Administratorhandbuch

# Amazon Connect Connect-Entscheidungen

# Amazon Connect Connect-Entscheidungen: Administratorhandbuch

# Table of Contents

# Was ist Amazon Connect Decisions

Amazon Connect Decisions ist eine Supply-Chain-Planungs- und Informationslösung mit KI-Teamkollegen, die mit Ihrem Team zusammenarbeiten, um Nachfragesignale zu Konsensprognosen zu harmonisieren, beschränkungsbewusste Angebotspläne zu erstellen und Ihre Abläufe aktiv zu überwachen, um Probleme zu vermeiden, Probleme zu lösen und Grundursachen für kontinuierliche Verbesserungen zu ermitteln.

KI-Teammitglieder passen sich an Ihre Arbeitsweise an: Sie orientieren sich an Ihren Betriebsabläufen und Regeln, integrieren sich in Ihre bestehenden Systeme und lernen aus den Entscheidungen Ihrer Praktiker. Es nutzt das Fachwissen von Amazon in der Lieferkette, um vom ersten Tag an effektive Pläne und Empfehlungen zu liefern.

Sie leiten ein Team von KI-Agenten, die sich um die Koordination und Durchführung von Maßnahmen kümmern, sodass Sie sich auf strategische Entscheidungen konzentrieren können, die das Serviceniveau und die Effizienz des Betriebskapitals verbessern.

## Vorteile

Passen Sie sich Ihrem Unternehmen an

KI-Teamkollegen passen sich an Ihr Unternehmen, Ihre Systeme und Entscheidungen an und sorgen so schnell für eine Transformation Ihrer bestehenden Workflows. Die Teammitglieder orientieren sich an Ihren Betriebsabläufen und Geschäftsregeln und arbeiten mit Ihren vorhandenen Planungs- und ERP-Systemen. Sie lernen aus den Entscheidungen der Planer, orientieren sich an Ihren Prioritäten und institutionalisieren Wissen, sodass Ihre Abläufe im Laufe der Zeit besser werden und jedes Teammitglied effektiver ist.

Bleiben Sie dem, was kommt, einen Schritt voraus

Leite ein Team von KI-Agenten, die sich um die Koordination kümmern 24/7 — indem sie Bedarfssignale harmonisieren, Pläne erstellen, die Einschränkungen berücksichtigen, und genehmigte Aktionen ausführen. Teammitglieder erkennen auch Muster, die für manuelle Analysen unsichtbar sind, wie z. B. kaskadierende Störungen bei Lieferanten oder Fehlausrichtungen bei Lagerbeständen bei Tausenden von SKUs, und finden heraus, worauf es ankommt, bevor es zu einem Problem wird. Planer wechseln von reaktiver Brandbekämpfung zu proaktiver Planung, führen effektivere Abläufe durch und verbessern das Serviceniveau durch strategische Entscheidungen, die zu Geschäftsergebnissen beitragen.

Bauen Sie vom ersten Tag an Vertrauen auf

KI-Teammitglieder werden durch wissenschaftliche Erkenntnisse unterstützt, die in mehr als 30 Jahren Erfahrung in der Betreuung von mehr als 400 Millionen Amazon-SKUs weiterentwickelt und mit speziellen Supply-Chain-Tools ausgestattet sind. Ihr Team profitiert von Fachwissen, das in einem der komplexesten Supply-Chain-Netzwerke der Welt gesammelt wurde. Es bietet sofort umsetzbare Erkenntnisse und Empfehlungen mit klaren, erklärbaren Argumenten, denen Sie vertrauen und die Sie überprüfen können.

# Capabilities

Adaptive Intelligenz

KI-Teamkollegen lernen aus jedem Plan und jeder Entscheidung in einem kontinuierlichen Kreislauf: Sie beobachten Muster, erkennen, worauf es ankommt, empfehlen Maßnahmen und führen genehmigte Entscheidungen aus. Dadurch wird Wissen institutionalisiert — wenn Planer gehen, bleibt Fachwissen erhalten. Neue Mitglieder sind vom ersten Tag an produktiv und verbessern die Ergebnisse ohne manuelle Umschulung.

Informationen nachfragen

KI-Teamkollegen orchestrieren dynamisch mehr als 18 Prognosetools und Basismodelle, die auf Amazon-Daten trainiert wurden, und optimieren selbstständig auf SKU-Ebene. Generieren Sie vom ersten Tag an genaue Prognosen, auch bei begrenzter Historie. Harmonisieren Sie statistische Prognosen, Kundenverpflichtungen und funktionsübergreifende Eingaben durch Konsensplanung bei gleichzeitiger kontinuierlicher Überwachung der Genauigkeit.

Liefern Sie Informationen

KI-Teammitglieder erstellen vorausschauende Angebotspläne (Vorschauversion) und fassen Ausnahmen intelligent zu strategischen Entscheidungen zusammen, die nach ihrer Wirkung geordnet sind. Führen Sie Optimierungsmodelle für eine engmaschige Planung in Ihrem gesamten Netzwerk durch. Überwachen Sie den Betrieb 24/7, finden Sie heraus, worauf es ankommt, und führen Sie dann genehmigte Entscheidungen direkt in bestehenden Systemen aus. So reduzieren Sie die Zyklen von Wochen auf Stunden.

Agentäres Onboarding

AI-powered Onboarding-Agenten führen Sie in natürlicher Sprache durch die Einrichtung. Verbinden Sie fragmentierte Daten über JDBC oder Amazon S3, bereiten Sie sie für Connect Decisions vor

und melden Sie Probleme automatisch, bevor sie sich auf Prognosen auswirken. Konfigurieren Sie Geschäftsregeln und Richtlinien in verständlicher Sprache mit Echtzeitvorschauen, sodass Sie innerhalb von Wochen statt Monaten einsatzbereit sind.

# Erste Schritte

In diesem Abschnitt erfahren Sie, wie Sie eine Amazon Connect Decisions-Instance erstellen, Benutzerberechtigungsrollen zuweisen und sich bei der Amazon Connect Decisions-Webanwendung anmelden.

## Voraussetzungen für die Nutzung von Amazon Connect Decisions

Bevor Sie eine Amazon Connect Decisions-Instance erstellen, stellen Sie sicher, dass Sie die folgenden Schritte ausführen:

- Sie haben ein AWS Konto. Informationen zum Erstellen eines AWS Kontos finden Sie unter Ein AWS-Konto einrichten.
- Stellen Sie sicher, dass IAM Identity Center aktiviert ist. Informationen zur Aktivierung von IAM Identity Center finden Sie unter IAM Identity Center aktivieren.
- Eine IAM Identity Center-Instance muss in derselben Region aktiviert sein, in der Sie Ihre Amazon Connect Decisions-Instance erstellen möchten. Amazon Connect Decisions wird nur in den Regionen USA Ost (Nord-Virginia) und Europa (Irland) unterstützt.
- Wenn sich die Amazon Connect Decisions-Instance nicht in derselben Region wie Ihre bestehende IAM Identity Center-Region befindet, kontaktieren Sie uns für weitere Unterstützung.
- Sie müssen mindestens einen Benutzer in der IAM Identity Center-Instance haben, den Sie als Amazon Connect Decisions-Administrator zuweisen können. Sie können Ihr Active Directory mit dem IAM Identity Center verbinden. Weitere Informationen finden Sie unter Connect zu einem Microsoft AD-Verzeichnis herstellen.
- Fügen Sie alle weiteren Benutzer, die Zugriff auf Amazon Connect Decisions benötigen, zum IAM Identity Center hinzu.
- Sie benötigen den AWS Key Management Service (AWS KMS), um eine Instance zu erstellen. Amazon Connect Decisions verwendet diesen AWS KMS-Schlüssel, um alle Daten zu verschlüsseln, die in Amazon Connect Decisions eingehen. Informationen zu AWS KMS-Schlüsseln finden Sie unter Schlüssel erstellen.
- Wenn Sie die Aktionsfunktion aktivieren möchten, müssen Sie eine Verbindung zu dem System konfigurieren, das Sie zur Verwaltung der relevanten Daten verwenden, und Anmeldeinformationen für Amazon Connect Decisions angeben. Bitte kontaktieren Sie uns für weitere Unterstützung.

# Von Amazon Connect Decisions unterstützte Browser

Bevor Sie mit Amazon Connect Decisions arbeiten, überprüfen Sie anhand der folgenden Tabelle, ob Ihr Browser unterstützt wird.

| Browser | Unterstützte Versionen |
| --- | --- |
| Google Chrome | Die letzten drei Versionen. |
| Mozilla Firefox ESR | Versionen werden bis zum Ende ihrer Lebensdauer von Firefox unterstützt. Einzelheiten finden Sie im Firefox ESR-Veröffentlichungskalender. |
| Mozilla Firefox | Die letzten drei Versionen. |
| Microsoft Edge und Edge Chromium | Version 84 und höher. |
| Safari | Safari 10 oder höher auf macOS. |

# Von Amazon Connect Decisions unterstützte Sprachen

Amazon Connect Decisions unterstützt die folgenden Sprachen:

- Englisch (USA)

# Einrichten eines AWS-Kontos

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

## Melden Sie sich an für ein AWS Konto

Wenn Sie noch kein AWS Konto haben, führen Sie die folgenden Schritte aus, um eines zu erstellen.

Um sich für ein zu registrieren AWS Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für ein AWS Konto registrieren, wird ein Root-Benutzer für das AWS Konto erstellt. Der Root-Benutzer hat Zugriff auf alle AWS -Services und -Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Benutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

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

## Erstellen eines Benutzers mit Administratorzugriff

Nachdem Sie sich für ein AWS Konto registriert haben, sichern Sie Ihren AWS Root-Benutzer, aktivieren Sie AWS IAM Identity Center und erstellen Sie einen Administratorbenutzer, damit Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Schützen Sie Ihre AWS Stammbenutzer des Kontos

1. Melden Sie sich als Kontoinhaber bei der AWS Management Console an, indem Sie Root-Benutzer auswählen und die E-Mail-Adresse Ihres AWS Kontos eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

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

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

Erstellen eines Benutzers mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

Anweisungen finden Sie unter Aktivieren von AWS IAM Identity Center im AWS IAM Identity Center-Benutzerhandbuch.

2. Gewähren Sie einem Administratorbenutzer im IAM Identity Center Benutzerzugriff.

   Ein Tutorial zur Verwendung des IAM Identity Center-Verzeichnisses als Identitätsquelle finden Sie unter Benutzerzugriff mit dem standardmäßigen IAM Identity Center-Verzeichnis konfigurieren im IAM Identity Center-Benutzerhandbuch.AWS

Anmelden als Administratorbenutzer

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im Benutzerhandbuch unter Anmeldung beim AWS Zugriffsportal.AWS Sign-In

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

   Anweisungen finden Sie im AWS IAM Identity Center-Benutzerhandbuch unter Einen Berechtigungssatz erstellen.

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

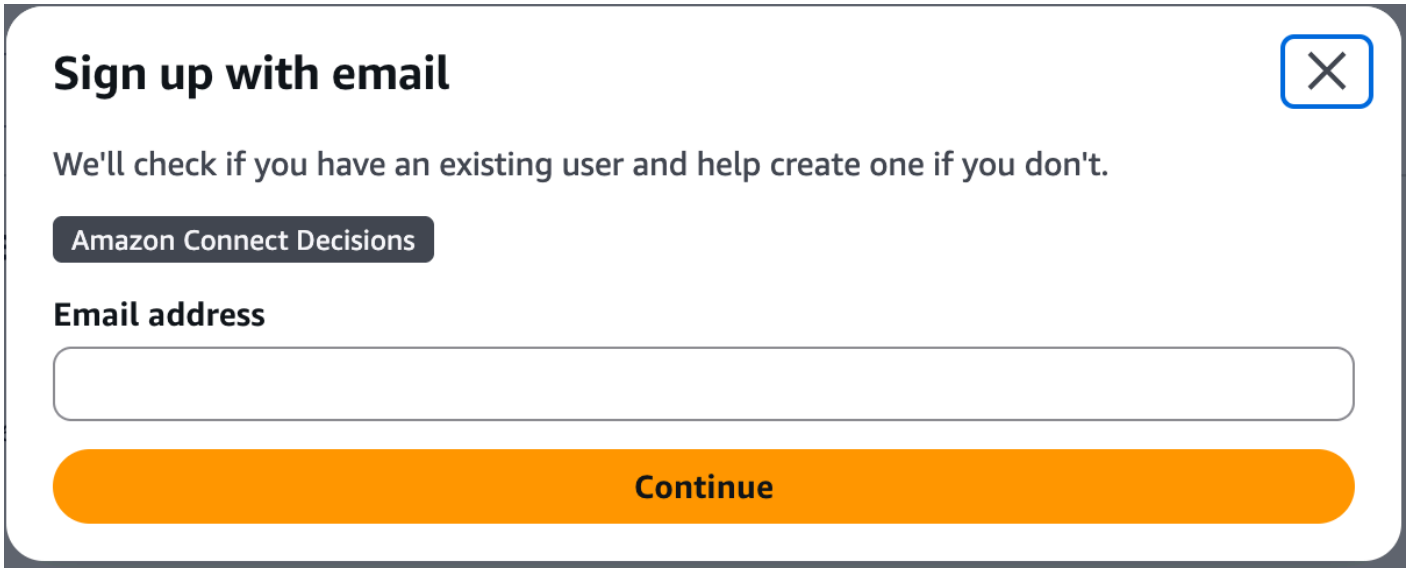
   Anweisungen finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center-Benutzerhandbuch.

# Konfiguration der AWS Identity Center-Integration

Um eine Instance zu erstellen und den Amazon Connect Decisions-Service zu verwenden, müssen Sie entweder ein vorhandenes IAM Identity Center-Benutzerprofil verbinden oder ein neues erstellen.

1. Öffnen Sie die Amazon Connect Decisions-Konsole. Sie können auch in der AWS Hauptverwaltungskonsole nach „Amazon Connect Decisions“ suchen.

2. Ändern Sie bei Bedarf die AWS-Region, indem Sie oben in der Konsole die Option Region auswählen auswählen auswählen auswählen. Wählen Sie Ihre Region aus der Drop-down-Liste aus.
3. Wählen Sie Amazon Connect Decisions-Instanz erstellen aus. Eine Benachrichtigung wird angezeigt.




4. Geben Sie Ihre E-Mail-Adresse ein und wählen Sie Weiter. iDC überprüft, ob die E-Mail mit einem vorhandenen Benutzer übereinstimmt.
5. Führen Sie eine der folgenden Aktionen aus:
   - Wenn iDC die E-Mail-Adresse einem Nutzer zuordnet, wählen Sie Connect your identity source aus und binden Sie Ihr Team ein.

     > **Note**
     >
     > Dies kann verwendet werden, wenn Ihre Organisation über eine etablierte IdC-Instance verfügt, die Sie für Amazon Connect Connect-Entscheidungen verwenden möchten.

   - Wenn IdC keine Übereinstimmung mit einem vorhandenen Benutzer findet, wird die Benachrichtigung „Neuen Benutzer erstellen“ angezeigt. Fahren Sie mit dem nächsten Schritt fort.
6. Geben Sie in der Benachrichtigung Folgendes ein und wählen Sie dann Weiter aus:
   - E-Mail-Adresse
   - Vorname
   - Nachname

IdC erstellt den Benutzer automatisch und fügt ihn als Amazon Connect Decisions-Administrator hinzu.

7. Führen Sie eine der folgenden Aktionen aus:
   - Um eine Instance mit der Standardkonfiguration zu erstellen, wählen Sie Create aus. Siehe Standardkonfiguration verwenden.
   - Um eine Instanz mit einer benutzerdefinierten Konfiguration zu erstellen, wählen Sie in den erweiterten Einstellungen die Option Bearbeiten aus. Siehe Erweiterte Konfiguration verwenden.

Bei Verwendung in Verbindung mit IAM Identity Center ruft Amazon Connect Decisions die Felder „Benutzername“ und „E-Mail“ aus dem IAM Identity Center-Verzeichnis ab. Keines dieser Attribute ist nativ in Ihrer Amazon Connect Decisions-Instance gespeichert und wird immer zur Laufzeit abgerufen. Amazon Connect Decisions verschlüsselt diese Identitätsattribute im Ruhezustand standardmäßig mit einem AWS eigenen KMS-Schlüssel. Vom Kunden verwaltete KMS-Schlüssel werden in Amazon Connect Connect-Entscheidungen nicht unterstützt. Wenn Sie einen Benutzer in Ihrer AWS IAM Identity Center-Instance löschen, löscht Amazon Connect Decisions diesen Benutzer auch aus Ihrer Instance.

# Verwaltung Ihrer Amazon Connect Decisions-Instance

Durch das Erstellen einer Instanz in Amazon Connect Decisions wird eine spezielle Umgebung für Supply-Chain-Management und Analysen eingerichtet. Um eine Instance einzurichten, konfigurieren Sie grundlegende Details, legen Einstellungen fest und definieren erste Benutzerzugriffsberechtigungen.

