



管理者ガイド

AWS Supply Chain



AWS Supply Chain: 管理者ガイド

Copyright © 2026 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	1
サポートされるブラウザ	1
サポートされている言語	1
.....	1
AWS アカウントのセットアップ	3
にサインアップする AWS アカウント	3
管理アクセスを持つユーザーを作成する	4
を使用するための前提条件 AWS Supply Chain	6
の開始方法 AWS Supply Chain	7
ステップ 1: IAM Identity Center ユーザープロフィールを割り当てる	7
ステップ 2: インスタンスを作成する	8
標準設定を使用する	9
詳細設定を使用する	11
ステップ 3: AWS Supply Chain アプリケーション所有者を選択する	16
AWS Supply Chain ウェブアプリケーションにログオンする	18
の使用 AWS Supply Chain	20
AWS Supply Chain コンソールの使用	20
プロフィールの更新	21
アカウントプロフィールの更新	21
組織プロフィールの更新	21
ユーザーアクセス許可ロールの管理	22
ユーザーの追加	23
ユーザーアクセス許可の更新	23
ユーザーの削除	24
カスタムユーザーアクセス許可ロールの作成	24
インスタンスの削除	25
セキュリティ	27
データ保護	28
によって処理されるデータ AWS Supply Chain	29
オプトアウト設定	29
保管中の暗号化	29
転送中の暗号化	30
キー管理	30
ネットワーク間トラフィックのプライバシー	30

でが許可 AWS Supply Chain を使用する方法 AWS KMS	30
AWS PrivateLink	34
考慮事項	34
インターフェイスエンドポイントの作成	35
エンドポイントポリシーを作成する	35
IAM	36
オーディエンス	36
アイデンティティを使用した認証	37
ポリシーを使用したアクセスの管理	38
が IAM と AWS Supply Chain 連携する方法	40
アイデンティティベースのポリシーの例	44
トラブルシューティング	46
AWS マネージドポリシー	48
AWSSupplyChainFederationAdminAccess	48
ポリシーの更新	50
コンプライアンス検証	52
耐障害性	52
AWS サプライチェーンのログ記録とモニタリング	53
AWS Supply Chain CloudTrail のデータイベント	54
AWS Supply Chain CloudTrail の管理イベント	55
ウェブアプリケーション API	55
を使用したイベントの管理 EventBridge	61
AWS Supply Chain イベント	62
AWS Supply Chain イベントの送信	63
イベントの詳細リファレンス	63
クォータ	66
よくある質問 (FAQ)	68
管理サポート	70
ドキュメント履歴	71
.....	lxxiv

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環として、電話またはテキストメッセージを受け取り、電話キーパッドで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、を保護し AWS IAM アイデンティティセンター、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 マネジメントコンソール](#) としてサインインします。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 アイデンティティセンター ユーザーガイド」の [「AWS 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。

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 アイデンティティセンター 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 アイデンティティセンター 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 アイデンティティセンター ユーザーガイド」の「[Add groups](#)」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 ユーザープロフィールを割り当てる](#)
- [ステップ 2: インスタンスを作成する](#)
- [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 Supply Chain ウェブアプリケーションにログオンする](#)

ステップ 1: IAM Identity Center ユーザープロフィールを割り当てる

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 ユーザープロフィールを接続するか、新しいプロフィー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 マネジメントコンソール。
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。

Continue with email




We'll check if you have an existing user and help create one if you don't.

AWS Supply Chain

Email address

Continue

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 がユーザーに E メールアドレスと一致する場合 – 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、組織で使用する確立済みの IdC インスタンスがある場合に使用できます AWS Supply Chain。

- IdC が既存のユーザーと一致しない場合 – 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 マネジメントコンソール 管理者のみです。AWS Supply Chain インスタンスを作成する AWS マネジメントコンソール 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

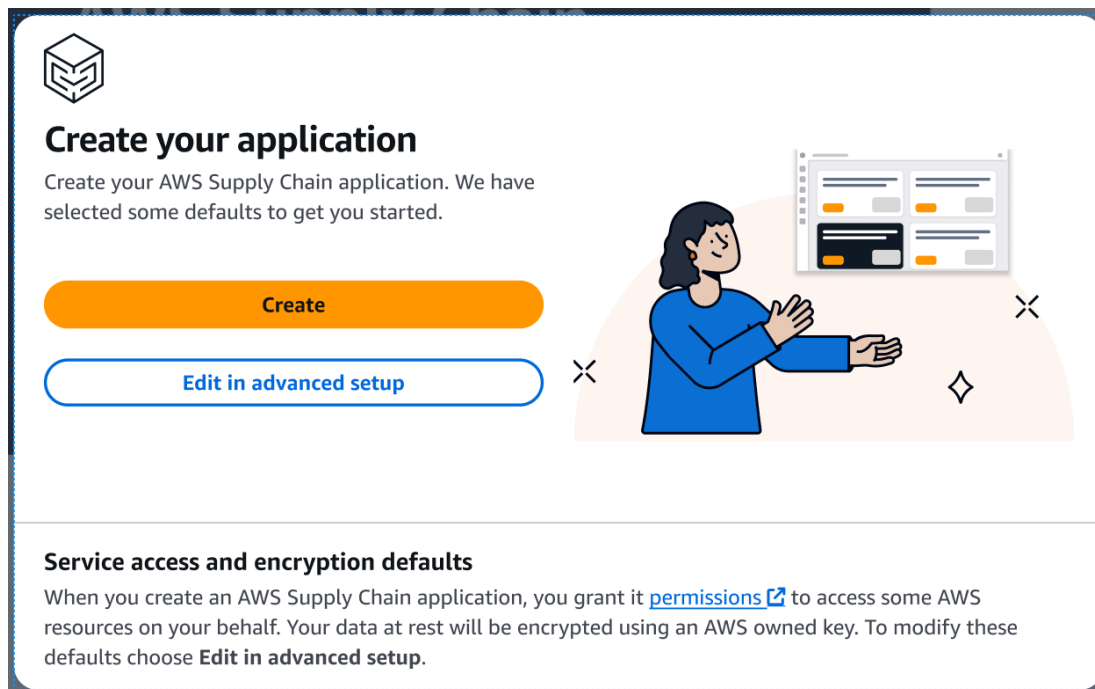
- [標準設定を使用する](#)
- [詳細設定を使用する](#)

