Benutzer-Leitfaden

AWS Tagging-Ressourcen und Tag-Editor

Version 1.0

AWS Tagging-Ressourcen und Tag-Editor: Benutzer-Leitfaden

Table of Contents

Was ist Tag Editor? 1
Methoden zur Kennzeichnung 2
Weitere Informationen 3
Bewährte Verfahren und Strategien 3
Bewährte Methoden 3
Bewährte Methoden zur Benennung von Tags 4
Häufig verwendete Tagging-Strategien 6
Tagging-Kategorien 8
Erste Schritte 10
Voraussetzungen 11
Melden Sie sich an für ein AWS-Konto 11
Erstellen eines Benutzers mit Administratorzugriff 12
Erstellen von -Ressourcen 13
Berechtigungen einrichten 13
Berechtigungen für einzelne Dienste 14
Für die Verwendung der Tag Editor-Konsole sind Berechtigungen erforderlich 14
Erteilen von Berechtigungen für die Verwendung des Tag-Editors 17
Autorisierung und Zugriffskontrolle auf der Grundlage von Tags 18
Ressourcen zum Taggen finden 20
Bestehende Tags für eine ausgewählte Ressource anzeigen und bearbeiten 22
Exportieren Sie die Ergebnisse in eine CSV-Datei 23
Tags verwalten 24
Fügen Sie ausgewählten Ressourcen Stichwörter hinzu 25
Bearbeiten Sie die Tags der ausgewählten Ressourcen 26
Entfernen Sie Tags aus ausgewählten Ressourcen 28
Verwenden von Tags in IAM-Richtlinien 30
Tags und attributebasierte Zugriffskontrolle 30
Bedingungsschlüssel, die sich auf Tags beziehen 31
Beispiel für IAM-Richtlinien, die Tags verwenden 32
AWS Organizations Tag-Richtlinien 34
Voraussetzungen und Berechtigungen 34
Voraussetzungen für die Bewertung der Einhaltung der Tag-Richtlinien 34
Berechtigungen zur Bewertung der Einhaltung der Vorschriften für ein Konto 35
Berechtigungen für die Bewertung der unternehmensweiten Einhaltung 36

Amazon S3 S3-Bucket-Richtlinie für die Berichtsspeicherung ... 38
Bewertung der Einhaltung der Vorschriften für ein Konto ... 39
Bewertung der unternehmensweiten Einhaltung der Vorschriften ... 42
Überwachung von Tag-Änderungen ... 45
Tag-Änderungen generieren Ereignisse EventBridge ... 45
Lambda und Serverless ... 47
Tutorial zur Überwachung ... 47
Schritt 1. So erstellen Sie die Lambda-Funktion: ... 49
Schritt 2. Richten Sie die erforderlichen IAM-Berechtigungen ein ... 52
Schritt 3. Führen Sie einen Vortest Ihrer Lambda-Funktion durch ... 54
Schritt 4. Erstellen Sie die EventBridge Regel, die die Funktion startet ... 57
Schritt 5. Testen Sie die komplette Lösung ... 58
Zusammenfassung des Tutorials ... 60
Problembehandlung bei Tag-Änderungen ... 61
Fehlgeschlagene Tag-Änderungen erneut versuchen ... 62
Sicherheit ... 63
Datenschutz ... 63
Datenverschlüsselung ... 65
Richtlinie für den Datenverkehr zwischen Netzwerken ... 65
Identity and Access Management ... 65
Zielgruppe ... 66
Authentifizierung mit Identitäten ... 66
Verwalten des Zugriffs mit Richtlinien ... 67
So funktioniert der Tag-Editor mit IAM ... 69
Beispiele für identitätsbasierte Richtlinien ... 73
Fehlerbehebung ... 77
Protokollierung und Überwachung ... 79
CloudTrail Integration ... 79
Compliance-Validierung ... 82
Ausfallsicherheit ... 82
Sicherheit der Infrastruktur ... 83
Tag-Editor-Dienstkontingente ... 84
Dokumentverlauf ... 86
... xc

Was ist Tag Editor?

Mit dem Tag Editor können Sie Tags effektiv verwalten. Tags sind Schlüssel- und Wertepaare, die als Metadaten für die Organisation Ihrer AWS Ressourcen dienen. Bei den meisten AWS Ressourcen haben Sie die Möglichkeit, Tags hinzuzufügen, wenn Sie die Ressource erstellen. Zu den Ressourcen gehören beispielsweise 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 Abrechnungs- und Verwaltungsdienste bereitzustellen. Tags sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

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.

Note

Obwohl bei Tagschlüsseln zwischen Groß- und Kleinschreibung unterschieden wird, verfügt IAM über zusätzliche Validierungen für IAM-Ressourcen, um die Anwendung von Tagschlüsseln zu verhindern, die sich nur in der Groß- und Kleinschreibung unterscheiden. Wir empfehlen, keine Schlüssel zu verwenden, die sich nur in der Groß- und Kleinschreibung unterscheiden. Weitere Informationen finden Sie unter Tags für IAM-Ressourcen.

Methoden zur Kennzeichnung von Ressourcen

Es gibt drei Möglichkeiten, Ihren AWS Ressourcen Tags hinzuzufügen:

- AWS-Service API-Betrieb — Die Tagging-API-Operationen wurden direkt unterstützt und. AWS-Service Welche Tagging-Funktionen die einzelnen Funktionen AWS-Service bieten, finden Sie in der Dokumentation des Dienstes im AWS Dokumentationsindex.
- Tag-Editor-Konsole — Einige Dienste unterstützen das Tagging mit der Tag Editor-Konsole.
- Tagging-API für Resource Groups — Die meisten Dienste unterstützen auch das Tagging mithilfe der. AWS Resource Groups Tagging API

> **Note**
>
> Sie können die AWS Service Catalog TagOptions Bibliothek auch verwenden, um Tags für bereitgestellte Produkte einfach zu verwalten. A TagOptionist ein Schlüssel-Wert-Paar, das im Service Catalog verwaltet wird. Es ist kein AWS Tag, sondern dient als Vorlage für die Erstellung eines AWS Tags auf der Grundlage von. TagOption

Sie können Ressourcen für alle Services mit anfallenden Kosten in AWS markieren. AWS Empfiehlt für die folgenden Dienste eine neuere Alternative, AWS-Services die Tagging 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 Glacier Direkt	Amazon SimpleDB
WorkSpaces Amazon-An wendungsmanager	AWS DeepLens	

Weitere Informationen

Diese Seite enthält allgemeine Informationen zur Kennzeichnung von AWS Ressourcen. Weitere Informationen zum Markieren von Ressourcen in einem bestimmten AWS Dienst finden Sie in der zugehörigen Dokumentation. Im Folgenden finden Sie auch gute Informationsquellen zum Tagging:

- Weitere Informationen zu finden Sie im AWS Resource Groups Tagging APIResource Groups Tagging API Reference Guide.
- Informationen zu den jeweils AWS-Service bereitgestellten Tagging-Funktionen finden Sie in der Dokumentation des Dienstes im AWS Dokumentationsindex.
- Informationen zur Verwendung von Tags in IAM-Richtlinien, um zu kontrollieren, wer Ihre AWS Ressourcen einsehen und mit ihnen interagieren kann, finden Sie im IAM-Benutzerhandbuch unter Steuern des Zugriffs auf und für IAM-Benutzer und -Rollen mithilfe von Tags.

Bewährte Verfahren und Strategien

In diesen Abschnitten finden Sie Informationen zu bewährten Methoden und Strategien für das Tagging Ihrer AWS Ressourcen und die Verwendung des Tag-Editors.

Bewährte Methoden beim Taggen

Beachten Sie bei der Erstellung 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, auch für die Abrechnung. Tags sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.
- 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, um Ressourcen-Tags zu verwalten. Der Tag-Editor und die Resource Groups Tagging API ermöglichen die programmatische 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.

Bewährte Methoden zur Benennung von Tags

Dies sind mehrere bewährte Methoden und Benennungskonventionen, die Sie bei Ihren Tags verwenden sollten. Weitere Informationen finden Sie unter Benennen von Tags im IAM-Benutzerhandbuch.

Eine Reihe von Tags ist von verschiedenen AWS-Services vordefiniert AWS oder wird automatisch von ihnen erstellt. Viele AWS generierte Tags verwenden Schlüsselnamen, die alle in Kleinbuchstaben geschrieben sind, wobei Wörter im Namen durch Bindestriche voneinander getrennt werden, und Präfixe, gefolgt von Doppelpunkten, um den Quelldienst für das Tag zu identifizieren. Sehen Sie sich zum Beispiel Folgendes an:

- `aws:ec2spot:fleet-request-i`dist ein Tag, das die Amazon EC2 Spot-Instance-Anfrage identifiziert, mit der die Instance gestartet wurde.
- `aws:cloudformation:stack-name`ist ein Tag, das den CloudFormation Stack 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 anhand der folgenden Regeln zu benennen:

- Verwenden Sie für die Wörter ausschließlich 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.

Beispielsweise könnten Sie für ein fiktives Unternehmen mit dem Namen AnyCompanyTags definieren wie:

- `anycompany:cost-center`um den internen Kostenstellencode zu identifizieren.
- `anycompany:environment-type`um festzustellen, ob es sich bei der Umgebung um eine Entwicklungs-, Test- oder Produktionsumgebung handelt.
- `anycompany:application-id`um die Anwendung zu identifizieren, für die die Ressource erstellt wurde.

Das Präfix stellt sicher, dass Tags eindeutig erkennbar sind, da sie von Ihrer Organisation und nicht von AWS einem Drittanbieter-Tool, das Sie möglicherweise verwenden, definiert wurden. 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`.

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 mindestens 1 und maximal 128 Unicode-Zeichen in UTF-8 enthalten.
- Der Tag-Wert muss eine Länge zwischen 0 und 256 Unicode-Zeichen in UTF-8 aufweisen.
- Die zulässigen Zeichen können je nach AWS Dienst variieren. Informationen darüber, welche Zeichen Sie verwenden können, um Ressourcen in einem bestimmten AWS Dienst zu taggen, finden Sie in der zugehörigen 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 für die Kostenzuordnung
- Tags für die Automatisierung
- Tags für die Zugriffskontrolle
- Tagging-Governance

Tags zur Ressourcenorganisation

Tags sind eine gute Möglichkeit, AWS Ressourcen in der zu organisieren AWS-Managementkonsole. Sie können Tags so konfigurieren, dass sie mit Ressourcen angezeigt werden, und Sie können nach Tags suchen und filtern. Mit dem AWS -Ressourcengruppen Dienst können Sie Gruppen von AWS Ressourcen erstellen, die auf einem oder mehreren Tags oder Teilen von Tags basieren. Sie können Gruppen auch auf der Grundlage ihres Vorkommens in einem AWS CloudFormation Stapel 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 Mit dem Cost Explorer und detaillierten Abrechnungsberichten können Sie die AWS Kosten nach Schlagwörtern aufschlüsseln. In der Regel verwenden Sie betriebswirtschaftliche Stichwörter wie center/business Kosteneinheit, Kunde oder Projekt, um AWS Kosten herkömmlichen

Kostenverteilungsdimensionen 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.

Bei einigen Services können Sie ein AWS generiertes `createdBy` Tag für die Kostenzuweisung verwenden, um Ressourcen zu berücksichtigen, die andernfalls möglicherweise nicht kategorisiert werden. 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 Fakturierung und Kostenmanagement -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 Methode, um Instances zu identifizieren, die von dieser Aktion ausgeschlossen werden sollen. Für Skripts, die veraltete oder fortlaufende Amazon EBS-Snapshots suchen und löschen, können Snapshot-Tags zusätzliche Suchkriterien hinzufügen. out-of-date

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 enthalten, um EC2 API-Aufrufe anhand ihrer Tags 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 sie konsistent und programmgesteuert auf alle Ressourcen an. AWS Sie können sowohl reaktive als auch proaktive Ansätze zur Steuerung von Tags in Ihrer Umgebung verwenden. AWS

- Reactive Governance dient zum Auffinden von Ressourcen, die nicht richtig gekennzeichnet sind, mithilfe von Tools wie der Resource Groups Tagging API und benutzerdefinierten Skripten. AWS-Config-Regeln Um Ressourcen manuell zu suchen, können Sie Tag-Editor und detaillierte Abrechnungsberichte verwenden.
- Proactive Governance verwendet Tools wie Service Catalog CloudFormation, Tag-Richtlinien in oder IAM-Berechtigungen auf Ressourcenebene AWS Organizations, um sicherzustellen, dass standardisierte Tags bei der Ressourcenerstellung einheitlich angewendet werden.

