管理者ガイド

AWS Supply Chain

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Supply Chain: 管理者ガイド

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスはAmazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

とは AWS Supply Chain

AWS Supply Chain は、データを統合し、需要予測と在庫の可視性を向上させる ML を活用した予測方法を提供するクラウドベースのサプライチェーン管理アプリケーションです。 実用的なインサイト、 組み込みのコンテキストコラボレーション、 需要計画、 供給計画、 n 層のサプライヤー可視性、 と持続可能性情報管理。 AWS Supply Chain は既存のエンタープライズリソースプランニング (ERP) とサプライチェーン管理システムに接続し、ML と生成 AI を使用してさまざまなデータを変換し、サプライチェーンデータレイク (SCDL) に統合できます。AWS Supply Chain は、リプラットフォーム、前払いライセンス料金、または長期契約なしで、サプライチェーンのリスク管理を改善できます。

トピック

- でサポートされているブラウザ AWS Supply Chain
- でサポートされている言語 AWS Supply Chain

でサポートされているブラウザ AWS Supply Chain

AWS Supply Chain を使用する前に、次の表を使用してブラウザがサポートされていることを確認します。

ブラウザ	サポートされるバージョン
Google Chrome	最新 3 バージョン
Mozilla Firefox ESR	バージョンは、Firefox の販売終了日までサポートされます。詳細については、「Firefox ESR release calendar」を参照してください。
Mozilla Firefox	最新 3 バージョン
Microsoft Edge および Edge Chromium	バージョン 84 以降
Safari	macOS 上の Safari 10 以降

でサポートされている言語 AWS Supply Chain

AWS Supply Chain では、次の言語がサポートされています。

- 英語 (米国)
- 英語 (英国)
- ドイツ語
- スペイン語
- フランス語
- イタリア語
- ポルトガル語
- 簡体字中国語
- 繁体字中国語
- 日本語
- 韓国語

AWS アカウントのセットアップ

このセクションを使用して、 AWS アカウントを作成し、IAM ユーザーを作成します。 AWS アカウントを作成するためのベストプラクティスについては、「ベストプラクティス AWS 環境の確立」を参照してください。

トピック

- にサインアップする AWS アカウント
- 管理アクセスを持つユーザーを作成する

にサインアップする AWS アカウント

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一部では、電話またはテキストメッセージを受信し、電話のキーパッドに検証コードを入力します。

   にサインアップすると AWS アカウント、 AWS アカウントのルートユーザー が作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティベストプラクティスとして、ユーザーに管理アクセス権を割り当て、ルートユーザーアクセスが必要なタスクの実行にはルートユーザーのみを使用するようにしてください。

AWS サインアッププロセスが完了すると、 から確認メールが送信されます。https://aws.amazon.com/ の [マイアカウント] をクリックして、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理することができます。

管理アクセスを持つユーザーを作成する

にサインアップしたら AWS アカウント、日常的なタスクにルートユーザーを使用しないように AWS アカウントのルートユーザー、 のセキュリティを確保し AWS IAM Identity Center、 を有効にして管理ユーザーを作成します。

を保護する AWS アカウントのルートユーザー

1. ルートユーザーを選択し、 AWS アカウント E メールアドレスを入力して、アカウント所有者AWS Management Consoleとして にサインインします。次のページでパスワードを入力します。

   ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドのルートユーザーとしてサインインするを参照してください。
2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、IAM ユーザーガイドの AWS アカウント 「ルートユーザー (コンソール) の仮想 MFA デバイスを有効にする」を参照してください。

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「AWS IAM Identity Centerの有効化」を参照してください。
2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

   を ID ソース IAM アイデンティティセンターディレクトリ として使用する方法のチュートリアルについては、「 AWS IAM Identity Center ユーザーガイド」の「デフォルトを使用してユーザーアクセスを設定する IAM アイデンティティセンターディレクトリ」を参照してください。

管理アクセス権を持つユーザーとしてサインインする

- IAM アイデンティティセンターのユーザーとしてサインインするには、IAM アイデンティティセンターのユーザーの作成時に E メールアドレスに送信されたサインイン URL を使用します。

  IAM Identity Center ユーザーを使用してサインインする方法については、AWS サインイン 「 ユーザーガイド」の AWS 「 アクセスポータルにサインインする」を参照してください。

追加のユーザーにアクセス権を割り当てる

1. IAM アイデンティティセンターで、最小特権のアクセス許可を適用するというベストプラクティスに従ったアクセス許可セットを作成します。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」を参照してください。
2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「グループの結合」を参照してください。

を使用するための前提条件 AWS Supply Chain

AWS Supply Chain インスタンスを作成する前に、必ず次のステップを完了してください。

- があります AWS アカウント。を作成するには AWS アカウント、「」を参照してくださいAWS アカウントのセットアップ。
- IAM Identity Center が有効になっていることを確認します。IAM アイデンティティセンターを有効にするには、「IAM アイデンティティセンターの有効化」を参照してください。
- 必要な管理権限がある。アクセス許可の詳細については、「詳細設定」を参照してください。
- IAM アイデンティティセンターインスタンスは、 AWS Supply Chain インスタンスを作成するリージョンと同じリージョンでアクティブ化する必要があります。 AWS Supply Chain は、米国東部 (バージニア北部) 、米国西部 (オレゴン) 、欧州 (フランクフルト) 、アジアパシフィック (シドニー) 、欧州 (アイルランド) リージョンでのみサポートされています。

  AWS Supply Chain インスタンスが IAM Identity Center リージョンと同じリージョンにない場合は、お問い合わせください。

- AWS Supply Chain 管理者として割り当てる IAM Identity Center インスタンスには、少なくとも 1 人のユーザーがいる必要があります。アクティブディレクトリを IAM アイデンティティセンターに接続できます。詳細については、「Microsoft AD ディレクトリに接続する」を参照してください。
- IAM AWS Supply Chain Identity Center にアクセスする必要があるユーザーを追加します。
- インスタンスを作成するには AWS Key Management Service 、 (AWS KMS) が必要です。 は AWS KMS key 、これ AWS Supply Chain を使用して、入ってくるすべてのデータを暗号化します AWS Supply Chain。 AWS KMS キーの詳細については、「キーの作成」を参照してください。

の開始方法 AWS Supply Chain

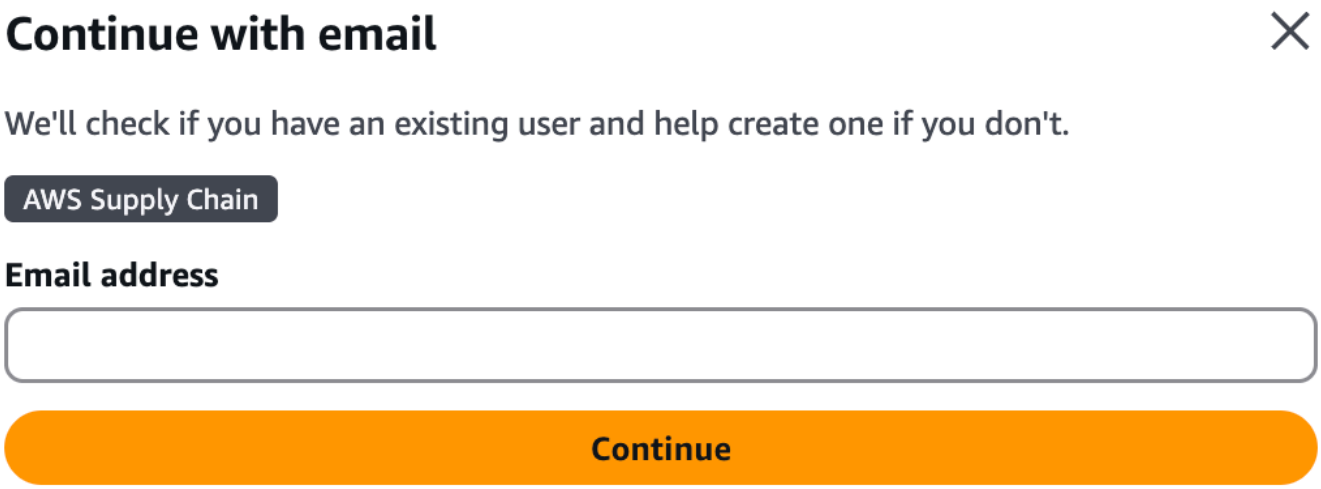
このセクションでは、 AWS Supply Chain インスタンスの作成、ユーザーアクセス許可ロールの付与、 AWS Supply Chain ウェブアプリケーションへのログイン、カスタムユーザーアクセス許可ロールの作成について説明します。は、アクティブまたは初期化状態の AWS Supply Chain インスタンスを最大 10 個持つ AWS アカウント ことができます。

トピック

ステップ 1: IAM Identity Center ユーザープロファイルを割り当てる

インスタンスを作成して AWS Supply Chain サービスを使用するには、既存の IAM Identity Center ユーザープロファイルを接続するか、新しいプロファイルを作成する必要があります。

1. AWS Supply Chain コンソールを開きます。メインからAWS Supply Chain「」を検索することもできます AWS Management Console。
2. 必要に応じて、コンソールの上部にあるAWS リージョンの選択を選択して、リージョンを変更します。ドロップダウンリストからリージョンを選択します。
3. AWS Supply Chain インスタンスの作成 を選択します。通知が表示されます。



4. E メールアドレスを入力し、続行を選択します。IdC は、E メールが既存のユーザーと一致するかどうかを確認します。
5. 次のいずれかを行います：

   - IdC が E メールアドレスをユーザーに一致させる場合 – ID ソースを接続してチームをオンボーディングを選択します。

     > **Note**
     >
     > これは、組織で使用する IdC インスタンスが確立している場合に使用できます AWS Supply Chain。

   - IdC が既存のユーザーとの一致を見つけられない場合 – 新しいユーザーの作成通知が表示されます。次のステップに進みます。
6. 通知で、次のように入力し、続行を選択します。

   - E メールアドレス
   - 名
   - 姓

   IdC はユーザーを自動的に作成し、 AWS Supply Chain 管理者として追加します。
7. 次のいずれかを行います：

   - 標準設定を使用してインスタンスを作成するには – 作成を選択します。「the section called “標準設定を使用する”」を参照してください。

- カスタム設定を使用してインスタンスを作成するには – 詳細設定で編集を選択します。「the section called “詳細設定を使用する”」を参照してください。

ステップ 2: インスタンスを作成する

でインスタンスを作成すると、サプライチェーンの管理と分析専用の環境 AWS Supply Chain が確立されます。インスタンスを設定するには、基本的な詳細を設定し、設定を確立し、初期ユーザーアクセス許可を定義します。

> **Note**
>
> インスタンスを作成できるのは AWS Management Console 管理者のみです。 AWS Supply Chain インスタンスを作成する AWS Management Console 管理者には、 にリストされているすべてのアクセス許可が必要ですの使用 AWS Supply Chain。この管理者は、 を管理する AWS Supply Chain 管理者として IAM ユーザーを招待する必要があります AWS Supply Chain。

インスタンスは、標準設定または詳細設定の 2 つの方法のいずれかを使用して作成します。標準設定では、プリセットパラメータを使用してインスタンスをすばやく作成する自動プロセスを使用します。詳細設定では、独自のパラメータを設定してインスタンスをカスタマイズできます。