Nur der Administrator der AWS Management Console kann eine Instanz erstellen. Der AWS Management Console-Administrator, der die Amazon Connect Decisions-Instance erstellt, sollte über alle unter Identity-based Richtlinienbeispiele aufgeführten Berechtigungen verfügen. Dieser Administrator sollte einen IAM-Benutzer als Amazon Connect Decisions-Administrator einladen, um Amazon Connect Decisions zu verwalten.

Auf den folgenden Seiten wird der Vorgang zum Erstellen und Löschen einer Instance detailliert beschrieben.

## Ihre Instanz erstellen

Sie erstellen eine Instanz mit einer von zwei Methoden: Standardkonfiguration oder Erweiterte Konfiguration. Die Standardkonfiguration verwendet einen automatisierten Prozess, der Ihre Instanz

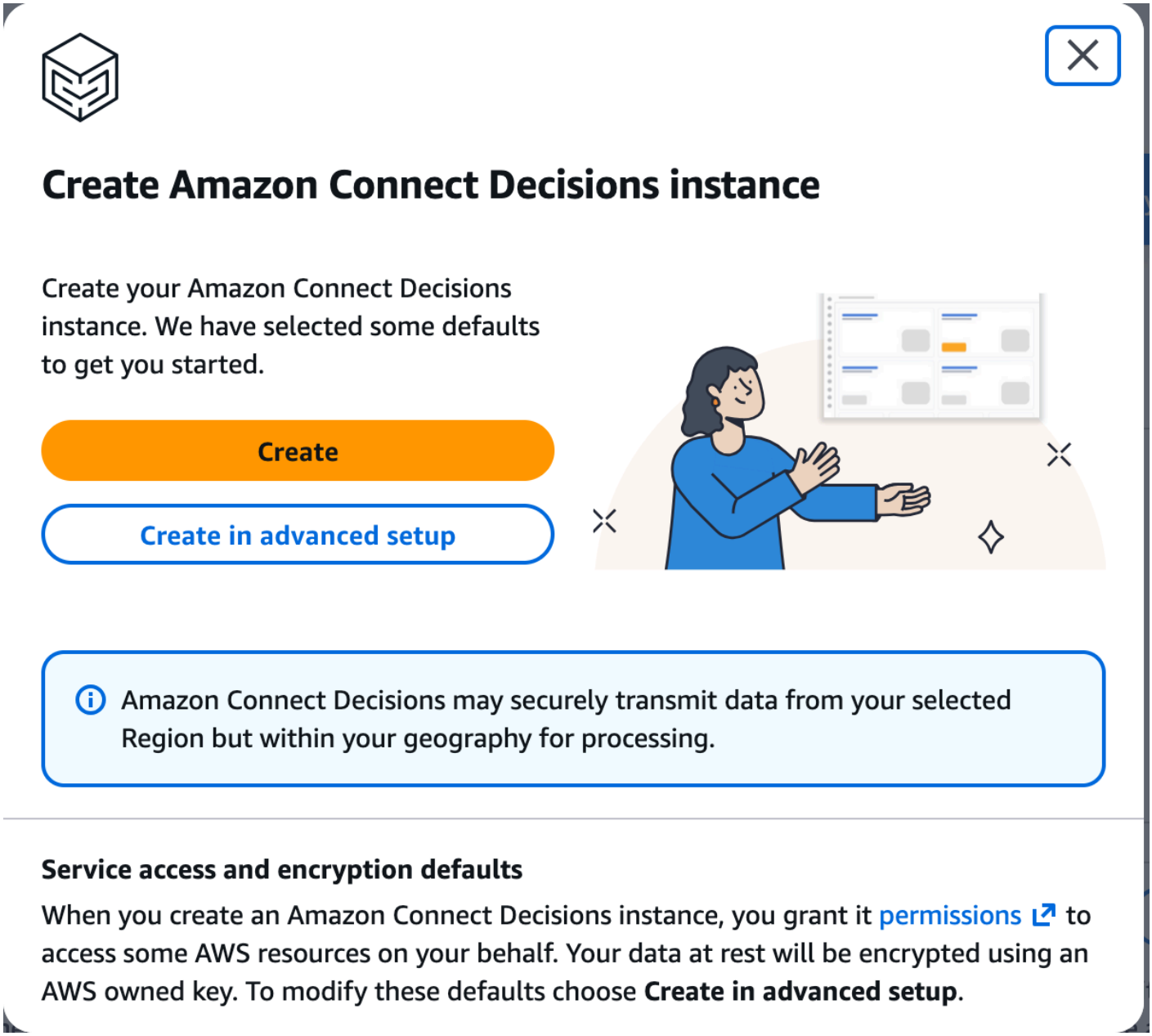
mithilfe voreingestellter Parameter schnell erstellt. Mit der erweiterten Konfiguration können Sie Ihre Instanz anpassen, indem Sie Ihre eigenen Parameter festlegen.

## Verwenden Sie die Standardkonfiguration

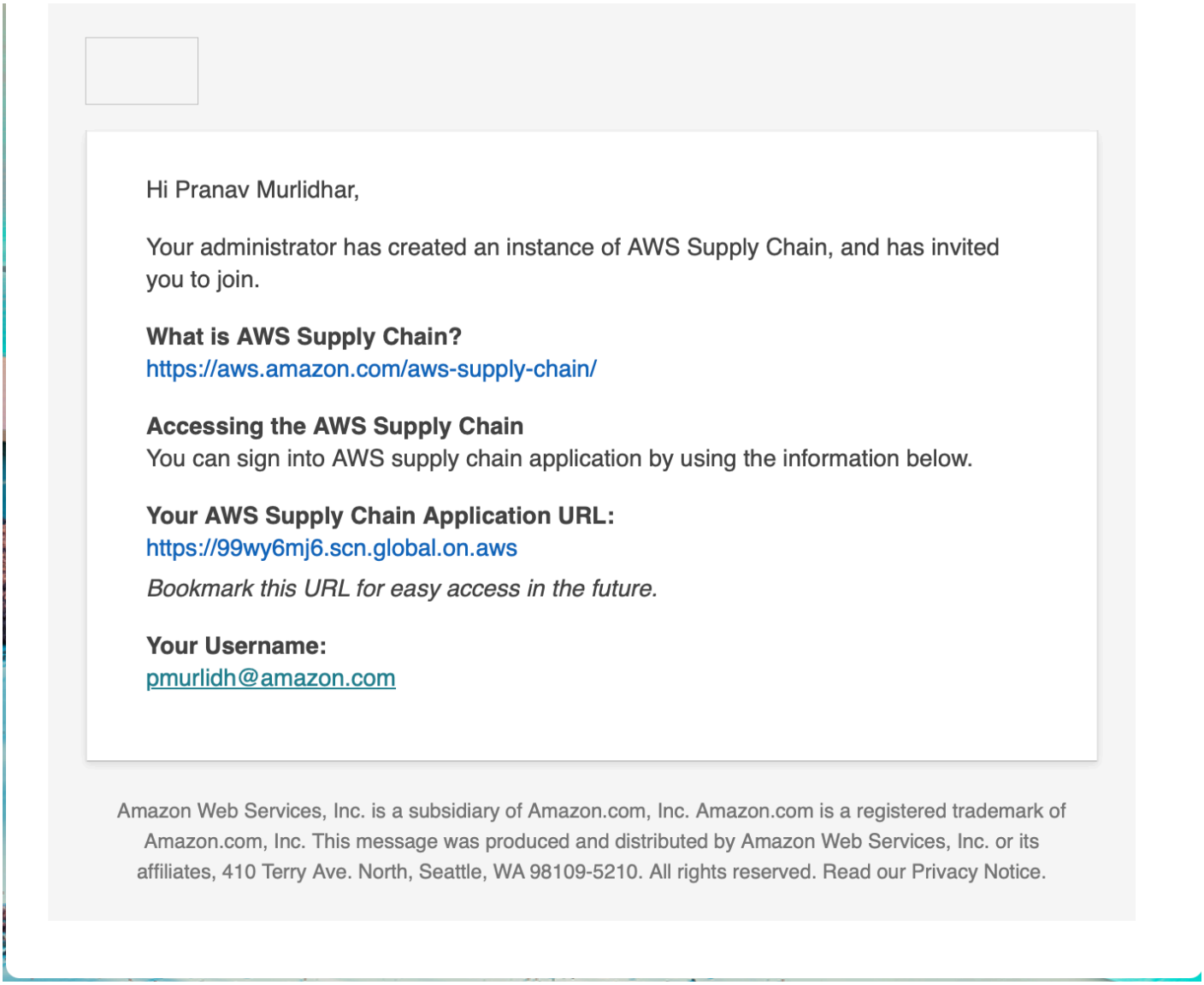
Die Standardkonfiguration erstellt Ihre Amazon Connect Decisions-Instance mit den standardmäßigen Sicherheits- und Verschlüsselungseinstellungen. Instances werden in AWS geografischen Regionen betrieben. Weitere Informationen zu Regionen finden Sie unter Regionen und Endpunkte im IAM-Benutzerhandbuch und Regionale Endpunkte in der AWS allgemeinen Referenz.

Gehen Sie wie folgt vor, um eine Amazon Connect Decisions-Instance mit einer Standardkonfiguration von voreingestellten Parametern zu erstellen.

1. Wählen Sie Erstellen aus.




2. Überprüfen Sie Ihre E-Mail auf Folgendes:
   - Eine E-Mail vom iDC-Team.
   - Eine E-Mail vom Identity Management Team.

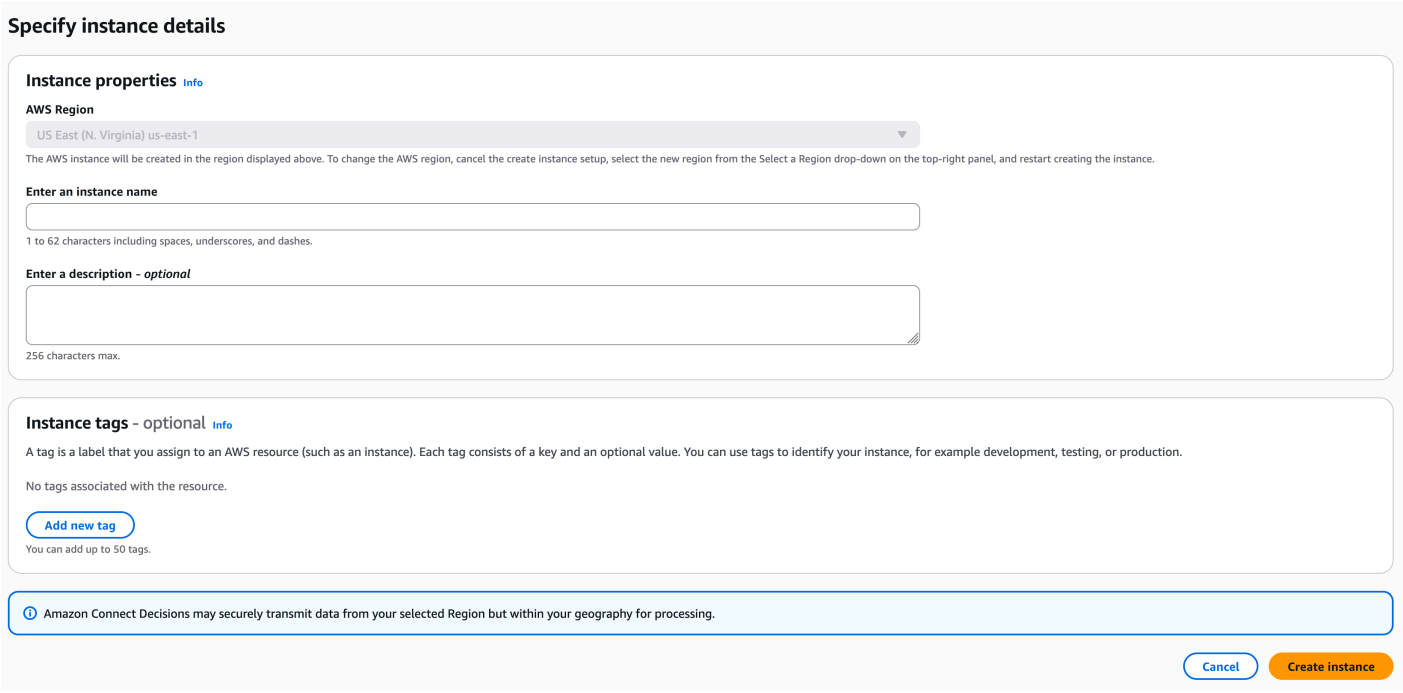



3. Sobald Sie die Einladungs-E-Mail erhalten haben, melden Sie sich bei Amazon Connect Decisions an. Weitere Informationen finden Sie unter Anmelden bei der Amazon Connect Decisions-Webanwendung.

## Verwenden Sie die erweiterte Konfiguration

Mit der erweiterten Konfiguration können Sie Ihre Instanz anpassen, indem Sie Ihre eigenen Parameter festlegen. Gehen Sie wie folgt vor, um eine Amazon Connect Decisions-Instance mit einer erweiterten Konfiguration voreingestellter Parameter zu erstellen.

1. Wählen Sie In der erweiterten Konfiguration erstellen aus.
2. Die Seite mit den Instanzeigenschaften wird angezeigt.




3. Geben Sie auf der Seite mit den Instanzeigenschaften Folgendes ein:
   - Name — Geben Sie einen Instanznamen ein.
   - Beschreibung — Geben Sie eine Beschreibung Ihrer Amazon Connect Decisions-Instance ein (z. B. Produktions-Instance, Test-Instance usw.).
   - Instance-Tags — Sie können Ihrer Instance Tags hinzufügen, die zur Identifizierung verwendet werden können. Sie können beispielsweise ein Tag hinzufügen, um den Instanztyp zu definieren, den Sie erstellen (z. B. Produktion, Test, UAT usw.).
4. Wählen Sie Instanz erstellen aus.

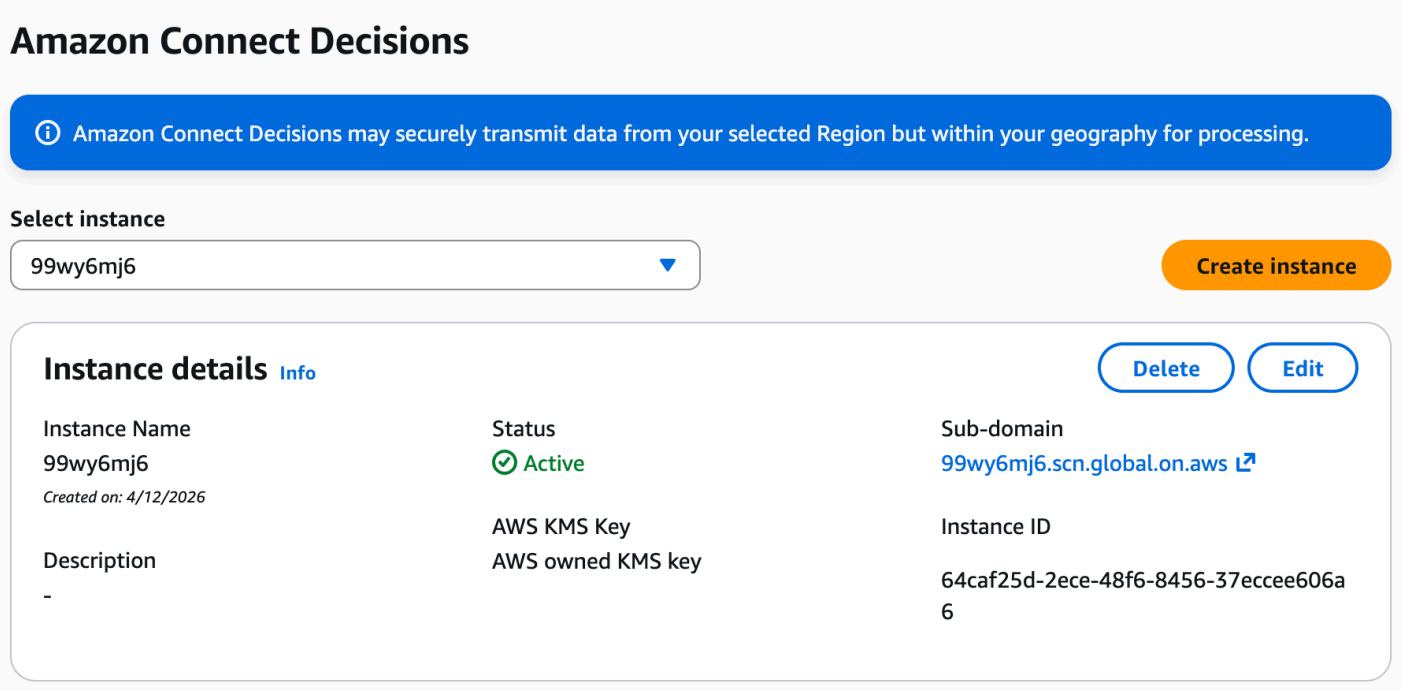
## Eine Instance löschen

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

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

1. Öffnen Sie die Amazon Connect Decisions-Konsole unter https://console.aws.amazon.com/scn/home.