  Sie können die CloudFormation `Resource Tags` Eigenschaft beispielsweise 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.

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	• Datum/Uhrzeit – Identifizieren des Datums oder der Uhrzeit, zu dem/der eine Ressource	• Projekt – Identifizieren von Projekten, die von der Ressource unterstützt werden	• Vertraulichkeit – Eine Kennung für die spezifische Datenvertraulichkeitsebene, die eine

Technische Tags	Tags für die Automatisierung	Business-Tags	Sicherheits-Tags
Ressourcen, die mit einer bestimmten Anwendung verknüpft sind • Anwendungsrolle – Beschreibung der Funktion einer bestimmten Ressource (z. B. Webserver, Message Broker, Datenbank) • Cluster – Identifizieren von Ressourcenfarmen, die eine gemeinsame Konfiguration verwenden und eine bestimmte Funktion für eine Anwendung ausführen • Umgebung – Unterscheiden zwischen Entwicklungs-, Test- und Produktionsressourcen • Version – Unterscheiden zwischen Versionen von Ressourcen oder Anwendungen	gestartet, gestoppt, gelöscht oder rotiert werden soll • Opt-In/Opt-out – Angabe, ob eine Ressource in eine automatisierte 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 Sicherheitsgruppen, die eine zusätzliche Prüfung erfordern	• Eigentümer – Identifizieren der für die Ressource verantwortlichen Person • Kostenstelle/ Geschäftseinheit – Identifizieren der Kostenstelle oder Geschäftseinheit, die einer Ressource zugeordnet ist, in der Regel für die Kostenzuordnung und -verfolgung • Kunde – Identifizieren eines bestimmten Clients, für den eine bestimmte Gruppe von Ressourcen da ist	Ressource unterstützt • Compliance – Ein Bezeichner für Workloads, die bestimmte Compliance-Anforderungen erfüllen müssen

Erste Schritte mit dem Tag Editor

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

Verwenden Sie den Tag-Editor, um mehreren Ressourcen gleichzeitig Tags hinzuzufügen oder sie 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-Managementkonsole an.
2. Führen Sie einen der folgenden Schritte aus:
   - Wählen Sie Dienste. Wählen Sie dann unter Management & Governance die Option Resource Groups & 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 Tag-Editor-Tagging-Spalte unter Unterstützte Ressourcentypen im AWS -Ressourcengruppen Benutzerhandbuch. Wenn ein Ressourcentyp, den Sie taggen möchten, nicht unterstützt wird, AWS teilen Sie uns dies mit, indem Sie in der unteren linken Ecke des Konsolenfensters Feedback auswählen.

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

Themen

- Voraussetzungen für die Arbeit mit dem Tag Editor
- Berechtigungen einrichten

Voraussetzungen für die Arbeit mit dem Tag Editor

Bevor Sie beginnen, Ihre Ressourcen zu taggen, sollten Sie sicherstellen, dass Sie über aktive AWS-Konto Ressourcen verfügen und über die entsprechenden Rechte zum Taggen von Ressourcen und zum Erstellen von Gruppen verfügen.

Themen

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

Melden Sie sich an für ein AWS-Konto

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

Um sich für eine anzumelden AWS-Konto

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

   Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen einen Verifizierungscode über die Telefontasten eingeben.

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

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

Erstellen eines Benutzers mit Administratorzugriff

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

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS-Managementkonsoleals 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 Benutzers mit Administratorzugriff

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 Benutzerzugriff.

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

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 im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Access-Portal.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

   Anweisungen hierzu finden Sie unter Berechtigungssatz erstellen im AWS IAM Identity Center Benutzerhandbuch.
2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

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

Erstellen von -Ressourcen

Sie müssen Ressourcen in Ihrem AWS-Konto To-Tag haben. Weitere Informationen zu den unterstützten Ressourcentypen finden Sie in der Spalte Tag-Editor-Tagging unter Unterstützte Ressourcentypen im AWS -Ressourcengruppen Benutzerhandbuch.

Berechtigungen einrichten

Um den Tag Editor in vollem Umfang nutzen zu können, benötigen Sie möglicherweise zusätzliche Berechtigungen, um Ressourcen zu taggen oder die Tag-Schlüssel und -Werte einer Ressource zu sehen. Diese Berechtigungen lassen sich in die folgenden Kategorien einteilen:

- 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 ein Administrator sind, können Sie Ihren Benutzern Berechtigungen gewähren, indem Sie Richtlinien über den AWS Identity and Access Management (IAM-) Dienst erstellen. Sie erstellen zunächst IAM-Rollen, -Benutzer oder -Gruppen und wenden dann die Richtlinien mit den erforderlichen Berechtigungen an. Informationen zum Erstellen und Anhängen von IAM-Richtlinien finden Sie unter Mit Richtlinien arbeiten.

Berechtigungen für einzelne Dienste

> **Important**
>
> In diesem Abschnitt werden die Berechtigungen beschrieben, die erforderlich sind, wenn Sie Ressourcen von anderen AWS Servicekonsolen kennzeichnen möchten und APIs.

Um Tags zu einer Ressource hinzuzufügen, benötigen Sie die erforderlichen Berechtigungen für den Service, zu dem die Ressource gehört. Um beispielsweise EC2 Amazon-Instances zu taggen, müssen Sie über Berechtigungen für die Tagging-Operationen in der API dieses Dienstes verfügen, z. B. für den EC2CreateTagsAmazon-Vorgang.

Für die Verwendung der Tag Editor-Konsole sind Berechtigungen erforderlich

Um die Tag Editor-Konsole zum Auflisten und Markieren von Ressourcen zu verwenden, müssen die folgenden Berechtigungen zur Richtlinienerklärung eines Benutzers in IAM 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 AWS verwalteter Richtlinien für Tag-Editor-Berechtigungen

Der 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 jeder Rolle, jedem Benutzer oder jeder Gruppe zuordnen, genau wie jede andere Richtlinie, die Sie erstellen.

ResourceGroupsandTagEditorReadOnlyAccess

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

ResourceGroupsandTagEditorFullAccess

Diese Richtlinie gewährt der angehängten IAM-Rolle oder dem Benutzer die Berechtigung, alle Resource Groups sowie die Lese- und Schreib-Tag-Operationen im Tag Editor aufzurufen. Um die Tags einer Ressource lesen oder schreiben zu können, müssen Sie im Rahmen einer separaten Richtlinie auch über Berechtigungen für diese Ressource verfügen. Weitere Informationen finden Sie im folgenden Wichtigen Hinweis.

Important

Die beiden vorherigen Richtlinien gewähren die Erlaubnis, die Tag Editor-Operationen aufzurufen und die Tag Editor-Konsole zu verwenden. Sie müssen jedoch nicht nur über die erforderlichen Berechtigungen zum Aufrufen des Vorgangs verfügen, 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 außerdem eine der folgenden Richtlinien anhängen:

- Die AWS verwaltete Richtlinie ReadOnlyAccessgewährt Berechtigungen für schreibgeschützte Operationen für die Ressourcen aller Dienste. AWS hält diese Richtlinie automatisch auf dem neuesten Stand, AWS-Services sobald neue verfügbar sind.
- Viele Dienste bieten dienstspezifische AWS verwaltete Richtlinien mit Schreibschutz, mit denen Sie den Zugriff nur auf die von diesem Dienst bereitgestellten Ressourcen beschränken können. Zum Beispiel EC2 bietet Amazon AmazonEC2ReadOnlyAccess.
- Sie können Ihre eigene Richtlinie erstellen, die nur Zugriff auf die spezifischen schreibgeschützten Operationen für die wenigen Dienste und Ressourcen gewährt, auf die Ihre Benutzer zugreifen sollen. Diese Richtlinie verwendet entweder eine Allowlist-Strategie oder eine Denylist-Strategie.

  Eine Allowlist-Strategie macht sich die Tatsache zunutze, dass der Zugriff standardmäßig verweigert wird, bis Sie ihn in einer Richtlinie ausdrücklich zulassen. Sie können also eine Richtlinie wie das folgende Beispiel verwenden.

  JSON

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

```
            "Effect": "Allow",
            "Action": [ "tag:*" ],
            "Resource": [
                "arn:aws:ec2:us-east-1:444455556666:*",
                "arn:aws:s3:::amzn-s3-demo-bucket2"
                ]
        }
    ]
}
```

Alternativ könnten Sie eine Denylist-Strategie verwenden, die den Zugriff auf alle Ressourcen ermöglicht, mit Ausnahme der Ressourcen, die Sie explizit blockieren. Dies erfordert eine separate Richtlinie, die für die jeweiligen Benutzer gilt und den Zugriff ermöglicht. Die folgende Beispielrichtlinie verweigert dann den Zugriff auf die spezifischen Ressourcen, die im Amazon-Ressourcennamen (ARN) aufgeführt sind.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [ "tag:*" ],
            "Resource": [
                "arn:aws:ec2:us-east-1:123456789012:instance:*",
                "arn:aws:s3:::amzn-s3-demo-bucket3"
             ]
        }
    ]
}
```

Manuelles Hinzufügen von Tag Editor-Berechtigungen

- `tag:*`(Diese Berechtigung ermöglicht 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 Kommas getrennte Liste von Aktionen ersetzen.)
- `tag:GetResources`

- `tag:TagResources`
- `tag:UntagResources`
- `tag:getTagKeys`
- `tag:getTagValues`
- `resource-explorer:*`
- `resource-groups:SearchResources`
- `resource-groups:ListResourceTypes`

> **Note**
>
> Mit dieser `resource-groups:SearchResources` Berechtigung kann der Tag-Editor Ressourcen auflisten, wenn Sie Ihre Suche anhand von Tagschlüsseln oder -werten filtern. Mit dieser `resource-explorer:ListResources` Berechtigung kann der Tag-Editor Ressourcen auflisten, wenn Sie nach 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 AWS -Ressourcengruppen und den Tag-Editor hinzuzufügen.

1. Öffnen Sie die IAM-Konsole auf der Seite Rollen.
2. Suchen Sie die Rolle, der Sie Tag-Editor-Berechtigungen gewähren möchten. Wählen Sie den Namen der Rolle, um die Übersichtsseite 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.

   JSON

```
{
  "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 beispielhafte Richtlinienanweisung gewährt nur Berechtigungen zur Ausführung von Tag-Editor-Aktionen.

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.

Da die Richtlinie nun in IAM gespeichert ist, können Sie sie anderen Prinzipalen wie Rollen, Gruppen oder Benutzern zuordnen. Weitere Informationen zum Hinzufügen einer Richtlinie zu einem Prinzipal finden Sie unter Hinzufügen und Entfernen von IAM-Identitätsberechtigungen im IAM-Benutzerhandbuch.

Autorisierung und Zugriffskontrolle auf der Grundlage von Tags

AWS-Services unterstützt Folgendes:

- Aktionsbasierte Richtlinien — Sie können beispielsweise eine Richtlinie erstellen, die es Benutzern ermöglicht, `GetTagValues` Operationen auszuführen`GetTagKeys`, andere jedoch nicht.

- Berechtigungen auf Ressourcenebene in Richtlinien — Viele Dienste unterstützen die Angabe einzelner Ressourcen in der Richtlinie. ARNs
- Autorisierung auf der Grundlage von Tags — Viele Dienste unterstützen die Verwendung von Ressourcen-Tags unter 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 Wozu dient ABAC? AWS im AWS Identity and Access Management Benutzerhandbuch.
- Temporäre Anmeldeinformationen — Benutzer können eine Rolle mit einer Richtlinie annehmen, die Tag-Editor-Operationen erlaubt.

Der Tag Editor verwendet keine dienstbezogenen Rollen.