トピック

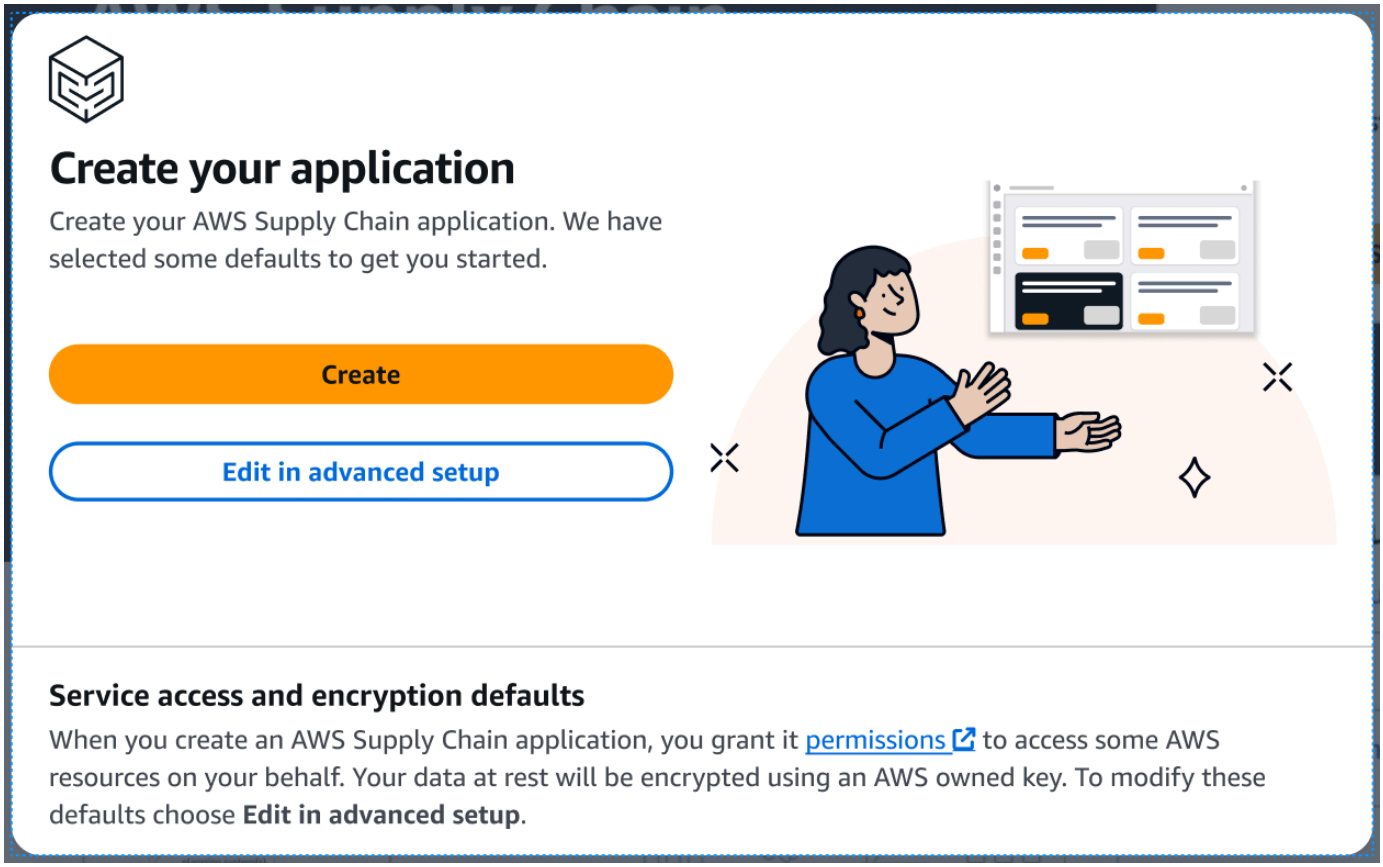
- 標準設定を使用する
- 詳細設定を使用する

標準設定を使用する

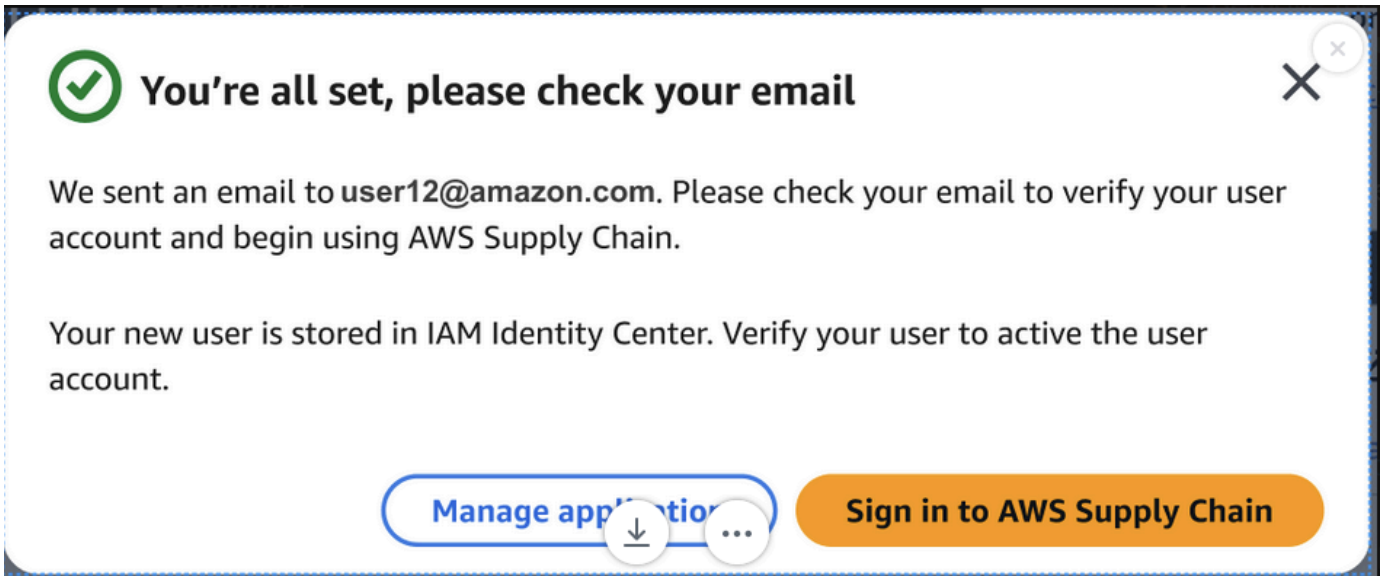
標準設定では、デフォルトのセキュリティおよび暗号化設定を使用して AWS Supply Chain インスタンスが作成されます。インスタンスは AWS 地理的リージョンで動作します。リージョンの詳細については、「IAM ユーザーガイド」の「リージョンとエンドポイント」および「」の「リージョンエンドポイント」を参照してくださいAWS 全般のリファレンス。

プリセットパラメータの標準設定を使用して AWS Supply Chain インスタンスを作成するには、次の手順に従います。

1. [作成] を選択します。

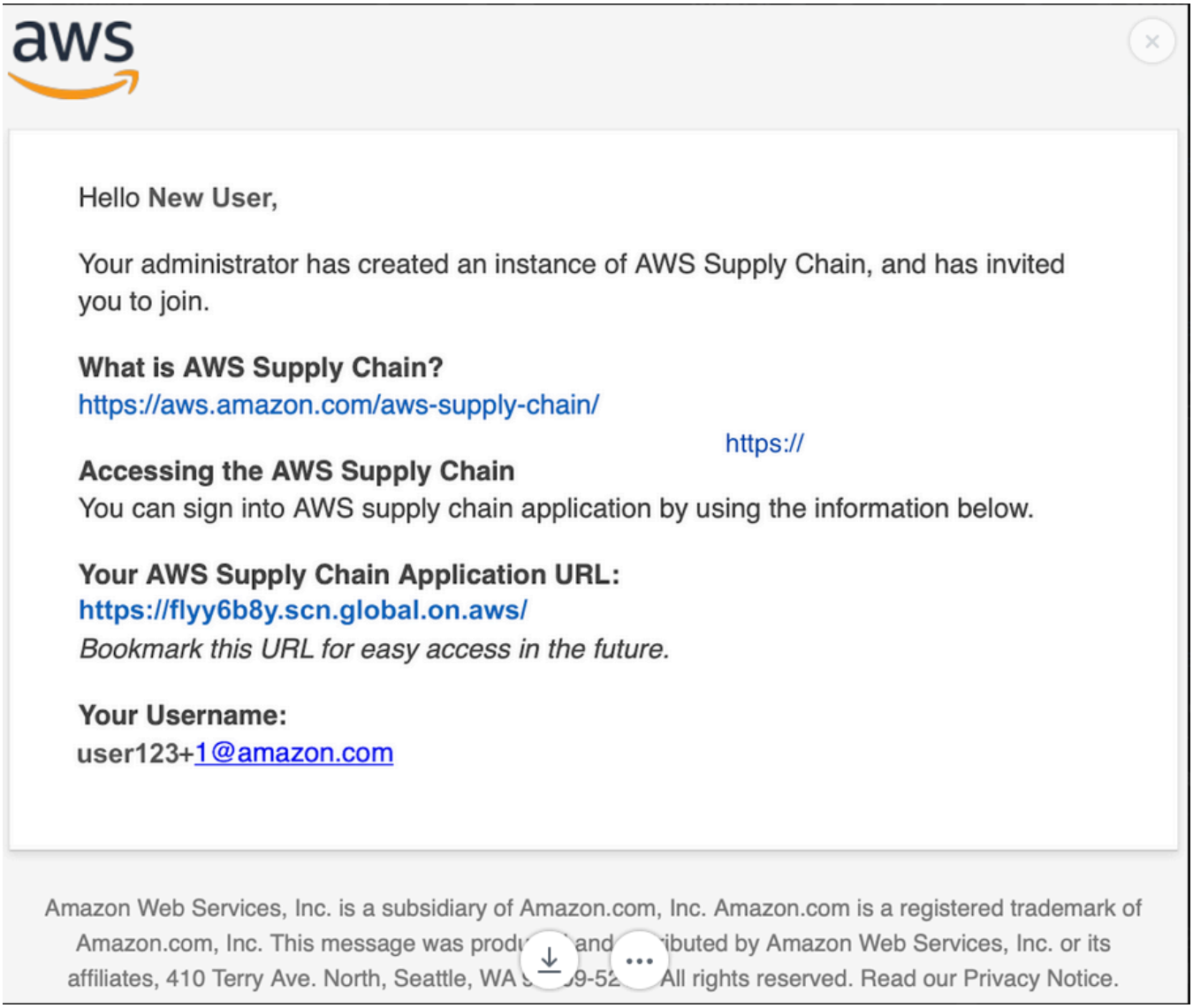


確認が表示されます。



2. E メールで以下を確認します。

   - IdC チームからの E メール。
   - ID 管理チームからの E メール。

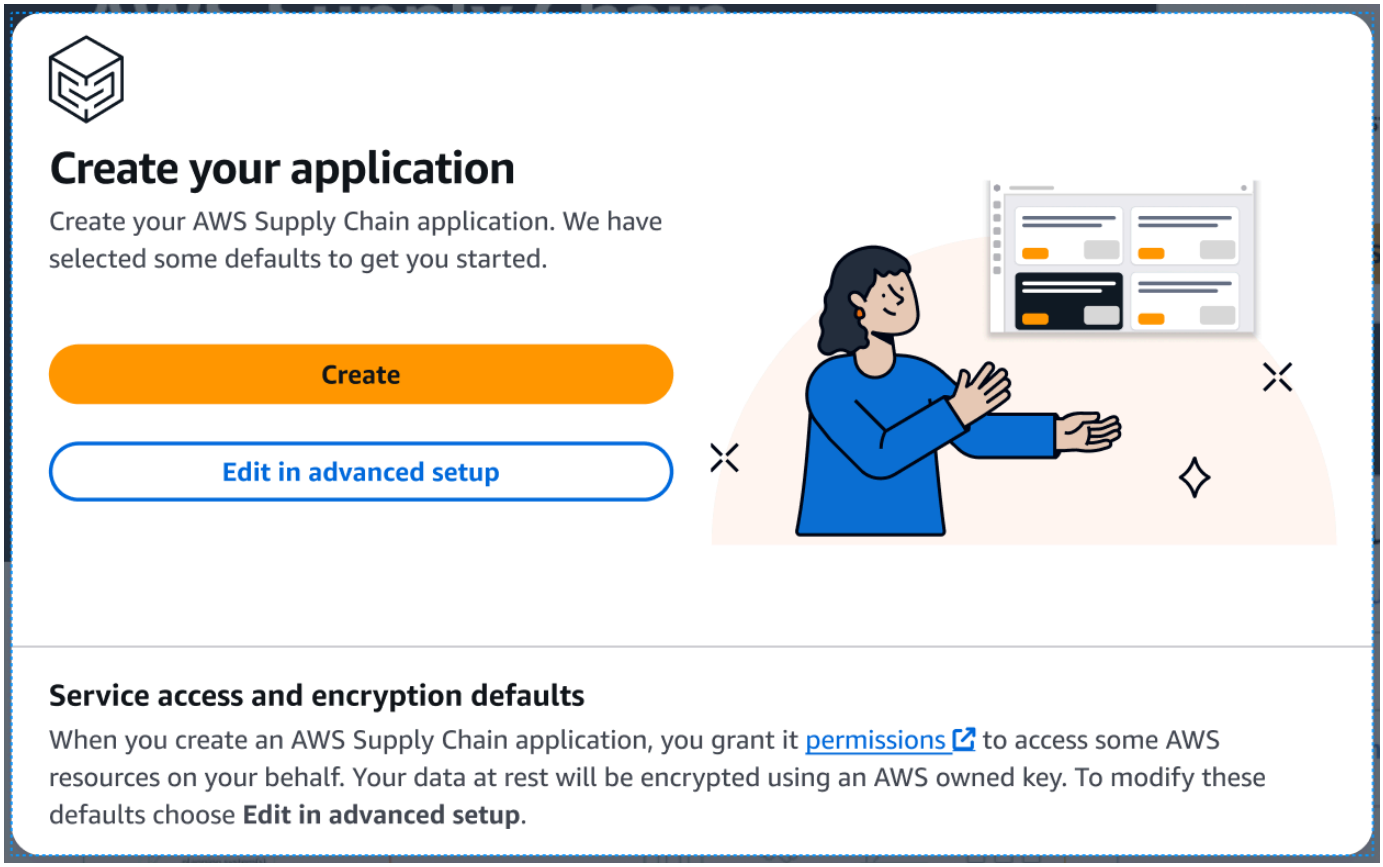


3. 招待メールを受け取ったら、 にログオンします AWS Supply Chain。the section called “AWS Supply Chain ウェブアプリケーションにログオンする”「」を参照してください。

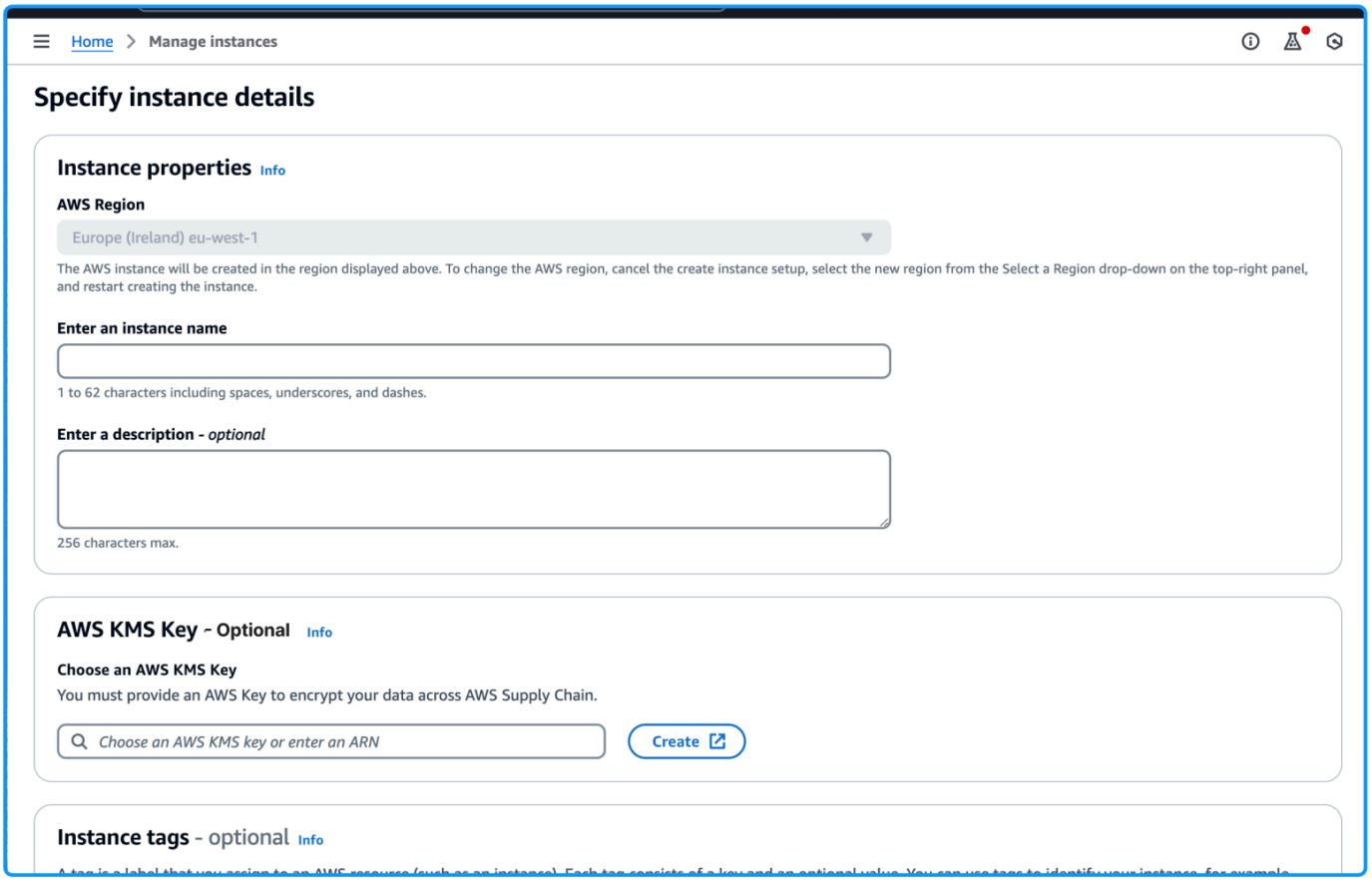
詳細設定を使用する

詳細設定では、独自のパラメータを設定してインスタンスをカスタマイズできます。プリセットパラメータの高度な設定を使用して AWS Supply Chain インスタンスを作成するには、次の手順に従います。

