POST EDIT. ADDED PROOFREAD. ADDED PP1

AWS Supply Chain

AWS Supply Chain: POST EDIT. ADDED PROOFREAD. ADDED PP1

Table of Contents

Was ist AWS Supply Chain?

AWS Supply Chainist eine cloudbasierte Supply-Chain-Management-Anwendung, die mit Ihren bestehenden Lösungen wie Enterprise Resource Planning (ERP) und Supply-Chain-Management-Systemen funktioniert. MithilfeAWS Supply Chain können Sie Ihre Bestands-, Angebots- und Nachfragedaten aus bestehenden ERP- oder Lieferkettensystemen verbinden und in einem einheitlichenAWS Supply Chain Datenmodell extrahieren.

Themen

Von AWS Supply Chain unterstützte Browser

Bevor Sie mitAWS Supply Chain arbeiten, überprüfen Sie anhand der folgenden Tabelle, ob Ihr Browser unterstützt wird.

Browser	Unterstützte Versionen
Google Chrome	Letzte drei Versionen.
Mozilla Firefox ESR	Versionen werden bis zu ihrem end-of-life Firefox-Datum unterstützt. Einzelheiten finden Sie im Veröffentlichungskalender von Firefox ESR.
Mozilla Firefox	Letzte drei Versionen.
Microsoft Edge und Edge Chromium	Version 84 und später.
Safari	Safari 10 oder höher unter macOS.

Sprachen, die unterstützt werden vonAWS Supply Chain

AWS Supply Chain unterstützt die folgenden Sprachen:

- Englisch (USA)
- Englisch (UK)
- Deutsch
- Spanisch
- Französisch
- Italienisch
- portugiesisch
- Chinesisch (vereinfacht)
- Chinesisch (traditionell)
- Japanisch
- Koreanisch
- Indonesisch

Ein AWS Konto einrichten

Verwenden Sie diesen Abschnitt, um ein AWS Konto und einen IAM-Benutzer zu erstellen. Informationen zu bewährten Methoden für die Erstellung eines AWS Kontos finden Sie unter Einrichtung einer AWS Umgebung mit bewährten Methoden.

Themen

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/signup.
2. Folgen Sie den Online-Anweisungen.

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

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen Sie einen Benutzer mit Administratorzugriff

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

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

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

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

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

Erstellen Sie einen Benutzer 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 Benutzer in IAM Identity Center Administratorzugriff.

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

Melden Sie sich als Benutzer mit Administratorzugriff an

- 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 Zugriffsportal.

Weisen Sie weiteren Benutzern Zugriff zu

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

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

   Anweisungen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen.

Ein AWS Konto schließen

Informationen zum Schließen eines AWS Kontos finden Sie unter Konto schließen.

Erste Schritte mit AWS Supply Chain

In diesem Abschnitt erfahren Sie, wie Sie eine AWS Supply Chain Instanz erstellen, Benutzerberechtigungsrollen zuweisen, sich bei der AWS Supply Chain Webanwendung anmelden und benutzerdefinierte Benutzerberechtigungsrollen erstellen. Eine AWS-Konto kann bis zu 10 AWS Supply Chain Instanzen im aktiven oder initialisierenden Zustand haben.

Themen

Voraussetzungen

Bevor Sie eine AWS Supply Chain Instanz erstellen, stellen Sie sicher, dass Sie die folgenden Schritte ausführen:

- Sie haben eine erstellt AWS-Konto. Weitere Informationen finden Sie unter Ein AWS Konto einrichten.

> **Note**
>
> Wenn Sie es nicht aktiviert haben AWS IAM Identity Center, erstellen Sie eine AWS Organisation und aktivieren Sie IAM Identity Center. Weitere Informationen zum Erstellen einer AWS Organisation finden Sie unter Organisation erstellen.

- Aktivieren Sie IAM Identity Center an derselben AWS-Region Stelle, an der Sie Ihre AWS Supply Chain Instanz erstellen möchten. AWS Supply Chain wird nur in den Regionen USA Ost (Nord-Virginia), USA West (Oregon), Europa (Frankfurt) und Europa (Irland) unterstützt. Weitere Informationen finden Sie unter IAM Identity Center aktivieren .

> **Note**
>
> AWS Supply Chain Bedarfsplanung und Angebotsplanung werden in der Region Europa (Irland) nicht unterstützt.

> **Note**
>
> Wenn Sie IAM Identity Center nicht in einer anderen als den hier aufgeführten Regionen aktiviert haben, können Sie keine AWS Supply Chain Instanz erstellen.

- Sie können IAM-Benutzer von der AWS Identity and Access Management (IAM-) Konsole aus erstellen. Weitere Informationen finden Sie unter Ein AWS Konto einrichten.
- Fügen Sie Benutzer hinzu, die Zugriff auf das IAM AWS Supply Chain Identity Center benötigen. Weitere Informationen finden Sie unter Benutzer im IAM Identity Center hinzufügen. Sie können Ihr Active Directory auch mit dem IAM Identity Center verbinden. Weitere Informationen finden Sie unter Connect zu einem Microsoft AD-Verzeichnis herstellen im AWS IAM Identity Center Benutzerhandbuch.
- Wenn Sie Microsoft Active Directory verwenden, stellen Sie sicher, dass die Active Directory-Synchronisierung aktiviert ist.
- Sie benötigen AWS Key Management Service (AWS KMS), um eine Instanz zu erstellen. AWS Supply Chain verwendet dies AWS KMS key , um alle AWS Supply Chain eingehenden Daten zu verschlüsseln.

Verwenden der AWS Supply Chain -Konsole

> **Note**
>
> Wenn Ihr AWS Konto ein Mitgliedskonto einer AWS Organisation ist und eine Service Control Policy (SCP) beinhaltet, stellen Sie sicher, dass der SCP der Organisation dem Mitgliedskonto die folgenden Berechtigungen gewährt. Wenn die folgenden Berechtigungen nicht in der SCP-Richtlinie der Organisation enthalten sind, schlägt die AWS Supply Chain Instanzerstellung fehl.

Um auf die AWS Supply Chain Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den AWS Supply Chain Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die AWS Supply Chain Konsole weiterhin verwenden können, fügen Sie den Entitäten auch die AWS Supply Chain `ConsoleAccess` oder die `ReadOnly` AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Der Konsolenadministrator benötigt die folgenden Berechtigungen, um AWS Supply Chain Instanzen erfolgreich zu erstellen und zu aktualisieren.

```
        {
"Version": "2012-10-17",
"Statement": [
    {
        "Action": "scn:*",
        "Resource": "*",
        "Effect": "Allow"
    },
    {
        "Action": [
```

```
                "s3:GetObject",
                "s3:PutObject",
                "s3:ListBucket",
                "s3:CreateBucket",
                "s3:PutBucketVersioning",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutEncryptionConfiguration",
                "s3:PutBucketPolicy",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketPublicAccessBlock",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutBucketOwnershipControls",
                "s3:PutBucketNotification",
                "s3:PutAccountPublicAccessBlock",
                "s3:PutBucketLogging",
                "s3:PutBucketTagging"
            ],
            "Resource": "arn:aws:s3:::aws-supply-chain-*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "cloudtrail:CreateTrail",
                "cloudtrail:PutEventSelectors",
                "cloudtrail:GetEventSelectors",
                "cloudtrail:StartLogging"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "events:DescribeRule",
                "events:PutRule",
                "events:PutTargets"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "chime:CreateAppInstance",
                "chime:DeleteAppInstance",
```

```
                "chime:PutAppInstanceRetentionSettings",
                "chime:TagResource"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "cloudwatch:PutMetricData",
                "cloudwatch:Describe*",
                "cloudwatch:Get*",
                "cloudwatch:List*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:CreateOrganization",
                "organizations:EnableAWSServiceAccess"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "kms:CreateGrant",
                "kms:RetireGrant",
                "kms:DescribeKey",
                "kms:ListAliases"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "iam:CreateRole",
                "iam:CreatePolicy",
                "iam:GetRole",
                "iam:PutRolePolicy",
                "iam:AttachRolePolicy",
                "iam:CreateServiceLinkedRole"
            ],
```

```
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "sso:StartPeregrine",
                "sso:DescribeRegisteredRegions",
                "sso:ListDirectoryAssociations",
                "sso:GetPeregrineStatus",
                "sso:GetSSOStatus",
                "sso:ListProfiles",
                "sso:GetProfile",
                "sso:AssociateProfile",
                "sso:AssociateDirectory",
                "sso:RegisterRegion",
                "sso:StartSSO",
                "sso:CreateManagedApplicationInstance",
                "sso:DeleteManagedApplicationInstance",
                "sso:GetManagedApplicationInstance",
                "sso-directory:SearchUsers"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

Eine Instance erstellen

> **Note**
>
> Sie können bis zu 10 Instanzen innerhalb eines erstellen AWS-Konto. Zu den 10 Instanzen gehören aktive und initialisierende Instanzen. Wenn Sie IAM Identity Center (Nachfolger von AWS Single Sign-On) bereits aktiviert haben, müssen Sie Ihre AWS Supply Chain Instanz dort erstellen, AWS-Region wo Sie IAM Identity Center aktiviert haben. AWS Supply Chain unterstützt keine regionsübergreifenden IAM Identity Center-Aufrufe.

Gehen Sie wie folgt vor, um eine AWS Supply Chain Instanz zu erstellen.

> **Note**
>
> Nur der AWS Management Console Administrator kann eine Instanz erstellen. Der AWS Management Console Administrator, der die AWS Supply Chain Instanz erstellt, sollte über alle unter aufgeführten Berechtigungen verfügenVerwenden der AWS Supply Chain -Konsole. Dieser Administrator sollte einen IAM-Benutzer als AWS Supply Chain Administrator zur Verwaltung AWS Supply Chain einladen.

1. Öffnen Sie die AWS Supply Chain Konsole unter. https://console.aws.amazon.com/scn/home
2. Ändern Sie, falls erforderlich, die AWS-Region. Öffnen Sie in der Leiste oben im Konsolenfenster die Liste Region auswählen und wählen Sie eine Region aus. Weitere Informationen zu Regionen finden Sie im IAM-Benutzerhandbuch unter Regionen und Endpunkte. Weitere Informationen finden Sie unter Regionen und Endpunkte im. Allgemeine Amazon Web Services-Referenz

   > **Note**
   >
   > AWS Supply Chain wird nur in den Regionen USA Ost (Nord-Virginia), USA West (Oregon), Europa (Frankfurt), Asien-Pazifik (Sydney) und Europa (Irland) unterstützt. AWS Supply Chain Bedarfsplanung und Angebotsplanung werden in der Region Europa (Irland) nicht unterstützt.

3. Wählen Sie im AWS Supply Chain Dashboard die Option Instanz erstellen aus.
4. Geben Sie auf der Seite mit den Instanzeigenschaften die folgenden Informationen ein:

   - AWS Region — Wählen Sie die Region aus, in der Sie IAM Identity Center aktiviert haben. Um die Region zu ändern, wählen Sie im Drop-down-Menü oben rechts die Option Region auswählen aus. Sie können die Region nicht ändern, nachdem Sie die Instanz erstellt haben.
   - Name — Geben Sie den Instanznamen ein.
   - (Optional) Beschreibung — Geben Sie eine Beschreibung für die Instanz ein.

5. Geben Sie unter AWS KMS-Schlüssel Ihren KMS-Schlüssel ein und aktualisieren Sie Ihre KMS-Schlüsselrichtlinie wie folgt:

> **Note**
>
> Wenn Sie als Anwendungsadministrator Benutzer zur AWS Supply Chain Instanz hinzufügen, haben diese Zugriff auf die AWS KMS key. Sie können die Benutzerberechtigungen zum Hinzufügen oder Entfernen von Benutzern verwalten. Weitere Informationen zu Benutzerberechtigungen finden Sie unterRollen mit Benutzerberechtigungen.

> **Note**
>
> Ersetzen Sie *Region YourAccountNumber*, *YourInstanceID* und *YourKmsKeyArn*durch Ihre AWS Region AWS-Konto, AWS Supply Chain Instanz-ID und den AWS KMS Schlüssel.

