aws

管理者ガイド

Amazon Connect の決定事項

Amazon Connect の決定事項: 管理者ガイド

Table of Contents

Amazon Connect の決定とは

Amazon Connect Decisions は、AI チームメイトと連携するサプライチェーンの計画とインテリジェンスのソリューションです。チームは需要シグナルをコンセンサス予測に調整し、制約を考慮した供給計画を生成し、運用を積極的にモニタリングして問題を防止し、問題を解決し、継続的な改善の根本原因を特定します。

AI チームメイトは、作業方法に適応します。これは、運用手順とルール、既存のシステムとの統合、実践者の意思決定からの学習によって決まります。Amazon サプライチェーンの専門知識を活用して、1 日目から効果的な計画と推奨事項を提供します。

調整を処理してアクションを実行する AI エージェントチームを率いて、サービスレベルと運転資本効率を促進する戦略的意思決定に集中できるようにします。

利点

ビジネスに適応する

AI チームメイトは、ビジネス、システム、意思決定に適応し、既存のワークフロー内で迅速に変革を実現します。運用手順とビジネスルールに基づいて、チームメイトは既存の計画システムと ERP システムを使用します。プランナーの決定から学び、優先順位に合わせ、知識を体系化し、時間の経過とともに運用が改善し、すべてのチームメンバーがより効果的になります。

今後の一歩先を行く

24 時間 365 日の調整作業を処理する AI エージェントチームを率い、需要シグナルの伝達、制約対応計画の生成、承認されたアクションの実行を行います。また、チームメイトは、数千の SKUs、問題になる前に重要なものを明らかにします。プランナーは、ビジネスの成果を促進する戦略的意思決定を通じて、事後対応型戦闘から事前対応型計画に移行し、より効果的な運用を実行し、サービスレベルを改善します。

1 日目から信頼を構築する

AI チームメイトは、30 年以上にわたって 400Mを超える Amazon SKUs を監督し、専用のサプライチェーンツールを備えたサイエンスに支えられています。チームは、世界でも最も複雑なサプライチェーンネットワークの 1 つによって評価されたドメインの専門知識を活用し、信頼できる説明可能な明確な推論 out-of-the-box ですぐに実用的なインサイトとレコメンデーションを提供します。

機能

アダプティブインテリジェンス

AI チームメイトは、パターンの監視、重要なことの検出、アクションの推奨、承認された決定の実行など、継続的なループを通じてすべての計画と決定から学習します。これにより、プランナーが離れたときの知識が体系化され、専門知識が維持されます。新規メンバーは初日から生産性が高くなり、手動の再トレーニングなしで成果が向上します。

需要インテリジェンス

AI チームメイトは、Amazon データでトレーニングされた 18 以上の予測ツールと基盤モデルを動的に調整し、SKU レベルで自律的に最適化します。履歴が限られている場合でも、1 日目から正確な予測を生成します。精度を継続的にモニタリングしながら、コンセンサスプランニングを通じて統計予測、顧客コミットメント、部門間のインプットを調整します。

インテリジェンスの提供

AI チームメイトは、将来を見据えた供給計画 (プレビュー) を作成し、影響別にランク付けされた戦略的意思決定に例外をインテリジェントにクラスター化します。ネットワーク全体で制約対応計画の最適化モデルを実行します。オペレーションを 24 時間 365 日モニタリングし、重要なことを明らかにし、承認された決定を既存のシステムに直接実行して、サイクルを数週間から数時間に短縮します。

エージェントオンボーディング

AI を活用したオンボーディングエージェントは、自然言語の会話を通じてセットアップを案内します。JDBC または Amazon S3 を介してフラグメント化されたデータを接続し、Connect Decisions に備えて準備し、予測に影響を与える前に問題に自動的にフラグを付けます。リアルタイムプレビューを使用して、ビジネスルールとポリシーをプレーン言語で設定します。数か月ではなく数週間で運用できるようになります。

開始方法

このセクションでは、Amazon Connect Decisions 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、Amazon Connect Decisions ウェブアプリケーションへのログインについて説明します。

Amazon Connect Decisions を使用するための前提条件

Amazon Connect Decisions インスタンスを作成する前に、次の手順を完了してください。

- AWS アカウントがある。 AWS アカウントを作成するには、「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 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。
- IAM Identity Center インスタンスは、Amazon Connect Decisions 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。Amazon Connect Decisions は、米国東部 (バージニア北部) 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。
- Amazon Connect Decisions インスタンスが既存の IAM アイデンティティセンター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。
- Amazon Connect Decisions 管理者として割り当てる IAM アイデンティティセンターインスタンスには、少なくとも 1 人のユーザーが必要です。アクティブディレクトリを IAM Identity Center 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。
- Amazon Connect Decisions にアクセスする必要があるユーザーを IAM アイデンティティセンターに追加します。
- インスタンスを作成するには、 AWS Key Management Service (AWS KMS) が必要です。Amazon Connect Decisions はこの AWS KMS キーを使用して、Amazon Connect Decisions に含まれるすべてのデータを暗号化します。KMS キーの詳細については、 AWS「キーの作成」を参照してください。
- アクション機能を有効にする場合は、関連するデータを維持するために使用するシステムへの接続を設定し、使用する Amazon Connect Decisions の認証情報を提供する必要があります。詳細については、お問い合わせください。

Amazon Connect Decisions でサポートされているブラウザ

Amazon Connect Decisions 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

Amazon Connect Decisions でサポートされている言語

Amazon Connect Decisions では、次の言語がサポートされています。

- 英語 (米国)

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。

AWS アカウントにサインアップする

AWS アカウントがない場合は、次の手順を実行してアカウントを作成します。

AWS アカウントにサインアップするには

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。

AWS アカウントにサインアップすると、AWS アカウントのルートユーザーが作成されます。ルートユーザーは、アカウントのすべての AWS サービスとリソースにアクセスできます。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

AWS アカウントにサインアップしたら、 AWS アカウントのルートユーザーを保護し、 AWS IAM Identity Center を有効にして、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。

AWS アカウントのルートユーザーを保護する

1. [ルートユーザー] を選択し、 AWS アカウントの E メールアドレスを入力することで、アカウント所有者として AWS マネジメントコンソール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のヘルプは、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」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、IAM Identity Center AWS ユーザーガイドの「IAM Identity Center の有効化」を参照してください。 AWS
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。

IAM Identity Center ディレクトリを ID ソースとして使用する方法のチュートリアルについては、IAM Identity Center ユーザーガイドの「デフォルトの IAM Identity Center ディレクトリを使用してユーザーアクセスを設定する」を参照してください。 AWS

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、「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。 AWS

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。

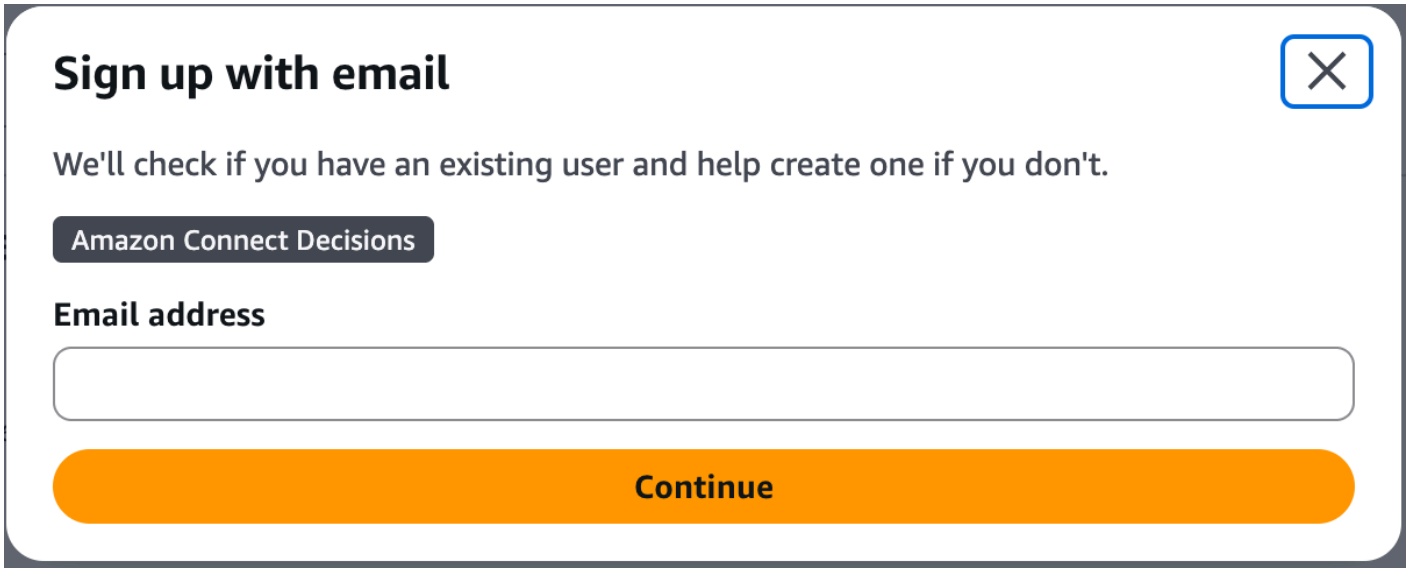
   手順については、AWS IAM Identity Center ユーザーガイドの「アクセス許可セットの作成」を参照してください。
2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

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

AWS Identity Center 統合の設定

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

1. Amazon Connect Decisions コンソールを開きます。メイン AWS マネジメントコンソールから Amazon Connect Decisions」を検索することもできます。
2. 必要に応じて、コンソールの上部にあるリージョンの選択を選択して、AWS 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. Amazon Connect Decisions インスタンスの作成を選択します。通知が表示されます。



4. E メールアドレスを入力し、続行を選択します。IdC は、E メールが既存のユーザーと一致するかどうかを確認します。
5. 次のいずれかを行います。
   - IdC がユーザーに 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、組織に Amazon Connect Decisions に使用する確立された IdC インスタンスがある場合に使用できます。

   - 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、Amazon Connect Decisions 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。「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。「詳細設定を使用する」を参照してください。

IAM Identity Center と組み合わせて使用すると、Amazon Connect Decisions は IAM Identity Center ディレクトリから「username」フィールドと「email」フィールドを取得します。これらの属性はいずれも Amazon Connect Decisions インスタンスにネイティブに保存されず、常に実行時に取得されます。Amazon Connect Decisions は、デフォルトで AWS 所有の KMS キーを使用して、保管中のこれらの ID 属性を暗号化します。カスタマーマネージド KMS キーは、Amazon Connect Decisions ではサポートされていません。 AWS IAM Identity Center インスタンスでユーザーを削除すると、Amazon Connect Decisions はそのユーザーもインスタンスから削除します。

Amazon Connect Decisions インスタンスの管理

Amazon Connect Decisions 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。

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。Amazon Connect Decisions 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、アイデンティティベースのポリシー例にリストされているすべてのアクセス許可が必要です。この管理者は、Amazon Connect Decisions を管理するために、IAM ユーザーを Amazon Connect Decisions 管理者として招待する必要があります。

以下のページでは、インスタンスを作成および削除するプロセスについて詳しく説明します。

インスタンスの作成

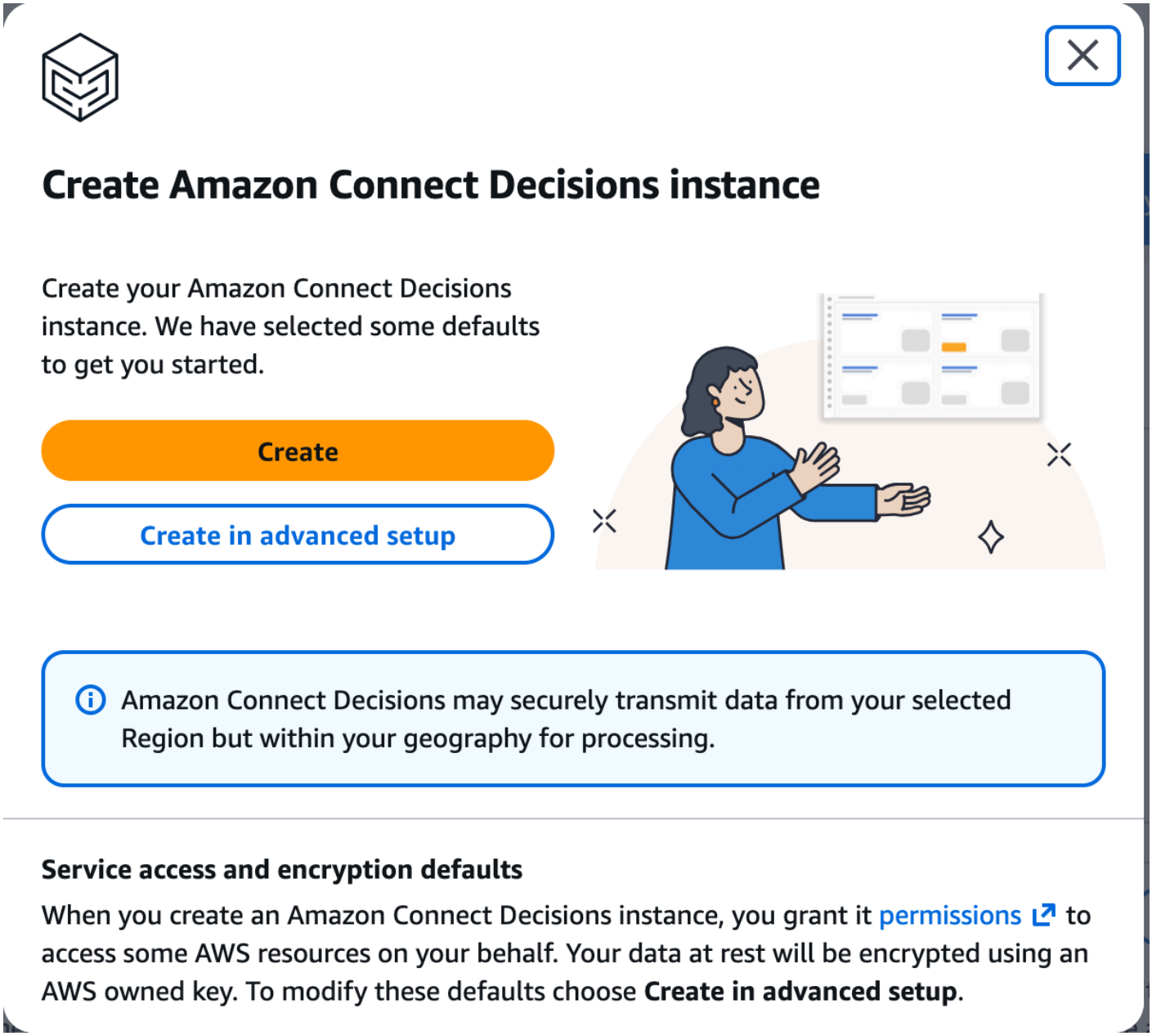
インスタンスは、標準設定または詳細設定の 2 つの方法のいずれかを使用して作成します。標準設定では、プリセットパラメータを使用してインスタンスをすばやく作成する自動プロセスを使用します。詳細設定では、独自のパラメータを設定してインスタンスをカスタマイズできます。

標準設定の使用

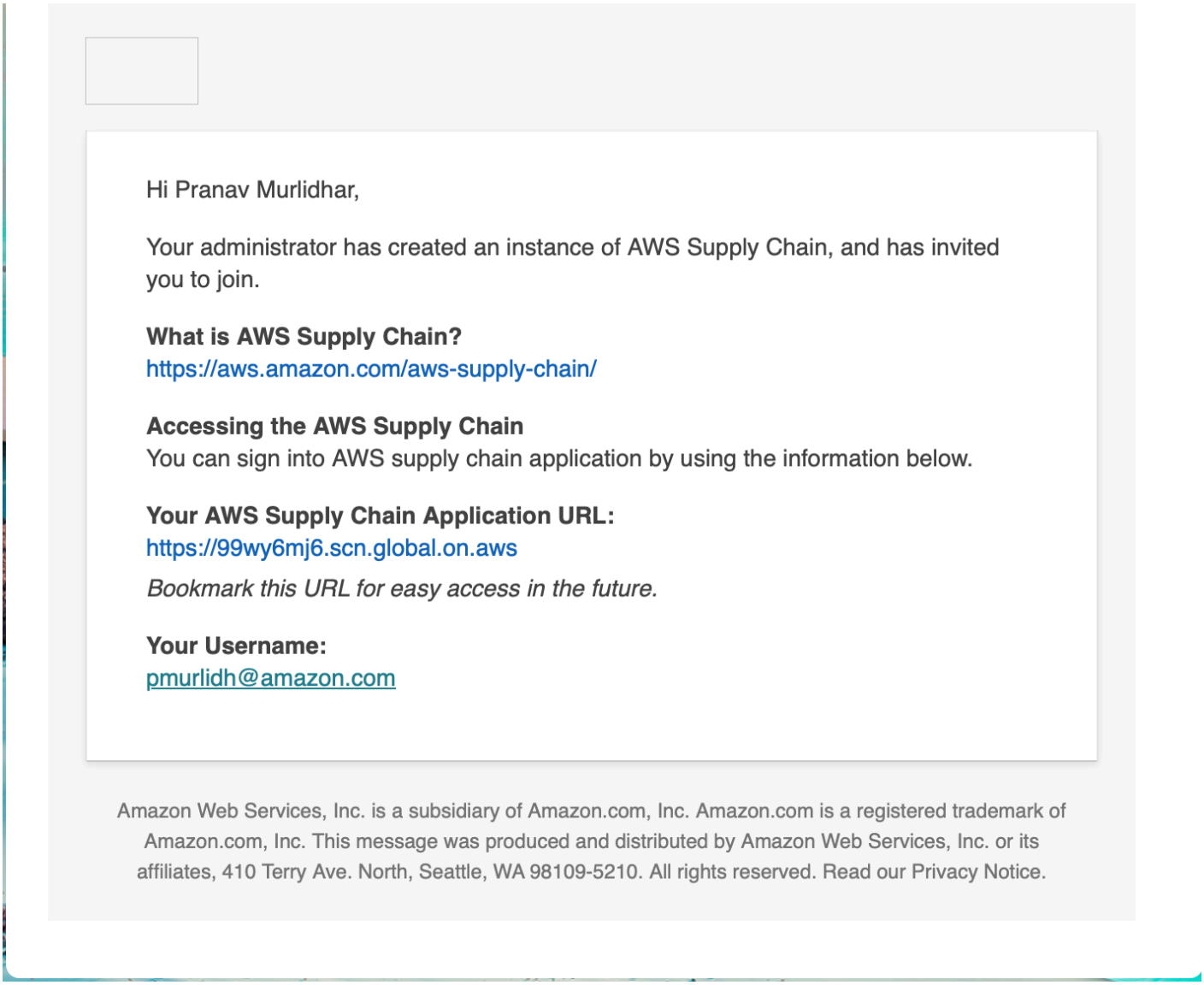
標準設定では、デフォルトのセキュリティおよび暗号化設定を使用して Amazon Connect Decisions インスタンスが作成されます。インスタンスは AWS 地理的リージョンで動作します。リージョンの詳細については、「IAM ユーザーガイド」の「リージョンとエンドポイント」およびAWS 「 全般のリファレンス」の「リージョンエンドポイント」を参照してください。

プリセットパラメータの標準設定を使用して Amazon Connect Decisions 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。



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。

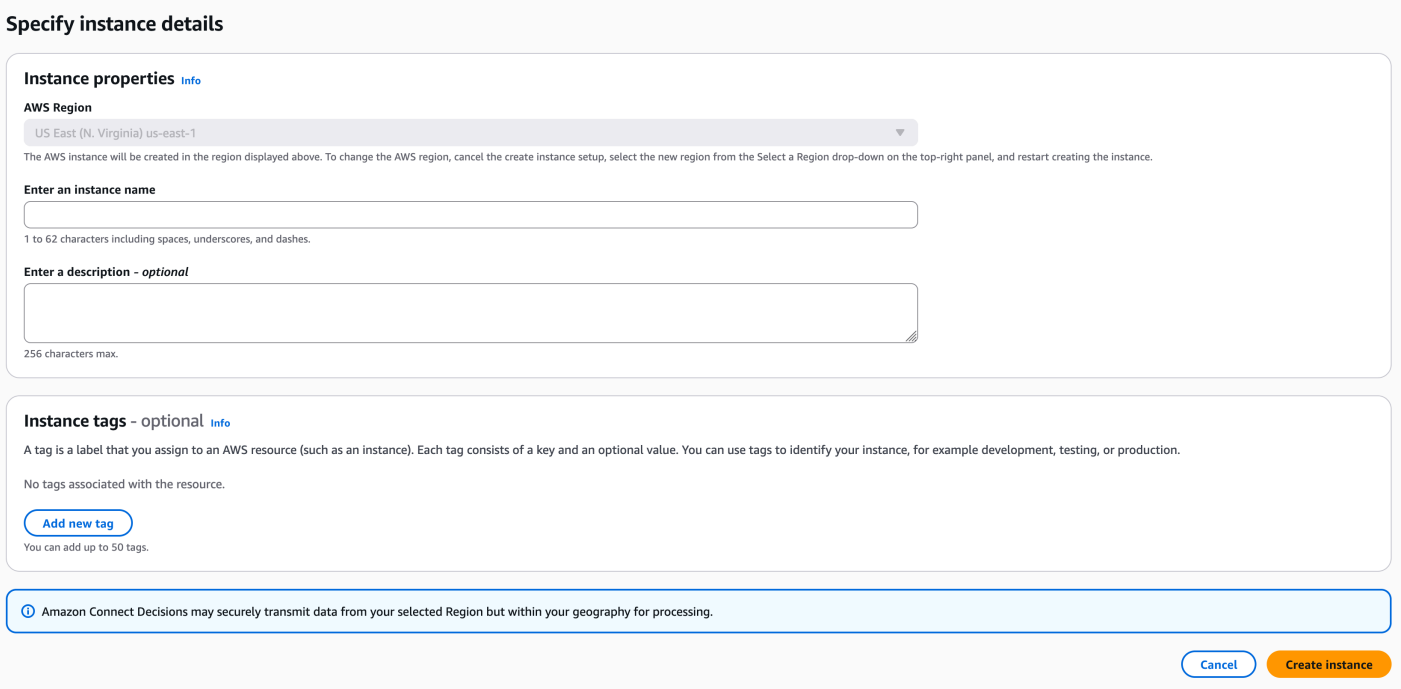


3. 招待メールを受信したら、Amazon Connect Decisions にログオンします。Amazon Connect Decisions ウェブアプリケーションにログオンする」を参照してください。

