Verwaltungskontos der Organisation für die Organisation, in der Sie die Richtlinie anwenden

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TagPolicyACL",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "tagpolicies.tag.amazonaws.com"
                 ]
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::<your-bucket-name>",
            "Condition": {
                "StringLike": {
                    "aws:SourceAccount": "<organization-management-account-id>",
                    "aws:SourceArn": "arn:aws:tag:us-east-1:<organization-management-
account-id>:*"
                }
            }
         },
         {
            "Sid": "TagPolicyBucketDelivery",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "tagpolicies.tag.amazonaws.com"
                 ]
            },
            "Action": [
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::<your-bucket-name>/AwsTagPolicies/<your-
organization-id>/*",
            "Condition": {
                "StringLike": {
                    "aws:SourceAccount": "<organization-management-account-id>",
                    "aws:SourceArn": "arn:aws:tag:us-east-1:<organization-management-
account-id>:*"
                }
            }
         }
```

```
    ]
}
```

Bewertung der Compliance für ein Konto

Sie können die Compliance eines Kontos in Ihrer Organisation mit seiner effektiven Tag-Richtlinie bewerten.

> **Important**
>
> Ressourcen ohne Tags werden in den Ergebnisses nicht als nichtkonform angezeigt. Um nicht markierte Ressourcen in Ihrem Konto zu finden, verwenden Sie AWS Ressourcen Explorer mit einer Abfrage, die verwendet**`tag:none`**. Weitere Informationen finden Sie unter Suchen nach nicht markierten Ressourcen im AWS Ressourcen Explorer - Benutzerhandbuch.

Die effektive Tag-Richtlinie gibt die Tagging-Regeln an, die für ein Konto gelten. Die effektive Tag-Richtlinie ist die Aggregation aller Tag-Richtlinien, die das Konto erbt, sowie aller Tag-Richtlinien, die direkt an das Konto angefügt sind. Wenn Sie dem Organisationsstamm eine Tag-Richtlinie hinzufügen, gilt dies für alle Konten in Ihrer Organisation. Wenn Sie eine Tag-Richtlinie an eine Organisationseinheit (OU) anfügen, gilt sie für alle Konten und OUs, die zur OU gehören.

> **Note**
>
> Wenn Sie noch keine Tag-Richtlinien erstellt haben, finden Sie weitere Informationen unter Erste Schritte mit Tag-Richtlinien im AWS Organizations -Benutzerhandbuch.

Um nicht konforme Tags zu finden, müssen Sie über die folgenden Berechtigungen verfügen:

- `organizations:DescribeEffectivePolicy`
- `tag:GetResources`
- `tag:TagResources`
- `tag:UntagResources`

So bewerten Sie die Compliance eines Kontos mit seiner effektiven Tag-Richtlinie (Konsole)

1. Öffnen Sie die Tag-Richtlinien-Konsole, während Sie bei dem Konto angemeldet sind, dessen Compliance Sie überprüfen möchten.
2. Der Abschnitt Effektive Tag-Richtlinie zeigt an, wann die Richtlinie zuletzt aktualisiert wurde, und die definierten Tag-Schlüssel. Sie können einen Tag-Schlüssel erweitern, um Informationen zu seinen Werten, der Fallbehandlung und ob die Werte für bestimmte Ressourcentypen erzwungen werden, anzuzeigen.

   > **Note**
   >
   > Wenn Sie beim Verwaltungskonto angemeldet sind, müssen Sie ein Konto auswählen, um die effektive Richtlinie und die Compliance-Informationen anzuzeigen.

3. Geben Sie im Abschnitt Ressourcen mit nicht konformen Tags an, welche nach nicht konformen Tags gesucht AWS-Region werden soll. Optional können Sie auch nach Ressourcentyp suchen. Wählen Sie dann Ressourcen suchen aus.

   Echtzeitergebnisse werden im Abschnitt Suchergebnisse angezeigt.
   Um die Anzahl der pro Seite zurückgegebenen Ergebnisse oder die anzuzeigenden Spalten zu ändern, wählen Sie das Einstellungssymbol ().
4. Wählen Sie in den Suchergebnissen eine Ressource mit nicht konformen Tags aus.
5. Wählen Sie im Dialogfeld, das die Tags der Ressource auflistet, den Hyperlink aus, um die zu öffnen, AWS-Service in der die Ressource erstellt wurde. Korrigieren Sie von dieser Konsole aus das nicht konforme Tag.

   > **Tip**
   >
   > Wenn Sie sich nicht sicher sind, welche Tags nicht konform sind, gehen Sie in der Konsole Tag-Richtlinien zum Abschnitt Effektive Tag-Richtlinie für das Konto. Sie können einen Tag-Schlüssel erweitern, um seine Tagging-Regeln anzuzeigen.

6. Wiederholen Sie den Vorgang zum Suchen und Korrigieren von Tags, bis die Kontoressourcen, die Ihnen wichtig sind, in jeder Region konform sind.

So finden Sie nicht konforme Tags (AWS CLI, AWS API)

Verwenden Sie die folgenden Befehle und Operationen, um nicht konforme Tags zu finden:

- AWS Command Line Interface (AWS CLI):
  - aws resourcegroupstaggingapi get-resources
  - aws resourcegroupstaggingapi tag-resources
  - aws resourcegroupstaggingapi untag-resources

  Das vollständige Verfahren zur Verwendung von Tag-Richtlinien in der AWS CLIfinden Sie unter Verwenden von Tag-Richtlinien im AWS CLI im AWS Organizations -Benutzerhandbuch.
- AWS Resource Groups Tagging API:
  - GetResources
  - TagResources
  - UntagResources

Nächste Schritte

Wir empfehlen Ihnen, den Vorgang der Suche und Behebung von Compliance-Problemen zu wiederholen. Fahren Sie fort, bis die Ressourcen des Kontos, die Ihnen wichtig sind, mit der effektiven Tag-Richtlinie in jeder Region konform sind.

Das Suchen und Korrigieren nicht konformer Tags ist ein iterativer Prozess aus mehreren Gründen, darunter:

- Die Verwendung von Tag-Richtlinien durch Ihre Organisation kann sich im Laufe der Zeit weiterentwickeln.
- Es dauert einige Zeit, bis Änderungen in Ihrer Organisation wirksam werden, wenn Ressourcen erstellt werden.
- Compliance kann sich jederzeit ändern, wenn eine neue Ressource erstellt oder einer Ressource neue Tags zugewiesen werden.
- Die effektive Tag-Richtlinie eines Kontos wird aktualisiert, wenn eine Tag-Richtlinie an sie angehängt oder von ihr getrennt wird. Die effektive Tag-Richtlinie wird auch aktualisiert, wenn Änderungen am Tag der Richtlinien vorgenommen werden, die das Konto erbt.

Wenn Sie als Verwaltungskonto in der Organisation angemeldet sind, können Sie auch einen Bericht erstellen. Dieser Bericht enthält Informationen zu allen markierten Ressourcen in den Konten

Ihrer Organisation. Weitere Informationen finden Sie unter Bewertung der unternehmensweiten Compliance.

Bewertung der unternehmensweiten Compliance

Sie können die Compliance Ihrer Organisation mit ihrer effektiven Tag-Richtlinie bewerten. Sie können einen Bericht erstellen, der alle markierten Ressourcen in Konten in Ihrer gesamten Organisation auflistet und ob jede Ressource mit der effektiven Tag-Richtlinie konform ist.

> **Important**
>
> Ressourcen ohne Tags werden in den Ergebnisses nicht als nichtkonform angezeigt. Um nicht markierte Ressourcen in Ihrem Konto zu finden, verwenden Sie AWS Ressourcen Explorer mit einer Abfrage, die verwendet**`tag:none`**. Weitere Informationen finden Sie unter Suchen nach nicht markierten Ressourcen im AWS Ressourcen Explorer - Benutzerhandbuch.

Sie können den Bericht `us-east-1` AWS-Region nur aus dem Verwaltungskonto Ihrer Organisation in der generieren. Das Konto, das den Bericht generiert, muss Zugriff auf einen Amazon S3-Bucket in der Region USA Ost (Nord-Virginia) haben. Dem Bucket muss eine Bucket-Richtlinie angefügt sein, wie in der Amazon S3-Bucket-Richtlinie zum Speichern des Berichts gezeigt.

Um einen organisationsweiten Compliance-Bericht zu erstellen, müssen Sie über die folgenden Berechtigungen verfügen:

- `organizations:DescribeEffectivePolicy`
- `tag:StartReportCreation`
- `tag:DescribeReportCreation`
- `tag:GetComplianceSummary`

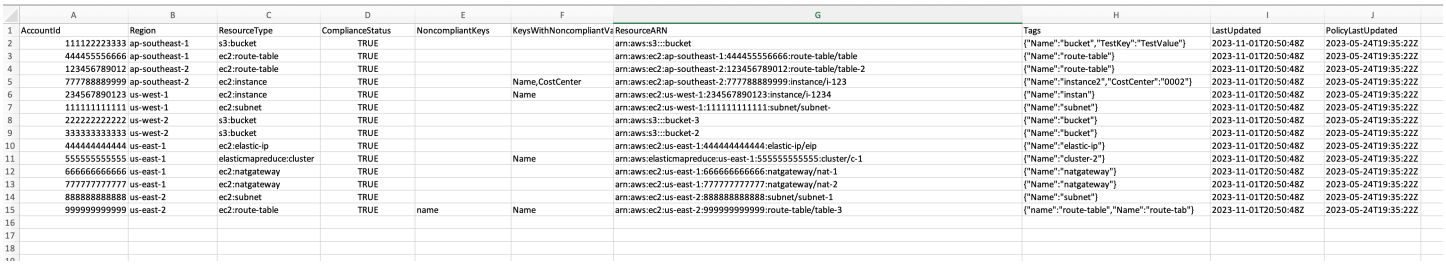
So generieren Sie einen organisationsweiten Compliance-Bericht (Konsole)

1. Öffnen Sie die Tag-Richtlinien-Konsole .
2. Wählen Sie die Registerkarte Organisationsstamm und unten auf der Seite die Option Bericht generieren aus.
3. Geben Sie auf dem Bildschirm Bericht generieren an, wo der Bericht gespeichert werden soll.

4. Wählen Sie Export starten aus.

Wenn der Bericht abgeschlossen ist, können Sie ihn im Abschnitt Bericht über Compliance-Verstöße auf der Registerkarte Organisationsstamm herunterladen.

Im Folgenden sehen Sie ein Beispiel für einen Berichtsauszug.



	A	B	C	D	E	F	G	H	I	J
1	AccountId	Region	ResourceType	ComplianceStatus	NoncompliantKeys	KeysWithNoncompliantVa	ResourceARN	Tags	LastUpdated	PolicyLastUpdated
2	111122223333	ap-southeast-1	s3:bucket	TRUE			arn:aws:s3:::bucket	{"Name":"bucket","TestKey":"TestValue"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
3	444455556666	ap-southeast-1	ec2:route-table	TRUE			arn:aws:ec2:ap-southeast-1:444455556666:route-table/table	{"Name":"route-table"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
4	123456789012	ap-southeast-2	ec2:route-table	TRUE			arn:aws:ec2:ap-southeast-2:123456789012:route-table/table-2	{"Name":"route-table"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
5	777788889999	ap-southeast-2	ec2:instance	TRUE		Name,CostCenter	arn:aws:ec2:ap-southeast-2:777788889999:instance/i-123	{"Name":"instance2","CostCenter":"0002"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
6	234567890123	us-west-1	ec2:instance	TRUE		Name	arn:aws:ec2:us-west-1:234567890123:instance/i-1234	{"Name":"instan"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
7	111111111111	us-west-1	ec2:subnet	TRUE			arn:aws:ec2:us-west-1:111111111111:subnet/subnet-	{"Name":"subnet"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
8	222222222222	us-west-2	s3:bucket	TRUE			arn:aws:s3:::bucket-3	{"Name":"bucket"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
9	333333333333	us-west-2	s3:bucket	TRUE			arn:aws:s3:::bucket-2	{"Name":"bucket"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
10	444444444444	us-east-1	ec2:elastic-ip	TRUE			arn:aws:ec2:us-east-1:444444444444:elastic-ip/eip	{"Name":"elastic-ip"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
11	555555555555	us-east-1	elasticmapreduce:cluster	TRUE		Name	arn:aws:elasticmapreduce:us-east-1:555555555555:cluster/c-1	{"Name":"cluster-2"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
12	666666666666	us-east-1	ec2:natgateway	TRUE			arn:aws:ec2:us-east-1:666666666666:natgateway/nat-1	{"Name":"natgateway"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
13	777777777777	us-east-1	ec2:natgateway	TRUE			arn:aws:ec2:us-east-1:777777777777:natgateway/nat-2	{"Name":"natgateway"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
14	888888888888	us-east-2	ec2:subnet	TRUE			arn:aws:ec2:us-east-2:888888888888:subnet/subnet-1	{"Name":"subnet"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
15	999999999999	us-east-2	ec2:route-table	TRUE	name	Name	arn:aws:ec2:us-east-2:999999999999:route-table/table-3	{"name":"route-table","Name":"route-tab"}	2023-11-01T20:50:48Z	2023-05-24T19:35:22Z
16										
17										
18										

Hinweise

Die unternehmensweite Compliance wird alle 48 Stunden bewertet. Dies führt zu Folgendem:

- Es kann bis zu 48 Stunden dauern, bis Änderungen an einer Tag-Richtlinie oder Ressourcen im organisationsweiten Compliance-Bericht angezeigt werden. Angenommen, Sie haben eine Tag-Richtlinie, die ein neues standardisiertes Tag für einen Ressourcentyp definiert. Ressourcen dieses Typs, die dieses Tag nicht haben, können bis zu 48 Stunden lang als konform im Bericht angezeigt werden.
- Sie können den Bericht zwar jederzeit erstellen, die Berichtsergebnisse werden jedoch erst aktualisiert, wenn die nächste Auswertung abgeschlossen ist.
- Die NoncompliantKeys Spalte listet Tag-Schlüssel auf der Ressource auf, die nicht mit der effektiven Tag-Richtlinie übereinstimmen.
- Die KeysWithNonCompliantValues Spalte listet die in der effektiven Richtlinie definierten Schlüssel auf, die sich auf der Ressource befinden, entweder mit falscher Fallbehandlung oder nicht konformen Werten.
- Wenn Sie ein schließenAWS-Konto, das Mitglied der Organisation war, kann es bis zu 90 Tage lang im Tag-Compliance-Bericht erscheinen.

So generieren Sie einen organisationsweiten Compliance-Bericht (AWS CLI, AWS API)

Verwenden Sie die folgenden Befehle und Operationen, um einen organisationsweiten Compliance-Bericht zu generieren, seinen Status zu überprüfen und den Bericht anzuzeigen:

- AWS Command Line Interface AWS CLI):
  - aws resourcegroupstaggingapi start-report-creation
  - aws resourcegroupstaggingapi describe-report-creation
  - aws resourcegroupstaggingapi get-compliance-summary

  Das vollständige Verfahren zur Verwendung von Tag-Richtlinien in der AWS CLIfinden Sie unter Verwenden von Tag-Richtlinien im AWS CLI im AWS Organizations -Benutzerhandbuch.
- AWS-API:
  - StartReportCreation
  - DescribeReportCreation
  - GetComplianceSummary

Überwachen von Tag-Änderungen mit Serverless-Workflows und Amazon EventBridge

Amazon EventBridge unterstützt Tag-Änderungen an -AWSRessourcen. Mit diesem EventBridge Typ können Sie Regeln erstellen EventBridge, um Tag-Änderungen abzugleichen und die Ereignisse an ein oder mehrere Ziele weiterzuleiten. Ein Ziel könnte beispielsweise eine -AWS LambdaFunktion zum Aufrufen automatisierter Workflows sein. Dieses Thema enthält ein Tutorial zur Verwendung von Lambda zum Erstellen einer kosteneffektiven Serverless-Lösung zur sicheren Verarbeitung von Tag-Änderungen an Ihren -AWSRessourcen.

Tag-Änderungen generieren EventBridge Ereignisse

EventBridge stellt einen Stream von Systemereignissen in nahezu Echtzeit bereit, der Änderungen an -AWSRessourcen beschreibt. Viele -AWSRessourcen unterstützen Tags, bei denen es sich um benutzerdefinierte, benutzerdefinierte Attribute handelt, um AWS Ressourcen einfach zu organisieren und zu kategorisieren. Häufige Anwendungsfälle für Tags sind die Kategorisierung der Kostenzuordnung, die Sicherheit der Zugriffskontrolle und die Automatisierung.

Mit können EventBridgeSie Änderungen an Tags überwachen und den Tag-Status auf AWS Ressourcen verfolgen. Um ähnliche Funktionen zu erreichen, haben Sie zuvor möglicherweise kontinuierlich APIs abgefragt und mehrere Aufrufe orchestriert. Jetzt initiiert jede Änderung an einem Tag, einschließlich einzelner Service-APIs , Tag Editor und der Tagging-API, die Tag-Änderung bei Ressourcenereignissen. Das folgende Beispiel zeigt ein typisches EventBridge Ereignis, das durch

eine Tag-Änderung ausgelöst wird. Es zeigt die neuen, aktualisierten oder gelöschten Tag-Schlüssel und die zugehörigen Werte an.