2. Wählen Sie im Dashboard der Amazon Connect Decisions-Konsole aus der Dropdownliste die Instance aus, die Sie löschen möchten.




3. Wählen Sie Löschen aus.
4. Geben Sie auf der Seite Delete Amazon Connect Decisions Instance unter Bestätigung ein, `delete` um zu bestätigen, dass Sie die Instance löschen möchten.
5. Wählen Sie Löschen aus. Das Löschen der Instance beginnt und sobald die Instance gelöscht ist, wird eine Bestätigungsnachricht angezeigt.

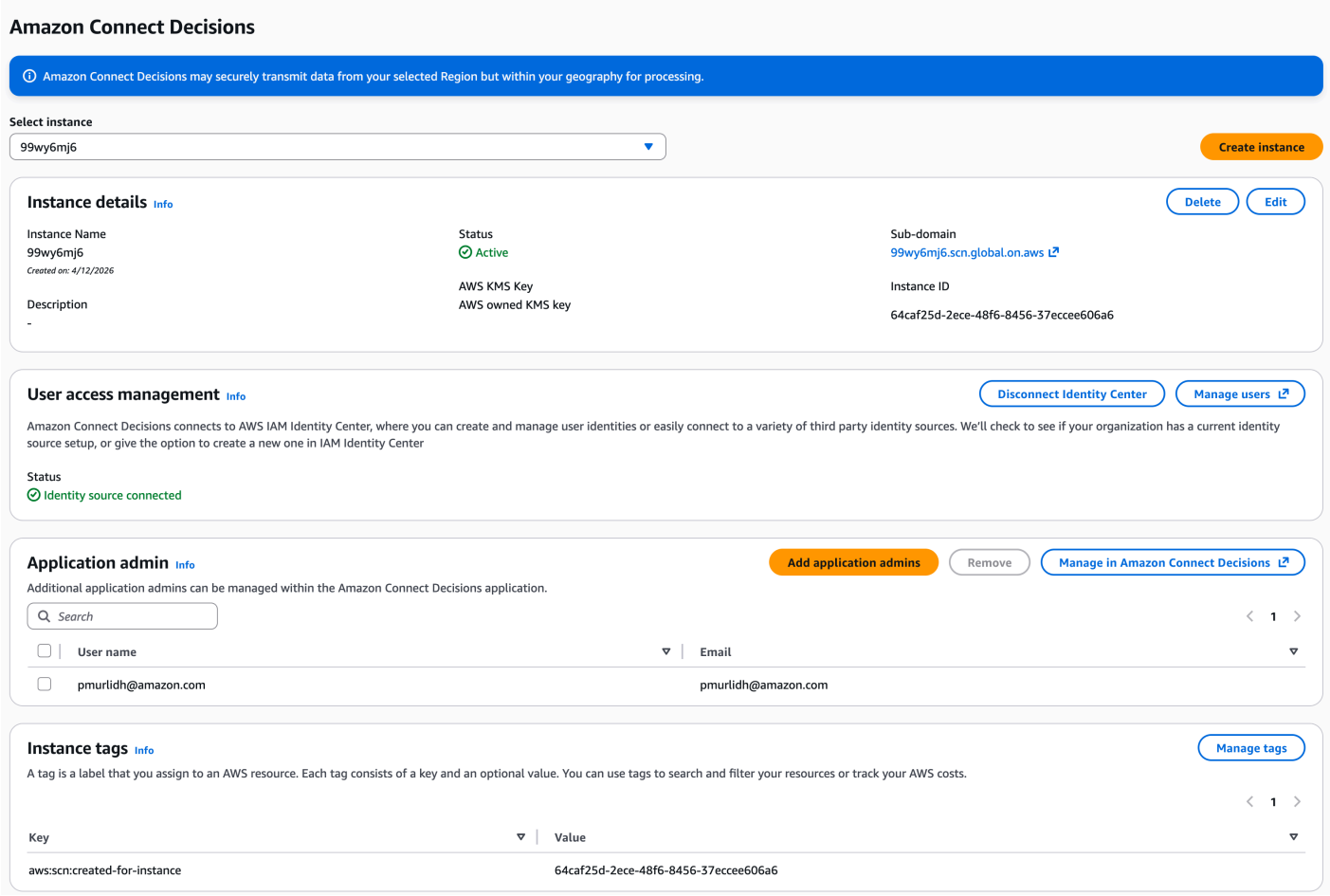
## Wählen Sie einen Anwendungsadministrator

Als AWS Konsolenadministrator wählen Sie einen Amazon Connect Decisions-Anwendungsadministrator aus, um den Zugriff auf die Amazon Connect Decisions-Webanwendung zu verwalten. Der Administrator der Amazon Connect Decisions-Anwendung kann Benutzerberechtigungsrollen zur Amazon Connect Decisions-Webanwendung hinzufügen oder entfernen.

Nachdem die Instance erstellt und eine Identitätsquelle verbunden wurde, gehen Sie wie folgt vor, um einen Amazon Connect Decisions-Anwendungsadministrator auszuwählen.

1. Öffnen Sie das Dashboard der Amazon Connect Decisions-Konsole.

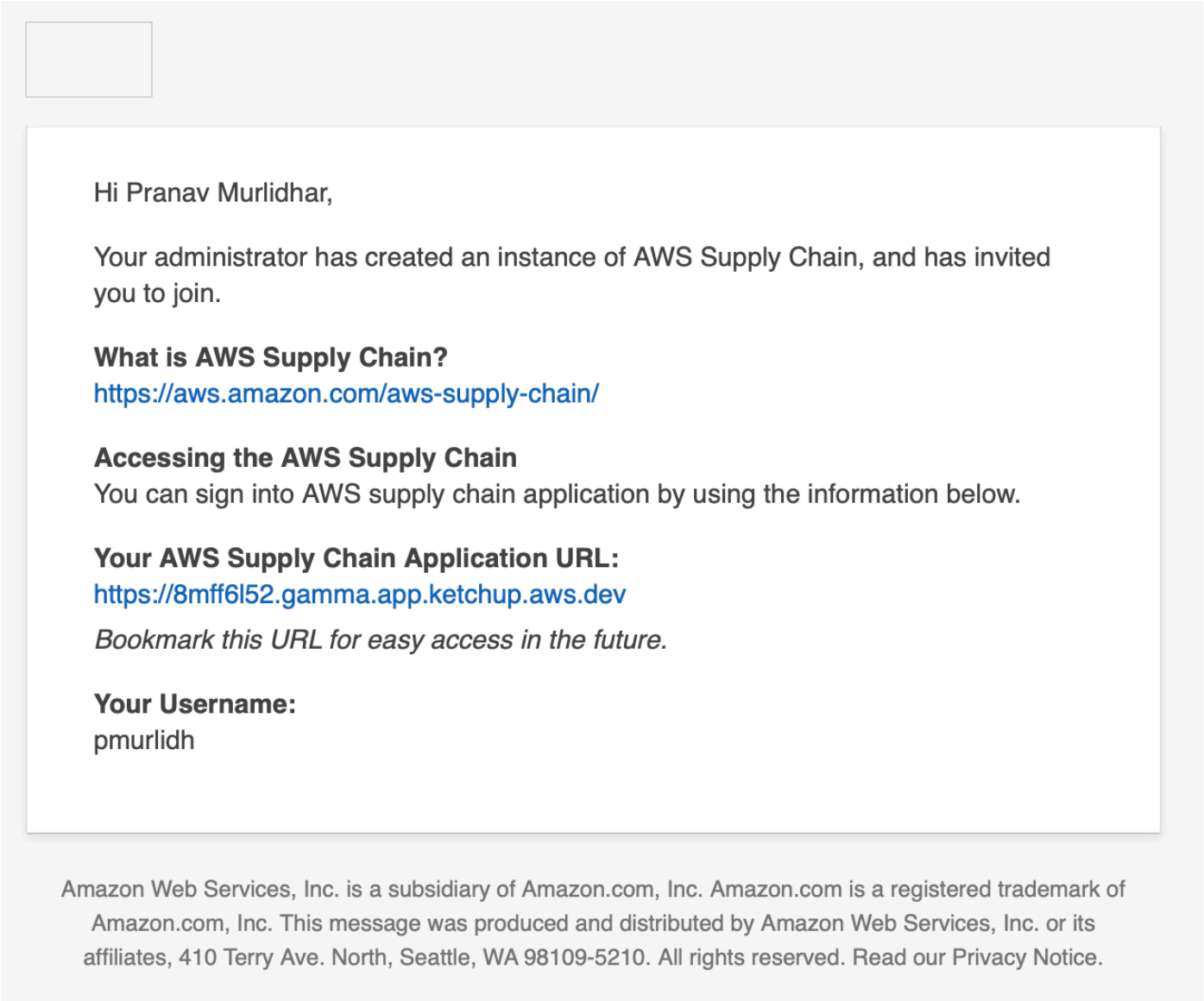
2. Gehen Sie zu Anwendungsadministrator auswählen und wählen Sie einen Benutzer als Amazon Connect Decisions-Anwendungsadministrator aus. In den Suchergebnissen werden nur Benutzer angezeigt, die den Suchkriterien entsprechen.




3. (Optional) Wählen Sie Gehe zu IAM Identity Center, um weitere Benutzer hinzuzufügen. Weitere Informationen zum Hinzufügen von Benutzern finden Sie unter Verwalten Ihrer Identitätsquelle im AWS IAM Identity Center-Benutzerhandbuch und weitere Informationen zu Benutzerberechtigungsrollen finden Sie unter Benutzerberechtigungsrollen.

> **Note**
>
> Sie können jeweils nur einen Benutzer über die Amazon Connect Decisions Console hinzufügen. Sie können in Amazon Connect Decisions keine Gruppe als Anwendungsadministrator hinzufügen.

4. Wählen Sie Einladung senden. Eine E-Mail wird an den Administrator der Webanwendung gesendet. Sobald der Administrator der Webanwendung die Einladungs-E-Mail erhalten hat, kann er die Anwendungs-URL auswählen und sich bei Amazon Connect Decisions anmelden.


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.

In der Amazon Connect Decisions-Webapp wird der Benutzer unter Anwendungsadministrator aufgeführt.

## Zugriff auf Ihre Instance

Die Verwendung der Konsole ist der einfachste Weg, um Ihre Serviceressourcen und Konfigurationen zu verwalten. Die Konsole bietet eine intuitive webbasierte Oberfläche, über die Sie Ihre Ressourcen anzeigen, erstellen, ändern und überwachen können.

Um auf die Amazon Connect Decisions-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Amazon Connect Decisions-Ressourcen in Ihrem AWS Konto aufzulisten und einzusehen. Wenn Sie

eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

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

Als Amazon Connect Decisions-Administrator sollten Sie eine E-Mail-Einladung zur Amazon Connect Decisions-Webanwendung erhalten haben.

1. Sie können entweder den Link in der E-Mail oder im Dashboard der Amazon Connect Decisions-Konsole unter Sub-domainWeb-URL auswählen auswählen auswählen.
2. Die Anmeldeseite der Amazon Connect Decisions-Webanwendung wird angezeigt.
3. Geben Sie die Benutzeranmeldedaten für das AWS IAM Identity Center ein und wählen Sie Anmelden.
4. Jeder Benutzer, den Sie hinzugefügt haben, erhält eine E-Mail-Nachricht mit einem Link zu Amazon Connect Decisions, oder Sie können Link kopieren wählen und den Link an die Benutzer senden.

Nach erfolgreicher Anmeldung landen Sie auf Ihrer personalisierten Startseite. Weitere Informationen zu Ihrer Startseite finden Sie im Benutzerhandbuch unter Grundlegendes zu Ihrer Homepage.

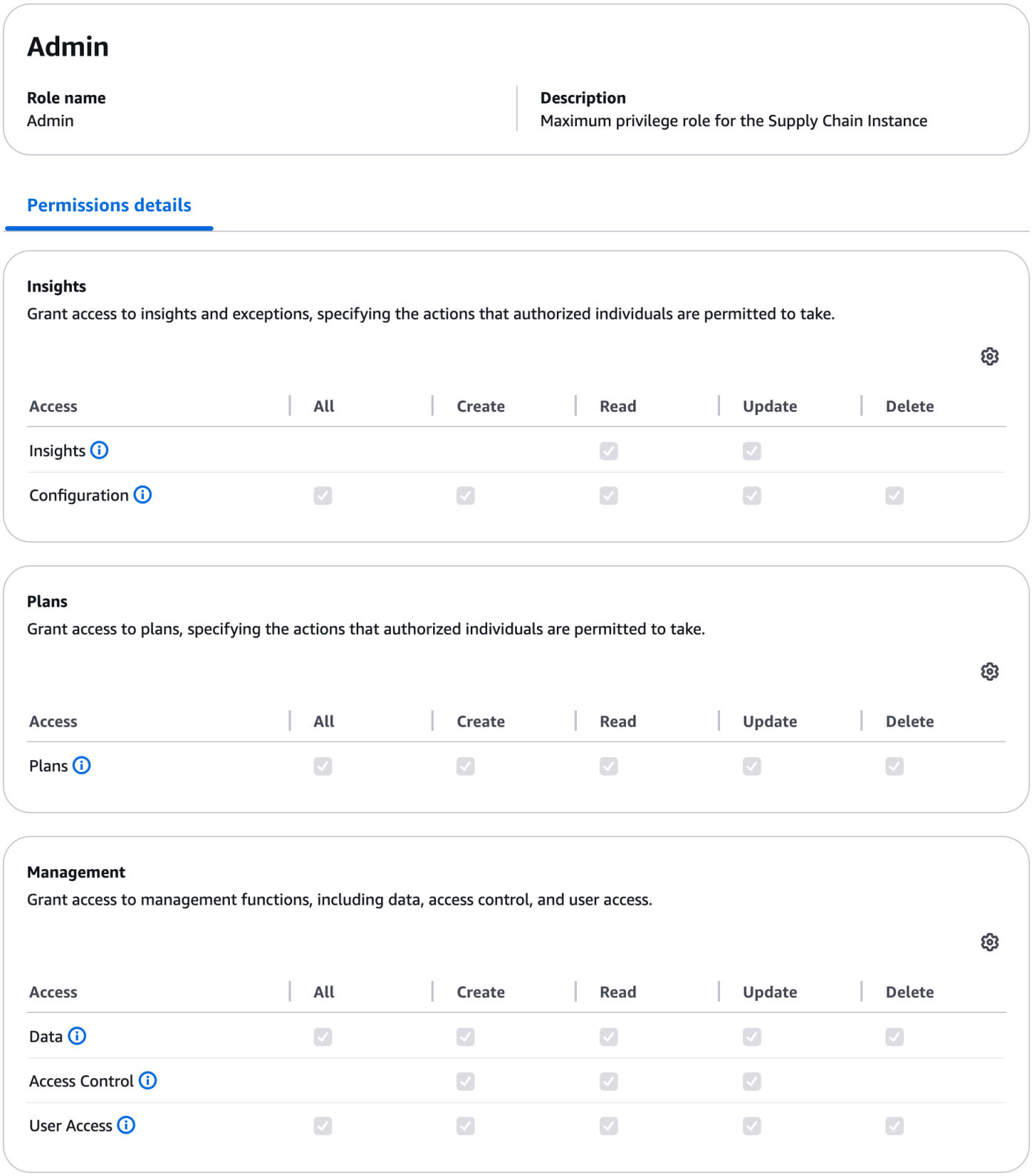
# Zugriffskontrolle

Amazon Connect Decisions bietet ein Zugriffsmanagement auf Unternehmensniveau, mit dem Sie präzise kontrollieren können, wer auf welche Daten zugreifen und welche Aktionen innerhalb Ihrer Instance ausführen kann. Dadurch wird sichergestellt, dass Ihre Benutzer nur die Informationen sehen, die für ihre Aufgaben relevant sind, während gleichzeitig die Sicherheits- und Compliance-Standards eingehalten werden, die Ihr Unternehmen benötigt.

## Überblick über Rollen und Berechtigungen

Als Amazon Connect Decisions-Administrator können Sie entweder die standardmäßigen Benutzerberechtigungsrollen verwenden oder benutzerdefinierte Berechtigungsrollen erstellen. Amazon Connect Decisions hat die folgenden Standard-Benutzerberechtigungsrollen:

- Administrator — Zugriff zum Erstellen, Anzeigen und Verwalten aller Daten und Benutzerberechtigungen.



