aws

管理者ガイド

AWS Supply Chain

AWS Supply Chain: 管理者ガイド

Table of Contents

AWS Supply Chain とは

AWS Supply Chain は、エンタープライズリソースプランニング (ERP) やサプライチェーン管理システムなどの既存のソリューションと連携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。AWS Supply Chain を使用すると、既存の ERP システムやサプライチェーンシステムから在庫、供給、需要に関するデータに接続して抽出し、単一の AWS Supply Chain データモデルに統合できます。

トピック

AWS Supply Chain でサポートされるブラウザ

AWS Supply Chain を使用する前に、次の表を参照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	Firefox の サポート終了日 前のバージョンがサポートされます。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 と Edge Chromium	バージョン 84 以降
Safari	macOS 上の Safari 10 以降

AWS Supply Chain でサポートされている言語

AWS Supply Chain は、次の言語をサポートしています。

- 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
- インドネシア語

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

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環として、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

   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。セキュリティのベストプラクティスとして、ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用してルートユーザーアクセスが必要なタスクを実行してください。

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] を選んで、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、 を保護し AWS アカウントのルートユーザー、 を有効にして AWS IAM Identity Center、日常的なタスクにルートユーザーを使用しないように管理ユーザーを作成します。

のセキュリティ保護 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 「ルートユーザーの仮想 MFA デバイスを有効にする (コンソール)」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、「 ユーザーガイド」の「デフォルト でユーザーアクセス IAM アイデンティティセンターディレクトリを設定するAWS IAM Identity Center 」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「グループの参加」を参照してください。

AWS アカウントの閉鎖

AWS アカウントを解約する方法については、「アカウントを解約する」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

前提条件

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。

- を作成しました AWS アカウント。詳細については、「AWS アカウントのセットアップ」を参照してください。

> **Note**
>
> をアクティブ化していない場合は AWS IAM Identity Center、 AWS 組織を作成し、IAM Identity Center をアクティブ化します。 AWS 組織の作成の詳細については、「組織の作成」を参照してください。

- AWS Supply Chain インスタンスを作成する AWS リージョン のと同じ で IAM Identity Center を有効にします。 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) 、および欧州 (アイルランド) リージョンでのみサポートされています。詳細については、「IAM アイデンティティセンターを有効にする 」を参照してください。

> **Note**
>
> AWS Supply Chain Demand Planning と Supply Planning は、欧州 (アイルランド) リージョンではサポートされていません。

> **Note**
>
> ここに記載されているリージョン以外のリージョンで IAM Identity Center をアクティブ化していない場合、 AWS Supply Chain インスタンスを作成することはできません。

- AWS Identity and Access Management (IAM) コンソールから IAM ユーザーを作成できます。詳細については、「AWS アカウントのセットアップ」を参照してください。
- IAM Identity Center AWS Supply Chain へのアクセスを必要とするユーザーを追加します。詳細については、「IAM アイデンティティセンターへのユーザーの追加」を参照してください。Active Directory を IAM アイデンティティセンターに接続することもできます。詳細については、「AWS IAM Identity Center ユーザーガイド」の「Microsoft AD ディレクトリへの接続」を参照してください。
- Microsoft Active Directory を使用する場合は、Active Directory 同期が有効になっていることを確認します。
- インスタンスを作成するには AWS Key Management Service （ AWS KMS) が必要です。 AWS Supply Chain は、これ AWS KMS key を使用して に送信されるすべてのデータを暗号化します AWS Supply Chain。

AWS Supply Chain コンソールを使用する

> **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、 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。

ユーザーとロールが AWS Supply Chain 引き続きコンソールを使用できるようにするには、エンティティに または AWS Supply Chain `ConsoleAccessReadOnly` AWS 管理ポリシーもアタッチします。詳細については、「IAM ユーザーガイド」の「ユーザーへのアクセス許可の追加」を参照してください。