```
{
  "version": "0",
  "id": "bddcf1d6-0251-35a1-aab0-adc1fb47c11c",
  "detail-type": "Tag Change on Resource",
  "source": "aws.tag",
  "account": "123456789012",
  "time": "2018-09-18T20:41:38Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa"
  ],
  "detail": {
    "changed-tag-keys": [
      "a-new-key",
      "an-updated-key",
      "a-deleted-key"
    ],
    "tags": {
      "a-new-key": "tag-value-on-new-key-just-added",
      "an-updated-key": "tag-value-was-just-changed",
      "an-unchanged-key": "tag-value-still-the-same"
    },
    "service": "ec2",
    "resource-type": "instance",
    "version": 3,
  }
}
```

Alle EventBridge Ereignisse haben dieselben Felder der obersten Ebene:

- -Version – Standardmäßig ist dieser Wert in allen Ereignissen auf `0` (Null) gesetzt.
- id – Für jedes Ereignis wird ein eindeutiger Wert generiert. Dies kann hilfreich sein, um Ereignisse nachzuverfolgen, während sie Regeln zu Zielen durchlaufen und verarbeitet werden.
- Detailtyp – Identifiziert in Kombination mit dem `source` Feld die Felder und Werte, die im Detailfeld angezeigt werden.
- Quelle – Identifiziert den Service, der die Quelle des Ereignisses war. Die Quelle für Tag-Änderungen ist `aws.tag`.
- time – Der Zeitstempel des Ereignisses.

- Region – Identifiziert die AWS-Region, aus der das Ereignis stammt.
- -Ressourcen – Dieses JSON-Array enthält Amazon-Ressourcennamen (ARNs), die Ressourcen identifizieren, die an dem Ereignis beteiligt sind. Dies ist die Ressource, in der sich Tags geändert haben.
- Detail – Ein JSON-Objekt, dessen Inhalt je nach Ereignistyp unterschiedlich ist. Für die Tag-Änderung der Ressource sind die folgenden detaillierten Felder enthalten:
  - changed-tag-keys – Die Tag-Schlüssel, die sich durch dieses Ereignis geändert haben.
  - service – Der Service, zu dem die Ressource gehört. In diesem Beispiel ist der Service `ec2`, d. h. Amazon EC2.
  - resource-type – Der Typ der Ressource des Services. In diesem Beispiel handelt es sich um eine Amazon EC2.
  - Version – Die Version des Tag-Sets. Die Version beginnt bei 1 und wird erhöht, wenn Tags geändert werden. Sie können die Version verwenden, um die Reihenfolge der Tag-Änderungsereignisse zu überprüfen.
  - Tags – Die Tags, die nach der Änderung an die Ressource angehängt wurden.

Weitere Informationen finden Sie unter Amazon- EventBridge Ereignismuster im Amazon-EventBridge Benutzerhandbuch.

Mit können Sie Regeln erstellen EventBridge, die bestimmten Ereignismustern basierend auf den verschiedenen Feldern entsprechen. Wir zeigen, wie dies geschieht, im Tutorial. Außerdem zeigen wir, wie eine Amazon EC2-Instance automatisch angehalten werden kann, wenn der Instance kein bestimmtes Tag angefügt ist. Wir verwenden die EventBridge Felder, um ein Muster zu erstellen, das den Tag-Ereignissen für die Instance entspricht, die eine Lambda-Funktion startet.

Lambda und Serverless

AWS Lambda folgt dem Serverless-Parameter, um Code in der Cloud auszuführen. Sie führen Code nur dann aus, wenn er benötigt wird, ohne über Server nachdenken zu müssen. Sie zahlen nur für die genaue Rechenzeit, die Sie tatsächlich nutzen. Obwohl es als Serverless bezeichnet wird, bedeutet dies nicht, dass es keine Server gibt. Serverless bedeutet in diesem Kontext, dass Sie die Server, die zum Ausführen Ihres Codes verwendet werden, nicht bereitstellen, konfigurieren oder verwalten müssen. AWS erledigt all dies für Sie, sodass Sie sich auf Ihren Code konzentrieren können. Weitere Informationen zu Lambda finden Sie unter AWS Lambda Produktübersicht.

Tutorial: Automatisches Stoppen von Amazon EC2-Instances, denen die erforderlichen Tags fehlen

Themen

Wenn Ihr AWS Ressourcenpool wächst und AWS-Konten Sie verwalten, können Sie Tags verwenden, um die Kategorisierung Ihrer Ressourcen zu vereinfachen. Tags werden häufig für kritische Anwendungsfälle wie Kostenzuweisung und Sicherheit verwendet. Um AWS Ressourcen effektiv verwalten zu können, müssen Ihre Ressourcen konsistent markiert werden. Wenn eine Ressource bereitgestellt wird, erhält sie häufig alle entsprechenden Tags. Ein späterer Prozess kann jedoch zu einer Tag-Änderung führen, die zu einer Abweichung von der Tag-Richtlinie des Unternehmens führt. Durch die Überwachung von Änderungen an Ihren Tags können Sie Tag-Abweichungen erkennen und sofort reagieren. Dies gibt Ihnen mehr Sicherheit, dass die Prozesse, die davon abhängen, dass Ihre Ressourcen ordnungsgemäß kategorisiert werden, die gewünschten Ergebnisse liefern.

Das folgende Beispiel zeigt, wie Sie Tag-Änderungen auf Amazon EC2-Instances überwachen, um zu überprüfen, ob eine bestimmte Instance weiterhin über die erforderlichen Tags verfügt. Wenn sich die Tags der Instance ändern und die Instance nicht mehr über die erforderlichen Tags verfügt, wird eine Lambda-Funktion aufgerufen, um die Instance automatisch herunterzufahren. Warum sollten Sie dies tun? Es stellt sicher, dass alle Ressourcen gemäß Ihrer Unternehmens-Tag-Richtlinie, für eine effektive Kostenzuweisung oder um Sicherheit basierend auf attributbasierter Zugriffskontrolle (ABAC) vertrauen zu können.

> **Important**
>
> Wir empfehlen dringend, dieses Tutorial in einem Nicht-Produktionskonto durchzuführen, in dem Sie wichtige Instances nicht versehentlich herunterfahren können.
> Der Beispielcode in diesem Tutorial beschränkt bewusst die Auswirkungen dieses Szenarios auf die Instances in einer Liste von Instance-IDs . Sie müssen die Liste mit Instance-IDs

aktualisieren, die Sie für den Test herunterfahren möchten. Dadurch wird sichergestellt, dass Sie nicht versehentlich jede Instance in einer Region in Ihrem herunterfahren könnenAWS-Konto.
Stellen Sie nach dem Testen sicher, dass alle Ihre Instances gemäß der Tagging-Strategie Ihres Unternehmens gekennzeichnet sind. Anschließend können Sie den Code entfernen, der die Funktion auf die Instance-IDs in der Liste beschränkt.

In diesem Beispiel werden JavaScript und die Version 16.x von verwendetNode.js. Das Beispiel verwendet die BeispielAWS-Konto-ID 123456789012 und USA Ost (NordAWS-Region-Virginia) (`us-east-1`). Ersetzen Sie diese durch Ihre eigene Testkonto-ID und -Region.

> **Note**
>
> Wenn Ihre Konsole eine andere Region als Standard verwendet, stellen Sie sicher, dass Sie die Region, die Sie in diesem Tutorial verwenden, wechseln, wenn Sie die Konsole ändern. Eine häufige Ursache für das Fehlschlagen dieses Tutorials ist, dass die Instance und Funktion in zwei verschiedenen Regionen gespeichert sind.

Wenn Sie eine andere Region als verwendenus`-east-1`, stellen Sie sicher, dass Sie alle Referenzen in den folgenden Codebeispielen in die von Ihnen gewählte Region ändern.

Schritt 1. So erstellen Sie die Lambda-Funktion:

So erstellen Sie die Lambda-Funktion:

1. Öffnen Sie die AWS Lambda Management Console.
2. Wählen Sie Funktion erstellen und dann Von Grund auf neu erstellen aus.
3. Geben Sie im Feld Function name (Funktionsname) **`AutoEC2Termination`** ein.
4. Wählen Sie unter Laufzeit die Option Node.js 16.x aus.
5. Behalten Sie alle anderen Felder auf ihren Standardwerten bei und wählen Sie Funktion erstellen aus.
6. Öffnen Sie auf der `AutoEC2Termination` Detailseite auf der Registerkarte Code die Datei index.js, um ihren Code anzuzeigen.

- Wenn eine Registerkarte mit index.js geöffnet ist, können Sie das Bearbeitungsfeld auf dieser Registerkarte auswählen, um ihren Code zu bearbeiten.
- Wenn eine Registerkarte mit index.js nicht geöffnet ist, klicken Sie mit der rechten Maustaste auf die Datei index.js im Ordner AutoEC2Terminator im Navigationsbereich. Klicken Sie auf Open.

7. Fügen Sie auf der Registerkarte index.js den folgenden Code in das Editorfeld ein und ersetzen Sie alles, was bereits vorhanden ist.

   Ersetzen Sie den Wert `RegionToMonitor` durch die Region, in der Sie diese Funktion ausführen möchten.