Weitere Informationen zur Integration von Tag Editor in AWS Identity and Access Management (IAM) finden Sie unter den folgenden Themen im AWS Identity and Access Management Benutzerhandbuch:

- AWS Dienste, die mit IAM funktionieren
- Aktionen, Ressourcen und Bedingungsschlüssel für den Tag-Editor
- Steuern des Zugriffs auf AWS Ressourcen mithilfe von Richtlinien

Ressourcen zum Taggen finden

Mit dem Tag-Editor erstellen Sie eine Abfrage, um Ressourcen in einer oder mehreren Ressourcen zu finden AWS-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 Tag-Editor-Tagging unter Unterstützte Ressourcentypen im AWS -Ressourcengruppen 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 Ressourcen gesucht werden soll, die markiert werden sollen. Standardmäßig wird Ihre aktuelle Region verwendet. Wählen Sie für dieses Verfahren us-east-1 und us-west-2.
3. Wählen Sie mindestens einen Ressourcentyp aus der Dropdownliste 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::Instanceund AWS::S3::Bucket.
4. (Optional) Geben Sie in den Tag-Feldern einen Tag-Schlüssel oder ein Tag-Schlüssel-Wert-Paar ein, um die Ressourcen in der aktuellen Version AWS-Region auf diejenigen zu beschränken, die mit Ihren angegebenen Werten gekennzeichnet sind. Wenn Sie einen Tag-Schlüssel eingeben, werden passende Tag-Schlüssel in der aktuellen Region in einer Liste 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, grenzt die Ergebnisse der Abfrage jedoch weiter ein. Um weitere Tags hinzuzufügen, wählen Sie Add (Hinzufügen) aus. Abfragen weisen Tags einen AND Operator zu, sodass von der Abfrage nur Ressourcen zurückgegeben werden, die sowohl dem angegebenen Ressourcentyp als auch allen angegebenen Tags entsprechen.

> **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 für Tags leer, um alle Ressourcen des angegebenen Typs in der ausgewählten AWS-Regionen Datei zu finden. 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 nach Ressourcen zu suchen, die zwar ein Tag, aber einen leeren Wert haben, wählen Sie (leerer Wert).

> **Note**
>
> Bevor Sie Ressourcen mit den angegebenen Tags finden können, müssen sie in der aktuellen Version auf mindestens eine Ressource des angegebenen Typs angewendet worden sein AWS-Region.

5. Wenn Ihre Abfrage bereit ist, wählen Sie Search resources (Ressourcen durchsuchen) aus. Die Ergebnisse werden als Tabelle im Bereich Ergebnisse der Ressourcensuche 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 Ressourcentuchergebnissen anzeigt, wählen Sie in den Ergebnissen der Ressourcensuche das Zahnradsymbol „Einstellungen“.

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 Zeilenumbruch.

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

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

Bestehende Tags für eine ausgewählte Ressource anzeigen und bearbeiten

Der Tag-Editor zeigt Ihnen die vorhandenen Tags für ausgewählte Ressourcen, die in den Ergebnissen Ihrer Suche nach Ressourcen zum Markieren enthalten sind.

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

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

Um Tags direkt in der Suchergebnistabelle zu bearbeiten

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

   > **Note**
   >
   > - Wenn die gewählte Ressource derzeit kein Tag mit dem ausgewählten Schlüssel hat, wird der Wert als (nicht markiert) angezeigt.

- Wenn die gewählte Ressource über ein Tag mit dem ausgewählten Schlüssel, aber ohne Wert verfügt, wird der Wert als '—' angezeigt.

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

Um alle Tags für eine einzelne Ressource anzuzeigen

1. Wählen Sie in den Ergebnissen Ihrer Abfrage „Zu taggende Ressourcen 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 für ausgewählte Ressourcen verwalten auswählen, wenn Sie Tags auf der Seite „Stichwörter 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 Sie die Ergebnisse in eine CSV-Datei

Sie können die Ergebnisse einer Abfrage vom Typ „Ressourcen zum Markieren suchen“ in eine Datei mit kommagetrennten Werten (.csv) exportieren. Die CSV-Datei enthält die Ressourcennamen, Dienste, Region, Ressource IDs, die Gesamtzahl der Tags und eine Spalte für jeden eindeutigen Tagschlüssel in der Sammlung. Die CSV-Datei kann Ihnen dabei helfen, eine Tagging-Strategie für Ressourcen in Ihrer Organisation zu entwickeln oder festzustellen, wo es Überschneidungen oder Inkonsistenzen bei der ressourcenübergreifenden Tagging 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, können Sie die CSV-Datei öffnen oder sie an einem geeigneten Ort speichern.

Verwaltung von Tags mit dem Tag Editor

Nachdem Sie Ressourcen gefunden haben, die Sie taggen möchten, können Sie die Tags für einige oder alle Ihrer Suchergebnisse hinzufügen, entfernen und bearbeiten. Der Tag-Editor zeigt Ihnen alle Tags, die mit Ressourcen verknüpft sind. Außerdem wird angezeigt, ob diese Tags im Tag Editor, von der 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 Abrechnungs- und Verwaltungsdienste bereitzustellen. Tags sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

Andere Möglichkeiten, deine Tags zu verwalten

In diesem Thema wird das Taggen von Ressourcen mithilfe des Tag-Editors in der AWS-Managementkonsole beschrieben. Sie können die Tags Ihrer AWS Ressourcen jedoch auch mithilfe der folgenden Tools verwalten:

- Sie können Befehle an Ihrer Shell-Eingabeaufforderung eingeben oder als Skript verwenden, indem Sie die `resourcegroupstaggingapi`Befehle in der AWS Command Line Interface (AWS CLI) verwenden.
- Sie können PowerShell Skripts mithilfe der AWS -Ressourcengruppen Tagging-API in der AWS Tools for PowerShell Core erstellen und ausführen.
- Sie können Programme mit allen verfügbaren Programmen erstellen und ausführen, AWS SDKsindem Sie das Tagging für Ressourcengruppen verwenden APIs, z. B. das Tagging APIs für Python oder das Tagging APIs für Java.

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

Fügen Sie ausgewählten Ressourcen Stichwörter hinzu

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 gleichzeitig bearbeiten können. Sie können auch die Tag-Werte für eine einzelne Ressource bearbeiten. Weitere Informationen finden Sie unter Bestehende Tags für eine ausgewählte Ressource anzeigen und bearbeiten.

1. Öffnen Sie die Tag-Editor-Konsole und senden Sie eine Abfrage, die mehrere Ressourcen zurückgibt, die Sie taggen möchten.
2. Aktivieren Sie in der Ergebnistabelle Ihrer Abfrage „Zu taggende Ressourcen suchen“ die Kontrollkästchen neben den Ressourcen, denen Sie Tags hinzufügen möchten. Geben Sie oben in der Tabelle im Feld Ressourcen filtern eine Textzeichenfolge ein, um nach einem Teil des Namens, der ID, der Tagschlüssel oder der Tagwerte einer Ressource zu filtern. Beachten Sie in der Spalte Tags (Tags), dass auf die Ressourcen in den Ergebnissen bereits Tags angewendet wurden.
3. Aktivieren Sie das Kontrollkästchen für eine oder mehrere Ressourcen und wählen Sie dann Tags der ausgewählten Ressourcen verwalten aus.
4. Klicken Sie auf der SeiteManage tags (Tags verwalten) auf die Ressourcen, die Sie ausgewählt haben. Ihre ursprüngliche Abfrage hat zwar mehr Ressourcen zurückgegeben, Sie fügen jedoch nur den Ressourcen Tags 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 von Benutzern zugewiesene Tags nähern. AWS Die generierten 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 Ihren ausgewählten Ressourcen vorhanden ist.

6. Wenn Sie mit dem Hinzufügen von Tags fertig sind, wählen Sie Überprüfen und Änderungen übernehmen 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 im selben Browser-Tab. 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 Problembehandlung bei Tag-Änderungen. Nachdem Sie die erfolglosen Tagänderungen behoben haben (z. B. unzureichende Berechtigungen), können Sie erneut versuchen, die Tag-Änderungen an Ressourcen durchzuführen, für die Tag-Änderungen fehlgeschlagen sind. Weitere Informationen finden Sie unter the section called “Fehlgeschlagene Tag-Änderungen erneut versuchen”.

Bearbeiten Sie die Tags der ausgewählten 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 Abrechnungs- und Verwaltungsdienste bereitzustellen. Tags sind nicht dazu bestimmt, für private oder sensible Daten verwendet zu werden.

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.
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 die 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, wird die Option Ausgewählte Ressourcen haben unterschiedliche Tag-Werte im Feld Tag-Wert angezeigt. In diesem Fall öffnet sich eine Dropdownliste mit allen verfügbaren Werten für diesen Tag-Schlüssel in den ausgewählten Ressourcen, wenn Sie den Cursor in dem Feld platzieren.

   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 Dropdownliste tragen dazu bei, dass die Tag-Werte ressourcenübergreifend konsistent bleiben. 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 Stichwörtern fertig sind, wählen Sie „Änderungen überprüfen und anwenden“.
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 im selben Browser-Tab. 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 Problembehandlung bei Tag-Änderungen. Nachdem Sie die Hauptursachen für erfolglose Tag-Änderungen behoben haben (z. B. unzureichende Berechtigungen), können Sie erneut versuchen, Tag-Änderungen an Ressourcen vorzunehmen, für die Tag-Änderungen fehlgeschlagen sind. Weitere Informationen finden Sie unter the section called “Fehlgeschlagene Tag-Änderungen erneut versuchen”.

Entfernen Sie 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 die 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.

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 im selben Browser-Tab. 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 Hauptursachen für erfolglose Tag-Änderungen behoben haben (z. B. unzureichende Berechtigungen), können Sie erneut versuchen, Tag-Änderungen an Ressourcen vorzunehmen, für die Tag-Änderungen fehlgeschlagen sind. Weitere Informationen finden Sie unter the section called “Fehlgeschlagene Tag-Änderungen erneut versuchen”.

Verwendung von Tags in IAM-Berechtigungsrichtlinien

AWS Identity and Access Management (IAM) verwenden Sie AWS-Service , um Berechtigungsrichtlinien zu erstellen und zu verwalten, mit denen festgelegt wird, wer auf Ihre AWS Ressourcen zugreifen kann. Jeder Versuch, auf einen AWS Dienst zuzugreifen oder eine AWS Ressource zu lesen oder zu schreiben, wird durch eine IAM-Richtlinie gesteuert.

Diese Richtlinien ermöglichen Ihnen einen detaillierten Zugriff auf Ihre Ressourcen. Eine der Funktionen, die Sie zur Feinabstimmung dieses Zugriffs verwenden können, ist das `Condition`Element der Richtlinie. Mit diesem Element können Sie die Bedingungen angeben, die mit der Anfrage übereinstimmen müssen, um festzustellen, ob die Anfrage bearbeitet werden kann. Mit dem `Condition` Element können Sie unter anderem Folgendes überprüfen:

- Tags, die an den Benutzer oder die Rolle angehängt sind, die die Anfrage gestellt haben.
- Tags, die an die Ressource angehängt sind, die das Objekt der Anfrage ist.

Tags und attributebasierte Zugriffskontrolle

Tags können ein wichtiger Bestandteil Ihrer AWS Zugriffskontrollstrategie sein. Informationen zur Verwendung von Tags als Attribute in einer Strategie zur attributebasierten Zugriffskontrolle (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.

Ein umfangreiches Tutorial, das zeigt, wie Sie mithilfe von Tags Zugriff auf verschiedene Projekte und Gruppen gewähren können, finden Sie im IAM-Tutorial: Definieren von Berechtigungen für den Zugriff auf AWS Ressourcen auf der Grundlage von Tags im Benutzerhandbuch.AWS Identity and Access Management

Wenn Sie einen SAML-basierten Identitätsanbieter (IdP) für Single Sign-In verwenden, können Sie Tags an die angenommenen Rollen anhängen, die Ihren Benutzern Zugriff gewähren. Weitere Informationen finden Sie unter IAM-Tutorial: Verwenden von SAML-Sitzungs-Tags für ABAC im Benutzerhandbuch.AWS Identity and Access Management

Bedingungsschlüssel, die sich auf Tags beziehen

In der folgenden Tabelle werden die Bedingungsschlüssel beschrieben, die Sie in einer IAM-Berechtigungsrichtlinie verwenden können, um den Zugriff anhand von Tags zu steuern. Mit diesen Bedingungsschlüsseln können Sie Folgendes tun:

- Vergleichen Sie die Tags auf dem Principal, der die Operation aufruft.
- Vergleichen Sie die Tags, die der Operation als Parameter zur Verfügung gestellt wurden.
- Vergleichen Sie die Tags, die der Ressource zugeordnet sind, auf die der Vorgang zugreifen würde.

Vollständige Informationen zu einem Bedingungsschlüssel und seiner Verwendung finden Sie auf der Seite, die in der Spalte Name des Bedingungsschlüssels verlinkt ist.