```
   {
   "Version": "2012-10-17",
   "Statement": [{
           "Sid": "Enable IAM User Permissions",
           "Effect": "Allow",
           "Principal": {
               "AWS": "arn:aws:iam::YourAccountNumber:root"
           },
           "Action": "kms:*",
           "Resource": "*"
       },
       {
           "Sid": "Allow access through SecretManager for all principals in the
account that are authorized to use SecretManager",
           "Effect": "Allow",
           "Principal": {
               "AWS": "*"
           },
           "Action": [
               "kms:Encrypt",
               "kms:Decrypt",
```

```
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:CreateGrant",
                "kms:DescribeKey",
                "kms:GenerateDataKeyWithoutPlaintext",
                "kms:ReEncryptFrom",
                "kms:ReEncryptTo"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "secretsmanager.Region.amazonaws.com",
                    "kms:CallerAccount": "YourAccountNumber"
                }

            }
        }
    ]
}
```

Wenn Sie keinen KMS-Schlüssel haben, wählen Sie Create, um zur AWS KMS Konsole zu gelangen, in der Sie diesen Schlüssel erstellen können. Verwenden Sie die vorherige KMS-Schlüsselrichtlinie. Ausführliche Informationen zum Erstellen von KMS-Schlüsseln finden Sie unter Creating Keys im AWS Key Management Service Developer Guide.

Wenn Sie beabsichtigen, eine S/4-Hana-Datenverbindung zu verwenden, stellen Sie sicher, dass der von Ihnen angegebene KMS-Schlüssel das aws-supply-chain-accessTag mit dem zugehörigen Wert true enthält.

6. (Optional) Wählen Sie unter Instanz-Tags die Option Neues Tag hinzufügen aus, um Ihrer Instance ein Tag zuzuweisen. Sie können diese Tags verwenden, um Ihre Instance zu identifizieren. Informationen zu Tags finden Sie unter Tags erstellen.
7. Wählen Sie Create instance (Instance erstellen).

   Es dauert ungefähr 2 bis 3 Minuten, bis die AWS Supply Chain Instanz erstellt ist. Sobald die Instanz erstellt wurde, wird im Statusfeld auf dem AWS Supply Chain Dashboard der Status Aktiv angezeigt.
8. Sobald Ihre AWS Supply Chain Instanz erstellt wurde, aktualisieren Sie Ihre KMS-Richtlinie, um den Zugriff auf Ihren AWS KMS Schlüssel AWS Supply Chain zu ermöglichen.

> **Note**
>
> Ersetzen Sie *YourInstanceID* durch Ihre AWS Supply Chain Instanz-ID. Sie finden Ihre Instanz-ID im AWS Supply Chain Konsolen-Dashboard.