```
// Set the following line to specify which Region's instances you want to monitor
// Only instances in this Region are succesfully stopped on a match

const RegionToMonitor = "us-east-1"

// Specify the instance ARNs to check.
// This limits the function for safety to avoid the tutorial shutting down all
 instances in account
// The first ARN is a "dummy" that matches the test event you create in Step 3.
// Replace the second ARN with one that matches a real instance that you want to
 monitor and that you can
// safely stop

const InstanceList = [
    "i-0000000aaaaaaaaaa",
    "i-05db4466d02744f07"
];

// The tag key name and value that marks a "valid" instance. Instances in the
 previous list that
// do NOT have the following tag key and value are stopped by this function

const ValidKeyName = "valid-key";
const ValidKeyValue = "valid-value";

// Load and configure the AWS SDK
const AWS = require('aws-sdk');
// Set the AWS Region
AWS.config.update({region: RegionToMonitor});
// Create EC2 service object.
```

```
const ec2 = new AWS.EC2({apiVersion: '2016-11-15'});

exports.handler = (event, context, callback) => {

  // Retrieve the details of the reported event.
  var detail = event.detail;
  var tags = detail["tags"];
  var service = detail["service"];
  var resourceType = detail["resource-type"];
  var resource = event.resources[0];
  var resourceSplit = resource.split("/");
  var instanceId = resourceSplit[resourceSplit.length - 1];

  // If this event is not for an EC2 resource, then do nothing.
  if (!(service === "ec2")) {
    console.log("Event not for correct service -- no action (", service, ")" );
    return;
  }

  // If this event is not about an instance, then do nothing.
  if (!(resourceType === "instance")) {
    console.log("Event not for correct resource type -- no action (", resourceType,
 ")" );
    return;
  }

  // CAUTION - Removing the following 'if' statement causes the function to run
 against
  //           every EC2 instance in the specified Region in the calling AWS-
Konto.
  //           If you do this and an instance is not tagged with the approved tag
 key
  //           and value, this function stops that instance.