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。



Create your application

Create your AWS Supply Chain application. We have selected some defaults to get you started.

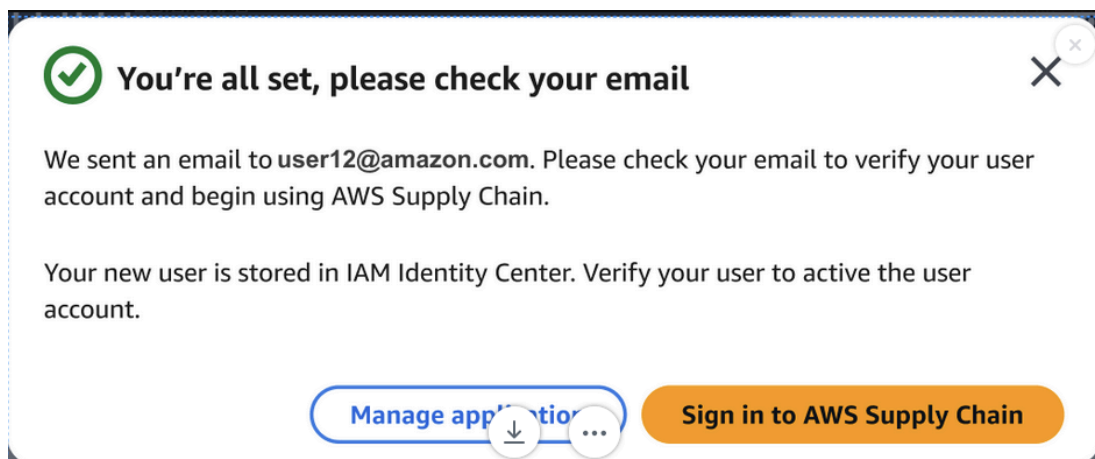
[Create](#)

[Edit in advanced setup](#)

Service access and encryption defaults

When you create an AWS Supply Chain application, you grant it [permissions](#) to access some AWS resources on your behalf. Your data at rest will be encrypted using an AWS owned key. To modify these defaults choose [Edit in advanced setup](#).

確認メッセージが表示されます。



You're all set, please check your email

We sent an email to `user12@amazon.com`. Please check your email to verify your user account and begin using AWS Supply Chain.

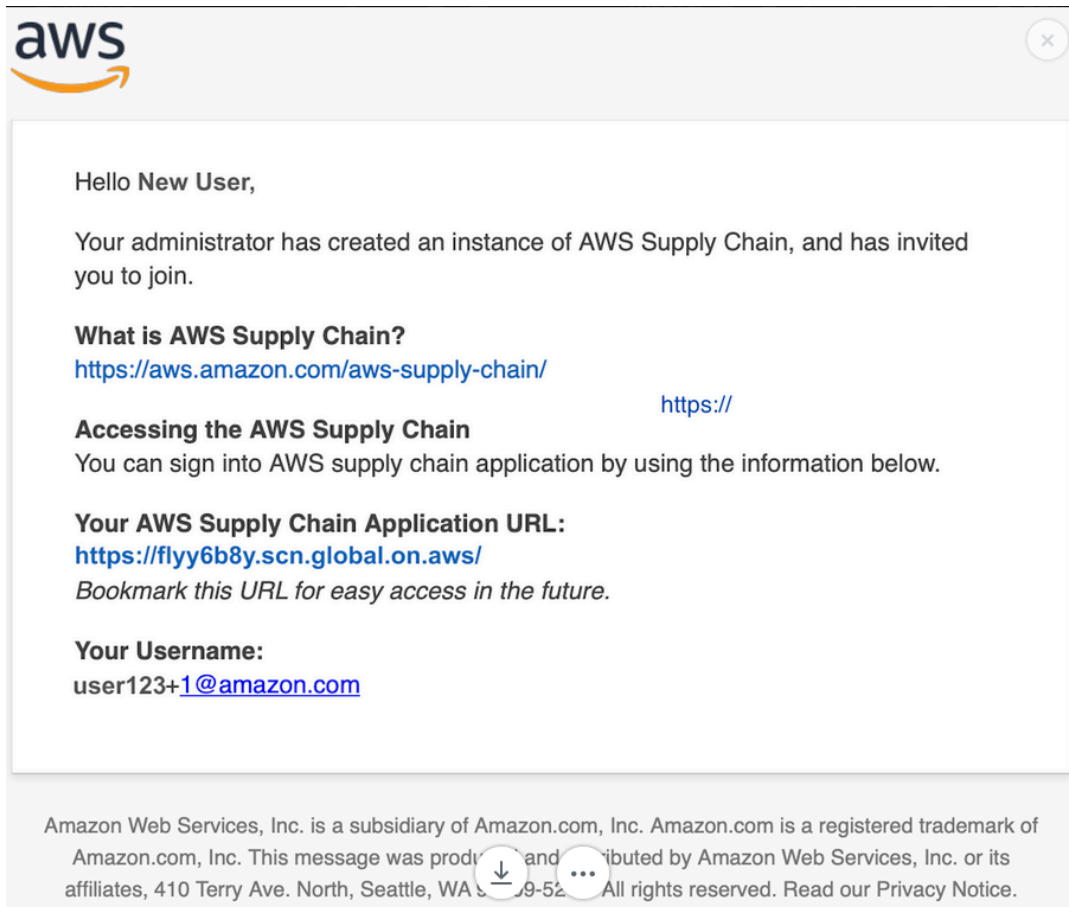
Your new user is stored in IAM Identity Center. Verify your user to active the user account.