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

Beispiel für IAM-Richtlinien, die Tags verwenden

Example Beispiel 1: Benutzer dazu zwingen, bei der Erstellung einer Ressource ein bestimmtes Tag anzuhängen

Das folgende Beispiel für eine IAM-Berechtigungsrichtlinie zeigt, wie Sie den Benutzer, der die Tags einer IAM-Richtlinie erstellt oder ändert, zwingen können, dem Schlüssel ein Tag beizufügen. `Owner` Außerdem erfordert die Richtlinie, dass der Wert des Tags auf denselben Wert gesetzt wird wie das Tag, das derzeit `Owner` dem aufrufenden Principal zugeordnet ist. Damit diese Strategie funktioniert, muss allen Prinzipalen ein `Owner` Tag angehängt werden, und Benutzer müssen daran gehindert werden, dieses Tag zu ändern. Wenn versucht wird, eine Richtlinie zu erstellen oder zu ändern, ohne das `Owner` Tag einzubeziehen, stimmt die Richtlinie nicht überein und der Vorgang ist nicht zulässig.

JSON

```
{
    "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 Sie Tags, um den Zugriff auf eine Ressource auf ihren „Besitzer“ zu beschränken

Das folgende Beispiel für eine IAM-Berechtigungsrichtlinie ermöglicht es dem Benutzer, eine laufende EC2 Amazon-Instance nur dann zu beenden, wenn der aufrufende Principal mit demselben `project` Tag-Wert wie die Instance gekennzeichnet ist.

JSON

```
{
  "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 attributebasierte Zugriffskontrolle (ABAC). Weitere Informationen und weitere Beispiele für die Verwendung von IAM-Richtlinien zur Implementierung einer tagbasierten Zugriffskontrollstrategie finden Sie in den folgenden Themen im Benutzerhandbuch:AWS Identity and Access Management

- Steuern des Zugriffs auf AWS Ressourcen mithilfe von Tags
- Steuern des Zugriffs auf und für IAM-Benutzer und -Rollen mithilfe von Tags
- IAM-Tutorial: Berechtigungen für den Zugriff auf AWS Ressourcen anhand von Tags definieren — 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 erstellen AWS Organizations. Mithilfe von Tag-Richtlinien können Sie Tags für alle Ressourcen in den Konten Ihrer Organisation 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 Auffinden und Korrigieren nicht konformer Tags. Um diese Aufgaben auszuführen, verwenden Sie die Tag Editor-Konsole.

Voraussetzungen und Berechtigungen

Bevor Sie die Einhaltung der Tag-Richtlinien im Tag Editor bewerten können, müssen Sie die Anforderungen erfüllen und die erforderlichen Berechtigungen einrichten.

Themen

- Voraussetzungen für die Bewertung der Einhaltung der Tag-Richtlinien
- Berechtigungen zur Bewertung der Einhaltung der Vorschriften für ein Konto
- Berechtigungen für die Bewertung der unternehmensweiten Einhaltung
- Amazon S3 S3-Bucket-Richtlinie für die Berichtsspeicherung

Voraussetzungen für die Bewertung der Einhaltung der Tag-Richtlinien

Für die Bewertung der Einhaltung der Tag-Richtlinien ist Folgendes erforderlich:

- Sie müssen die Funktion zunächst in AWS Organizations Tag-Richtlinien aktivieren und Tag-Richtlinien erstellen und anhängen. Weitere Informationen finden Sie auf den folgenden Seiten des AWS Organizations Benutzerhandbuchs:
  - Voraussetzungen und Berechtigungen für die Verwaltung von Tag-Richtlinien
  - Aktivieren von Tag-Richtlinien
  - Erste Schritte mit Tag-Richtlinien
- Um unzulässige Tags auf den Ressourcen eines Kontos zu finden, benötigen Sie die Anmeldedaten für dieses Konto und die unter aufgeführten Berechtigungen. Berechtigungen zur Bewertung der Einhaltung der Vorschriften für ein Konto
- Um die unternehmensweite Einhaltung der Vorschriften beurteilen zu können, benötigen Sie die Anmeldedaten für das Verwaltungskonto der Organisation und die unter aufgeführten

Berechtigungen. Berechtigungen für die Bewertung der unternehmensweiten Einhaltung Sie können den Konformitätsbericht nur im Osten der AWS-Region USA (Nord-Virginia) anfordern.

Berechtigungen zur Bewertung der Einhaltung der Vorschriften für ein Konto

Für die Suche nach nicht konformen Tags auf den Ressourcen eines Kontos sind die folgenden Berechtigungen erforderlich:

- `organizations:DescribeEffectivePolicy`— Um den Inhalt der aktuellen Tag-Richtlinie für das Konto abzurufen.
- `tag:GetResources`— Um eine Liste von Ressourcen zu erhalten, die nicht der beigefügten Tag-Richtlinie entsprechen.
- `tag:TagResources`— Um Tags hinzuzufügen oder zu aktualisieren. Sie benötigen außerdem dienstspezifische Berechtigungen, um Tags zu erstellen. Um beispielsweise Ressourcen in Amazon Elastic Compute Cloud (Amazon EC2) zu taggen, benötigen Sie Berechtigungen für`ec2:CreateTags`.
- `tag:UnTagResources`— Um ein Tag zu entfernen. Sie benötigen außerdem dienstspezifische Berechtigungen, um Tags zu entfernen. Um beispielsweise Ressourcen in Amazon zu entkennzeichnen EC2, benötigen Sie Berechtigungen für`ec2:DeleteTags`.

Die folgende Beispielrichtlinie AWS Identity and Access Management (IAM) bietet Berechtigungen zur Bewertung der Tag-Konformität für ein Konto.

JSON

```
{
    "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 für die Bewertung der unternehmensweiten Einhaltung

Für die Bewertung der unternehmensweiten Einhaltung der Tag-Richtlinien sind die folgenden Berechtigungen erforderlich:

- `organizations:DescribeEffectivePolicy`— Um den Inhalt der Tag-Richtlinie abzurufen, die der Organisation, Organisationseinheit (OU) oder dem Konto zugeordnet ist.
- `tag:GetComplianceSummary`— Um eine Zusammenfassung der nicht konformen Ressourcen in allen Konten der Organisation abzurufen.
- `tag:StartReportCreation`— Um die Ergebnisse der letzten Konformitätsprüfung in eine Datei zu exportieren. Die unternehmensweite Einhaltung der Vorschriften wird alle 48 Stunden bewertet.
- `tag:DescribeReportCreation`— Um den Status der Berichtserstellung zu überprüfen.
- `s3:ListAllMyBuckets`— Zur Unterstützung beim Zugriff auf den unternehmensweiten Compliance-Bericht.
- `s3:GetBucketAcl`— Um die Access Control List (ACL) des Amazon S3 S3-Buckets zu überprüfen, der den Konformitätsbericht erhält.
- `s3:GetObject`— Um den Compliance-Bericht aus dem service-eigenen Amazon S3 S3-Bucket abzurufen.
- `s3:PutObject`— Um den Konformitätsbericht im angegebenen Amazon S3 S3-Bucket zu platzieren.

Wenn der Amazon S3 S3-Bucket, in den der Bericht übermittelt wird, über SSE-KMS verschlüsselt ist, benötigen Sie auch die `kms:GenerateDataKey` Erlaubnis für diesen Bucket.

Die folgende Beispiel-IAM-Richtlinie bietet Berechtigungen für die Bewertung der unternehmensweiten Einhaltung. Ersetzen Sie jede durch Ihre *`placeholder`* eigenen Informationen:

- *`bucket_name`*— Ihr Amazon S3 S3-Bucket-Name
- *`organization_id`*— Die ID Ihrer Organisation

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "EvaluateAccountCompliance",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeEffectivePolicy",
                "tag:StartReportCreation",
                "tag:DescribeReportCreation",
                "tag:GetComplianceSummary",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "GetBucketAclForReportDelivery",
            "Effect": "Allow",
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::bucket_name",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "tagpolicies.tag.amazonaws.com"
                }
            }
        },
        {
            "Sid": "GetObjectForReportDelivery",
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::*/tag-policy-compliance-reports/*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "tagpolicies.tag.amazonaws.com"
                }
            }
        },
        {
            "Sid": "PutObjectForReportDelivery",
            "Effect": "Allow",
            "Action": "s3:PutObject",
```

```
            "Resource": "arn:aws:s3:::bucket_name/AwsTagPolicies/organization_id/
*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "tagpolicies.tag.amazonaws.com"
                },
                "StringLike": {
                    "s3:x-amz-copy-source": "*/tag-policy-compliance-reports/*"
                }
            }
        }
    ]
}
```

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

Amazon S3 S3-Bucket-Richtlinie für die Berichtsspeicherung

Um einen unternehmensweiten Compliance-Bericht zu erstellen, muss die Identität, mit der Sie die `StartReportCreation` API aufrufen, Zugriff auf einen Amazon Simple Storage Service (Amazon S3) -Bucket in der Region USA Ost (Nord-Virginia) haben, um den Bericht zu speichern. Tag Policies verwendet die Anmeldeinformationen der aufrufenden Identität, um den Compliance-Bericht an den angegebenen Bucket zu senden.

Wenn der Bucket und die Identität, die zum Aufrufen der `StartReportCreation` API verwendet werden, zu demselben Konto gehören, sind für diesen Anwendungsfall keine zusätzlichen Amazon S3 S3-Bucket-Richtlinien erforderlich.

Wenn sich das Konto, das mit der für den `StartReportCreation` API-Aufruf verwendeten Identität verknüpft ist, von dem Konto unterscheidet, das den Amazon S3 S3-Bucket besitzt, muss die folgende Bucket-Richtlinie an den Bucket angehängt werden. Ersetzen Sie jede *`placeholder`* durch Ihre eigenen Informationen:

- *`bucket_name`*— Ihr Amazon S3 S3-Bucket-Name
- *`organization_id`*— Die ID Ihrer Organisation
- *`identity_ARN`*— Der ARN der IAM-Identität, die zum Aufrufen der `StartReportCreation` API verwendet wurde