1. 詳細設定で編集を選択します。



インスタンスのプロパティページが表示されます。



2. インスタンスプロパティページで以下を入力します。

   - 名前 – インスタンス名を入力します。
   - 説明 – AWS Supply Chain インスタンスの説明 (本番稼働用インスタンス、テストインスタンスなど) を入力します。
   - AWS KMS キー (オプション) – デフォルトの AWS KMS キーを使用するか (推奨)、独自の AWS KMS キーを指定できます。詳細については「the section called “カスタム AWS KMS キーの使用”」を参照してください。
   - インスタンスタグ – 識別に使用できるタグをインスタンスに追加できます。たとえば、タグを追加して、作成するインスタンスのタイプ (本番稼働、テスト、UAT など) を定義できます。

   > **Note**
   >
   > S/4 Hana データ接続を使用する予定の場合は、指定した AWS KMS キーに の値に関連付けられた `aws-supply-chain-access` タグがあることを確認してください`true`。

3. インスタンスの作成 を選択します。
4. （オプション) AWS Supply Chain インスタンスが作成され、 AWS KMS キーで独自のAWS KMS キーを使用することを選択した場合は、KMS ポリシーを更新して AWS Supply Chain が AWS KMS キーにアクセスできるようにします。

> **Note**
>
> *YourAccountNumber* と *YourInstanceID* を AWS アカウント と AWS Supply Chain インスタンス ID に置き換えます。

```
 {

    "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": "*"
}
```

カスタム AWS KMS キーの使用

インスタンスの作成時に独自の AWS KMS キーを使用できます。独自のキーを管理するが、既存のキーを使用しない場合は、新しいキーを作成できます。

> **Note**
>
> AWS Supply Chain インスタンスでは、 AWS 所有キーの使用がデフォルト設定として推奨されます。

既存の AWS KMS キーの使用

1. 暗号化設定をカスタマイズを選択します。
2. AWS KMS 「キーの選択」に移動します。
3. 指定されたフィールドにキーを入力します。
4. [更新] を選択します。

AWS KMS キーの作成

1. [作成] を選択します。
2. 「KMS キーの作成」のステップに従います。
3. 次のアクセス許可で新しいキーを更新します。

   - 主要な管理アクセス許可を定義する: オフのままにする
   - キーの使用許可を定義する: チェックしないままにする
   - キーポリシーの更新: キーポリシーを編集し、 を以下に置き換えます。

```
{

    "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",
```

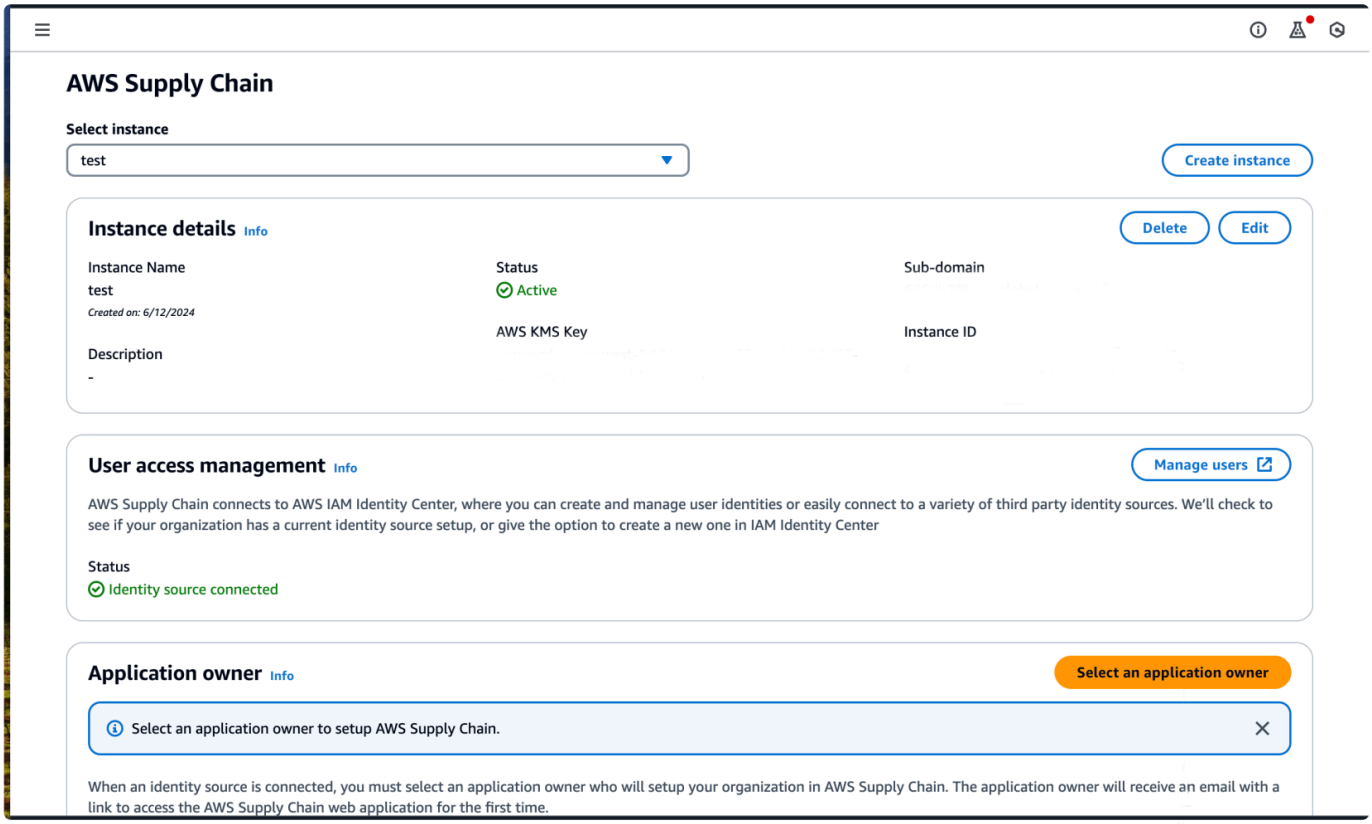
```
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:CreateGrant",
                "kms:DescribeKey",
                "kms:GenerateDataKeyWithoutPlaintext",
                "kms:ReEncryptFrom",
                "kms:ReEncryptTo"
            ],
            "Resource": "*",
            "Condition":  {
                "StringEquals":  {
                    "kms:ViaService": "secretsmanager.Region.amazonaws.com",
                    "kms:CallerAccount": "YourAccountNumber"
                }
            }
        },
        {
            "Sid": "Allow AWS Supply Chain to access the AWS KMS Key",
            "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":"*"
        }
    ]
}
```

ステップ 3: AWS Supply Chain アプリケーション所有者を選択する

AWS コンソール管理者は、 AWS Supply Chain ウェブアプリケーションへのアクセスを管理するアプリケーション所有者を選択します AWS Supply Chain 。 AWS Supply Chain アプリケーションオーナーは、 AWS Supply Chain ウェブアプリケーションにユーザーアクセス許可ロールを追加したり削除したりできます。

インスタンスが作成され、ID ソースが接続されたら、以下の手順に従って AWS Supply Chain アプリケーション所有者を選択します。

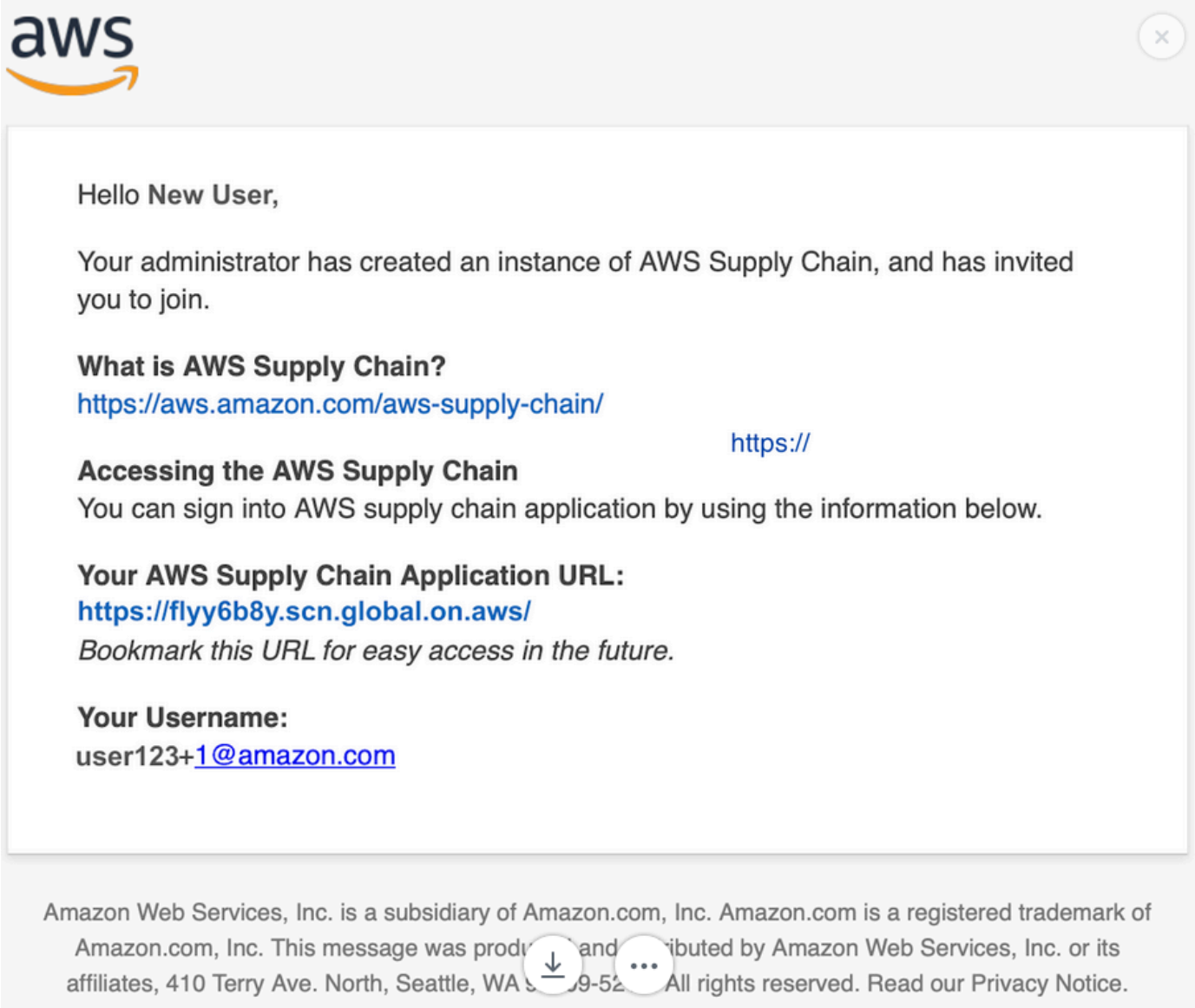
1. AWS Supply Chain コンソールダッシュボードを開きます。
2. 「アプリケーション所有者の選択」に移動し、 AWS Supply Chain アプリケーション所有者になるユーザーを選択します。検索結果には、検索条件に一致するユーザーのみが表示されます。



3. （オプション) IAM Identity Center に移動 を選択して、ユーザーを追加します。ユーザーの追加の詳細については、「AWS IAM Identity Center ユーザーガイド」の「ID ソースの管理」を参照してください。ユーザーアクセス許可ロールの詳細については、「ユーザーアクセス許可ロール」を参照してください。

> **Note**
>
> AWS Supply Chain コンソールから一度に追加できるユーザーは 1 人のみです。 AWS Supply Chainでは、グループをアプリケーションオーナーとして追加することはできません。

4. Send Invite を選択します。ウェブアプリケーション管理者に E メールが送信されます。ウェブアプリケーション管理者が招待 E メールを受信すると、アプリケーション URL を選択して にログインできるようになります AWS Supply Chain。



AWS Supply Chain コンソールダッシュボードには、アプリケーション所有者の下にユーザーが表示されます。

AWS Supply Chain で管理を選択して、 AWS Supply Chain ウェブアプリケーションでユーザーを追加および削除する

AWS Supply Chain ウェブアプリケーションにログオンする

AWS Supply Chain 管理者は、 AWS Supply Chain ウェブアプリケーションへの招待メールを受信しているはずです。

1. メールに記載されているリンクをクリックするか、 AWS Supply Chain コンソールのダッシュボードの [サブドメイン] で [ウェブ URL] をクリックします。

   AWS Supply Chain ウェブアプリケーションのログインページが表示されます。
2. IAM Identity Center AWS のユーザー認証情報を入力し、サインインを選択します。