[Manage application](#)

[Sign in to AWS Supply Chain](#)

2. Eメールで以下を確認してください。

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

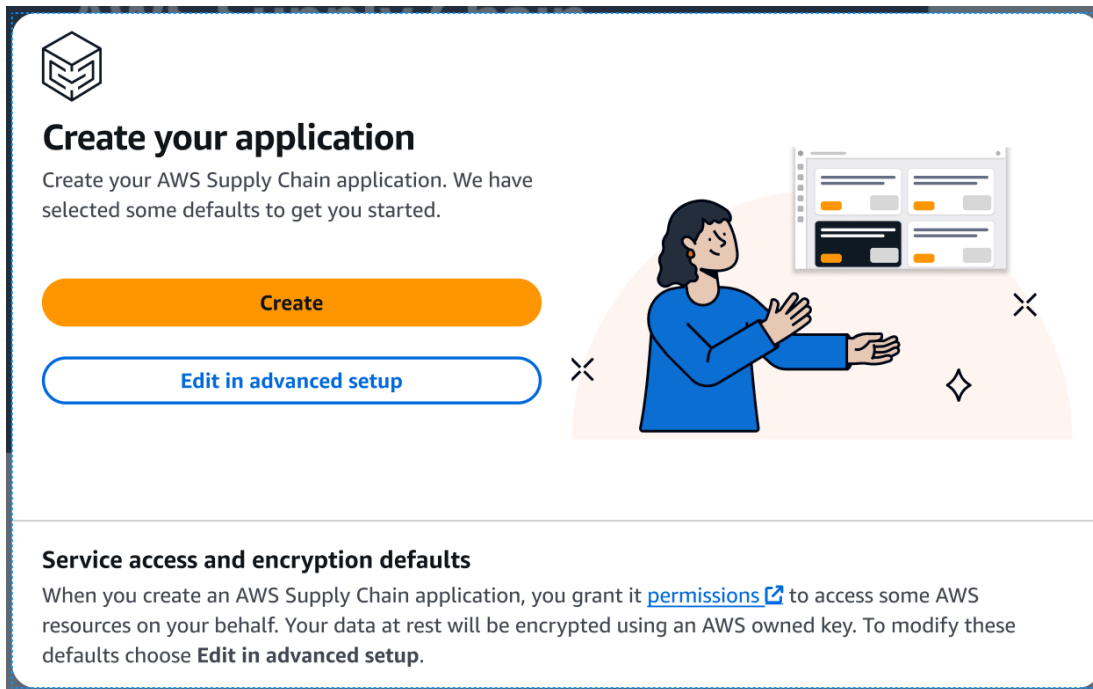


3. 招待メールを受け取ったら、にログインします AWS Supply Chain。「[the section called “AWS Supply Chain ウェブアプリケーションにログインする”](#)」を参照してください。

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. 詳細セットアップで編集を選択します。



Create your application

Create your AWS Supply Chain application. We have selected some defaults to get you started.