詳細設定の使用

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 Amazon Connect Decisions 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作成を選択します。
2. インスタンスのプロパティページが表示されます。



3. 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 – Amazon Connect Decisions インスタンス (本番稼働用インスタンス、テストインスタンスなど) の説明を入力します。
   - インスタンスタグ – 識別に使用できるタグをインスタンスに追加できます。たとえば、タグを追加して、作成するインスタンスのタイプ (本番稼働用、テスト用、UAT など) を定義できます。
4. インスタンスの作成 を選択します。

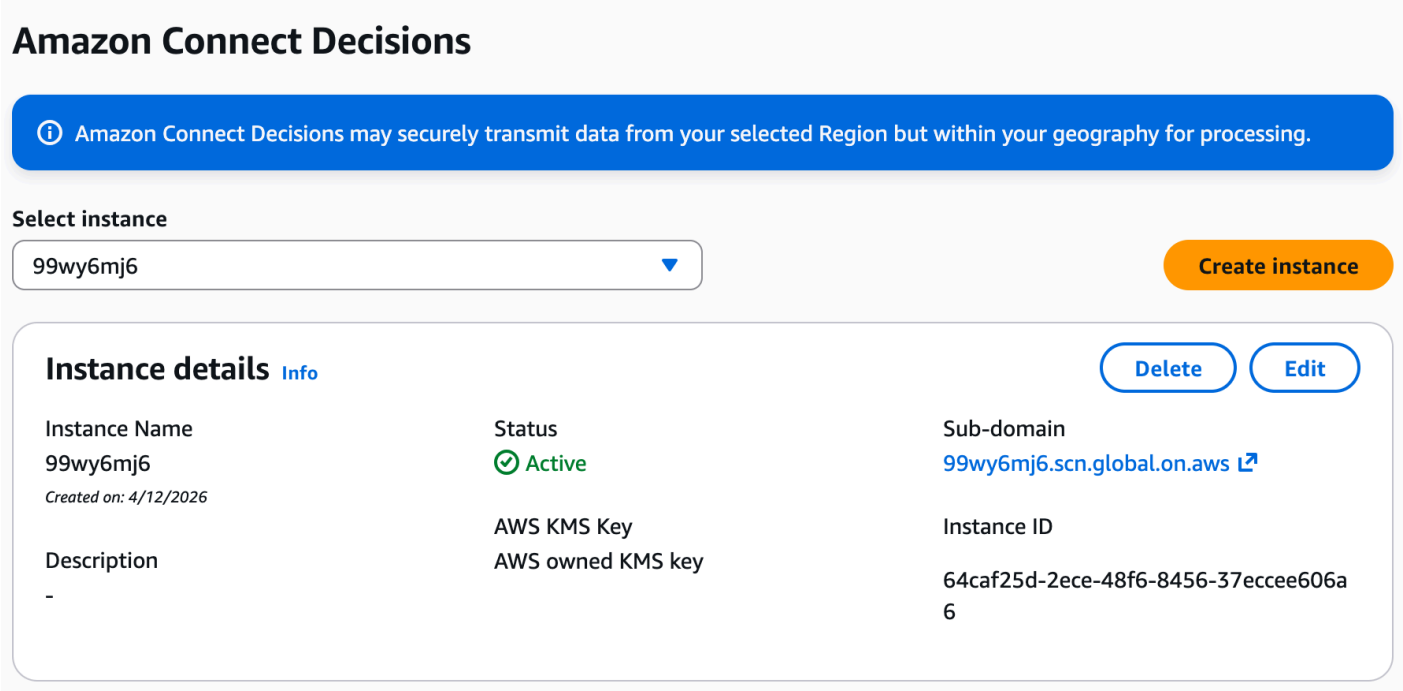
インスタンスの削除

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. https://console.aws.amazon.com/scn/home で Amazon Connect Decisions コンソールを開きます。

2. Amazon Connect Decisions 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. Amazon Connect 決定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。

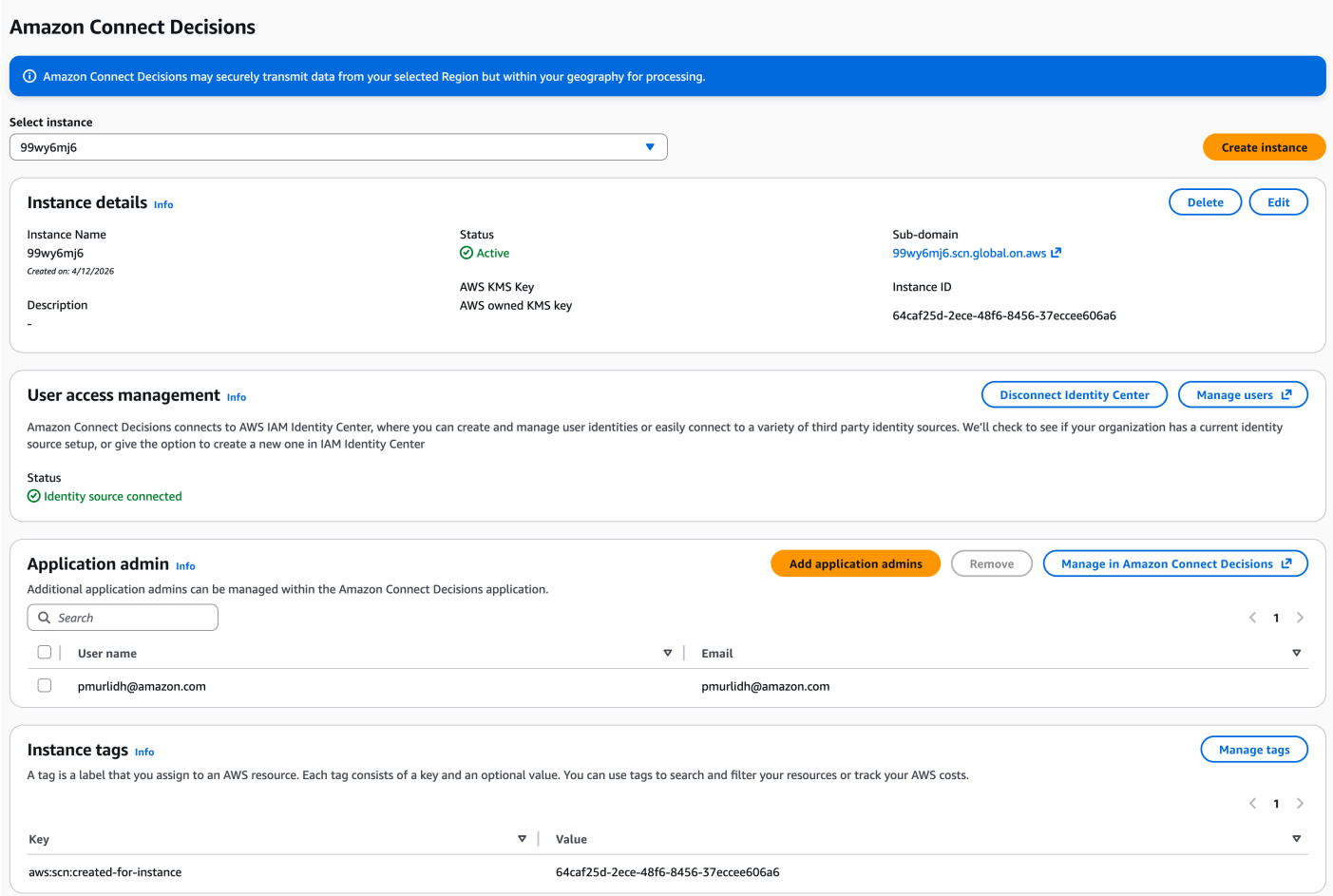
アプリケーション管理者を選択する

AWS コンソール管理者は、Amazon Connect Decisions ウェブアプリケーションへのアクセスを管理する Amazon Connect Decisions アプリケーション管理者を選択します。Amazon Connect Decisions アプリケーション管理者は、Amazon Connect Decisions 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または削除できます。

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 Amazon Connect Decisions アプリケーション管理者を選択します。

1. Amazon Connect Decisions コンソールダッシュボードを開きます。

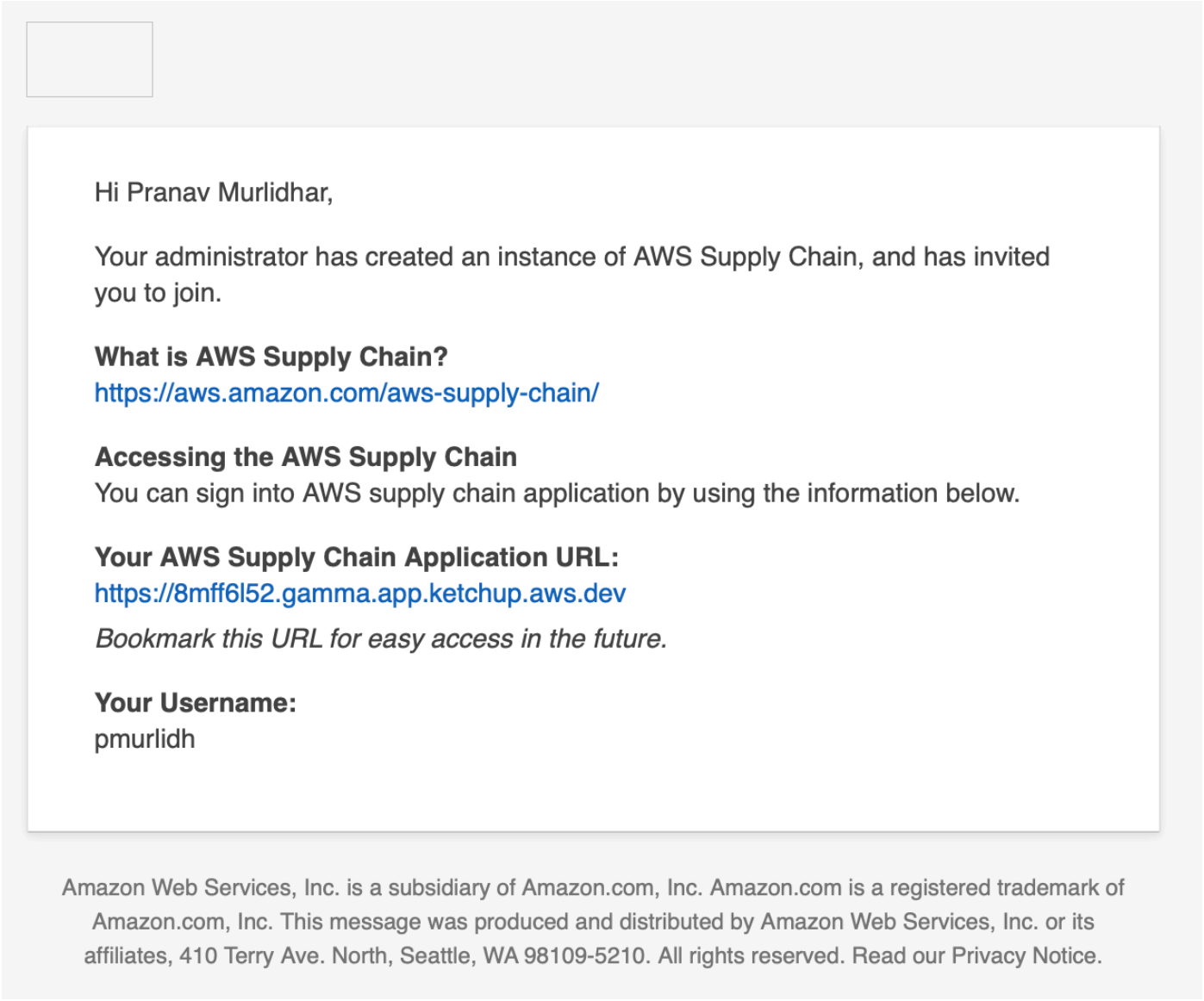
2. 「アプリケーション管理者の選択」に移動し、Amazon Connect Decisions アプリケーション管理者になるユーザーを選択します。検索結果には、検索条件に一致するユーザーのみが表示されます。



3. (オプション) IAM 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**
>
> Amazon Connect 決定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。Amazon Connect Decisions でアプリケーション管理者としてグループを追加することはできません。

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



Hi Pranav Murlidhar,

Your administrator has created an instance of AWS Supply Chain, and has invited you to join.

What is AWS Supply Chain?
https://aws.amazon.com/aws-supply-chain/

Accessing the AWS Supply Chain
You can sign into AWS supply chain application by using the information below.

Your AWS Supply Chain Application URL:
https://8mff6l52.gamma.app.ketchup.aws.dev
Bookmark this URL for easy access in the future.

Your Username:
pmurlidh

Amazon Web Services, Inc. is a subsidiary of Amazon.com, Inc. Amazon.com is a registered trademark of Amazon.com, Inc. This message was produced and distributed by Amazon Web Services, Inc. or its affiliates, 410 Terry Ave. North, Seattle, WA 98109-5210. All rights reserved. Read our Privacy Notice.

Amazon Connect Decisions ウェブアプリには、アプリケーション管理者の下にユーザーが表示されます。

インスタンスへのアクセス

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。

Amazon Connect Decisions 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、 AWS アカウントの Amazon Connect Decisions リソースの詳細を一覧表示および表示できます。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。

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。

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

1. E メールのリンクを選択するか、Amazon Connect Decisions コンソールダッシュボードのサブドメインでウェブ URL を選択します。
2. Amazon Connect Decisions 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。
3. 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。
4. 追加した各ユーザーは、Amazon Connect Decisions へのリンクを含む E メールメッセージを受信するか、リンクをコピーしてユーザーに送信できます。

ログインに成功すると、パーソナライズされたホームページに移動します。ホームページをよりよく理解するには、ユーザーガイドの「ホームページを理解する」を参照してください。

アクセスコントロール

Amazon Connect Decisions は、インスタンス内で誰がどのデータにアクセスしてどのアクションを実行できるかを正確に制御できるエンタープライズグレードのアクセス管理を提供します。これにより、組織が必要とするセキュリティおよびコンプライアンス標準を維持しながら、ユーザーの責任に関連する情報のみが表示されるようになります。

ロールとアクセス許可の概要

Amazon Connect Decisions 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。Amazon Connect Decisions 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

Admin

Role name
Admin

Description
Maximum privilege role for the Supply Chain Instance

Permissions details

Insights
Grant access to insights and exceptions, specifying the actions that authorized individuals are permitted to take.

Access	All	Create	Read	Update	Delete
Insights			☑	☑	
Configuration	☑	☑	☑	☑	☑

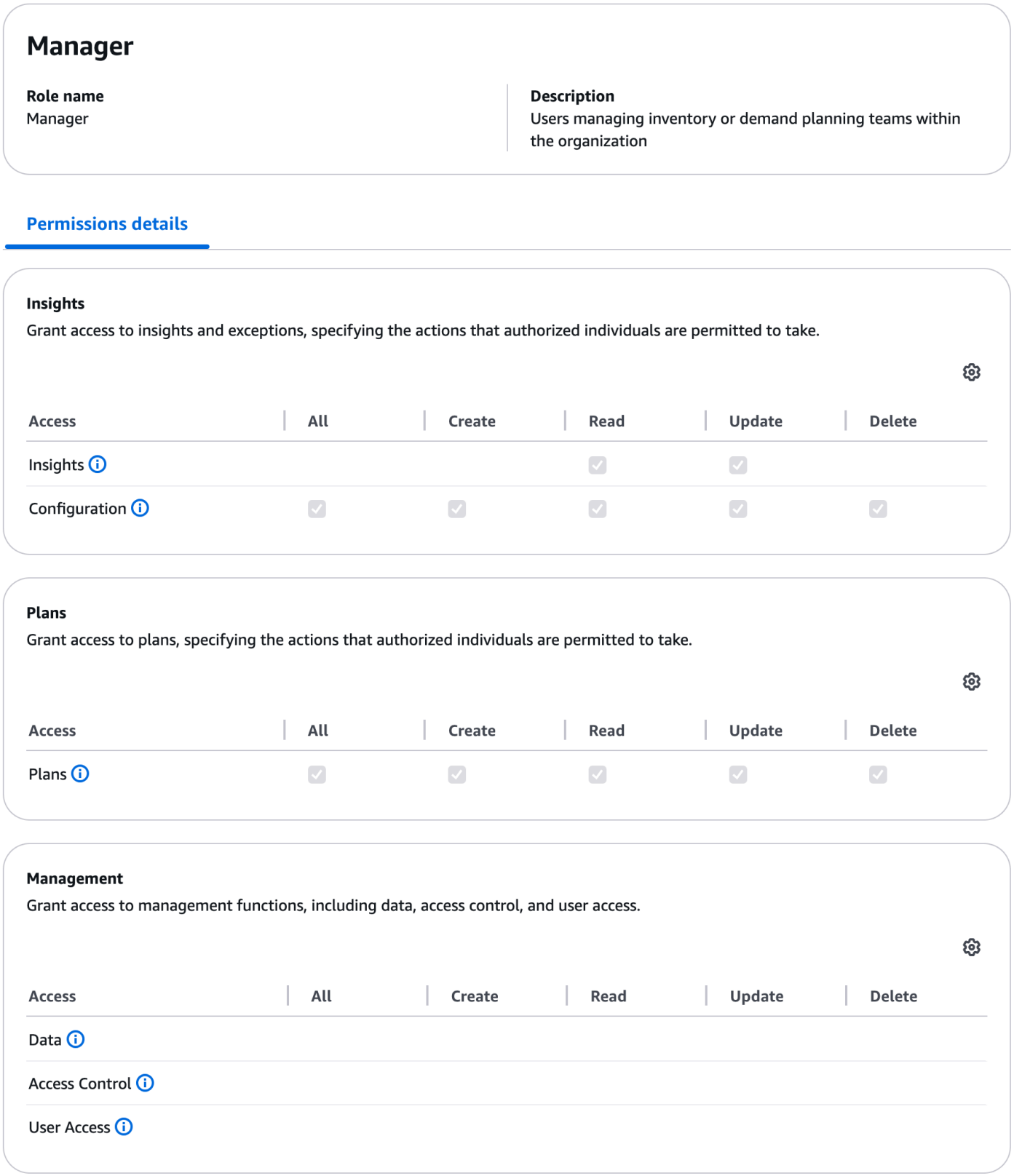
Plans
Grant access to plans, specifying the actions that authorized individuals are permitted to take.

Access	All	Create	Read	Update	Delete
Plans	☑	☑	☑	☑	☑

Management
Grant access to management functions, including data, access control, and user access.

Access	All	Create	Read	Update	Delete
Data	☑	☑	☑	☑	☑
Access Control		☑	☑	☑	
User Access	☑	☑	☑	☑	☑

- マネージャー – 以下を作成、表示、管理するためのアクセス許可。



- プランナー – 以下を作成、表示、管理するためのアクセス許可。

Planner

Role name
Planner

Description
Users planning inventory or demand within the organization

Permissions details

Insights

Grant access to insights and exceptions, specifying the actions that authorized individuals are permitted to take.

Access	All	Create	Read	Update	Delete
Insights			☑	☑	
Configuration		☑	☑	☑	

Plans

Grant access to plans, specifying the actions that authorized individuals are permitted to take.

Access	All	Create	Read	Update	Delete
Plans		☑	☑	☑	

Management

Grant access to management functions, including data, access control, and user access.