```
        {
    "Sid": "Allow AWS Supply Chain to access the AWS KMS Key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::YourAccountNumber:role/service-role/scn-instance-
role-YourInstanceID"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": "*"
},
{
    "Sid": "Enable ASC to backfill KMS permissions",
    "Effect": "Allow",
    "Principal": {
        "Service": "scn.Region.amazonaws.com"
    },
    "Action": [
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "kms:DescribeKey",
        "kms:CreateGrant",
        "kms:RetireGrant"
    ],
    "Resource":"YourKmsKeyArn"
}
```

IAM Identity Center aktivieren

Bevor Sie mit der Nutzung beginnen AWS Supply Chain, müssen Sie eine Verbindung zu einer Identitätsquelle herstellen. Weitere Informationen finden Sie unter Erste Schritte mit IAM im IAM-Benutzerhandbuch.

Benutzer im IAM Identity Center hinzufügen

Sie können Benutzer für die AWS Supply Chain Nutzung des IAM Identity Center-Dienstes verwalten. IAM Identity Center ist ein cloudbasierter IAM Identity Center-Dienst, mit dem Sie den IAM Identity Center-Zugriff auf all Ihre AWS-Konten und Cloud-Anwendungen bequem zentral verwalten können. Informationen zum Hinzufügen von IAM-Benutzern finden Sie unter Erstellen eines IAM-Benutzers in Ihrem AWS-Konto im IAM-Benutzerhandbuch.

Weitere Informationen zum Erstellen von IAM-Benutzergruppen finden Sie unter Erstellen von IAM-Benutzergruppen im IAM-Benutzerhandbuch.

> **Note**
>
> Um einen Benutzer hinzuzufügen AWS Supply Chain, müssen Benutzer Teil einer IAM Identity Center-Gruppe sein.

Einen AWS Supply Chain Anwendungseigentümer auswählen

> **Note**
>
> Als AWS Konsolenadministrator wählen Sie einen AWS Supply Chain Anwendungsbesitzer aus, der den Zugriff auf die AWS Supply Chain Webanwendung verwaltet. Der AWS Supply Chain Anwendungsbesitzer kann der AWS Supply Chain Webanwendung Benutzerberechtigungsrollen hinzufügen oder entfernen.

Nachdem die Instanz erstellt und eine Identitätsquelle verbunden wurde, gehen Sie wie folgt vor, um einen AWS Supply Chain Anwendungsbesitzer auszuwählen.

1. Wählen Sie im AWS Supply Chain Konsolen-Dashboard unter Anwendungsbesitzer die Option Anwendungsbesitzer zuweisen aus.
2. Wählen Sie unter Anwendungsbesitzer auswählen einen Benutzer aus, der als AWS Supply Chain Anwendungsbesitzer fungieren soll. Sie können nur nach dem Benutzernamen suchen und die Benutzer, die den Suchkriterien entsprechen, werden angezeigt.

   Um weitere Benutzer hinzuzufügen, wählen Sie Gehe zu IAM Identity Center. Weitere Informationen zum Hinzufügen von Benutzern finden Sie unter Benutzer im IAM Identity Center hinzufügen und weitere Informationen zu Benutzerberechtigungsrollen finden Sie unterRollen mit Benutzerberechtigungen.

   > **Note**
   >
   > Sie können jeweils nur einen Benutzer von der AWS Supply Chain Konsole aus hinzufügen. Sie können keine Gruppe als Anwendungsbesitzer hinzufügen AWS Supply Chain.

3. wählen Sie Einladung senden.

   Auf dem AWS Supply Chain Konsolen-Dashboard wird der Benutzer unter Anwendungsbesitzer aufgeführt.
4. Wählen Sie Verwalten in AWS Supply Chain, um Benutzer in der AWS Supply Chain Webanwendung hinzuzufügen oder zu entfernen.

Gruppen zuweisen

Als Besitzer oder AWS Supply Chain Administrator einer Anwendung können Sie nur Benutzer hinzufügen, die Teil einer IAM Identity Center-Gruppe sind. AWS Supply Chain

1. Wählen Sie im AWS Supply Chain Konsolen-Dashboard unter Gruppen die Option Gruppen zuweisen aus.

   Die Seite „Gruppen“ wird angezeigt.
2. Wählen Sie unter Gruppenname die Gruppe mit Benutzern aus, die darauf zugreifen können, AWS Supply Chain und wählen Sie Zuweisen.

   Sie sehen die Gruppe, die Sie unter Gruppen aufgeführt haben, im AWS Supply Chain Dashboard.

3. Sie können Gruppen verwalten wählen, um eine neue Gruppe in IAM Identity Center hinzuzufügen. Sobald die Gruppe in IAM Identity Center hinzugefügt wurde, wird die Gruppe unter Gruppenname in aufgeführt. AWS Supply Chain

Melden Sie sich bei der AWS Supply Chain-Webanwendung an

Als AWS Supply Chain Administrator sollten Sie eine E-Mail-Einladung zur AWS Supply Chain Webanwendung erhalten haben.

1. Sie können entweder den Link in der E-Mail oder im AWS Supply Chain Konsolen-Dashboard unter Subdomain die Web-URL auswählen.

   Die Anmeldeseite der AWS Supply ChainWebanwendung wird angezeigt.
2. Geben Sie die Benutzeranmeldedaten für das AWS IAM Identity Center ein und wählen Sie Anmelden.

Melden Sie sich AWS Supply Chain zum ersten Mal an

> **Note**
>
> Sie werden nur dann aufgefordert, Profile für Ihr Konto und Ihre Organisation auszufüllen, wenn Sie sich zum ersten Mal anmelden.

Nachdem Sie sich als AWS Supply Chain Administrator bei der AWS Supply Chain Webanwendung angemeldet haben, folgen Sie diesen Schritten, um die Einrichtung abzuschließen.

1. Geben Sie auf der Seite Vervollständigen Sie Ihr Profil Ihre Berufsbezeichnung und Ihre Zeitzone ein. Wählen Sie Weiter aus.
2. Geben Sie auf der Seite „Lassen Sie uns Ihre Organisation hinzufügen“ den Namen der Organisation ein und wählen Sie den Standort des Hauptsitzes aus. Optional können Sie ein Firmenlogo hinzufügen. Wählen Sie Weiter aus.
3. Wählen Sie auf der AWS Supply Chain Seite Teammitglieder einrichten auf die Benutzer aus, die Zugriff auf die AWS Supply Chain Webanwendung haben sollen. Klicken Sie auf Invite Users. Informationen zum Hinzufügen von Benutzern zu IAM Identity Center finden

Sie unter. Benutzer im IAM Identity Center hinzufügen Informationen zu AWS Supply Chain Benutzerberechtigungsrollen finden Sie unterRollen mit Benutzerberechtigungen.

4. Wenn Sie später Benutzer hinzufügen möchten, können Sie „Vorerst überspringen“ wählen.

   Die Seite „Onboarding abgeschlossen“ wird angezeigt.

5. Jeder Benutzer, den Sie hinzugefügt haben, erhält eine E-Mail-Nachricht mit einem Link zu AWS Supply Chain, oder Sie können Link kopieren wählen und den Link an die Benutzer senden.
6. Wählen Sie Weiter zur Startseite, um das AWS Supply Chain Dashboard aufzurufen.

Aktualisierung Ihres Kontoprofils

Sie können Ihr Kontoprofil jederzeit in der AWS Supply Chain Webanwendung aktualisieren. Folgen Sie diesen Schritten, um das Konto zu aktualisieren.

1. Wählen Sie im Dashboard der AWS Supply Chain Webanwendung im linken Navigationsbereich das Symbol Einstellungen aus.
2. Wählen Sie Kontoprofil aus.

   Die Seite „Kontoprofil“ wird angezeigt.

3. Aktualisieren Sie die Kontoinformationen und wählen Sie Speichern.

Aktualisierung Ihres Unternehmensprofils

Sie können das Organisationsprofil jederzeit in der AWS Supply Chain Webanwendung aktualisieren. Gehen Sie wie folgt vor, um das Organisationsprofil zu aktualisieren.

1. Wählen Sie im Dashboard der AWS Supply Chain Webanwendung im linken Navigationsbereich das Symbol Einstellungen aus.
2. Wählen Sie Organisation und dann Organisationsprofil aus.

   Die Seite „Organisationsprofil“ wird angezeigt.

3. Aktualisieren Sie das Logo der Organisation oder den Standort des Hauptsitzes und wählen Sie dann Speichern.

Rollen mit Benutzerberechtigungen

Als AWS Supply Chain Administrator können Sie entweder die standardmäßigen Benutzerberechtigungsrollen verwenden oder benutzerdefinierte Berechtigungsrollen erstellen. AWS Supply Chain hat die folgenden standardmäßigen Benutzerberechtigungsrollen:

- Administrator — Zugriff zum Erstellen, Anzeigen und Verwalten aller Daten und Benutzerberechtigungen.
- Datenanalyst — Zugriff zum Erstellen, Anzeigen und Verwalten aller Datenverbindungen.
- Inventory Manager — Zugriff zum Erstellen, Anzeigen und Verwalten von Insights.
- Planner — Zugriff zum Erstellen, Anzeigen und Verwalten von Prognosen, Überschreibungen und zum Veröffentlichen von Bedarfsplänen.
- Partnerdatenmanager — Zugriff auf die Verwaltung und Anzeige von Partnern, die Verwaltung und Anzeige von Datenanfragen sowie die Anzeige von Nachhaltigkeitsdaten.
- Supply Planner — Zugriff auf die Verwaltung und Anzeige von Lieferplänen.

> **Note**
>
> Beachten Sie als AWS Supply Chain Administrator Folgendes, bevor Sie Benutzer hinzufügen:
>
> - Jede standardmäßige Benutzerberechtigungsrolle ist mit einer Reihe von Berechtigungen definiert. Sie können Benutzer zu Standard-Benutzerberechtigungsrollen hinzufügen oder benutzerdefinierte Berechtigungsrollen erstellen.
> - Ein Benutzer kann nur einer Benutzerberechtigungsrolle zugewiesen werden.
> - Sie können Standard-Benutzerberechtigungsrollen nicht bearbeiten oder löschen.
> - Wenn Sie eine von Ihnen erstellte benutzerdefinierte Berechtigungsrolle bearbeiten, werden die Berechtigungen für alle Benutzer aktualisiert, die der benutzerdefinierten Berechtigungsrolle unterstehen.
> - Wenn Sie eine von Ihnen erstellte benutzerdefinierte Berechtigungsrolle löschen, verlieren alle Benutzer unter der benutzerdefinierten Berechtigungsrolle den Zugriff auf AWS Supply Chain.
> - Das Hinzufügen von Gruppen wird in nicht unterstützt AWS Supply Chain.

Themen

Hinzufügen von Benutzern

> **Note**
>
> Bevor Sie Benutzer hinzufügen, stellen Sie sicher, dass der Benutzer Teil einer IAM Identity Center-Gruppe ist und dass die Gruppe zugewiesen AWS Supply Chain ist.

Als AWS Supply Chain Administrator können Sie Benutzer hinzufügen, um auf die AWS Supply Chain Webanwendung zuzugreifen. Gehen Sie wie folgt vor, um einen Benutzer hinzuzufügen.

1. Wählen Sie auf dem AWS Supply Chain Dashboard im linken Navigationsbereich das Symbol Einstellungen aus.
2. Wählen Sie Berechtigungen und dann Benutzer aus.

   Die Seite „Benutzer verwalten“ wird angezeigt.
3. Wählen Sie Neuen Benutzer hinzufügen.

   Die Seite „Benutzer hinzufügen“ wird angezeigt.
4. Wählen Sie im Dropdownmenü Benutzer hinzufügen den Benutzer aus und wählen Sie unter Rolle auswählen die Rolle für den Benutzer aus.
5. Wählen Sie Hinzufügen aus.

Benutzerberechtigungen aktualisieren

Sie können die Benutzerberechtigungsrolle für die aktuellen AWS Supply Chain Benutzer aktualisieren. Gehen Sie wie folgt vor, um die Benutzerberechtigungsrolle zu aktualisieren.

1. Wählen Sie auf dem AWS Supply Chain Dashboard im linken Navigationsbereich das Symbol Einstellungen aus.
2. Wählen Sie Berechtigungen und dann Benutzer aus.

Die Seite „Benutzer verwalten“ wird angezeigt.