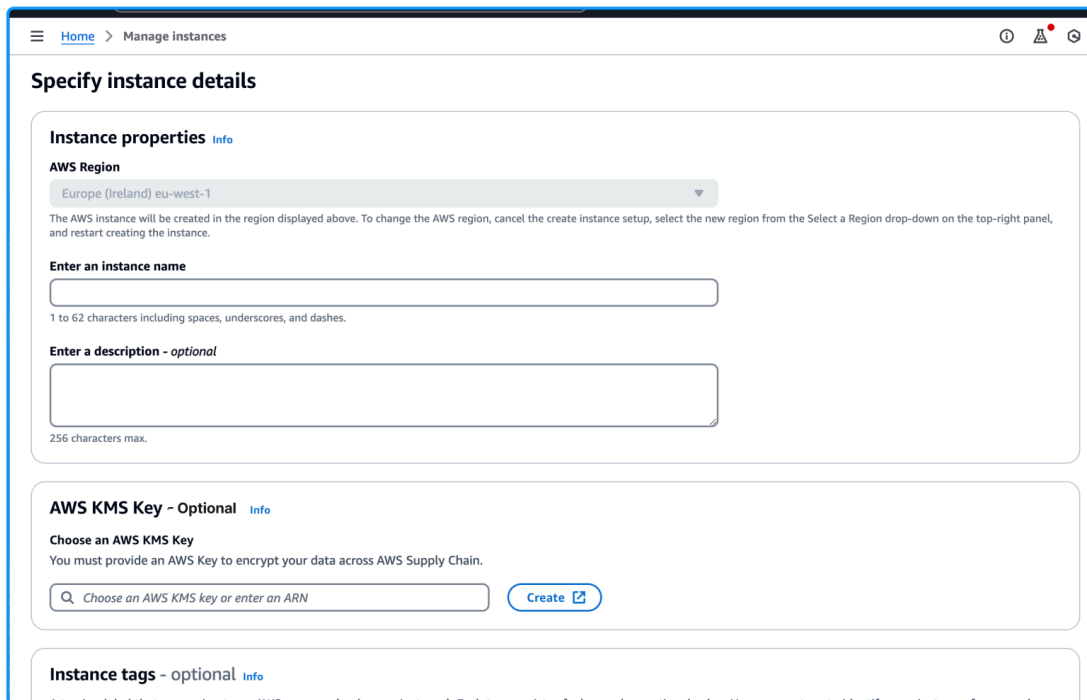
[Create](#)

[Edit in advanced setup](#)

Service access and encryption defaults

When you create an AWS Supply Chain application, you grant it [permissions](#) to access some AWS resources on your behalf. Your data at rest will be encrypted using an AWS owned key. To modify these defaults choose [Edit in advanced setup](#).

インスタンスのプロパティページが表示されます。



Home > Manage instances

Specify instance details

Instance properties [Info](#)

AWS Region

Europe (Ireland) eu-west-1

The AWS instance will be created in the region displayed above. To change the AWS region, cancel the create instance setup, select the new region from the Select a Region drop-down on the top-right panel, and restart creating the instance.

Enter an instance name

1 to 62 characters including spaces, underscores, and dashes.

Enter a description - optional

256 characters max.

AWS KMS Key - Optional [Info](#)

Choose an AWS KMS Key

You must provide an AWS Key to encrypt your data across AWS Supply Chain.

[Create](#)

Instance tags - optional [Info](#)

A key-value label that you assign to an AWS resource (such as an instance). Each tag consists of a key and an optional value. You can use tags to identify your instances, for example,

2. インスタンスの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を入力します (本番稼働用インスタンス、テストインスタンスなど)。

- 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 (本番稼働用、テスト用、UAT など) を定義できます。

Note

S/4 Hana データ接続を使用する場合は、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、 が AWS KMS キー AWS Supply Chain にアクセスできるように KMS ポリシーを更新します。

Note

YourAccountNumber と *YourInstanceID* を AWS アカウント および 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 所有キーの使用は、AWS Supply Chain インスタンスで推奨されるデフォルト設定です。

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. キーの選択に移動します AWS KMS。
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 キーを作成する](#)」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: オフのままにします
 - キー使用許可を定義する: オフのままにする
 - 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。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
```

```

    "Principal": {
      "AWS": "arn:aws:iam::111122223333: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.us-
east-1.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 アプリケーション所有者は、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、次のステップに従って 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。

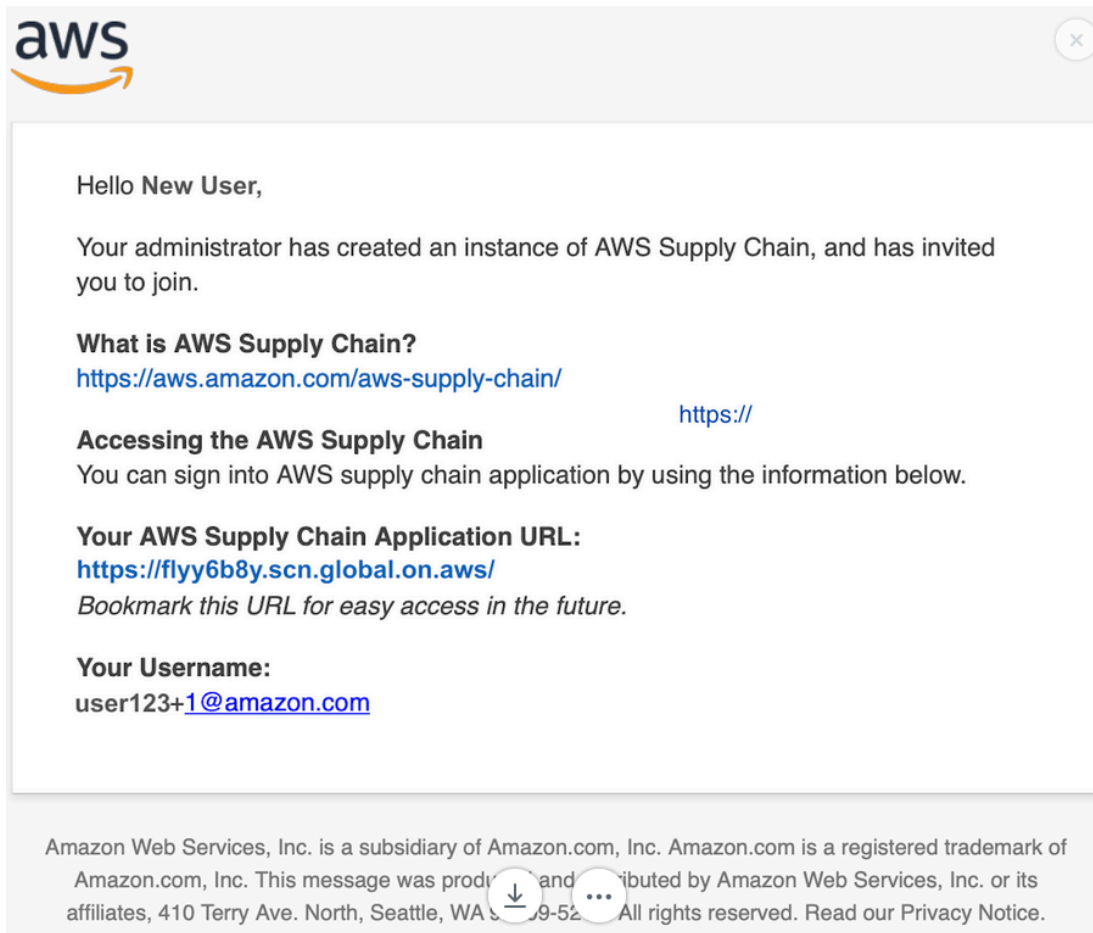
The screenshot shows the AWS Supply Chain console interface. At the top, there is a navigation menu and a title 'AWS Supply Chain'. Below the title, there is a 'Select instance' dropdown menu with 'test' selected and a 'Create instance' button. The main content area is divided into three sections: 'Instance details', 'User access management', and 'Application owner'. The 'Instance details' section shows a table with columns for Instance Name, Status, Sub-domain, Description, AWS KMS Key, and Instance ID. The 'User access management' section shows a 'Manage users' button and a status indicator 'Identity source connected'. The 'Application owner' section shows a 'Select an application owner' button and a dropdown menu with the text 'Select an application owner to setup AWS Supply Chain.' and a close button 'X'.