## 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 | ☑ | ☑ | ☑ | ☑ | ☑ |

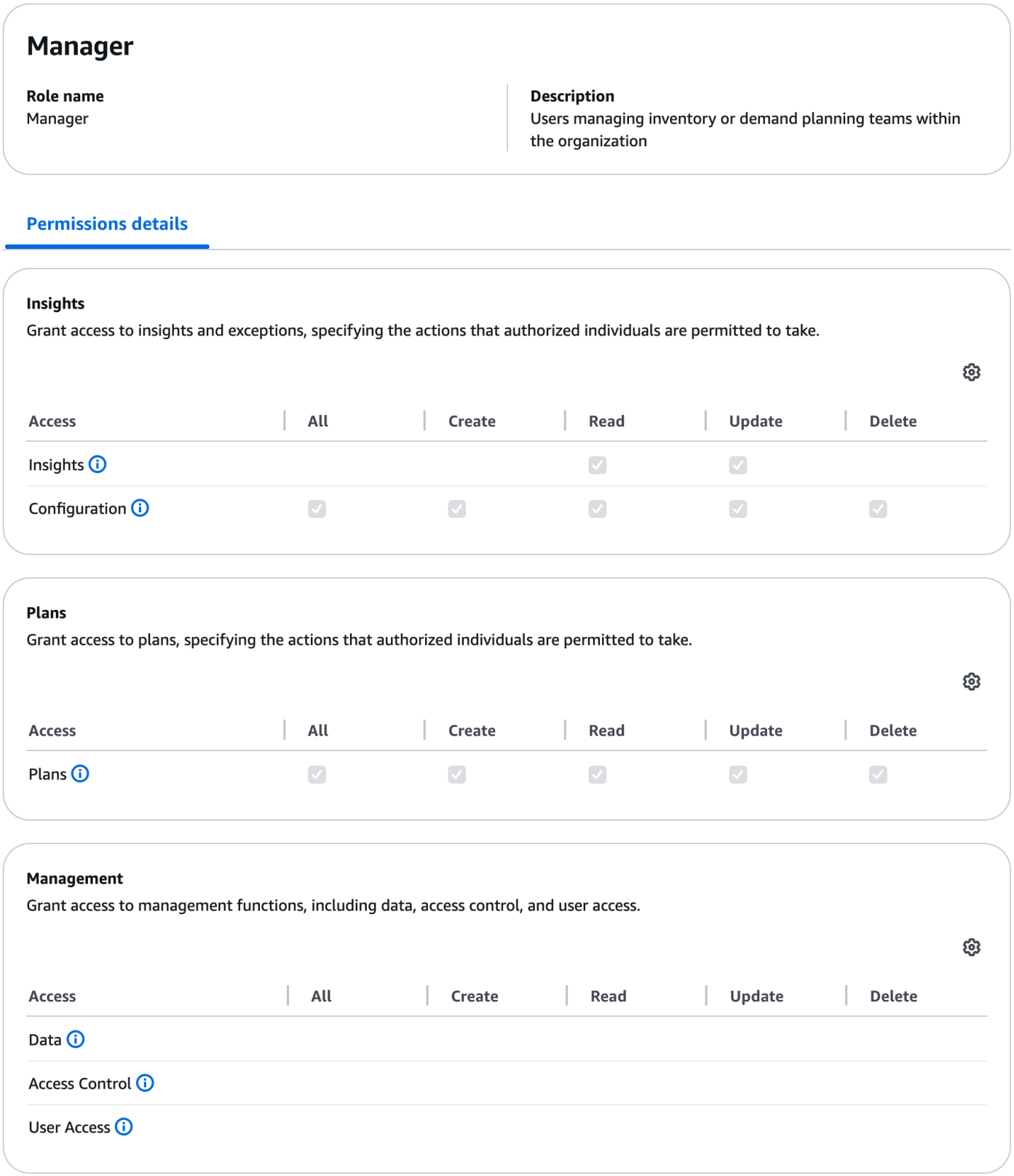
**Plans**
Grant access to plans, specifying the actions that authorized individuals are permitted to take.

| 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 | ☑ | ☑ | ☑ | ☑ | ☑ |

- Manager — Zugriff zum Erstellen, Anzeigen und Verwalten der folgenden Elemente.




- Planer — Zugriff zum Erstellen, Anzeigen und Verwalten der folgenden Elemente.

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

# Rollen mit Benutzerberechtigungen verwalten

## Hinzufügen von Benutzern

Als Amazon Connect Decisions-Administrator können Sie Benutzer hinzufügen, um auf die Amazon Connect Decisions-Webanwendung zuzugreifen. Benutzer müssen zuerst zu IAM Identity Center (IdC) hinzugefügt werden. Anschließend können sie zu Amazon Connect Decisions hinzugefügt werden. Weitere Informationen zum Hinzufügen von Benutzern zu iDC finden Sie unter Benutzerzugriff zuweisen.

Sobald Benutzer zu iDC hinzugefügt wurden, gehen Sie wie folgt vor, um einen Benutzer hinzuzufügen.

1. Wählen Sie das Menü Einstellungen auf der linken Seite
2. Wählen Sie Benutzer aus. Wählen Sie Benutzer zuweisen aus
3. Suchen Sie, um den Benutzer zu identifizieren. Sie können nach Anzeigename, E-Mail, Vorname, Nachname und Benutzername suchen

4. Wählen Sie die Benutzer aus, die Sie hinzufügen möchten.
5. Weisen Sie ihnen eine Rolle zu. Sehen Sie sich die Übersicht über Rollen und Berechtigungen an, um mehr über Benutzerrollen in Amazon Connect Decisions zu erfahren.
6. Wählen Sie Zuweisen aus. Vergewissern Sie sich, dass Ihre Auswahl korrekt ist.

## Benutzerberechtigungen aktualisieren

Gehen Sie wie folgt vor, um die Benutzerberechtigungsrolle für die aktuellen Amazon Connect Decisions-Benutzer zu aktualisieren.

1. Wählen Sie das Menü Einstellungen auf der linken Seite
2. Wählen Sie Benutzer aus. Wählen Sie Benutzer zuweisen aus
3. Wählen Sie in der Benutzerliste den Benutzer aus, um die Seite mit den Benutzerdetails zu öffnen.
4. Verwenden Sie die Rollen-Dropdownliste, um die Rollenberechtigungen für den Benutzer zu aktualisieren.
5. Bestätigen Sie, dass Sie die Rolle ändern möchten, indem Sie auf die Schaltfläche Rolle ändern klicken

## Löschen von Benutzern

Als Amazon Connect Decisions-Administrator können Sie Benutzer aus der Amazon Connect Decisions-Webanwendung löschen. Gehen Sie wie folgt vor, um Benutzer zu löschen.

1. Wählen Sie die linke Schublade „Einstellungen“
2. Wählen Sie Benutzer aus. Wählen Sie Benutzer zuweisen aus
3. Wählen Sie in der Benutzerliste den Benutzer aus, um die Seite mit den Benutzerdetails zu öffnen.
4. Wählen Sie Löschen
5. Bestätigen Sie, dass Sie den Benutzer löschen möchten, indem Sie auf die Schaltfläche Löschen klicken

# Zugriff auf Attributebene einrichten

Attribute-Based Access Control (ABAC) sorgt für zusätzliche Präzision, indem der Zugriff je nach Geschäftskontext eingeschränkt wird. Mithilfe von Produkt- und Standortattributen können Sie

sicherstellen, dass Planer nur Details zu den spezifischen Produkten und Standorten sehen, die sie verwalten, während Manager den Überblick über die Zuständigkeitsbereiche ihrer Teams behalten.

Jeder Benutzer mit der Rolle „Administrator“ kann den Zugriff für andere Benutzer nach Produkten und Websites konfigurieren:

1. Navigieren Sie von der linken Navigationsleiste zur Benutzerseite.
2. Wählen Sie aus der Liste der Benutzer in dieser Instanz den Benutzer aus, der konfiguriert werden muss.
3. Standardmäßig ist für Benutzer im Bereich Datenzugriff die Option „Vollzugriff auf alle Produkte und Websites gewähren“ aktiviert. Wenn dieser Schalter aktiviert ist, ermöglicht er den Zugriff auf alle Produkte und Websites (so, wie es vor dieser Markteinführung funktioniert hat).
4. Wenn Sie „Vollzugriff auf alle Produkte und Websites gewähren“ deaktivieren, wird der Abschnitt zur Konfiguration von Produkten und Websites angezeigt. Beim ersten Zugriff werden keine Produkte oder Websites zugewiesen.
5. Klicken Sie auf die Add/Remove Schaltfläche für Produkte oder Websites, je nachdem, was Sie konfigurieren müssen. Verwenden Sie die Suche, um die für diesen Benutzer benötigten Artikel zu finden und auszuwählen.
6. Mehreren Benutzern kann dasselbe Produkt oder dieselbe Website zugewiesen werden. Einem Benutzer können maximal 1.000 Kombinationen aus Produkten und Websites zugewiesen werden.
7. Zuvor konfigurierte Produkte oder Websites können über dieselbe Oberfläche entfernt werden.
8. Überprüfen und bestätigen Sie die vollständige Liste der Hinzufügungen und Löschungen auf der letzten Seite des Assistenten, um die Zugriffskonfiguration abzuschließen.

Sobald der Produkt- und Standortzugriff konfiguriert wurde, wird der Zugriff für diesen Benutzer auf der Grundlage der folgenden Zuweisungen eingeschränkt:

- Alle Benutzer können jede Ausnahme- oder Empfehlungsseite aufrufen, unabhängig davon, ob sie für ein Produkt oder eine Website generiert wurde, die in ihrer Zugriffskontrolle enthalten ist.
- Um Mutationsaktionen durchführen zu können (z. B. das Schließen einer Ausnahme oder das Ändern des Status von „In Bearbeitung“ in „Abgeschlossen“), müssen Benutzer das entsprechende Produkt ODER die entsprechende Website in ihrer Zugriffskontrolle konfiguriert haben.
- Benutzer mit konfigurierter Zugriffskontrolle können auch die Option „Benutzerzuweisung“ und „Zugriffsansicht umschalten“ verwenden.

# Benutzerzuweisung

Die Benutzerzuweisung ist eine Funktion, die es einfacher macht, Erkenntnisse zwischen mehreren Benutzern abzugleichen. Mithilfe der Benutzerzuweisung können Kunden Benutzern bestimmte Erkenntnisse zuweisen, um besser widerzuspiegeln, wie diese Aufgaben im wirklichen Leben aufgeteilt werden. Diese funktioniert folgendermaßen:

- Immer wenn eine Ausnahme erstellt wird, vergleicht das System das Produkt und den Standort, für den die Ausnahme erstellt wurde, mit allen Benutzern, die dasselbe Produkt ODER dieselbe Website für ihre Zugriffskontrolle konfiguriert haben
- Wenn das System einen passenden Benutzer findet, wird das Feld Zugewiesen an für diese Ausnahme mit dem Benutzernamen aktualisiert. In Fällen, in denen mehr als ein Benutzer Produkte oder Websites anbietet, die mit der Ausnahme übereinstimmen, wird die Ausnahme nach dem Zufallsprinzip einem von ihnen zugewiesen
- Jeder Ausnahme kann nur ein Benutzer zugewiesen werden, aber eine Ausnahme kann bei Bedarf einem anderen Benutzer zugewiesen werden. Sie kann nur einem Benutzer mit Produkt- oder Site-Zugriff neu zugewiesen werden
- Auto-assignment for insights tritt auf, wenn die Ausnahme zum ersten Mal erstellt wird. Zuvor erstellte Erkenntnisse werden nicht automatisch neu zugewiesen. Außerdem wird die Benutzerzuweisung nicht automatisch aktualisiert, wenn ein Benutzer gelöscht oder seine Zugriffskontrolle aktualisiert wird
- Auf der Seite mit der Insights-Liste kann ein Benutzer nach der Dimension „Zugewiesen an“ filtern, um alle ihm zugewiesenen Erkenntnisse auf einfache Weise zu identifizieren. Sie können denselben Filter auch verwenden, um nicht zugewiesene Erkenntnisse anzuzeigen. Die Benutzerzuweisung ist derzeit nur für Einblicke verfügbar

# Daten-Onboarding

## Ihre Daten verbinden

### Voraussetzungen

Bevor Sie mit dem Daten-Onboarding beginnen, stellen Sie sicher, dass Sie über Folgendes verfügen:

- Amazon Connect Connect-Entscheidungsinstanz
  - Ihre Instance sollte bereits mit einem zugehörigen S3-Bucket erstellt worden sein
- Daten vorbereitet
  - Ermitteln Sie gemeinsam mit Ihrem Ansprechpartner bei Amazon Customer Success, welche Daten Sie benötigen, je nachdem, wie Sie Amazon Connect Decisions verwenden möchten. Zu den Basisdatenanforderungen gehören:
    - Sales/Order Verlauf: Transaktionsaufzeichnungen von mehr als 12 Monaten
    - Produktdetails: Vollständiger Produktkatalog mit Spezifikationen
    - Site/Location Informationen: Lagerhäuser, Vertriebszentren, Einzelhandelsstandorte
    - Aktuelle Inventarbestände: On-hand Inventar an jedem Standort
  - Alle Quelldaten im CSV-Format mit UTF-8 Kodierung

### Erstmaliger Login: Onboarding-Fragebogen

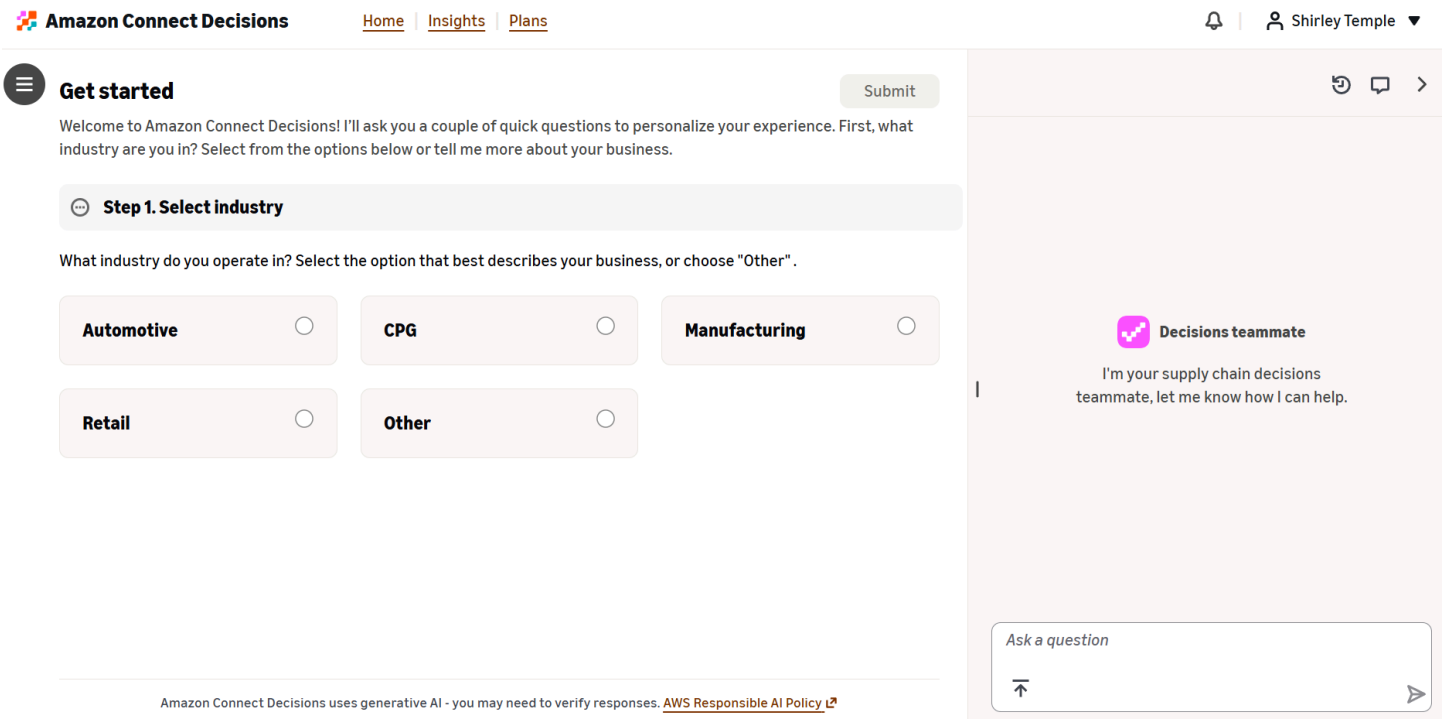
Wenn Sie sich zum ersten Mal bei Amazon Connect Decisions anmelden, zeigt das System einen geführten Onboarding-Fragebogen an. Dieser Personalisierungsassistent hilft den Teamkollegen von Decisions dabei, die Funktionen, die für Ihr Unternehmen am relevantesten sind, zu kontextualisieren. Der Fragebogen sammelt Informationen über Ihre Branche, die wichtigsten geschäftlichen Herausforderungen und den bevorzugten Planungsansatz. Ihre Antworten helfen Ihnen dabei, die Onboarding-Schritte auf der Grundlage Ihrer Auswahl zu optimieren, sodass das System die nachfolgenden Einrichtungsabläufe rationalisieren und die für Ihr Unternehmen relevantesten Konfigurationspfade ermitteln kann. Sie müssen alle Schritte abschließen, bevor Sie auf die vollständige Anwendung zugreifen können. Der Decisions-Teamkollege steht während des gesamten Onboarding-Prozesses über die rechte Seitenleiste zur Verfügung, um Fragen in Echtzeit zu beantworten.