  // If this event is not for the ARN of an instance in our include list, then do
 nothing.
  if (InstanceList.indexOf(instanceId)<0) {
    console.log("Event not for one of the monitored instances -- no action (",
 resource, ")");
    return;
  }

  console.log("Tags changed on monitored EC2 instance (",instanceId,")");
```

```
  // Check attached tags for expected tag key and value pair
  if ( tags.hasOwnProperty(ValidKeyName) && tags[ValidKeyName] == "valid-value"){
    // Required tags ARE present
    console.log("The instance has the required tag key and value -- no action");
    callback(null, "no action");
    return;
  }

  // Required tags NOT present
  console.log("This instance is missing the required tag key or value -- attempting
 to stop the instance");

  var params = {
    InstanceIds: [instanceId],
    DryRun: true
  };

  // call EC2 to stop the selected instances
  ec2.stopInstances(params, function(err, data) {
    if (err && err.code === 'DryRunOperation') {
      // dryrun succeeded, so proceed with "real" stop operation
      params.DryRun = false;
      ec2.stopInstances(params, function(err, data) {
        if (err) {
          console.log("Failed to stop instance");
          callback(err, "fail");
        } else if (data) {
          console.log("Successfully stopped instance", data.StoppingInstances);
          callback(null, "Success");
        }
      });
    } else {
      console.log("Dryrun attempt failed");
      callback(err);
    }
  });
};
```

8. Wählen Sie Bereitstellen, um Ihre Änderungen zu speichern und die neue Version der Funktion zu aktivieren.

Diese Lambda-Funktion überprüft die Tags einer Amazon EC2-Instance, wie vom Tag-Änderungsereignis in gemeldet EventBridge. Wenn in diesem Beispiel der Instance im Ereignis der

erforderliche Tag-Schlüssel fehlt `valid-key` oder dieses Tag nicht den Wert hat`valid-value`, versucht die Funktion, die Instance zu stoppen. Sie können diese logische Prüfung oder die Tag-Anforderungen für Ihre eigenen spezifischen Anwendungsfälle ändern.

Lassen Sie das Lambda-Konsolenfenster in Ihrem Browser geöffnet.

Schritt 2. Einrichten der erforderlichen IAM-Berechtigungen

Bevor die Funktion erfolgreich ausgeführt werden kann, müssen Sie der Funktion die Berechtigung zum Anhalten einer EC2-Instance erteilen. Die AWS bereitgestellte Rolle lambda_basic_execution hat diese Berechtigung nicht. In diesem Tutorial ändern Sie die standardmäßige IAM-Berechtigungsrichtlinie, die der Ausführungsrolle der Funktion mit dem Namen angefügt ist`AutoEC2Termination-role-`*`uniqueid`*. Die für dieses Tutorial erforderliche Mindestberechtigung ist `ec2:StopInstances`.

Weitere Informationen zum Erstellen von Amazon EC2-spezifischen IAM-Richtlinien finden Sie unter Amazon EC2: Ermöglicht das Starten oder Stoppen einer EC2-Instance und das Ändern einer Sicherheitsgruppe programmgesteuert und in der Konsole im IAM-Benutzerhandbuch.

So erstellen Sie eine IAM-Berechtigungsrichtlinie und fügen sie der Ausführungsrolle der Lambda-Funktion an

1. Öffnen Sie in einer anderen Browser-Registerkarte oder einem anderen Fenster die Seite Rollen der IAM-Konsole.
2. Beginnen Sie mit der Eingabe des Rollennamens **`AutoEC2Termination`**. Wenn er in der Liste erscheint, wählen Sie den Rollennamen aus.
3. Wählen Sie auf der Seite Zusammenfassung der Rolle die Registerkarte Berechtigungen und wählen Sie den Namen der Richtlinie aus, die bereits angefügt ist.
4. Wählen Sie auf der Seite Zusammenfassung der Richtlinie die Option Richtlinie bearbeiten aus.
5. Wählen Sie auf der Registerkarte Visueller Editor die Option Zusätzliche Berechtigungen hinzufügen aus.
6. Wählen Sie bei -Service EC2 aus.
7. Wählen Sie für Aktionen die Option ausStopInstances. Sie können **`Stop`** in die Suchleiste eingeben und dann auswählen, `StopInstances` wann sie angezeigt wird.
8. Wählen Sie für Ressourcen die Option Alle Ressourcen aus, wählen Sie Richtlinie überprüfen und wählen Sie dann Änderungen speichern aus.

Dadurch wird automatisch eine neue Version der Richtlinie erstellt und diese Version wird als Standard festgelegt.

Ihre endgültige Richtlinie sollte dem folgenden Beispiel ähneln.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:StopInstances",
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": "logs:CreateLogGroup",
            "Resource": "arn:aws:logs:us-east-1:123456789012:*"
        },
        {
            "Sid": "VisualEditor2",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:us-east-1:123456789012:log-group:/aws/lambda/
AutoEC2Termination:*"
        }
    ]
}
```

Schritt 3. Führen Sie einen Vorabtest Ihrer Lambda-Funktion durch

In diesem Schritt übermitteln Sie ein Testereignis an Ihre Funktion. Die Lambda-Testfunktion funktioniert, indem sie ein manuell bereitgestelltes Testereignis absendet. Die Funktion verarbeitet das Testereignis genauso, als ob das Ereignis von stammen würde EventBridge. Sie können mehrere Testereignisse mit unterschiedlichen Werten definieren, um alle verschiedenen Teile Ihres Codes zu trainieren. In diesem Schritt übermitteln Sie ein Testereignis, das angibt, dass sich die Tags einer

Amazon EC2-Instance geändert haben, und die neuen Tags enthalten nicht den erforderlichen Tag-Schlüssel und -Wert.

So testen Sie Ihre Lambda-Funktion

1. Kehren Sie mit der Lambda-Konsole zum Fenster oder zur Registerkarte zurück und öffnen Sie die Registerkarte Test für Ihre AutoEC2Termination-Funktion.
2. Wählen Sie Neues Ereignis erstellen aus.
3. Geben Sie für Event name (Ereignisname) **`SampleBadTagChangeEvent`** ein.
4. Ersetzen Sie im Ereignis-JSON den Text durch das Beispielereignis, das im folgenden Beispieltext angezeigt wird. Sie müssen die Konten, die Region oder die Instance-ID nicht ändern, damit dieses Testereignis ordnungsgemäß funktioniert.

```
{
  "version": "0",
  "id": "bddcf1d6-0251-35a1-aab0-adc1fb47c11c",
  "detail-type": "Tag Change on Resource",
  "source": "aws.tag",
  "account": "123456789012",
  "time": "2018-09-18T20:41:38Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa"
  ],
  "detail": {
    "changed-tag-keys": [
      "valid-key"
    ],
    "tags": {
      "valid-key": "NOT-valid-value"
    },
    "service": "ec2",
    "resource-type": "instance",
    "version": 3
  }
}
```

5. Wählen Sie Save (Speichern) und dann Test aus.

   Der Test scheint fehlzuschlagen, aber das ist in Ordnung.

Der folgende Fehler sollte auf der Registerkarte Ausführungsergebnisse unter Antwort angezeigt werden.

```
{
  "errorType": "InvalidInstanceID.NotFound",
  "errorMessage": "The instance ID 'i-0000000aaaaaaaaaa' does not exist",
  ...
}
```

Der Fehler tritt auf, weil die im Testereignis angegebene Instance nicht vorhanden ist.

Die Informationen auf der Registerkarte Ausführungsergebnisse im Abschnitt Funktionsprotokolle zeigen, dass Ihre Lambda-Funktion erfolgreich versucht hat, eine EC2-Instance zu stoppen. Es ist jedoch fehlgeschlagen, weil der Code zunächst versucht, die Instance `DryRun` zu stoppen, was darauf hinweist, dass die Instance-ID ungültig ist.

```
START RequestId: 390c1f8d-0d9b-4b44-b087-8de64479ab44 Version: $LATEST
2022-11-30T20:17:30.427Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    INFO    Tags
 changed on monitored EC2 instance ( i-0000000aaaaaaaaaa )
2022-11-30T20:17:30.427Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    INFO    This
 instance is missing the required tag key or value -- attempting to stop the
 instance
2022-11-30T20:17:31.206Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    INFO    Dryrun
 attempt failed
2022-11-30T20:17:31.207Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    ERROR   Invoke
 Error     {"errorType":"InvalidInstanceID.NotFound","errorMessage":"The instance
 ID 'i-0000000aaaaaaaaaa' does not
 exist","code":"InvalidInstanceID.NotFound","message":"The instance ID
 'i-0000000aaaaaaaaaa' does not
 exist","time":"2022-11-30T20:17:31.205Z","requestId":"a5192c3b-142d-4cec-
bdbc-685a9b7c7abf","statusCode":400,"retryable":false,"retryDelay":36.87870631147607,"stack
["InvalidInstanceID.NotFound: The instance ID 'i-0000000aaaaaaaaaa' does
 not exist","    at Request.extractError (/var/runtime/node_modules/aws-sdk/
lib/services/ec2.js:50:35)","    at Request.callListeners (/var/runtime/
node_modules/aws-sdk/lib/sequential_executor.js:106:20)","    at Request.emit
 (/var/runtime/node_modules/aws-sdk/lib/sequential_executor.js:78:10)","    at
 Request.emit (/var/runtime/node_modules/aws-sdk/lib/request.js:686:14)","    at
 Request.transition (/var/runtime/node_modules/aws-sdk/lib/request.js:22:10)","
    at AcceptorStateMachine.runTo (/var/runtime/node_modules/aws-sdk/lib/
state_machine.js:14:12)","    at /var/runtime/node_modules/aws-sdk/lib/
state_machine.js:26:10","    at Request.<anonymous> (/var/runtime/node_modules/aws-
```

```
sdk/lib/request.js:38:9)","    at Request.<anonymous> (/var/runtime/node_modules/
aws-sdk/lib/request.js:688:12)","    at Request.callListeners (/var/runtime/
node_modules/aws-sdk/lib/sequential_executor.js:116:18)"]}
END RequestId: 390c1f8d-0d9b-4b44-b087-8de64479ab44
```

6. Um nachzuweisen, dass der Code nicht versucht, die Instance anzuhalten, wenn das richtige Tag verwendet wird, können Sie ein weiteres Testereignis erstellen und einreichen.