   > **Note**
   >
   > 初めてログインする場合にのみ、アカウントと組織のプロフィールの入力が求められます。
3. [Complete your profile] ページで、[Job Title] と [タイムゾーン] を入力します。[次へ] を選択します。
4. [Let's add your organization information] ページで、[組織名] を入力して、[Headquarters location] を選択します。必要に応じて、会社のロゴを追加できます。[次へ] を選択します。
5. [Set up your teammates on AWS Supply Chain] ページで、 AWS Supply Chain ウェブアプリケーションにアクセスを付与するユーザーを選択します。[Invite Users] を選択します。 AWS Supply Chain ユーザーアクセス許可ロールの詳細については、「」を参照してください[ユーザーアクセス許可ロールの管理]。
6. ユーザーの追加を後で行う場合は、[Skip for now] をクリックします。

   [Onboarding complete] ページが開きます。
7. 追加した各ユーザーは、 へのリンクを含む E メールメッセージを受信するか AWS Supply Chain、リンクをコピーしてユーザーに送信できます。
8. [Continue to homepage] をクリックして、 AWS Supply Chain ダッシュボードを表示します。

の使用 AWS Supply Chain

AWS Supply Chain は、サプライチェーンネットワークを可視化し、情報に基づいた意思決定を迅速に行い、サプライチェーンの耐障害性を向上させるのに役立つクラウドベースのアプリケーションです。を使用すると AWS Supply Chain、さまざまなデータソースを接続し、機械学習を使用してインサイトを生成し、内部チームや外部パートナーとコラボレーションできます。このセクションでは、いくつかの AWS Supply Chain 基本的な機能について説明します。

トピック

AWS Supply Chain コンソールの使用

コンソールを使用することは、サービスのリソースと設定を管理する最も簡単な方法です。コンソールには、 リソースを表示、作成、変更、モニタリングできる直感的なウェブベースのインターフェイスが用意されています。このセクションでは、 コンソールにアクセスしてナビゲートし、一般的な管理タスクを実行する方法について説明します。

> **Note**
>
> AWS アカウントが AWS 組織のメンバーアカウントであり、サービスコントロールポリシー (SCP) が含まれている場合は、組織の SCP がメンバーアカウントに次のアクセス許可を付与していることを確認してください。次のアクセス許可が組織の SCP ポリシーに含まれていない場合、 AWS Supply Chain インスタンスの作成は失敗します。

AWS Supply Chain コンソールにアクセスするには、最小限のアクセス許可のセットが必要です。これらのアクセス許可により、 内の AWS Supply Chain リソースの詳細を一覧表示および表示できます AWS アカウント。最小限必要な許可よりも制限が厳しいアイデンティティベースのポリシーを作成すると、そのポリシーを持つエンティティ (ユーザーまたはロール) に対してコンソールが意図したとおりに機能しません。

AWS CLI または AWS API のみを呼び出すユーザーには、最小限のコンソールアクセス許可を付与する必要はありません。代わりに、実行しようとしている API オペレーションに一致するアクションのみへのアクセスが許可されます。

コンソール管理者が AWS Supply Chain インスタンスの作成と更新を正常に実行するには、次のアクセス許可が必要です。

```
{
 "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:CreateOrganization",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:EnableAWSServiceAccess",
    "organizations:ListDelegatedAdministrators"
   ],
   "Resource": "*",
   "Effect": "Allow"
```

```
  },
  {
   "Action": [
    "kms:CreateGrant",
    "kms:RetireGrant",
    "kms:DescribeKey"
   ],
   "Resource": key_arn,
   "Effect": "Allow"
  },
  {
   "Action": [
    "kms:ListAliases"
   ],
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": [
    "iam:CreateRole",
    "iam:CreatePolicy",
    "iam:GetRole",
    "iam:PutRolePolicy",
    "iam:AttachRolePolicy",
    "iam:CreateServiceLinkedRole"
   ],
   "Resource": "*",
   "Effect": "Allow"
  },
  {
   "Action": [
    "sso:AssociateDirectory",
    "sso:AssociateProfile",
    "sso:CreateApplication",
    "sso:CreateApplicationAssignment",
    "sso:CreateInstance",
    "sso:CreateManagedApplicationInstance",
    "sso:DeleteApplication",
    "sso:DeleteApplicationAssignment",
    "sso:DeleteManagedApplicationInstance",
    "sso:DescribeApplication",
    "sso:DescribeDirectories",
    "sso:DescribeInstance",
    "sso:DescribeRegisteredRegions",
```

```
    "sso:DescribeTrusts",
    "sso:DisassociateProfile",
    "sso:GetManagedApplicationInstance",
    "sso:GetPeregrineStatus",
    "sso:GetProfile",
    "sso:GetSharedSsoConfiguration",
    "sso:GetSsoConfiguration",
    "sso:GetSSOStatus",
    "sso:ListApplicationAssignments",
    "sso:ListApplicationTemplates",
    "sso:ListDirectoryAssociations",
    "sso:ListInstances",
    "sso:ListProfileAssociations",
    "sso:ListProfiles",
    "sso:PutApplicationAuthenticationMethod",
    "sso:PutApplicationGrant",
    "sso:RegisterRegion",
    "sso:SearchDirectoryGroups",
    "sso:SearchDirectoryUsers",
    "sso:SearchGroups",
    "sso:SearchUsers",
    "sso:StartPeregrine",
    "sso:StartSSO",
    "sso:UpdateSsoConfiguration",
    "sso-directory:SearchUsers"
   ],
   "Resource": "*",
   "Effect": "Allow"
  }
 ]
}
```

key_arn は、 AWS Supply Chain インスタンスに使用するキーを指定します。ベストプラクティスと、使用するキーのみへのアクセスを制限する方法については AWS Supply Chain、「IAM ポリシーステートメントでの KMS キーの指定」を参照してください。すべての KMS キーを表すには、ワイルドカード文字のみ (「*」) を使用します。

プロファイルの更新

アカウントと組織プロファイルは、 AWS Supply Chain ウェブアプリケーションでいつでも更新できます。

アカウントプロファイルの更新

アカウントプロファイルを更新するには、次の手順に従います。

1. AWS Supply Chain ウェブアプリケーションダッシュボードの左側のナビゲーションペインで、設定アイコンを選択します。
2. [アカウントプロファイル] をクリックします。

   [アカウントプロファイル] ページが開きます。
3. アカウントの情報を更新して、[保存] をクリックします。

組織プロファイルの更新

組織プロファイルを更新するには、次の手順に従います。

1. AWS Supply Chain ウェブアプリケーションダッシュボードの左側のナビゲーションペインで、設定アイコンを選択します。
2. [組織] を選択して、[Organization Profile] をクリックします。

   [Organization Profile] ページが開きます。
3. 組織の [ロゴ] や [Headquarters location] を更新して、[保存] をクリックします。

ユーザーアクセス許可ロールの管理

AWS Supply Chain 管理者は、デフォルトのユーザーアクセス許可ロールを使用するか、カスタムアクセス許可ロールを作成できます。 AWS Supply Chain には、次のデフォルトのユーザーアクセス許可ロールがあります。

- 管理者 – すべてのデータとユーザーのアクセスを作成、表示、管理するアクセス許可
- データアナリスト – すべてのデータ接続を作成、表示、管理するアクセス許可
- 在庫マネージャー – Insights を作成、表示、管理するアクセス許可
- Demandプランナー – 予測、オーバーライド、および公開需要計画を作成、表示、管理するためのアクセス許可。
- パートナーデータマネージャー – パートナーの管理と表示、データリクエストの管理と表示、持続可能性データの表示のアクセス許可
- サプライプランナー – 供給計画を管理、表示するアクセス許可

> **Note**
>
> AWS Supply Chain 管理者としてユーザーを追加する前に、次の点に注意してください。
>
> - デフォルトの各ユーザーアクセス許可ロールは、アクセス許可のセットで定義されます。ユーザーをデフォルトのユーザーアクセス許可ロールに追加することも、カスタムアクセス許可ロールを作成することもできます。
> - 各ユーザーに割り当てることができるのは、単一のユーザーアクセス許可ロールのみです。
> - デフォルトのユーザーアクセス許可ロールを編集または削除することはできません。
> - 作成したカスタムアクセス許可ロールを編集すると、そのカスタムアクセス許可ロールに属するすべてのユーザーのアクセス許可が更新されます。
> - 作成したカスタムアクセス許可ロールを削除すると、カスタムアクセス許可ロールのすべてのユーザーがアクセスできなくなります AWS Supply Chain。
> - グループの追加は ではサポートされていません AWS Supply Chain。

トピック

ユーザーの追加

AWS Supply Chain 管理者は、 AWS Supply Chain ウェブアプリケーションにアクセスするためのユーザーを追加できます。ユーザーは、まず IAM Identity Center (IdC) に追加され、次に追加できます AWS Supply Chain。IdC へのユーザーの追加の詳細については、「ユーザーアクセスの割り当て」を参照してください。

ユーザーを IdC に追加したら、以下の手順に従って ユーザーを追加します。

1. AWS Supply Chain ダッシュボードの設定アイコンを選択します。
2. ユーザーとアクセス許可を選択します。
3. ユーザー、 ユーザーを選択します。[ユーザーを管理] ページが開きます。

4. 新しいユーザーの追加を選択します。[Add User] ページが開きます。
5. ユーザーの追加 (複数可) ドロップダウンメニューからユーザーを選択します。
6. 「ロールの選択」ドロップダウンメニューからユーザーのロールを選択します。
7. [追加] を選択します。

ユーザーアクセス許可の更新

現在のユーザーの AWS Supply Chain ユーザーアクセス許可ロールを更新するには、次の手順に従います。

1. AWS Supply Chain ダッシュボードの左側のナビゲーションペインで、設定アイコンを選択します。
2. [アクセス許可]、[ユーザー] の順に選択します。

   [ユーザーを管理] ページが開きます。
3. ユーザー管理ページで、ユーザーアクセス許可ロールを更新するユーザーまたはグループを選択し、アクセス許可ロールドロップダウンメニューからアクセス許可ロールのいずれかを選択します。

   > **Note**
   >
   > AWS Supply Chain ダッシュボードは、割り当てたロールアクセス許可に応じてカスタマイズされます。詳細については、「カスタムユーザーアクセス許可ロールの作成」を参照してください。
4. [Save] を選択します。

ユーザーの削除

AWS Supply Chain 管理者は、 AWS Supply Chain ウェブアプリケーションからユーザーを削除できます。ユーザーは、次の手順で削除できます。

1. AWS Supply Chain ダッシュボードの左側のナビゲーションペインで、設定アイコンを選択します。
2. [アクセス許可]、[ユーザー] の順に選択します。

   [ユーザーを管理] ページが開きます。

3. [ユーザーを管理] ページで削除するユーザーを選択して、[削除] アイコンをクリックします。

カスタムユーザーアクセス許可ロールの作成

デフォルトのユーザーアクセス許可ロールに加え、カスタムユーザーアクセス許可ロールを作成して、複数のアクセス許可ロールを含めたり、特定のロケーションや製品を追加したりできます。新しいアクセス許可ロールは、次の手順で作成できます。

1. AWS Supply Chain ダッシュボードの左側のナビゲーションペインで、設定アイコンを選択します。[アクセス許可]、[アクセス許可ロール] の順に選択します。

   [アクセス許可ロール] ページが開きます。
2. [Create New Role (新しいロールを作成)] を選択します。
3. [アクセス許可を管理する] ページの [ロール名] に名前を入力します。
4. スライダーを動かしてユーザーアクセス許可ロールを選択します。

   - 管理 – ユーザーに管理アクセス許可を割り当てると、情報を追加、編集、管理できます。
   - 表示 – ユーザーに表示アクセス許可を割り当てると、現在の情報のみを表示できます。
5.

   > **Note**
   >
   > インスタンスがデータソースに接続している場合、[Location Access] と [Product Access] の下で製品とロケーションのみが選択できます。例えば、シアトルのロケーションでアボカドのみを管理するカスタム管理者ユーザーを作成したり、シアトルのロケーションでアボカドのインサイトを管理するのみのインサイトユーザーを作成したりできます。

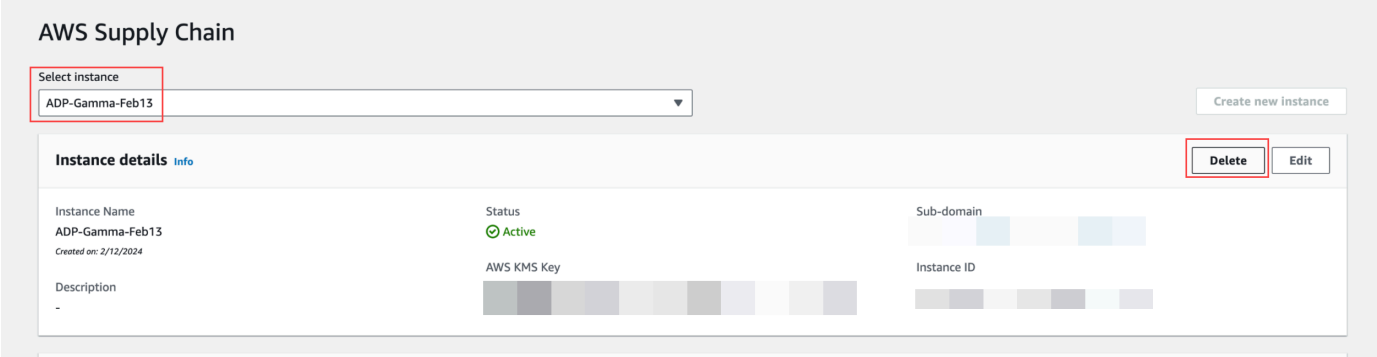
   [Location Access] の下で、検索バーにリージョンを入力して検索し、選択します。
6. [Product Access] の下で、検索バーに製品を入力して検索し、選択します。
7. [Save] を選択します。

インスタンスの削除

インスタンスを削除するには、次の手順に従います。

> **Note**
>
> インスタンスを削除しても、Amazon S3 バケットの情報は自動的に削除されません。

1. で AWS Supply Chain コンソールを開きますhttps://console.aws.amazon.com/scn/home。
2. AWS Supply Chain コンソールダッシュボードのドロップダウンから、削除するインスタンスを選択します。



3. [削除] を選択します。
4. AWS Supply Chain 「インスタンスの削除」ページの「確認」に「」と入力**delete**して、インスタンスを削除することを確認します。
5. [削除] を選択します。インスタンスの削除が開始され、インスタンスが削除されると、確認メッセージが表示されます。