> **Note**
>
> Dies ist nur eine einmalige Auswahl bei der ersten Anmeldung. Ihre Antworten bieten zusätzlichen Kontext, um nachfolgende Onboarding-Schritte zu optimieren und den Mitarbeitern zu helfen, Ihr Geschäftsumfeld zu verstehen. Alle Funktionen bleiben unabhängig von Ihrer Auswahl uneingeschränkt zugänglich.

## Schritt 1: Branche auswählen

Was Sie sehen: Eine Willkommensnachricht und eine Reihe von Optionsfeldern, mit denen Sie die Branche auswählen können, die Ihr Unternehmen am besten beschreibt.

1. Wählen Sie das Optionsfeld aus, das Ihr Unternehmen am besten repräsentiert.
2. Wenn keine der vordefinierten Optionen zutrifft, wählen Sie Andere aus.




## Schritt 2: Definieren Sie Ihre größte Herausforderung

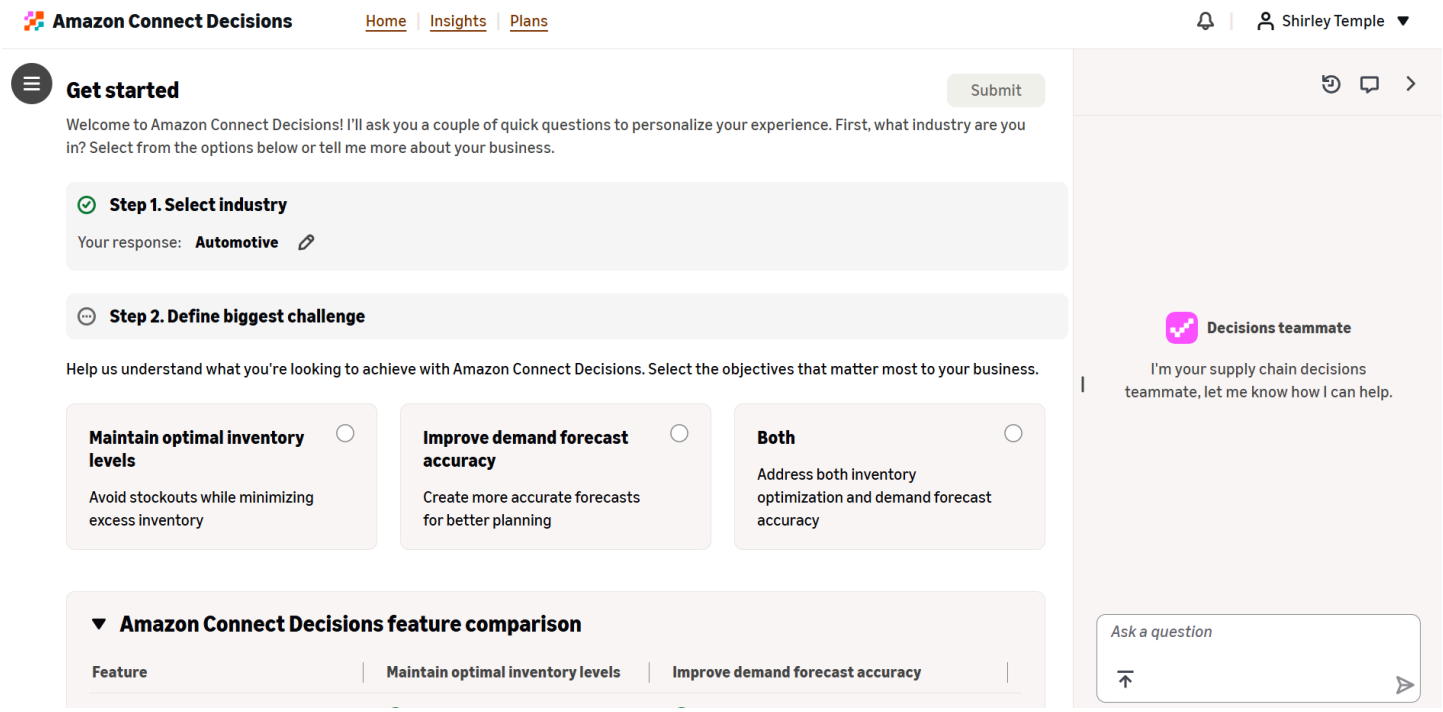
Was Sie sehen: Ihre Antwort aus Schritt 1 wird mit einer Bearbeitungsoption angezeigt. Darunter werden Sie gebeten, anhand von drei Optionen Ihr primäres geschäftliches Problem zu identifizieren.

Eine Tabelle mit einem Funktionsvergleich wird angezeigt, damit Sie besser verstehen, welche Funktionen mit den einzelnen Optionen verknüpft sind.

1. Überprüfen Sie die Optionen. In der folgenden Tabelle finden Sie die verfügbaren Optionen und ihre Bedeutung.
2. Wählen Sie das Optionsfeld aus, das Ihre dringendste Herausforderung darstellt.
3. Sehen Sie sich optional die Vergleichstabelle der Funktionen unter den Optionen an, um zu erfahren, was in den einzelnen Optionen enthalten ist.

Optionen für geschäftliche Herausforderungen

| Option | Description | Die wichtigsten Funktionen sind aktiviert |
|---|---|---|
| Sorgen Sie für optimale Lagerbestände | Wählen Sie diese Option, wenn Ihre größte Herausfor derung darin besteht, Fehlbestände zu vermeiden und gleichzeitig Überbestände zu minimieren. | Bestandsoptimierung; Vermeidung von Fehlbestä nden; Reduzierung von Überbeständen; Angebotsp lanung; Erfassung der Lieferzeiten |
| Verbessern Sie die Genauigke it der Bedarfsprognose | Wählen Sie diese Option, wenn Ihre größte Herausfor derung darin besteht, genauere Prognosen für bessere Planungsentscheidu ngen zu erstellen. | Basisprognosen; Konsenspl anung; Verfolgung der Prognosegenauigkeit |
| Beides | Wählen Sie diese Option, wenn Sie sich gleichzeitig mit der Bestandsoptimierung und der Genauigkeit der Bedarfspr ognosen befassen müssen. | Alle angebots- und nachfrage spezifischen Funktionen sind aktiviert |




## Schritt 3: Wählen Sie Ihren Ansatz zur Bestandsplanung

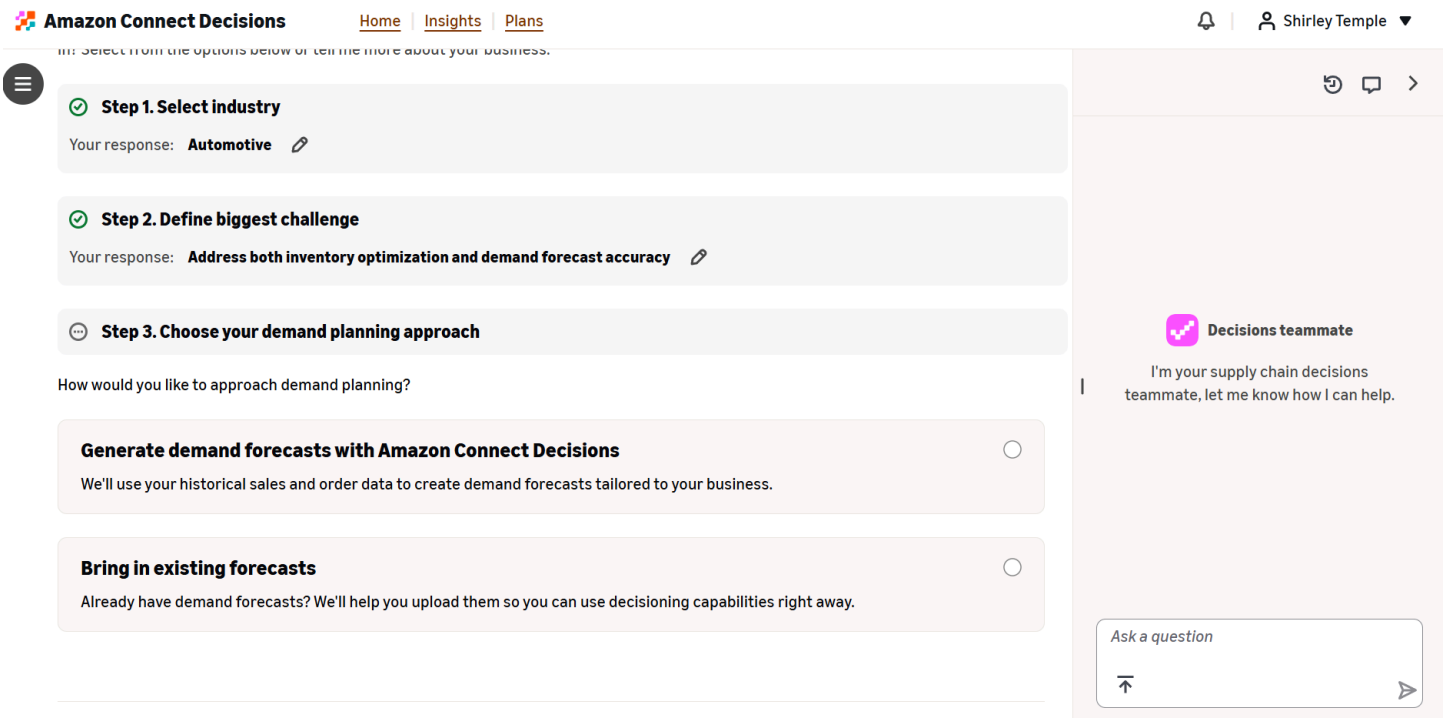
Was Sie sehen: Die Schritte 1 und 2 werden als abgeschlossen angezeigt (gekennzeichnet durch grüne Häkchen). Ihre Antworten werden angezeigt und können bearbeitet werden. In Schritt 3 werden Sie gefragt, wie Sie an die Bestandsplanung herangehen möchten. Dabei werden zwei Optionen hervorgehoben.

1. Sehen Sie sich die beiden Optionen für die Bestandsplanung an. In der folgenden Tabelle finden Sie die verfügbaren Optionen und ihre Bedeutung.
2. Wählen Sie das Optionsfeld für den Ansatz aus, der Ihrem aktuellen Status entspricht.

Optionen für den Ansatz zur Bestandsplanung

| Option | Description | Am besten für |
|---|---|---|
| Generieren Sie Inventarpläne mit Amazon Connect Decisions | Das System verwendet Ihre historischen Verkaufs- und Inventardaten, um Pläne zu erstellen, die auf Ihr Unternehmen zugeschnitten sind. | Organizations, die noch nicht über eine bestehende Planungslösung verfügen oder KI-generierte Pläne aus ihren historischen Daten nutzen möchten. |

| Option | Description | Am besten für |
| --- | --- | --- |
| Bringen Sie bestehende Inventarprognosen oder -pläne mit ein | Laden Sie Ihre vorhandenen Inventarpläne oder -prognosen hoch, damit Sie die Entscheid ungsmöglichkeiten sofort nutzen können. Das System hilft Ihnen beim Hochladen und Zuordnen Ihrer Daten. | Organizations, die bereits über etablierte Planungsprozesse verfügen und Funktionen zur Überwachung, Gewinnung von Erkenntnissen und Empfehlun gen nutzen möchten, ohne ihre Planquelle zu ändern. |




## Schritt 4: Wählen Sie Ihren Ansatz zur Bedarfsplanung

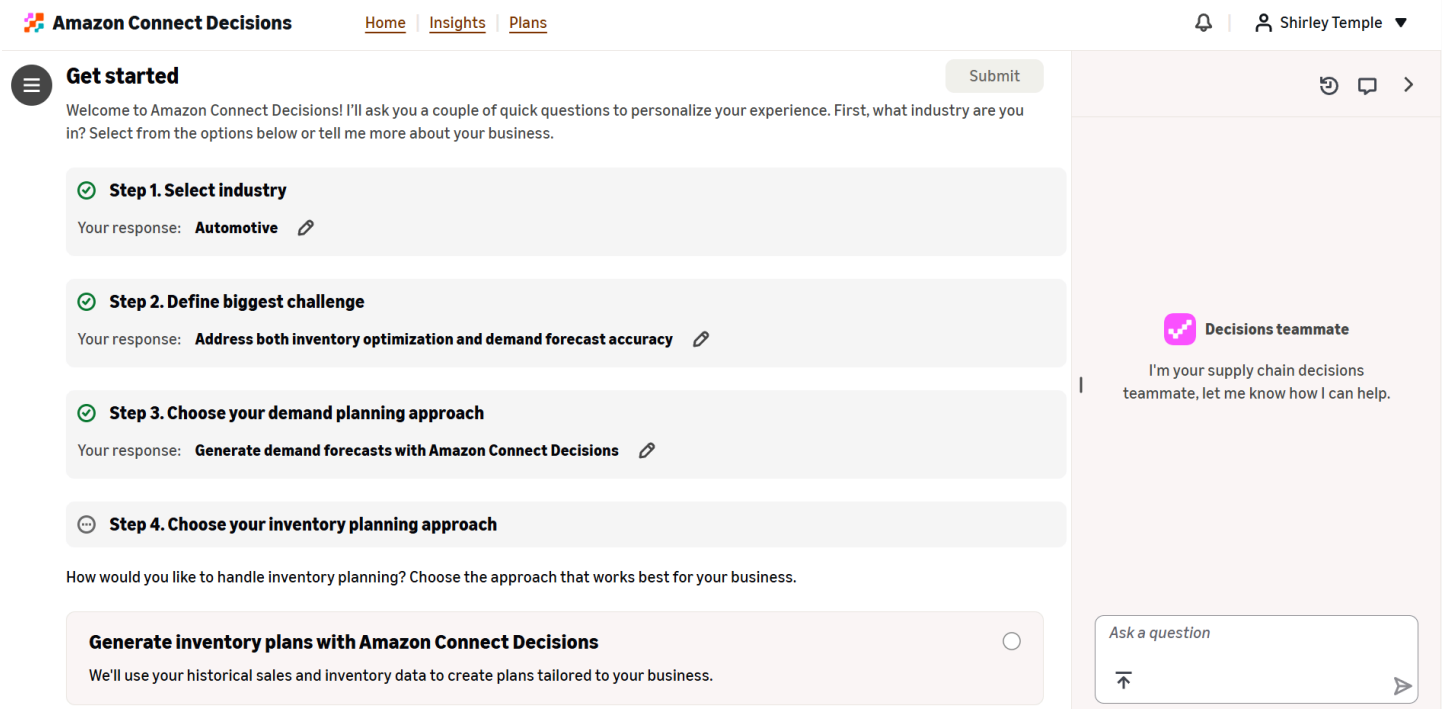
Was Sie sehen: Die Schritte 1 bis 3 werden als abgeschlossen angezeigt. In Schritt 4 werden Sie gefragt, wie Sie die Bedarfsplanung angehen möchten.

1. Sehen Sie sich die beiden Optionen für die Bedarfsplanung an. In der folgenden Tabelle finden Sie die verfügbaren Optionen und ihre Bedeutung.
2. Wählen Sie das Optionsfeld für den Ansatz aus, der Ihrem aktuellen Status entspricht.
3. Klicken Sie auf Senden, um den Onboarding-Fragebogen abzuschließen.

Denken Sie daran: Dieser Onboarding-Fragebogen ist eine einmalige kontextbezogene Eingabe, mit deren Hilfe Sie die Onboarding-Schritte auf der Grundlage Ihrer Auswahl optimieren können. Es verändert nicht das Verhalten der Agenten und schränkt den Zugriff auf Funktionen nicht ein. Alle Funktionen von Amazon Connect Decisions stehen Ihnen weiterhin in vollem Umfang zur Verfügung.