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CrossAccountTagPolicyACL",
            "Effect": "Allow",
            "Principal": {
                "AWS": "identity_ARN"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::bucket_name"
         },
         {
            "Sid": "CrossAccountTagPolicyBucketDelivery",
            "Effect": "Allow",
            "Principal": {
                "AWS": "identity_ARN"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::bucket_name/AwsTagPolicies/organization_id/
*"
         }
    ]
}
```

Bewertung der Einhaltung der Vorschriften für ein Konto

Sie können überprüfen, ob ein Konto in Ihrer Organisation die geltenden Tag-Richtlinien einhält.

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

Die geltende Tag-Richtlinie legt die Tag-Regeln fest, die für ein Konto gelten. Die effektive Tag-Richtlinie ist die Zusammenfassung aller Tag-Richtlinien, die das Konto erbt, sowie aller Tag-Richtlinien, die direkt mit dem Konto verknüpft sind. Wenn Sie dem Organisationsstamm eine Tag-Richtlinie hinzufügen, gilt dies für alle Konten in Ihrer Organisation. Wenn Sie einer Organisationseinheit (OU) eine Tag-Richtlinie zuordnen, gilt sie für alle Konten, OUs die zur Organisationseinheit 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, benötigen Sie die folgenden Berechtigungen:

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

Um zu überprüfen, ob ein Konto die geltenden Tag-Richtlinien einhält (Konsole)

1. Öffnen Sie die Konsole mit den Tag-Richtlinien, während Sie bei dem Konto angemeldet sind, dessen Einhaltung Sie überprüfen möchten.
2. Im Abschnitt Effektive Tag-Richtlinie werden das Datum der letzten Aktualisierung und die definierten Tag-Schlüssel angezeigt. Sie können einen Tagschlüssel erweitern, um Informationen zu seinen Werten, zur Fallbehandlung und darüber, ob die Werte für bestimmte Ressourcentypen durchgesetzt werden, anzuzeigen.

   > **Note**
   >
   > Wenn Sie beim Verwaltungskonto angemeldet sind, müssen Sie ein Konto auswählen, um die geltenden Richtlinien und Compliance-Informationen zu sehen.

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

Ergebnisse in Echtzeit werden im Bereich 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 den Ort zu öffnen, an AWS-Service dem 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 Tag-Richtlinien-Konsole zum Abschnitt Effektive Tag-Richtlinie für das Konto. Sie können einen Tag-Schlüssel erweitern, um die zugehörigen Tag-Regeln anzuzeigen.

6. Wiederholen Sie das Suchen und Korrigieren von Stichwörtern, bis die Kontoressourcen, die Ihnen wichtig sind, in jeder Region den Vorschriften entsprechen.

Um nicht konforme Tags zu finden (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 finden Sie unter Verwenden von Tag-Richtlinien AWS CLI im im AWS Organizations Benutzerhandbuch. AWS CLI
- AWS Resource Groups Tagging API:
  - GetResources
  - TagResources
  - UntagResources

Nächste Schritte

Wir empfehlen Ihnen, den Vorgang zur Suche und Behebung von Compliance-Problemen zu wiederholen. Fahren Sie fort, bis die Ressourcen des Accounts, die Ihnen wichtig sind, den in jeder Region geltenden Tag-Richtlinien entsprechen.

Das Auffinden und Korrigieren nicht konformer Tags ist aus mehreren Gründen ein iterativer Prozess, unter anderem aus den folgenden Gründen:

- Die Verwendung von Tag-Richtlinien in Ihrem Unternehmen kann sich im Laufe der Zeit ändern.
- Es braucht Zeit, um bei der Erstellung von Ressourcen Veränderungen in Ihrer Organisation zu bewirken.
- Die Einhaltung von Vorschriften kann sich jederzeit ändern, wenn eine neue Ressource erstellt wird oder wenn einer Ressource neue Tags zugewiesen werden.
- Die aktuelle Tag-Richtlinie eines Accounts wird immer dann aktualisiert, wenn eine Tag-Richtlinie an das Konto angehängt oder davon getrennt wird. Die effektive Tag-Richtlinie wird auch aktualisiert, wenn Änderungen an den Tag-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 Einhaltung der Vorschriften.

Bewertung der unternehmensweiten Einhaltung der Vorschriften

Sie können überprüfen, ob Ihre Organisation die geltenden Tag-Richtlinien einhält. Sie können einen Bericht erstellen, der alle markierten Ressourcen in Konten in Ihrer Organisation auflistet und angibt, ob jede Ressource den geltenden Tag-Richtlinien entspricht.

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

Sie können den Bericht `us-east-1` AWS-Region nur über das Verwaltungskonto Ihrer Organisation erstellen. Das Konto, das den Bericht generiert, muss Zugriff auf einen Amazon S3 S3-Bucket in der

Region USA Ost (Nord-Virginia) haben. Dem Bucket muss eine Bucket-Richtlinie angehängt sein, wie in der Amazon S3 S3-Bucket-Richtlinie zum Speichern des Berichts dargestellt.

Um einen unternehmensweiten Compliance-Bericht zu erstellen, benötigen Sie die folgenden Berechtigungen:

- `organizations:DescribeEffectivePolicy`
- `tag:GetComplianceSummary`
- `tag:StartReportCreation`
- `tag:DescribeReportCreation`
- `s3:ListAllMyBuckets`
- `s3:GetBucketAcl`
- `s3:GetObject`
- `s3:PutObject`

Ein Beispiel für eine IAM-Richtlinie, in der diese Berechtigungen angezeigt werden, finden Sie unter Berechtigungen zur Bewertung der unternehmensweiten Einhaltung.

So erstellen Sie einen unternehmensweiten Compliance-Bericht (Konsole)

1. Öffnen Sie die Konsole „Tag-Richtlinien“.
2. Wählen Sie die Stammregisterkarte Diese Organisation und wählen Sie unten auf der Seite die Option Bericht erstellen aus.
3. Geben Sie auf dem Bildschirm Bericht erstellen an, wo der Bericht gespeichert werden soll.
4. Wählen Sie Export starten.

Wenn der Bericht vollständig ist, können Sie ihn im Bereich Bericht über Verstöße auf der Stammregisterkarte Organisation herunterladen.

> **Hinweise**
>
> Die unternehmensweite Einhaltung der Vorschriften wird alle 48 Stunden überprüft. Daraus resultiert Folgendes:
>
> - Es kann bis zu 48 Stunden dauern, bis Änderungen an einer Tag-Richtlinie oder an Ressourcen im unternehmensweiten Compliance-Bericht angezeigt werden. Angenommen,

Sie haben eine Tag-Richtlinie, die ein neues standardisiertes Tag für einen Ressourcentyp definiert. Ressourcen dieses Typs, die nicht über dieses Tag verfügen, können im Bericht bis zu 48 Stunden lang als konform angezeigt werden.

- Sie können den Bericht zwar jederzeit erstellen, die Berichtsergebnisse werden jedoch erst aktualisiert, wenn die nächste Auswertung abgeschlossen ist.
- In der NoncompliantKeysSpalte werden Tag-Schlüssel für die Ressource aufgeführt, die nicht der geltenden Tag-Richtlinie entsprechen.
- In der KeysWithNonCompliantValuesSpalte werden die in der effektiven Richtlinie definierten Schlüssel aufgeführt, die sich auf der Ressource befinden und entweder falsche Fallbehandlung oder nicht konforme Werte aufweisen.
- Wenn Sie ein Dokument schließen AWS-Konto , das Mitglied der Organisation war, kann es bis zu 90 Tage lang weiterhin im Tag-Compliance-Bericht erscheinen.

Um einen unternehmensweiten Compliance-Bericht (AWS CLI, AWS API) zu erstellen

Verwenden Sie die folgenden Befehle und Operationen, um einen unternehmensweiten Compliance-Bericht zu erstellen, dessen 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 finden Sie unter Verwenden von Tag-Richtlinien im AWS CLI im AWS Organizations Benutzerhandbuch. AWS CLI
- AWS API:
  - StartReportCreation
  - DescribeReportCreation
  - GetComplianceSummary

Überwachen Sie Tag-Änderungen mit serverlosen Workflows und Amazon EventBridge

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

Tag-Änderungen generieren Ereignisse EventBridge

EventBridge liefert einen Stream von Systemereignissen, die Änderungen an AWS Ressourcen beschreiben, nahezu in Echtzeit. Viele AWS Ressourcen unterstützen Tags, bei denen es sich um benutzerdefinierte Attribute handelt, mit denen Ressourcen einfach organisiert und kategorisiert AWS werden können. Typische Anwendungsfälle für Tags sind Kostenzuweisung, Kategorisierung, Zugriffskontrolle, Sicherheit und Automatisierung.

Mit EventBridge können Sie nach Änderungen an Tags suchen und den Status der Tags auf Ressourcen verfolgen. AWS Um eine ähnliche Funktionalität zu erreichen, mussten Sie zuvor möglicherweise kontinuierlich mehrere Anrufe abgefragt APIs und orchestriert haben. Jetzt wird bei jeder Änderung an einem Tag, einschließlich einzelner Dienste APIs, Tag-Editor und Tagging-API, die Tag-Änderung bei einem Ressourcenereignis ausgelöst. 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.

```
{
  "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 auf oberster Ebene:

- Version — Standardmäßig ist dieser Wert bei allen Ereignissen auf `0` (Null) gesetzt.
- id — Für jedes Ereignis wird ein eindeutiger Wert generiert. Dies kann bei der Nachverfolgung von Ereignissen hilfreich sein, wenn sie Regeln zu Zielen durchlaufen und verarbeitet werden.
- detail-type — Identifiziert in Kombination mit dem `source` Feld die Felder und Werte, die im Detailfeld erscheinen.
- Quelle — Identifiziert den Service, der die Quelle des Ereignisses war. Die Quelle für Tag-Änderungen ist`aws.tag`.
- Zeit — Der Zeitstempel des Ereignisses.
- Region — Identifiziert den AWS-Region Ort, an dem das Ereignis seinen Ursprung hat.
- resources — Dieses JSON-Array enthält Amazon-Ressourcennamen (ARNs), die Ressourcen identifizieren, die an dem Ereignis beteiligt sind. Dies ist die Ressource, bei der sich die Tags geändert haben.
- Detail — Ein JSON-Objekt, dessen Inhalt je nach Ereignistyp unterschiedlich ist. Für Tag-Änderungen auf einer Ressource sind die folgenden detaillierten Felder enthalten:
  - changed-tag-keys— Die Tag-Schlüssel, die sich durch dieses Ereignis geändert haben.
  - service — Der Dienst, zu dem die Ressource gehört. In diesem Beispiel ist `ec2` der Service Amazon EC2.
  - resource-type — Der Ressourcentyp des Dienstes. In diesem Beispiel handelt es sich um eine EC2 Amazon-Instance.

- 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 Event Patterns im EventBridge Amazon-Benutzerhandbuch.

Mithilfe von können Sie Regeln erstellen EventBridge, die bestimmten Ereignismustern auf der Grundlage der verschiedenen Felder entsprechen. Wie das geht, zeigen wir im Tutorial. Außerdem zeigen wir, wie eine EC2 Amazon-Instance automatisch gestoppt werden kann, wenn der Instance kein bestimmtes Tag zugeordnet ist. Wir verwenden die EventBridge Felder, um ein Muster zu erstellen, das den Tag-Ereignissen für die Instanz entspricht, die eine Lambda-Funktion startet.

Lambda und Serverless

AWS Lambda folgt dem serverlosen Paradigma zur Ausführung von Code in der Cloud. Sie führen Code nur dann aus, wenn er benötigt wird, ohne an Server zu denken. Sie zahlen nur für die exakte Rechenzeit, die Sie tatsächlich nutzen. Auch wenn es als serverlos bezeichnet wird, bedeutet das nicht, dass es keine Server gibt. Serverlos bedeutet in diesem Zusammenhang, dass Sie die Server, auf denen Ihr Code ausgeführt wird, nicht bereitstellen, konfigurieren oder verwalten müssen. AWS erledigt all das für Sie, sodass Sie sich auf Ihren Code konzentrieren können. Weitere Informationen zu Lambda finden Sie in der AWS Lambda Produktübersicht.

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

Wenn Ihr AWS Ressourcenpool AWS-Konten , den Sie verwalten, wächst, können Sie Tags verwenden, um Ihre Ressourcen einfacher zu kategorisieren. Tags werden häufig für kritische Anwendungsfälle wie Kostenverteilung und Sicherheit verwendet. Um AWS Ressourcen effektiv zu verwalten, müssen Ihre Ressourcen konsistent gekennzeichnet werden. Wenn eine Ressource bereitgestellt wird, erhält sie häufig alle entsprechenden Tags. Ein späterer Prozess kann jedoch zu einer Änderung des Tags führen, was zu einer Abweichung von der unternehmenseigenen Tag-Richtlinie führt. Indem Sie die Änderungen an Ihren Tags überwachen, können Sie Abweichungen bei den Stichwörtern erkennen und sofort reagieren. Auf diese Weise können Sie sich darauf verlassen,

dass die Prozesse, die von der richtigen Kategorisierung Ihrer Ressourcen abhängen, zu den gewünschten Ergebnissen führen.

Das folgende Beispiel zeigt, wie Sie Tag-Änderungen auf EC2 Amazon-Instances überwachen können, um sicherzustellen, dass eine angegebene Instance weiterhin über die erforderlichen Tags verfügt. Wenn sich die Tags der Instanz ändern und die Instance nicht mehr über die erforderlichen Tags verfügt, wird eine Lambda-Funktion aufgerufen, um die Instance automatisch herunterzufahren. Warum sollten Sie das tun wollen? Es stellt sicher, dass alle Ressourcen gemäß Ihrer unternehmenseigenen Tag-Richtlinie gekennzeichnet sind, um eine effektive Kostenverteilung zu gewährleisten oder um der Sicherheit auf der Grundlage der attributebasierten Zugriffskontrolle (ABAC) vertrauen zu können.

> **Important**
>
> Wir empfehlen dringend, dass Sie dieses Tutorial in einem Konto durchführen, das nicht zur Produktion gehört, sodass Sie wichtige Instanzen nicht versehentlich herunterfahren können. Der Beispielcode in diesem Tutorial beschränkt die Auswirkungen dieses Szenarios bewusst nur auf die Instanzen in einer Instanzliste. IDs Sie müssen die Liste mit der Instanz aktualisieren IDs , die Sie für den Test herunterfahren möchten. Dadurch wird sichergestellt, dass Sie nicht versehentlich jede Instanz in einer Region in Ihrer herunterfahren können AWS-Konto.
>
> Stellen Sie nach dem Testen sicher, dass alle Ihre Instanzen gemäß der Tagging-Strategie Ihres Unternehmens gekennzeichnet sind. Anschließend können Sie den Code entfernen, der die Funktion nur IDs auf die Instanz in der Liste beschränkt.