Access	All	Create	Read	Update	Delete
Data					
Access Control					
User Access					

> **Note**
>
> Amazon Connect Decisions 管理者は、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 Amazon Connect Decisions にアクセスできなくなります。
> - グループの追加は、Amazon Connect Decisions ではサポートされていません。

ユーザーアクセス許可ロールの管理

ユーザーの追加

Amazon Connect Decisions 管理者は、Amazon Connect Decisions 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、その後 Amazon Connect Decisions に追加できます。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、次のステップに従ってユーザーを追加します。

1. 左側のドロワーの設定を選択する
2. ユーザーを選択します。ユーザーの割り当てを選択する
3. 検索してユーザーを識別します。表示名、E メール、名、姓、ユーザー名を使用して検索できます
4. 追加するユーザーを選択します。
5. ロールを割り当てます。Amazon Connect Decisions のユーザーロールの詳細については、ロールとアクセス許可の概要を参照してください。

6. [割り当て] を選択します。選択内容が正確であることを確認します。

ユーザーアクセス許可の更新

現在の Amazon Connect Decisions ユーザーの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. 左側のドロワーの設定を選択します。
2. ユーザーを選択します。ユーザーの割り当てを選択する
3. ユーザーリストで、ユーザーを選択してユーザーの詳細ページを開きます。
4. ロールドロップダウンを使用して、ユーザーのロールのアクセス許可を更新します。
5. ロールの変更ボタンをクリックして、ロールを変更することを確認します。

ユーザーの削除

Amazon Connect Decisions 管理者は、Amazon Connect Decisions 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. 左側のドロワーの設定を選択します。
2. ユーザーを選択します。ユーザーの割り当てを選択する
3. ユーザーリストで、ユーザーを選択してユーザーの詳細ページを開きます。
4. [削除] を選択します。
5. 削除ボタンをクリックしてユーザーを削除することを確認します。

属性レベルのアクセスの設定

属性ベースのアクセスコントロール (ABAC) は、ビジネスコンテキストに基づいてアクセスを制限することで、精度をさらに高めます。製品属性とサイト属性を使用すると、プランナーが管理する特定の製品と場所の詳細のみを表示し、マネージャーはチームの責任範囲を可視化できます。

「管理者」ロールを持つユーザーは、製品およびサイトごとに他のユーザーのアクセスを設定できます。

1. 左側のナビゲーションバーからユーザーページに移動します。

2. そのインスタンスのユーザーのリストから、設定が必要なユーザーを選択します。
3. デフォルトでは、データアクセスセクションでは、ユーザーは「すべての製品とサイトへのフルアクセスの付与」が有効になります。このトグルをオンにすると、すべての製品とサイト (この起動前の動作) にアクセスできます。
4. 「すべての製品とサイトへのフルアクセスを許可する」をオフにすると、製品とサイトの設定セクションが表示されます。初回アクセス時に製品やサイトは割り当てられません。
5. 設定内容に基づいて、製品またはサイトの Add/Remove ボタンをクリックします。検索を使用して、そのユーザーに必要な項目を検索して選択します。
6. 複数のユーザーに同じ製品またはサイトを割り当てることができます。ユーザーは、最大 1,000 個の製品サイトの組み合わせを持つことができます。
7. 以前に設定した製品またはサイトは、同じインターフェイスを使用して削除できます。
8. ウィザードの最後のページで追加と削除の完全なリストを確認して確認し、アクセス設定を完了します。

製品とサイトへのアクセスが設定されると、そのユーザーのアクセスは、次の割り当てに基づいて制限されます。

- すべてのユーザーは、アクセスコントロールに含まれる製品またはサイトに対して生成されたかどうかにかかわらず、例外またはレコメンデーションページを表示できます。
- 変更アクションを実行するには (例外を却下する、ステータスを進行中から完了に変更するなど) 、ユーザーはアクセスコントロールで適切な製品またはサイトを設定する必要があります。
- アクセスコントロールが設定されたユーザーは、ユーザー割り当てとアクセスビューの切り替えを使用することもできます。

ユーザー割り当て

ユーザー割り当ては、複数のユーザー間でインサイトのバランスを簡単にする機能です。ユーザー割り当てを使用すると、ユーザーは特定のインサイトを割り当てて、これらのタスクが実際にどのように共有されるかをより適切に反映できます。このプロセスは、次のように機能します。

- 例外が作成されるたびに、システムは例外が作成された製品とサイトを、アクセスコントロール用に設定された同じ製品またはサイトを持つすべてのユーザーに対してチェックします。
- 一致するユーザーが検出されると、その例外の割り当て先フィールドがユーザー名で更新されます。複数のユーザーに例外に一致する製品またはサイトがある場合、その 1 つにランダムに割り当てられます。

- 各例外に割り当てることができるユーザーは 1 人のみですが、必要に応じて別のユーザーに例外を再割り当てできます。製品またはサイトへのアクセス権を持つユーザーにのみ再割り当てできます。
- インサイトの自動割り当ては、例外が最初に作成されたときに行われます。以前に作成したインサイトは自動的に再割り当てされません。さらに、ユーザーが削除されたり、アクセスコントロールが更新されたりしても、ユーザー割り当ては自動的に更新されません。
- インサイトのリストページで、ユーザーは割り当てられた宛先ディメンションでフィルタリングして、自分に割り当てられたすべてのインサイトを簡単に識別できます。また、この同じフィルターを使用して、未割り当てのインサイトを表示することもできます。ユーザー割り当ては現在、インサイトでのみ使用できます

データオンボーディング

データの接続

前提条件

データオンボーディングを開始する前に、以下を確認してください。

- Amazon Connect 決定インスタンス
  - インスタンスは、関連付けられた S3 バケットで既に作成されている必要があります
- 準備済みデータ
  - Amazon Customer Success カウンターパートと協力して、Amazon Connect Decisions の使用方法に基づいて、必要なデータを決定します。基本データの要件は次のとおりです。
    - 販売/注文履歴: 12 か月を超えるトランザクションレコード
    - 製品の詳細: 仕様を含む製品カタログを完成させる
    - サイト/ロケーション情報: 倉庫、ディストリビューションセンター、小売ロケーション
    - 現在の在庫保有: 各ロケーションの手元在庫
  - UTF-8 エンコードを使用した CSV 形式のすべてのソースデータ

初回ログイン: オンボーディングアンケート

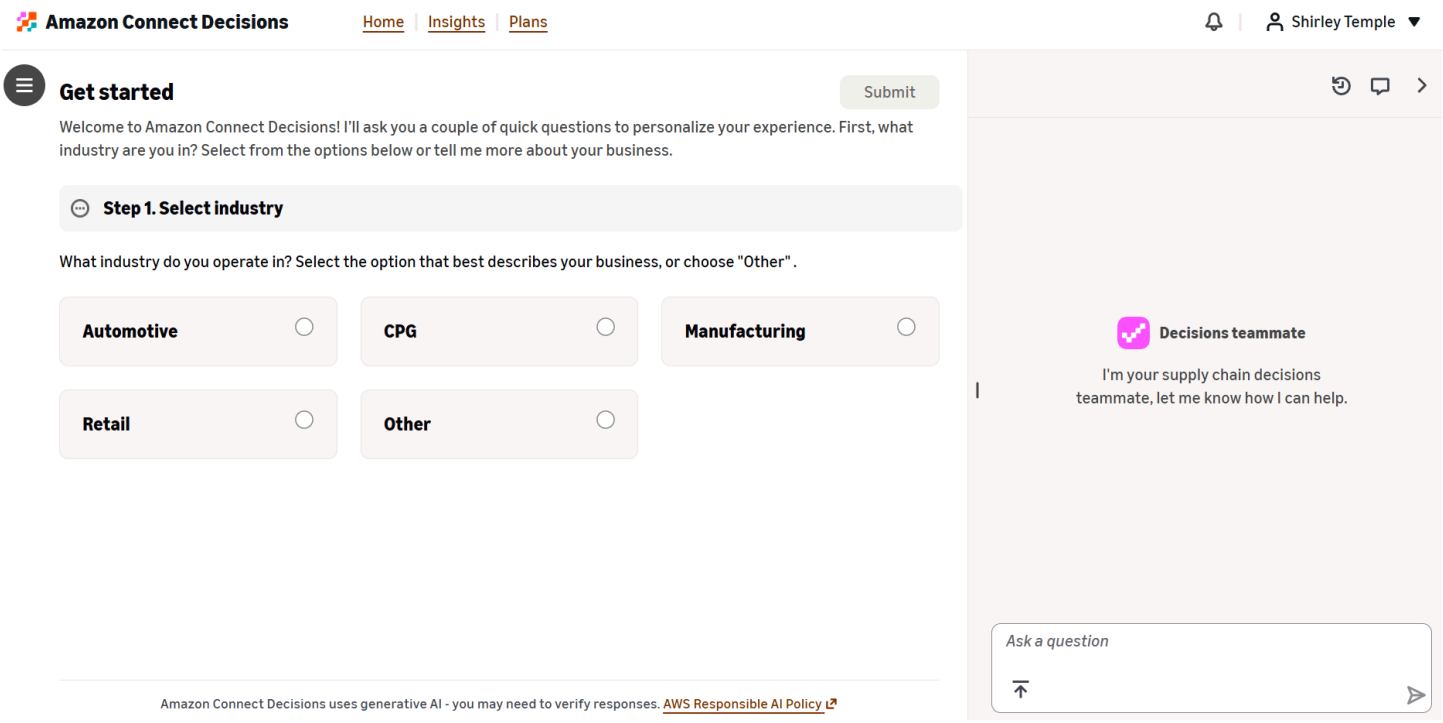
Amazon Connect Decisions に初めてログインすると、ガイド付きオンボーディングアンケートが表示されます。このパーソナライゼーションウィザードは、Decisions チームメイトがビジネスに最も関連性の高い機能をコンテキスト化するのに役立ちます。このアンケートでは、業界、主要なビジネス上の課題、および計画の推奨アプローチに関する情報を収集します。レスポンスは、選択した内容に基づいてオンボーディングステップを最適化するのに役立ちます。これにより、システムは後続のセットアップワークフローを合理化し、ビジネスに最も関連性の高い設定パスを表示できます。アプリケーション全体にアクセスする前に、すべての手順を完了する必要があります。Decisions Teammate は、オンボーディングプロセスを通じて右側のサイドバーからリアルタイムで質問に答えることができます。

> **Note**
>
> これは、初回ログイン時のみの 1 回限りの選択です。レスポンスは、後続のオンボーディングステップを最適化し、エージェントがビジネス環境を理解するのに役立つ追加のコンテキストを提供します。選択内容に関係なく、すべての機能に完全にアクセスできます。

ステップ 1: 業界を選択する

表示される内容: ウェルカムメッセージと、ビジネスを最もよく表す業界を選択するように求める一連のラジオボタン。

1. ビジネスを最もよく表すラジオボタンを選択します。
2. 事前定義されたオプションのいずれにも当てはまらない場合は、その他を選択します。



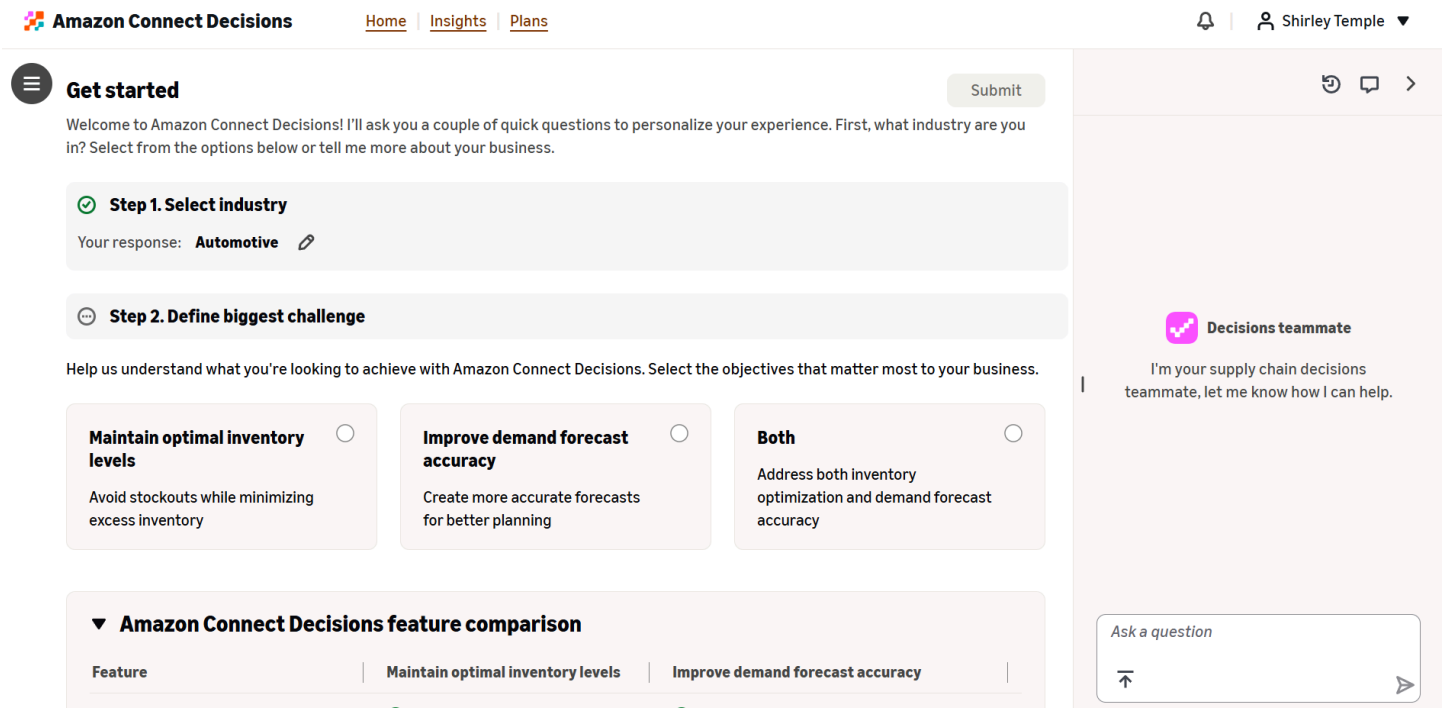
ステップ 2: 最大のチャレンジを定義する

表示内容: ステップ 1 のレスポンスは編集オプションで表示されます。その下に、3 つのオプションから主なビジネス上の課題を特定するように求められます。各選択に関連付けられている機能を理解するのに役立つ機能比較テーブルが表示されます。

1. オプションを確認します。使用可能なオプションとその意味については、次の表を参照してください。
2. 最も差し迫った課題を表すラジオボタンを選択します。
3. 必要に応じて、オプションの下にある機能比較表を確認して、各選択に含まれる内容を理解します。

ビジネスチャレンジのオプション

オプション	説明	有効になっている主な機能
最適なインベントリレベルを維持する	在庫過剰を最小限に抑えながら在庫切れを回避することが主な課題である場合は、これを選択します。	在庫の最適化、在庫切れの防止、在庫の過剰削減、供給計画、ベンダーリードタイムの追跡
需要予測の精度の向上	計画の決定を改善するために、より正確な予測を作成することが主な課題である場合は、これを選択します。	ベースライン予測、コンセンサス計画、予測精度の追跡
[Both] (両方)	インベントリの最適化と需要予測の精度の両方に同時に対処する必要がある場合は、これを選択します。	すべての供給固有および需要固有の機能が有効になっている



ステップ 3: インベントリプランニングアプローチを選択する

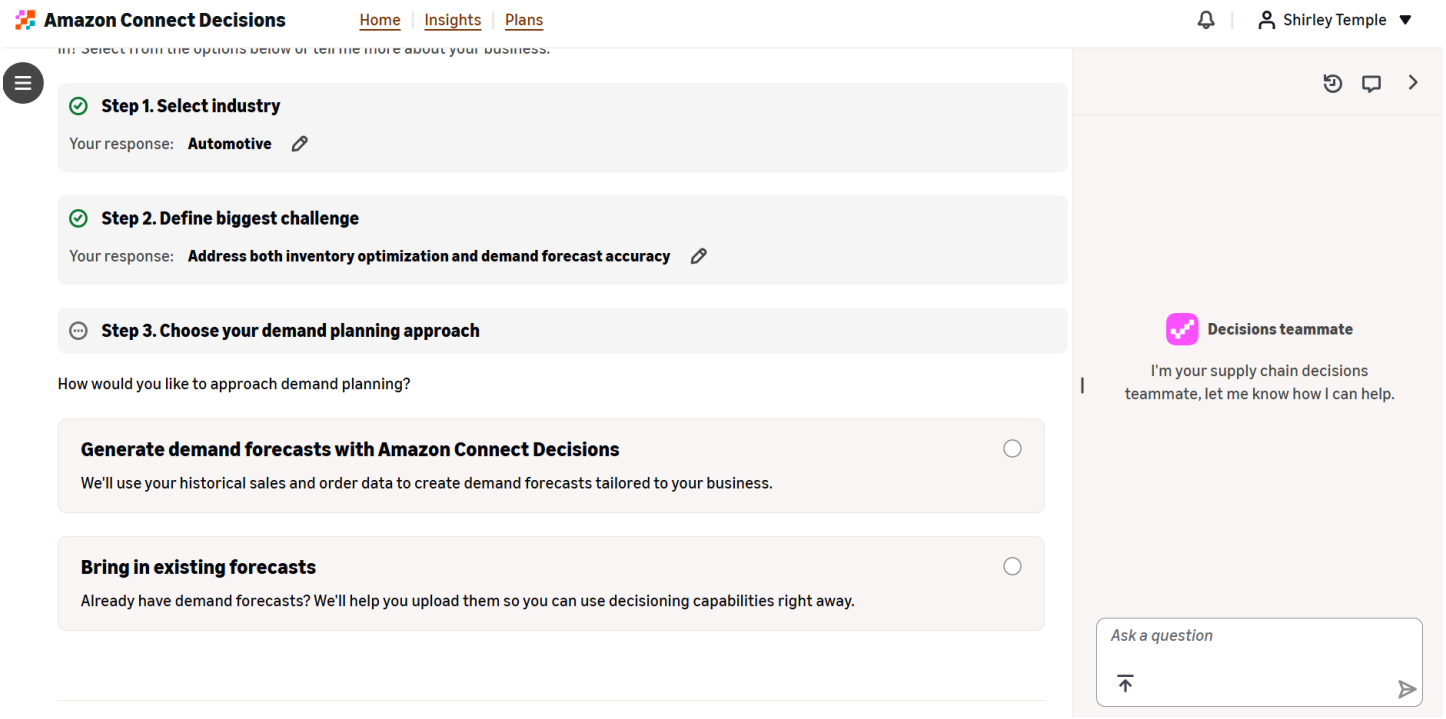
表示される内容: ステップ 1 と 2 は完了 (緑色のチェックマークで示される) として表示され、レスポンスは表示され、編集可能です。ステップ 3 では、在庫計画にどのようにアプローチするかを尋ねます。2 つのオプションが強調表示されています。

1. 2 つのインベントリ計画オプションを確認します。使用可能なオプションとその意味については、次の表を参照してください。
2. 現在の状態に一致するアプローチのラジオボタンを選択します。

インベントリプランニングアプローチのオプション

オプション	説明	最適な用途
Amazon Connect Decisions を使用してインベントリプランを生成する	システムは、過去の売上データと在庫データを使用して、ビジネスに合わせた計画を作成します。	既存の計画ソリューションがない組織、または履歴データから AI が生成した計画を活用する組織。
既存の在庫予測または計画を取り込む	既存のインベントリプランまたは予測をアップロードして、決定機能をすぐに使用で	すでに計画プロセスを確立しており、計画ソースを変更せずにモニタリング、インサイ

オプション	説明	最適な用途
	きるようにします。システムは、データのアップロードとマッピングに役立ちます。	ト生成、レコメンデーション機能を活用する組織。



ステップ 4: 需要計画アプローチを選択する

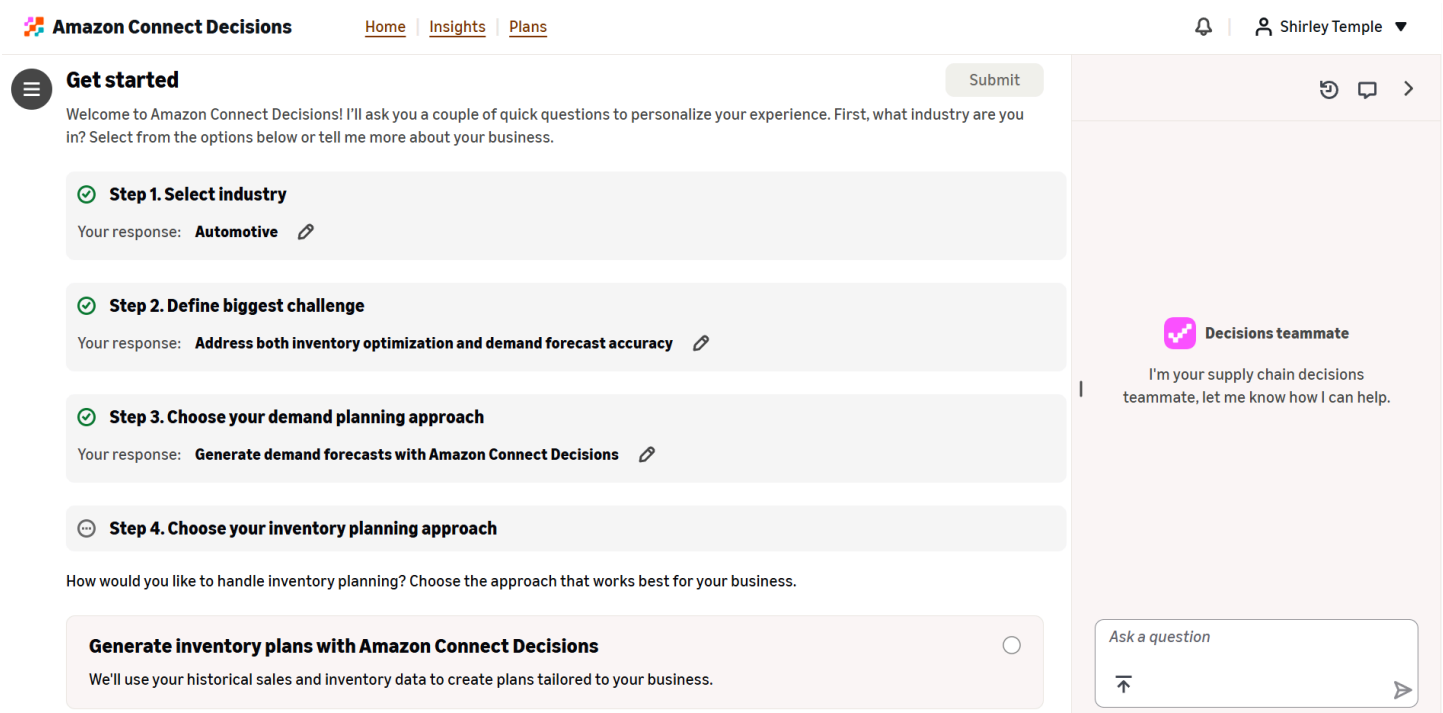
表示される内容: ステップ 1 ~ 3 は完了として表示されます。ステップ 4 では、需要計画にどのようにアプローチするかを尋ねます。

1. 2 つの需要計画オプションを確認します。使用可能なオプションとその意味については、次の表を参照してください。
2. 現在の状態に一致するアプローチのラジオボタンを選択します。
3. 送信をクリックしてオンボーディングアンケートを確定します。

注意: このオンボーディングアンケートは、選択内容に基づいてオンボーディングステップを最適化するのに役立つ 1 回限りのコンテキスト入力です。エージェントの動作を変更したり、機能へのアクセスを制限したりすることはありません。Amazon Connect Decisions のすべての機能は、引き続き完全に利用できます。