- (オプション) IAM アイデンティティセンターに移動を選択して、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。

- 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、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が、

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 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](#)
- [プロファイルの更新](#)
- [ユーザーアクセス許可ロールの管理](#)
- [インスタンスの削除](#)

AWS Supply Chain コンソールの使用

コンソールを使用すると、サービスリソースと設定を簡単に管理できます。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

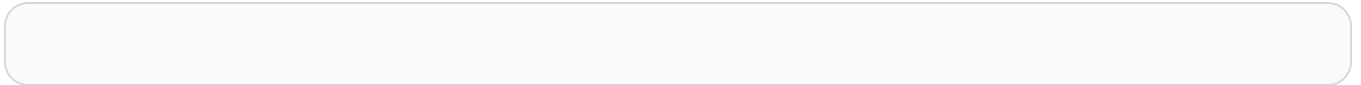
AWS アカウントが AWS 組織のメンバーアカウントで、サービスコントロールポリシー (SCP) が含まれている場合は、組織の SCP がメンバーアカウントに次のアクセス許可を付与していることを確認してください。次のアクセス許可が組織の SCP ポリシーに含まれていない場合、AWS Supply Chain インスタンスの作成は失敗します。

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。

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。

JSON



`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。

プロフィールの更新

アカウントと組織プロフィールは、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。

アカウントプロフィールの更新

アカウントプロフィールを更新するには、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. [アカウントプロフィール] をクリックします。

[アカウントプロフィール] 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。

組織プロフィールの更新

組織プロフィールを更新するには、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
- 需要プランナー – 需要計画を作成、表示、管理、上書き、公開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 ではありません AWS Supply Chain。

トピック

- [ユーザーの追加](#)
- [ユーザーアクセス許可の更新](#)
- [ユーザーの削除](#)
- [カスタムユーザーアクセス許可ロールの作成](#)

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) に追加してから、追加できます AWS Supply Chain。ユーザーを IdC に追加する方法の詳細については、[「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. [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. [保存] を選択します。

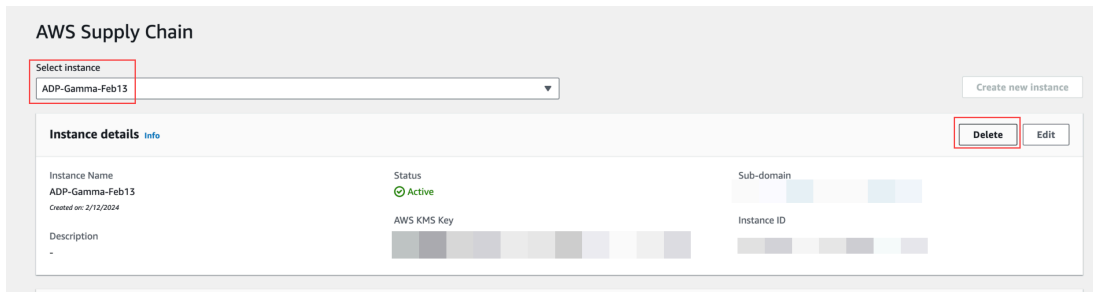
インスタンスの削除

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 管理ポリシー 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 アイデンティティセンターまたは 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 は必須ですが、TLS 1.3 を推奨します。
- 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、API、または SDK を使用して AWS CLI AWS Supply Chain または他の AWS のサービス を操作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。