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

> **Note**
>
> Wenn Ihre Konsole standardmäßig eine andere Region verwendet, stellen Sie sicher, dass Sie bei jedem Konsolenwechsel die Region, die Sie in diesem Tutorial verwenden, wechseln. Ein häufiger Grund dafür, dass dieses Tutorial fehlschlägt, ist, dass sich die Instanz und die Funktion in zwei verschiedenen Regionen befinden.

Wenn Sie eine andere Region als verwendenus-east-1, stellen Sie sicher, dass Sie alle Verweise in den folgenden Codebeispielen auf Ihre gewählte Region ändern.

Themen

- Schritt 1. So erstellen Sie die Lambda-Funktion:
- Schritt 2. Richten Sie die erforderlichen IAM-Berechtigungen ein
- Schritt 3. Führen Sie einen Vortest Ihrer Lambda-Funktion durch
- Schritt 4. Erstellen Sie die EventBridge Regel, die die Funktion startet
- Schritt 5. Testen Sie die komplette Lösung
- Zusammenfassung des Tutorials

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 anschließend „Von Grund auf neu erstellen“.
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 die Standardwerte für alle anderen Felder bei und wählen Sie „Funktion erstellen“.
6. Öffnen Sie auf der `AutoEC2Termination` Detailseite auf der Registerkarte Code die Datei index.js, um den zugehörigen Code anzuzeigen.

   - Wenn eine Registerkarte mit index.js geöffnet ist, können Sie das Bearbeitungsfeld auf dieser Registerkarte auswählen, um den Code zu bearbeiten.
   - Wenn eine Registerkarte mit index.js nicht geöffnet ist, klicken Sie im Navigationsbereich unter dem Ordner Auto EC2 Terminator sekundär auf die Datei index.js. 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 Deploy, um Ihre Änderungen zu speichern und die neue Version der Funktion zu aktivieren.

Diese Lambda-Funktion überprüft die Tags einer EC2 Amazon-Instance, wie vom Tag-Änderungsereignis in EventBridge gemeldet. In diesem Beispiel versucht die Funktion, die Instance zu stoppen, wenn der Instanz in dem Ereignis der erforderliche Tag-Schlüssel fehlt `valid-key` oder wenn das Tag nicht den Wert `valid-value` hat. 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. Richten Sie die erforderlichen IAM-Berechtigungen ein

Bevor die Funktion erfolgreich ausgeführt werden kann, müssen Sie der Funktion die Berechtigung zum Stoppen einer EC2 Instanz erteilen. Die AWS angegebene Rolle lambda_basic_executionhat diese Berechtigung nicht. In diesem Tutorial ändern Sie die standardmäßige IAM-Berechtigungsrichtlinie, die der genannten `AutoEC2Termination-role-`*`uniqueid`* Ausführungsrolle der Funktion zugeordnet ist. Für dieses Tutorial ist `ec2:StopInstances` mindestens eine zusätzliche Berechtigung erforderlich.

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

Um eine IAM-Berechtigungsrichtlinie zu erstellen und sie an die Ausführungsrolle der Lambda-Funktion anzuhängen

1. Öffnen Sie in einem anderen Browser-Tab oder Fenster die Rollenseite der IAM-Konsole.
2. Beginnen Sie mit der Eingabe des Rollennamens**`AutoEC2Termination`**, und wählen Sie den Rollennamen aus, wenn er in der Liste angezeigt wird.
3. Wählen Sie auf der Übersichtsseite der Rolle die Registerkarte Berechtigungen und dann den Namen der Richtlinie aus, die bereits angehängt ist.
4. Wählen Sie auf der Übersichtsseite der Richtlinie die Option Richtlinie bearbeiten aus.
5. Wählen Sie auf der Registerkarte Visual Editor die Option Zusätzliche Berechtigungen hinzufügen aus.
6. Wählen Sie unter Service die Option EC2aus.
7. Wählen Sie für Aktionen die Option StopInstances. Sie können **`Stop`** in die Suchleiste etwas eingeben und dann auswählen, `StopInstances` wann sie angezeigt wird.
8. Wählen Sie unter Ressourcen die Option Alle Ressourcen, dann Richtlinie überprüfen und anschließend Änderungen speichern aus.

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

   Ihre endgültige Richtlinie sollte dem folgenden Beispiel ähneln.

   JSON

```
{
    "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 Vortest Ihrer Lambda-Funktion durch

In diesem Schritt reichen Sie ein Testereignis für Ihre Funktion ein. Die Lambda-Testfunktion funktioniert, indem ein manuell bereitgestelltes Testereignis gesendet wird. Die Funktion verarbeitet das Testereignis so, als ob das Ereignis von EventBridge gekommen wäre. Sie können mehrere Testereignisse mit unterschiedlichen Werten definieren, um all die verschiedenen Teile Ihres Codes auszuführen. In diesem Schritt reichen Sie ein Testereignis ein, das darauf hinweist, dass sich die Tags einer EC2 Amazon-Instance geändert haben und die neuen Tags nicht den erforderlichen Tag-Schlüssel und -Wert enthalten.

Um Ihre Lambda-Funktion zu testen

1. Kehren Sie zum Fenster oder zur Registerkarte mit der Lambda-Konsole zurück und öffnen Sie die Registerkarte Test für Ihre EC2Auto-Termination-Funktion.
2. Wählen Sie Neues Ereignis erstellen.
3. Geben Sie für Event name (Ereignisname) **`SampleBadTagChangeEvent`** ein.
4. Ersetzen Sie in der Event-JSON den Text durch das Beispielereignis, das im folgenden Beispieltext gezeigt wird. Sie müssen die Konten, die Region oder die Instanz-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 fehlgeschlagen zu sein, aber das ist in Ordnung.

   Auf der Registerkarte Ausführungsergebnisse unter Antwort sollte der folgende Fehler angezeigt werden.

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

   Der Fehler tritt auf, weil die im Testereignis angegebene Instanz nicht existiert.

   Die Informationen auf der Registerkarte Ausführungsergebnisse im Abschnitt Funktionsprotokolle zeigen, dass Ihre Lambda-Funktion erfolgreich versucht hat, eine EC2 Instanz zu stoppen. Dies schlug jedoch fehl, da der Code zunächst versucht, die `DryRun`Instanz zu stoppen, was darauf hinwies, dass die Instanz-ID nicht gültig war.

```
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 zu beweisen, dass der Code nicht versucht, die Instanz zu stoppen, wenn das richtige Tag verwendet wird, können Sie ein weiteres Testereignis erstellen und einreichen.

   Wählen Sie über der Codequelle den Tab Test aus. In der Konsole wird Ihr vorhandenes SampleBadTagChangeEventTestereignis angezeigt.

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 auf zu zu ändern**`valid-value`**.

10. Wählen Sie oben im Fenster „Testereignis“ die Option „Speichern“ und anschließend „Testen“ aus.

In der Ausgabe wird Folgendes angezeigt, was zeigt, dass die Funktion das gültige Tag erkennt und nicht versucht, die Instanz 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 Sie die EventBridge Regel, die die Funktion startet

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

Um die Regel zu erstellen EventBridge

1. Öffnen Sie in einer anderen Browser-Registerkarte oder einem anderen Browserfenster die EventBridge Konsole und öffnen Sie die Seite „Regel erstellen“.
2. Geben Sie als Namen ein**`ec2-instance-rule`**, und wählen Sie dann Weiter aus.
3. Scrollen Sie nach unten zu Erstellungsmethode und wählen Sie Benutzerdefiniertes Muster (JSON-Editor) aus.
4. Fügen Sie den folgenden Mustertext in das Bearbeitungsfeld ein und wählen Sie dann Weiter.

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

```
    ]
  }
}
```

Diese Regel ordnet `Tag Change on Resource` Ereignisse für EC2 Amazon-Instances zu 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 Funktion Automatische EC2 Terminierung aus, die Sie zuvor erstellt haben, und klicken Sie dann auf Weiter.
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 Erlaubnis erteilt EventBridge , die angegebene Lambda-Funktion aufzurufen.

Schritt 5. Testen Sie die komplette Lösung

Sie können Ihr Endergebnis testen, indem Sie eine EC2 Instanz erstellen und beobachten, was passiert, wenn Sie ihre Tags ändern.

Um die Monitoring-Lösung mit einer echten Instanz zu testen

1. Öffnen Sie die EC2Amazon-Konsole auf der Instance-Seite.
2. Erstellen Sie eine EC2 Amazon-Instance. Bevor Sie sie starten, fügen Sie ein Tag mit dem Schlüssel `valid-key` und dem Wert hinzu`valid-value`. Informationen zum Erstellen und Starten einer Instance finden Sie unter Schritt 1: Starten einer Instance im EC2 Amazon-Benutzerhandbuch. In dem Verfahren Um eine Instance zu starten, wählen Sie in Schritt 3, in dem Sie das Namen-Tag eingeben, auch Zusätzliche Tags hinzufügen, wählen Sie Tag hinzufügen und geben Sie dann den Schlüssel von **`valid-key`** und den Wert von ein**`valid-value`**. Sie können ohne key pair fortfahren, wenn diese Instanz ausschließlich für die Zwecke dieses Tutorials bestimmt ist und Sie planen, diese Instanz zu löschen, nachdem Sie sie abgeschlossen haben. Kehren Sie zu diesem Tutorial zurück, wenn Sie das Ende von Schritt 1 erreicht haben. Sie müssen Schritt 2: Verbindung mit Ihrer Instance herstellen nicht ausführen.
3. Kopieren Sie das InstanceIdvon der Konsole.
4. Wechseln Sie von der EC2 Amazon-Konsole zur Lambda-Konsole. Wählen Sie Ihre automatische EC2 Terminierungsfunktion, wählen Sie die Registerkarte Code und dann die Registerkarte index.js, um Ihren Code zu bearbeiten.

5. Ändern Sie den zweiten Eintrag in der, `InstanceList` indem Sie den Wert einfügen, den Sie aus der EC2 Amazon-Konsole kopiert haben. Stellen Sie sicher, dass der `RegionToMonitor` Wert mit der Region übereinstimmt, die die Instance enthält, die Sie eingefügt haben.
6. Wählen Sie Deploy, um Ihre Änderungen zu aktivieren. Die Funktion kann jetzt durch Tag-Änderungen an dieser Instanz in der angegebenen Region aktiviert werden.
7. Wechseln Sie von der Lambda-Konsole zur EC2 Amazon-Konsole.
8. Ändern Sie die der Instance zugewiesenen Tags, indem Sie entweder das Gültigkeitsschlüssel-Tag löschen oder den Wert dieses Schlüssels ändern.