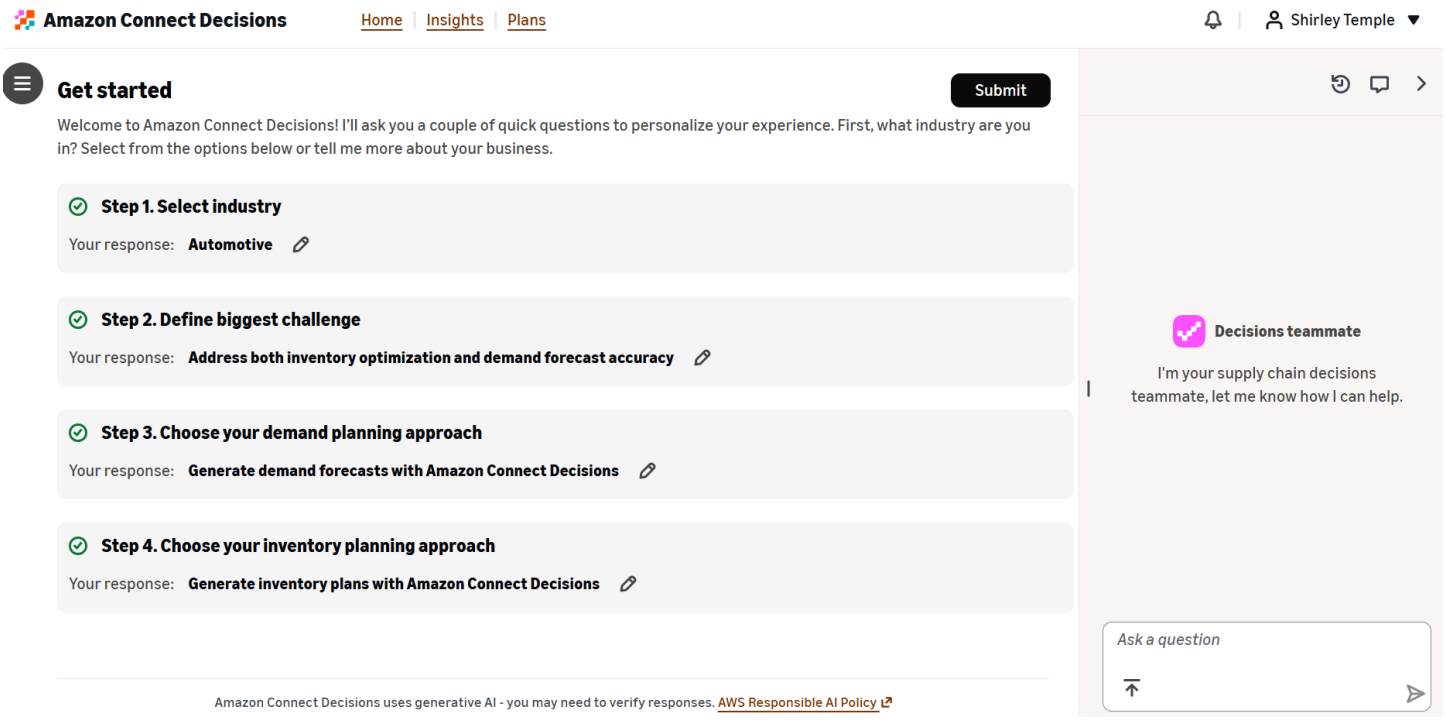
需要計画アプローチのオプション

オプション	説明	最適な用途
Amazon Connect Decisions を使用して需要予測を生成する	システムは、過去の売上および注文データを使用して、ビジネスに合わせた需要予測を作成します。Amazon Connect Decisions は、18 以上の予測ツールを調整して、正確なベースライン予測を生成します。	既存の予測ソリューションがない組織、または現在のアプローチを AI 生成予測に置き換えたい組織。
既存の予測を取り込む	既存の需要予測をアップロードして、決定機能をすぐに使用できるようにします。システムは、予測データのマッピングとインポートに役立ちます。	すでに予測プロセスを確立しており、予測ソースを変更せずにモニタリング、インサイト生成、レコメンデーション機能を活用する組織。

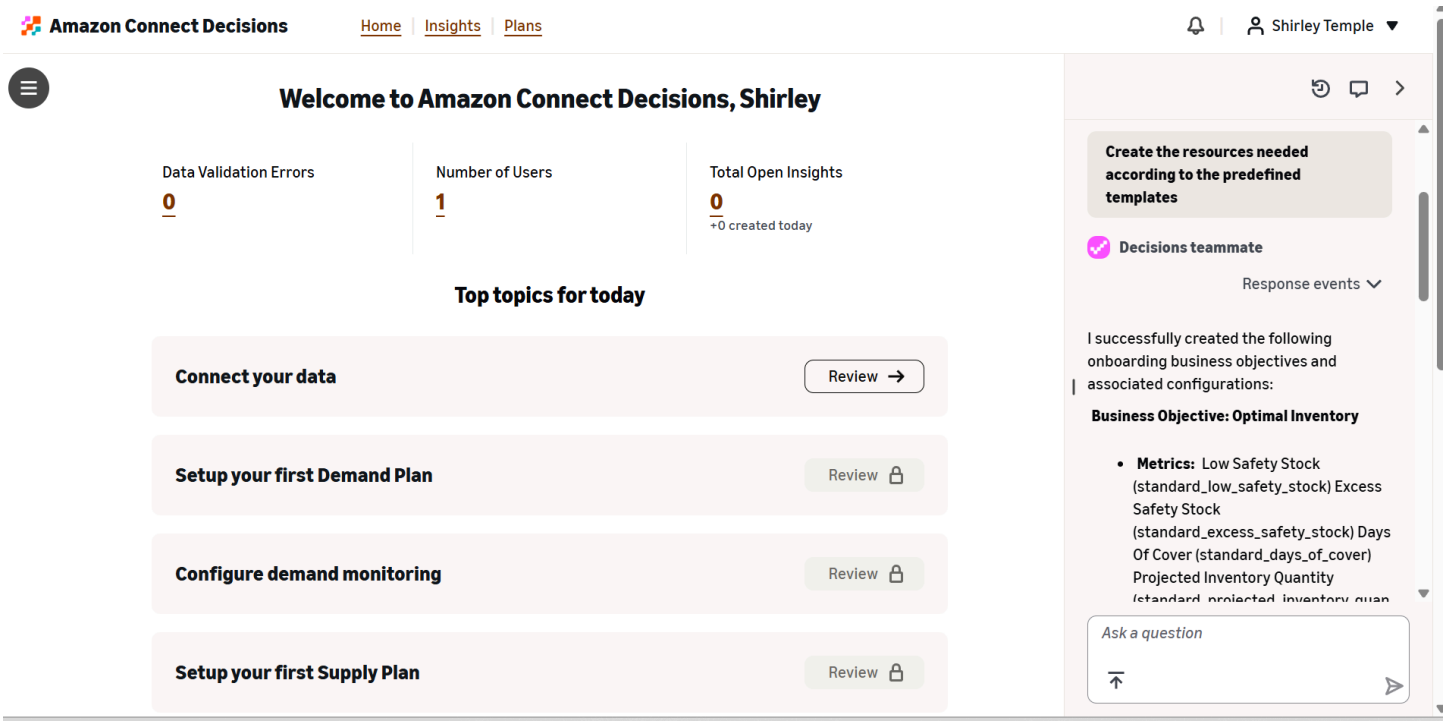


アンケートの完了後

4 つのステップをすべて完了したら、送信をクリックします。

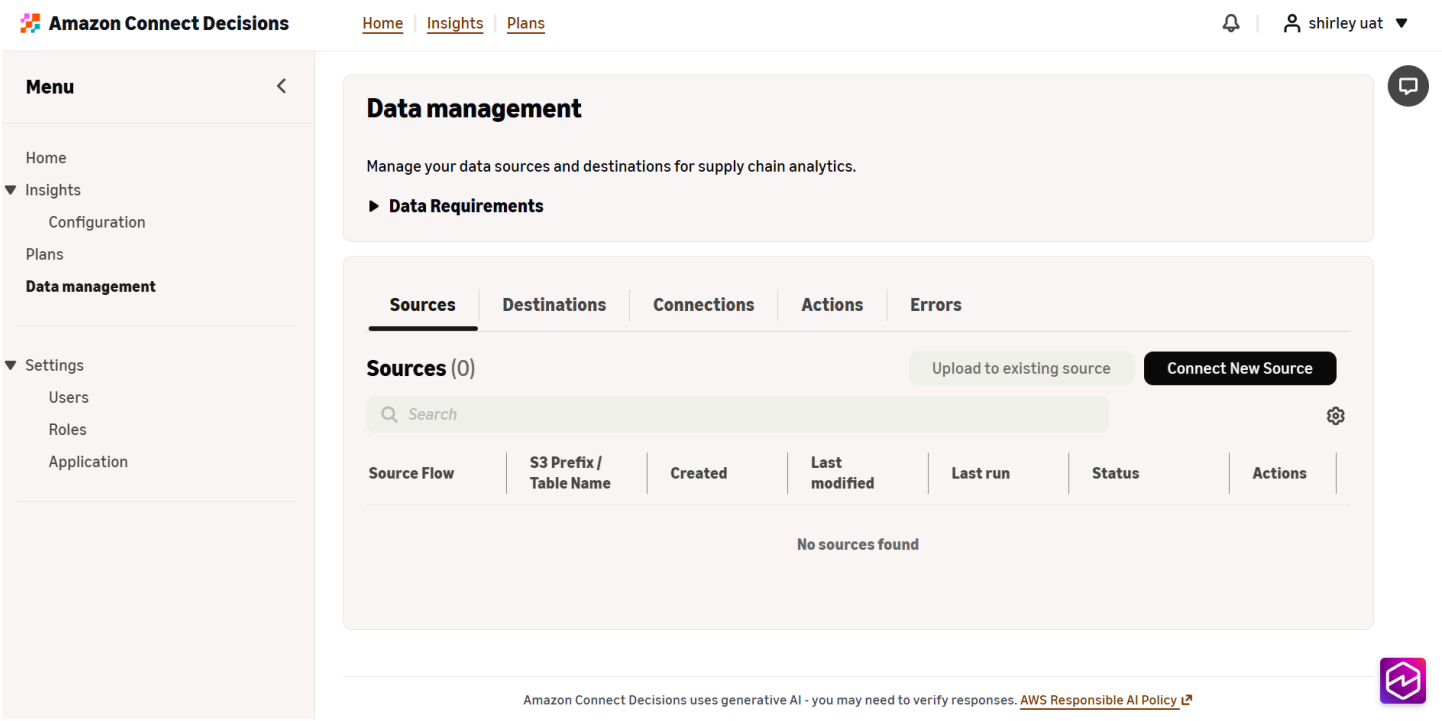


- ホームページにリダイレクトされ、ダッシュボードとトピックカードを使用して、残りのオンボーディングステップを案内します。
- システムは、選択した内容に基づいてアプリケーション内にメトリクスとルールを自動的に作成します。これらはドラフトステータスで作成され、すぐにはアクティブになりません。
- 自動作成されたメトリクスとルールを確認し、ニーズに応じてアクティブ化したり、特定のビジネス要件に合わせた独自のメトリクスとルールを作成したりできます。



最初のソースフローの作成

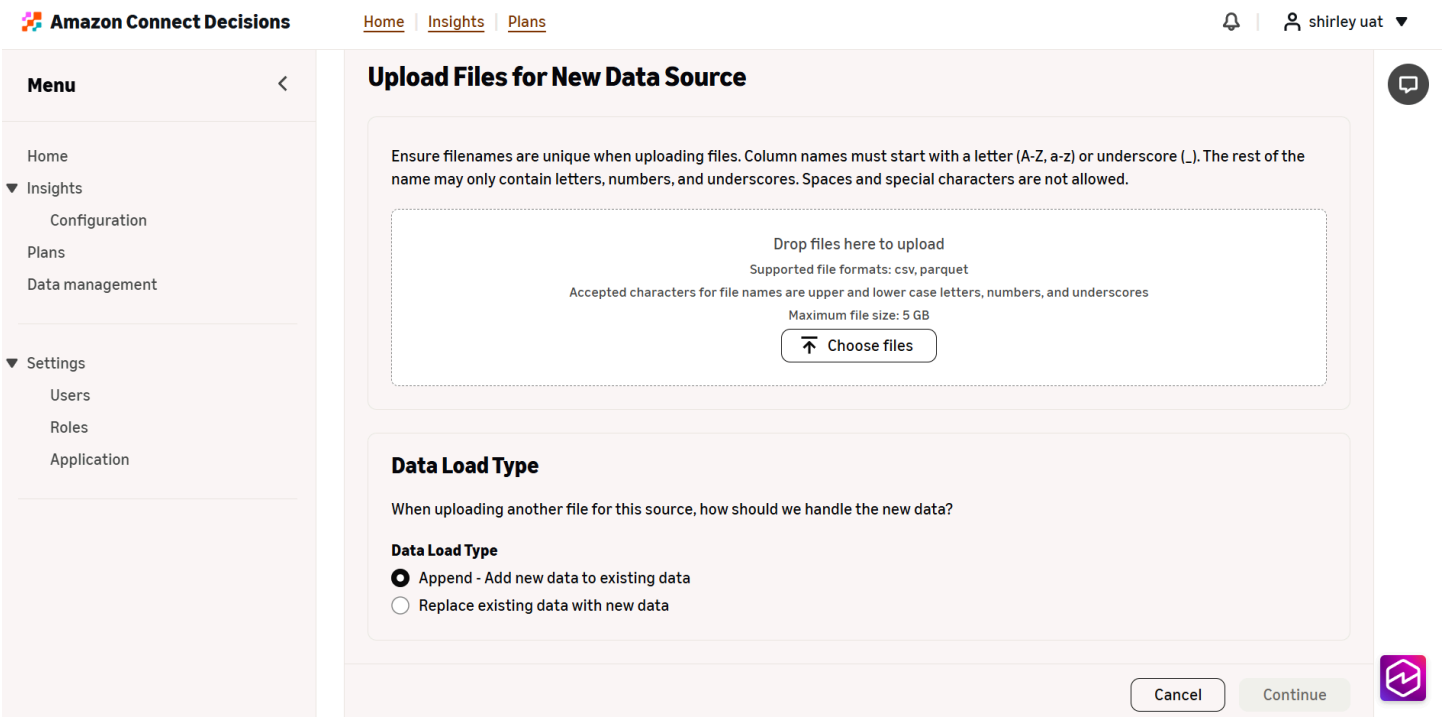
データのオンボーディングを開始するには、データトピックカードの接続の確認をクリックするか、Amazon Connect Decisions の「ハンバーガーメニュー」の「データ管理」タブに移動します。ここでは、既存のソースフローをすべて確認できます。まだセットアップしていない場合は、「新しいソースの接続」をクリックして開始します。



ソースデータをアップロードする

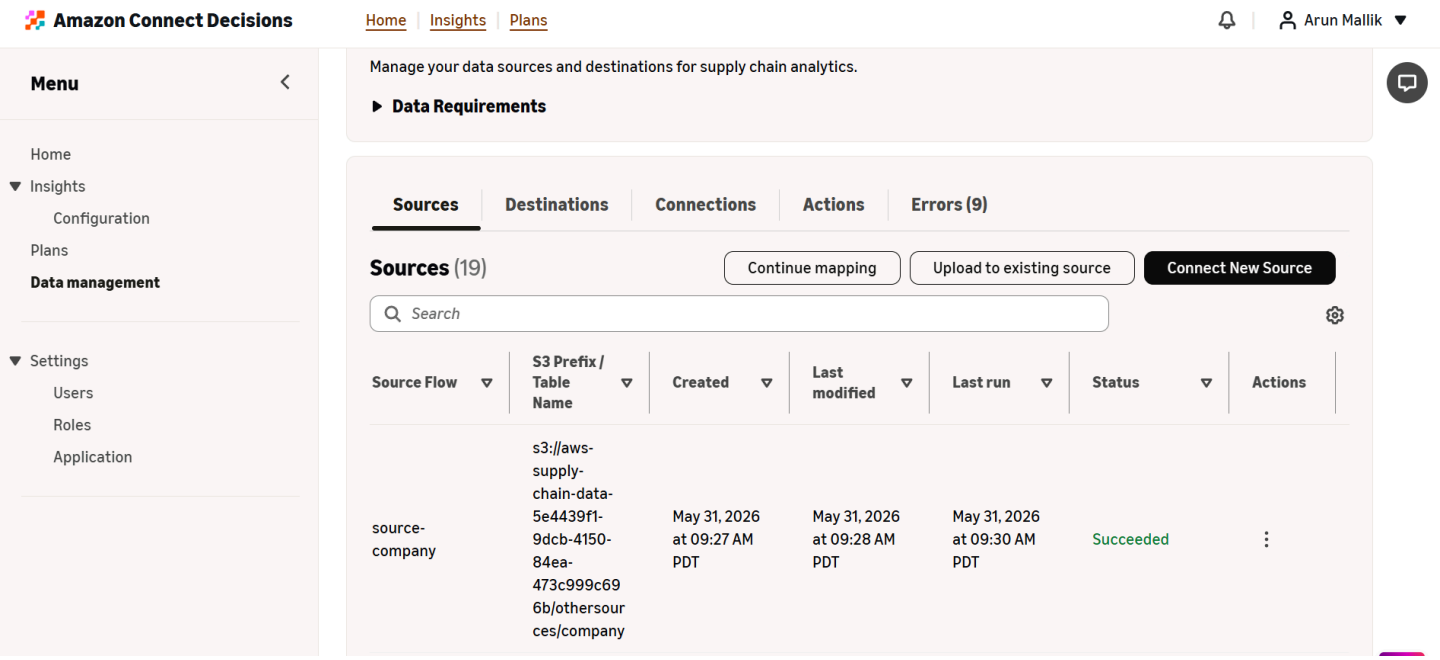
ユースケースに必要な CDM テーブルに基づいて、ソースデータを含む CSV ファイルをアップロードします。データ更新の処理方法を選択できます。

- 追加: 既存のデータに新しいデータを追加する
- 置換: 既存のデータを新しいデータに置き換える



ファイルをアップロードすると、Amazon Connect Decisions は S3 に以下のデータ用のフォルダ構造を自動的に作成します。

- 選択したソースシステムにちなんで名付けられた親フォルダ
- 選択したソーステーブル名の後に という名前のサブフォルダ
- サブフォルダのすべてのファイルは、同じソーステーブルに対して保存されます。
- このファイル構造は、Amazon S3 フォルダパスの作成にも使用されます。

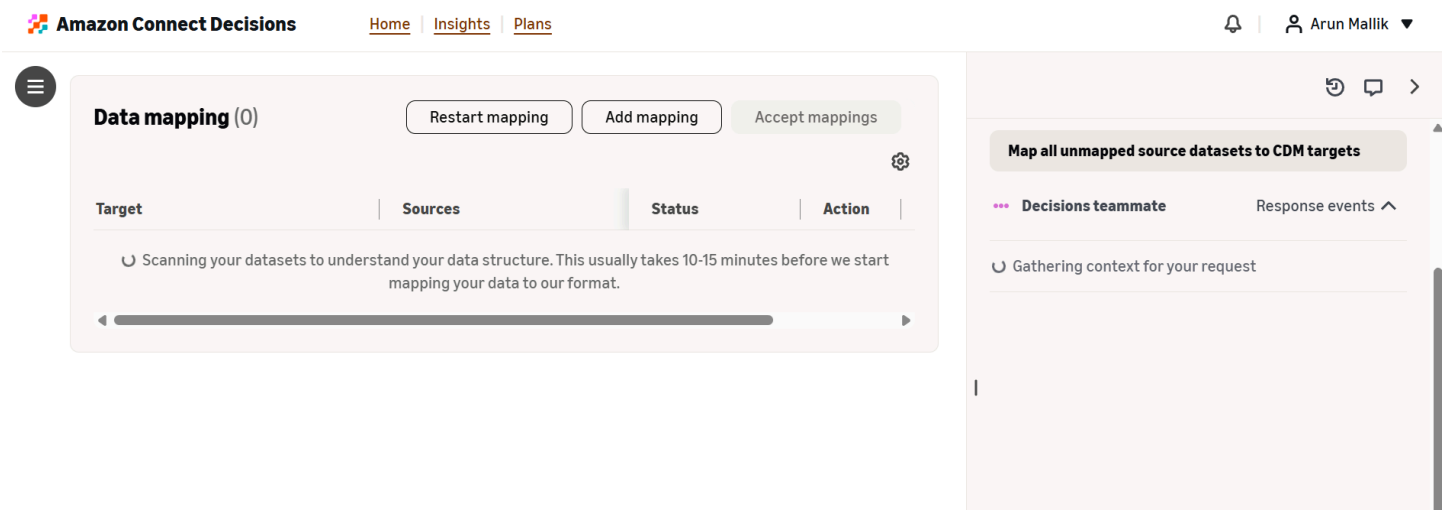


Source-to-CDM 送信先マッピング

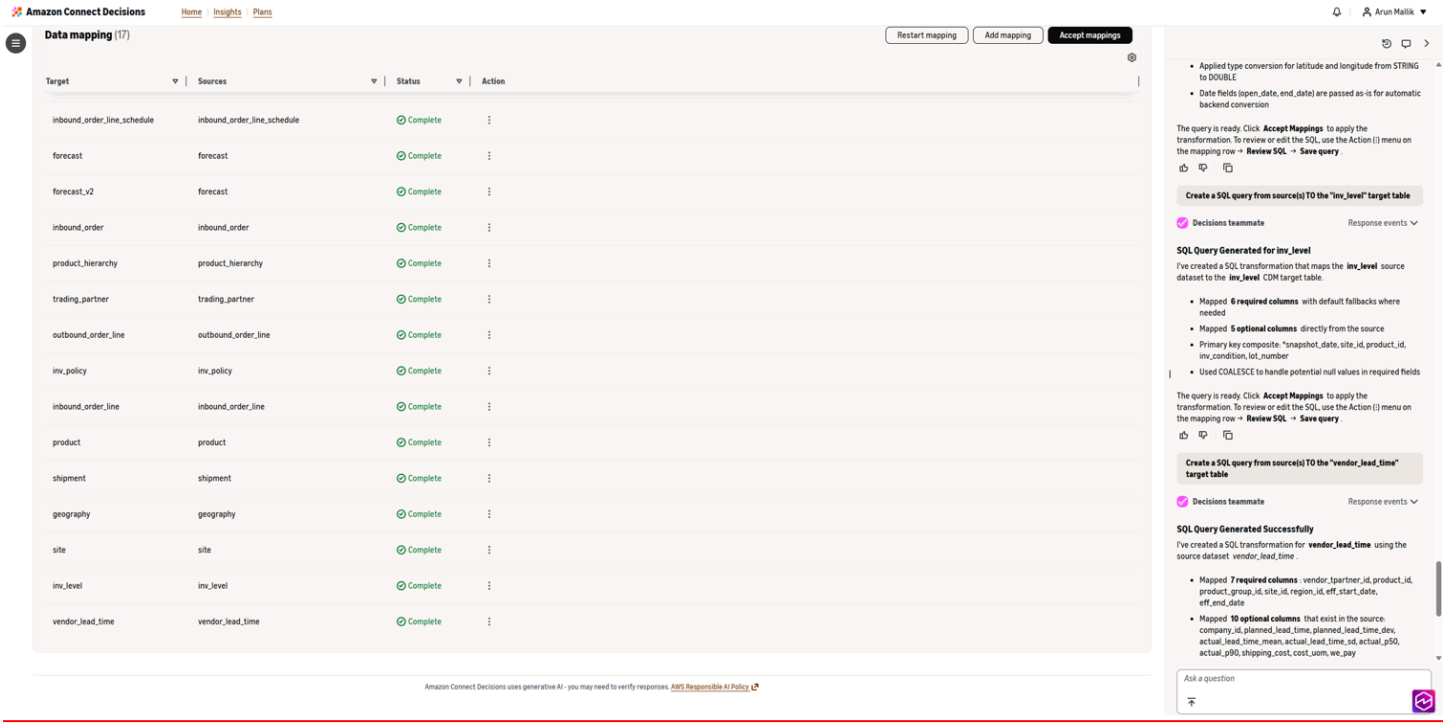
ファイルがアップロードされると、Amazon Connect Decisions はデータの分析を開始し、1 つ以上の Amazon Connect Decisions の CDM 送信先テーブルに自動的にマッピングします。