によって処理されるデータ AWS Supply Chain

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

当社は、[AWS サービス条件](#)に記載されているように AWS Supply Chain、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 AWS Supply Chain してコンテンツ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 内の 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、または保存される前) に、時間制限があり、AWS Supply Chain インスタンスに固有の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 間の転送中に保護されます。

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。

の仮想プライベートクラウド (VPC) エンドポイント AWS Supply Chain は、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。

で が許可 AWS Supply Chain を使用する方法 AWS KMS

AWS Supply Chain には、カスターマネージドキーを使用するための [許可](#) が必要です。

AWS Supply Chain は、CreateInstance オペレーション中に渡される 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。の権限 AWS KMS は、カスタマーアカウントの 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。ユーザーが に追加されると AWS Supply Chain、AWS KMS ポリシーを使用して同じユーザーのリストを拒否することはできません。

AWS Supply Chain は、以下の権限を使用します。

- GenerateDataKey リクエストを 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。
- DescribeKey、CreateGrant、RetireGrant のアクセス許可を追加して、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。その場合、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はアクセス AWS Supply Chain できず、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によって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、および 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 Direct Connect 接続を使用せずに、VPC 内にある AWS Supply Chain かのよう 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ト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
```

インターフェイス・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 リソースの使用を許可する (アクセス許可を付与する) かを制御します。IAM は、追加料金なしで使用できる AWS のサービス です。

トピック

- [オーディエンス](#)
- [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](#)
- [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 ID とアクセスのトラブルシューティング](#)

オーディエンス

AWS Identity and Access Management (IAM) の使用方法は、ロールによって異なります。

- サービスユーザー - 機能にアクセスできない場合は、管理者にアクセス許可をリクエストします (「[AWS Supply Chain ID とアクセスのトラブルシューティング](#)」を参照)。

- サービス管理者 - ユーザーアクセスを決定し、アクセス許可リクエストを送信します (「[が IAM と AWS Supply Chain 連携する方法](#)」を参照)
- IAM 管理者 - アクセスを管理するためのポリシーを作成します (「[のアイデンティティベースのポリシーの例 AWS Supply Chain](#)」を参照)

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。、IAM ユーザー AWS アカウントのルートユーザー、または IAM ロールを引き受けることで認証される必要があります。

AWS IAM アイデンティティセンター (IAM Identity Center)、シングルサインオン認証、Google/Facebook 認証情報などの ID ソースからの認証情報を使用して、フェデレーテッド ID としてサインインできます。サインインの詳細については、「AWS サインイン ユーザーガイド」の「[AWS アカウントにサインインする方法](#)」を参照してください。

プログラムによるアクセスの場合、 は SDK と CLI AWS を提供してリクエストを暗号化して署名します。詳細については、「IAM ユーザーガイド」の「[API リクエストに対するAWS 署名バージョン 4](#)」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、すべての AWS のサービス および リソースへの完全なアクセス権を持つ AWS アカウント root ユーザーと呼ばれる 1 つのサインインアイデンティティから始めます。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。ルートユーザー認証情報を必要とするタスクについては、「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。

フェデレーテッドアイデンティティ

ベストプラクティスとして、人間のユーザーが一時的な認証情報 AWS のサービス を使用して にアクセスするには、ID プロバイダーとのフェデレーションを使用する必要があります。

フェデレーテッド ID は、エンタープライズディレクトリ、ウェブ ID プロバイダー、または ID Directory Service ソースからの認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーテッドアイデンティティは、一時的な認証情報を提供するロールを引き受けます。

アクセスを一元管理する場合は、AWS IAM アイデンティティセンターをお勧めします。詳細については、「AWS IAM アイデンティティセンター ユーザーガイド」の「[IAM アイデンティティセンターとは](#)」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、特定の個人やアプリケーションに対する特定のアクセス許可を持つアイデンティティです。長期認証情報を持つ IAM ユーザーの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。詳細については、IAM ユーザーガイドの「[ID プロバイダーとのフェデレーションを使用してアクセスすることを人間のユーザーに要求する AWS](#)」を参照してください。

[IAM グループ](#)は、IAM ユーザーの集合を指定し、大量のユーザーに対するアクセス許可の管理を容易にします。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を持つアイデンティティであり、一時的な認証情報を提供します。[ユーザーから IAM ロール \(コンソール\) に切り替えるか、または API オペレーションを呼び出すことで、ロールを引き受けることができます。](#) AWS CLI AWS 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 ロールは、フェデレーションユーザーアクセス、一時的な IAM ユーザーのアクセス許可、クロスアカウントアクセス、クロスサービスアクセス、および Amazon EC2 で実行するアプリケーションに役立ちます。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。

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、ID またはリソースに関連付けられたときにアクセス許可を定義します。は、プリンシパル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。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、ポリシーを使用して、どのプリンシパルがどのリソースに対して、どのような条件でアクションを実行できるかを定義することで、誰が何にアクセスできるかを指定します。

デフォルトでは、ユーザーやロールにアクセス許可はありません。IAM 管理者は IAM ポリシーを作成してロールに追加し、このロールをユーザーが引き受けられるようにします。IAM ポリシーは、オペレーションの実行方法を問わず、アクセス許可を定義します。

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のポリシーは、アイデンティティ (ユーザー、グループ、またはロール) にアタッチできる JSON アクセス許可ポリシードキュメントです。これらのポリシーは、アイデンティティがどのリソースに対してどのような条件下でどのようなアクションを実行できるかを制御します。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、インラインポリシー (単一の ID に直接埋め込む) または管理ポリシー (複数の ID にアタッチされたスタンドアロンポリシー) にすることができます。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。例としては、IAM ロール信頼ポリシーや Amazon S3 バケットポリシーなどがあります。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。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。

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。

その他のポリシータイプ

AWS は、より一般的なポリシータイプによって付与されるアクセス許可の最大数を設定できる追加のポリシータイプをサポートしています。

- アクセス許可の境界 – アイデンティティベースのポリシーで IAM エンティティに付与することのできるアクセス許可の数の上限を設定します。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 (SCP) - AWS Organizations内の組織または組織単位の最大のアクセス許可を指定します。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](#)」を参照してください。
- リソースコントロールポリシー (RCP) – は、アカウント内のリソースで利用できる最大数のアクセス許可を定義します。詳細については、「AWS Organizations ユーザーガイド」の「[リソースコントロールポリシー \(RCP\)](#)」を参照してください。

- セッションポリシー – ロールまたはフェデレーションユーザーの一時セッションを作成する際にパラメータとして渡される高度なポリシーです。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アクセス許可を理解するのがさらに難しくなります。が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、で利用できる IAM 機能について説明します AWS Supply Chain。

で利用できる IAM 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	あり
リソースベースのポリシー	なし
ポリシーアクション	あり
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	あり
サービスリンクロール	いいえ

AWS Supply Chain および他の 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、ユーザーグループ、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。

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。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の[アイデンティティベースのポリシーの例 AWS Supply Chain](#)。

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コントロールできます。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、[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、全体のアカウント、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。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。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の [アイデンティティベースのポリシーの例 AWS Supply Chain](#)。

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。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。リソースレベ

ルのアクセス許可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の[アイデンティティベースのポリシーの例 AWS Supply Chain](#)。

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 要素は、定義された基準に基づいてステートメントが実行される時期を指定します。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。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の[アイデンティティベースのポリシーの例 AWS Supply Chain](#)。

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

一時的な認証情報は、AWS リソースへの短期的なアクセスを提供し、フェデレーションまたはスウィッチロールの使用時に自動的に作成されます。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 AWS 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「[IAM の一時的な認証情報](#)」および「[AWS のサービスと IAM との連携](#)」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

転送アクセスセッション (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 へのリクエストをリクエストする を使用します。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。

のサービスロール AWS Supply Chain

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。AWS Supply Chain が指示する場合にのみ、サービスロールを編集します。

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。サービスにリンクされた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。

のアイデンティティベースのポリシーの例 AWS Supply Chain

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、リソースに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

アイデンティティベースのポリシーは、アカウント内の AWS Supply Chain リソースを作成、アクセス、または削除できるかどうかを決定します。これらのアクションでは、AWS アカウントに費用が発生する場合があります。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 – ユーザーとワークロードにアクセス許可の付与を開始するには、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することで、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 ポリシーでアクセス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。たとえば、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 を通じて使用されている場合に 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 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 アクセスアナライザー 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 アクセスアナライザー 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、MFA をオンにしてセキュリティを強化します。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 以外のユーザーに自分の 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 マネジメントコンソール が通知した場合、管理者に問い合わせる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、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と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。Mary には、ロールをサービスに渡すアクセス許可がありません。