> **Note**
>
> インスタンスが削除されると、 の Amazon Q に関連する情報 AWS Supply Chain が自動的に削除されます。

のセキュリティ AWS Supply Chain

でのクラウドセキュリティが最優先事項 AWS です。 AWS のお客様は、セキュリティを最も重視する組織の要件を満たすように AWS 構築されたデータセンターとネットワークアーキテクチャからメリットを得られます。

セキュリティは、 AWSとお客様の間で共有される責任です。責任共有モデルでは、これをクラウドのセキュリティおよびクラウド内のセキュリティと説明しています。

- クラウドのセキュリティ – AWS は、 AWS のサービス で実行されるインフラストラクチャを保護する責任があります AWS クラウド。 AWS また、 は、お客様が安全に使用できるサービスも提供します。サードパーティーの監査人は、AWS コンプライアンスプログラム の一環として、セキュリティの有効性を定期的にテストおよび検証します。が適用されるコンプライアンスプログラムの詳細については AWS Supply Chain、「コンプライアンスプログラムAWS による対象範囲内のサービスコンプライアンスプログラム」を参照してください。
- クラウド内のセキュリティ – 使用する によって、お客様の責任 AWS のサービス が決まります。またお客様は、お客様のデータの機密性、組織の要件、適用される法令や規制などのその他の要素についても責任を負います。

このドキュメントは、 AWS Supply Chainの使用時における責任共有モデルの適用方法を理解するために役立ちます。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成する AWS Supply Chain ように を設定する方法について説明します。また、 AWS Supply Chain リソースのモニタリングや保護 AWS のサービス に役立つ他の の使用方法についても説明します。

トピック

- でのデータ保護 AWS Supply Chain
- インターフェイスエンドポイント (AWS PrivateLink) AWS Supply Chain を使用した へのアクセス
- の IAM AWS Supply Chain
- AWS の マネージドポリシー AWS Supply Chain
- のコンプライアンス検証 AWS Supply Chain
- の耐障害性 AWS Supply Chain
- ログ記録とモニタリング AWS Supply Chain
- を使用した AWS Supply Chain イベントの管理 Amazon EventBridge

でのデータ保護 AWS Supply Chain

責任 AWS 共有モデル、 でのデータ保護に適用されます AWS Supply Chain。このモデルで説明されているように、 AWS はすべての を実行するグローバルインフラストラクチャを保護する責任があります AWS クラウド。ユーザーは、このインフラストラクチャでホストされるコンテンツに対する管理を維持する責任があります。また、使用する「 AWS のサービス 」のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、データプライバシーに関するよくある質問を参照してください。欧州でのデータ保護の詳細については、AWS セキュリティブログに投稿された AWS 責任共有モデルおよび GDPR のブログ記事を参照してください。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用して AWS リソースと通信します。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」のCloudTrail 証跡の使用」を参照してください。
- AWS 暗号化ソリューションと、その中のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度な管理されたセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-3 検証済み暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報を、タグ、または [名前] フィールドなどの自由形式のテキストフィールドに含めないことを強くお勧めします。これは、コンソール AWS Supply Chain 、API、または SDK を使用して AWS CLIまたは他の AWS のサービス を使用する場合も同様です。 AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

AWS Supply Chainによって処理されるデータ

特定の AWS Supply Chain インスタンスの承認されたユーザーがアクセスできるデータを制限するため、 AWS Supply Chain 内に保持されているデータは、 AWS アカウント ID と AWS Supply Chain インスタンス ID によって分離されます。

AWS Supply Chain は、ユーザー情報、データコネクタから抽出された情報、インベントリの詳細など、さまざまなサプライチェーンデータを処理します。

オプトアウト設定

AWS サービス条件に記載されているように AWS Supply Chain、AWS は、 によって処理されたお客様のコンテンツを使用および保存することがあります。からオプトアウトしてコンテンツ AWS Supply Chain を使用または保存する場合は、AWS Organizations でオプトアウトポリシーを作成できます。オプトアウトポリシーの作成の詳細については、「AI サービスのオプトアウトポリシーの構文と例」を参照してください。

保管中の暗号化

PII として分類された問い合わせデータ、または によって保存 AWS Supply Chain されている の Amazon Q で使用されるコンテンツを含む顧客コンテンツを表すデータは AWS Supply Chain、保管時 (つまり、ディスクに格納、保存される前) に、 AWS Supply Chain インスタンスに固有の制限されたキーで暗号化されます。

お客様のアカウントごとに固有の AWS Key Management Service データキーを使用した Amazon S3 サーバー側の暗号化は、すべてのコンソールとウェブアプリケーションのデータを暗号化するために使用されます。の詳細については AWS KMS keys、「 AWS Key Management Service デベロッパーガイド」の「 とは AWS Key Management Service」を参照してください。

> **Note**
>
> AWS Supply Chain 機能 Supply Planning と N-Tier Visibility は、提供された KMS-CMK data-at-rest暗号化をサポートしていません。

転送中の暗号化

AWS Supply Chain と AWS Supply Chain 引き換えに Amazon Q で使用されるコンテンツを含むデータは、業界標準の TLS 暗号化を使用して、ユーザーのウェブブラウザと AWS Supply Chain 間で転送される際に保護されます。

キー管理

AWS Supply Chain は KMS-CMK を部分的にサポートしています。

での AWS KMS キーの更新については AWS Supply Chain、「」を参照してくださいステップ 2: インスタンスを作成する。

ネットワーク間トラフィックのプライバシー

> **Note**
>
> AWS Supply Chain は PrivateLink をサポートしていません。

の Virtual Private Cloud (VPC) エンドポイント AWS Supply Chain は、VPC 内の論理エンティティで、接続のみを許可します AWS Supply Chain。VPC はリクエストを にルーティング AWS Supply Chain し、レスポンスを VPC にルーティングします。詳細については、VPC ユーザーガイドの VPC エンドポイントを参照してください。

が で許可 AWS Supply Chain を使用する方法 AWS KMS

AWS Supply Chain では、カスタマーマネージドキーを使用するにはグラントが必要です。

AWS Supply Chain は、CreateInstance オペレーション中に渡された AWS KMS キーを使用して複数の許可を作成します。 は、CreateGrantリクエストを送信することで、ユーザーに代わって許可 AWS Supply Chain を作成します AWS KMS。の許可 AWS KMS は、顧客アカウントの AWS KMS キー AWS Supply Chain へのアクセスを許可するために使用されます。

> **Note**
>
> AWS Supply Chain は、独自の認可メカニズムを使用します。ユーザーを追加すると AWS Supply Chain、 AWS KMS ポリシーを使用して同じユーザーを拒否することはできません。

AWS Supply Chain は、次の目的でグラントを使用します。

- GenerateDataKey リスエストを AWS KMS に送信して、インスタンスに保管されたデータを 暗号化 する。
- インスタンスに関連付けられた暗号化されたデータを読み取る AWS KMS ために Decrypt リクエストを に送信するには。
- Amazon Forecast などの他の AWS サービスに送信する際にデータを保護するため、DescribeKey、CreateGrant、RetireGrant のアクセス許可を追加するには。

グラントへのアクセスの取り消しや、カスタマーマネージドキーに対するサービスのアクセスの取り消しは、いつでもできます。これを行う AWS Supply Chain と、カスタマーマネージドキーによって暗号化されたデータにアクセスできなくなり、そのデータに依存するオペレーションに影響します。

の暗号化のモニタリング AWS Supply Chain

次の例はEncrypt、カスタマーマネージドキーで暗号化されたデータにアクセスDecryptするために によって呼び出される KMS オペレーションをモニタリング AWS Supply Chain するための GenerateDataKey、、 の AWS CloudTrail イベントです。

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"
}
```

インターフェイスエンドポイント (AWS PrivateLink) AWS Supply Chain を使用した へのアクセス

を使用して AWS PrivateLink 、VPC と の間にプライベート接続を作成できます AWS Supply Chain。インターネットゲートウェイ、NAT デバイス、VPN 接続、または AWS Direct Connect 接続を使用せずに、VPC 内にある AWS Supply Chain かのように にアクセスできます。VPC内のインスタンスは AWS Supply ChainにアクセスするためにパブリックIPアドレスを必要としません。

このプライベート接続を確立するには、 AWS PrivateLinkを利用したインターフェイスエンドポイントを作成します。インターフェイスエンドポイントに対して有効にする各サブネットにエンドポイントネットワークインターフェイスを作成します。これらは、 AWS Supply Chain宛てのトラフィックのエントリポイントとして機能するリクエスタ管理型ネットワークインターフェイスです。

詳細については、「 AWS PrivateLink ガイド」の「Access AWS のサービス through AWS PrivateLink 」を参照してください。

に関する考慮事項 AWS Supply Chain

のインターフェイスエンドポイントを設定する前に AWS Supply Chain、「 AWS PrivateLink ガイド」の「考慮事項」を参照してください。

AWS Supply Chain は、インターフェイスエンドポイントを介したすべての API アクションの呼び出しをサポートしています。

のインターフェイスエンドポイントを作成する AWS Supply Chain

Amazon VPC コンソールまたは AWS Command Line Interface () AWS Supply Chain を使用して、のインターフェイスエンドポイントを作成できますAWS CLI。詳細については、「AWS PrivateLink ガイド」の「インターフェイスエンドポイントを作成」を参照してください。

次のサービス名 AWS Supply Chain を使用して、 のインターフェイスエンドポイントを作成します。

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

インターフェース· エンドポイントのプライベートDNSを有効にすると、デフォルトの地域DNS名を使用して AWS Supply Chain へのAPI要求を行うことができます。例えば、*scn*.*region*.amazonaws.com と指定します。

インターフェイスエンドポイントのエンドポイントポリシーを作成する

エンドポイントポリシーは、インターフェイスエンドポイントにアタッチできる IAM リソースです。デフォルトのエンドポイントポリシーでは、インターフェイスエンドポイント AWS Supply Chain を介した へのフルアクセスが許可されます。VPC AWS Supply Chain から に許可されるアクセスを制御するには、カスタムエンドポイントポリシーをインターフェイスエンドポイントにアタッチします。

エンドポイントポリシーは以下の情報を指定します。

- アクションを実行できるプリンシパル (AWS アカウント、IAM ユーザー、IAM ロール)
- 実行可能なアクション
- このアクションを実行できるリソース

詳細については[AWS PrivateLink Guide] (ガイド) の[Control access to services using endpoint policies] (エンドポイントポリシーを使用してサービスへのアクセスをコントロール) を参照してください。

例: AWS Supply Chain アクションの VPC エンドポイントポリシー

以下は、カスタムエンドポイントポリシーの例です。インターフェイスエンドポイントにアタッチされると、このポリシーは、すべてのリソースですべてのプリンシパルに、リストされている AWS Supply Chain アクションへのアクセス権を付与します。

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

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

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

の IAM AWS Supply Chain

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。IAM 管理者は、誰を認証 (サインイン) し、誰に AWS Supply Chain リソースの使用を承認する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで AWS のサービス 使用できる です。

トピック

- 対象者
- アイデンティティを使用した認証
- ポリシーを使用したアクセスの管理
- と IAM の AWS Supply Chain 連携方法
- AWS Supply Chainのアイデンティティベースのポリシーの例
- AWS Supply Chain ID とアクセスのトラブルシューティング

対象者

AWS Identity and Access Management (IAM) の使用方法は、作業内容によって異なります AWS Supply Chain。

サービスユーザー – AWS Supply Chain サービスを使用してジョブを実行する場合、管理者から必要な認証情報とアクセス許可が与えられます。さらに多くの AWS Supply Chain 機能を使用して作業を行う場合は、追加のアクセス許可が必要になることがあります。アクセスの管理方法を理解すると、管理者から適切な権限をリクエストするのに役に立ちます。 AWS Supply Chain機能にアクセスできない場合は、「AWS Supply Chain ID とアクセスのトラブルシューティング」を参照してください。

サービス管理者 – 社内の AWS Supply Chain リソースを担当している場合は、通常、 へのフルアクセスがあります AWS Supply Chain。サービスユーザーがどの AWS Supply Chain 機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。会社で IAM を で使用する方法の詳細については AWS Supply Chain、「」を参照してくださいと IAM の AWS Supply Chain 連携方法。

IAM 管理者 - 管理者は、 AWS Supply Chainへのアクセスを管理するポリシーの書き込み方法の詳細について確認する場合があります。IAM で使用できる AWS Supply Chain アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS Supply Chainのアイデンティティベースのポリシーの例。

アイデンティティを使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。として、IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けて認証 (サインイン AWS) される必要があります。

ID ソースを介して提供された認証情報を使用して、フェデレーティッド ID AWS として にサインインできます。 AWS IAM Identity Center （ IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google または Facebook 認証情報は、フェデレーティッド ID の例です。フェデレーティッド ID としてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーションを使用して にアクセスすると、間接的 AWS にロールを引き受けます。

ユーザーのタイプに応じて、 AWS Management Console または AWS アクセスポータルにサインインできます。へのサインインの詳細については AWS、「 AWS サインイン ユーザーガイド」の「 にサインインする方法 AWS アカウント」を参照してください。

AWS プログラムで にアクセスする場合、 は Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) AWS を提供し、認証情報を使用してリクエストに暗号で署名します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。リクエストに自分で署名する推奨方法の使用については、「IAM ユーザーガイド」の「API リクエストに対するAWS Signature Version 4」を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、 AWS では、多要素認証 (MFA) を使用してアカウントのセキュリティを強化することをお勧めします。詳細については、「AWS IAM Identity Center ユーザーガイド」の「多要素認証」および「IAM ユーザーガイド」の「IAM のAWS 多要素認証」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、アカウント内のすべての およびリソースへの AWS のサービス 完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。この ID は AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることでアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「IAM ユーザーガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーティッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、一時的な認証情報 AWS のサービス を使用して にアクセスするために ID プロバイダーとのフェデレーションを使用することを要求します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、、AWS Directory Serviceアイデンティティセンターディレクトリのユーザー、または ID ソースを通じて提供された認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーティッド ID が にアクセスすると AWS アカウント、ロールを引き受け、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成することも、独自の ID ソース内のユーザーとグループのセットに接続して同期し、すべての AWS アカウント とアプリケーションで使用することもできます。IAM Identity Center の詳細については、「AWS IAM Identity Center ユーザーガイド」の「What is IAM Identity Center?」(IAM Identity Center とは) を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、単一のユーザーまたはアプリケーションに特定のアクセス許可 AWS アカウントを持つ 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「IAM ユーザーガイド」の「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する許可を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可 AWS アカウント を持つ 内のアイデンティティです。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。で IAM ロールを一時的に引き受けるには AWS Management Console、ユーザーから IAM ロール (コンソール) に切り替えることができます。ロールを引き受けるには、 または AWS API オペレーションを AWS CLI 呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID はロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールについては、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity

Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center User Guide」の「Permission sets」を参照してください。

- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の では AWS のサービス、(ロールをプロキシとして使用する代わりに) リソースに直接ポリシーをアタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。
- クロスサービスアクセス — 一部の では、他の の機能 AWS のサービス を使用します AWS のサービス。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用してアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可と AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストリクエストを組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除することができます。詳細については、「IAM ユーザーガイド」の「AWS のサービスに許可を委任するロールを作成する」を参照してください。
  - サービスにリンクされたロール – サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、 サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。

- Amazon EC2 で実行されているアプリケーション – IAM ロールを使用して、EC2 インスタンスで実行され、 AWS CLI または AWS API リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。 AWS ロールを EC2 インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、「IAM ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与する」を参照してください。

ポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、ID AWS またはリソースにアタッチします。ポリシーは のオブジェクト AWS であり、アイデンティティまたはリソースに関連付けられると、そのアクセス許可を定義します。 は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うときに、これらのポリシー AWS を評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、IAM ユーザーガイドの JSON ポリシー概要を参照してください。

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの許可を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。そのポリシーを持つユーザーは、 AWS Management Console、、 AWS CLIまたは AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、 内の複数のユーザー、グループ、ロールにアタッチできるスタンドアロンポリシーです AWS アカウント。管理ポリシーには、 AWS 管理ポリシーとカスタマー管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「管理ポリシーとインラインポリシーのいずれかを選択する」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、 AWS WAF、および Amazon VPC は、ACLs。ACL の詳細については、「Amazon Simple Storage Service デベロッパーガイド」の「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS は、一般的ではない追加のポリシータイプをサポートしています。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エ

ンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。Principal フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。

- サービスコントロールポリシー (SCPs) – SCPsは、 の組織または組織単位 (OU) の最大アクセス許可を指定する JSON ポリシーです AWS Organizations。 AWS Organizations は、ビジネスが所有する複数の AWS アカウント をグループ化して一元管理するためのサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP は、各 を含むメンバーアカウントのエンティティのアクセス許可を制限します AWS アカウントのルートユーザー。Organizations と SCP の詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー (SCP)」を参照してください。
- リソースコントロールポリシー (RCP) – RCP は、所有する各リソースにアタッチされた IAM ポリシーを更新することなく、アカウント内のリソースに利用可能な最大数のアクセス許可を設定するために使用できる JSON ポリシーです。RCP は、メンバーアカウントのリソースのアクセス許可を制限し、組織に属しているかどうかにかかわらず AWS アカウントのルートユーザー、 を含む ID の有効なアクセス許可に影響を与える可能性があります。RCP をサポートする のリストを含む Organizations と RCP の詳細については、AWS Organizations RCPs「リソースコントロールポリシー (RCPs」を参照してください。 AWS のサービス
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。複数のポリシータイプが関係する場合に がリクエストを許可するかどうか AWS を決定する方法については、「IAM ユーザーガイド」の「ポリシー評価ロジック」を参照してください。

と IAM の AWS Supply Chain 連携方法

IAM を使用して へのアクセスを管理する前に AWS Supply Chain、 で使用できる IAM 機能について学びます AWS Supply Chain。

で使用できる IAM の機能 AWS Supply Chain

IAM 機能	AWS Supply Chain サポート
アイデンティティベースポリシー	はい
リソースベースのポリシー	いいえ
ポリシーアクション	はい
ポリシーリソース	あり
ポリシー条件キー	はい
一時的な認証情報	あり
転送アクセスセッション (FAS)	あり
サービスロール	はい
サービスリンクロール	いいえ

AWS Supply Chain およびその他の AWS のサービスがほとんどの IAM 機能とどのように連携するかの概要については、「IAM ユーザーガイド」のAWS 「IAM と連携する のサービス」を参照してください。

のアイデンティティベースのポリシー AWS Supply Chain

アイデンティティベースのポリシーのサポート: あり

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。ID ベースのポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素について学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

のアイデンティティベースのポリシーの例 AWS Supply Chain

AWS Supply Chain アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS Supply Chainのアイデンティティベースのポリシーの例。

内のリソースベースのポリシー AWS Supply Chain

リソースベースのポリシーのサポート: なし

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、または を含めることができます AWS のサービス。

クロスアカウントアクセスを有効にするには、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、リソースにアクセスするためのアクセス許可をプリンシパルエンティティ (ユーザーまたはロール) に付与する必要もあります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーをさらに付与する必要はありません。詳細については、「IAM ユーザーガイド」の「IAM でのクロスアカウントリソースアクセス」を参照してください。

のポリシーアクション AWS Supply Chain

ポリシーアクションのサポート:あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの Action 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連する AWS API オペレーションと同じです。一致する API オペレーションのない許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは依存アクションと呼ばれます。

このアクションは関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

のポリシーアクションは、アクションの前に次のプレフィックス AWS Supply Chain を使用します。