   Wählen Sie die Registerkarte Test über der Codequelle aus. Die Konsole zeigt Ihr vorhandenes SampleBadTagChangeEvent Testereignis an.

7. Wählen Sie Neues Ereignis erstellen aus.
8. Geben Sie für Event Name (Ereignisname) den Namen **`SampleGoodTagChangeEvent`** ein.
9. Löschen Sie in Zeile 17, **`NOT-`** um den Wert in zu ändern**`valid-value`**.
10. Wählen Sie oben im Fenster Testereignis die Option Speichern und dann Testen aus.

    Die Ausgabe zeigt Folgendes an, was zeigt, dass die Funktion das gültige Tag erkennt und nicht versucht, die Instance herunterzufahren.

```
START RequestId: 53631a49-2b54-42fe-bf61-85b9e91e86c4 Version: $LATEST
2022-12-01T23:24:12.244Z    53631a49-2b54-42fe-bf61-85b9e91e86c4    INFO    Tags
 changed on monitored EC2 instance ( i-0000000aaaaaaaaaa )
2022-12-01T23:24:12.244Z    53631a49-2b54-42fe-bf61-85b9e91e86c4    INFO    The
 instance has the required tag key and value -- no action
END RequestId: 53631a49-2b54-42fe-bf61-85b9e91e86c4
```

    Lassen Sie die Lambda-Konsole in Ihrem Browser geöffnet.

Schritt 4. Erstellen der EventBridge Regel, die die Funktion startet

Jetzt können Sie eine EventBridge Regel erstellen, die dem Ereignis entspricht und auf Ihre Lambda-Funktion verweist.

So erstellen Sie die EventBridge Regel

1. Öffnen Sie in einer anderen Browser-Registerkarte oder einem anderen Fenster die EventBridge Konsole zur Seite Regel erstellen.
2. Geben Sie für Name ein **`ec2-instance-rule`**und wählen Sie dann Weiter aus.

3. Scrollen Sie nach unten zur Erstellungsmethode und wählen Sie Benutzerdefiniertes Muster (JSON-Editor).
4. Fügen Sie im Bearbeitungsfeld den folgenden Mustertext ein und wählen Sie dann Weiter aus.

```
{
  "source": [
    "aws.tag"
  ],
  "detail-type": [
    "Tag Change on Resource"
  ],
  "detail": {
    "service": [
      "ec2"
    ],
    "resource-type": [
      "instance"
    ]
  }
}
```

   Diese Regel gleicht `Tag Change on Resource` Ereignisse für Amazon EC2-Instances ab und ruft alles auf, was Sie im nächsten Schritt als Ziel angeben.
5. Fügen Sie als Nächstes Ihre Lambda-Funktion als Ziel hinzu. Wählen Sie im Feld Ziel 1 unter Ziel auswählen die Option Lambda-Funktion aus.
6. Wählen Sie unter Funktion die zuvor erstellte AutoEC2Termination-Funktion und dann Weiter aus.
7. Wählen Sie auf der Seite Tags konfigurieren die Option Weiter aus. Wählen Sie dann auf der Seite Überprüfen und erstellen die Option Regel erstellen aus. Dadurch wird auch automatisch die Berechtigung für erteilt EventBridge , die angegebene Lambda-Funktion aufzurufen.

Schritt 5. Testen der vollständigen Lösung

Sie können Ihr Endergebnis testen, indem Sie eine EC2-Instance erstellen und sich ansehen, was passiert, wenn Sie ihre Tags ändern.

So testen Sie die Überwachungslösung mit einer echten Instance

1. Öffnen Sie die Amazon EC2-Konsole zur Seite Instances.

2. Erstellen Sie eine Amazon EC2-Instance. Bevor Sie es starten, fügen Sie ein Tag mit dem Schlüssel `valid-key` und dem Wert an`valid-value`. Informationen zum Erstellen und Starten einer Instance finden Sie unter Schritt 1: Starten einer Instance im Amazon EC2-Benutzerhandbuch für Linux-Instances. Wählen Sie im Verfahren Zum Starten einer Instance in Schritt 3, in dem Sie das Tag Name eingeben, auch Zusätzliche Tags hinzufügen aus, wählen Sie Tag hinzufügen und geben Sie dann den Schlüssel von **`valid-key`** und den Wert von ein**`valid-value`**. Sie können ohne Schlüsselpaar fortfahren, wenn diese Instance ausschließlich für die Zwecke dieses Tutorials bestimmt ist und Sie planen, diese Instance zu löschen, nachdem Sie sie abgeschlossen haben. Kehren Sie zu diesem Tutorial zurück, wenn Sie das Ende von Schritt 1 erreicht haben. Schritt 2: Herstellen einer Verbindung mit Ihrer Instance .
3. Kopieren Sie die InstanceId aus der -Konsole.
4. Wechseln Sie von der Amazon EC2-Konsole zur Lambda-Konsole. Wählen Sie Ihre AutoEC2Termination-Funktion, wählen Sie die Registerkarte Code und dann die Registerkarte index.js, um Ihren Code zu bearbeiten.
5. Ändern Sie den zweiten Eintrag in , `InstanceList` indem Sie den Wert einfügen, den Sie aus der Amazon EC2-Konsole kopiert haben. Stellen Sie sicher, dass der `RegionToMonitor` Wert mit der Region übereinstimmt, die die eingefügte Instance enthält.
6. Wählen Sie Bereitstellen, um Ihre Änderungen aktiv zu machen. Die Funktion kann jetzt durch Tag-Änderungen an dieser Instance in der angegebenen Region aktiviert werden.
7. Wechseln Sie von der Lambda-Konsole zur Amazon EC2-Konsole.
8. Ändern Sie die der Instance angefügten Tags, indem Sie entweder das gültige Schlüssel-Tag löschen oder den Wert dieses Schlüssels ändern.

   > **Note**
   >
   > Informationen zum Ändern der Tags auf einer laufenden Amazon EC2-Instance finden Sie unter Hinzufügen und Löschen von Tags auf einer einzelnen Ressource im Amazon EC2-Benutzerhandbuch für Linux-Instances.

9. Warten Sie einige Sekunden und aktualisieren Sie dann die Konsole. Die Instance sollte ihren Instance-Status in Anhalten und dann in Angehalten ändern.
10. Wechseln Sie mit Ihrer Funktion von der Amazon EC2-Konsole zur Lambda-Konsole und wählen Sie die Registerkarte Überwachen.

11. Wählen Sie die Registerkarte Protokolle und in der Tabelle Aktuelle Aufrufe den neuesten Eintrag in der LogStream Spalte aus.

    Die Amazon- CloudWatch Konsole öffnet die Seite Protokollereignisse für den letzten Aufruf Ihrer Lambda-Funktion. Der letzte Eintrag sollte dem folgenden Beispiel ähneln.

```
2022-11-30T12:03:57.544-08:00    START RequestId: b5befd18-2c41-43c8-
a320-3a4b2317cdac Version: $LATEST
2022-11-30T12:03:57.548-08:00    2022-11-30T20:03:57.548Z b5befd18-2c41-43c8-
a320-3a4b2317cdac INFO Tags changed on monitored EC2 instance ( arn:aws:ec2:us-
west-2:123456789012:instance/i-1234567890abcdef0 )
2022-11-30T12:03:57.548-08:00    2022-11-30T20:03:57.548Z b5befd18-2c41-43c8-
a320-3a4b2317cdac INFO This instance is missing the required tag key or value --
 attempting to stop the instance
2022-11-30T12:03:58.488-08:00    2022-11-30T20:03:58.488Z b5befd18-2c41-43c8-
a320-3a4b2317cdac INFO Successfully stopped instance [ { CurrentState: { Code: 64,
 Name: 'stopping' }, InstanceId: 'i-1234567890abcdef0', PreviousState: { Code: 16,
 Name: 'running' } } ]
2022-11-30T12:03:58.546-08:00    END RequestId: b5befd18-2c41-43c8-
a320-3a4b2317cdac
```

Übersicht

In diesem Tutorial wurde gezeigt, wie Sie eine - EventBridge Regel erstellen, die mit einer Tag-Änderung eines Ressourcenereignisses für Amazon EC2 übereinstimmt. Die Regel verweist auf eine Lambda-Funktion, die die Instance automatisch herunterfährt, wenn sie nicht über das erforderliche Tag verfügt.