3. Wählen Sie auf der Seite „Benutzer verwalten“ den Benutzer oder die Gruppe aus, für die Sie die Benutzerberechtigungsrolle aktualisieren möchten, und wählen Sie im Dropdownmenü „Berechtigungsrolle“ eine der folgenden Berechtigungsrollen aus:

> **Note**
>
> Abhängig von den Rollenberechtigungen, die Sie zuweisen, ist das AWS Supply Chain Dashboard angepasst. Weitere Informationen finden Sie unter Benutzerdefinierte Benutzerberechtigungsrollen erstellen.

   - Administrator — Zugriff zum Erstellen, Anzeigen und Verwalten aller Daten und Benutzerberechtigungen.
   - Datenanalyst — Zugriff zum Erstellen, Anzeigen und Verwalten aller Datenverbindungen.
   - Inventory Manager — Zugriff zum Erstellen, Anzeigen und Verwalten von Insights.
   - Planer — Zugriff zum Erstellen, Anzeigen und Verwalten von Prognosen, Überschreibungen und zum Veröffentlichen von Bedarfsplänen.
4. Wählen Sie Speichern.

Löschen von Benutzern

Als AWS Supply Chain Administrator können Sie Benutzer aus der AWS Supply Chain Webanwendung löschen. Gehen Sie wie folgt vor, um Benutzer zu löschen.

1. Wählen Sie im AWS Supply Chain Dashboard im linken Navigationsbereich das Symbol Einstellungen aus.
2. Wählen Sie Berechtigungen und dann Benutzer aus.

   Die Seite „Benutzer verwalten“ wird angezeigt.
3. Wählen Sie auf der Seite „Benutzer verwalten“ den Benutzer aus, den Sie löschen möchten, und klicken Sie auf das Symbol Löschen.

Benutzerdefinierte Benutzerberechtigungsrollen erstellen

Zusätzlich zu den standardmäßigen Benutzerberechtigungsrollen können Sie benutzerdefinierte Benutzerberechtigungsrollen erstellen, die mehrere Berechtigungsrollen enthalten und bestimmte Standorte und Produkte hinzufügen. Gehen Sie wie folgt vor, um neue Berechtigungsrollen zu erstellen.

> **Note**
>
> Sie können die Produkte und Standorte unter Standortzugriff und Produktzugriff nur auswählen, wenn Ihre Instanz mit einer Datenquelle verbunden ist. Sie können beispielsweise einen benutzerdefinierten Admin-Benutzer erstellen, um Avocados am Standort Seattle zu verwalten, oder einen Insight-Benutzer, nur um die Erkenntnisse für Avocados am Standort Seattle zu verwalten.

1. Wählen Sie auf dem AWS Supply Chain Dashboard im linken Navigationsbereich das Symbol Einstellungen aus. Wählen Sie „Berechtigungen“ und anschließend „Berechtigungsrollen“ aus.

   Die Seite „Berechtigungsrollen“ wird angezeigt.
2. Klicken Sie auf Create New Role.
3. Geben Sie auf der Seite „Berechtigungsrolle verwalten“ unter Rollenname einen Namen ein.
4. Bewegen Sie den Schieberegler, um die Benutzerberechtigungsrolle auszuwählen.

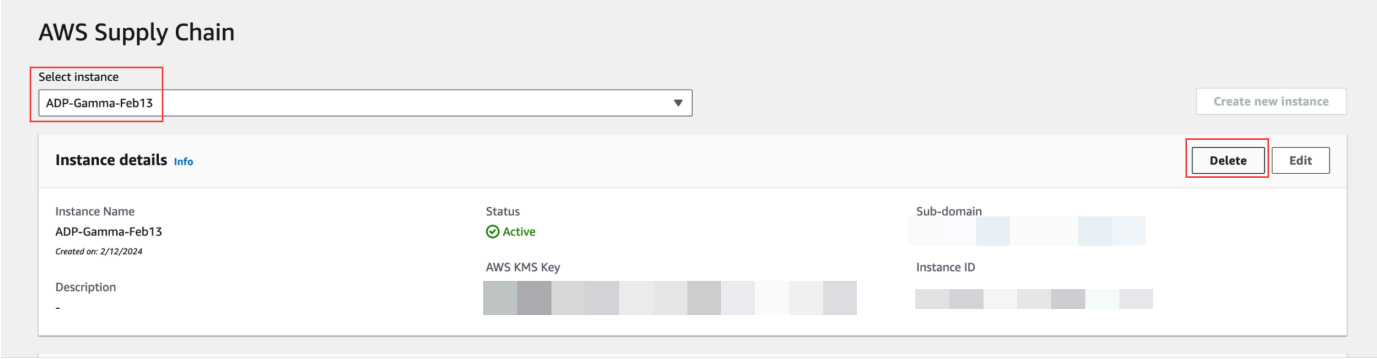
   - Verwalten — Benutzern mit Verwaltungsberechtigungen können Informationen hinzugefügt, bearbeitet und verwaltet werden.
   - Anzeigen — Wenn Benutzern Leseberechtigungen zugewiesen werden, können nur die aktuellen Informationen angezeigt werden.
5. Suchen Sie unter Standortzugriff nach den Regionen, während Sie in die Suchleiste eingeben, und wählen Sie die Regionen aus.
6. Suchen Sie unter Produktzugriff nach den Produkten, während Sie in die Suchleiste eingeben, und wählen Sie die Produkte aus.
7. Wählen Sie Speichern.

Eine Instance löschen

Gehen Sie wie folgt vor, um eine Instanz zu löschen.

> **Note**
>
> Wenn Sie eine Instance löschen, werden Informationen aus dem Amazon S3 S3-Bucket nicht automatisch gelöscht.

1. Öffnen Sie die AWS Supply Chain Konsole unterhttps://console.aws.amazon.com/scn/home.
2. Wählen Sie im AWS Supply Chain Konsolen-Dashboard aus der Dropdownliste die Instanz aus, die Sie löschen möchten.



3. Wählen Sie Löschen aus.
4. Geben Sie auf der Seite „ AWS Supply Chain Instanz löschen“ unter Bestätigung ein, **`delete`** um zu bestätigen, dass Sie die Instanz löschen möchten.
5. Wählen Sie Löschen aus. Das Löschen der Instanz beginnt und sobald die Instanz gelöscht ist, wird eine Bestätigungsnachricht angezeigt.

Sicherheit in AWS Supply Chain

Cloud-Sicherheit bei AWS hat höchste Priorität. Als - AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die AWS Builds sind, um die Anforderungen der sicherheitssensibelsten Organisationen zu erfüllen.

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

- Sicherheit der Cloud – AWS ist für den Schutz der Infrastruktur verantwortlich, die AWS-Services in der ausgeführt wird AWS Cloud. stellt Ihnen AWS außerdem Services bereit, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS -Compliance-Programme regelmäßig. Informationen zu den Compliance-Programmen, die für gelten AWS Supply Chain, finden Sie unter AWS Im Rahmen des Compliance-Programms zugelassene -ServicesIm -Services.
- Sicherheit in der Cloud – Die AWS-Service , die Sie verwenden, bestimmt Ihre Verantwortung. Sie sind auch für andere Faktoren verantwortlich. umfassen die Vertraulichkeit Ihrer Daten, Ihre Anforderungen und die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der geteilten Verantwortung bei der Verwendung von einsetzen können AWS Supply Chain. Die folgenden Themen zeigen Ihnen, wie Sie konfigurieren, AWS Supply Chain um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere verwenden AWS-Services , die Ihnen bei der Überwachung und Sicherung Ihrer - AWS Supply Chain Ressourcen helfen.

Themen

Datenschutz in AWS Supply Chain

Das Modell der AWS gemeinsamen Verantwortung und geteilter Verantwortung gilt für den Datenschutz in AWS Supply Chain. 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
- 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 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit der Konsole, der API AWS Supply Chain oder den SDKs arbeiten oder diese anderweitig AWS-Services verwenden. AWS CLI AWS 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.

Daten, die von AWS Supply Chain verarbeitet werden

Um die Daten einzuschränken, auf die autorisierte Benutzer einer bestimmten AWS Supply-Chain-Instanz zugreifen können, werden die in AWS Supply Chain gespeicherten Daten nach Ihrer AWS Konto-ID und Ihrer AWS Supply-Chain-Instanz-ID getrennt.

AWS Supply Chain verarbeitet eine Vielzahl von Lieferkettendaten wie Benutzerinformationen, aus dem Datenkonnektor extrahierte Informationen und Inventardetails.

Bevorzugte Abmeldung

Wir können Ihre Inhalte, die von verarbeitet werden, verwenden und speichern AWS Supply Chain, wie in den AWS-Servicebedingungen angegeben. Wenn Sie sich von AWS Supply Chain der Nutzung oder Speicherung Ihrer Inhalte abmelden möchten, können Sie in AWS Organizations eine Opt-Out-Richtlinie erstellen. Weitere Informationen zur Erstellung einer Opt-Out-Richtlinie finden Sie unter Syntax und Beispiele für die Opt-Out-Richtlinie für AI-Services.

Verschlüsselung im Ruhezustand

Als PII eingestufte Kontaktdaten oder Daten, die Kundeninhalte darstellen AWS Supply Chain, von denen gespeichert wird, werden im Ruhezustand (d. h. bevor sie gespeichert, gespeichert oder auf einer Festplatte gespeichert werden) mit einem zeitlich begrenzten und instanzspezifischen Schlüssel verschlüsselt. AWS Supply Chain

Die serverseitige Amazon S3 S3-Verschlüsselung wird verwendet, um alle Konsolen- und Webanwendungsdaten mit einem AWS Key Management Service Datenschlüssel zu verschlüsseln, der für jedes Kundenkonto einzigartig ist. Weitere Informationen dazu finden Sie AWS KMS keys unter Was ist? AWS Key Management Service im AWS Key Management Service Entwicklerhandbuch.

> **Note**
>
> AWS Supply Chain bietet Supply Planning und N-Tier Visibility und unterstützt keine Verschlüsselung data-at-rest mit dem mitgelieferten KMS-CMK.

Verschlüsselung während der Übertragung

Mit AWS Supply Chain ausgetauschte Daten werden bei der Übertragung zwischen dem Webbrowser des Benutzers und der AWS Lieferkette mithilfe der branchenüblichen TLS-Verschlüsselung geschützt.

Schlüsselverwaltung

AWS Supply Chain unterstützt teilweise KMS-CMK.

Informationen zur Aktualisierung des AWS-KMS-Schlüssels in AWS Supply Chain finden Sie unterEine Instance erstellen.

Datenschutz für den Datenverkehr zwischen Netzwerken

> **Note**
>
> AWS Supply Chain unterstützt nicht PrivateLink.

Ein Virtual Private Cloud (VPC) -Endpunkt für AWS Supply Chain ist eine logische Einheit innerhalb einer VPC, die nur Konnektivität für ermöglicht. AWS Supply Chain Die VPC leitet Anfragen an die VPC weiter AWS Supply Chain und leitet Antworten zurück an sie. Weitere Informationen finden Sie unter VPC-Endpoints im VPC-Benutzerhandbuch.

Wie verwendet Grants AWS Supply Chain in AWS KMS

AWS Supply Chain erfordert einen Zuschuss, um Ihren vom Kunden verwalteten Schlüssel verwenden zu können.

AWS Supply Chain erstellt mehrere Zuschüsse mithilfe des AWS KMS Schlüssels, der während des CreateInstanceVorgangs übergeben wird. AWS Supply Chain erstellt in Ihrem Namen einen Zuschuss, indem CreateGrantAnfragen an gesendet AWS KMS werden. Zuschüsse in AWS KMS werden verwendet, um AWS Supply Chain Zugriff auf den AWS KMS Schlüssel in einem Kundenkonto zu gewähren.

> **Note**
>
> AWS Supply Chain verwendet seinen eigenen Autorisierungsmechanismus. Sobald ein Benutzer hinzugefügt wurde AWS Supply Chain, können Sie denselben Benutzer mithilfe der AWS KMS Richtlinie nicht mehr auf die Liste setzen.

AWS Supply Chain verwendet den Zuschuss für folgende Zwecke:

- Um GenerateDataKeyAnfragen AWS KMS zur Verschlüsselung der in Ihrer Instanz gespeicherten Daten zu senden.
- Um Decrypt-Anfragen an zu AWS KMS senden, um Ihre mit der Instance verknüpften verschlüsselten Daten zu lesen.
- Um DescribeKey, und RetireGrantBerechtigungen hinzuzufügen CreateGrant, um Ihre Daten zu schützen, wenn Sie sie an andere AWS Dienste wie Amazon Forecast senden.

Sie können den Zugriff auf die Genehmigung jederzeit widerrufen oder den Zugriff des Services auf den vom Kunden verwalteten Schlüssel entfernen. Wenn Sie dies tun, können Sie auf AWS Supply Chain keine der mit dem vom Kunden verwalteten Schlüssel verschlüsselten Daten zugreifen, was sich auf Vorgänge auswirkt, die von diesen Daten abhängig sind.

Überwachen Sie Ihre Verschlüsselung für AWS Supply Chain

Die folgenden Beispiele sind AWS CloudTrail Ereignisse für`Encrypt`, und `Decrypt` zur Überwachung von KMS-Vorgängen`GenerateDataKey`, die aufgerufen werden, AWS Supply Chain um auf Daten zuzugreifen, die mit Ihrem vom Kunden verwalteten Schlüssel verschlüsselt wurden:

Encrypt