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: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"
        }
    ]
}
```

インスタンスの作成

> **Note**
>
> AWS アカウントには、最大 10 個のインスタンスを作成できます。この 10 個のインスタンスには、アクティブなインスタンスと初期化中のインスタンスが含まれます。IAM アイデンティティセンター (Single Sign-On の後継) AWS を既にアクティブ化している場合は、IAM アイデンティティセンターを AWS Supply Chain アクティブ化した AWS リージョン のと同じ にインスタンスを作成する必要があります。 AWS Supply Chain は、リージョン間の IAM アイデンティティセンター呼び出しをサポートしていません。

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。

> **Note**
>
> AWS Management Console 管理者のみがインスタンスを作成できます。 AWS Supply Chain インスタンスを作成する管理者 AWS Management Console 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AWS Supply Chain コンソールを使用する。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。

1. で AWS Supply Chain コンソールを開きますhttps://console.aws.amazon.com/scn/home。
2. 必要に応じて AWS リージョンを変更します。コンソールウィンドウの上部にあるバーで、[リージョンを選択] リストを開き、リージョンを選択します。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」を参照してください。「Amazon Web Services 全般のリファレンス」の「リージョンとエンドポイント」も参照してください。

   > **Note**
   >
   > 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 Demand Planning と Supply Planning は、欧州 (アイルランド) リージョンではサポートされていません。

3. AWS Supply Chain ダッシュボードで、インスタンスの作成 を選択します。
4. [インスタンスプロパティ] ページで、次の情報を入力します。
   - AWS リージョン — IAM Identity Center をアクティブ化したリージョンを選択します。リージョンを変更するには、右上のドロップダウンメニューから [リージョンの選択] を選択します。インスタンス作成後は、リージョンを変更できません。
   - 名前 – インスタンス名を入力します。
   - (オプション) 説明 – インスタンスの説明を入力します。
5. [AWS KMS キー] には、使用する KMS キーを入力して、次のとおり KMS キーポリシーを更新します。

> **Note**
>
> アプリケーション管理者として、 AWS Supply Chain ユーザーをインスタンスに追加すると、そのユーザーは AWS KMS keyにアクセスできるようになります。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、「ユーザーのアクセス許可ロール」を参照してください。

> **Note**
>
> *YourAccountNumber*、*#####* 、*YourInstanceID #### YourKmsKeyArn*を AWS アカウント、 AWS リージョン、 AWS Supply Chain インスタンス ID、および AWS KMS キーに置き換えます。

```
   {
   "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"
                }

            }
        }
    ]
}
```

KMS キーがない場合は、[作成] をクリックして、 AWS KMS コンソールに移動します。このコンソールでキーを作成できます。以前の KMS キーポリシーを使用します。KMS キーの作成方法の詳細については、「AWS Key Management Service デベロッパーガイド」の「キーの作成」を参照してください。

S/4 Hana データ接続を使用する場合は、指定した KMS キーに、関連付けられた値が true の aws-supply-chain-access タグがあることを確認してください。

6. (オプション) [インスタンスタグ] の下の [新しいタグを追加] をクリックして、このインスタンスのタグを割り当てます。このようなタグを使用すると、インスタンスを識別できます。タグの詳細については、「タグとは」を参照してください。
7. [インスタンスの作成] を選択します。

   AWS Supply Chain インスタンスが作成されるまでに約 2 ~ 3 分かかります。インスタンスが作成されると、 AWS Supply Chain ダッシュボードのステータスフィールドにはアクティブ と表示されます。
8. AWS Supply Chain インスタンスが作成されたら、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**
>
> *YourInstanceID* を AWS Supply Chain インスタンス ID に置き換えます。インスタンス ID は、 AWS Supply Chain コンソールのダッシュボードで確認できます。

```
        {
    "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": "*"
},
{
    "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 アイデンティティセンターを有効にする

の使用を開始する前に AWS Supply Chain、ID ソースに接続する必要があります。詳細については、「IAM ユーザーガイド」の「https://docs.aws.amazon.com/IAM/latest/UserGuide/getting-started.htmlIAM の使用開始」を参照してください。

IAM アイデンティティセンターへのユーザーの追加

IAM Identity Center サービス AWS Supply Chain を使用して のユーザーを管理できます。IAM Identity Center はクラウドベースの IAM Identity Center サービスで、すべての AWS アカウント およびクラウドアプリケーションへの IAM Identity Center アクセスを一元管理するのに便利です。IAM ユーザーの追加方法の詳細については、「IAM ユーザーガイド」の「AWS アカウント での IAM ユーザーの作成」を参照してください。

IAM ユーザーグループの作成方法の詳細については、「IAM ユーザーガイド」の「IAM ユーザーグループの作成」を参照してください。

> **Note**
>
> にユーザーを追加するには AWS Supply Chain、ユーザーは IAM Identity Center グループのメンバーである必要があります。

AWS Supply Chain アプリケーション所有者の選択

> **Note**
>
> 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のアプリケーション所有者 で、アプリケーション所有者の割り当て を選択します。
2. 「アプリケーション所有者の選択」で、 AWS Supply Chain アプリケーション所有者として機能するユーザーを選択します。検索できるのはユーザー名のみです。検索条件に一致するユーザーが表示されます。

   さらにユーザーを追加するには、[IAM アイデンティティセンターに移動する] をクリックします。ユーザーの追加の詳細については「IAM アイデンティティセンターへのユーザーの追加」、ユーザーのアクセス許可の詳細については「ユーザーの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。