```
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。サインイン資格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 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:

- [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](#) [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 管理ポリシー 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、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るように、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 は、新しい が起動されるか、新しい API オペレーション AWS のサービス が既存のサービスで使用できるようになったときに、AWS 管理ポリシーを更新する可能性が高くなります。

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 フェデレーテッドユーザーに 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ために必要なアクセス許可が含まれます。このポリシーは、IAM Identity Center ユーザーとグループに対する管理アクセス許可を提供し、によって作成されたロールに AWS Supply Chain アタッチされます。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ており、管理者 APIs に対する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。チャンネル、チャンネルのメンバー、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。チャン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、IAM アイデンティティセンターでの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: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-supply-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 マネジメントコンソールの「[AWSSupplyChainFederationAdminAccess](#)」を参照してください。

AWS Supply Chain AWS 管理ポリシーの更新

次の表に、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 AWS Supply Chain 管理ポリシーの更新の詳細を示します。このページの変更に関する自動アラートについては、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、マネージドポリシーを更新して、フェデレーテッドユーザーがカスタマーマネージド KMS キー (CMKs)。	2025 年 10 月 30 日
AWSSupplyChainFederationAdminAccess – ポリシーの更新	AWS Supply Chain は マネージドポリシーを更新し、フェデレーテッドユーザーが IAM アイデンティティセンターの ListApplicationAssignments、DescribeInstance、および DescribeApplicationAssignmentConfiguration	2024 年 12 月 10 日