```
          {
"eventVersion": "1.08",
"userIdentity": {
    "type": "AWSService",
    "invokedBy": "scn.amazonaws.com"
},
"eventTime": "2024-03-06T22:39:32Z",
"eventSource": "kms.amazonaws.com",
"eventName": "Encrypt",
```

```
    "awsRegion": "us-east-1",
    "sourceIPAddress": "172.12.34.56"
    "userAgent": "Example/Desktop/1.0 (V1; OS)",
    "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
    },
    "responseElements": null,
    "requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "readOnly": true,
    "resources": [
        {
            "accountId": account ID,
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "112233445566",
    "sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
    "eventCategory": "Management"
}
```

GenerateDataKey

```
            {
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "scn.amazonaws.com"
    },
     "eventTime": "2024-03-06T22:39:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "172.12.34.56"
    "userAgent": "Example/Desktop/1.0 (V1; OS)",
```

```
    "requestParameters": {
        "encryptionContext": {
            "aws:s3:arn": "arn:aws:s3:::test/rawEvent/bf6666c1-111-48aaca-b6b0-
dsadsadsa3432423/noFlowName/scn.data.inboundorder/20240306_223934_536"
        },
        "keyId": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample",
        "keySpec": "AES_222"
    },
    "responseElements": null,
    "requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "readOnly": true,
    "resources": [
        {
            "accountId": account ID,
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "112233445566",
    "sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
    "eventCategory": "Management"
}
```

Decrypt

```
            {
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "scn.amazonaws.com"
    },
     "eventTime": "2024-03-06T22:39:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "172.12.34.56"
```

```
    "userAgent": "Example/Desktop/1.0 (V1; OS)",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample",
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "readOnly": true,
    "resources": [
        {
            "accountId": account ID,
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "112233445566",
    "sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
    "eventCategory": "Management"
}
```

Zugriff AWS Supply Chain über einen Schnittstellenendpunkt (AWS PrivateLink)

Sie können verwenden AWS PrivateLink , um eine private Verbindung zwischen Ihrer VPC und herzustellen AWS Supply Chain. Sie können auf zugreifen, AWS Supply Chain als wäre es in Ihrer VPC, ohne die Verwendung eines Internet-Gateways, NAT-Geräts, einer VPN-Verbindung oder einer - AWS Direct Connect Verbindung. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um auf zuzugreifen AWS Supply Chain.

Sie stellen diese private Verbindung her, indem Sie einen Schnittstellen-Endpunkt erstellen, der von AWS PrivateLink unterstützt wird. Wir erstellen eine Endpunkt-Netzwerkschnittstelle in jedem Subnetz, das Sie für den Schnittstellen-Endpunkt aktivieren. Hierbei handelt es sich um vom Anforderer verwaltete Netzwerkschnittstellen, die als Eingangspunkt für den Datenverkehr dienen, der für AWS Supply Chain bestimmt ist.

Weitere Informationen finden Sie unter Zugriff AWS-Services über AWS PrivateLink im AWS PrivateLink -Handbuch.

Überlegungen für AWS Supply Chain

Bevor Sie einen Schnittstellenendpunkt für einrichten AWS Supply Chain, lesen Sie Überlegungen im AWS PrivateLink -Handbuch.

AWS Supply Chain unterstützt Aufrufe aller API-Aktionen über den Schnittstellenendpunkt.

Erstellen eines Schnittstellenendpunkts für AWS Supply Chain

Sie können einen Schnittstellenendpunkt für entweder AWS Supply Chain über die Amazon-VPC-Konsole oder die AWS Command Line Interface (AWS CLI) erstellen. Weitere Informationen finden Sie unter Erstellen eines Schnittstellenendpunkts im AWS PrivateLink -Leitfaden.

Erstellen Sie einen Schnittstellenendpunkt für AWS Supply Chain unter Verwendung des folgenden Servicenamens:

```
com.amazonaws.region.scn
```

Wenn Sie ein privates DNS für den Schnittstellenendpunkt aktivieren, können Sie API-Anforderungen an AWS Supply Chain unter Verwendung des standardmäßigen regionalen DNS-Namens senden. Beispiel: `scn.region.amazonaws.com`

Erstellen einer Endpunktrichtlinie für Ihren Schnittstellen-Endpunkt

Eine Endpunktrichtlinie ist eine IAM-Ressource, die Sie an einen Schnittstellen-Endpunkt anfügen können. Die Standard-Endpunktrichtlinie ermöglicht vollen Zugriff auf AWS Supply Chain über den Schnittstellenendpunkt. Um den Zugriff auf AWS Supply Chain von Ihrer VPC aus zu steuern, fügen Sie dem Schnittstellenendpunkt eine benutzerdefinierte Endpunktrichtlinie hinzu.

Eine Endpunktrichtlinie gibt die folgenden Informationen an:

- Die Prinzipale, die Aktionen ausführen können (AWS-Konten, IAM-Benutzer und IAM-Rollen)
- Aktionen, die ausgeführt werden können
- Die Ressourcen, für die die Aktionen ausgeführt werden können

Weitere Informationen finden Sie unter Steuern des Zugriffs auf Services mit Endpunktrichtlinien im AWS PrivateLink -Leitfaden.

Beispiel: VPC-Endpunktrichtlinie für - AWS Supply Chain Aktionen

Im Folgenden finden Sie ein Beispiel für eine benutzerdefinierte Endpunktrichtlinie. Wenn Sie diese Richtlinie an Ihren Schnittstellen-Endpunkt anhängen, gewährt sie allen Prinzipalen auf allen Ressourcen den Zugriff auf die aufgeführten AWS Supply Chain -Aktionen.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [

            "scn:action-1",
            "scn:action-2",
            "scn:action-3"

         ],
         "Resource":"*"
      }
   ]
}
```

IAM für AWS Supply Chain

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 Ressourcen zu verwenden. AWS Supply Chain IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

Zielgruppe

Die Art und Weise, wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, in der Sie tätig sind. AWS Supply Chain

Dienstbenutzer — Wenn Sie den AWS Supply Chain Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen zur Verfügung. Wenn Sie für Ihre Arbeit mehr AWS Supply Chain Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Fuktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Unter Problembehebung bei Identität und Zugriff AWS Supply Chain finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf eine Feature in AWS Supply Chain haben.

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

IAM-Administrator: Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf AWS Supply Chain verfassen können. Beispiele für AWS Supply Chain identitätsbasierte Richtlinien, die Sie in IAM verwenden können, finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Supply Chain

Authentifizierung mit Identitäten

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

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

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

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

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

AWS-Konto Root-Benutzer

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

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine

Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center - Benutzerhandbuch.

IAM-Benutzer und -Gruppen

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

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen wechseln. Sie können eine Rolle übernehmen, indem Sie eine AWS

CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

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

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontenübergreifenden Zugriff finden Sie unter Kontenübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige verwenden Funktionen in anderen. AWS-Services AWS-Services Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon-EC2 aus oder speichert Objekte in Amazon-S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über

Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

- Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
- Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

- Anwendungen, die auf Amazon EC2 ausgeführt werden — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

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

Verwalten des Zugriffs mit Richtlinien

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

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

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

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

Identitätsbasierte Richtlinien

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

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

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen

in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

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

Zugriffssteuerungslisten (ACLs)

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

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

Weitere Richtlinientypen

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

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Service Control Policies (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos

Weitere Informationen zu Organizations und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations -Benutzerhandbuch.

- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

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

Wie AWS Supply Chain funktioniert mit IAM

Bevor Sie IAM zur Verwaltung des Zugriffs auf verwenden, sollten Sie sich darüber informieren AWS Supply Chain, mit welchen IAM-Funktionen Sie arbeiten können. AWS Supply Chain

IAM-Funktionen, die Sie mit verwenden können AWS Supply Chain

IAM-Feature	AWS Supply Chain Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
Temporäre Anmeldeinformationen	Ja

IAM-Feature	AWS Supply Chain Unterstützung
Forward Access Sessions (FAS)	Ja
Servicerollen	Ja
Service-verknüpfte Rollen	Nein

Einen allgemeinen Überblick darüber, wie AWS Supply Chain und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

Identitätsbasierte Richtlinien für AWS Supply Chain

Unterstützt Richtlinien auf Identitätsbasis.	Ja

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

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für AWS Supply Chain

Beispiele für AWS Supply Chain identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Supply Chain

Ressourcenbasierte Richtlinien finden Sie in AWS Supply Chain

Unterstützt ressourcenbasierte Richtlinien	Nein

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

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Kontenübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Politische Maßnahmen für AWS Supply Chain

Unterstützt Richtlinienaktionen	Ja

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

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

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

Bei Richtlinienaktionen wird vor der Aktion das folgende Präfix AWS Supply Chain verwendet:

```
scn
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "scn:action1",
      "scn:action2"
         ]
```

Beispiele für AWS Supply Chain identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Supply Chain

Politische Ressourcen für AWS Supply Chain

Unterstützt Richtlinienressourcen	Ja

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

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

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

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

Beispiele für AWS Supply Chain identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Supply Chain

Bedingungsschlüssel für Richtlinien für AWS Supply Chain

Unterstützt servicespezifische Richtlinienbedingungsschlüssel	Ja

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

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

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

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Beispiele für AWS Supply Chain identitätsbasierte Richtlinien finden Sie unter. Beispiele für identitätsbasierte Richtlinien für AWS Supply Chain

Verwenden temporärer Anmeldeinformationen mit AWS Supply Chain

Unterstützt temporäre Anmeldeinformationen	Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Zugriffssitzungen weiterleiten für AWS Supply Chain

Unterstützt Forward Access Sessions (FAS)	Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für AWS Supply Chain

Unterstützt Servicerollen	Ja

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Durch das Ändern der Berechtigungen für eine Servicerolle kann die AWS Supply Chain Funktionalität beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, AWS Supply Chain wenn Sie dazu eine Anleitung erhalten.