3. [招待を送信する] をクリックします。

   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。
4. で管理 AWS Supply Chain 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します。

グループの割り当て

アプリケーション所有者または AWS Supply Chain 管理者は、IAM Identity Center グループに属するユーザーのみを に追加できます AWS Supply Chain。

1. AWS Supply Chain コンソールダッシュボードのグループ で、グループの割り当て を選択します。

   [グループ] ページが開きます。
2. グループ名 で、アクセスできるユーザーを含むグループを選択し AWS Supply Chain 、 の割り当て を選択します。

   AWS Supply Chain ダッシュボードの「グループ」の下にリストしたグループが表示されます。

3. [グループを管理] をクリックすると、IAM アイデンティティセンターに新しいグループを追加できます。IAM アイデンティティセンターにグループが追加されると、作成したグループが [グループ名] の下に一覧表示されます。 AWS Supply Chain

AWS Supply Chain ウェブアプリケーションへのログイン

AWS Supply Chain 管理者として、 AWS Supply Chain ウェブアプリケーションへの招待メールが届いているはずです。

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. AWS IAM Identity Center のユーザー認証情報を入力し、「サインイン」を選択します。

AWS Supply Chain に初めてログインする

> **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。

管理者として AWS Supply Chain AWS Supply Chain ウェブアプリケーションにログインしたら、以下の手順に従ってセットアップを完了します。

1. [Complete your profile] ページで、[Job Title] と [タイムゾーン] を入力します。[次へ] をクリックします。
2. [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] をクリックします。
3. [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。IAM アイデンティティセンターユーザーまたはグループの追加方法の詳細については、「IAM アイデンティティセンターへのユーザーの追加」を参照してください。 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のアクセス許可ロール。
4. 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。

5. 追加した各ユーザーには、 へのリンクが記載された E メールメッセージが届きます。または AWS Supply Chain、リンクをコピーしてユーザーに送信することもできます。
6. [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。

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。アカウントは、次の手順で更新できます。

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

[Organization profile] 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。組織プロファイルは、次の手順で更新できます。

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。

ユーザーのアクセス許可ロール

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
- プランナー – 予測と上書きを作成、表示、管理し、需要計画を公開するアクセス許可
- 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 に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

> **Note**
>
> ユーザーを追加する前に、ユーザーが IAM Identity Center グループの一部であり、グループが に割り当てられていることを確認してください AWS Supply Chain。

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、次の手順で追加できます。

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. [Add New User] をクリックします。

   [Add User] ページが開きます。
4. [ユーザーを追加] ドロップダウンメニューでユーザーを選択して、[ロールの選択] の下でこのユーザーのロールを選択します。
5. [追加] を選択します。

ユーザーアクセス許可の更新

現在のユーザーのユーザーアクセス許可ロールを更新できます AWS Supply Chain 。ユーザーのアクセス許可ロールは、次の手順で更新できます。

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、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て、[アクセス許可ロール] ドロップダウンメニューから次の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。

- 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
- プランナー – 予測と上書きを作成、表示、管理し、需要計画を公開するアクセス許可

4. [保存] 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、特定の口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。

> **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] の下で製品と口ケーションのみが選択できます。例えば、シアトルの口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。

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。

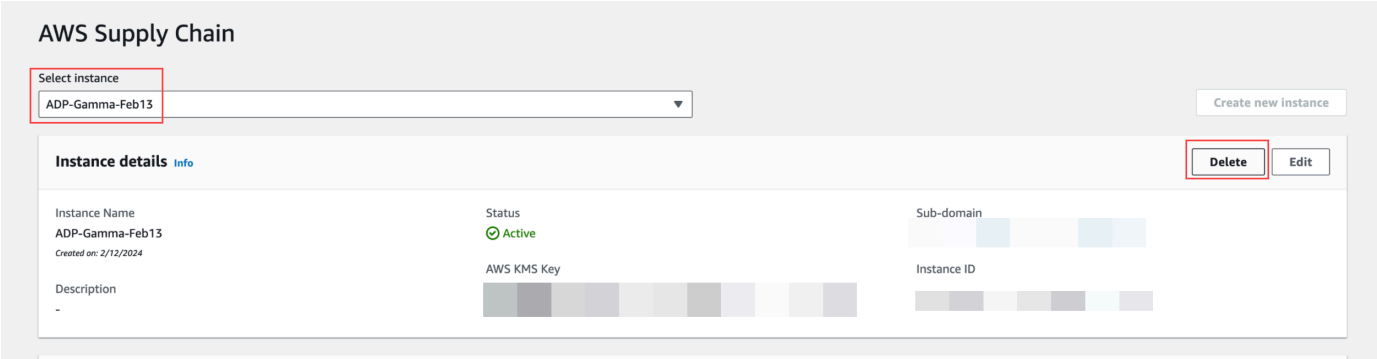
   [アクセス許可ロール] ページが開きます。
2. [Create New Role (新しいロールを作成)] を選択します。
3. [アクセス許可を管理する] ページの [ロール名] に名前を入力します。
4. スライダーを動かしてユーザーアクセス許可ロールを選択します。
   - 管理 – ユーザーに管理アクセス許可を割り当てると、情報を追加、編集、管理できます。
   - 表示 – ユーザーに表示アクセス許可を割り当てると、現在の情報のみを表示できます。
5. [Location Access] の下で、検索バーにリージョンを入力して検索し、選択します。
6. [Product Access] の下で、検索バーに製品を入力して検索し、選択します。
7. [保存] 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、次の手順を実行します。