Die Amazon- EventBridge Unterstützung für Tag-Änderungen an -AWSRessourcen öffnet Möglichkeiten, ereignisgesteuerte Automatisierung über viele hinweg aufzubauenAWS-Services. Durch die Kombination dieser Funktion mit AWS Lambda erhalten Sie Tools zum Erstellen von Serverless-Lösungen, die sicher auf AWS Ressourcen zugreifen, bei Bedarf skalieren und kostengünstig sind.

Weitere mögliche Anwendungsfälle für das tag-change-on-resource EventBridge Ereignis sind:

- Starten einer Warnung, wenn jemand von einer ungewöhnlichen IP-Adresse auf Ihre Ressource zugreift – Verwenden Sie ein Tag, um die Quell-IP-Adresse jedes Besuchers zu speichern, der auf Ihre Ressource zugreift. Änderungen am Tag erzeugen ein CloudWatch Ereignis. Sie können

dieses Ereignis verwenden, um die Quell-IP-Adresse mit einer Liste gültiger IP-Adressen zu vergleichen und eine Warn-E-Mail zu aktivieren, wenn die Quell-IP-Adresse nicht gültig ist.

- Überwachen, ob es Änderungen an Ihrer Tag-basierten Zugriffskontrolle für eine Ressource gibt – Wenn Sie den Zugriff auf eine Ressource mithilfe der attribut (Tag)-basierten Zugriffskontrolle (ABAC) eingerichtet haben, können Sie Ereignisse verwenden EventBridge, die durch Änderungen am Tag generiert wurden, um eine Prüfung durch Ihr Sicherheitsteam einzuleiten.

Fehlerbehebung bei Tag-Änderungen

Die folgende Checkliste ist möglicherweise nützlich, wenn Fehler beim Anwenden oder Ändern von Tags für ausgewählte Ressourcen in den Ergebnissen für die Abfrage Find resources to tag (Ressourcen suchen, die markiert werden sollen) auftreten.

- Die Ressource verfügt möglicherweise bereits über die maximale Anzahl von Tags. Im Allgemeinen können Ressourcen maximal 50 benutzerdefinierte Tags haben. Von AWS generierte Tags zählen nicht zum Maximum von 50 Tags. Möglicherweise fügen andere Benutzer derselben Ressource zur selben Zeit Tags hinzu. Dies könnte die Zahl der Tags der Ressource auf die maximal zulässige Zahl erhöhen.
- Einige Services lassen einen anderen Zeichensatz für das Erstellen von Tags zu (oder schränken den zulässigen Zeichensatz ein). Wenn Sie Tags mit Sonderzeichen hinzugefügt oder geändert haben, überprüfen Sie die Tag-Anforderungen in der Servicedokumentation der Ressource, um sicherzustellen, dass diese Zeichen vom Service zugelassen werden.
- Möglicherweise haben Sie keine Berechtigungen zum Ändern der Tags für die Ressource. Wenn Sie keine Berechtigungen zum Anzeigen vorhandener Tags für eine Ressource haben, können Sie keine Änderungen an den Tags der Ressource vornehmen.
- Möglicherweise haben Sie keine Berechtigungen zum Ändern der Ressource. Änderungen der Metadaten der Ressource wurden möglicherweise von einem anderen Administrator eingeschränkt.
- Die Ressource wurde möglicherweise von einem anderen Benutzer oder Prozess bearbeitet oder gelöscht. Angenommen, eine Ressource wurde im Rahmen der Erstellung eines -AWS CloudFormationStacks gestartet. Wenn der Stack gelöscht wurde oder sich nicht mehr in einem aktiven Zustand befindet, ist die Ressource möglicherweise nicht mehr verfügbar.
- Tag-Änderungen sind möglicherweise nicht möglich, wenn eine Ressource offline ist, beendet wurde oder andere Updates (z. B. Software-Upgrades) für die Ressource ausgeführt werden.

- Tag-Änderungen können fehlschlagen, wenn Sie die Browser-Registerkarte schließen oder die Seite ändern, bevor die Tag-Änderungen abgeschlossen sind. Bleiben Sie auf der Seite, bis die Tag-Änderungen abgeschlossen sind, und warten Sie, bis das Banner für Erfolg oder Misserfolg auf der Seite angezeigt wird, bevor Sie die Seite verlassen.
- Während es ein Ratenlimit für die gibtAWS Resource Groups Tagging API, kann der Service, den Sie markieren, ein separates Limit festlegen, das Sie möglicherweise vor dem API-Limit für das Markieren von Ressourcengruppen erreichen.

Ähnliche Informationen

- Verwenden von Kostenzuordnungs-Tags im AWS Billing-Benutzerhandbuch

Sicherheit im Tag-Editor

Die Sicherheit in der Cloud hat für 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 selbst – 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, die für den Tag-Editor gelten, finden Sie unter AWS Im Rahmen des Compliance-Programms zugelassene -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 hilft Ihnen zu verstehen, wie Sie das Modell der geteilten Verantwortung bei der Verwendung des Tag-Editors einsetzen können. Die folgenden Themen zeigen Ihnen, wie Sie den Tag-Editor konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen.

Themen

Datenschutz im Tag Editor

Das Modell der AWS geteilten gilt für den Datenschutz im Tag Editor. https://aws.amazon.com/compliance/shared-responsibility-model/ Wie in diesem Modell beschrieben, ist AWS für den Schutz

der globalen Infrastruktur verantwortlich, 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 Tag Editor oder anderen unter AWS-Services Verwendung der Konsole, APIAWS CLI, 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

Markierungsinformationen sind nicht verschlüsselt. Obwohl sie nicht verschlüsselt sind, können Tags Informationen enthalten, die als Teil Ihrer Sicherheitsstrategie verwendet werden. Daher ist es wichtig

zu steuern, wer auf Tags auf Ressourcen zugreifen kann. Es ist besonders wichtig, zu kontrollieren, wer Tags ändern kann, da ein solcher Zugriff verwendet werden könnte, um die Berechtigungen zu erweitern.

Verschlüsselung im Ruhezustand

Es gibt keine zusätzlichen Möglichkeiten, Service- oder Netzwerkverkehr zu isolieren, der für den Tag Editor spezifisch ist. Verwenden Sie gegebenenfalls eine AWS spezifische Isolierung. Sie können die Tag-Editor-API und die Konsole in einer Virtual Private Cloud (VPC) verwenden, um den Datenschutz und die Infrastruktursicherheit zu maximieren.

Verschlüsselung während der Übertragung

Tag-Editor-Daten werden während der Übertragung zur internen Datenbank des Services für Backups verschlüsselt. Dies ist nicht vom Benutzer konfigurierbar.

Schlüsselverwaltung

Der Tag-Editor ist derzeit nicht in integriert AWS Key Management Service und unterstützt nichtAWS KMS keys.

Richtlinie für den Datenverkehr zwischen Netzwerken

Tag Editor verwendet HTTPS für alle Übertragungen zwischen Tag-Editor-Benutzern und AWS. Tag Editor verwendet Transport Layer Security (TLS) 1.3, unterstützt aber auch TLS 1.2.

Identity and Access Management für Tag Editor

AWS Identity and Access Management (IAM) ist ein AWS-Service, mit dem Administratoren den Zugriff auf AWS-Ressourcen sicher steuern können. IAM-Administratoren steuern, wer authentifiziert (angemeldet) und autorisiert (im Besitz von Berechtigungen) ist, Tag-Editor-Ressourcen zu nutzen. IAM ist ein AWS-Service, den Sie ohne zusätzliche Kosten verwenden können.

Themen

- Funktionsweise von Tag Editor mit IAM
- Beispiele für identitätsbasierte Tag-Editor-Richtlinien
- Fehlerbehebung für Tag-Editor-Identität und -Zugriff

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, unterscheidet sich je nach Ihrer Arbeit im Tag-Editor.

Service-Benutzer – Wenn Sie den Tag-Editor zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Wenn Sie zur Ausführung von Aufgaben weitere Tag-Editor-Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Featuresweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie auf ein Feature im Tag Editor nicht zugreifen können, finden Sie weitere Informationen unter Fehlerbehebung für Tag-Editor-Identität und -Zugriff.

Service-Administrator – Wenn Sie in Ihrem Unternehmen für die Ressourcen des Tag-Editors verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf den Tag-Editor. Ihre Aufgabe besteht darin, zu bestimmen, auf welche Tag-Editor-Funktionen und -Ressourcen Ihre Service-Benutzer 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 dazu, wie Ihr Unternehmen IAM mit dem Tag Editor verwenden kann, finden Sie unter Funktionsweise von Tag Editor mit IAM.

IAM-Administrator – Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf den Tag Editor verfassen können. Beispiele für identitätsbasierte Tag-Editor-Richtlinien, die Sie in IAM verwenden können, finden Sie unter Beispiele für identitätsbasierte Tag-Editor-Richtlinien.

Authentifizierung mit Identitäten

Authentifizierung ist die Art, 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 So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch von AWS-Anmeldung.

Bei programmgesteuertem 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-Faktor Authentifizierung (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-Root-Benutzer

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.

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.

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. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie 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.
- Kontoübergreifender 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 kontoübergreifenden 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 Dienst 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 auslösen. 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-Anfragen werden nur dann gestellt, wenn ein Service eine Anfrage erhält, die eine Interaktion mit anderen AWS-Services oder -Ressourcen erfordert. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - 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 serviceverbundene 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 Diensts. Sie können verwaltete AWS-Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (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 Dienste, 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. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis 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 Dienst 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 Tag Editor mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf den Tag-Editor zu verwalten, sollten Sie verstehen, welche IAM-Funktionen Sie mit dem Tag-Editor verwenden können. Einen Überblick über das AWS-Services Zusammenwirken von Tag Editor und anderen mit IAM finden Sie unter , AWS-Services die mit IAM funktionieren im IAM-Benutzerhandbuch.