Dienstbezogene Rollen für AWS Supply Chain

Unterstützt serviceverknüpfte Rollen	Nein

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von dienstbezogenen Rollen finden Sie unter AWS-Services Diese Rollen funktionieren mit IAM. Suchen Sie in der Tabelle nach einem Service mit einem `Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Beispiele für identitätsbasierte Richtlinien für AWS Supply Chain

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Ressourcen zu erstellen oder zu ändern AWS Supply Chain . Sie können auch keine Aufgaben mithilfe der AWS-Managementkonsole, der AWS-Befehlszeilenschnittstelle (AWS CLI) oder der AWS-API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen zum Erstellen einer identitätsbasierten IAM-Richtlinie mithilfe dieser Beispieldokumente zu JSON-Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Themen

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. AWS Supply Chain Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst 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 AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen 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. AWS 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 zum 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 Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

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

Problembehebung bei Identität und Zugriff AWS Supply Chain

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS Supply Chain und IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS Supply Chain
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS Supply Chain Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS Supply Chain

Wenn Sie nicht berechtigt sind AWS Management Console , eine Aktion auszuführen, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator ist die Person, die Ihnen Ihren Benutzernamen und Ihr Passwort bereitgestellt hat.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `scn:`*`GetWidget`*-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 scn:GetWidget on resource: my-example-widget
```

In diesem Fall bittet Mateo seinen Administrator um die Aktualisierung seiner Richtlinien, um unter Verwendung der Aktion *my-example-widget* auf die Ressource `scn:GetWidget` zugreifen zu können.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Durchführen der `iam:PassRole`-Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an AWS Supply Chainübergeben zu 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 in AWS Supply Chain 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.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine AWS Supply Chain Ressourcen ermöglichen

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

Weitere Informationen dazu finden Sie hier:

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

AWS Von verwaltete Richtlinien für AWS Supply Chain

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

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

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

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

AWSverwaltete Richtlinie: AWSSupplyChainFederationAdminAccess

AWSSupplyChainFederationAdminAccess bietet AWS Supply Chain Verbundbenutzern Zugriff auf die AWS Supply Chain Anwendung, einschließlich der erforderlichen Berechtigungen, um Aktionen innerhalb der AWS Supply Chain Anwendung auszuführen. Die Richtlinie gewährt Administratorberechtigungen für IAM Identity Center-Benutzer und -Gruppen und ist einer Rolle zugeordnet, die von AWS Supply Chain Ihnen erstellt wurde. Sie sollten die AWSSupplyChainFederationAdminAccess Richtlinie nicht an andere IAM-Entitäten anhängen.

Diese Richtlinie gewährt zwar den gesamten Zugriff AWS Supply Chain über die scn: *-Berechtigungen, Ihre Berechtigungen werden jedoch von der AWS Supply Chain Rolle bestimmt. Die AWS Supply Chain Rolle umfasst nur die erforderlichen Berechtigungen und hat keine Berechtigungen für die Admin-APIs.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `Chime`— Ermöglicht den Zugriff auf das Erstellen oder Löschen von Benutzern unter einem Amazon Chime AppInstance; Ermöglicht den Zugriff auf die Verwaltung von Kanälen, Kanalmitgliedern und Moderatoren; Ermöglicht den Zugriff zum Senden von Nachrichten an den Kanal. Chime-Operationen sind auf App-Instances beschränkt, die mit „SCN“ gekennzeichnet sind. InstanceId
- `AWS IAM Identity Center (AWS SSO)`— Stellt die erforderlichen Berechtigungen bereit, um Benutzerprofile zuzuordnen und zu trennen und Profile aufzulisten, die mit der IAM Identity Center-Anwendungsinstanz verknüpft sind.
- `AppFlow`— Ermöglicht den Zugriff auf das Erstellen, Aktualisieren und Löschen von Verbindungsprofilen; Ermöglicht den Zugriff auf das Erstellen, Aktualisieren, Löschen, Starten und Beenden von Flows; Ermöglicht den Zugriff auf Flows mit Tags und Untags sowie die Beschreibung von Flow-Datensätzen.
- `Amazon S3`— Ermöglicht den Zugriff auf eine Liste aller Buckets. Stellt GetBucketLocation,, GetBucketPolicy PutObject GetObject, und ListBucket Zugriff auf Buckets mit der Ressource arn arn:aws:s3::: -* bereit. aws-supply-chain-data

- `SecretsManager`— Ermöglicht den Zugriff auf die Erstellung von Geheimnissen und die Aktualisierung von Geheimrichtlinien.
- `KMS`— Ermöglicht Amazon AppFlow Service den Zugriff auf Listenschlüssel und Schlüsselalias. Stellt KMS-Schlüssel zur ListGrants Verfügung DescribeKey, die mit dem Schlüsselwert aws-suply-chain-access : true gekennzeichnet sind, CreateGrant und berechtigt dazu. Ermöglicht den Zugriff auf die Erstellung von Geheimnissen und die Aktualisierung von Geheimrichtlinien.

  Die Berechtigungen (kms: ListKeys, kms: ListAliases, kms: GenerateDataKey und kms:Decrypt) sind nicht auf Amazon beschränkt AppFlow und diese Berechtigungen können für jeden AWS KMS Schlüssel in Ihrem Konto gewährt werden.

Die Berechtigungen dieser Richtlinie finden Sie in der. AWSSupplyChainFederationAdminAccessAWS Management Console

AWS Supply Chain-Aktualisierungen für AWS verwaltete Richtlinien

In der folgenden Tabelle sind Einzelheiten zu den Aktualisierungen der AWS verwalteten Richtlinien aufgeführt, die AWS Supply Chain seit Beginn der Erfassung dieser Änderungen durch diesen Dienst vorgenommen wurden. Um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Seite AWS Supply Chain-Dokumentverlauf.

Änderung	Beschreibung	Datum
AWSSupplyChainFederationAdminAccess— Aktualisierte Richtlinie	AWS Supply ChainDie verwaltete Richtlinie wurde aktualisiert, um Verbundbenutzern den Zugriff auf ListProfileAssociations Vorgänge im IAM Identity Center zu ermöglichen.	01. November 2023
AWSSupplyChainFederationAdminAccess— Aktualisierte Richtlinie	AWS Supply ChainDie verwaltete Richtlinie wurde aktualisiert, um Verbundbenutzern den Zugriff auf die	21. September 2023

Änderung	Beschreibung	Datum
	PutObject und GetObject - Operationen im dedizierten S3-Bucket mit der Ressource arn arn:aws:s3: ::aws-supply-chaindata-* zu ermöglichen.	
AWSSupplyChainFederationAdminAccess – Neue Richtlinie.	AWS Supply Chainhat eine neue Richtlinie hinzugefügt, die Verbundbenutzern den Zugriff auf die Anwendung ermöglicht. AWS Supply Chain Dazu gehören auch Berechtigungen, die für die Ausführung von Aktionen innerhalb der AWS Supply Chain Anwendung erforderlich sind.	01. März 2023
AWS Supply Chain hat die Änderungsverfolgung gestartet	AWS Supply Chain hat mit der Verfolgung von Änderungen für seine AWS-verwalteten Richtlinien begonnen.	01. März 2023

Compliance-Validierung für AWS Supply Chain

Die Auditoren Dritter bewerten die Sicherheit und die Compliance von AWS Supply Chain im Rahmen mehrerer AWS-Compliance-Programme. Hierzu zählen unter anderem SOC, PCI, FedRAMP und HIPAA.

Allgemeine Informationen finden Sie unter AWS-Compliance-Programme.

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

Ihre Compliance-Verantwortung bei der VerwendungAWS Supply Chain der Daten, den geltenden Gesetzen und Vorschriften, hängt von der Vertraulichkeit der Daten, den geltenden Gesetzen und

Vorschriften ab. AWSstellt die folgenden Ressourcen bereit, um Sie bei der folgenden Ressourcen bei der folgenden zu unterstützen:

- Kurzanleitungen für Sicherheit und Compliance Kurzanleitungen für — In diesen Bereitstellungsleitfäden finden Sie wichtige Überlegungen zur Architektur sowie die einzelnen Schritte zur Bereitstellung von sicherheits- und Compliance-orientiertenAWS Basisumgebungen.
- Whitepaper zur Erstellung einer Architektur mit HIPAA-konformer Sicherheit und Compliance – In diesem Whitepaper wird beschrieben, wie Unternehmen mithilfe von AWS HIPAA-konforme Anwendungen erstellen können.
- AWS Compliance Ressourcen – Diese Sammlung von Arbeitsbüchern und Leitfäden könnte auf Ihre Branche und Ihren Standort zutreffen.
- Evaluating Resources with Rules in theAWS Config Developer Guide — In diesem Leitfaden, wie gut Ihre Ressourcenkonfigurationen mit internen Praktiken, Branchenrichtlinien und Vorschriften übereinstimmen.
- AWS Security Hub— DieserAWS-Service liefert einen umfassenden Überblick über den Sicherheitsstatus in. So können SieAWS die Compliance mit den Sicherheitsstandards in der Branche und den bewährten Methoden in.

Ausfallsicherheit in AWS Supply Chain

Im Zentrum derAWS globalen -Infrastruktur stehen dieAWS-Regionen -Availability Zones. AWS-Regionenstellen Sie mehrere physisch getrennte und isolierte Availability Zones bereit. Diese sind mit Netzwerken mit niedriger Latenz und hohem Durchsatz verbunden mit Netzwerken mit niedriger Latenz und hohem Durchsatz. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

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

Zusätzlich zur globalen AWS-Infrastruktur stellt AWS Supply Chain verschiedene Funktionen bereit, um Ihren Anforderungen in Bezug auf Ausfallsicherheit und Datensicherung zu erfüllen.

Protokollierung und Überwachung AWS Supply Chain

Protokollierung und Überwachung sind ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von AWS Supply Chain und Ihren anderen AWS Lösungen. AWS bietet das AWS CloudTrail Überwachungstool, mit dem Sie die AWS Lieferkette überwachen, melden können, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen ergreifen können.

> **Note**
>
> APIs, die nur von der AWS Supply Chain Konsole aus aufgerufen werden, werden erfasst AWS CloudTrail.

AWS CloudTrail erfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS-Konto -Kontos erfolgten, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon-S3-Bucket. Sie können die Benutzer und Konten, die AWS aufgerufen haben, identifizieren, sowie die Quell-IP-Adresse, von der diese Aufrufe stammen, und den Zeitpunkt der Aufrufe ermitteln. Sie können die Ereignisse in der AWS Lieferkette unter scn.amazonaws.com einsehen. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

> **Note**
>
> Beachten Sie Folgendes bei: AWS Supply Chain
>
> - Wenn Sie Benutzer einladen, die keinen Zugriff darauf haben AWS Supply Chain, erhalten diese Benutzer in den Benachrichtigungen, die sie von der Webanwendung erhalten, keine Informationen. Eingeladene Benutzer erhalten eine E-Mail-Benachrichtigung mit einem Link zur Webanwendung. Sie können sich nur anmelden und den Inhalt der Benachrichtigung ansehen, wenn sie über die erforderlichen Benutzerberechtigungen verfügen.
> - Alle Benutzer mit oder ohne Benutzerberechtigungen für einen bestimmten Insight können die Insights-Chat-Nachrichten einsehen.
> - Wenn Sie als Anwendungsadministrator Benutzer zur AWS Supply Chain Instanz hinzufügen, haben diese Zugriff auf die AWS KMS key. Sie können die Benutzerberechtigungen zum Hinzufügen oder Entfernen von Benutzern verwalten. Weitere Informationen zu Benutzerberechtigungen finden Sie unterRollen mit Benutzerberechtigungen.

AWS Supply Chain Datenereignisse in CloudTrail

Datenereignisse liefern Informationen über die Ressourcenoperationen, die auf oder in einer Ressource ausgeführt werden (z. B. Lesen oder Schreiben in ein Amazon-S3-Objekt). Sie werden auch als Vorgänge auf Datenebene bezeichnet. Datenereignisse sind oft Aktivitäten mit hohem Volume. Protokolliert standardmäßig CloudTrail keine Datenereignisse. Der CloudTrail Ereignisverlauf zeichnet keine Datenereignisse auf.

Für Datenereignisse werden zusätzliche Gebühren fällig. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preisgestaltung.

Sie können Datenereignisse für die AWS Supply Chain Ressourcentypen mithilfe der CloudTrail Konsole oder CloudTrail API-Operationen protokollieren. AWS CLI

- Um Datenereignisse mithilfe der CloudTrail Konsole zu protokollieren, erstellen Sie einen Trail - oder Ereignisdatenspeicher, um Datenereignisse zu protokollieren, oder aktualisieren Sie einen vorhandenen Trail- oder Ereignisdatenspeicher, um Datenereignisse zu protokollieren.

  1. Wählen Sie Datenereignisse aus, um Datenereignisse zu protokollieren.
  2. Wählen Sie aus der Liste Datenereignistyp den Ressourcentyp aus, für den Sie Datenereignisse protokollieren möchten.
  3. Wählen Sie die Protokollauswahlvorlage aus, die Sie verwenden möchten. Sie können alle Datenereignisse für den Ressourcentyp protokollieren, alle `readOnly` Ereignisse protokollieren, alle `writeOnly` Ereignisse protokollieren oder eine benutzerdefinierte Protokollauswahlvorlage erstellen, um nach den Feldern `readOnly`eventName, und `resources.`ARN zu filtern.

- Um Datenereignisse mithilfe von zu protokollieren AWS CLI, konfigurieren Sie den `--advanced-event-selectors` Parameter so, dass das `eventCategory` Feld dem Wert des Ressourcentyps entspricht `Data` und das `resources.type` Feld dem Ressourcentypwert entspricht. Sie können Bedingungen hinzufügen, um nach den Werten der `resources.`ARN Felder `readOnly`eventName, und zu filtern.
  - Führen Sie den put-event-selectorsBefehl aus, um einen Trail zum Protokollieren von Datenereignissen zu konfigurieren. Weitere Informationen finden Sie unter Protokollieren von Datenereignissen für Trails mit dem AWS CLI.
  - Um einen Ereignisdatenspeicher für die Protokollierung von Datenereignissen zu konfigurieren, führen Sie den create-event-data-storeBefehl aus, um einen neuen Ereignisdatenspeicher zum Protokollieren von Datenereignissen zu erstellen, oder führen Sie den update-event-

data-storeBefehl aus, um einen vorhandenen Ereignisdatenspeicher zu aktualisieren. Weitere Informationen finden Sie unter Protokollieren von Datenereignissen für Ereignisdatenspeicher mit dem AWS CLI.

*Sie können erweiterte Event-Selektoren so konfigurieren, dass sie nach den `resources.ARN` Felder`eventName`, und filtern`readOnly`, sodass nur die Ereignisse protokolliert werden, die für Sie wichtig sind. Weitere Informationen zu diesen Feldern finden Sie unter AdvancedFieldSelector.

AWS Supply Chain Verwaltungsereignisse in CloudTrail

Verwaltungsereignisse enthalten Informationen über Verwaltungsvorgänge, die mit Ressourcen in Ihrem AWS Konto ausgeführt werden. Sie werden auch als Vorgänge auf Steuerebene bezeichnet. CloudTrail Protokolliert standardmäßig Verwaltungsereignisse.

AWS Supply Chain protokolliert alle Operationen auf der Kontrollebene CloudTrail als Managementereignisse.

AWS Supply Chain APIs für Webanwendungen

Die in diesem Abschnitt aufgeführten APIs werden von AWS Supply Chain Anwendungen im Namen von Verbundbenutzern aufgerufen. Diese APIs sind in den CloudTrail Protokollen nicht sichtbar und werden auch nicht im Referenzdokument zur Serviceautorisierung erfasst, siehe AWS Supply Chain. Der Zugriff auf diese APIs wird durch AWS Supply Chain Anwendungen gesteuert, die auf Verbundberechtigungen für Benutzerrollen basieren. Sie sollten nicht versuchen, den Zugriff auf diese APIs zu kontrollieren, um zu verhindern, dass die Anwendungen gestört werden. AWS Supply Chain

Benutzerrollen

Die folgenden APIs werden für die Verwaltung von Benutzern, Benutzerrollen, Benutzerbenachrichtigungen und Chat-Nachrichten in verwendet. AWS Supply Chain