変更	説明	日付
AWSSupplyChainFederationAdminAccess – ポリシーの更新	<p>n オペレーションにアクセスできるようにしました。</p> <p>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。</p>	2023 年 11 月 1 日
AWSSupplyChainFederationAdminAccess – ポリシーの更新	<p>AWS Supply Chain は、リソース <code>arn:aws:s3::aws-supply-chain-data-*</code> 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。</p>	2023 年 9 月 21 日
AWSSupplyChainFederationAdminAccess – 新しいポリシー	<p>AWS Supply Chain は、フェデレーテッドユーザーが 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。</p>	2023 年 3 月 1 日
AWS Supply Chain が変更の追跡を開始しました	<p>AWS Supply Chain は、AWS 管理ポリシーの変更の追跡を開始しました。</p>	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 Programs Assurance」](#)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 CSPM](#) – 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ゾーンを提供します。アベイラビリティゾーンは、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 サプライチェーンやその他の 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 サプライチェーンを監視し、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、呼び出し元のソース IP アドレス、および呼び出しの発生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](#)」を参照してください。

Note

次の点に注意してください AWS Supply Chain。

- アクセス権限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、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ログ記録しません。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、データイベントをログに記録する [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ログに記録します。
 1. データイベントをログに記録するには、[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、データイベントをログ記録するリソースのタイプを選択します。
 3. 使用するログセクタ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、すべての readOnly イベントをログに記録したり、すべての writeOnly イベントをログに記録したり、カスタムログセクタ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ログに記録するには AWS CLI、`--advanced-event-selectors` パラメータを設定して `eventCategory` フィールドを `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しないでください。

ユーザーロール

以下の APIs は、 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:CreateSap0DataConnection
scn:CreateUpdateDatasetSchemaJob
scn>DeleteConnection
scn>DeleteDataflow
scn>DeleteExtractFlows
scn>DeleteSap0DataConnection
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

の 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
```

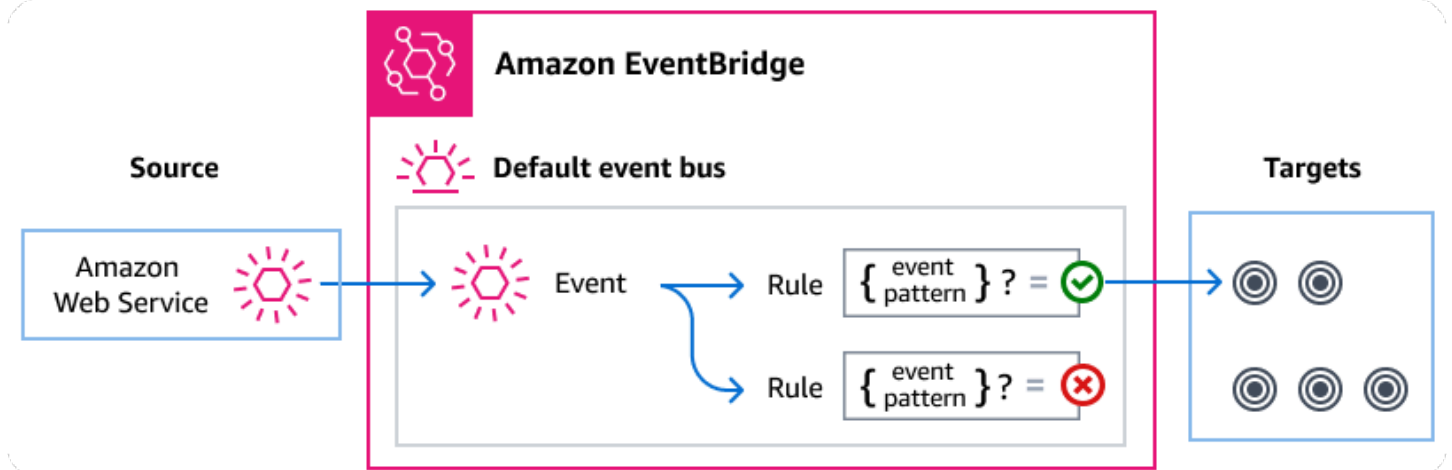
を使用した AWS Supply Chain イベントの管理 Amazon EventBridge

を使用すると EventBridge、他の 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するサーバーレスサービスであり、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、イベントを受信して、ゼロ個以上の送信先 (ターゲット) に配信するルーターです。イベントを受信されると、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がターゲットに 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、イベントバスで受信した各イベント EventBridge と一致するイベントパターンが含まれています。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 `aws.supplychain` です。
- (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 イベントと一致します 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「[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 に設定されず 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。
- 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": "accountID",
  "time": "2024-03-30T12:26:13Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "version": "1.0",
    "instanceId": "instanceID",
    "flowArn": "arn:aws:scn:region:accountID: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	10	いいえ
<div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> Note</p> <p>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。</p> </div>		
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 アイデンティティセンター 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 アイデンティティセンター 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
	<p>いては、AWS 「Organizations の委任管理者」を参照してください。</p> <p>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。</p>

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 マネジメントコンソール](#)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 管理ポリシーの更新	AWS Supply Chain は、マネージドポリシーを更新して、フェデレーティッドユーザーがカスタマーマネージド KMS キー (CMKs)。	2025 年 10 月 30 日
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 マネージドポリシーを更新し、フェデレーティッドユーザーが IAM Identity Center の ListApplicationAssignments、DescribeInstance、および DescribeApplicationGetApplicationAssignmentConfiguration オペレーションにアクセスできるようにしました。	2024 年 12 月 10 日
KMS ポリシーの更新	が AWS KMS キー AWS Supply Chain にアクセスできるように KMS 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	2024 年 2 月 26 日

Supply Chain を使用して にアクセスできます。

[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: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。