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

9. Warten Sie ein paar Sekunden und aktualisieren Sie dann die Konsole. Die Instanz sollte ihren Instanzstatus in Stopping und dann in Stopped ändern.
10. Wechseln Sie mit Ihrer Funktion von der EC2 Amazon-Konsole zur Lambda-Konsole und wählen Sie die Registerkarte Monitor.
11. Wählen Sie die Registerkarte Protokolle und wählen Sie in der Tabelle Letzte Aufrufe den neuesten Eintrag in der Spalte aus. LogStream

    In der CloudWatch Amazon-Konsole wird die Seite Ereignisse protokollieren für den letzten Aufruf Ihrer Lambda-Funktion geöffnet. 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
```

Zusammenfassung des Tutorials

In diesem Tutorial wurde gezeigt, wie Sie eine EventBridge Regel erstellen, die mit einer Tagänderung bei einem Ressourcenereignis für EC2 Amazon-Instances übereinstimmt. Die Regel wies auf eine Lambda-Funktion hin, die die Instanz automatisch herunterfährt, wenn sie nicht über das erforderliche Tag verfügt.

Die EventBridge Unterstützung von Amazon für Tag-Änderungen an AWS Ressourcen eröffnet Möglichkeiten, ereignisgesteuerte Automatisierung für viele Ressourcen aufzubauen. AWS-Services In Kombination mit dieser Funktion stehen Ihnen Tools zur AWS Lambda Verfügung, mit denen Sie serverlose Lösungen entwickeln können, die sicher auf AWS Ressourcen zugreifen, bei Bedarf skalieren und kostengünstig sind.

Zu den weiteren möglichen Anwendungsfällen für die tag-change-on-resource EventBridge Veranstaltung gehören:

- Eine Warnung ausgeben, wenn jemand über eine ungewöhnliche 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 führen zu einem CloudWatch Ereignis. Sie können dieses Ereignis verwenden, um die Quell-IP-Adresse mit einer Liste gültiger IP-Adressen zu vergleichen und eine Warnmail zu aktivieren, falls die Quell-IP-Adresse nicht gültig ist.
- Überwachen Sie, ob es Änderungen an Ihrer tagbasierten Zugriffskontrolle für eine Ressource gibt — Wenn Sie den Zugriff auf eine Ressource mithilfe der attribut- (tag-) basierten Zugriffskontrolle (ABAC) eingerichtet haben, können Sie EventBridge Ereignisse verwenden, die durch Änderungen am Tag generiert werden, um eine Prüfung durch Ihr Sicherheitsteam zu veranlassen.

Problembehandlung 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. AWS Generierte Tags werden nicht auf das Maximum von 50 Tags angerechnet. 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 mithilfe von Sonderzeichen hinzugefügt oder geändert haben, überprüfen Sie die Tag-Anforderungen in der Servicedokumentation der Ressource, um sicherzustellen, dass diese Zeichen für den Service zulässig sind.
- Möglicherweise sind Sie nicht berechtigt, die Tags für die Ressource zu ändern. Wenn Sie nicht berechtigt sind, vorhandene Tags für eine Ressource anzuzeigen, können Sie keine Änderungen an den Tags der Ressource vornehmen.
- Möglicherweise sind Sie nicht berechtigt, die Ressource zu ändern. 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. Nehmen wir beispielsweise an, dass eine Ressource im Rahmen der Erstellung eines CloudFormation Stacks gestartet wurde. Wenn der Stapel 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 den Browser-Tab schließen oder die Seite wechseln, 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.
- Es gibt zwar ein Ratenlimit für, aber der Dienst AWS Resource Groups Tagging API, den Sie taggen, kann ein separates Limit festlegen, das Sie möglicherweise vor dem API-Limit für das Tagging von Resource Groups erreichen.

Fehlgeschlagene Tag-Änderungen erneut versuchen

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 für jede Art von Fehler, die auftreten, eine Fehlermeldung an. 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 an Ressourcen erneut versuchen, um Änderungen nur an den Ressourcen zu wiederholen, bei denen Tag-Änderungen fehlgeschlagen sind.

Sicherheit im Tag Editor

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

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

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS-Services in der läuft AWS Cloud. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. 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 Tag Editor gelten, finden Sie unter AWS Services in Scope by Compliance Program.
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS-Service , was Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung des Tag Editors anwenden können. In den folgenden Themen erfahren Sie, wie Sie den Tag Editor so konfigurieren, dass er Ihre Sicherheits- und Compliance-Ziele erfüllt.

Themen

- Datenschutz im Tag Editor
- Identitäts- und Zugriffsmanagement für Tag Editor
- Protokollierung und Überwachung im Tag Editor
- Konformitätsprüfung für Tag Editor
- Resilienz im Tag-Editor
- Infrastruktursicherheit im Tag Editor

Datenschutz im Tag Editor

Das Modell der AWS gemeinsamen Verantwortung und geteilter Verantwortung gilt für den Datenschutz im Tag Editor. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz

der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie 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, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

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 dem Tag Editor oder einem anderen Programm AWS-Services über die Konsole, die API oder arbeiten. AWS CLI AWS SDKs Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie 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

Die Tagging-Informationen sind nicht verschlüsselt. Obwohl nicht verschlüsselt, können Tags Informationen enthalten, die im Rahmen Ihrer Sicherheitsstrategie verwendet werden. Daher ist es wichtig zu kontrollieren, wer auf Tags in Ressourcen zugreifen kann. Es ist besonders wichtig, dass Sie kontrollieren, wer Tags ändern kann, da ein solcher Zugriff dazu genutzt werden könnte, die eigenen Berechtigungen zu erweitern.

Verschlüsselung im Ruhezustand

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

Verschlüsselung während der Übertragung

Tag Editor-Daten werden bei der Übertragung in die interne Datenbank des Dienstes zur Sicherung verschlüsselt. Dies ist nicht vom Benutzer konfigurierbar.

Schlüsselverwaltung

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

Richtlinie für den Datenverkehr zwischen Netzwerken

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

Identitäts- und Zugriffsmanagement für Tag Editor

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Tag Editor-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

- Zielgruppe
- Authentifizierung mit Identitäten

- Verwalten des Zugriffs mit Richtlinien
- So funktioniert der Tag-Editor mit IAM
- Beispiele für identitätsbasierte Richtlinien im Tag-Editor
- Problembehandlung bei Identität und Zugriff auf den Tag-Editor

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von Ihrer Rolle ab:

- Servicebenutzer – Fordern Sie von Ihrem Administrator Berechtigungen an, wenn Sie nicht auf Funktionen zugreifen können (siehe Problembehandlung bei Identität und Zugriff auf den Tag-Editor).
- Serviceadministrator – Bestimmen Sie den Benutzerzugriff und stellen Sie Berechtigungsanfragen (siehe So funktioniert der Tag-Editor mit IAM).
- IAM-Administrator – Schreiben Sie Richtlinien zur Zugriffsverwaltung (siehe Beispiele für identitätsbasierte Richtlinien im Tag-Editor).

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen sich als IAM-Benutzer authentifizieren oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich als föderierte Identität anmelden, indem Sie Anmeldeinformationen aus einer Identitätsquelle wie AWS IAM Identity Center (IAM Identity Center), Single Sign-On-Authentifizierung oder Anmeldeinformationen verwenden. Google/Facebook Weitere Informationen zum Anmelden finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch für AWS-Anmeldung .

AWS Bietet für den programmatischen Zugriff ein SDK und eine CLI zum kryptografischen Signieren von Anfragen. Weitere Informationen finden Sie unter AWS Signature Version 4 for API requests im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, dem sogenannten AWS-Konto Root-Benutzer, der vollständigen Zugriff auf alle AWS-Services Ressourcen hat. Wir

raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Eine Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Tasks that require root user credentials im IAM-Benutzerhandbuch.

Benutzer und Gruppen

Ein IAM-Benutzer ist eine Identität mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Verwenden Sie möglichst temporäre Anmeldeinformationen statt IAM-Benutzer mit langfristigen Anmeldeinformationen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erfordern, dass menschliche Benutzer für den Zugriff AWS mithilfe temporärer Anmeldeinformationen einen Verbund mit einem Identitätsanbieter verwenden müssen.

Eine IAM-Gruppe gibt eine Sammlung von IAM-Benutzern an und vereinfacht die Verwaltung von Berechtigungen bei großer Benutzerzahl. Weitere Informationen finden Sie unter Use cases for IAM users im IAM-Benutzerhandbuch.

Rollen

Eine IAM-Rolle ist eine Identität mit bestimmten Berechtigungen, die temporäre Anmeldeinformationen bereitstellt. Sie können eine Rolle übernehmen, indem Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln oder indem Sie eine AWS Oder-API-Operation AWS CLI aufrufen. Weitere Informationen finden Sie unter Methods to assume a role im IAM-Benutzerhandbuch.

IAM-Rollen sind nützlich für Verbundbenutzerzugriff, temporäre IAM-Benutzerberechtigungen, kontoübergreifenden Zugriff, dienstübergreifenden Zugriff und Anwendungen, die auf Amazon ausgeführt werden. EC2 Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an Identitäten oder Ressourcen anhängen. AWS Eine Richtlinie definiert Berechtigungen, wenn sie mit einer Identität oder Ressource verknüpft sind. AWS bewertet diese Richtlinien, wenn ein Principal eine Anfrage stellt. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu JSON-Richtliniendokumenten finden Sie unter Overview of JSON policies im IAM-Benutzerhandbuch.

Mithilfe von Richtlinien legen Administratoren fest, wer auf was Zugriff hat, indem sie definieren, welcher Prinzipal Aktionen mit welchen Ressourcen und unter welchen Bedingungen ausführen kann.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator erstellt IAM-Richtlinien und fügt sie Rollen hinzu, die Benutzer dann übernehmen können. IAM-Richtlinien definieren Berechtigungen unabhängig von der Methode, die zur Ausführung der Operation verwendet wird.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität (Benutzer, Gruppe oder Rolle) anfügen können. Diese Richtlinien steuern, welche Aktionen Identitäten für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können Inline-Richtlinien (Richtlinien, die direkt in eine einzelne Identität eingebettet sind) oder verwaltete Richtlinien (eigenständige Richtlinien, die mehreren Identitäten zugeordnet sind) sein. Informationen dazu, wie Sie zwischen verwalteten und Inline-Richtlinien wählen, finden Sie unter Choose between managed policies and inline policies im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele hierfür sind Vertrauensrichtlinien für IAM-Rollen und Bucket-Richtlinien von Amazon S3. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben.

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

Zugriffskontrolllisten () ACLs

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

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

Weitere Richtlinientypen

AWS unterstützt zusätzliche Richtlinientypen, mit denen die maximalen Berechtigungen festgelegt werden können, die durch gängigere Richtlinientypen gewährt werden:

- Berechtigungsgrenzen – Eine Berechtigungsgrenze legt die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einer IAM-Entität erteilen kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im -IAM-Benutzerhandbuch.
- Richtlinien zur Dienstkontrolle (SCPs) — Geben Sie die maximalen Berechtigungen für eine Organisation oder Organisationseinheit in an AWS Organizations. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.
- Richtlinien zur Ressourcenkontrolle (RCPs) — Legen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten fest. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter Richtlinien zur Ressourcenkontrolle (RCPs).
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die als Parameter übergeben werden, wenn Sie eine temporäre Sitzung für eine Rolle oder einen Verbundbenutzer erstellen. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn für eine Anfrage mehrere Arten von Richtlinien gelten, sind die sich daraus ergebenden Berechtigungen schwieriger zu verstehen. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie unter Bewertungslogik für Richtlinien im IAM-Benutzerhandbuch.

So funktioniert der Tag-Editor mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf den Tag Editor zu verwalten, sollten Sie wissen, welche IAM-Funktionen für die Verwendung mit dem Tag Editor verfügbar sind. Einen allgemeinen Überblick darüber, wie Tag Editor und andere mit IAM AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch.

Themen

- Identitätsbasierte Richtlinien für den Tag-Editor
- Ressourcenbasierte Richtlinien
- Autorisierung auf der Basis von Markierungen

- IAM-Rollen im Tag-Editor

Identitätsbasierte Richtlinien für den Tag-Editor

Mit identitätsbasierten IAM-Richtlinien können Sie zusätzlich zu den Bedingungen, unter denen Aktionen zugelassen oder verweigert werden, zulässige oder verweigerte Aktionen und Ressourcen angeben. Der 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 mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs zu erteilen.

Für Richtlinienaktionen im Tag Editor wird vor der Aktion das folgende Präfix verwendet:`tag:`. Tag-Editor-Aktionen werden vollständig in der Konsole ausgeführt, haben jedoch das Präfix `tag` in den Protokolleinträgen.

Um beispielsweise jemandem die Erlaubnis zu erteilen, eine Ressource mit dem `tag:TagResources` API-Vorgang zu taggen, nehmen Sie die `tag:TagResources` Aktion in seine Richtlinie auf. Richtlinienanweisungen müssen entweder ein – `Action`oder ein `NotAction`-Element enthalten. Der Tag-Editor definiert eigene Aktionen, die Aufgaben beschreiben, die Sie mit diesem Dienst ausführen 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 Serviceautorisierungsreferenz.

Ressourcen

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

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Der Tag Editor verfügt über keine eigenen Ressourcen. Stattdessen manipuliert er die Metadaten (Tags), die an Ressourcen angehängt sind, die von anderen erstellt wurden. AWS-Services

Bedingungsschlüssel

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

Das `Condition`-Element legt fest, ob Anweisungen auf der Grundlage definierter Kriterien ausgeführt werden. 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. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Der Tag-Editor definiert keine dienstspezifischen Bedingungsschlüssel.

Beispiele

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

Ressourcenbasierte Richtlinien

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

Autorisierung auf der Basis von Markierungen

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

Um den Zugriff auf eine Ressource anhand ihrer Tags zu steuern, geben Sie Taginformationen im Bedingungselement einer Richtlinie mithilfe der Bedingungsschlüssel `aws:ResourceTag/key-name` `aws:RequestTag/key-name`, oder ein. `aws:TagKeys` 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 Gruppen auf der Grundlage von Stichwörtern anzeigen. Weitere Informationen zur attributebasierten Zugriffskontrolle (ABAC) finden Sie unter Wozu dient ABAC? AWSim IAM-Benutzerhandbuch.

IAM-Rollen im Tag-Editor

Eine IAM-Rolle ist eine Entität innerhalb von Ihnen AWS-Konto , die über bestimmte Berechtigungen verfügt. Der Tag-Editor hat oder verwendet keine Servicerollen.

Verwenden temporärer Anmeldeinformationen mit dem Tag Editor

Im Tag Editor können Sie temporäre Anmeldeinformationen verwenden, um sich bei Federation anzumelden, eine IAM-Rolle anzunehmen oder eine kontoübergreifende Rolle anzunehmen.
Sie erhalten temporäre Sicherheitsanmeldedaten, indem Sie AWS STS API-Operationen wie AssumeRoleoder aufrufen. GetFederationToken

Service-verknüpfte Rollen

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

Der Tag-Editor hat oder verwendet keine dienstbezogenen Rollen.

Servicerollen

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

Der Tag-Editor hat oder verwendet keine Servicerollen.

Beispiele für identitätsbasierte Richtlinien im Tag-Editor

Standardmäßig sind IAM-Prinzipale, wie Rollen und Benutzer, nicht berechtigt, Tags zu erstellen oder zu ändern. Sie können auch keine Aufgaben mit AWS-Managementkonsole, AWS Command Line Interface (AWS CLI) oder ausführen. AWS APIs Ein IAM-Administrator muss IAM-Richtlinien erstellen, die den Prinzipalen die Erlaubnis gewähren, bestimmte API-Operationen auf den angegebenen Ressourcen auszuführen, die sie benötigen. Der Administrator muss diese Richtlinien dann den Prinzipalen zuordnen, für die diese Berechtigungen erforderlich sind.

Anweisungen zum Erstellen einer identitätsbasierten IAM-Richtlinie anhand dieser Beispieldokumente zu JSON-Richtlinien finden Sie unter Creating Policies on the JSON Tab 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
- Gruppen auf der Grundlage von Stichwörtern anzeigen

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. Wenn du identitätsbasierte Richtlinien erstellst oder bearbeitest, befolge diese Richtlinien und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien oder Von 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 Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. CloudFormation B. 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 mit IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA 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, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Tags, die den Ressourcen in Ihrem AWS-Konto zugewiesen sind, aufzulisten und einzusehen. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die restriktiver ist als die erforderlichen Mindestberechtigungen, funktionieren die Konsolen- und API-Befehle für die IAM-Prinzipale mit dieser Richtlinie nicht wie vorgesehen.

Um sicherzustellen, dass diese Prinzipale den Tag Editor weiterhin 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:

JSON

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

Weitere Informationen zur Gewährung des Zugriffs auf den Tag Editor und die Resource Groups Tagging API finden Sie unterErteilen 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 umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der AWS CLI API oder. AWS

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

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

Gruppen auf der Grundlage von Stichwörtern anzeigen

Sie können Bedingungen in Ihrer identitätsbasierten Richtlinie verwenden, um den Zugriff auf Tag-Editor-Ressourcen anhand von Stichwörtern zu steuern. Dieses Beispiel zeigt, wie Sie eine Richtlinie erstellen könnten, die das Anzeigen einer Ressource, in diesem Beispiel einer Ressourcengruppe, ermöglicht. Die Berechtigung wird jedoch nur erteilt, wenn das Gruppen-Tag denselben Wert `project` hat wie das `project` Tag, das dem aufrufenden Prinzipal zugewiesen ist.

JSON

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