> **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。

のセキュリティ AWS Supply Chain

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利点を得られます。

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を担います AWS クラウド。また、 は、ユーザーが安全に使用できるサービス AWS 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。に適用す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 AWS のサービス によって、お客様の責任が決まります。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 AWS Supply Chain を達成するために を設定する方法を示します。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 を使用したアクセス
- の IAM AWS Supply Chain
- AWS の AWS Supply Chain 向け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 での耐障害性
- ロギングとモニタリング AWS Supply Chain

でのデータ保護 AWS Supply Chain

AWS のデータ保護には、https://aws.amazon.com/compliance/shared-responsibility-model/、 (責任分担モデル) が適用されます AWS Supply Chain。このモデルで説明したように、 AWS は、 AWS クラウドすべてを稼働させ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。お客様は、このインフラストラクチャでホストされてい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のよくある質問」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。

データ保護の観点から、 AWS アカウント 認証情報を保護し、 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。こうすると、それぞれのジョブを遂行するために必要なアクセス許可のみを各ユーザーに付与できます。また、以下の方法でデータを保護することをお勧めします。

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用してリソースと通信します。 AWS TLS 1.2、できれば TLS 1.3 が必要です。
- を使用して API とユーザーアクティビティのロギングを設定します。 AWS CloudTrail
- AWS 暗号化ソリューションと、 AWS のサービスその中に含まれるデフォルトのセキュリティコントロールをすべて使用してください。
- Amazon Macie などの高度なマネージド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 を介してアクセスするときに FIPS 140-2 で検証された暗号モジュールが必要な場合は、FIPS エンドポイントを使用してください。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) 140-2」を参照してください。

お客様の E メールアドレスなどの機密情報やセンシティブ情報は、タグや名前フィールドなどの自由形式のフィールドに配置しないことを強くお勧めします。これには、コンソール、API、または SDK を操作する場合や、 AWS のサービス その他の方法でコンソール、API、 AWS Supply Chain または SDK を使用する場合も含まれます。 AWS CLI AWS 名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。外部サーバーへの URL を提供する場合は、そのサーバーへのリクエストを検証するための認証情報を URL に含めないように強くお勧めします。

AWS Supply Chainによって処理されるデータ

AWS 特定のサプライチェーンインスタンスの権限を持つユーザーがアクセスできるデータを制限するために、サプライチェーン内に保持されているデータは、 AWS アカウント ID AWS とサプライチェーンインスタンス ID によって分離されます。 AWS

AWS Supply Chainは、ユーザー情報、データコネクターから抽出された情報、在庫の詳細など、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

当社は、AWS サービス規約に記載されているとおり AWS Supply Chain、処理されたお客様のコンテンツを使用および保存する場合があります。コンテンツの使用や保存をオプトアウトしたい場合は、AWS Organizations でオプトアウトポリシーを作成できます。 AWS Supply Chain オプトアウトポリシーの作成に関する詳細については、「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 に分類される連絡先データ、またはによって保存されている顧客コンテンツを表すデータは AWS Supply Chain、保存時 (つまり、ディスクに保存、保存、保存される前) に、期間限定のインスタンス固有のキーで暗号化されます。 AWS Supply Chain

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。について詳しくは AWS KMS keys、「What is?」を参照してください。 AWS Key Management Service『 AWS Key Management Service 開発者ガイド』の。

> **Note**
>
> AWS Supply Chain 機能供給計画と N 層可視性は、提供されている KMS-CMK data-at-rest による暗号化をサポートしていません。

転送中の暗号化

AWS Supply Chain と交換されるデータは、業界標準の TLS 暗号化を使用して、 AWS ユーザーのウェブブラウザとサプライチェーン間の転送中に保護されます。