期待すること

- このステップは、アップロードされたデータの量に応じて 10 ~ 15 分かかる場合があります。
- データエージェントはバックグラウンドで動作し、ソースデータに最適な CDM 送信先データセットを特定します。
- このページから移動すると、自動マッピングが失敗します。待機中は、Amazon Connect Decisions and Data Management タブを開いたままにして、自動マッピングが完了していることを確認してください。

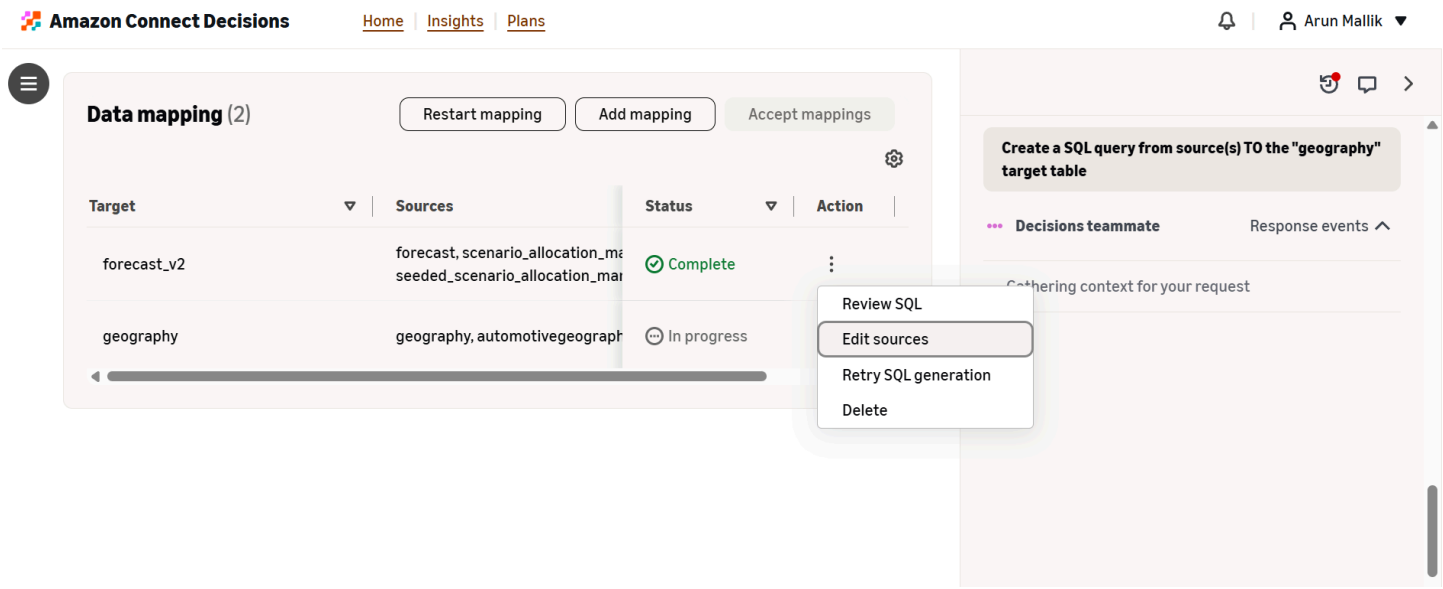


完了すると、データエージェントは重複するデータに基づいてsource-to-destinationマッピングの理論的根拠を提供し、マッピング結果を確認してエージェントに質問できます。



ソースマッピングを確認して編集するには、次の操作を行います。

- 自然言語を使用してデータエージェントと直接やり取りし、送信元と送信先のマッピングを更新します。
- アクションをクリックし、「ソースの編集」を選択します。



マッピングの編集

ここから、次のことができます。

- 必要に応じて、送信元と送信先のマッピングを手動で更新する
- 画面の右側にあるデータエージェントを使用して質問し、マッピングを確認します。
- 特定のデータセットの詳細については、ユーザーガイドを参照してください。

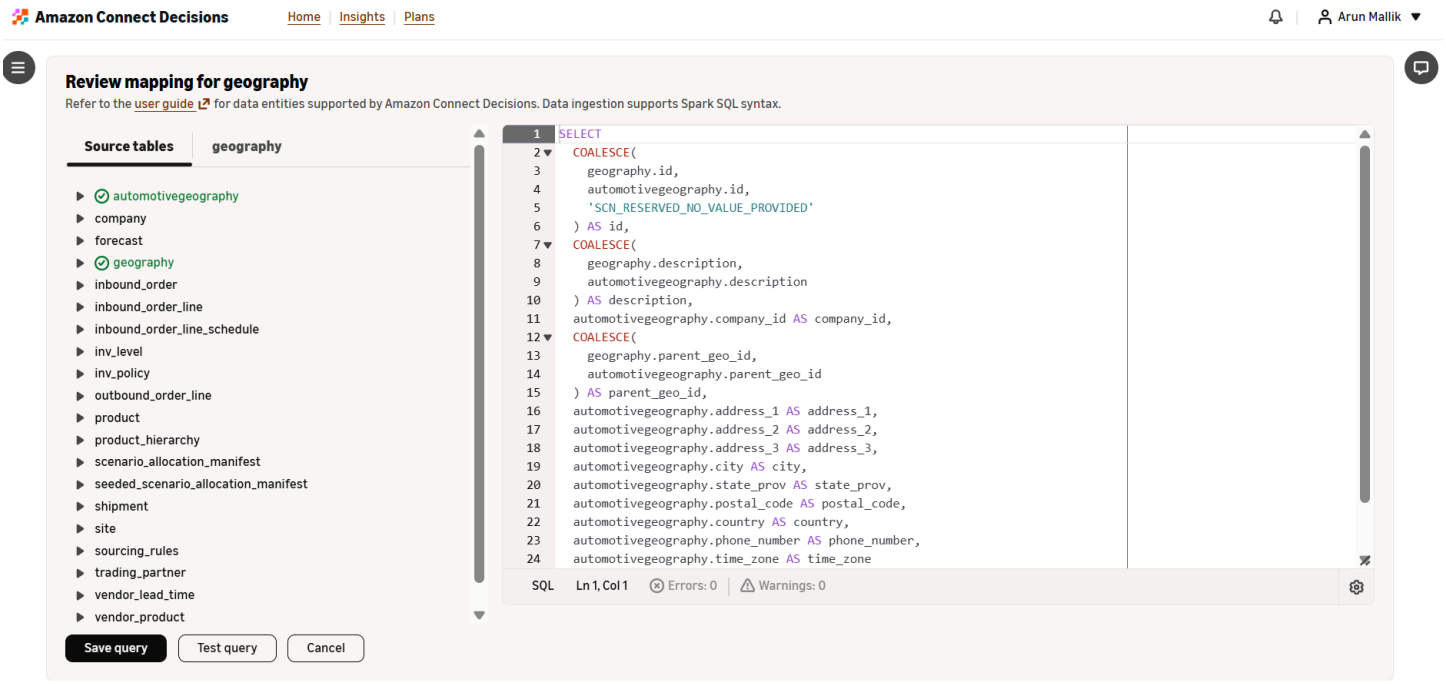
列/データマッピング

source-to-destinationマッピングが完了すると、Amazon Connect Decisions は送信元データセットから CDM 送信先への SQL 変換クエリを自動的に作成します。マッピングが完了すると、マッピングの結果を詳述した通知がデータエージェントから届きます。

ここから、アクションメニューから「SQL のレビュー」を選択して、マッピング用に生成された SQL を確認する必要があります。

マッピング (SQL) を確認すると、以下が表示されます。

- 追加したソースデータセット列
- 参照先 CDM テーブル列
- それらを接続している変換 SQL
- データエージェントが提供するマッピングの根拠



マッピングの編集

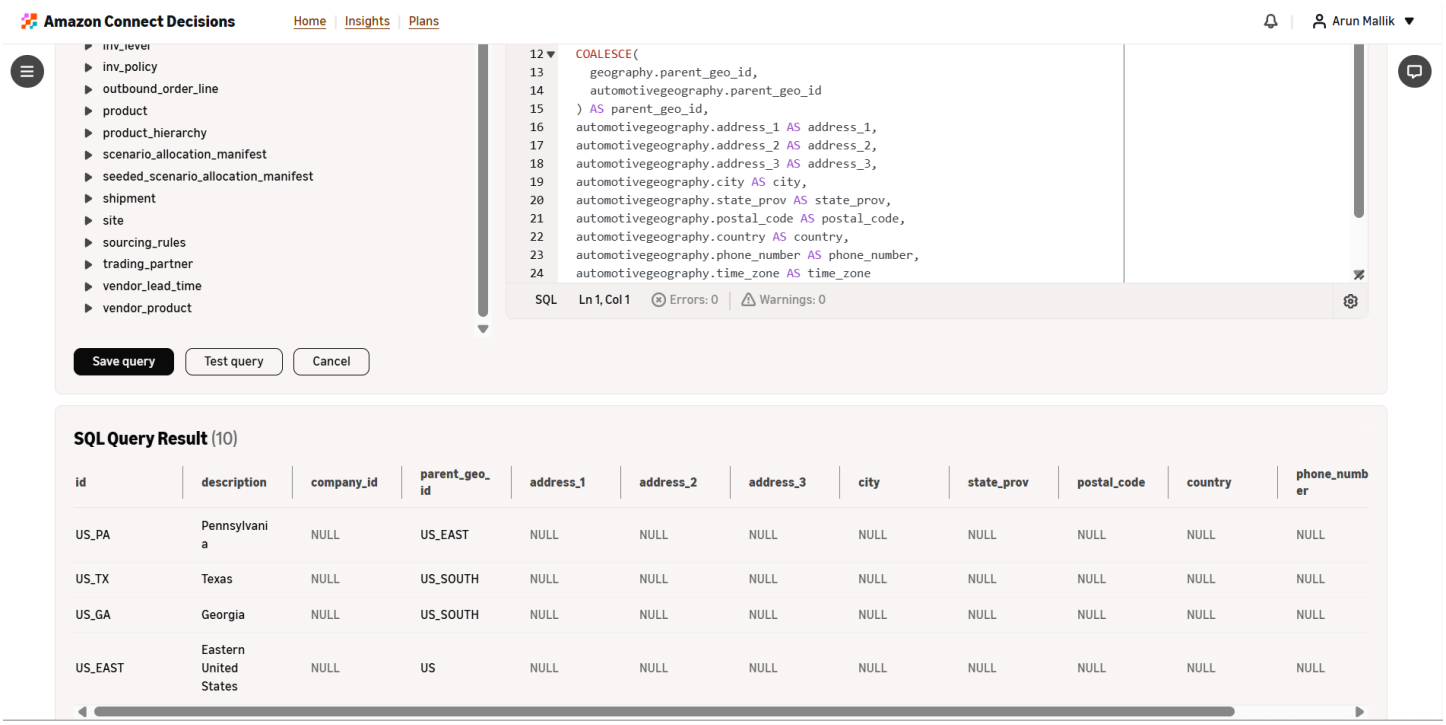
マッピングを編集するには、次の 2 つのオプションがあります。

- データエージェントの使用: 自然言語を使用してマッピングを質問、管理、更新する
- SQL を直接編集する: SQL に精通している場合は、クエリを直接変更できます。

変更のテスト

マッピングクエリを編集するときは、「テストクエリ」機能を使用してテストを続行します。これにより、データの送信先 CDM への変換方法のサンプルがスクロール可能にプレビューされます。これを使用して、変換が正しく実行されることを確認し、送信source-to-destination CDM からの適切な更新を検証します。

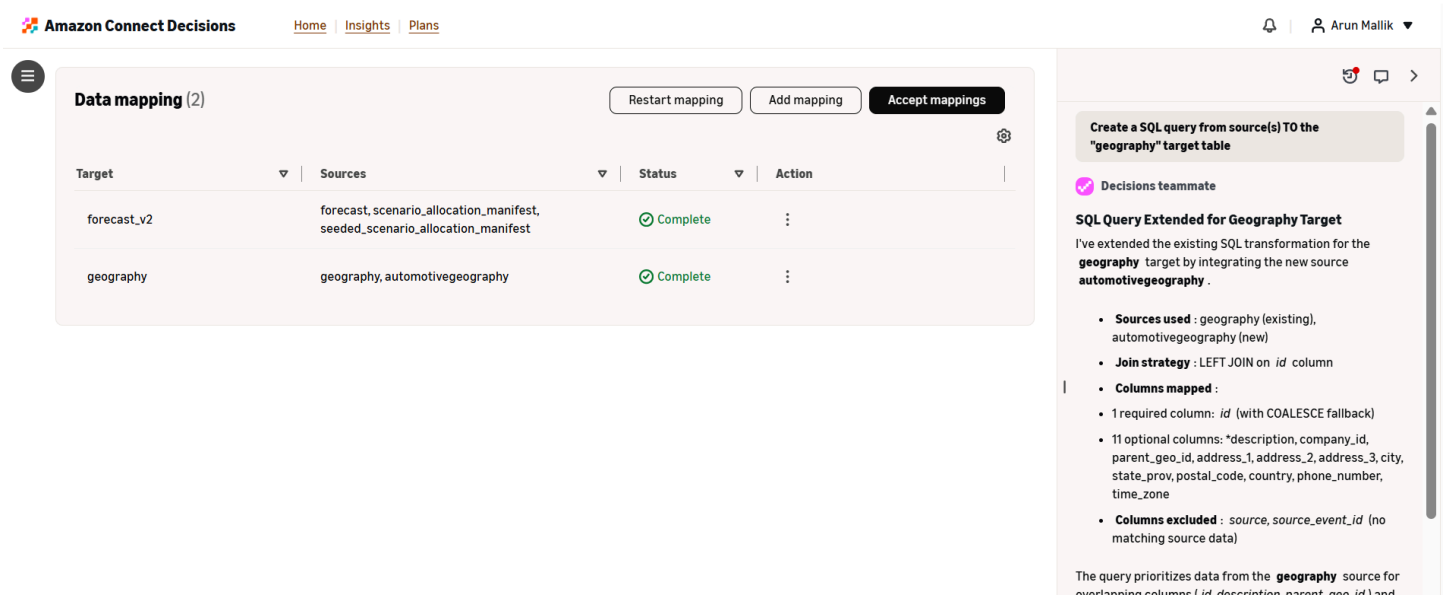
マッピング出力に満足したら、「クエリの保存」を選択して、その送信元と送信先のペアの変換クエリを保存します。



マッピングの確認と承認

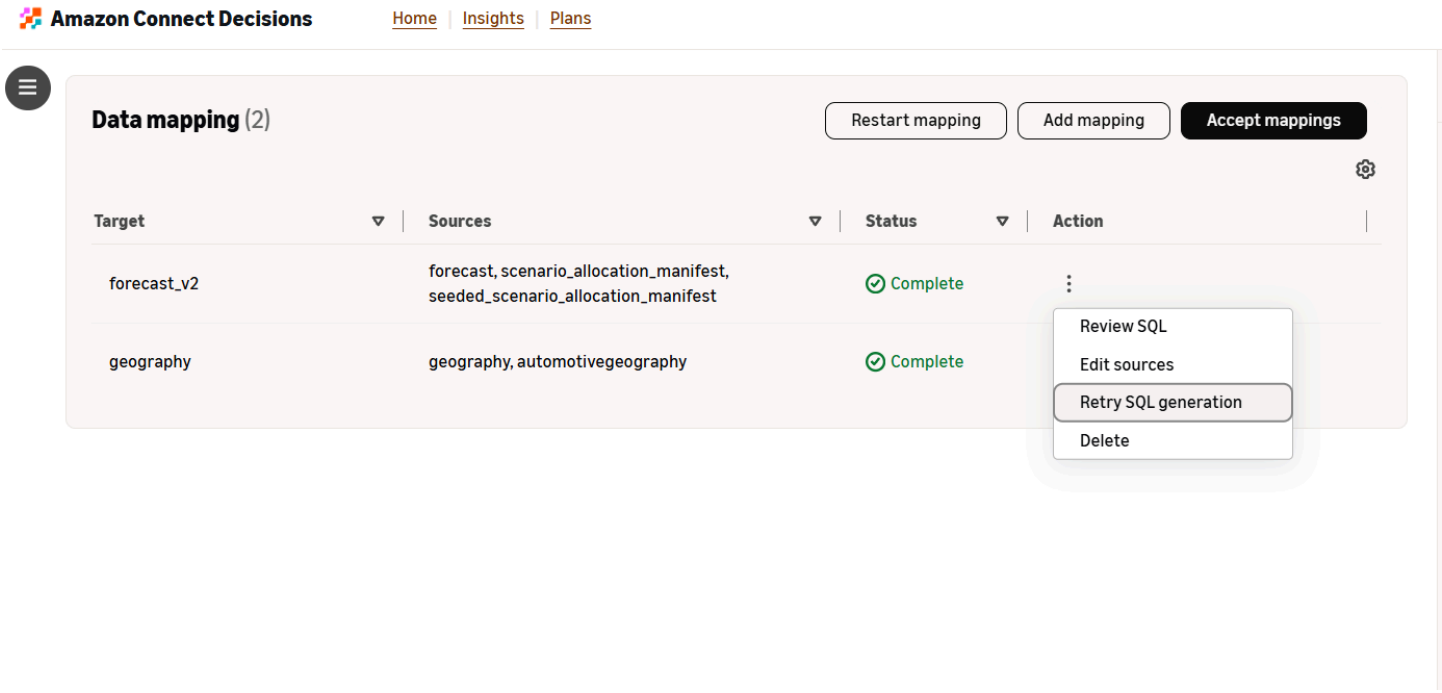
各ソースデータセットの残りのマッピングを確認します。データエージェントは、質問やトラブルシューティングのヘルプのために、画面の右側で永続的に残ります。

すべてのマッピングに満足したら、マッピングを受け入れるをクリックしてデータのオンボーディングを完了します。



失敗したマッピングの処理

マッピングが失敗した場合は、「マッピングの再開」を選択してすべてのマッピングを再起動するか、「SQL 生成の再試行」を介してアクションメニューから 1 つのマッピングを手動で再試行できます。データエージェントは自然言語を使用してマッピングを再試行することもでき、エラーが解決しない場合は引き続き問題の特定と解決に役立ちます。