```
scn:AddMembersToResourceBasedChat
scn:AssignGalaxyRoleToUser
scn:AssociateUser
scn:BatchGetUsers
scn:BatchMarkNotificationAsDelivered
scn:CreateRole
```

```
scn:DeleteRole
scn:DescribeChatForUser
scn:GetAccessDetailConfig
scn:GetChatPreferencesForUser
scn:GetMessagingSessionConnectionDetails
scn:GetNotificationsPreference
scn:GetOrCreateChimeUser
scn:GetOrCreateResourceBasedChat
scn:GetOrCreateUserBasedChat
scn:GetOrganizationInfo
scn:GetResourceBasedChatArn
scn:GetUserDetails
scn:ListChatMembers
scn:ListChatMessages
scn:ListChatModerators
scn:ListChats
scn:ListRoles
scn:ListUserNotifications
scn:ListUsersWithRole
scn:MarkNotificationAsDelivered
scn:MarkNotificationAsRead
scn:RemoveMemberFromResourceBasedChat
scn:RemoveUser
scn:SearchChimeUsers
scn:SearchUsers
scn:SendChatMessage
scn:SetNotificationsPreference
scn:UpdateChatPreferencesForUser
scn:UpdateChatReadMarker
scn:UpdateOrganizationInfo
scn:UpdateRole
scn:UpdateUser
```

Datensee

Die folgenden APIs werden für die Erstellung und Verwaltung von Datenflüssen und Verbindungen im Data Lake verwendet.

```
scn:CreateConnection
```

```
scn:CreateDataflow
scn:CreateDeleteDataByPartitionJob
scn:CreateExtractFlows
scn:CreatePresignedUrl
scn:CreateSampleParsingJob
scn:CreateSapODataConnection
scn:CreateUpdateDatasetSchemaJob
scn:DeleteConnection
scn:DeleteDataflow
scn:DeleteExtractFlows
scn:DeleteSapODataConnection
scn:describeDatasetGroup
scn:DescribeDataset
scn:DescribeJob
scn:GetConnection
scn:GetCreateExtractFlowsStatus
scn:GetDataflow
scn:ListConnections
scn:ListCustomerFiles
scn:ListDataflows
scn:ListDataflowStats
scn:ListDatasets
scn:UpdateConnection
scn:UpdateDataflow
scn:UpdateExtractFlow
```

Insights

Die folgenden APIs werden von der Insights-Anwendung verwendet, um Filter und Beobachtungslisten zu verwalten und Inventaränderungen anzuzeigen.