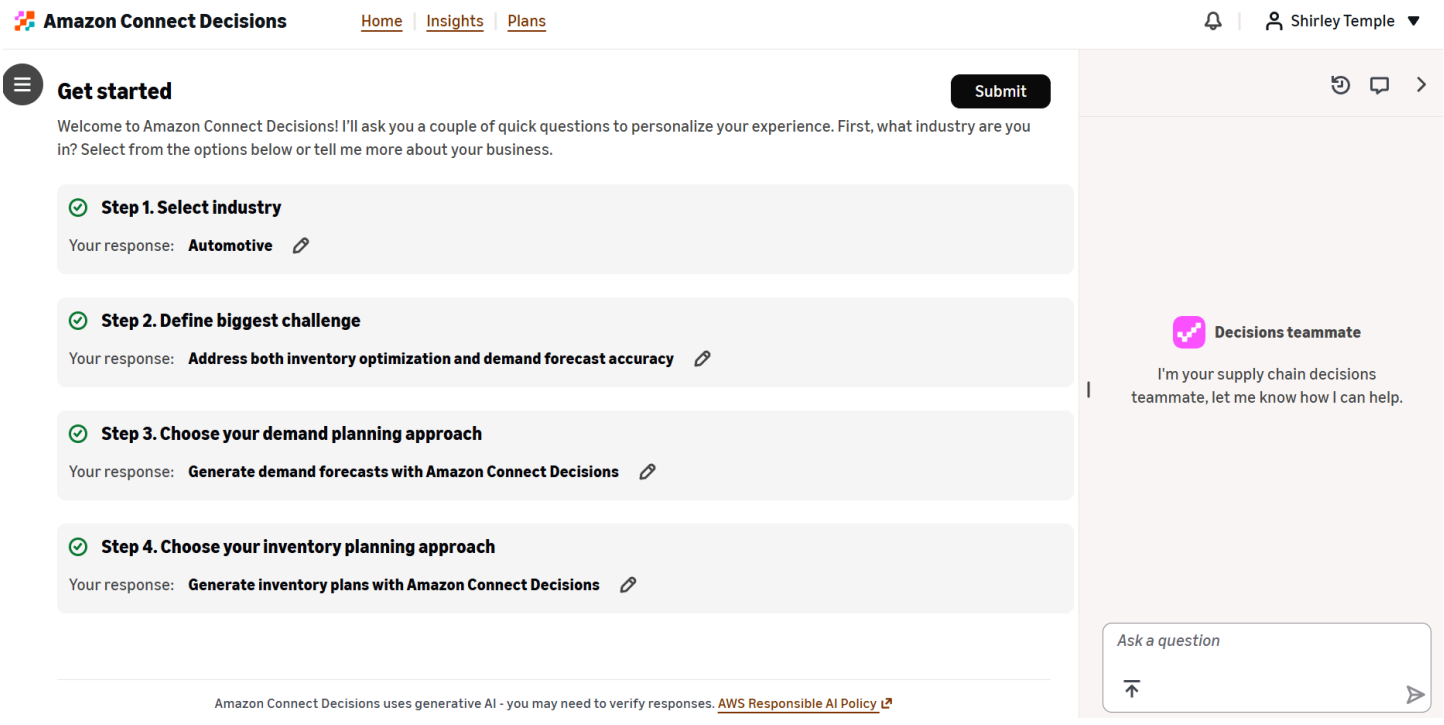
Optionen für den Ansatz zur Bedarfsplanung

| Option | Description | Am besten für |
|---|---|---|
| Generieren Sie Bedarfsprognosen mit Amazon Connect Decisions | Das System verwendet Ihre historischen Verkaufs- und Bestelldaten, um Bedarfsprognosen zu erstellen, die auf Ihr Unternehmen zugeschnitten sind. Amazon Connect Decisions orchestriert mehr als 18 Prognosetools, um genaue Basisprognosen zu erstellen. | Organizations, die über keine bestehende Prognoselösung verfügen oder ihren aktuellen Ansatz durch KI-generierte Prognosen ersetzen möchten. |
| Integrieren Sie bestehende Prognosen | Laden Sie Ihre vorhandenen Bedarfsprognosen hoch, damit Sie die Entscheidungsfunktionen sofort nutzen können. Das System hilft Ihnen dabei, Ihre Prognosedaten abzubilden und zu importieren. | Organizations, die bereits über Prognoseprozesse verfügen und die Funktionen zur Überwachung, Gewinnung von Erkenntnissen und Empfehlungen nutzen möchten, ohne ihre Prognosequelle zu ändern. |



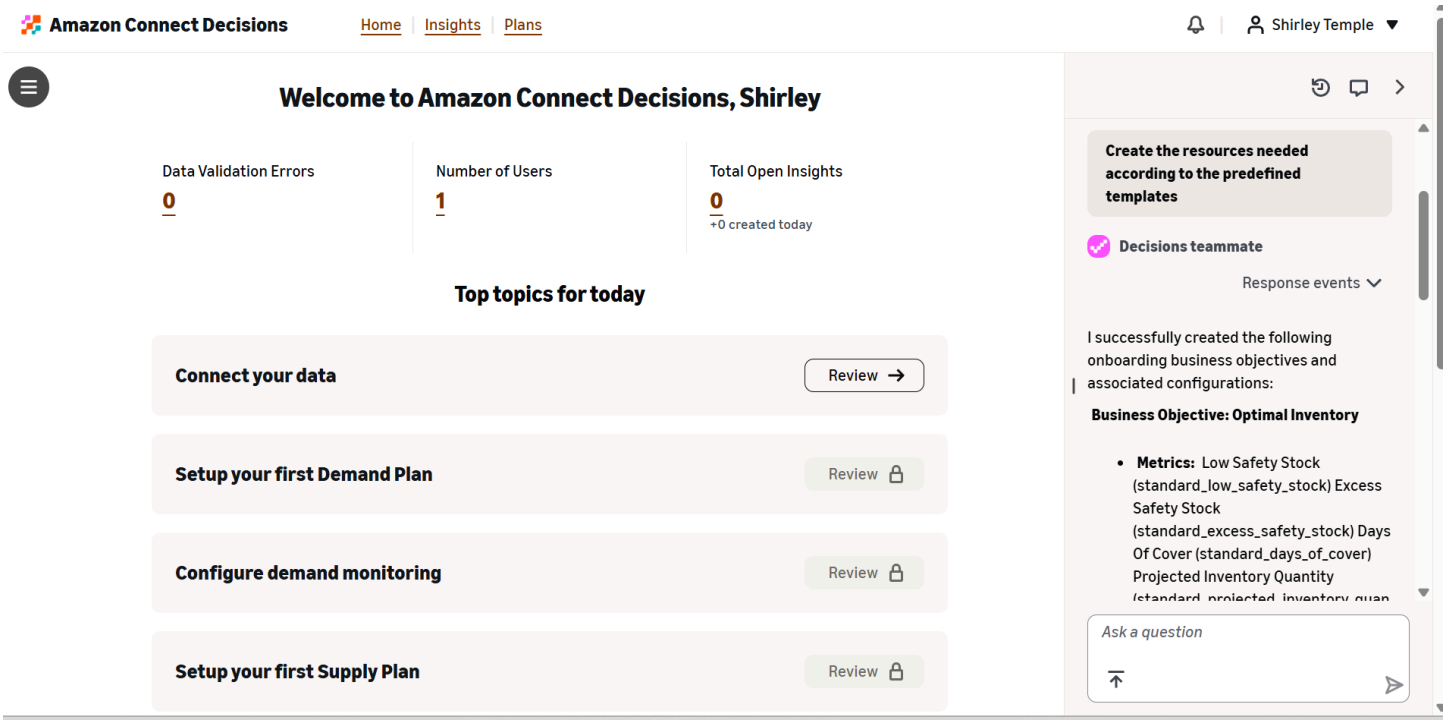

## Nach dem Ausfüllen des Fragebogens

Klicken Sie nach Abschluss aller vier Schritte auf Senden:



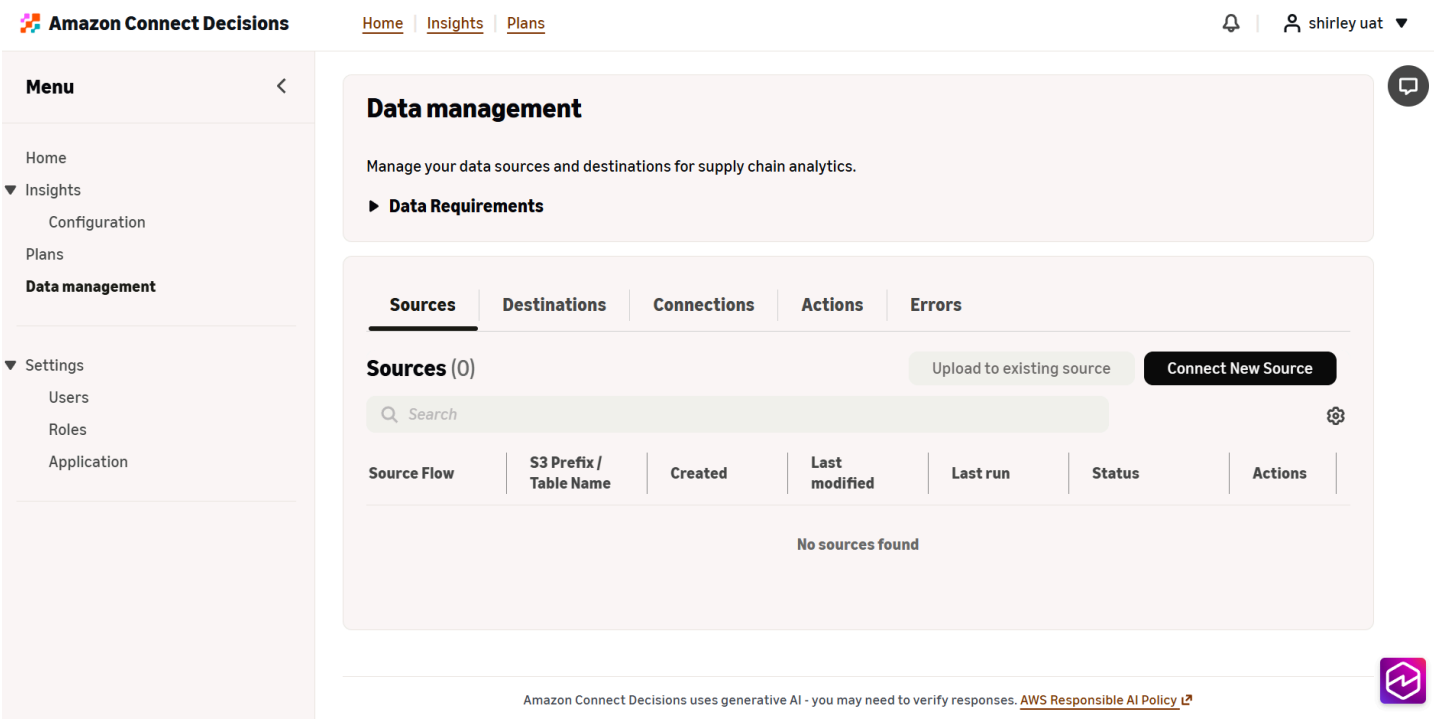

- Sie werden auf die Startseite weitergeleitet. Dort finden Sie ein Dashboard und Themenkarten, die Sie durch die verbleibenden Onboarding-Schritte führen sollen.

- Das System erstellt auto Metriken und Regeln innerhalb der Anwendung auf der Grundlage Ihrer Auswahl. Diese werden im Status Entwurf erstellt und sind nicht sofort aktiv.
- Sie können die auto erstellten Metriken und Regeln überprüfen und sie dann aktivieren, wenn sie Ihren Anforderungen entsprechen, oder Ihre eigenen Metriken und Regeln erstellen, die auf Ihre spezifischen Geschäftsanforderungen zugeschnitten sind.




## Erstellen Sie Ihren ersten Source-Flow

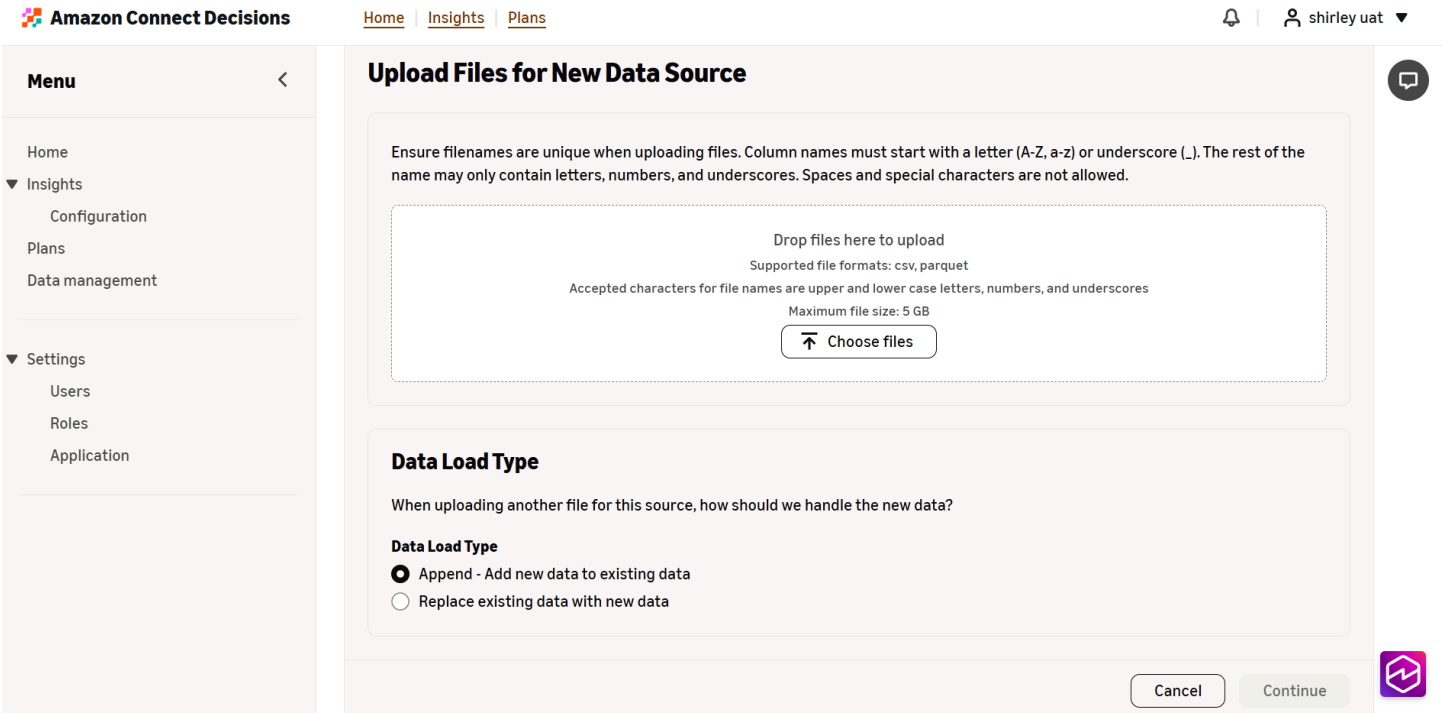
Um mit dem Onboarding Ihrer Daten zu beginnen, klicken Sie auf Überprüfen für die Themenkarte Connect your data oder navigieren Sie in Amazon Connect Decisions im „Hamburger-Menü“ zum Tab Datenmanagement. Hier können Sie alle Ihre bestehenden Quellflüsse sehen. Wenn Sie noch keine eingerichtet haben, klicken Sie zunächst auf „Neue Quelle Connect“.