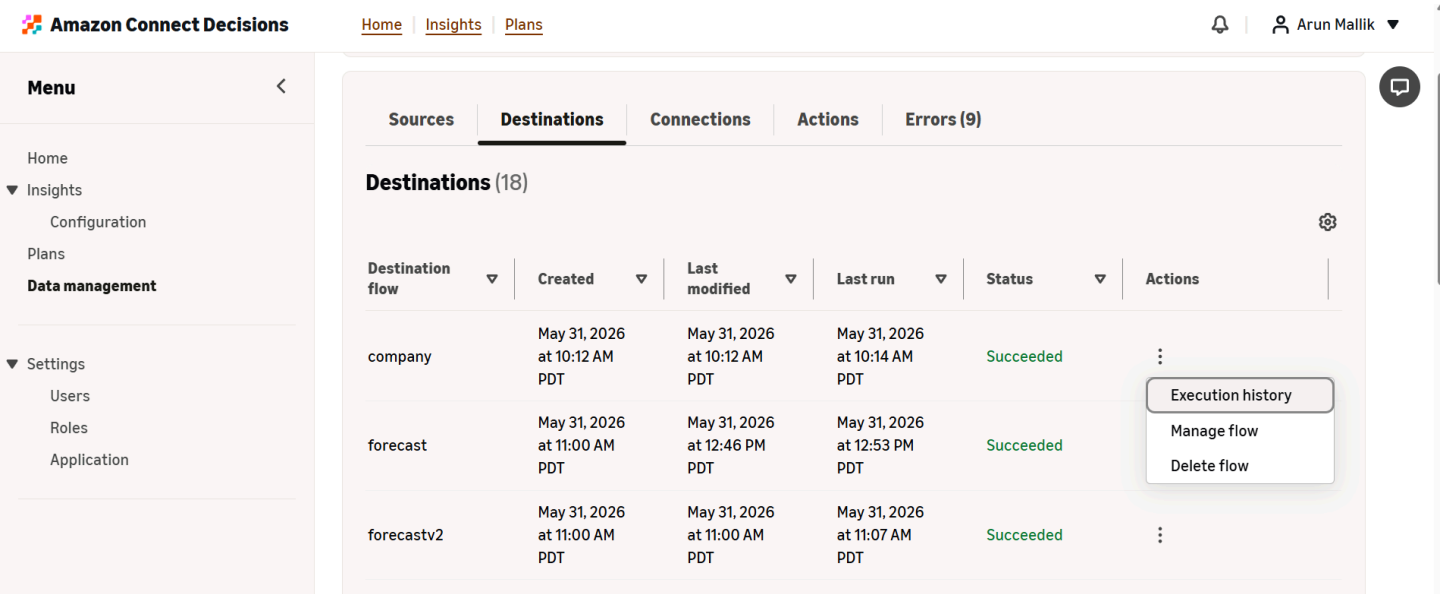


フローのモニタリング

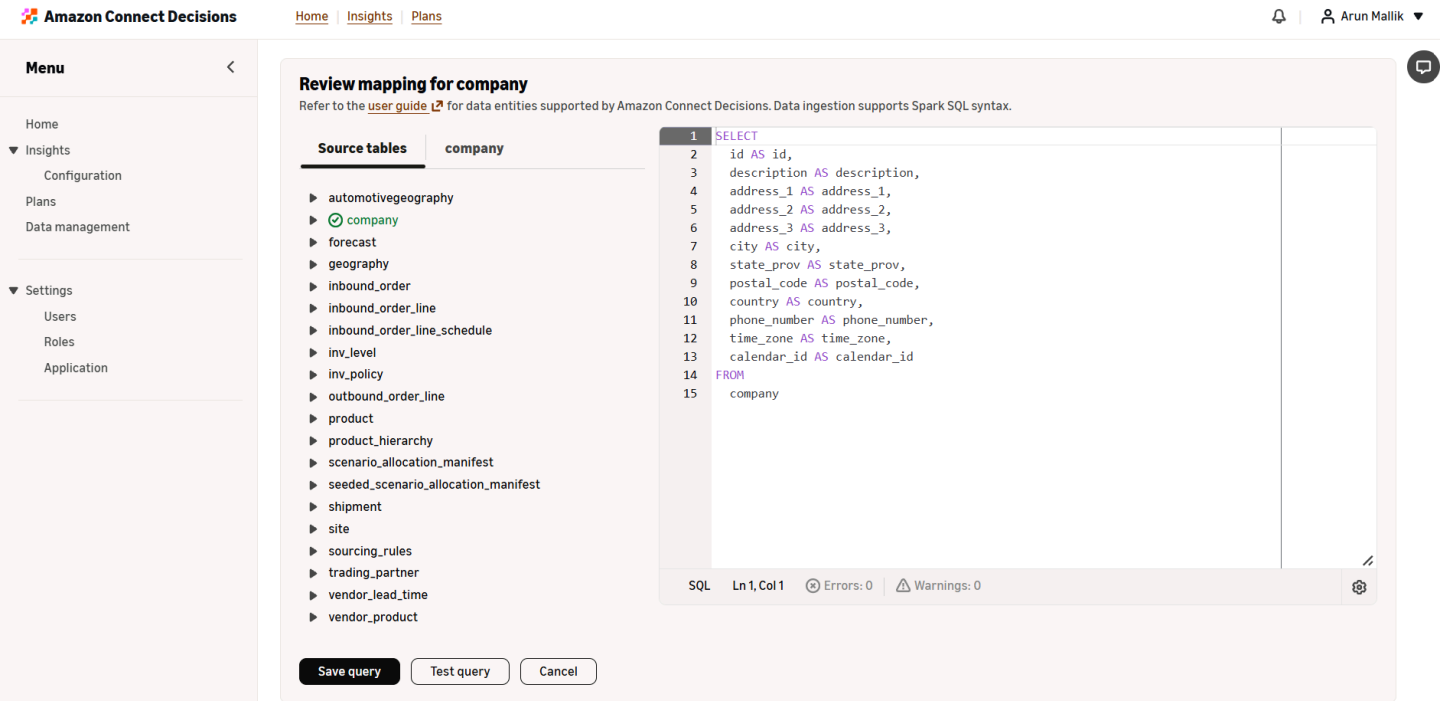
送信先タブ

マッピングを受け入れると、データ管理内の送信先タブに移動し、以下を実行できます。

- 送信先フローを確認する
- マッピングの管理と編集 (「フローの管理」)
- 古いフローを削除する
- これらのフローの実行ステータスを確認する



「フローの管理」を選択すると、データマッピングエクスペリエンスに戻り、データエージェントと連携して時間の経過とともにマッピングを絞り込むことができます。



ソースタブ

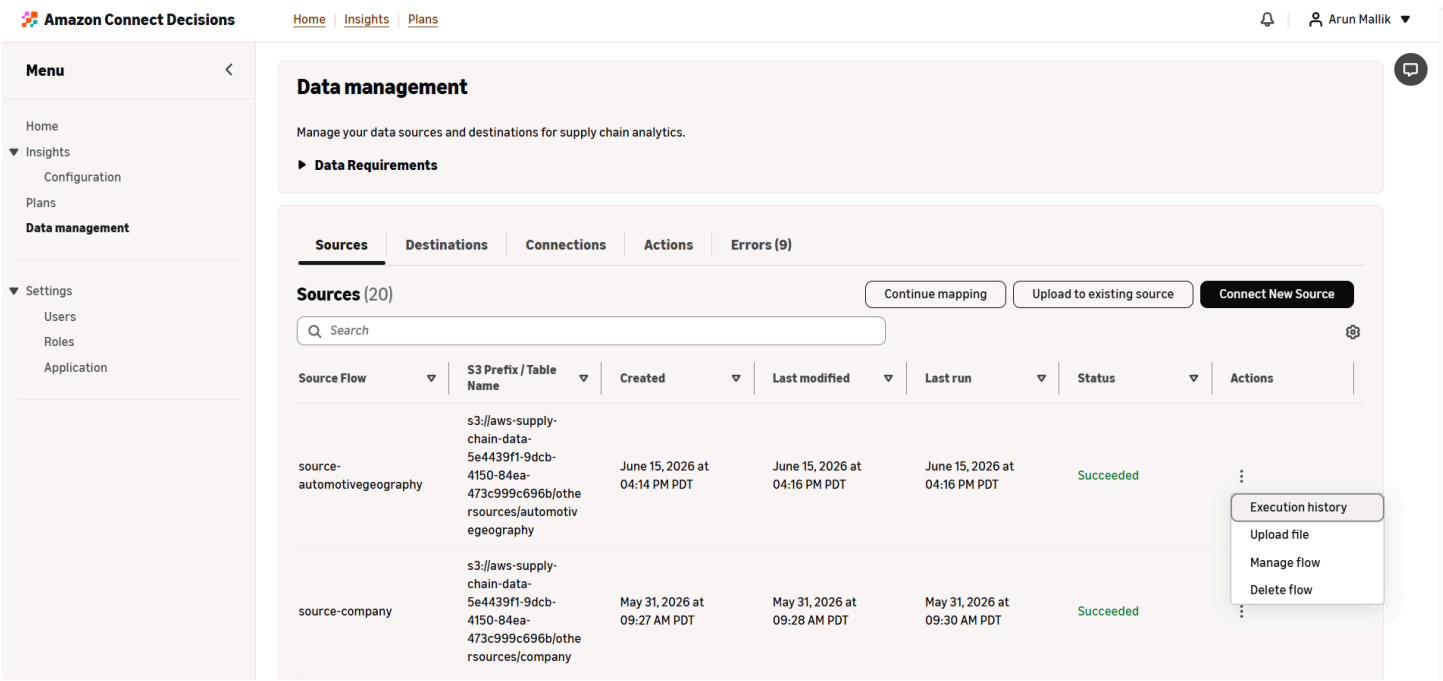
ソースタブに戻ります。

- 作成されたソースデータセット
- 関連付けられた S3 バケット

- 以下のオプション:
  - 別のファイルアップロードを介してソースデータを追加する
  - フローを管理する
  - フローを削除する
  - 実行の確認

「フローの管理」を選択すると、データマッピングエクスペリエンスに戻り、データエージェントと連携して時間の経過とともにマッピングを絞り込むことができます。

また、必要に応じて新しいソースを作成して、新しいデータソースのデータオンボーディングプロセスを再起動することもできます。



ベストプラクティス

データ準備

- 「前提条件」セクションのステップに従う
- すべての CSV ファイルで UTF-8 エンコードを使用する
- ファイル名が一意であることを確認する
- アップロード前にデータ品質を検証する

データエージェントの使用

- リクエストに具体的に記述する
- 決定事項がわからない場合は説明を求める
- 受け入れる前にすべての SQL 変更をテストする
- プレビュー機能を使用して変換を検証する

継続的なメンテナンス

- ソースデータを最新の状態に保つ
- フロー実行を定期的にモニタリングする
- 通知されたらすぐにデータエラーに対処する
- チームのカスタム変換を文書化する

JDBC を使用したデータベースへの接続

このガイドでは、Java Database Connectivity (JDBC) を使用してデータベースを Amazon Connect Decisions に接続する方法について説明します。データベース認証情報の安全な暗号化を設定し、Amazon Connect Decisions がデータにアクセスするために使用できる接続を確立します。

JDBC 接続とは何ですか? いつ使用すべきですか?

JDBC 接続を使用すると、Amazon Connect Decisions は既存のデータベースに接続してデータを読み取ることができます。CSV ファイルをエクスポートしてアップロードしたり、独自の抽出、変換、ロード (ETL) パイプラインを S3 にセットアップしたりする必要はありません。このアプローチは、次の場合に最適です。

- データはすでに AWS Glue 互換のリレーショナルデータベースに保存されています。互換性のあるデータベースとバージョンについては、このガイドを参照してください。
- 手動ファイルエクスポートなしでnear-real-timeデータアクセスが必要
- データボリュームが大きく、頻繁に更新される
- データを複製するのではなく、現在の場所に保持したい
- より小さなデータセットを使用する場合や、ファイルベースのアップロードを優先する場合は、必要に応じて標準の CSV アップロードプロセスがよりシンプルになる場合があります。このプロセスの詳細については、「データオンボーディングユーザーガイド」を参照してください。

前提条件

開始する前に、以下があることを確認してください。

- KMS キーと Secrets Manager リソースを作成するアクセス許可を持つ AWS アカウント
- AWS アカウント ID と Amazon Connect Decisions が動作するリージョン
- データベース接続の詳細: ホスト名、ポート、データベース名、認証情報
- 接続を検証するためのデータベースへの管理アクセス
- AWS サービスからの接続を受け入れるように設定されたデータベース

カスタマー管理の KMS キーを作成する

データベースを Amazon Connect Decisions に接続する前に、データベース認証情報の暗号化を設定する必要があります。AWS Key Management Service (KMS) は、このセキュリティレイヤーを提供し、接続の詳細を確実に保護します。

KMS キーを作成する

1. AWS KMS コンソールに移動する
   - ブラウザで AWS マネジメントコンソールを開く
   - 上部の検索バーに「KMS」と入力し、結果から「Key Management Service」を選択します。
   - これにより、暗号化キーを管理する KMS ダッシュボードが開きます。
2. キーの作成を開始する
   - KMS ダッシュボードで、右上のキーの作成ボタンを見つけてクリックします。
   - これにより、キー作成ウィザードが開始され、セットアッププロセスが案内されます。
3. キータイプと使用法を設定する
   - 「キーの設定」ページで、キータイプとして対称を選択します (これはデフォルトおよび推奨オプションです) 。
   - キーの使用時に「暗号化と復号」を選択したままにする
4. キー識別の詳細を設定する
   - 「エイリアス」フィールドに、次のようにキーのわかりやすい名前を入力します。 `aws-supply-chain-database-key`
   - 「説明」フィールドに、Amazon Connect Decisions データベース認証情報の暗号化キー」などのコンテキストを追加します。

- 必要に応じて、AWS リソースの整理と追跡に役立つタグを追加します (例: Key: "Project"、Value: "Amazon Connect Decisions")。

5. 主要な管理アクセス許可を定義する
   - このキーを管理できる IAM ユーザーまたはロールを選択します (ポリシーの作成、削除、変更)
   - 少なくとも、必要に応じて後でキーを変更できるように、独自の管理者ロールを含めます。
   - これらの管理者はキーを管理できますが、暗号化/復号に使用するアクセス許可は自動的に付与されません。
   - 「キーの削除」セクションで、キー管理者にこのキーの削除を許可します (これはデフォルトおよび推奨オプションです) 。
6. キーの使用許可を定義する
   - このページには、 キーを使用できる IAM ユーザーとロールを選択するオプションが表示されます。
   - ここで特定のユーザーの選択をスキップし、次のステップでサービスアクセス許可を設定します。
7. Amazon Connect Decisions サービスのキーポリシーを設定する
   - デフォルトの JSON を含むポリシーエディタが表示されます。
   - KMS キーポリシーエディタで、既存の「Statement」配列に次のステートメントを追加します。
   - このポリシーは、アカウントにフルコントロールを付与し、Amazon Connect Decisions のサービス (Secrets Manager および Glue) がデータベース認証情報を復号できるようにします。

```
{
  "Sid": "Allow GDIS service to decrypt",
  "Effect": "Allow",
  "Principal": {
    "Service": "scn.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:DescribeKey",
    "kms:CreateGrant",
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource": "*"
}
```

8. レビューと確定

- 概要ページですべての設定を確認する
- エイリアス、説明、ポリシーが正しいことを確認します。
- 完了をクリックしてキーを作成します
- 作成されると、新しいキーがリストに表示される KMS ダッシュボードに戻ります。

期待すること

キーの作成は即時です。作成されると、KMS コンソールに「有効」というステータスの新しいキーが表示されます。これで、キーは Secrets Manager でデータベース認証情報を暗号化する準備ができました。

AWS Secrets Manager を設定する

KMS キーを取得したら、AWS Secrets Manager でシークレットを作成してデータベース認証情報を安全に保存し、Amazon Connect Decisions がこのシークレットにアクセスできるようにするリソースポリシーを設定します。

シークレットを作成する

1. AWS Secrets Manager に移動する
   - AWS マネジメントコンソールの検索バーに「Secrets Manager」と入力します。
   - 結果から「Secrets Manager」を選択してサービスダッシュボードを開きます。
2. 新しいシークレットの作成を開始する
   - 新しいシークレットを保存するボタンをクリックします。
   - 「シークレットタイプを選択」ページで、他のタイプのシークレットを選択します (これにより、認証情報を柔軟に構成できます) 。
3. データベース認証情報を入力する
   - キーと値のペアセクションで、データベース接続の詳細を文字列として追加します。

```
Key: username, Value: your database username
Key: password, Value: your database password
Key: host, Value: your database hostname (e.g., database.example.com)
Key: port, Value: your database port (e.g., 3306 for MySQL)
Key: database, Value: your database name
```

4. 暗号化キーを選択する

- 「暗号化キー」で、AWS KMS キーの選択を選択します
- ドロップダウンから、ステップ 1 で作成した KMS キーを選択します (例: `aws-supply-chain-database-key`)。
- これにより、認証情報がカスタマーマネージドキーで暗号化されます。

5. シークレットに名前を付ける
   - シークレットのわかりやすい名前を入力します。 `aws-supply-chain-production-database`
   - 必要に応じて、Amazon Connect Decisions 本番環境のデータベース認証情報」などの説明を追加します。
   - 組織に必要なタグを追加する (例: Key: "Environment"、Value: "Production")
6. リソースアクセス許可を追加する
   - 「アクセス許可の編集」をクリックします。ポリシーエディタで、次のポリシーを貼り付けます。このポリシーは、Amazon Connect Decisions のサービスがシークレットを読み取ることを許可します。

```
{
  "Version" : "2012-10-17",
  "Statement" : [ {
    "Effect" : "Allow",
    "Principal" : {
      "Service" : "scn.amazonaws.com"
    },
    "Action" : [ "secretsmanager:GetSecretValue", "secretsmanager:DescribeSecret" ],
    "Resource" : "<COPY-THE-SECRET-ARN-HERE-AFTER-CREATING>"
  } ]
}
```

7. ポリシーを保存する
   - 保存をクリックしてリソースポリシーを適用します
   - ポリシーがアクティブになり、Amazon Connect Decisions がデータベース認証情報を取得できるようになりました。
8. ローテーションを設定する (オプション)
   - この設定では、自動ローテーションを無効にするを選択して自動ローテーションをスキップできます。
   - セキュリティポリシーで必要な場合は、後でローテーションを有効にできます。
9. 確認と作成

- すべてのシークレットの詳細を確認する
- Store をクリックしてシークレットを作成します。
- Secrets Manager ダッシュボードに戻ります。

10.シークレット ARN を保存する

- シークレットリストで新しく作成したシークレットを検索する
- シークレット名をクリックして詳細ページを開きます。
- 上部にシークレット ARN が表示されます。
- この ARN をコピーして保存する
- ARN 形式は次のようになります。 `arn:aws:secretsmanager:us-east-1:123456789012:secret:aws-supply-chain-production-database-AbCdEf`

11.リソースのアクセス許可を編集する

- 「アクセス許可の編集」をクリックします。
- コピーしたシークレット ARN を貼り付け、コピーした ARN <COPY-THE-SECRET-ARN-HERE-AFTER-CREATING>に置き換えます。
- 保存をクリックしてポリシーをアタッチする

期待すること

これで、シークレットは KMS キーで安全に保存および暗号化されます。Amazon Connect Decisions のサービスには、データベース接続を確立するときに認証情報を取得するアクセス許可がありますが、認証情報は保管中および転送中に暗号化されたままです。

データベースを Amazon Connect 決定に接続する

KMS キーとシークレットを設定したら、Amazon Connect Decisions で JDBC 接続を確立する準備が整います。

JDBC 接続を設定する

1. Amazon Connect Decisions > Data Management に移動する
   - Amazon Connect Decisions インスタンスにログインする
   - メインナビゲーションから「データ管理」を選択します。
   - タブナビゲーション内で「Connections」に移動します。
   - 「新しい接続」を選択して新しい接続を作成します。

2. 接続の詳細を入力する

- 接続名 (必須): この接続の一意の識別子 (「production-database」など) を入力します。
- 説明 (オプション): この接続の目的と使用に関する詳細を追加して、チームがアクセスするデータを理解するのに役立ちます。
- JDBC URL (必須): 完全な JDBC 接続文字列を 形式で入力します `jdbc:<database-type>://<hostname>:<port>/<database>` (例: `jdbc:postgresql://db.example.com:5432/mydb`)。
- スキーマ名 (オプション): 必要に応じてデータベーススキーマを指定します (「パブリック」、「dbo」、「myschema」など) 。データベースのデフォルトスキーマを使用するには、空白のままにします。
- シークレット ARN (必須): ステップ 2 で保存したシークレット ARN を貼り付けます。これにより、Amazon Connect Decisions は Secrets Manager からデータベース認証情報を安全に取得できます。
- SSL 接続を強制する: データベース接続に SSL/TLS 暗号化を要求するには、このチェックボックスを選択したままにします (推奨) 。
- VPC エンドポイントサービス名 (必須): AWS PrivateLink を介したプライベート接続用の VPC エンドポイントサービス名を入力します (形式: `com.amazonaws.vpce.<region>.vpce-svc-xxxxxxxxx`)

3. データベースに接続する

- 「Connect」をクリックして、接続をテストして確立します。Amazon Connect Decisions は、提供された認証情報を使用してデータベースに正常に接続できることを確認します。このステップには最大 2 分かかる場合があるため、接続中にこの画面を離れないでください。
- 接続が成功すると、テーブル選択に自動的に移動します。
- 接続が失敗した場合:
  - 接続の詳細を確認して、すべてのフィールドが正確であることを確認します。
    - シークレット ARN が正しいことを確認する
    - データベース認証情報が正確であることを確認する
    - JDBC URL 形式が正しいことを確認します。
    - AWS のサービスからの接続を受け入れるようにデータベースが設定されていることを確認します。
    - KMS キーと Secrets Manager ポリシーが正しく設定されていることを確認します。

- チャットエクスペリエンスを使用して、「データベース接続が失敗する理由」などの質問をすることで、接続の問題のトラブルシューティングに役立てることもできます。または「JDBC 接続のデバッグを手伝ってください」

4. 取り込むテーブルを選択する
   - 接続すると、データベースから使用可能なすべてのテーブルがテーブルの選択画面に表示されます。
   - 取り込む各テーブルの横にあるチェックボックスをオンにします。
5. テーブルの更新スケジュールを設定する
   - 選択したテーブルごとに、アクション列の 3 つのドットメニューをクリックし、「スケジュールの更新」を選択します。
   - ロードの詳細の設定ダイアログで、以下を設定します。
     - 頻度: 更新する頻度 (時間単位、日単位、週単位、またはカスタム)
     - 開始時間: 更新を開始する時間 (タイムゾーンオフセットで UTC で表示)
     - 更新タイプ: 完全な更新 (すべてのデータを置き換える) または増分更新 (既存の に新しいデータを追加する。タイムスタンプを記録する列を選択する必要がある) を選択します。
     - 必要に応じてテーブルごとに繰り返します。
   - すべてのテーブルが設定されている場合にマッピングを開始するをクリックします。
6. データマッピングを続行する
   - この時点から、エクスペリエンスはデータオンボーディングフローと同じです。
   - Data Onboarding ユーザーガイドの「データマッピング」セクションに従ってセットアップを完了します。

予想されること

接続が確立され、テーブルが選択されると、Amazon Connect Decisions はデータベースからデータを読み取ることができます。接続はアクティブで安全であり、認証情報は AWS Secrets Manager を通じて暗号化および管理されます。Amazon Connect Decisions で認証情報を手動で更新する必要はありません。Secrets Manager で行った変更は、自動的に反映されます。

ベストプラクティス

セキュリティとアクセスの管理

- 認証情報を安全に保存する: 常に AWS Secrets Manager を使用してデータベース認証情報を保存し、接続文字列や設定ファイルに認証情報をハードコードしないでください。
- SSL/TLS 暗号化を有効にする: 転送中にデータが暗号化されるように、「SSL 接続の強制」オプションを有効にしておきます。
- KMS および Secrets Manager ポリシーを定期的に確認する: 承認されたサービスとアカウントのみが暗号化キーとシークレットにアクセスできることを確認します
- 最小特権アクセスを使用する: Amazon Connect Decisions が接続に使用する必要最小限のアクセス許可のみをデータベースユーザーに付与します

接続設定

- わかりやすい接続名を使用する: 環境と目的を示すわかりやすい名前を選択します (例 : 「db1」ではなくproduction-inventory-db」) 。
- 接続を文書化する: 説明フィールドを使用して、接続がアクセスするデータ、その所有者、および特別な考慮事項を書き留めます。
- 続行する前に接続をテストする: テーブルを選択し、更新スケジュールを設定する前に、必ず接続が機能することを確認してください。
- JDBC URL 形式を検証する: 接続エラーを避けるために、JDBC URL 構文がデータベースタイプと一致することを再確認します。

データ更新戦略

- 適切な更新頻度を選択する: ソースデータの変更頻度とビジネスニーズに基づいて更新頻度を選択します。
- 低アクティビティ期間中に更新をスケジュールする: データベースの負荷が低い場合に更新時間を設定し、パフォーマンスへの影響を最小限に抑える
- 可能な場合は増分更新を使用する: 頻繁に変更される大規模なデータセットの場合、増分更新は完全な更新よりも効率的です
- 意味のあるタイムスタンプ列を選択する: 増分更新を使用する場合は、レコードがいつ作成または変更されたかを正確に反映する列を選択します。