Themen

- Identitätsbasierte Tag-Editor-Richtlinien
- Ressourcenbasierte Richtlinien
- Autorisierung auf der Basis von Markierungen
- Tag-Editor-IAM-Rollen

Identitätsbasierte Tag-Editor-Richtlinien

Mit identitätsbasierten IAM-Richtlinien können Sie zusätzlich zu den Bedingungen, unter denen Aktionen erlaubt oder verweigert werden, auch erlaubte oder verweigerte Aktionen und Ressourcen angeben. Tag Editor 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 AWS JSON-Richtlinien verwenden, um anzugeben, wer Zugriff auf was hat. 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 in der Regel 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 im Tag Editor verwenden das folgende Präfix vor der Aktion: `tag:`. Tag-Editor-Aktionen werden vollständig in der Konsole ausgeführt, haben jedoch das Präfix `tag` in Protokolleinträgen.

Um beispielsweise jemandem die Berechtigung zu erteilen, eine Ressource mit der `tag:TagResources` -API-Operation zu markieren, fügen Sie die `tag:TagResources` Aktion in seine Richtlinie ein. Richtlinienanweisungen müssen entweder ein `Action`- oder ein `NotAction`-Element enthalten. Der Tag-Editor definiert einen eigenen Satz von Aktionen, die Aufgaben beschreiben, die Sie mit diesem Service durchführen können.

Um mehrere Tagging-Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie wie folgt durch Kommas.

```
"Action": [
      "tag:action1",
      "tag:action2",
      "tag:action3"
```

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

```
"Action": "tag:Get*"
```

Eine Liste der Tag-Editor-Aktionen finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für den Tag-Editor in der Service-Autorisierungs-Referenz.

Ressourcen

Administratoren können AWS JSON-Richtlinien verwenden, um anzugeben, wer Zugriff auf was hat. 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": "*"
```

Der Tag-Editor hat keine eigenen Ressourcen. Stattdessen werden die Metadaten (Tags) manipuliert, die Ressourcen angefügt sind, die von anderen erstellt wurden AWS-Services.

Bedingungsschlüssel

Administratoren können AWS JSON-Richtlinien verwenden, um anzugeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

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

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

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. 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. Informationen zum Anzeigen aller AWS globalen Bedingungsschlüssel finden Sie unter AWS Globale Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Der Tag-Editor definiert keine servicespezifischen Bedingungsschlüssel.

Beispiele

Beispiele für identitätsbasierte Tag-Editor-Richtlinien finden Sie unter Beispiele für identitätsbasierte Tag-Editor-Richtlinien.

Ressourcenbasierte Richtlinien

Der Tag-Editor unterstützt keine ressourcenbasierten Richtlinien, da er keine seiner eigenen Ressourcen definiert.

Autorisierung auf der Basis von Markierungen

Die Autorisierung auf der Basis von Tags ist Teil der Sicherheitsstrategie, die als attributbasierte Zugriffskontrolle (ABAC) bezeichnet wird.

Um den Zugriff auf eine Ressource basierend auf ihren Tags zu steuern, geben Sie Tag-Informationen im Bedingungselement einer Richtlinie mithilfe der `aws:TagKeys` Bedingungsschlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`oder an. Sie können Tags auf eine Ressource anwenden, wenn Sie die Ressource erstellen oder aktualisieren.

Ein Beispiel für eine identitätsbasierte Richtlinie zur Einschränkung des Zugriffs auf eine Ressource auf der Grundlage der Markierungen dieser Ressource finden Sie unter Anzeigen von Gruppen basierend auf Tags. Weitere Informationen zur attributbasierten Zugriffskontrolle (ABAC) finden Sie unter Was ist ABAC für AWS? im IAM-Benutzerhandbuch.

Tag-Editor-IAM-Rollen

Eine IAM-Rolle ist eine Entität in Ihrem AWS-Konto mit bestimmten Berechtigungen. Der Tag-Editor hat keine Servicerollen oder verwendet diese.

Verwenden temporärer Anmeldeinformationen mit dem Tag Editor

Im Tag-Editor können Sie temporäre Anmeldeinformationen verwenden, um sich mit einem Verbund anzumelden, eine IAM-Rolle anzunehmen oder eine kontoübergreifende Rolle anzunehmen. Sie erhalten temporäre Sicherheitsanmeldeinformationen, indem Sie AWS STS -API-Operationen wie AssumeRole oder aufrufenGetFederationToken.

Service-verknüpfte Rollen

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

Der Tag-Editor verfügt nicht über serviceverknüpfte Rollen oder verwendet diese.

Servicerollen

Dieses Feature ermöglicht einem Service das Annehmen einer Servicerolle in Ihrem Namen.

Der Tag-Editor hat keine Servicerollen oder verwendet diese.

Beispiele für identitätsbasierte Tag-Editor-Richtlinien

Standardmäßig haben IAM-Prinzipale wie Rollen und Benutzer keine Berechtigung zum Erstellen oder Ändern von Tags. Sie können auch keine Aufgaben über die AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS APIs ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Prinzipalen die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die sie benötigen. Der Administrator muss diese Richtlinien dann den Prinzipalen anfügen, die diese Berechtigungen benötigen.

Anweisungen zum Erstellen einer identitätsbasierten IAM-Richtlinie mithilfe dieser Beispiel-JSON-Richtliniendokumente finden Sie unter Erstellen von Richtlinien auf der Registerkarte JSON im IAM-Benutzerhandbuch.

Themen

- Bewährte Methoden für Richtlinien
- Verwenden der Tag-Editor-Konsole und der Resource Groups Tagging API
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer
- Anzeigen von Gruppen basierend auf Tags

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Tag-Editor-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie 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 vom Kunden verwaltete AWS-Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS-verwaltete Richtlinien oder AWS-verwaltete Richtlinien für Auftragsfunktionen im IAM-Benutzerhandbuch.

- Anwendung von Berechtigungen mit den geringsten Rechten:Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs:Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Service-Aktionen zu gewähren, wenn diese durch ein bestimmtes AWS-Service, wie beispielsweise AWS CloudFormation, verwendet werden. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten:IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.
- Bedarf einer Multi-Faktor-Authentifizierung (MFA):Wenn Sie ein Szenario haben, das IAM-Benutzer oder Root-Benutzer in Ihrem AWS-Konto erfordert, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

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

Verwenden der Tag-Editor-Konsole und der Resource Groups Tagging API

Um auf die Tag-Editor-Konsole und die Resource Groups Tagging API zugreifen zu können, müssen Sie über einen Mindestsatz von Berechtigungen verfügen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Tags aufzulisten und anzuzeigen, die Ressourcen in Ihrem zugeordnet

sindAWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die restriktiver ist als die mindestens erforderlichen Berechtigungen, funktionieren die Konsolen- und API-Befehle für die IAM-Prinzipale mit dieser Richtlinie nicht wie vorgesehen.

Um sicherzustellen, dass diese Prinzipale weiterhin Tag Editor verwenden können, fügen Sie den Entitäten die folgende Richtlinie (oder eine Richtlinie, die die in der folgenden Richtlinie aufgeführten Berechtigungen enthält) hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer imIAM-Benutzerhandbuch:

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

Weitere Informationen zum Gewähren des Zugriffs auf den Tag-Editor und die Resource Groups Tagging API finden Sie unter Erteilen von Berechtigungen für die Verwendung des Tag Editors.

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": "*"
        }
    ]
}
```

Anzeigen von Gruppen basierend auf Tags

Sie können Bedingungen in Ihrer identitätsbasierten Richtlinie verwenden, um den Zugriff auf Tag-Editor-Ressourcen basierend auf Tags zu steuern. Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen können, die das Anzeigen einer Ressource erlaubt, in diesem Beispiel einer Ressourcengruppe. Die Berechtigung wird jedoch nur erteilt, wenn das Gruppen-Tag denselben Wert `project` hat wie das `project` Tag, das dem aufrufenden Prinzipal angefügt 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 -Benutzern in Ihrem Konto zuweisen. Wenn ein Benutzer mit dem Tag-Schlüssel `project` und dem Tag-Wert `alpha` versucht, eine Ressourcengruppe anzuzeigen, muss die Gruppe auch mit markiert sein`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 Tag-Editor-Identität und -Zugriff

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

Themen

- Ich bin nicht autorisiert, eine Aktion im Tag Editor auszuführen
- Ich bin nicht autorisiert, iam durchzuführen:PassRole

Ich bin nicht autorisiert, eine Aktion im Tag Editor 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 hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Der folgende Beispielfehler tritt auf, wenn der Benutzer `mateojackson` versucht, die Konsole zum Anzeigen von Tags für eine Ressource zu verwenden, jedoch keine `tag:GetTagKeys` Berechtigungen hat.

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

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

Ich bin nicht autorisiert, iam durchzuführen:PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Ausführen der `iam:PassRole` Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an den Tag Editor übergeben zu können.