キー管理

AWS Supply Chain KMS-CMK を部分的にサポートします。

で AWS KMS キーを更新する方法については AWS Supply Chain、を参照してくださいインスタンスの作成。

ネットワーク間トラフィックのプライバシー

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

の仮想プライベートクラウド (VPC) AWS Supply Chain エンドポイントは、への接続のみを許可する VPC 内の論理エンティティです。 AWS Supply Chain VPC は VPC AWS Supply Chain にリクエストをルーティングし、応答を 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。

AWS Supply Chain でのグラントの使用方法 AWS KMS

AWS Supply Chain カスタマーマネージドキーを使用するには権限が必要です。

AWS Supply Chain AWS KMS CreateInstance操作中に渡されたキーを使用して複数の権限を作成します。 AWS Supply Chain CreateGrantにリクエストを送信して、ユーザーに代わってグラントを作成します AWS KMS。 AWS KMS の権限は、 AWS Supply Chain AWS KMS 顧客アカウントのキーへのアクセスを許可するために使用されます。

> **Note**
>
> AWS Supply Chain 独自の認証メカニズムを使用します。いったんユーザを追加すると AWS Supply Chain、 AWS KMS そのポリシーを使用して同じユーザを拒否リストに追加することはできません。

AWS Supply Chain この権限を以下の目的で使用します。

- GenerateDataKey AWS KMS インスタンスに保存されているデータを暗号化するリクエストをに送信する。

- インスタンスに関連付けられている暗号化されたデータを読み取るために、 AWS KMS に復号化リクエストを送信します。
- データを Amazon Forecast AWS などの他のサービスに送信する際にデータを安全に保つためにDescribeKey、CreateGrant、RetireGrantの権限を追加すること。

任意のタイミングで、許可に対するアクセス権を取り消したり、カスタマーマネージドキーに対するサービスからのアクセス権を削除したりできます。追加すると、 AWS Supply Chain 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できなくなり、そのデータに依存する操作に影響します。

以下の暗号化を監視しています。 AWS Supply Chain

次の例はEncryptGenerateDataKey、Decrypt AWS Supply Chain 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するために呼び出される KMS オペレーションを監視する、、 AWS CloudTrail のイベントです。

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 のインスタンスは、パブリック IP アドレスがなくても AWS Supply Chain にアクセスできます。

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「 AWS のサービス によるアクセス 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」を確認してください。