トラブルシューティングのためのチャットの使用

- リクエストに具体的に記述する: 接続のトラブルシューティングや問題のマッピングにヘルプを求めるときは、明確なコンテキストを提供します。
- 説明を求める: 推奨事項や生成された SQL クエリがわからない場合は、明確化を求める
- 受け入れる前にすべての SQL 変更をテストする: プレビュー機能を使用して、変換が実際のデータで期待どおりに機能することを確認します。
- トラブルシューティングにチャットを活用する: 接続が失敗したり、更新で エラーが発生した場合は、「接続が失敗する理由」などの診断用の質問をしてください。または「この更新エラーについて教えてください」

継続的なメンテナンス

- 更新の実行を定期的にモニタリングする: Data Management の Destinations and Sources タブをチェックして、更新が正常に完了していることを確認します。
- エラーに迅速に対処する: Amazon Connect Decisions が エラーの更新を警告した場合、データギャップを回避するために問題を迅速に調査して解決する
- 認証情報を安全に更新する: データベースパスワードが変更された場合、AWS Secrets Manager で更新すると、Amazon Connect Decisions は自動的に新しい認証情報を使用します。
- カスタム設定を文書化する: チームのリファレンス用に、特別な更新スケジュール、変換ロジック、または接続要件についてメモしておきます。
- テーブルの選択を定期的に確認する: データのニーズが進化するにつれて、取り込むテーブルと、更新スケジュールがビジネス要件に合っているかどうかを再検討します。

正規データモデル (CDM) について

正規データモデル (CDM) は、 で使用される標準化されたデータ構造です。サプライチェーンデータをオンボードするときは、 がそれを計画、予測、運用上のインサイトのために処理できるように、CDM 形式に変換する必要があります。

このトピックでは、CDM とは何か、重要な理由、使用可能なデータエンティティについて説明します。

CDM とは

CDM は、製品、サイト、注文、出荷、在庫などのサプライチェーンの概念を表す一般的なデータエンティティとフィールドのセットを定義します。ソースデータの形式や構造に関係なく、CDM は、すべての機能で が使用する単一の整合性のあるスキーマを提供します。

データオンボーディング中、ソースデータは CDM 送信先テーブルにマッピングされます。データエージェントは、ソースフィールドと CDM フィールド間のマッピングを自動的に提案し、SQL 変換クエリを生成してデータを変換できます。

CDM が重要な理由

- 整合性 — のすべての機能は同じデータ構造で動作するため、需要計画、在庫の最適化、リードタイムインサイトにわたって一貫した動作が保証されます。
- 相互運用性 — さまざまなソースシステム (ERP、WMS、TMS) からのデータは 1 つのモデルに正規化され、システム間の分析が可能になります。
- オンボーディングの簡素化 — データエージェントは、自動マッピングを生成するときにターゲットスキーマとして CDM を使用し、手動作業を減らします。
- データ品質 — 検証チェックは CDM 定義に対して実行され、データが本番環境で使用される前に問題を検出します。

データエンティティカテゴリ

CDM データエンティティは 2 つのカテゴリに分類されます。

- 非トランザクションデータ — 製品、サイト、取引相手、地域など、頻繁に変更されない参照データまたはマスターデータ。
- トランザクションデータ — 予測、在庫レベル、注文、出荷など、頻繁に変化する運用データ。

サポートされているデータエンティティ

次の表に、CDM でサポートされているすべてのデータエンティティを示します。

サポートされている CDM データエンティティ

データエンティティ	データの種類	必須
Company	非トランザクションデータ	はい
製品	非トランザクションデータ	はい
取引先	非トランザクションデータ	はい
ベンダー製品	非トランザクションデータ	はい
Geography	非トランザクションデータ	はい
製品階層	非トランザクションデータ	はい
輸送レーン	非トランザクションデータ	はい
ベンダーリードタイム	非トランザクションデータ	はい
サイト	非トランザクションデータ	はい
ベンダーの休日	非トランザクションデータ	はい
Forecast	トランザクションデータ	はい
Inventory	トランザクションデータ	はい
インバウンド注文 (PO/STO)	トランザクションデータ	はい
アウトバウンド注文明細	トランザクションデータ	はい
Shipment	トランザクションデータ	はい
インベントリポリシー	トランザクションデータ	はい
インバウンド注文明細 (PO/STO)	トランザクションデータ	はい
アウトバウンド出荷	トランザクションデータ	はい

データエンティティ	データの種類	必須
インバウンド注文明細スケジュール	トランザクションデータ	はい

機能に必要なエンティティ

のすべての機能にすべての CDM エンティティが必要なわけではありません。以下のセクションでは、各機能に必須、オプション、または適用できないエンティティについて説明します。

インベントリの可視性

インベントリを可視化するための CDM エンティティ

データエンティティ	データの種類	必須
Company	非トランザクション	オプションです。
製品	非トランザクション	はい
取引先	非トランザクション	オプションです。
ベンダー製品	非トランザクション	該当しない
地域別	非トランザクション	オプションです。
製品階層	非トランザクション	オプションです。
輸送レーン	非トランザクション	オプションです。
ベンダーリードタイム	非トランザクション	該当しない
サイト	非トランザクション	はい
ベンダーの休日	非トランザクション	該当しない
Forecast	トランザクション	オプションです。
Inventory	トランザクション	はい
インバウンド注文 (PO/STO)	トランザクション	オプションです。

データエンティティ	データの種類	必須
アウトバウンド注文明細	トランザクション	オプションです。
Shipment	トランザクション	オプションです。
インベントリポリシー	トランザクション	はい
インバウンド注文明細	トランザクション	オプションです。
アウトバウンド出荷	トランザクション	オプションです。
インバウンド注文明細スケジュール	トランザクション	オプションです。

リードタイムに関するインサイト

リードタイムインサイトの CDM エンティティ

データエンティティ	データの種類	必須
Company	非トランザクション	オプションです。
製品	非トランザクション	はい
取引先	非トランザクション	はい
ベンダー製品	非トランザクション	はい
地域別	非トランザクション	オプションです。
製品階層	非トランザクション	オプションです。
輸送レーン	非トランザクション	はい
ベンダーのリードタイム	非トランザクション	はい
サイト	非トランザクション	はい
ベンダーの休日	非トランザクション	オプションです。

データエンティティ	データの種類	必須
Forecast	トランザクション	該当しない
Inventory	トランザクション	該当しない
インバウンド注文 (PO/STO)	トランザクション	はい
アウトバウンド注文明細	トランザクション	該当しない
Shipment	トランザクション	はい
インベントリポリシー	トランザクション	該当しない
インバウンド注文明細	トランザクション	はい
アウトバウンド出荷	トランザクション	該当しない
インバウンド注文明細スケジュール	トランザクション	はい

需要計画

需要計画用の CDM エンティティ

データエンティティ	データの種類	必須
Company	非トランザクション	オプションです。
製品	非トランザクション	はい
取引先	非トランザクション	該当しない
ベンダー製品	非トランザクション	該当しない
地域別	非トランザクション	オプションです。
製品階層	非トランザクション	オプションです。
輸送レーン	非トランザクション	該当しない

データエンティティ	データの種類	必須
ベンダーのリードタイム	非トランザクション	該当しない
サイト	非トランザクション	はい
ベンダーの休日	非トランザクション	該当しない
Forecast	トランザクション	該当しない
Inventory	トランザクション	該当しない
インバウンド注文 (PO/STO)	トランザクション	該当しない
アウトバウンド注文明細	トランザクション	はい
Shipment	トランザクション	該当しない
インベントリポリシー	トランザクション	該当しない
インバウンド注文明細	トランザクション	該当しない
アウトバウンド出荷	トランザクション	該当しない
インバウンド注文明細スケジュール	トランザクション	該当しない

CDM とデータオンボーディングの関係

データを にオンボードすると、プロセスは次のステップに従います。

1. アップロード — ソースデータを CSV ファイルとして Amazon S3 にアップロードします。
2. マップ — データエージェントはソースデータセットを分析し、データに最適な CDM 送信先テーブルを提案します。
3. 変換 — SQL 変換クエリは、ソースデータ形式を CDM 形式に変換します。
4. 検証 — 品質チェックは変換されたデータに対して実行され、CDM 要件に準拠していることを確認します。
5. アクティブ化 — 検証されると、データは に流れ、機能で使用できるようになります。

データのオンボーディングに関するstep-by-step手順については、「データオンボーディング」トピックを参照してください。

データ検証と品質チェック

概要

データ検証により、Amazon Connect Decisions 機能を実行する前にデータが品質要件を満たしていることを確認できます。システムは、設定された計画、メトリクス、ルールに基づいてデータを検証し、パフォーマンスをブロックまたは低下させる可能性のある問題を特定します。

データ検証の仕組み

検証トリガー

データ検証は、次のタイミングで自動的に実行されます。

- Insights 設定の変更: メトリクス、ルール、またはその他の設定を作成または変更する場合
- 計画の作成: アドホック計画を作成するとき、またはスケジュールされた計画の実行ごとに
- データ更新: 送信先フローへの各データ更新後
- 機能の実行: AI チームメイトのオペレーションの前または最中 (例: 例外を根本的に引き起こしたり、レコメンデーションを決定したりする場合)

検証タイプ

Amazon Connect Decisions は 2 種類の検証を実行します。

データ存在検証は、設定されたリソース (メトリクス、ルール、プラン) に基づいて、必要なデータセットとフィールドがロードされていることを確認します。

Data Quality Validation は、提供されたデータが、以下を含むセットアップ設定に基づいて品質要件を満たしていることを検証します。

- セットアップ基準の検証: 製品とサイトがルール基準 (製品カテゴリ、サイトの場所など) と一致することを確認します
- 階層の検証: セットアップで階層を使用する場合に、欠落している階層関係を識別します
- スコープの検証: 特定された製品とサイトに必要なすべてのデータが存在することを確認します

- 品質評価: 運用要件のデータ品質とユーザビリティを評価します

プログレッシブ検証

Amazon Connect Decisions は、データセット全体の機能をブロックするのではなく、有効なデータを持つ製品やサイトの機能を有効にします。検証の問題が特定の製品またはサイトに影響を与えると、システムは有効なデータを含む製品とサイトの処理を継続し、データの問題のある製品またはサイトを識別し、注意が必要な特定の項目を警告します。これにより、残りのデータ問題を解決しながら 機能の使用を開始できます。

データ検証エラーへのアクセス

データ検証エラーは、次の 3 つのエントリポイントで表示できます。

1. ホームページの「データ検証エラー」メトリクス
2. ホームページのデータ検証エラートピックカード
3. 左ナビゲーションの「データ管理」 >「エラー」タブ

検証エラーの確認

エラーページには、開いている検証エラーと解決された検証エラーがすべて表示されます。次のいずれかの列で検索およびフィルタリングできます。

- ID: 検証エラーの一意の識別子
- ステータス
  - オープン: エラーは解決されていません
  - 解決済み: エラーが修正および検証されました
- 説明: データ品質の問題の説明
- 問題タイプ
  - 必須データがない: オペレーションをトリガーするための必須データが提供されていない (例: Supply Plan の outbound_order_line ソーステーブルがない)
  - 無効なデータ値: データが存在するが、誤った値 (負の製品コストなど) が含まれている
  - 関係がない: 必要な階層関係または参照関係がない (製品階層がないなど)
  - 不十分なデータ: 必要なオペレーションを実行するのに十分なデータがない (例えば、需要計画には 12 か月の履歴注文データが必要だが、3 か月しか存在しない)

- 機能: 影響を受ける機能またはリソース
  - 供給計画
  - 需要計画
  - インサイト (供給または需要の例外、推奨事項、RCA を含む)
- 送信先: 影響を受ける送信先フロー
- 優先度
  - 重大: 少なくとも 1 つの機能が完全にブロックされており、実行できない
  - 高: 少なくとも 1 つの機能が部分的にブロックされている (一部の製品またはサイトを処理できない)
  - 中: 少なくとも 1 つの機能の精度が低下しています (は実行されますが、結果が低下します)
- 作成日時: エラーが最初に検出された日時を示すタイムスタンプ

エラーの詳細の表示

詳細情報を表示するには、エラーを選択します。詳細画面には、上記の情報と、Last Occurred On タイムスタンプ、関連するリソースとリンク (問題の影響を受ける機能を表すメトリクス、ルール、またはプラン) 、およびデータ検証エラーのマニフェスト方法を示す最大 100 行の影響を受けるデータのプレビューが表示されます。

使用可能なアクション

エラーの詳細画面から、次のことができます。

- トラブルシューティング: AI チームメイトを起動して自然言語による問題のトラブルシューティングを支援し、詳細な修復ガイダンスを受け取ります。
- エラーの解決: 根本的な問題を修正した場合は、エラーを手動で解決済みとしてマークします。
- ダウンロード: 詳細な分析と修正のために、影響を受けるデータセット全体をダウンロードする

データ検証エラーの解決

解決ワークフロー

1. エラーの説明と優先度を確認して、影響を理解する
2. 影響を受けるデータのプレビューを確認して、影響を受ける特定のレコードを確認します。
3. 修復のために提供された特定の推奨事項に従う

4. 適切なアクションを選択します。
   - 設定の問題の場合: マネージャーやプランナーと協力して、メトリクス、ルール、または計画の設定を調整します。
   - マッピングの問題の場合: アップロードされたソースデータを修正するか、データ変換とマッピングを更新します。
   - 欠落データまたは無効なデータの場合: 修正されたデータをアップロードする
5. 根本的な問題に対処したら、エラーを手動で解決済みとしてマークします

AI チームメイトの使用

トラブルシューティングオプションを使用して、「最初にどのエラーに焦点を当てるべきですか？」などの質問をします。または「どのエラーが需要計画をブロックしていますか？」、問題とその影響の詳細な説明を受け取り、解決アプローチに関するstep-by-stepガイダンスを取得し、エラーが特定の設定にどのように影響するかを理解します。AI チームメイトは、Amazon Connect Decisions 内およびソースデータシステム内で問題を解決するためのガイドとして行動できます。

ベストプラクティス

- 重要度で優先順位を付ける: 機能の実行を完全にブロックするため、まず重大なエラーに焦点を当てます。次に、処理を部分的にブロックする高優先度エラーに対処し、その後に精度を低下させる中優先度の問題が続きます。
- 推奨事項を慎重に確認する: 各エラーには、設定に基づいて問題に合わせた具体的で実用的なガイダンスが含まれています。
- プログレッシブ検証を利用する: 機能を使用する前に、すべてのエラーを解決するのを待たないでください。システムは、他のユーザーの問題を解決する作業中に、有効な製品とサイトの機能を有効にします。
- データ更新後のモニタリング: 各データ更新後に新しい検証エラーをチェックして、本番環境のワークフローに影響を与える前に問題を早期に検出します。
- 影響を受けるデータを戦略的にダウンロードする: プレビュー以外の影響を受けるすべてのレコードを分析する必要がある場合、または完全なデータセットをデータチームに提供する必要がある場合は、ダウンロードオプションを使用します。
- 複雑な問題に AI チームメイトを使用する: トラブルシューティングオプションは、特定の状況や設定に適応するコンテキストに応じたサポートを提供します。
- 解決の確認: データの問題を修正したら、エラーを手動で解決済みとしてマークして、修正が成功したことを確認し、オープンリストから削除します。

システム設定

Amazon Connect Decisions の設定は、スコープと対象者別に整理されています。一部の設定は個人用であり、各ユーザーが独自のエクスペリエンスを調整できます。その他には、管理者が管理するインスタンスレベルの設定があり、すべてのユーザーに対するシステムの動作や、より広範なテクノロジー環境への接続方法に影響します。

ユーザーレベルの設定により、個人はアカウント情報、通知設定、データアクセス範囲がビューにどのように適用されるかを管理できます。

インスタンスレベルの設定により、管理者は組織全体のアクセスコントロールフィルターの動作を設定し、ERP やその他の外部システムへの接続を確立し、システムが推奨されるアクションを処理する方法を定義できます。

これらの設定を組み合わせることで、組織全体の一貫性を維持しながら、特定の運用コンテキストに Amazon Connect Decisions を柔軟に適応させることができます。

ユーザープロファイルの設定

ユーザーは、アプリケーションの右上隅にある自分の名前を選択し、ドロップダウンメニューからプロファイルを選択することで、プロファイル設定にアクセスできます。プロファイルページでは、ユーザーはアカウント情報、通知設定、データアクセス設定を管理できます。

プロファイル設定へのアクセス

プロファイル設定にアクセスするには:

1. ページの右上隅にある名前を選択します。
2. ドロップダウンメニューからプロファイルを選択する
3. プロファイルページには、アカウント情報と設定が表示されます。

プロファイル情報

プロファイルページには、次のアカウントの詳細が表示されます。

ユーザー: ユーザー名

ロール: 割り当てられたロール (管理者、マネージャー、またはプランナー)

タイムゾーン: ドロップダウンメニューから任意のタイムゾーンを選択します。この設定により、Amazon Connect Decisions 全体で日付と時刻がどのように表示されるかが決まります。

E メール: Amazon Connect Decisions アカウントに関連付けられた E メールアドレス

作成日時: アカウントが作成された日時

更新: プロファイルが最後に変更された日時

右上隅にある保存 を選択して、プロファイル情報への変更を保存します。

通知設定

通知設定タブでは、さまざまなシステムイベントの通知の受信方法を設定できます。アプリケーション、E メール、またはその両方で通知を受信するように選択できます。

プラン

計画生成の成功: 計画生成が正常に完了したときに通知を受け取る方法を選択します。オプションには、アプリ内通知と E メール通知が含まれます。

計画生成の失敗: 計画生成が失敗したときに通知を受け取る方法を選択します。オプションには、アプリ内通知と E メール通知が含まれます。

Insights の設定

Insights Configurations Succeeded: Insights 設定が正常に完了したときに通知を受け取る方法を選択します。オプションには、アプリ内通知が含まれます。

インサイト設定の失敗: インサイト設定が失敗したときに通知を受け取る方法を選択します。オプションには、アプリ内通知が含まれます。

データ取り込み

データ取り込み失敗: データ取り込みが失敗したときに通知を受け取る方法を選択します。オプションには、アプリ内通知と E メール通知が含まれます。

管理者設定

管理者は、すべてのユーザーに適用されるシステム全体の通知設定を構成できます。

通知保持期間: システムから通知が自動的に削除されるまでの日数を設定します。保持期間を指定するには、数値を入力します。

保存を選択して、通知設定を適用します。

割り当てられたスコープ

割り当てられたスコープタブにはデータアクセス許可が表示され、割り当てられたスコープに基づいてデータビューをフィルタリングする方法を設定できます。

データアクセス

このセクションでは、現在のデータアクセスレベルを表示します。すべてのサイトと製品にアクセスできる場合は、「すべてのサイトと製品にアクセスできる」というメッセージが表示されます。

デフォルトビューフィルター

割り当てられたスコープでビューをフィルタリングする: 有効にすると、データビューは自動的にフィルタリングされ、割り当てられた製品とサイト内の項目のみが表示されます。この設定は、必要に応じてオンまたはオフを切り替えます。

このフィルターを有効にすると、割り当てられたスコープに関連する例外、計画、その他のデータのみが表示されます。無効にすると、ロールのアクセス許可によっては、割り当てられた範囲外のデータが表示される場合があります。

保存を選択してフィルター設定を適用します。

アクセスコントロールフィルターの切り替え

前述のように、すべてのユーザーは、適切な製品とサイトが設定されているかどうかに関係なく、すべての例外を表示できます (変更アクションには適切なアクセスが必要です) 。これにより、知識の共有が容易になりますが、特定の製品やサイトのみに焦点を当てているユーザーは、他の製品やサイトの例外やレコメンデーションに圧倒される可能性があります。ユーザーが自分にとって重要な例外と推奨事項に集中できるように、次のようにアクセスビューの切り替えを使用できます。

- まず、「管理者」ロールを持つユーザーは、そのインスタンスでこの機能を有効にする必要があります。左側のナビゲーションバーからインスタンス設定ページに移動します。
- デフォルトでは、インスタンス全体のデフォルトのアクセスビューフィルターを設定するトグルが表示されます。「Admin」は、インスタンス内のすべてのユーザーに 1 つの統一された設定を設定するか、ユーザーに自分の設定を決定させることができます。

- 統合アクセスビューのトグル設定を選択した場合、「管理者」はすべてのユーザーに対してトグルを有効または無効にするかどうかを決定することもできます。
- 各ユーザーが独自の設定を選択できるようにする場合、各ユーザーにはアクセスビューフィルターを自分で切り替えるオプションがあります。各ユーザーは、画面の右上隅にあるユーザードロップダウンからユーザー設定ページに移動できます。

インスタンスのアクセスコントロールの切り替えを変更します。

1. 左側のドロワーの設定を選択します。
2. アプリケーションを選択する
3. トグルとクリックの保存設定を更新する

設定が有効になっている場合、システムは例外と推奨事項のリストページを自動フィルタリングして、アクセスコントロール設定に一致する製品またはサイトに対して生成されたページのみを表示します。

「すべての製品とサイトへのフルアクセスの付与」が有効になっているユーザーの場合、アクセスビューの切り替えには引き続きすべての例外と推奨事項が表示されます。ユーザーがそのトグルを無効にしているが、製品やサイトが設定されていない場合、システムはそれを製品やサイトにアクセスできないと解釈するため、ユーザーには何も表示されません。

アクセスビューフィルターは別のタイプのフィルターと見なされるため、例外とレコメンデーションページのフィルターチップには表示されません。ユーザーは、他の製品やサイトのフィルターなど、以前と同じ方法で他のフィルターを適用できます。

アクセスビューの切り替えをオフにした場合、またはユーザーに直接ハイパーリンクがある場合でも、ユーザーは他の製品の例外とレコメンデーションに引き続きアクセスできます。

ERP への接続の設定

Amazon Connect Decisions が Enterprise Resource Planning (ERP) システムでユーザーに代わってオペレーションを実行できるようにするには、必要な接続パラメータと Amazon Connect Decisions がオペレーション中に使用する認証情報を指定する接続を設定する必要があります。

サポートされている ERP システム:

- SAP S/4HANA

Secrets Manager で認証情報を設定する

1. アカウントを使用して Secrets Manager を使用して Secrets Manager シークレットを作成する
   - Secrets Manager に認証情報を入力するときは、以下のプレースホルダー値 (<username> と <password>) を Amazon Connect Decisions が使用する実際のユーザー名とパスワードに置き換えます。
   - コンソールを使用する場合は、 `Other type of secret` Secret Type
   - コンソールのKey/value pairsタブから詳細を入力する場合は、2 つのペアを入力します。
     - キー: username、値: <*username*>
     - キー: password、値: <*password*>
   - Plaintext タブを使用してコンソールにシークレットを入力する場合は、2 つのペアを含む JSON オブジェクトを入力します。

```
{
  "Username": "<username>",
  "Password": "<password>"
}
```

2. KMS AWS キーでシークレットを暗号化し、キーの ID を書き留めます。後続のステップで必要になります。
3. シークレットが作成されたら、以降のステップで必要になるため、Amazon リソースネーム (ARN) を書き留めます。
   - 例: arn:aws:secretsmanager:<Region>:<AccountId>:secret:<SecretName>-<SixRandomCharacters>

KMS キーに対するアクセス許可を設定する

Amazon Connect Decisions がアクセスして使用するために必要なアクセス許可を提供する必要があります。

1. KMS ポリシーを更新して、Amazon Connect Decisions がインスタンスロールを介してキーにアクセスできるようにします。
   - 注: <YourAccountNumber>と を自分の AWS アカウントと Amazon Connect 決定インスタンス ID <YourInstanceID>に置き換えます。

```
{
```

```
    "Sid": "Allow Amazon Connect Decisions to access the AWS KMS Key",
    "Effect": "Allow",
    "Principal": {
       "Service": "scn.amazonaws.com",
        "AWS": "arn:aws:iam::YourAccountNumber:role/service-role/scn-instance-
role-YourInstanceID"
    },
    "Action": [
       "kms:DescribeKey",
       "kms:CreateGrant",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey",
       "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*"
}
```

2. インスタンスロールのインラインポリシーを更新して、キーに対するアクセス許可を付与する

- 注: <YourSecretArn>、<YourAccountNumber>、 をシークレット ARN、 AWS アカウント、 AWS サプライチェーンインスタンス ID <YourInstanceID>に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Action": "secretsmanager:*",
            "Resource": "YourSecretArn"
        },
        {
            "Sid": "AllowKmsForSecretsManager",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:DescribeKey"
            ],
            "Resource": "arn:aws:kms:us-east-1:YourAccountNumber:key/YourKeyId"
        }
    ]
}
```

シークレットの Secrets Manager リソースポリシーを更新する

1. シークレットの Secrets Manager リソースポリシーを更新する
   - 注: をシークレットの ARN <YourSecretArn>に置き換えます。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"scn.amazonaws.com"
         },
         "Action":[
            "secretsmanager:GetSecretValue",
            "secretsmanager:DescribeSecret"
         ],
         "Resource":"YourSecretArn"
      }
   ]
}
```

Amazon Connect 決定接続を設定する

1. Amazon Connect Decisions のインスタンスで、データ管理ページに移動します。
2. Connections タブを選択する
3. [Create Connection] ボタンをクリックします。
4. Create Connector ページで、SAP S/4HANAコネクタタイプの行のSelectボタンをクリックします。
5. Configure SAP S/4HANA API Connector ページに必要な情報を入力します。
   - Connection Name: 一意の接続名
   - API Endpoint URL: SAP S/4HANA インスタンスの OData API エンドポイント URL (例: https://<hostname>:<port>)
   - Client Number: 3 桁の SAP クライアント番号 (例: 100)
   - Secret ARN: Amazon Connect Decisions で使用される認証情報が保存されている Secrets Manager のシークレットの Amazon リソースネーム (ARN)

6. Create Connector ボタンをクリックする

アクション設定の構成

Amazon Connect Decisions を使用すると、Enterprise Resource Planning (ERP) システムでユーザーに代わってオペレーションを実行するために提供するアクションタイプを制御できます。デフォルトでは、すべてのアクションタイプが無効になっており、必要なアクションタイプごとにこの機能を有効にする必要があります。

> **Note**
>
> 特定のアクションタイプのサポートを有効にすると、ユーザーに代わってアクションを実行する Amazon Connect Decisions のオプションがシステム全体に表示されるかどうかが制御されます (例: 特定のタイプのレコメンデーションでインサイトを確認する場合) 。Amazon Connect Decisions は、特定のレコメンデーションを受け入れるまで (サポートが有効になっている場合でも) 、これらのアクションを実行しません。

サポートされているアクションタイプ:

- 発注書の作成
- 発注書の更新
- 発注書のキャンセル

各アクションタイプのアクションサポートを設定します。

1. Amazon Connect Decisions のインスタンスで、データ管理ページに移動します。
2. Actions タブを選択する
3. リストで設定するアクションタイプを検索する
4. アクションタイプのサポートを有効にするには:
   - そのアクションタイプのドロップダウンメニューに表示されている接続のいずれかを選択します。
   - 注意: ドロップダウンには、 Actions機能をサポートするタイプ (例: SAP S/4HANA) で設定された使用可能な接続のみが表示されます。
5. アクションタイプのサポートを無効にするには:

- そのアクションタイプのドロップダウンメニューNo connectionで を選択します。

6. Save クリックして変更を保存します。

セキュリティ

のクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、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を活用できます。

セキュリティは、 AWS お客様とお客様の間の責任共有です。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して説明しています。

- クラウドのセキュリティ – AWS は、 で AWS サービスを実行す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、 では、安全に使用できるサービスも提供しています。AWS コンプライアンスプログラムの一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。Amazon Connect Decisions に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、「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。
- クラウド内のセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、ユーザーは、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、Amazon Connect を使用するために、責任共有モデルを適用する方法を理解するのに役立ちます。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ように Amazon Connect Decisions を設定する方法について説明します。

データ保護

責任 AWS 共有モデルは、Amazon Connect Decisions でのデータ保護に適用されます。このモデルで説明されているように、 AWS はすべての AWS クラウド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。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 サービスのセキュリティ設定および管理タスクについても責任を負います。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の「AWS の責任共有モデルと 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、 AWS アカウントの認証情報を保護し、 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アクセス許可のみを各ユーザーに付与できます。また、次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 AWS リソースと通信します。TLS 1.2 以降が推奨されます。
- 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。
- AWS 暗号化ソリューションと、 サービス内のすべての AWS デフォルトのセキュリティコントロールを使用します。
- 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。これは、Amazon Simple Storage Service に保存されている機密データの検出と保護に役立ちます。
- 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 140-2 検証済みの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) 140-2」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、 マネジメントコンソール、API、 AWS Command Line Interface (AWS CLI)、または SDK を使用して AWS Amazon Connect Decisions または他の AWS サービスを使用する場合も同様です。 AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。

データ暗号化

このトピックでは、転送中の暗号化と保管中の暗号化に関する Amazon Connect の決定に固有の情報を提供します。

転送中の暗号化

顧客と Amazon Connect Decisions 間、および Amazon Connect Decisions とそのダウンストリームの依存関係間のすべての通信は、TLS 1.2 以降の接続を使用して保護されます。

保管中の暗号化

Amazon Connect Decisions は、DynamoDB と Amazon Simple Storage Service (Amazon S3) を使用して保管中のデータを保存します。保管中のデータは、デフォルトで暗号化ソリューションを使用して AWS 暗号化されます。Amazon Connect Decisions は、 () の AWS AWS Key Management Service 所有暗号化キーを使用してデータを暗号化しますAWS KMS。データを暗号化する AWS マネージドキーを保護するためのアクションを実行する必要はありません。詳細については、AWS KMS デベロッパーガイド の「AWS 所有キー」を参照してください。

AWS コンソールで Amazon Connect Decisions インスタンスのデータの暗号化に使用する KMS キーを変更する場合は、新しいインスタンスを作成して、新しいキーを使用してデータを暗号化する必要があります。前のキーで暗号化されたデータは保持されず、データのみが更新されたキーで暗号化されます。以前の暗号化方法のデータを維持する場合は、それらの会話中に使用していたキーに戻すことができます。

ウェブアプリおよびチャットアプリケーションでの Amazon Connect Decisions との会話は、AWS 所有のキーでのみ暗号化されます。

クロスリージョン処理

Amazon Connect Decisions は Amazon Bedrock を利用しており、クロスリージョン推論 (CRIS) を使用して異なる AWS リージョンにトラフィックを分散し、大規模言語モデル (LLM) 推論のパフォーマンスと信頼性を向上させます。クロスリージョン推論を使用すると、以下が可能になります。

- 高需要期間中のスループットと耐障害性の向上
- パフォーマンスの向上
- Amazon Bedrock でホストされている最も強力な LLMs に依存する、新しく起動された Amazon Connect Decisions 機能へのアクセス

クロスリージョン推論は、Amazon Connect Decisions インスタンスが作成された AWS リージョンによって動作が異なります。

米国の地理的リージョンで作成されたすべてのインスタンスについて、Amazon Connect Decisions は Global CRIS を使用します。つまり、推論リクエストは世界中のサポートされている商用 AWS リージョンにルーティングされ、利用可能なリソースを最適化してモデルスループットが向上します。Global CRIS の詳細については、Amazon Bedrock ユーザーガイドを参照してください。

EU の地理的リージョンで作成されたすべてのインスタンスについて、Amazon Connect Decisions は地理的 CRIS を使用します。つまり、推論リクエストは、データが最初に存在する地域の一部である AWS リージョン内に保持されます。地理的 CRIS の詳細については、Amazon Bedrock ユーザーガイドを参照してください。

例えば、米国東部 (バージニア北部) (us-east-1) リージョンで作成された Amazon Connect Decisions インスタンスから行われたリクエストは、アジアパシフィック (シドニー) (ap-southeast-2) などのグローバル AWS リージョンにルーティングできます。ただし、欧州 (アイルランド) (eu-west-1) リージョンで作成された Amazon Connect Decisions インスタンスから行われたリクエストは、欧州 (フランクフルト) (eu-central-1) などの欧州内の AWS リージョンにルーティングされます。詳細については、Amazon Connect Decisions でサポートされているリージョン」を参照してください。

クロスリージョン推論はデータの保存場所を変更しませんが、リクエストと出力結果がデータが存在するリージョン外に移動する可能性があります。すべてのデータは Amazon の安全なネットワーク経由で暗号化されて送信されます。クロスリージョン推論の使用に追加コストはかかりません。Amazon Connect Decisions を使用する際のデータの保存先については、Amazon Connect Decisions でのデータ保護」を参照してください。

Amazon Connect 決定の IAM

AWS Identity and Access Management (IAM) は、AWS リソースへのアクセスを管理者が安全に制御するために役立つ AWS のサービスです。IAM 管理者は、誰を認証 (サインイン) し、誰に Amazon Connect Decisions 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、AWS のサービスであり、追加料金は発生しません。

IAM と Amazon Connect Decisions の連携方法

IAM を使用して Amazon Connect Decisions へのアクセスを管理する前に、Amazon Connect Decisions で使用できる IAM 機能を確認してください。Amazon Connect Decisions 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については、IAM ユーザーガイドの「IAM と連携する AWS のサービス」を参照してください。

Amazon Connect Decisions のアイデンティティベースのポリシー

ID 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。

Amazon Connect Decisions 内のリソースベースのポリシー

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、フェデレーティッドユーザー、または AWS サービスを含めることができます。

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。

Amazon Connect Decisions のポリシーアクション

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。

Amazon Connect Decisions 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"
         ]
```

Amazon Connect Decisions のポリシーリソース

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": "*"
```

Amazon Connect Decisions のポリシー条件キー

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。

Amazon Connect Decisions での一時的な認証情報の使用

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イ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 と連携する IAM および AWS サービスの一時的なセキュリティ認証情報」を参照してください。 https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_aws-services-that-work-with-iam.html

Amazon Connect Decisions の転送アクセスセッション

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、 AWS サービスを呼び出すプリンシパルのアクセス許可と、リクエスト元の AWS サービスを組み合わせて、ダウンストリームサービスにリクエストを行いま

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。

Amazon Connect Decisions のサービスロール

サービスロールのサポート: あり

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、IAM ユーザーガイドの「 AWS サービスにアクセス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、Amazon Connect Decisions の機能が破損する可能性があります。Amazon Connect Decisions が指示する場合にのみ、サービスロールを編集します。

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 Amazon Connect Decisions 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はできません。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。

インスタンス管理 IAM ポリシー

以下は、コンソールまたはパブリック API (すべての Webapp オペレーションを除く) を使用してインスタンスを作成、更新、または削除するために必要な IAM ポリシーです。

```
{
    "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": [
                "cloudwatch:PutMetricData",
                "cloudwatch:Describe*",
                "cloudwatch:Get*",
                "cloudwatch:List*"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "organizations:CreateOrganization",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:EnableAWSServiceAccess",
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "kms:ListAliases"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "iam:CreateRole",
                "iam:CreatePolicy",
                "iam:GetRole",
                "iam:PutRolePolicy",
                "iam:AttachRolePolicy",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
```

```
            "Action": [
                "sso:AssociateDirectory",
                "sso:AssociateProfile",
                "sso:CreateApplication",
                "sso:CreateApplicationAssignment",
                "sso:CreateInstance",
                "sso:CreateManagedApplicationInstance",
                "sso:DeleteApplication",
                "sso:DeleteApplicationAssignment",
                "sso:DeleteManagedApplicationInstance",
                "sso:DescribeApplication",
                "sso:DescribeDirectories",
                "sso:DescribeInstance",
                "sso:DescribeRegisteredRegions",
                "sso:DescribeTrusts",
                "sso:DisassociateProfile",
                "sso:GetManagedApplicationInstance",
                "sso:GetPeregrineStatus",
                "sso:GetProfile",
                "sso:GetSharedSsoConfiguration",
                "sso:GetSsoConfiguration",
                "sso:GetSSOStatus",
                "sso:ListApplicationAssignments",
                "sso:ListApplicationTemplates",
                "sso:ListDirectoryAssociations",
                "sso:ListInstances",
                "sso:ListProfileAssociations",
                "sso:ListProfiles",
                "sso:PutApplicationAuthenticationMethod",
                "sso:PutApplicationGrant",
                "sso:RegisterRegion",
                "sso:SearchDirectoryGroups",
                "sso:SearchDirectoryUsers",
                "sso:SearchGroups",
                "sso:SearchUsers",
                "sso:StartPeregrine",
                "sso:StartSSO",
                "sso:UpdateSsoConfiguration",
                "sso-directory:SearchUsers"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
```

```
}
```

ポリシーに関するベストプラクティス

ID ベースのポリシーは、アカウント内で誰かが Amazon Connect Decisions 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を実行すると、 AWS アカウントに追加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 – 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 AWS アカウントで使用できます。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、アクセス許可を絞り込む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 管理ポリシー」または「職務機能用の AWS 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 AWS サービスを通じて使用されている場合に、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 – AWS アカウントで IAM ユーザーまたはルートユーザーを要求するシナリオがある場合は、セキュリティを強化するために MFA をオンにします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、IAM ユーザーガイド の MFA を使用した安全な API アクセス を参照してください。

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

IAM のトラブルシューティング

以下の情報は、Amazon Connect Decisions と IAM を使用する際に発生する可能性がある一般的な問題の診断と修正に役立ちます。

Amazon Connect Decisions でアクションを実行する権限がありません

アクションを実行する権限がない AWS マネジメントコンソールの場合は、管理者に連絡してサポートを依頼する必要があります。担当の管理者はお客様のユーザー名とパスワードを発行した人です。

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

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

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

iam:PassRole を実行する権限がない

`iam:PassRole` アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して Amazon Connect Decisions 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 サービスでは、新しいサービスロールまたはサービスにリンクされたロールを作成する代わりに、既存のロールをそのサービスに渡すことができます。そのためには、サービスにロールを渡すアクセス許可が必要です。

次の例のエラーは、 という IAM ユーザーがコンソールを使用して Amazon Connect Decisions `marymajor` でアクションを実行しようとすると発生します。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アクセス許可が必要です。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。

AWS アカウント以外のユーザーに Amazon Connect Decisions リソース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:

- Amazon Connect Decisions がこれらの機能をサポートしているかどうかを確認するには、Amazon Connect Decisions と IAM の連携方法」を参照してください。
- 所有している AWS アカウント間で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「所有している別の AWS アカウントの 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。
- サードパーティーアカウントに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 AWS 「サードパーティーが所有する AWS アカウントへのアクセスを提供する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、IAM ユーザーガイド の 外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可 を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

サードパーティーのサブプロセッサ

Amazon Connect Decisions は、サードパーティー API である Boomi を使用して、ユーザーに代わって外部システムでアクションを実行できるようにします。サードパーティーシステムに接続する Amazon Connect Decisions の機能を使用する場合、お客様は、Boomi を統合ミドルウェアとして使用して暗号化されたデータを送信および処理することを当社に許可します。お客様のデータは Boomi 内に個別に保存されません。

Boomi とその仕組みの詳細については、Boomi の公開ドキュメントを参照してください。

サポート対象のリージョン

このページでは、Amazon Connect Decisions を使用できる AWS リージョンについて説明します。AWS リージョンの詳細については、「 アカウント管理リファレンスガイド」の「アカウントで使用できる AWS リージョンを指定する」を参照してください。 AWS

データは、Amazon Connect Decisions を使用するリージョンとは異なるリージョンで処理される場合があります。Amazon Connect Decisions でのクロスリージョン処理の詳細については、「クロスリージョン処理」を参照してください。処理中にデータが保存される場所については、データ保護に関する説明を参照してください。

サポート対象のリージョン

Amazon Connect Decisions は、 AWS 以下の AWS リージョンの AWS マネジメントコンソール、コンソールモバイルアプリケーション、 AWS ウェブサイト、 AWS ドキュメントウェブサイトで利用できます。これらのリージョンはデフォルトで有効になっています。つまり、使用前に有効にする必要はありません。詳細については、デフォルトで有効になっているリージョンの説明を参照してください。

Amazon Connect Decisions は、次のリージョンで使用します。

AWS リージョン名	コード名	地域 (米国、欧州など)
米国東部 (バージニア北部)	us-east-1	米国
欧州 (アイルランド)	eu-west-1	EU

トラブルシューティング

Amazon Connect Decisions のセットアップ中またはday-to-day使用中に問題が発生した場合、このセクションは最も一般的な問題の診断と解決に役立つガイダンスを提供します。まず、発生している問題に最も一致するカテゴリを特定し、関連するページのトラブルシューティングステップに従います。どのカテゴリが適用されるかわからない場合は、初期設定の問題を最も広範囲にカバーする一般的なセットアップの問題から始めます。

一般的なセットアップの問題

参照整合性エラー: "product_id values do not match any id in Product dataset"

最も一般的な原因は、ID フィールドの末尾に空白があることです。固定幅データベースからエクスポートするソースシステムは、多くの場合、文字列フィールドをスペースで埋めます。製品マスターにはクリーン IDsMAT604」) があり、注文明細ファイルにはパディング IDs」) があります。MAT604 システムは厳密な文字列一致を行うため、これらは結合されません。

修正: データフロー SQL 変換のすべての文字列 ID フィールドに TRIM() を追加します。product_id、ship_from_site_id、customer_tpartner_id、およびその他の結合キーに適用します。また、ファイル間の引用の不整合も確認します。CSVs、QUOTE_ALL を使用して、数値表示 IDs (「111613」など) が 1 つのファイルで整数として扱われ、別のファイルで文字列として扱われる型推論の問題を防止します。

防止: 現在問題が表示されていなくても、SQL 変換のすべての ID フィールドをデフォルトのプラクティスとして常に TRIM します。ソースデータはエクスポート間で変更される可能性があります。

注文履歴の製品が製品マスターにない

注文履歴には、多くの場合、現在の製品マスターに含まれていない製品 (廃止された製品、1 回限りのアイテム、テスト SKUs) が含まれます。product_id に一致する製品マスターレコードがない場合、システムは注文ファイル全体を拒否します。

修正: (a) 最小限の必須フィールド (id、説明、base_uom) で欠落している製品の製品マスターにスタブ行を作成するか、(b) 注文履歴をフィルタリングして製品マスターに存在する製品のみを含めます。オプション (a) は、系統や傾向の検出に役立つ可能性のある需要履歴を保持するため、推奨されます。

製品マスターのアップロード時の CSV 解析エラー

カンマ、引用符、特殊文字を含む製品の説明は、CSV 解析を中断する可能性があります。特定の行に「予想 17 フィールド、19 フィールドを表示」などのエラーが表示される場合があります。

修正: 適切な引用符 (QUOTE_ALL) を使用してファイルを再エクスポートします。説明フィールドに埋め込まれたカンマがないか、特定の失敗した行を確認します。

アップロード後にデータが表示されない

- ファイル形式が変更されていないことを確認します (拡張子、列ヘッダー、エンコーディング)。
- ファイル名と拡張子が想定パターンと一致することを確認します。.csv を .csv000 などに変更すると、取り込みが中断されます。
- アップロード後にデータインジェストが完了するまでに最大 30 分かかります。
- 列ヘッダーがロード間で変更される場合 (月/年で という名前の列など)、アップロード前に前処理ステップが必要です。

データ更新後に PIV が更新されない

- PIV は、取り込みが完了してから約 15 分後にトリガーされ、実行までに約 20～30 分かかります。
- データアップロードから新しい PIV へのEnd-to-end: 約 1～1.5 時間。
- PIV が 24 時間以上更新されていない場合は、 サポートにお問い合わせください。

例外カウントが高すぎるか低すぎるように見える

- 高すぎる: しきい値が大きすぎるか、単一の product+site が異なる日付に対して複数の例外を生成している可能性があります。サポートに連絡して、ルール設定を確認してください。
- 低すぎる: しきい値が過度に制限されているか、一部の製品で必要なデータ (予測、インベントリレベルなど) が欠落している可能性があります。

よく知っているいくつかの製品をスポットチェックし、システムに表示されるものとソースシステムを比較します。

例外に対する財務上の影響なし

財務上の影響には、ユニットコストを製品データに入力する必要があります。製品のコストが欠落しているかゼロの場合、ドル値は表示されません。コストデータカバレッジについてサポートチームに確認してください。複数のコストフィールドにわたるウォーターフォールアプローチは通常、最適なカバレッジを提供します。

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。