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

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion im Tag Editor 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 Dienst.

```
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 zur Verfügung gestellt.

Protokollierung und Überwachung im Tag Editor

Alle Tag-Editor-Aktionen werden in protokolliertAWS CloudTrail.

Protokollieren von Tag-Editor-API-Aufrufen mit CloudTrail

Der Tag-Editor ist in integriert, einem ServiceAWS CloudTrail, der die Aktionen eines Benutzers, einer Rolle oder eines AWS-Service in Tag Editor aufzeichnet. CloudTrail erfasst alle API-Aufrufe für den Tag-Editor als Ereignisse, einschließlich Aufrufen von der Tag-Editor-Konsole und von Code-Aufrufen an die Resource Groups Tagging API. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3-Bucket aktivieren, einschließlich Ereignissen für den Tag-Editor. Wenn Sie keinen Trail konfigurieren, können Sie trotzdem die neuesten Ereignisse in der CloudTrail Konsole unter Ereignisverlauf anzeigen. Anhand der von CloudTrailgesammelten Informationen können Sie die an den Tag Editor 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 zu CloudTrailfinden Sie im AWS CloudTrail -Benutzerhandbuch.

Informationen zum Tag-Editor in CloudTrail

CloudTrail wird auf Ihrem aktiviertAWS-Konto, wenn Sie das Konto erstellen. Wenn eine Aktivität im Tag-Editor oder in der Tag-Editor-Konsole auftritt, wird diese Aktivität in einem CloudTrail Ereignis zusammen mit anderen AWS-Service Ereignissen im Ereignisverlauf aufgezeichnet. Sie können in Ihrem AWS-Konto die neusten Ereignisse anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail Ereignisverlauf .

Erstellen Sie für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto, einschließlich Ereignissen für den Tag-Editor, einen Trail. Ein Trail ermöglicht CloudTrail die Bereitstellung von Protokolldateien an einen Amazon S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon-S3-Bucket bereit. Darüber hinaus können Sie andere konfigurieren, AWS-Services um die in den CloudTrail Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie in den folgenden Ressourcen:

- Erstellen eines Trails für AWS-Konto
- In CloudTrail unterstützte Services und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien aus mehreren Konten

Alle Tag-Editor-Aktionen werden von protokolliert CloudTrail und sind in der API-Referenz zum Tag-Editor dokumentiert. Tag-Editor-Aktionen in der Konsole werden von protokolliert CloudTrailund als Ereignisse mit `tagging.amazonaws.com` als angezeigt`eventSource`.

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

Weitere Informationen finden Sie im CloudTrail `userIdentity` Element .

Grundlegendes zu Tag-Editor-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Bereitstellung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anforderungsparameter. 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`TagResources`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661372702",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661372702",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
```

```
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-24T20:25:03Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-24T20:27:14Z",
    "eventSource": "tagging.amazonaws.com",
    "eventName": "TagResources",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.65",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resourcegroupstaggingapi.tag-resources",
    "requestParameters": {
        "resourceARNList": [
            "arn:aws:events:us-east-1:123456789012:rule/SecretsManagerMonitorRule"
        ],
        "tags": {
            "owner": "alice"
        }
    },
    "responseElements": {
        "failedResourcesMap": {}
    },
    "requestID": "8f9ea891-4125-460c-802f-26c11EXAMPLE",
    "eventID": "b2c9322a-aad7-424b-8f0b-423daEXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "tagging.us-east-1.amazonaws.com"
    }
}
```

Compliance-Validierung für Tag Editor

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 im Tag-Editor

Der Tag-Editor führt automatisierte Backups für interne Serviceressourcen durch. Diese Backups sind nicht vom Benutzer konfigurierbar. Backups werden sowohl im Ruhezustand als auch während der Übertragung verschlüsselt. Der Tag-Editor 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.

Wenn Sie Tags versehentlich löschen, wenden Sie sich an AWS Support das -Center.

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

Sicherheit der Infrastruktur im Tag Editor

Der Tag-Editor bietet keine zusätzlichen Möglichkeiten, den Service- oder Netzwerkverkehr zu isolieren. Verwenden Sie gegebenenfalls eine AWS spezifische Isolierung. Sie können die Tag-Editor-API und die Konsole in einer Virtual Private Cloud (VPC) verwenden, um den Datenschutz und die Infrastruktursicherheit zu maximieren.

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

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

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

Der Tag-Editor unterstützt keine ressourcenbasierten Richtlinien.

Sie können Tag-Editor-API-Operationen von jedem Netzwerkstandort aus aufrufen, aber der Tag-Editor unterstützt ressourcenbasierte Zugriffsrichtlinien, die Einschränkungen auf der Grundlage der Quell-IP-Adresse enthalten können. Sie können auch Tag-Editor-Richtlinien verwenden, um den Zugriff von bestimmten Amazon Virtual Private Cloud (Amazon VPC)-Endpunkten oder bestimmten VPCs aus zu steuern. Dieser Ansatz isoliert effektiv den Netzwerkzugriff auf eine bestimmte Ressource nur von der spezifischen VPC innerhalb des AWS Netzwerks.

Referenzinformationen zum Tag-Editor

Die Referenzinformationen zum Tag-Editor umfassen die geltenden Service Quotas.

Service Quotas für Tag Editor

Die folgende Tabelle enthält Informationen zu den Servicekontingenten für den Tag-Editor.

Diese Kontingente sind derzeit nicht über die Service Quotas-Konsole anpassbar. Wenden Sie sich an AWS Support.

Name	Standard
Angefügte Tags pro Ressource	50 benutzerdefinierte Tags (AWS generierte Tags werden nicht auf dieses Limit angerechnet.)
Tag-Schlüsselname	Mindestens 1, maximal 128 Unicode-Zeichen in UTF-8. Zulässige Zeichen sind Buchstaben, Zahlen, Leerzeichen und die folgenden Zeichen: `_ . : / = + - @` Schlüsselnamen dürfen nicht mit beginnen, `aws:` da dieses Präfix für die AWS Verwendung reserviert ist. **Note** Einige AWS-Services haben einige zusätzliche Zeichen- oder

Name	Standard
	Längenbeschränkungen. Weitere Informationen finden Sie in der Dokumentation für den jeweiligen Service.
Tag-Werte	Mindestens 0, maximal 256 Unicode-Zeichen in UTF-8. Zulässige Zeichen sind Buchstaben, Zahlen, Leerzeichen und die folgenden Zeichen: `_ . : / = + - @` **Note** Einige AWS-Services haben einige zusätzliche Zeichen- oder Längenbeschränkungen. Weitere Informationen finden Sie in der Dokumentation für den jeweiligen Service.
Rate des Aufrufs des GetResources API-Vorgangs	Maximal 15 Aufrufe pro Sekunde

Name	Standard	
Rate zum Aufrufen der folgenden API-Operationen: • TagResources • UntagResources • GetTagKeys • GetTagValues	Maximal 5 Aufrufe pro Sekunde	

Dokumentverlauf des Tag-Editors

Änderung	Beschreibung	Datum
Markieren von Inhalten von , die in dieses Handbuch Allgemeine AWS-Referenz verschoben wurden	Die Themen zum Markieren Ihrer AWS Ressourcen wurden von Allgemeine AWS-Referenz in dieses Handbuch verschoben.	24. März 2023
Aktualisierung der bewährten Methoden für IAM	Aktualisierter Leitfaden, angepasst an die bewährten IAM-Methoden. Weitere Informationen finden Sie unter Bewährte IAM-Methoden.	3. Januar 2023
Verschieben der Dokumentation zum Tag Editor in einen eigenen Leitfaden	Die Dokumentation zum Tag-Editor wird jetzt in einem eigenen Benutzerhandbuch bereitgestellt, anstatt Teil des AWS Resource GroupsBenutzerhandbuchs zu sein.	13. Dezember 2022
Überprüfen der Compliance mit Tag-Richtlinien	Nachdem Sie Tag-Richtlinien mit erstellt und an Konten angefügt habenAWS Organizations, können Sie nicht konforme Tags für Ressourcen in den Konten Ihrer Organisation finden.	26. November 2019
Tag Editor unterstützt jetzt das Suchen von nicht markierten Ressourcen	Sie können jetzt im Tag Editor nach Ressourcen suchen, für die keine Tag-Werte für einen bestimmten Tag-Schlüssel angewendet wurden.	18. Juni 2019

Tag-Editor-Konsole wird aus der AWS Systems Manager Konsole verschoben	Die Tag-Editor-Konsole ist jetzt unabhängig von der Systems Manager-Konsole. Obwohl Sie in der linken Navigationsleiste von Systems Manager immer noch Zeiger auf die Tag-Editor-Konsole finden, können Sie die Tag-Editor-Konsole direkt aus dem Dropdown-Menü oben links in der öffnenAWS Management Console.	5. Juni 2019
Ältere, ältere Tag-Editor-Tools sind nicht mehr verfügbar	Hinweise zum älteren, klassischen oder älteren Tag Editor wurden entfernt. Diese Tools sind in nicht mehr verfügbarAWS. Verwenden Sie stattdessen den Tag-Edito r.	14. Mai 2019
Tag Editor unterstützt jetzt das Markieren 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 standardm äßig hinzugefügt wird.	2. Mai 2019

Der Tag-Editor unterstützt jetzt das Exportieren von Abfrageergebnissen in ein CSV	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

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 aktivieren. Wenn Tag-Änderungen für einige Ressourcen fehlschlagen, können Sie Tag-Änderungen nur für die Ressourcen wiederholen, für die die Tag-Änderungen fehlgeschlagen sind.	19. März 2019
Tag Editor unterstützt jetzt mehrere Ressourcentypen in 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

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.