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
```

インターフェイスエンドポイントのプライベート DNS を有効にすると、リージョンのデフォルト DNS 名を使用して、 AWS Supply Chain への API リクエストを実行できます。例えば *scn*.*region*.amazonaws.com です。

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 への許可された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
- アクションを実行できるリソース

詳細については、AWS PrivateLink 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する)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
- が IAM と AWS Supply Chain 連携する方法
- 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、 で行う作業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が IAM と AWS Supply Chain 連携する方法。

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 (にサインイン 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 の認証情報は、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 AWS を使用して にアクセスすると、間接的にロールを引き受けることになります。

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、「 ユーザーガイド」の「 へのサインイン AWS アカウント方法AWS サインイン 」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。推奨される方法を使用してリクエストを自分で署名する方法の詳細については、IAM ユーザーガイドの API AWS リクエストの署名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向上させ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「AWSでの多要素認証 (MFA) の使用」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、一時的な認証情報を使用して にアクセスするための ID プロバイダーとのフェデレーションの使用を要求 AWS のサービス 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て、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「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対して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、ロールでは一時的な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 (ロールではなく) の作成が適している場合」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。ロール を切り替える AWS Management Console ことで、 で IAM ロールを一時的に引き受けることができます。ロールを引き受けるには、 または AWS API AWS CLI オペレーションを呼び出すか、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「IAM ロールの使用」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詳細については、「IAM ユーザーガイド」の「Creating a role for a third-party Identity Provider」(サードパーティーアイデンティティプロバイダー向けロールの作成) 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 ユーザーガイド」の「アクセス許可セット」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) ポリシーをリソースに直接アタッチできます。クロスアカウントアクセスの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リソースアクセス」を参照してください。
- クロスサービスアクセス — 一部の 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 でアクションを実行する場合 AWS、ユーザーは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を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストリクエストリクエストと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 のサービスにアクセス許可を委任するロールの作成」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。

IAM ロールと IAM ユーザーのどちらを使用するかについては、「IAM ユーザーガイド」の「(IAM ユーザーではなく) IAM ロールをいつ作成したら良いのか?」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、 AWS ID またはリソースにアタッチします。ポリシーは、アイデンティティまたはリソースに関連付けられているときにアクセス許可を定義する のオブジェクトです。 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) AWS 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 AWS JSON 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んなリソースにどんな条件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継ぐことができます。

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、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 権限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。

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「マネージドポリシーとインラインポリシーの比較」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 IAM の AWS マネージドポリシーを使用することはできません。

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のポリシーによって 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) に対する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、 AWS アカウント ビジネスが所有する複数の をグループ化して一元管理するサービスです。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「SCP の仕組み」を参照してください。
- 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与する場合に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。

が IAM と AWS Supply Chain 連携する方法

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のポリシー	Yes
リソースベースのポリシー	No
ポリシーアクション	Yes

IAM 機能	AWS Supply Chain サポート
ポリシーリソース	Yes
ポリシー条件キー	はい
一時的な認証情報	はい
転送アクセスセッション (FAS)	はい
サービスロール	あり
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 機能と連携する方法の概要を把握するには、「IAM ユーザーガイド」の「IAM AWS 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ポリシーをサポートする	Yes

アイデンティティベースポリシーは、IAM ユーザー、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。

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	No

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 にある場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス許可も付与する必要があります。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に対するサポート	はい

管理者は AWS JSON 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んなリソースにどんな条件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、関連付けられた 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権限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

ポリシーリソースに対するサポート	はい

管理者は AWS JSON 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どのような条件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	はい

管理者は AWS JSON 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んなリソースにどんな条件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することで、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 要素を指定するか、1 つの Condition 要素に複数のキーを指定すると、 AWS 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	はい

一部の は、一時的な認証情報を使用してサインインすると機能 AWS のサービス しません。一時的な認証情報 AWS のサービス を使用する などの詳細については、IAM ユーザーガイドのAWS のサービス「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 Single Sign-On (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「ロールへの切り替え (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 . AWS recommends にアクセスできます AWS。この際、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) をサポート	はい

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を AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストリクエストリクエストと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

サービスロールに対するサポート	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 のサービスにアクセス許可を委任するロールの作成」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	いいえ

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

- ポリシーのベストプラクティス

ポリシーの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「AWS ジョブ機能の管理ポリシー」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、 などの特定の を介してサービスアクションが使用される場合に 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 policy elements: Condition] (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 ポリシーの検証」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 保護 API アクセスの設定」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、 および 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ない AWS Supply Chain
- iam を実行する権限がありません。PassRole
- 自分の 以外のユーザーに自分のリソース AWS アカウント へのアクセス AWS Supply Chain を許可したい

でアクションを実行する権限がない 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、scn:*GetWidget* アクションを使用して *my-example-widget* リソースへのアクセスが許可されるように、管理者にポリシーの更新を依頼します。