```
scn
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

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

AWS Supply Chain アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS Supply Chainのアイデンティティベースのポリシーの例。

のポリシーリソース AWS Supply Chain

ポリシーリソースのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルが、どのリソースに対してどのような条件下でアクションを実行できるかということです。

Resource JSON ポリシー要素はアクションが適用されるオブジェクトを指定します。ステートメントにはResource または NotResource 要素を含める必要があります。ベストプラクティスとし

て、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

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

AWS Supply Chain アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS Supply Chainのアイデンティティベースのポリシーの例。

のポリシー条件キー AWS Supply Chain

サービス固有のポリシー条件キーのサポート: あり

管理者は JSON AWS ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルが、どのリソースに対してどのような条件下でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成して、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition 要素を指定する場合、または 1 つの Condition 要素に複数のキーを指定する場合、 AWS では AND 論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 は論理ORオペレーションを使用して条件 AWS を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、「IAM ユーザーガイド」の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS は、グローバル条件キーとサービス固有の条件キーをサポートしています。すべての AWS グローバル条件キーを確認するには、「IAM ユーザーガイド」のAWS 「 グローバル条件コンテキストキー」を参照してください。

AWS Supply Chain アイデンティティベースのポリシーの例を表示するには、「」を参照してくださいAWS Supply Chainのアイデンティティベースのポリシーの例。

での一時的な認証情報の使用 AWS Supply Chain

一時的な認証情報のサポート: あり

一部の AWS のサービス は、一時的な認証情報を使用してサインインすると機能しません。一時的な認証情報 AWS のサービス を使用する機能などの詳細については、AWS のサービス 「IAM ユーザーガイド」の「IAM と連携する」を参照してください。

ユーザー名とパスワード以外の AWS Management Console 方法で にサインインする場合、一時的な認証情報を使用します。例えば、会社のシングルサインオン (SSO) リンク AWS を使用して にアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「ユーザーから IAM ロールに切り替える (コンソール)」を参照してください。

一時的な認証情報は、 AWS CLI または AWS API を使用して手動で作成できます。その後、これらの一時的な認証情報を使用してアクセスすることができます AWS。長期的なアクセスキーを使用する代わりに、一時的な認証情報 AWS を動的に生成することをお勧めします。詳細については、「IAM の一時的セキュリティ認証情報」を参照してください。

の転送アクセスセッション AWS Supply Chain

転送アクセスセッション (FAS) のサポート: あり

IAM ユーザーまたはロールを使用して でアクションを実行すると AWS、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、 を呼び出すプリンシパルのアクセス許可と AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストのリクエストリクエストを組み合わせて使用します。FAS リクエストは、サービスが他の AWS のサービス またはリソースとのやり取りを完了する必要があるリクエストを受け取った場合にのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FASリクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

AWS Supply Chainのサービスロール

サービスロールのサポート: あり

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスに許可を委任するロールを作成する」を参照してください。

> **Warning**
>
> サービスロールのアクセス許可を変更すると、 AWS Supply Chain 機能が破損する可能性があります。が指示する場合以外 AWS Supply Chain は、サービスロールを編集しないでください。

のサービスにリンクされたロール AWS Supply Chain

サービスにリンクされたロールのサポート: なし

サービスにリンクされたロールは、 にリンクされたサービスロールの一種です AWS のサービス。サービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。サービスにリンクされたロールは に表示され AWS アカウント 、 サービスによって所有されます。IAM 管理者は、サービスリンクロールの権限を表示できますが、編集することはできません。

サービスリンクロールの作成または管理の詳細については、「IAM と提携するAWS のサービス」を参照してください。表の中から、[Service-linked role (サービスリンクロール)] 列に Yes と記載されたサービスを見つけます。サービスリンクロールに関するドキュメントをサービスで表示するには、「はい」 リンクを選択します。

AWS Supply Chainのアイデンティティベースのポリシーの例

デフォルトでは、ユーザーとロールには AWS Supply Chain リソースを作成または変更するアクセス許可はありません。また、AWS マネジメントコンソール、AWS コマンドラインインターフェイス (AWS CLI)、または AWS API を使用してタスクを実行することもできません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

このような JSON ポリシードキュメントの例を使用して IAM のアイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーの作成」を参照してください。

トピック

- ポリシーに関するベストプラクティス

ポリシーに関するベストプラクティス

ID ベースのポリシーは、ユーザーのアカウントで誰かが AWS Supply Chain リソースを作成、アクセス、または削除できるどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可を付与するには、多くの一般的なユースケースにアクセス許可を付与する AWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の AWS カスタマー管理ポリシーを定義して、アクセス許可をさらに減らすことをお勧めします。詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」または「ジョブ機能のAWS マネージドポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、「IAM ユーザーガイド」の「IAM でのポリシーとアクセス許可」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。条件を使用して、サービスアクションが などの特定の を通じて使用される場合に AWS のサービス、サービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素:条件」を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer でポリシーを検証する」を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルートユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA を有効にします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細

については、「IAM ユーザーガイド」の「MFA を使用した安全な API アクセス」を参照してください。

IAM でのベストプラクティスの詳細については、IAM ユーザーガイドの IAM でのセキュリティのベストプラクティスを参照してください。

AWS Supply Chain ID とアクセスのトラブルシューティング

次の情報は、 と IAM の使用時に発生する可能性がある一般的な問題の診断 AWS Supply Chain と修正に役立ちます。

トピック

- でアクションを実行する権限がありません AWS Supply Chain
- iam:PassRole を実行する権限がない
- 自分の 以外のユーザーに AWS Supply Chain リソース AWS アカウント へのアクセスを許可したい

でアクションを実行する権限がありません AWS Supply Chain

アクションを実行する権限がないと AWS Management Console が通知した場合、管理者に問い合わせてサポートを依頼する必要があります。担当の管理者はお客様のユーザー名とパスワードを発行した人です。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要なscn:*GetWidget* アクセス許可を持っていない場合に発生するものです。

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

この場合、Mateo は、*my-example-widget* アクションを使用して scn:*GetWidget* リソースにアクセスできるように、ポリシーの更新を管理者に依頼します。

iam:PassRole を実行する権限がない

`iam:PassRole` アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して AWS Supply Chainにロールを渡すことができるようにする必要があります。

一部の AWS のサービス では、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、既存のロールをそのサービスに渡すことができます。そのためには、サービスにロールを渡す権限が必要です。

以下の例のエラーは、`marymajor` という IAM ユーザーがコンソールを使用して AWS Supply Chain でアクションを実行しようする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

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

この場合、Mary のポリシーを更新してメアリーに `iam:PassRole` アクションの実行を許可する必要があります。

サポートが必要な場合は、 AWS 管理者にお問い合わせください。サインイン認証情報を提供した担当者が管理者です。

自分の 以外のユーザーに AWS Supply Chain リソース AWS アカウント へのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください:

- がこれらの機能 AWS Supply Chain をサポートしているかどうかを確認するには、「」を参照してくださいと IAM の AWS Supply Chain 連携方法。
- 所有 AWS アカウント している 全体のリソースへのアクセスを提供する方法については、IAM ユーザーガイドの「所有 AWS アカウント している別の の IAM ユーザーへのアクセスを提供する」を参照してください。

- リソースへのアクセスをサードパーティーに提供する方法については AWS アカウント、「IAM ユーザーガイド」の「サードパーティー AWS アカウント が所有する へのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、「IAM ユーザーガイド」の「外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可」を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

AWS の マネージドポリシー AWS Supply Chain

AWS 管理ポリシーは、 によって作成および管理されるスタンドアロンポリシーです AWS。 AWS 管理ポリシーは、多くの一般的なユースケースにアクセス許可を付与するように設計されているため、ユーザー、グループ、ロールにアクセス許可の割り当てを開始できます。

AWS 管理ポリシーは、すべての AWS お客様が使用できるため、特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることに注意してください。ユースケースに固有のカスタマー管理ポリシーを定義して、アクセス許可を絞り込むことをお勧めします。

AWS 管理ポリシーで定義されているアクセス許可は変更できません。が AWS 管理ポリシーで定義されたアクセス許可 AWS を更新すると、ポリシーがアタッチされているすべてのプリンシパル ID (ユーザー、グループ、ロール) に影響します。 AWS AWS のサービス は、新しい が起動されたとき、または既存のサービスで新しい API オペレーションが利用可能になったときに、 AWS 管理ポリシーを更新する可能性が最も高くなります。

詳細については「IAM ユーザーガイド」の「AWS マネージドポリシー」を参照してください。

AWS マネージドポリシー: AWSSupplyChainFederationAdminAccess

AWSSupplyChainFederationAdminAccess は、 AWS Supply Chain アプリケーション内でアクションを実行するために必要なアクセス許可など、 AWS Supply Chain フェデレーティッドユーザーに AWS Supply Chain アプリケーションへのアクセスを提供します。このポリシーは、IAM アイデンティティセンターのユーザーとグループに対する管理アクセス許可を付与し、 によっ

て作成されたロールにアタッチ AWS Supply Chain されます。その他の IAM エンティティには AWSSupplyChainFederationAdminAccess ポリシーをアタッチすべきではありません。