# Laden Sie Ihre Quelldaten hoch

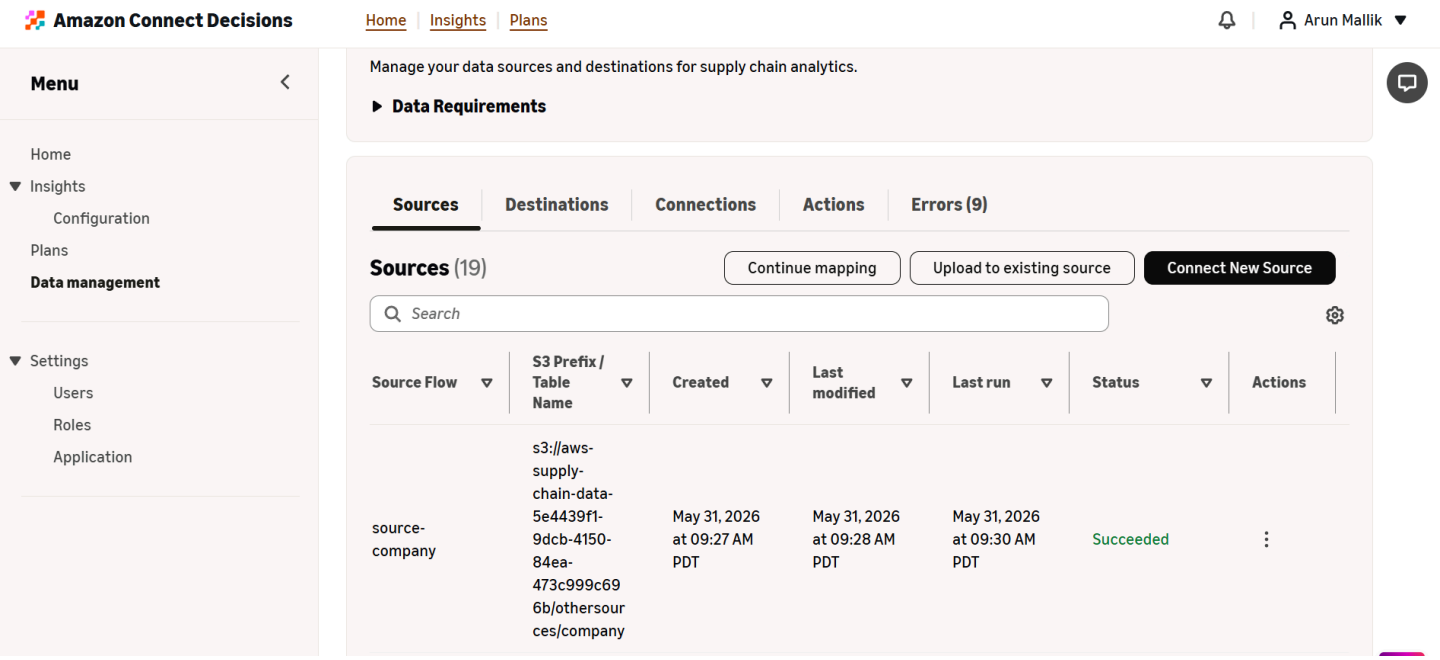
Laden Sie Ihre CSV-Dateien hoch, die Quelldaten enthalten, die auf den für Ihren Anwendungsfall erforderlichen CDM-Tabellen basieren. Sie können wählen, wie Sie mit Datenaktualisierungen umgehen möchten:

- Anhängen: Fügt neue Daten zu bestehenden Daten hinzu
- Ersetzen: Ersetzt bestehende Daten durch neue Daten




Wenn Sie Dateien hochladen, erstellt Amazon Connect Decisions automatisch eine Ordnerstruktur in S3 für diese Daten, einschließlich:

- Ein übergeordneter Ordner, der nach Ihrem ausgewählten Quellsystem benannt ist
- Ein Unterordner, der nach dem Namen der ausgewählten Quelltabelle benannt ist
- Alle Dateien in einem Unterordner werden in derselben Quelltabelle gespeichert
- Diese Dateistruktur wird auch verwendet, um den Amazon S3 S3-Ordnerpfad zu erstellen

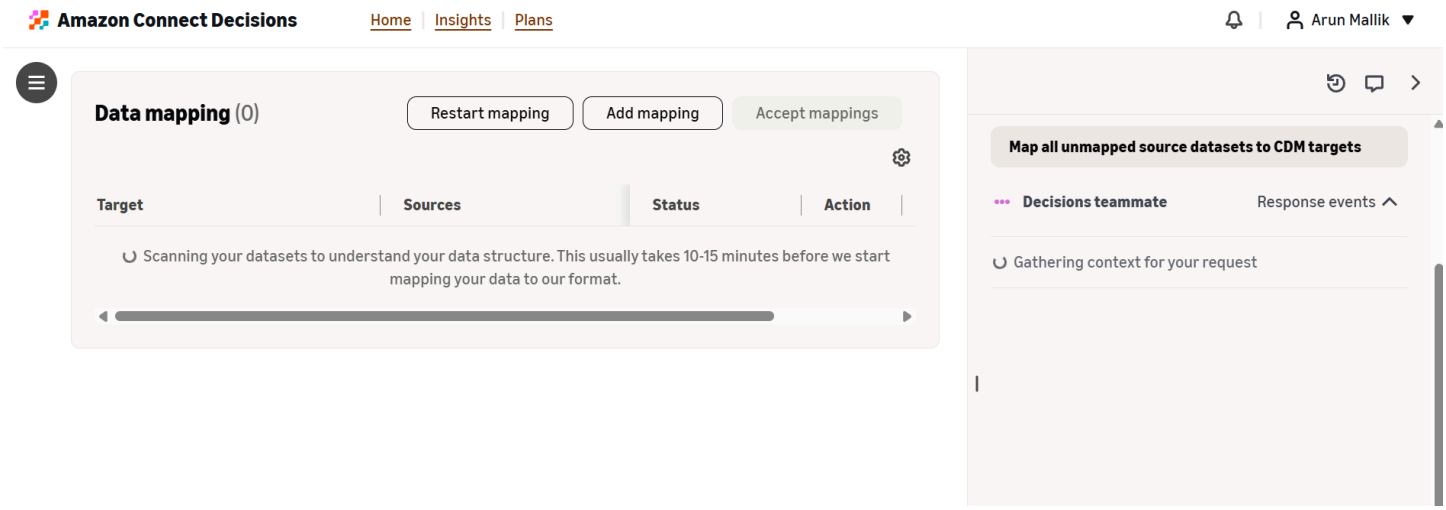



# Source-to-CDM Zielzuweisung

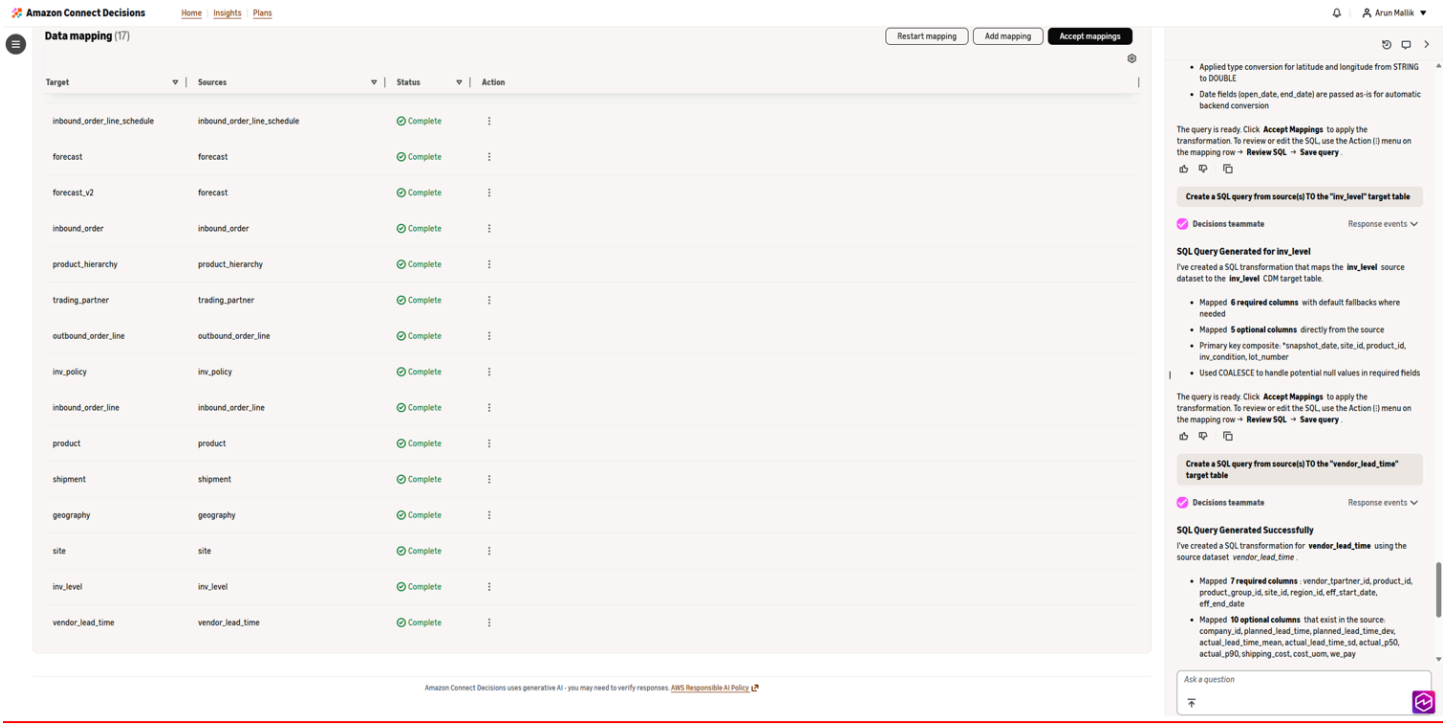
Sobald Ihre Dateien hochgeladen wurden, beginnt Amazon Connect Decisions mit der Analyse Ihrer Daten und ordnet sie automatisch einer oder mehreren CDM-Zieltabellen von Amazon Connect Decisions zu.

## Was ist zu erwarten

- Dieser Schritt kann je nach Menge der hochgeladenen Daten zwischen 10 und 15 Minuten dauern
- Der Data Agent arbeitet im Hintergrund, um die besten CDM-Zieldatensätze für Ihre Quelldaten zu identifizieren.
- Wenn Sie diese Seite verlassen, schlagen automatische Mappings fehl. Bitte lassen Sie während der Wartezeit die Registerkarte „Entscheidungen und Datenmanagement“ von Amazon Connect geöffnet, um sicherzustellen, dass die automatische Zuordnung abgeschlossen wird.

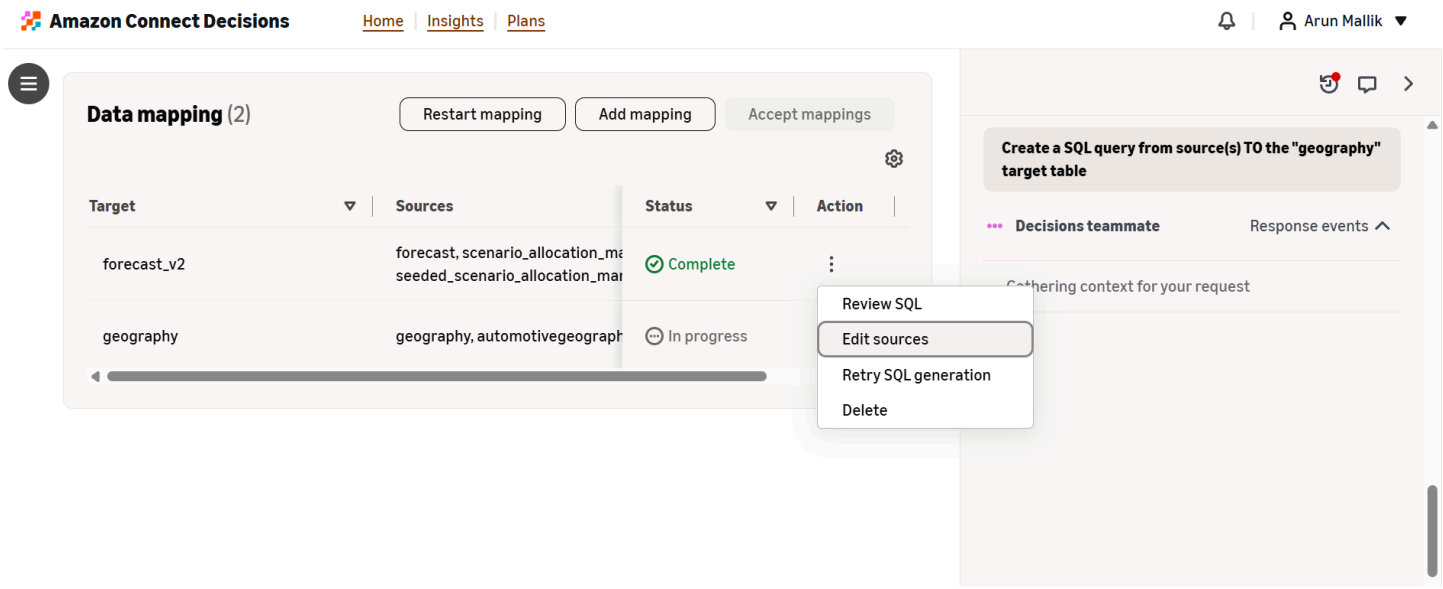



Sobald der Vorgang abgeschlossen ist, bietet der Data Agent eine Begründung für die Zuordnung von Quelle zu Ziel auf der Grundlage sich überschneidender Daten. Sie können diese überprüfen und dem Agenten Fragen zu allen Zuordnungsergebnissen stellen.




Um Quellzuordnungen zu überprüfen und zu bearbeiten, können Sie:

- Interagieren Sie direkt mit dem Data Agent und verwenden Sie dabei natürliche Sprache, um Quell-Ziel-Zuordnungen zu aktualisieren.
- Klicken Sie auf die Aktionen und wählen Sie „Quellen bearbeiten“.




## Zuordnungen bearbeiten

Von hier aus können Sie:

- Die Quell- und Zielzuordnung bei Bedarf manuell aktualisieren
- Stellen Sie Fragen, indem Sie den Data Agent auf der rechten Seite des Bildschirms verwenden, um die Zuordnungen zu bestätigen
- Weitere Informationen zu bestimmten Datensätzen finden Sie in den Benutzerhandbüchern

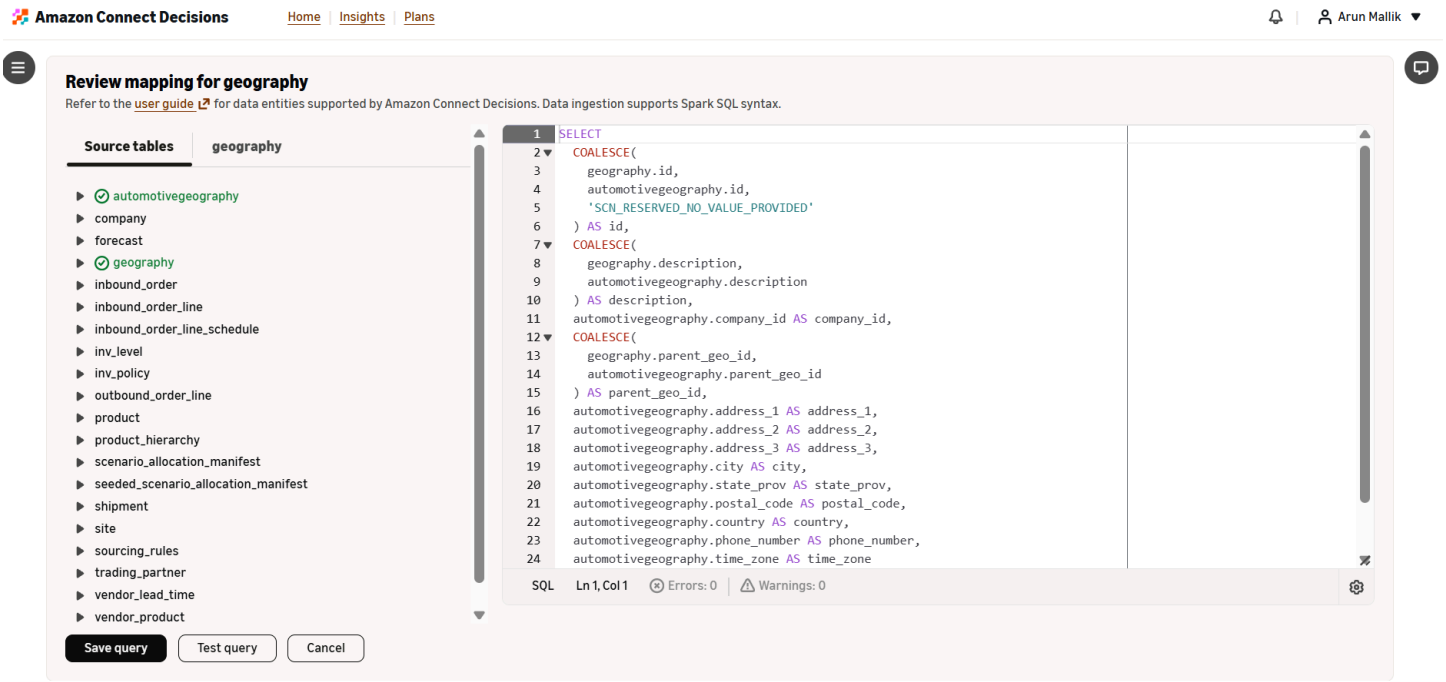
# Column/Data Kartierung

Nachdem die Zuordnung von Quelle zu Ziel abgeschlossen ist, erstellt Amazon Connect Decisions automatisch SQL-Transformationsabfragen von Ihrem Quelldatensatz zum CDM-Ziel. Nachdem eine Ihrer Zuordnungen abgeschlossen ist, erhalten Sie vom Data Agent eine Benachrichtigung, in der das Ergebnis der Zuordnung detailliert beschrieben wird.


Von hier aus sollten Sie die für Mappings generierte SQL überprüfen, indem Sie im Aktionsmenü „SQL überprüfen“ auswählen.