```
scn:AddModeratorToResourceBasedChat
scn:ComputePostRebalancedQuantities
scn:ComputePostRebalancedQuantitiesV1
scn:CreateInsightFilter
scn:CreateInsightSubscription
scn:DeleteInsightFilter
scn:DeleteInsightSubscription
scn:GetInsightLineItem
```

```
scn:GetInsightSubscription
scn:GetInstanceAttribute
scn:GetInstanceRequiredDatasetAvailabilityStatus
scn:GetKpiData
scn:GetModelEndpointStatus
scn:GetPIVForProduct
scn:GetPIVForSite
scn:GetPIVForSiteAndProduct
scn:GetPIVForSitesAndProducts
scn:GetProducts
scn:GetProductSummaryAggregates
scn:GetSites
scn:GetSiteSummaryAggregates
scn:IsUserAuthorizedForInsightLineItem
scn:ListCustomAttributeValues
scn:ListGeographiesAsGalaxyAdmin
scn:ListInsightFilters
scn:ListInsightLineItems
scn:ListInsightSubscriptions
scn:ListInventoryQuantityAggregates
scn:ListInventoryRisksBySiteAndProduct
scn:ListInventorySummariesBySite
scn:ListPIVProductsBySite
scn:ListProductHierarchiesAsGalaxyAdmin
scn:ListProducts
scn:ListProductsAsGalaxyAdmin
scn:ListSites
scn:ListUsers
scn:PotentiallyComputeThenListRebalancingOptionsForInsightLineItem
scn:RegisterInstanceAttribute
scn:UpdateInsightFilter
scn:UpdateInsightLineItemStatus
scn:UpdateInsightSubscription
scn:UpdateRebalancingOptionStatus
scn:UpdateRebalancingOptionStatusV1
```

Planung der Nachfrage

Die folgenden APIs werden AWS Supply Chain zur Erstellung und Verwaltung von Prognosen, Bedarfsplänen oder Arbeitsmappen verwendet.

```
scn:AssociateDatasetWithWorkbook
scn:CreateBaselineForecast
scn:CreateDemandPlan
scn:CreateDemandPlanningCycle
scn:CreateDemandPlanningDatasetExportJob
scn:CreateDerivedForecast
scn:CreateWorkbook
scn:DeleteDemandForecastConfig
scn:DeleteDemandPlanningCycle
scn:DeleteDerivedForecast
scn:DeleteWorkbook
scn:DescribeBaselineForecast
scn:DescribeDemandPlanningCycleAccuracyJob
scn:DescribeDerivedForecast
scn:DescribePlanningCycle
scn:DescribeWorkbook
scn:DisassociatePlanningCycle
scn:GetDemandForecastConfig
scn:GetDemandPlan
scn:GetDemandPlanningCycle
scn:GetDemandPlanningCycleAccuracy
scn:GetDemandPlanningDatasetJob
scn:ListDemandPlans
scn:ListDerivedForecasts
scn:ListForecastingJobs
scn:ListPlanningCycles
scn:ListWorkbooks
scn:PublishDemandPlan
scn:PutDemandForecastConfig
scn:StartDemandPlanningCycleAccuracyJob
scn:StartForecastingJob
scn:UpdateDemandPlan
scn:UpdateDemandPlanningCycleMetadata
scn:UpdateWorkbook
```

Angebotsplanung

Die folgenden APIs werden AWS Supply Chain zur Erstellung und Verwaltung von Lieferplänen verwendet.

```
scn:CreateReplenishmentPipeline
scn:GetReplenishmentPipeline
scn:UpdateReplenishmentPipeline
scn:ListReplenishmentPipelinesByInstance
scn:GetInstanceReplenishmentConfig
scn:CreateBacktest
scn:CreateReplenishmentReviewInstanceConfig
scn:GetReplenishmentReviewInstanceConfig
scn:ListReplenishmentVendors
scn:GetExceptionsSupplyInsightsStatistics
scn:GetPorSupplyInsightsStatistics
scn:GetPlanToPOConversionAnalytics
scn:GetPurchasePlanStatistics
scn:ListPlanExceptions
scn:ListPurchaseOrderRequestLines
scn:UpdatePurchaseOrderRequestLines
scn:ListBomPurchasePlans
scn:ListBomProductionPlans
scn:ListBomTransferPlans
scn:ListBomInsights
scn:ListBomProcesses
scn:ExportBomPlans
scn:GetBomPlanSummary
scn:GetDashboardAnalytics
scn:GetPurchaseOrderRequestExplanation
scn:ListBomSupplyPlan
scn:GetBomPlanRecordDetails
scn:GetBomPlanSummaryAnalytics
scn:ListBomPurchaseOrders
scn:ListBomTransferOrders
scn:ListBomProductionOrders
scn:ExportAllExplodedBoms
scn:ExportBillOfMaterials
scn:ExportInventoryPolicy
scn:ExportProductionProcess
scn:ExportSourcingRule
scn:ExportTransportationLane
scn:ExportVendorLeadTime
scn:ImportBillOfMaterials
scn:ImportInventoryPolicy
scn:ImportProductionProcess
```

```
scn:ImportSourcingRule
scn:ImportTransportationLane
scn:ImportVendorLeadTime
```

Kontingente für AWS Supply Chain

Ihr AWS-Konto verfügt über Standardkontingente, die früher als Limits bezeichnet wurden, für jede AWS-Service. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region. Sie können beantragen, die Kontingente für Ressourcen zu erhöhen, die auf Ihre Kontoebene festgelegt sind. Weitere Informationen zu Kontingenten auf Kontoebene finden Sie in der folgenden Tabelle.

Um die Kontingente für anzuzeigen AWS Supply Chain, öffnen Sie die Service Quotas-Konsole. Wählen Sie im Navigationsbereich AWS -Services und dann AWS Supply Chain aus.

Informationen zum Beantragen einer Kontingenterhöhung finden Sie unter Beantragen einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch. Wenn das Kontingent in Service Quotas noch nicht in verfügbar ist, verwenden Sie das Formular zur Erhöhung des Limits.

Ihr AWS-Konto verfügt über die folgenden Kontingente in Bezug auf AWS Supply Chain.

Ressource	Standard	Anpassbar
Anzahl der Instances **Note** Sie können bis zu 10 Instances innerhalb eines AWS Kontos erstellen.	10	Nein
Anzahl der Amazon S3-Buckets	100	Nein
Aktive und ausstehende Einladungen innerhalb eines AWS Kontos	30	Ja
Datenanforderungen innerhalb eines AWS Kontos	4.000	Ja

Ressource	Standard	Anpassbar
Insights-Einzelposten pro Watchlist	1.000	Nein
Insights-Watchlists pro Instance innerhalb eines AWS Kontos	1.000	Ja
Insights-Watchlists pro Benutzer innerhalb eines AWS Kontos	100	Ja

Anfordern administrativer Unterstützung für AWS Supply Chain

Wenn Sie als Administrator den Support für AWS Supply Chain kontaktieren möchten, wählen Sie eine der folgenden Optionen:

- Wenn Sie einAWS Support Konto haben, gehen Sie zum Support Center und reichen Sie ein Ticket ein.
- Öffnen Sie die AWS Management Consoleund wählen Sie AWSSupply Chain, Support, Create case.

Es ist hilfreich, die folgenden Informationen anzugeben:

- IhreAWS Supply-Chain-Instanz-ID/ARN.
- DeineAWS Region.
- Eine ausführliche Beschreibung Ihres Problems.

Dokumentenverlauf für das AWS Supply Chain Administratorhandbuch

In der folgenden Tabelle werden die Dokumentationsversionen für beschrieben AWS Supply Chain.

Änderung	Beschreibung	Datum
Aktualisierung der KMS-Richtlinie	Die KMS-Richtlinie wurde aktualisiert, um AWS Supply Chain den Zugriff auf Ihren AWS KMS Schlüssel zu ermöglichen.	18. März 2024
PrivateLink Unterstützung	Sie können AWS Supply Chain über einen Schnittstellenendpunkt (AWS PrivateLink) darauf zugreifen.	26. Februar 2024
Gruppen hinzufügen	Benutzer müssen Teil einer IAM Identity Center-Gruppe sein, um darauf zugreifen AWS Supply Chain zu können.	14. November 2023
Die AWS verwaltete Richtlinie wurde aktualisiert	AWS Supply Chain Die verwaltete Richtlinie wurde aktualisiert, um Verbundbenutzern den Zugriff auf ListProfileAssociations Vorgänge im IAM Identity Center zu ermöglichen.	1. November 2023
Die verwaltete Richtlinie wurde aktualisiert AWS	AWS Supply Chain hat die verwaltete Richtlinie aktualisiert, um Verbundbenutzern den Zugriff auf die PutObject GetObject AND-Operationen im dedizierten Amazon S3	21. September 2023

	S3-Bucket mit der Ressource arn arn:aws:s3: ::aws-supply-chaindata-* zu ermöglichen.	
Die Informationen zur Unterstützung der Regionen wurden aktualisiert	AWS Supply Chain Die Bedarfsplanung wird jetzt auch in der Region Asien-Pazifik (Sydney) unterstützt.	12. September 2023
Verwenden Sie die AWS Konsole, um sich an- und abzumelden AWS Supply Chain	AWS Supply Chain Benutzer können jetzt die AWS Konsole verwenden, um sich für die Verwendung oder Speicherung Ihrer Inhalte auf AWS Organizations an- und abzumelden AWS Supply Chain .	07. September 2023
Aktualisierte Informationen zum regionalen Support	AWS Supply Chain wird jetzt auch in der Region Asien-Pazifik (Sydney) und Europa (Irland) unterstützt.	19. Juli 2023
Aktualisierte Informationen zur Kontaktaufnahme mit dem AWS-Support und zur Erstellung einer Instance	AWS Supply Chain Benutzer können sich jetzt an den AWS-Support wenden, um Hilfe zu erhalten, und der Inhalt zur Erstellung einer Instance wurde aktualisiert.	03. April 2023

AWS Verwaltete Richtlinie hinzugefügt	AWS Supply Chain hat eine neue Richtlinie hinzugefügt, die Verbundbenutzern den Zugriff auf die AWS Supply Chain-Anwendung ermöglicht, einschließlich der Berechtigungen, die für die Ausführung von Aktionen innerhalb der AWS Supply Chain-Anwendung erforderlich sind.	1. März 2023
Erstversion	Erste Version des AWS Supply Chain Administratorhandbuchs.	29. November 2022

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.