このポリシーは scn:* アクセス許可 AWS Supply Chain を通じて へのすべてのアクセスを提供しますが、 AWS Supply Chain ロールによってアクセス許可が決まります。 AWS Supply Chain ロールには必要なアクセス許可のみが含まれ、管理者 APIs へのアクセス許可はありません。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- Chime – Amazon Chime AppInstance でユーザーを作成したり削除したりするためのアクセス許可を提供します。チャネル、チャネルのメンバー、モデレーターを管理するためのアクセス許可を提供します。チャネルにメッセージを送信するためのアクセス許可を提供します。Chime オペレーションの範囲は「SCNInstanceId」のタグが付いたアプリケーションインスタンスに限定されます。
- AWS IAM Identity Center (AWS SSO) – IAM アイデンティティセンターでユーザープロファイルの関連付けと関連付け解除、プロファイルの関連付けの一覧表示、アプリケーション割り当ての一覧表示、アプリケーションの記述、インスタンスの記述、およびアプリケーション割り当て設定の取得に必要なアクセス許可を提供します。
- AppFlow – 接続プロファイルを作成、更新、削除するためのアクセス許可を提供します。フローを作成、更新、削除、開始、停止するためのアクセス許可を提供します。フローのタグ付けとタグ解除、フローレコードの説明へのアクセス許可を提供します。
- Amazon S3 – すべてのバケットを一覧表示するためのアクセス許可を提供します。リソース arn arn:aws:s3:::aws-supply-chain-data-* を含むバケットへの GetBucketLocation、GetBucketPolicy、PutObject、GetObject、ListBucket のアクセス許可を提供します。
- SecretsManager – シークレットの作成とシークレットポリシーの更新のアクセス許可を提供します。
- KMS – Amazon AppFlow サービスにキーとキーのエイリアスへのアクセス許可を提供します。key-value aws-suply-chain-access : true でタグ付けされた KMS キーに DescribeKey、CreateGrant、ListGrants のアクセス許可を提供します。シークレットの作成とシークレットポリシーの更新のためのアクセス許可を提供します。

アクセス許可 (kms:ListKeys、kms:ListAliases、kms:GenerateDataKey、および kms:Decrypt) は Amazon AppFlow に制限されず、これらのアクセス許可はアカウントの任意の AWS KMS キーに付与できます。

このポリシーの許可を確認するには、 AWS Management Consoleの「AWSSupplyChainFederationAdminAccess」を参照してください。

AWS Supply ChainAWS 管理ポリシーの更新

次の表は、このサービスがこれらの変更の追跡を開始してからの の AWS Supply Chain AWS マネージドポリシーの更新に関する詳細を示しています。このページの変更に関する自動通知については、AWS Supply Chain ドキュメント履歴ページの RSS フィードにサブスクライブしてください。

変更	説明	日付
AWSSupplyChainFederationAdminAccess – ポリシーの更新	AWS Supply Chain は、IAM アイデンティティセンターの ListApplicationAssignments、DescribeApplication、DescribeInstance、および GetApplicationAssignmentConfiguration オペレーションへのアクセスをフェデレーティッドユーザーに許可するように マネージドポリシーを更新しました。	2024 年 12 月 10 日
AWSSupplyChainFederationAdminAccess – ポリシーの更新	AWS Supply Chain は、フェデレーティッドユーザーが IAM アイデンティティセンターの ListProfileAssociations オペレーションにアクセスできるように マネージドポリシーを更新しました。	2023 年 11 月 1 日

変更	説明	日付
AWSSupplyChainFederationAdminAccess – ポリシーの更新	AWS Supply Chain は、リソース arn arn:aws:s3::aws-Supply-chain-data-* を持つ専用 S3 バケットの PutObject および GetObject オペレーションへのアクセスをフェデレーティッドユーザーに許可するように マネージドポリシーを更新しました。	2023 年 9 月 21 日
AWSSupplyChainFederationAdminAccess – 新しいポリシー	AWS Supply Chain は、フェデレーティッドユーザーが AWS Supply Chain アプリケーションにアクセスすることを許可する新しいポリシーを追加しました。これには、 AWS Supply Chain アプリケーション内でアクションを実行するのに必要なアクセス許可が含まれます。	2023 年 3 月 1 日
AWS Supply Chain が変更の追跡を開始しました	AWS Supply Chain が AWS マネージドポリシーの変更の追跡を開始しました。	2023 年 3 月 1 日

のコンプライアンス検証 AWS Supply Chain

サードパーティーの監査者は、複数の コンプライアンスプログラム AWS Supply Chain の一環として のセキュリティと AWS コンプライアンスを評価します。これらのプログラムには、SOC、PCI、FedRAMP、HIPAA などがあります。

特定のコンプライアンスプログラムの範囲内 AWS のサービス にある のリストについては、「コンプライアンスプログラムAWS による対象範囲内のサービスコンプライアンスプログラム」を参照してください。一般的な情報については、AWS 「 Compliance ProgramsAssurance」を参照してください。

サードパーティーの監査レポートは でダウンロードできます AWS Artifact。詳細については、「Downloading AWS Artifact Reports 」を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS Supply Chain は、お客様のデータの機密性、貴社のコンプライアンス目的、適用される法律および規制によって決まります。 では、コンプライアンスに役立つ以下のリソース AWS を提供しています。

- 「セキュリティとコンプライアンスのクイックスタートガイド」 – これらのデプロイガイドには、アーキテクチャ上の考慮事項の説明と、セキュリティとコンプライアンスに重点を置いたベースラインの AWS 環境をデプロイするためのステップが記載されています。
- 「HIPAA セキュリティとコンプライアンスのためのアーキテクチャ設計」ホワイトペーパー – このホワイトペーパーでは、企業が AWS を使用して HIPAA 準拠のアプリケーションを作成する方法について説明します。
- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界と場所に適用される場合があります。
- 「AWS Config デベロッパーガイド」の ルールを使用したリソースの評価 – このガイドでは、リソース設定が社内慣行、業界ガイドライン、規制にどの程度準拠しているかを評価します。
- AWS Security Hub – これにより AWS のサービス 、 内のセキュリティ状態を包括的に把握 AWS し、セキュリティ業界標準とベストプラクティスへの準拠を確認できます。

の耐障害性 AWS Supply Chain

AWS グローバルインフラストラクチャは、 AWS リージョン およびアベイラビリティーゾーンを中心に構築されています。 AWS リージョン は、物理的に分離および分離された複数のアベイラビリティーゾーンを提供します。アベイラビリティーゾーンは、低レイテンシー、高スループット、高度の冗長ネットワークで接続されています。アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性が高く、フォールトトレラントで、スケーラブルです。

AWS リージョン およびアベイラビリティーゾーンの詳細については、AWS 「 グローバルインフラストラクチャ」を参照してください。

グローバル AWS インフラストラクチャに加えて、 AWS Supply Chain には、データの耐障害性とバックアップのニーズをサポートするのに役立ついくつかの機能が用意されています。

ログ記録とモニタリング AWS Supply Chain

ログ記録とモニタリングは、 AWS Supply Chain およびその他の AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。 は、 AWS Supply Chain を監視し、問題が発生したときに報告し、必要に応じて自動アクションを実行するための AWS CloudTrail モニタリングツール AWS を提供します。

> **Note**
>
> AWS Supply Chain コンソールからのみ呼び出される APIs がキャプチャされます AWS CloudTrail。

AWS CloudTrail は、 AWS アカウント により、またはそのアカウントに代わって行われた API コールや関連イベントを取得し、指定した Amazon S3 バケットにログファイルを配信します。 AWSを呼び出したユーザーとアカウント、呼び出し元の IP アドレス、および呼び出し日時を特定できます。 AWS Supply Chain イベントは、scn.amazonaws.com で確認できます。詳細については、AWS CloudTrail ユーザーガイドをご参照ください。

> **Note**
>
> 以下の点に注意してください AWS Supply Chain。
>
> - アクセス許可のないユーザーを招待すると AWS Supply Chain、これらのユーザーはウェブアプリケーションから受信した通知で情報を受信しません。招待されたユーザーは、ウェブアプリケーションへのリンクが記載されたメール通知を受け取ります。必要なユーザーアクセス許可を持っている場合にのみ、ログインして通知の内容を表示できます。
> - 特定の Insight に対するユーザーアクセス許可の有無を問わず、すべてのユーザーが Insights のチャットメッセージを表示できます。
> - アプリケーション管理者は、 AWS Supply Chain インスタンスにユーザーを追加するときに、 にアクセスできます AWS KMS key。ユーザーのアクセス許可を管理して、ユーザーを追加したり削除したりできます。ユーザーのアクセス許可の詳細については、「ユーザーアクセス許可ロールの管理」を参照してください。

AWS Supply Chain CloudTrail のデータイベント

> **Note**
>
> にリストされているウェブアプリケーション APIs AWS Supply Chain ウェブアプリケーション APIsは、CloudTrail のデータイベントにリストされています。

データイベントでは、リソース上またはリソース内で実行されるリソースオペレーション (Amazon S3 オブジェクトの読み取りまたは書き込みなど) についての情報が得られます。これらのイベントは、データプレーンオペレーションとも呼ばれます。データイベントは、多くの場合、高ボリュームのアクティビティです。デフォルトでは、CloudTrail はデータイベントを口グ記録しません。CloudTrail [イベント履歴] にはデータイベントは記録されません。

追加の変更がイベントデータに適用されます。CloudTrail の料金の詳細については、「AWS CloudTrail の料金」を参照してください。

CloudTrail コンソール、または CloudTrail CloudTrail API オペレーションを使用して AWS CLI、AWS Supply Chain リソースタイプのデータイベントを口グに記録できます。

- CloudTrail コンソールを使用してデータイベントを記録するには、データイベントを口グに記録する証跡またはイベントデータストアを作成するか、既存の証跡またはイベントデータストアを更新してデータイベントを口グに記録します。

  1. データイベントを口グに記録するには、[データイベント] を選択します。
  2. [データイベントタイプ] リストから、データイベントを口グ記録するリソースのタイプを選択します。
  3. 使用する口グセレクタテンプレートを選択します。リソースタイプのすべてのデータイベントを口グに記録したり、すべての `readOnly` イベントを口グに記録したり、すべての `writeOnly` イベントを口グに記録したり、カスタム口グセレクタテンプレートを作成して `readOnly`、`eventName`、`resources.ARN` フィールドでフィルタリングしたりできます。

- を使用してデータイベントを口グに記録するには AWS CLI、 `--advanced-event-selectors`パラメータを設定して、 `eventCategory`フィールドを に、 `Data` `resources.type`フィールドをリソースタイプ値 に設定します。条件を追加して、`readOnly`、`eventName` および `resources.ARN` フィールドの値でフィルタリングできます。

- データイベントをログに記録するように証跡を設定するには、put-event-selectors コマンドを実行します。詳細については、「AWS CLIを使用した証跡へのデータイベントのログ記録」を参照してください。
- データイベントをログ記録するようにイベントデータストアを設定するには、create-event-data-store コマンドを実行してデータイベントをログ記録する新しいイベントデータストアを作成するか、update-event-data-store コマンドを実行して既存のイベントデータストアを更新します。詳細については、「AWS CLIを使用したイベントデータストアへのデータイベントのログ記録」を参照してください。

*eventName、readOnly、および resources.ARN フィールドでフィルタリングして、自分にとって重要なイベントのみをログに記録するように高度なイベントセレクタを設定できます。フィールドの詳細については、「AdvancedFieldSelector」を参照してください。

AWS Supply Chain CloudTrail の管理イベント

管理イベントは、 AWS アカウントのリソースで実行される管理オペレーションに関する情報を提供します。これらのイベントは、コントロールプレーンオペレーションとも呼ばれます。CloudTrail は、デフォルトで管理イベントをログ記録します。

AWS Supply Chain は、すべてのコントロールプレーンオペレーションを管理イベントとして CloudTrail に記録します。

AWS Supply Chain ウェブアプリケーション APIs

このセクションに記載されている APIs は、フェデレーティッドユーザーに代わって AWS Supply Chain アプリケーションによって呼び出されます。これらの APIs「」を参照してくださいAWS Supply Chain。 CloudTrail これらの APIsは、フェデレーティッドユーザーロールのアクセス許可に基づいて AWS Supply Chain アプリケーションによって制御されます。 AWS Supply Chain アプリケーションの障害を防ぐために、これらの APIs へのアクセスを制御しようとしないでください。

ユーザーロール

以下の APIs は、 でユーザー、ユーザーロール、ユーザー通知、チャットメッセージを管理するために使用します 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
```

データレイク

次の API は、データレイク内のデータフローと接続の作成と管理に使用されます。

```
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

Insights アプリケーションでは、フィルター、ウォッチリストの管理、インベントリの変更の表示に次の API を使用します。

```
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
```

Demand Planning

次の APIsは、 で予測、需要計画、またはワークブックを作成および管理 AWS Supply Chain するために使用します。

```
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
```

供給計画

以下の APIsは、 で供給計画を作成および管理 AWS Supply Chain するために使用します。

```
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
```

の Amazon Q AWS Supply Chain

Amazon Q ではAPIs が使用されます AWS Supply Chain。

```
scn:GetQMessage
scn:ListQMessages
scn:PutQMessageFeedback
scn:SendQMessage
scn:GetQEnablementStatus
scn:UpdateQEnablementStatus
```