```
            "Effect": "Allow",
            "Action": "resource-groups:ListGroups",
            "Resource": "arn:aws:resource-groups:us-
east-1:111122223333:group/group_name"
        },
        {
            "Effect": "Allow",
            "Action": "resource-groups:ListGroups",
            "Resource": "arn:aws:resource-groups:us-
east-1:111122223333: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 aufzurufen, muss die Gruppe ebenfalls markiert werden`project=alpha`. Andernfalls wird dem Benutzer der Zugriff verweigert. Der Tag-Schlüssel `project` der Bedingung stimmt sowohl mit `Project` als auch mit `project` überein, da die Namen von Bedingungsschlüsseln nicht zwischen Groß- und Kleinschreibung unterscheiden. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

Problembehandlung bei Identität und Zugriff auf den Tag-Editor

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit dem Tag Editor und IAM auftreten können.

Themen

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

Ich bin nicht berechtigt, eine Aktion im Tag Editor durchzuführen

Wenn Ihnen AWS-Managementkonsole mitgeteilt wird, dass Sie nicht berechtigt sind, eine Aktion durchzuführen, 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 auf einer Ressource zu verwenden, aber nicht über die `tag:GetTagKeys` entsprechenden Berechtigungen verfügt.

```
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 berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zur Durchführung der `iam:PassRole` Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an den Tag Editor übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. 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.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Protokollierung und Überwachung im Tag Editor

Alle Tag Editor-Aktionen sind angemeldet AWS CloudTrail.

Protokollieren von Tag Editor-API-Aufrufen mit CloudTrail

Der Tag Editor ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen eines Benutzers, einer Rolle oder eines AWS-Service im Tag-Editor ausgeführten Aktionen bereitstellt. CloudTrail erfasst alle API-Aufrufe für den Tag Editor als Ereignisse, einschließlich Aufrufe von der Tag Editor-Konsole und von Codeaufrufen an die Resource Groups Tagging API. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für den Tag Editor. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von CloudTrail gesammelten Informationen können Sie die Anfrage an den Tag Editor, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen zu CloudTrail finden Sie im AWS CloudTrail Benutzerhandbuch.

Informationen zum Tag-Editor finden Sie unter CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn eine Aktivität im Tag Editor oder in der Tag Editor-Konsole stattfindet, wird diese Aktivität zusammen mit anderen AWS-Service Ereignissen im CloudTrail Event-Verlauf in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter Ereignisse mit dem CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto, einschließlich der Ereignisse für den Tag-Editor, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere konfigurieren, AWS-Services um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie in den folgenden Ressourcen:

- Erstellen Sie einen Trail für Ihren AWS-Konto
- In CloudTrail unterstützte Services und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle Tag Editor-Aktionen werden von der Tag Editor-API-Referenz protokolliert CloudTrail und sind in dieser Dokumentation dokumentiert. Tag-Editor-Aktionen in der Konsole werden von CloudTrail protokolliert und als Ereignisse mit dem `tagging.amazonaws.com` Symbol 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 unter dem CloudTrail`userIdentity`Element.

Grundlegendes zu den Logdateieinträgen im Tag-Editor

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anfrageparameter. CloudTrail -Protokolldateien sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher nicht in einer bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die Aktion demonstriert`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"
    }
}
```

Konformitätsprüfung für Tag Editor

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

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

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. Weitere Informationen zu Ihrer Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services finden Sie in der AWS Sicherheitsdokumentation.

Resilienz 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 bei der Übertragung verschlüsselt. Der Tag Editor speichert Kundendaten in Amazon DynamoDB.

Die AWS globale Infrastruktur basiert auf Availability AWS-Regionen Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander 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 versehentlich Tags löschen, wenden Sie sich an AWS -Support das Center.

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

Infrastruktursicherheit im Tag Editor

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

Sie verwenden 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.

Darüber hinaus müssen Anfragen mithilfe einer Zugriffsschlüssel-ID und eines geheimen Zugriffsschlüssels, der einem AWS Identity and Access Management (IAM-) Principal zugeordnet ist, signiert werden. 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, Tag Editor unterstützt jedoch ressourcenbasierte Zugriffsrichtlinien, die Einschränkungen auf der Quell-IP-Adresse beinhalten können. Sie können Tag Editor-Richtlinien auch verwenden, um den Zugriff von bestimmten Amazon Virtual Private Cloud (Amazon VPC) -Endpunkten oder bestimmten zu kontrollieren. VPCs Tatsächlich isoliert dieser Ansatz den Netzwerkzugriff auf eine bestimmte Ressource nur von der spezifischen VPC innerhalb des AWS Netzwerks.

Servicekontingente

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

Diese Kontingente können derzeit nicht über die Service Quotas Quotas-Konsole angepasst werden. Wenden Sie sich an 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. Zu den zulässigen Zeichen gehören Buchstaben, Zahlen, Leerzeichen und die folgenden Zeichen: `_ . : / = + - @` Schlüsselnamen dürfen nicht mit beginnen, `aws:` da dieses Präfix für die AWS Verwendung reserviert ist. **Note** Für AWS-Services einige gelten zusätzliche Zeichen- oder Längenbeschränkungen. Weitere Informationen finden Sie in der

Name	Standard
	Dokumentation für den jeweiligen Service.
Tag-Werte	Mindestens 0, maximal 256 Unicode-Zeichen in UTF-8. Zu den zulässigen Zeichen gehören Buchstaben, Zahlen, Leerzeichen und die folgenden Zeichen: `_ . : / = + - @` **Note** Für AWS-Services einige gelten zusätzliche Zeichen- oder Längenbeschränkungen. Weitere Informationen finden Sie in der Dokumentation für den jeweiligen Service.
Geschwindigkeit des Aufrufs der GetResources API-Operation	Maximal 15 Aufrufe pro Sekunde
Rate zum Aufrufen der folgenden API-Operationen: • TagResources • UntagResources • GetTagKeys • GetTagValues	Maximal 5 Aufrufe pro Sekunde

Dokumentenverlauf im Tag-Editor

Änderung	Beschreibung	Datum
Die Berechtigungen für die Bewertung der unternehmensweiten Einhaltung von Vorschriften wurden aktualisiert	Die Berechtigungen für die Bewertung der unternehmensweiten Einhaltung von Vorschriften wurden aktualisiert und enthalten nun auch Berechtigungen, die den Zugriff auf den Compliance-Bericht erleichtern.	28. August 2024
Aktualisierter Inhalt	Die Thementitel wurden aktualisiert und der Inhalt neu organisiert, um die Lesbarkeit und Auffindbarkeit zu verbessern.	25. Juli 2024
Taggen von Inhalten, die in dieses Handbuch verschoben Allgemeine AWS-Referenz wurden	Die Themen zum Markieren Ihrer AWS Ressourcen wurden aus dem Allgemeine AWS-Referenz in dieses Handbuch verschoben.	24. März 2023
Aktualisierung der bewährten Methoden für IAM	Aktualisierung des Leitfadens zur Ausrichtung an bewährten IAM-Methoden. Weitere Informationen finden Sie unter Bewährte Sicherheitsmethoden in IAM.	3. Januar 2023
Die Tag Editor-Dokumentation wird in ein eigenes Handbuch verschoben	Die Tag Editor-Dokumentation wird jetzt in einem eigenen Benutzerhandbuch bereitgestellt, anstatt Teil des	13. Dezember 2022

	AWS -Ressourcengruppen Benutzerhandbuchs zu sein.	
Prüfen Sie, ob die Tag-Richtlinien eingehalten werden	Nachdem Sie Tag-Richtlinien erstellt und an Konten angehängt haben AWS Organizations, können Sie in den Konten Ihrer Organisation nach nicht konformen Tags auf Ressourcen suchen.	26. November 2019
Der Tag-Editor unterstützt jetzt das Auffinden von Ressourcen ohne Tags	Sie können jetzt im Tag-Editor nach Ressourcen suchen, auf die keine Tag-Werte für einen bestimmten Tag-Schlüssel angewendet wurden.	18. Juni 2019
Die Tag-Editor-Konsole wird aus der AWS Systems Manager Konsole verschoben	Die Tag Editor-Konsole ist jetzt unabhängig von der Systems Manager Manager-Konsole. In der linken Navigationsleiste von Systems Manager finden Sie zwar immer noch Verweise auf die Tag Editor-Konsole, Sie können die Tag Editor-Konsole jedoch direkt über das Drop-down-Menü oben links in der AWS-Managementkonsoleöffnen.	5. Juni 2019
Ältere, veraltete Tag Editor-Tools sind nicht mehr verfügbar	Erwähnungen älterer, klassischer oder veralteter Tag Editors wurden entfernt. Diese Tools sind in nicht mehr verfügbar AWS. Verwenden Sie stattdessen den Tag-Editor.	14. Mai 2019

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

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

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.