iam を実行する権限がありません。PassRole

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、そのサービスに既存のロールを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 以外のユーザーに自分のリソース AWS アカウント へのアクセス AWS Supply Chain 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が IAM と AWS Supply Chain 連携する方法。
- 所有 AWS アカウント している 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認証されたユーザーへのアクセスの提供 (ID フェデレーション) を参照してください。

- クロスアカウントアクセスでのロールとリソースベースのポリシーの使用の違いについては、IAM ユーザーガイドの「IAM でのクロスアカウントリソースアクセス」を参照してください。

AWS の AWS Supply Chain 向けマネージドポリシー

AWS マネージドポリシーは、AWS が作成して管理するスタンドアロンのポリシーです。AWS マネージドポリシーは、多くの一般的なユースケースでアクセス許可を提供できるように設計されており、ユーザー、グループ、ロールへのアクセス許可の割り当てをすぐに開始できます。

AWS マネージドポリシーは、ご利用の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ご注意ください。AWS のすべてのお客様が使用できるようになるのを避けるためです。ユースケースに応じた カスタマー管理ポリシー を定義することで、アクセス許可を絞り込むことをお勧めします。

AWS マネージドポリシーで定義したアクセス許可は変更できません。AWS が AWS マネージドポリシーに定義されているアクセス許可を更新すると、更新はポリシーがアタッチされているすべてのプリンシパルアイデンティティ (ユーザー、グループ、ロール) に影響します。新しい AWS のサービスを起動するか、既存のサービスで新しい API オペレーションが使用可能になると、AWS が AWS マネージド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 アプリケーションないでアクションを実行するのに必要なアクセス許可を含めた AWS Supply Chain アプリケーションのアクセスを AWS Supply Chain フェデレーションユーザーに提供します。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管理アクセス許可を付与し、AWS Supply Chain が作成したロールにアタッチされています。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:* アクセス許可を介して AWS Supply Chain へのアクセスをすべて提供するとはいえ、ユーザーのアクセス許可は AWS Supply Chain ロールに応じて異なります。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 API へのアクセス許可はありません。

アクセス許可の詳細

このポリシーに含まれているアクセス許可は、次のとおりです。

- 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)– ユーザープロファイルの関連付けと関連付けの解除、IAM アイデンティティセンターのアプリケーションインスタンスに関連付けられたプロファイルの一覧表示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、kms:Decrypt) は Amazon AppFlow に限定されません。このアクセス許可はアカウント内の任意の AWS KMS キーにも付与できます。

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 マネージドポリシーの AWS Supply Chain に関する更新

このサービスによる追跡開始以降に行われた AWS Supply Chain 向けの AWS マネージドポリシーに対する更新の詳しい説明は、次の表のとおりです。このページの変更に関する自動通知については、「AWS Supply Chain ドキュメントの履歴」ページの RSS フィードを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 では、IAM アイデンティティセンターの ListProfileAssociations オペレーションへのアクセスをフェデレーション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
AWSSupplyChainFederationAdminAccess – ポリシーの更新	AWS Supply Chain では、リソース arn arn:aws:s3:::aws-supply- chain-data-* を含む専用 S3 バケットでの PutObject オペレーションと GetObject オペレーションへのアクセスをフェデレーション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 では、AWS Supply Chain アプリケーションへのアクセスをフェデレーション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。これには、AWS Supply Chain アプリケーション内でアクショ	2023 年 3月 1 日

変更	説明	日付
	ンを実行するのに必要なアクセス許可が含まれます。	
AWS Supply Chain での変更の追跡の開始	AWS Supply Chain での 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

AWS Supply Chain のコンプライアンス検証

第三者監査人が、複数の AWS コンプライアンスプログラムの一環として AWS Supply Chain のセキュリティとコンプライアンスを評価します。このようなプログラムには、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対象となる AWS のサービス サービスのリストについては、「コンプライアンスプログラムによる対象範囲内の AWS のサービス」を参照してください。一般的な情報については、「AWS コンプライアンスプログラム」「」「」を参照してください。

AWS Artifact を使用して、サードパーティーの監査レポートをダウンロードできます。詳細については、「AWS Artifact 内のレポートのダウンロード」を参照してください。

AWS Supply Chain を使用する際のお客様のコンプライアンス責任は、お客様のデータの機密性、企業のコンプライアンス目標、適用法と規制に応じて異なります。AWS は、コンプライアンスに役立つ次のリソースを提供しています。

- 「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 セキュリティおよびコンプライアンスホワイトペーパーのアーキテクチャの設計 - 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 コンプライアンスのリソース」- このワークブックおよびガイドのコレクションは、ユーザーの業界や拠点で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 – この AWS のサービス では、AWS 内のセキュリティ状態が包括的に示され、業界標準のセキュリティとベストプラクティスへの準拠の確認に役立ちます。

AWS Supply Chain での耐障害性

AWS のグローバルインフラストラクチャは、AWS リージョンと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、物理的に分離され、隔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 と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。

AWS では、AWS Supply Chain グローバルインフラストラクチャに加えて、データの耐障害性とバックアップのニーズに対応できるように複数の機能を提供しています。

ロギングとモニタリング AWS Supply Chain

ロギングとモニタリングは、 AWS AWS サプライチェーンやその他の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。 AWS AWS CloudTrail AWS サプライチェーンを監視し、問題が発生した場合は報告し、必要に応じて自動アクションを実行するための監視ツールを提供します。

> **Note**
>
> AWS Supply Chain コンソールからのみ呼び出された API AWS CloudTrailが取り込まれます。

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送信します。 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 サプライチェーンイベントは 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』を参照してください。

> **Note**
>
> AWS Supply Chain以下の点に注意してください。
>
> - アクセス権のないユーザーを招待しても AWS Supply Chain、そのユーザーはウェブアプリケーションから受け取る通知の情報を受け取りません。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 ユーザーをインスタンスに追加すると、そのユーザーは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、「ユーザーのアクセス許可ロール」を参照してください。

AWS Supply Chain 内のデータイベント CloudTrail

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 データイベントは記録されません。 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 価格について詳しくは、「AWS CloudTrail 価格設定」を参照してください。

CloudTrail コンソール、、または 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ログに記録できます。

- 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、トレイルまたはイベントデータストアを作成してデータイベントを記録するか、既存のトレイル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記録します。

  1. [データイベント] を選択してデータイベントをログに記録します。
  2. データイベントタイプリストから、データイベントを記録したいリソースタイプを選択します。

3. 使用するログセレクター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ログに記録したり、readOnlyすべてのイベントをログに記録したり、、フィールドをフィルタリングするカスタムログセレクターテンプレートを作成したりできます。writeOnly readOnly eventName resources.ARN

- を使用してデータイベントを記録するには AWS CLI、フィールドをリソースタイプ値と等しく、--advanced-event-selectorseventCategoryDataフィールドをリソースタイプ値と等しく設定するようにパラメータを設定します。resources.type、、readOnlyresources.ARNの各フィールドの値を基準にフィルタリングする条件を追加できます。eventName
  - データイベントをログに記録するようにトレイルを設定するには、put-event-selectorsコマンドを実行します。詳しくは、「トレイルのデータイベントのロギング」を参照してください。AWS CLI
  - データイベントを記録するようにイベントデータストアを構成するには、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、「を使用したイベントデータストアのデータイベントのロギング」を参照してください AWS CLI。

*高度なイベントセレクターを設定してeventName、readOnly、resources.ARNの各フィールドを絞り込んで、重要なイベントのみを記録できます。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 の管理イベント CloudTrail

管理イベントは、 AWS アカウント内のリソースに対して実行される管理操作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。デフォルトでは、 CloudTrail 管理イベントが記録されます。

AWS Supply Chain は、 CloudTrail すべてのコントロールプレーンの操作を管理イベントとして記録します。

AWS Supply Chain ウェブアプリケーション API

このセクションに記載されている API は、 AWS Supply Chain フェデレーティッドユーザーに代わってアプリケーションによって呼び出されます。これらの API CloudTrail はログには表示されず、「サービス認証リファレンス」ドキュメントにも記録されません。を参照してくださいAWS Supply

Chain。これらの API へのアクセスは、 AWS Supply Chain フェデレーティッドユーザーロールの権限に基づいてアプリケーションによって制御されます。アプリケーションの中断を防ぐためにこれらの API へのアクセスを制御しようとしてはいけません。 AWS Supply Chain

ユーザーロール

次の API は、でのユーザー、ユーザーロール、ユーザー通知、チャットメッセージの管理に使用されます。 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
```