を使用した AWS Supply Chain イベントの管理 Amazon EventBridge

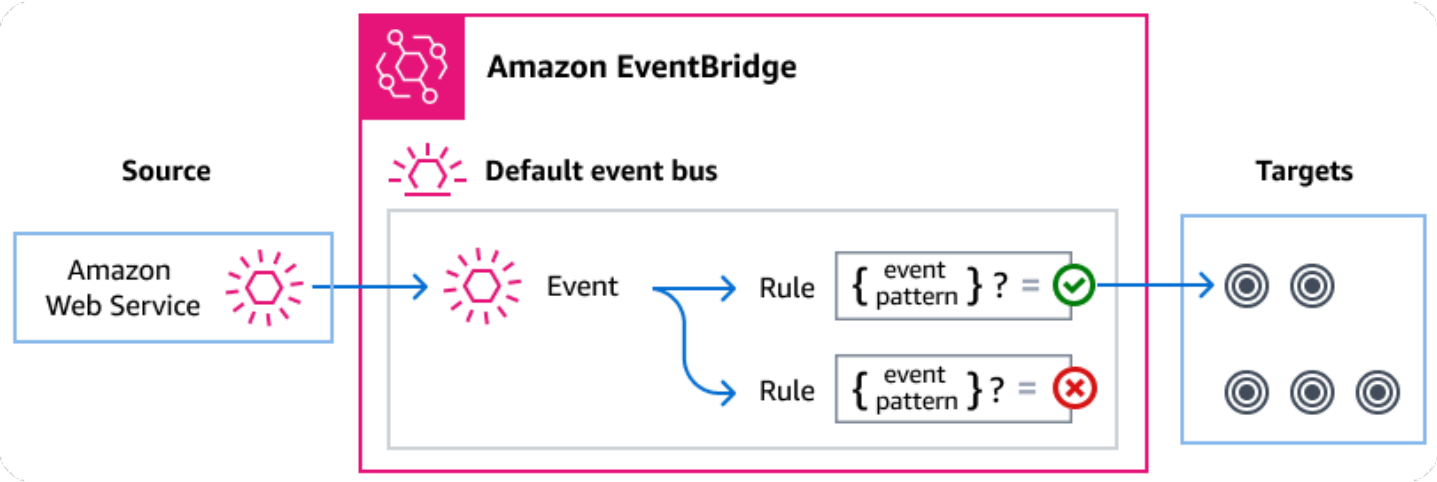
を使用すると EventBridge、他の のサービスを自動化して、 Step Functions 標準ワークフローの実行ステータスの変更に対応できます。

Amazon EventBridge は、イベントを使用してアプリケーションコンポーネントを接続できるサーバーレスサービスです。これにより、スケーラブルなイベント駆動型アプリケーションを簡単に構築できます。イベント駆動型アーキテクチャとは、イベントの発信と応答によって連携する、疎結合のソフトウェアシステムを構築するスタイルです。イベントとは、リソースまたは環境で発生した変更を指します。

処理の流れ

多くの AWS サービスと同様に、 はイベント AWS Supply Chain を生成し、 EventBridge デフォルトのイベントバスに送信します。(デフォルトのイベントバスはすべての AWS アカウントで自動的

にプロビジョニングされます）。イベントバスは、イベントを受信するルーターであり、ゼロ個以上の送信先やターゲットに配信します。イベントが受信されると、ユーザーがイベントバスに対して指定したルールによって評価されます。各ルールは、イベントがルールのイベントパターンに一致するかどうかをチェックします。一致する場合、イベントバスはそのイベントを指定されたターゲットに送信します。



トピック

- AWS Supply Chain イベント
- EventBridge ルールを使用した AWS Supply Chain イベントの配信
- AWS Supply Chain イベント詳細リファレンス

AWS Supply Chain イベント

AWS Supply Chain は、次のイベントをデフォルトの EventBridge イベントバスに自動的に送信します。ルールのイベントパターンに一致するイベントは、指定されたターゲットに配信されます。イベントは順不同で配信される可能性があります。

詳細については、「Amazon EventBridge ユーザーガイド」の「EventBridge イベント」を参照してください。

イベントの詳細のタイプ	説明
AWS Supply Chain データ統合ステータスの変更	取り込まれた各ファイルのステータスを表示します AWS Supply Chain。

EventBridge ルールを使用した AWS Supply Chain イベントの配信

EventBridge デフォルトのイベントバスでターゲットに AWS Supply Chain イベントを送信するには、ルールを作成する必要があります。各ルールにはイベントパターンが含まれており、イベントバスで受信した各イベントと EventBridge 照合します。イベントデータが指定されたイベントパターンと一致する場合、 はそのイベントをルールのターゲット (複数可) に EventBridge 配信します。

イベントバスルールの詳細な作成方法については、「EventBridge ユーザーガイド」の「イベントに反応する Amazon EventBridge ルールの作成」を参照してください。

イベントに一致する AWS Supply Chain イベントパターンの作成

各イベントパターンは JSON 形式のオブジェクトで、以下が含まれています。

- イベントを送信するサービスを識別する `source` 属性。 AWS Supply Chain イベントの場合、ソースは ですaws.supplychain。
- (オプション): 照合するイベントタイプの配列を含む `detail-type` 属性。
- (オプション): 照合対象となるその他のイベントデータを含む `detail` 属性。

たとえば、次のイベントパターンは、 からのすべてのAWS Supply Chain Data Integration Status Changeイベントに一致します AWS Supply Chain。

```
{
  "source": ["aws.supplychain"],
  "detail-type": ["AWS Supply Chain Data Integration Status Change"]
}
```

詳細については、「EventBridge ユーザーガイド」の「Amazon EventBridge のイベントパターン」を参照してください。

AWS Supply Chain イベント詳細リファレンス

AWS サービスからのすべてのイベントには、イベントのソースである AWS サービス、イベントが生成された時刻、イベントが発生したアカウントとリージョンなど、イベントに関するメタデータを含む共通のフィールドセットがあります。これらの一般的なフィールドの定義については、「Amazon EventBridge ユーザーガイド」の「イベント構造リファレンス」を参照してください。

さらに、各イベントには、その特定のイベントに固有のデータを含む detail フィールドがあります。以下のリファレンスでは、さまざまな AWS Supply Chain イベントの詳細フィールドを定義しています。

EventBridge を使用して AWS Supply Chain イベントを選択および管理する場合は、次の点に注意してください。

- からのすべてのイベントの sourceフィールド AWS Supply Chain は に設定されますaws.supplychain。
- detail-type フィールドはイベントタイプを指定します。

  例えば、AWS Supply Chain Data Integration Status Change と指定します。
- detail フィールドには、その特定のイベントに固有のデータが含まれます。

AWS Supply Chain イベントに一致するようにルールを有効化するイベントパターンの作成方法については、「Amazon EventBridge ユーザーガイド」の「Amazon EventBridge のイベントパターン」を参照してください。

イベントとその EventBridge 処理方法の詳細については、「 Amazon EventBridge ユーザーガイド」のAmazon EventBridge 「 イベント」を参照してください。

AWS Supply Chain データ統合ステータスの変更

以下は、 AWS Supply Chain Data Integration Status Change eventイベントの例です。

```
{
    "version": "0",
    "id": "instanceID",
    "detail-type": "AWS Supply Chain Data Integration Status Change",
    "source": "aws.supplychain",
    "account": "acccountID",
    "time": "2024-03-30T12:26:13Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "version": "1.0",
        "instanceId": "instanceID",
        "flowArn": "arn:aws:scn:region:acccountID:instance/instanceID/data-integration-
flows/flowname",
```

```
        "flowExecutionId": "flowExecutionId",
        "status": "IN_PROGRESS",
        "startTime": "2024-03-30T12:26:13Z",
        "endTime": "",
        "message": "",
        "sourceType": "S3",
        "sourceInfo": {
            "s3Source": {
                "bucketName": "aws-supply-chain-data-instanceID",
                "key": "flowname"
            }
        }
    }
}
```

endTime は、ステータスが失敗または成功の場合にのみ使用できます。

のクォータ AWS Supply Chain

AWS アカウント には、各 の制限と呼ばれるデフォルトのクォータがあります AWS のサービス。特に明記していない限り、クォータはリージョン固有です。アカウントレベルに設定されているリソースのクォータの引き上げをリクエストできます。アカウントレベルのクォータの詳細については、以下の表を参照してください。

のクォータを表示するには AWS Supply Chain、Service Quotas コンソールを開きます。ナビゲーションペインで、[AWS services] を選択し、AWS Supply Chain を選択します。

クォータの引き上げをリクエストするには、Service Quotas ユーザーガイド の「クォータ引き上げリクエスト」を参照してください。Service Quotas でクォータがまだ利用できない場合は、制限の引き上げ フォームを使用します。

AWS アカウント には、次のクォータが関連しています AWS Supply Chain。

リソース	デフォルト値	引き上げ可能
インスタンス数 **Note** AWS アカウント内に最大 10 個のインスタンスを作成できます。	10	いいえ
Amazon S3 バケット数	100	いいえ
AWS アカウント内のアクティブな招待と保留中の招待	30	はい
AWS アカウント内のデータリクエスト	4,000	はい
ウォッチリストあたりのインサイト明細項目	1,000	いいえ

リソース	デフォルト値	引き上げ可能
AWS アカウント内のインスタンスあたりの Insights ウォッチリスト	1,000	はい
AWS アカウント内のユーザーあたりの Insights ウォッチリスト	100	はい
AWS アカウント内のインスタンスあたりのデータ統合フロー	100	いいえ
AWS アカウント内のインスタンスあたりのカスタムデータセット名前空間	20	はい
AWS アカウント内のインスタンスあたりのカスタムデータセット名前空間あたりのデータセット	250	はい
AWS アカウント内のインスタンスあたりのデフォルトのデータセット名前空間のデータセット	1,000	いいえ

よくある質問 (FAQ)

以下の情報は、IAM アイデンティティセンターの有効化における一般的な問題のトラブルシューティングに役立ちます。

質問	回答
IAM Identity Center の統合が必要なのはなぜですか？	IAM アイデンティティセンターは、アイデンティティソースの同期を管理する IAM 内の機能です。IAM Identity Center は、 AWS Supply Chain インスタンスの ID ソースです。AWS コンソールと AWS Supply Chain ウェブアプリケーションをセットアップするには、IAM Identity Center を設定する必要があります。IAM Identity Center の詳細については、「AWS IAM Identity Center ユーザーガイド」の「IAM Identity Center AWS の有効化」を参照してください。
IAM Identity Center 組織インスタンスを使用する理由 AWS Supply Chain	組織インスタンスを作成することで、 AWS アカウント間で IAM Identity Center アクセスを有効にできます。例えば、 AWS Supply Chain インスタンス AWS アカウントと同じアカウントで IAM アイデンティティセンターが有効になっていない場合などです。組織の IAM アイデンティティセンターインスタンスを作成する利点の詳細については、「AWS IAM Identity Center ユーザーガイド」の「IAM アイデンティティセンターの組織インスタンス」を参照してください。
委任管理者権限が必要なのはなぜですか AWS Supply Chain？	委任された管理者が を使用する必要はありません AWS Supply Chain が、 AWS 組織の管理アカウントへのアクセスを制限し、IAM Identity Center を管理することは、組織のセットアップのベストプラクティスです。詳細につ

質問	回答
	いては、AWS 「Organizations の委任管理者」を参照してください。 組織インスタンスを作成するときは、 AWS Supply Chain インスタンスの作成に使用されるアカウントが IAM Identity Center アカウントと同じ組織の一部であることを確認します。インスタンスの作成に必要なアクセス許可が有効になっていることを確認し、IAM Identity Center アカウントと同じリージョンに AWS Supply Chain インスタンスを作成できます。AWS Supply Chain インスタンスの作成に必要なアクセス許可については、「」を参照してくださいの開始方法 AWS Supply Chain。

AWS サポート

管理者で、サポートに連絡する必要がある場合は AWS Supply Chain、次のいずれかのオプションを選択します。

- サポート アカウントをお持ちの場合は、 サポートセンターにアクセスしてチケットを送信してください。
- AWS Management Consoleを開き、[AWS Supply Chain]、[サポート]、[ケースを作成] の順に選択します。

次の情報を入力すると便利です。

- AWS Supply Chain インスタンス ID/ARN。
- AWS リージョン。
- 問題についての詳しい説明。

AWS Supply Chain 管理者ガイドのドキュメント履歴

次の表に、 のドキュメントリリースを示します AWS Supply Chain。

変更	説明	日付
AWS Supply Chain 更新されたクォータ	に関連する AWS アカウントのクォータを更新しました AWS Supply Chain。	2025 年 5 月 12 日
AWS 管理ポリシーの更新	AWS Supply Chain は、IAM アイデンティティセンターの ListApplicationAssignments、DescribeApplication、DescribeInstance、および GetApplicationAssignmentConfiguration オペレーションへのアクセスをフェデレーティッドユーザーに許可するように マネージドポリシーを更新しました。	2024 年 12 月 10 日
KMS ポリシーの更新	が AWS KMS キーにアクセスできるように KMS AWS Supply Chain ポリシーを更新しました。	2024 年 3 月 18 日
PrivateLink のサポート	インターフェイスエンドポイント (AWS PrivateLink) AWS Supply Chain を使用して にアクセスできます。	2024 年 2 月 26 日
グループの追加	AWS Supply Chainアクセスするには、ユーザーは IAM アイデンティティセンターグループに属している必要があります。	2023 年 11 月 14 日

AWS 管理ポリシーの更新	AWS Supply Chain は、IAM Identity Center の ListProfileAssociations オペレーションへのアクセスをフェデレーティッドユーザーに許可するように マネージドポリシーを更新しました。	2023 年 11 月 1 日
AWS 管理ポリシーの更新	AWS Supply Chain は、リソース arn arn:aws:s3::aws-Supply-chain-data-* を持つ専用の Amazon S3 バケットの PutObject および GetObject オペレーションへのアクセスをフェデレーティッドユーザーに許可するように マネージドポリシーを更新しました。	2023 年 9 月 21 日
リージョンのサポートに関する情報の更新	AWS Supply Chain Demand Planning がアジアパシフィック (シドニー) リージョンでもサポートされるようになりました。	2023 年 9 月 12 日
AWS コンソールを使用してオプトインおよびオプトアウトする AWS Supply Chain	AWS Supply Chain ユーザーは AWS コンソールを使用してオプトインおよびオプトアウト AWS Supply Chain し、AWS Organizations でコンテンツを使用または保存できるようになりました。	2023 年 9 月 7 日
リージョンのサポートに関する情報の更新	AWS Supply Chain は、アジアパシフィック (シドニー) リージョンおよび欧州 (アイルランド) リージョンでもサポートされるようになりました。	2023 年 7 月 19 日

AWS サポートへの問い合わせ方法とインスタンスの作成方法に関する情報の更新	AWS Supply Chain ユーザーは、AWS サポートに連絡してヘルプを求め、インスタンスの作成方法に関するコンテンツを更新できるようになりました。	2023 年 4 月 3 日
AWS 管理ポリシーを追加	AWS Supply Chain は、 AWS サプライチェーンアプリケーション内でアクションを実行するために必要なアクセス許可など、フェデレーティッドユーザーに AWS サプライチェーンアプリケーションへのアクセスを許可する新しいポリシーを追加しました。	2023 年 3 月 1 日
初回リリース	AWS Supply Chain 管理者ガイドの初回リリース。	2022 年 11 月 29 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。