インサイト

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 API は、予測、需要計画、またはワークブックの作成と管理に使用されます。 AWS Supply Chain

```
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

供給計画の作成と管理には AWS Supply Chain 、次の API が使用されます。

```
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
```

のクォータ AWS Supply Chain

AWS アカウント には、各 について、以前は制限と呼ばれていたデフォルトのクォータがありますAWS のサービス。特に明記されていない限り、クォータは地域固有です。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。

には、 に関連する以下のクォータ AWS アカウント があります 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および保留中の招待	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インサイトウォッチリスト	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 Supply Chain の管理サポートを受ける

管理者が AWS Supply Chain のサポートに問い合わせる必要がある場合、次のいずれかのオプションを選択します。

- AWS Support アカウントがある場合は、サポートセンター にアクセスして、チケットを送信します。
- AWS Management Console を開き、[AWS Supply Chain]、[サポート]、[Create case] の順に選択します。

次の情報を入力すると役に立ちます。

- 使用する AWS Supply Chain インスタンスの ID または ARN
- 使用する 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

次の表では、 AWS Supply Chainのドキュメンテーションリリースについて説明しています。

変更	説明	日付
KMS ポリシーアップデート	AWS Supply Chain キーへのアクセスを許可するように KMS ポリシーを更新しました。 AWS KMS	2024 年 3 月 18 日
PrivateLink 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 管理ポリシーを更新しました。	AWS Supply Chain フェデレーティッドユーザーが IAM Identity Center ListProfileAssociations の操作にアクセスできるように管理ポリシーを更新しました。	2023 年 11 月 1 日
管理ポリシーを更新しました AWS 。	AWS Supply Chain フェデレーティッドユーザーが arn: aws: s3:: aws-supply-chain-data-* というリソースを持つ専用の Amazon S3 PutObject GetObject バケットのおよびオペレーションにアクセスで	2023 年 9 月 21 日

	きるように管理ポリシーを更新しました。	
リージョンのサポートに関する情報の更新	AWS Supply Chain 需要計画は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とオプトアウトを行います。 AWS Supply Chain	AWS Supply Chain AWS ユーザーはコンソールを使用して、AWS Organizations AWS Supply Chain でのお客様のコンテンツの使用または保存をオプトインおよびオプトアウト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 アジアパシフィック (シドニー) リージョンとヨーロッパ (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 Support に連絡して支援を求め、インスタンスの作成方法に関する内容を更新できるようになりました。	2023 年 4 月 3 日
AWS 管理ポリシーが追加されました。	AWS Supply Chainは、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権限を含め、 AWS AWS フェデレーティッドユーザーにSupply Chain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。