Wenn Sie sich das Mapping (SQL) ansehen, werden Sie Folgendes sehen:

- Die Spalten des Quelldatensatzes, die Sie hinzugefügt haben
- Spalten der Ziel-CDM-Tabelle als Referenz
- Die Transformations-SQL, die sie verbindet
- Die vom Datenagenten bereitgestellte Begründung für die Zuordnung




## Zuordnungen bearbeiten

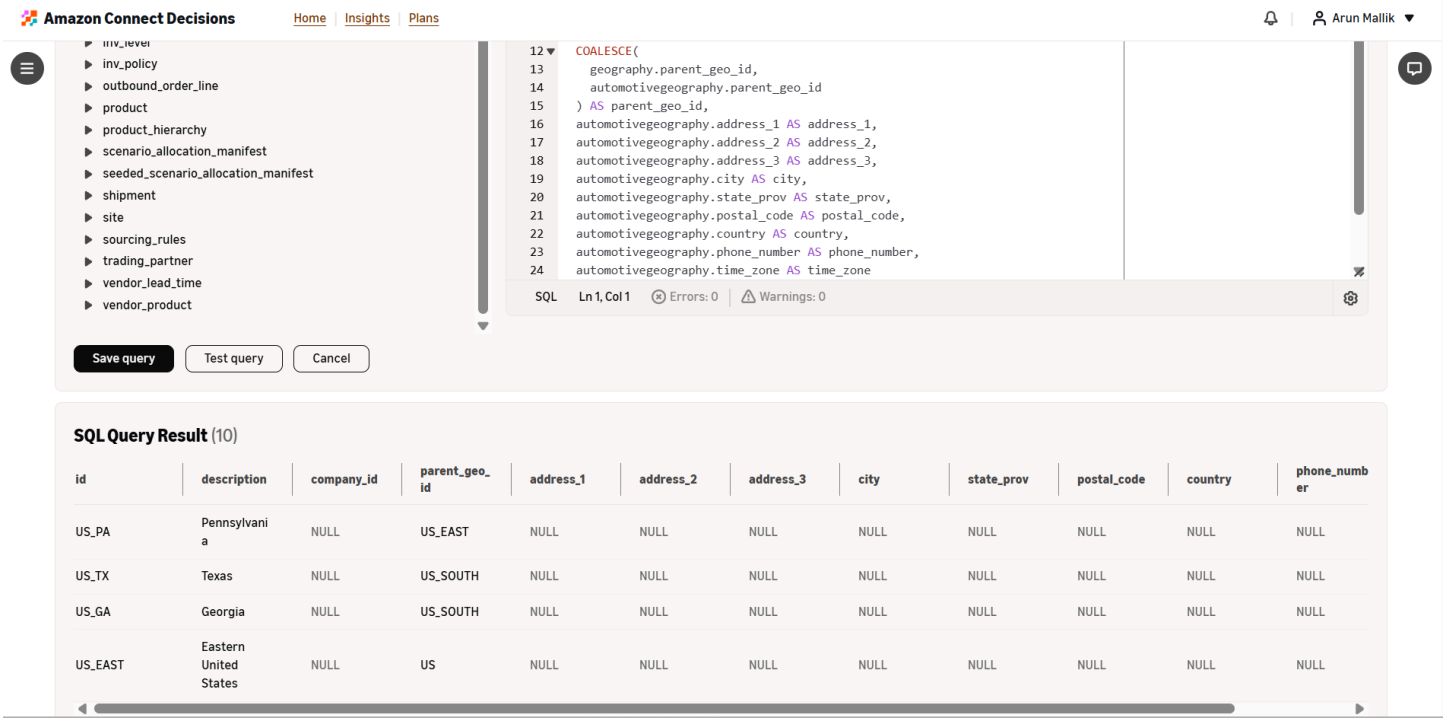
Sie haben zwei Möglichkeiten, Zuordnungen zu bearbeiten:

- Arbeiten Sie mit Data Agent: Verwenden Sie natürliche Sprache, um Fragen zu stellen und die Zuordnungen zu verwalten und zu aktualisieren
- SQL direkt bearbeiten: Wenn Sie mit SQL vertraut sind, können Sie die Abfrage direkt ändern

## Testen Sie Ihre Änderungen

Während Sie die Zuordnungsabfrage bearbeiten, testen Sie sie mit der Funktion „Testabfrage“ weiter. Dadurch erhalten Sie eine scrollbare Vorschau, wie ein Beispiel dafür, wie Ihre Daten in das Ziel-CDM umgewandelt werden. Verwenden Sie diese Option, um sicherzustellen, dass Ihre Transformation ordnungsgemäß ausgeführt wird, und um alle entsprechenden Aktualisierungen von Ihrem Quell- zum Ziel-CDM zu überprüfen.

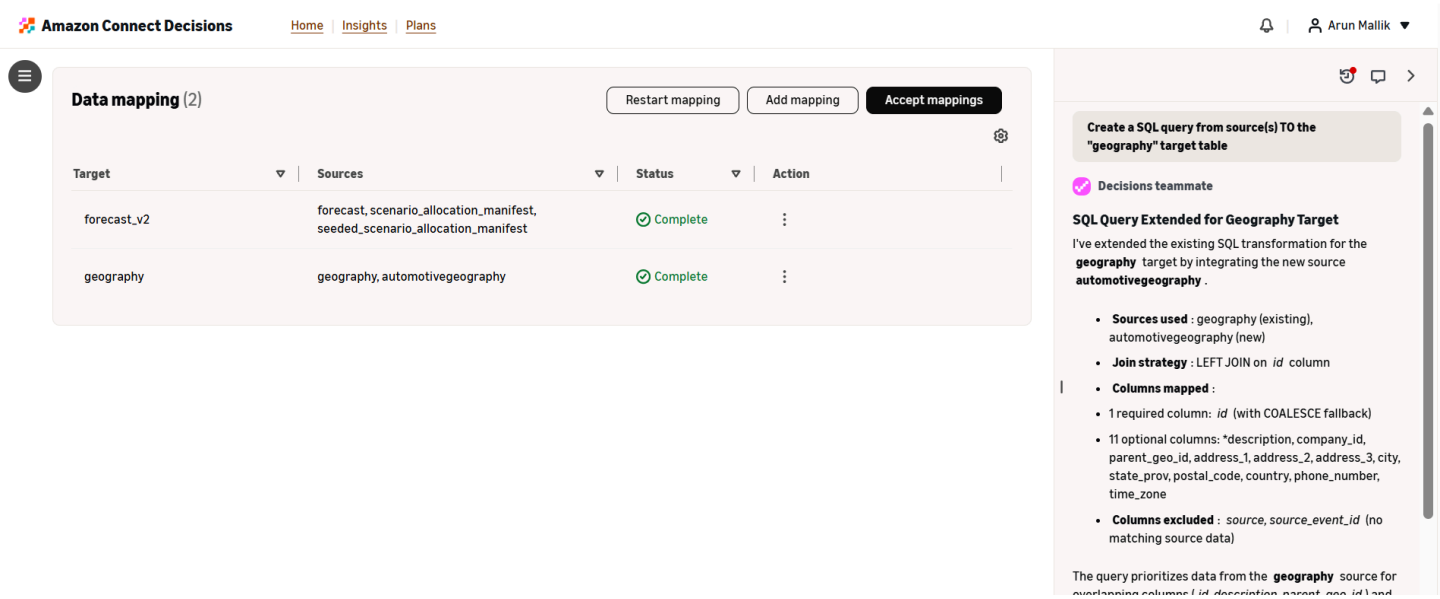
Wenn Sie mit der Mapping-Ausgabe zufrieden sind, wählen Sie "Abfrage speichern" aus, um die Transformationsabfrage für dieses Quell-Ziel-Paar zu speichern.




# Zuordnungen überprüfen und akzeptieren

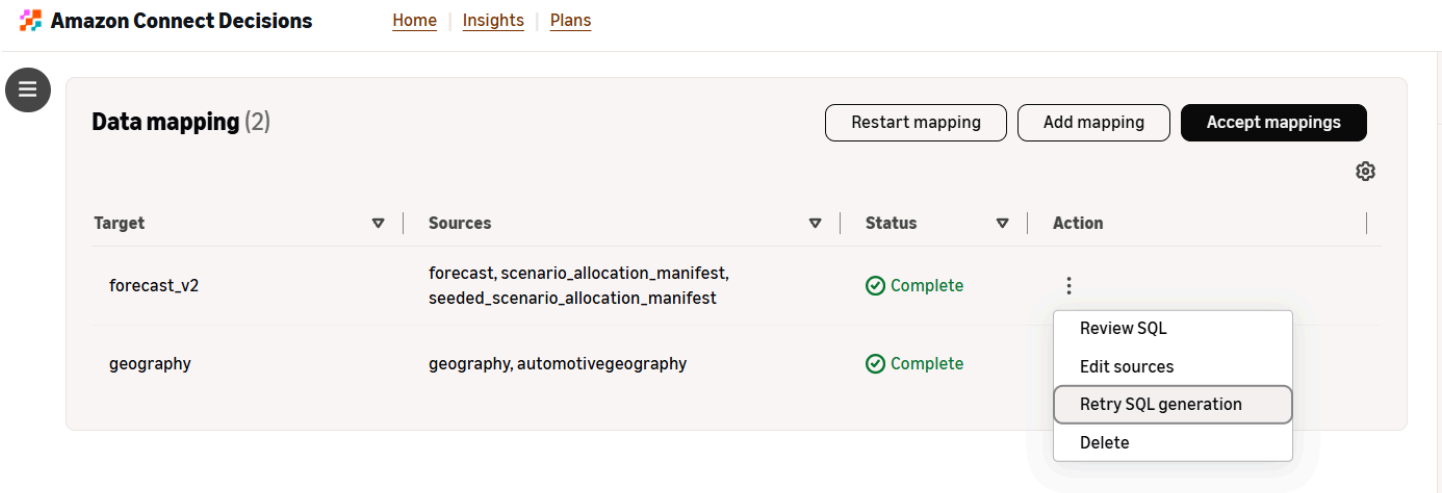
Überprüfen Sie die verbleibenden Zuordnungen für jeden Ihrer Quelldatensätze. Der Data Agent wird weiterhin auf der rechten Seite des Bildschirms angezeigt, wenn Sie Fragen haben oder Hilfe zur Fehlerbehebung benötigen.

Wenn Sie mit allen Zuordnungen zufrieden sind, akzeptieren Sie sie, um das Daten-Onboarding abzuschließen, indem Sie auf Zuordnungen akzeptieren klicken.



### Fehlgeschlagene Zuordnungen behandeln

Wenn Mappings fehlschlagen, können Sie „Mapping neu starten“ wählen, um alle Mappings neu zu starten, oder Sie können im Aktionsmenü über „SQL-Generierung erneut versuchen“ manuell versuchen, ein einzelnes Mapping erneut zu versuchen. Der Datenagent kann auch Mappings in natürlicher Sprache wiederholen und hilft Ihnen weiterhin, Probleme zu identifizieren und zu lösen, falls die Fehler weiterhin bestehen.

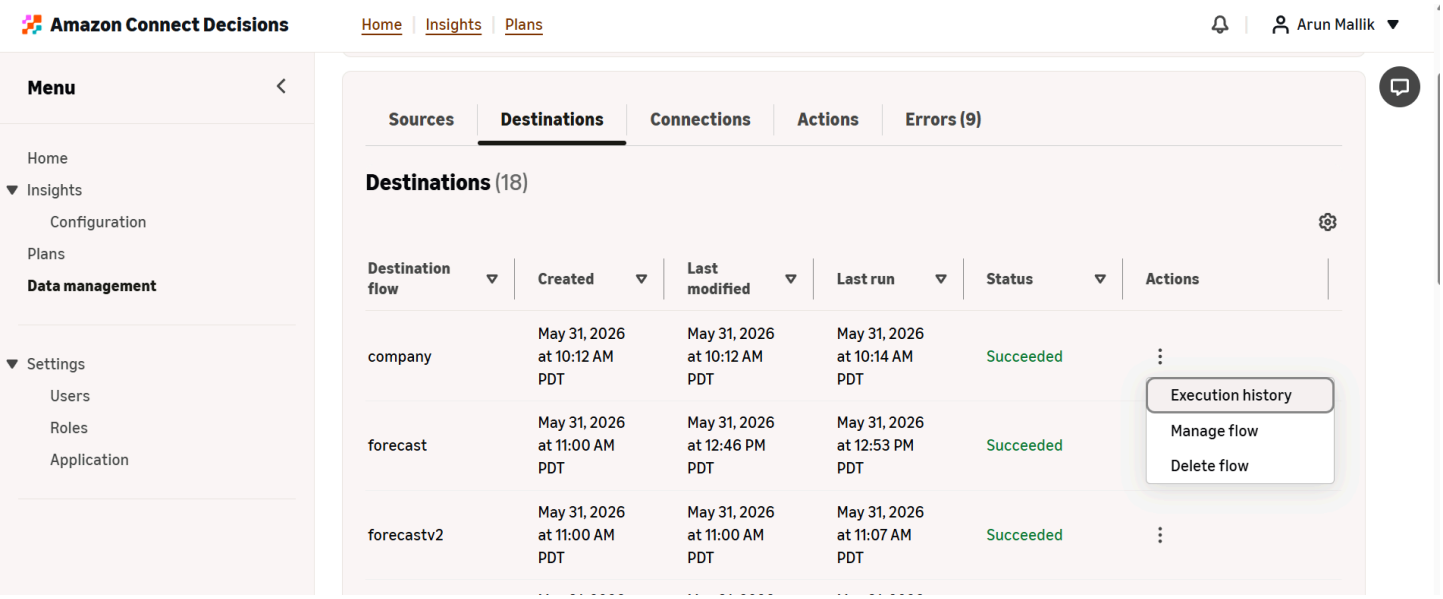



## Überwachen Sie Ihre Datenflüsse

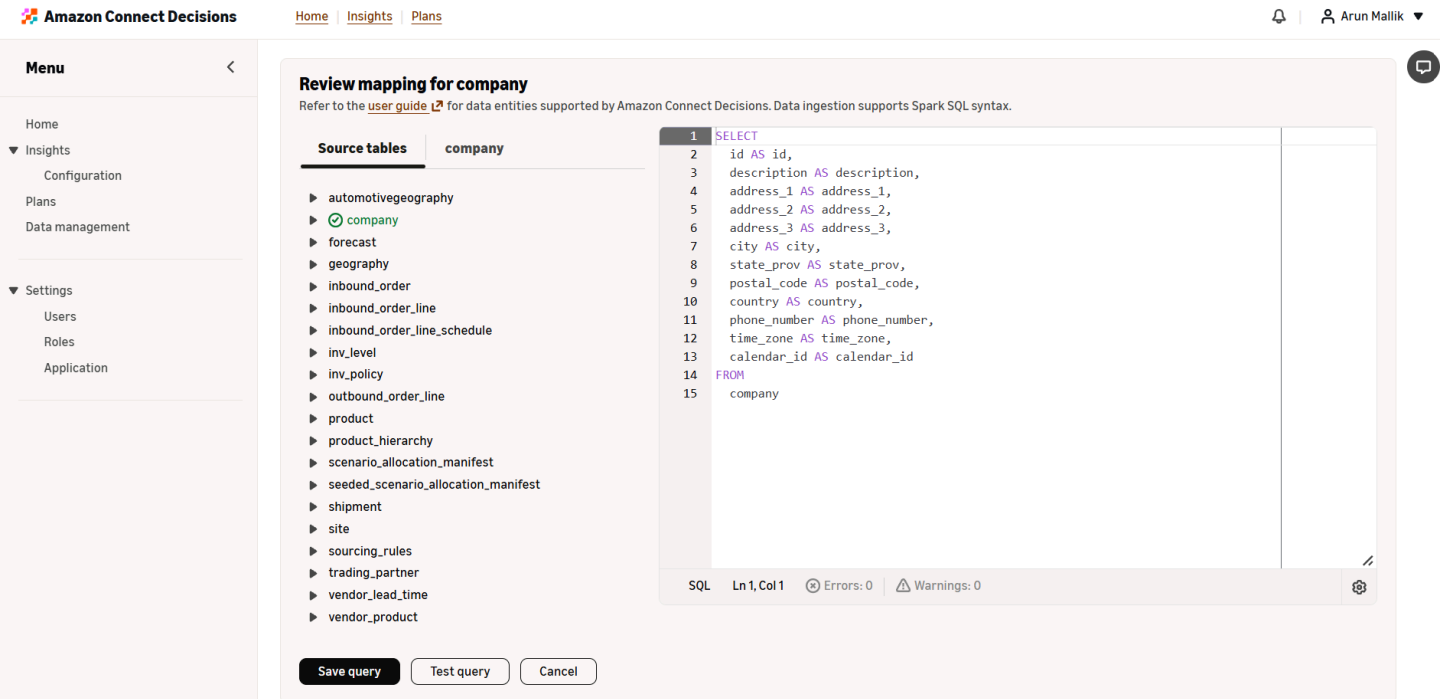
### Registerkarte „Ziele“

Nachdem Sie die Zuordnungen akzeptiert haben, werden Sie in Data Management zur Registerkarte Ziele weitergeleitet, wo Sie:

- Überprüfen Sie die Zielflüsse
- Mappings verwalten und bearbeiten („Flow verwalten“)
- Löschen Sie veraltete Flows
- Überprüfen Sie den Ausführungsstatus dieser Flows




Wenn Sie „Flow verwalten“ auswählen, kehren Sie zur Datenzuordnungsfunktion zurück, in der Sie weiterhin mit dem Datenagenten arbeiten können, um die Zuordnungen im Laufe der Zeit zu verfeinern.




## Registerkarte „Quellen“

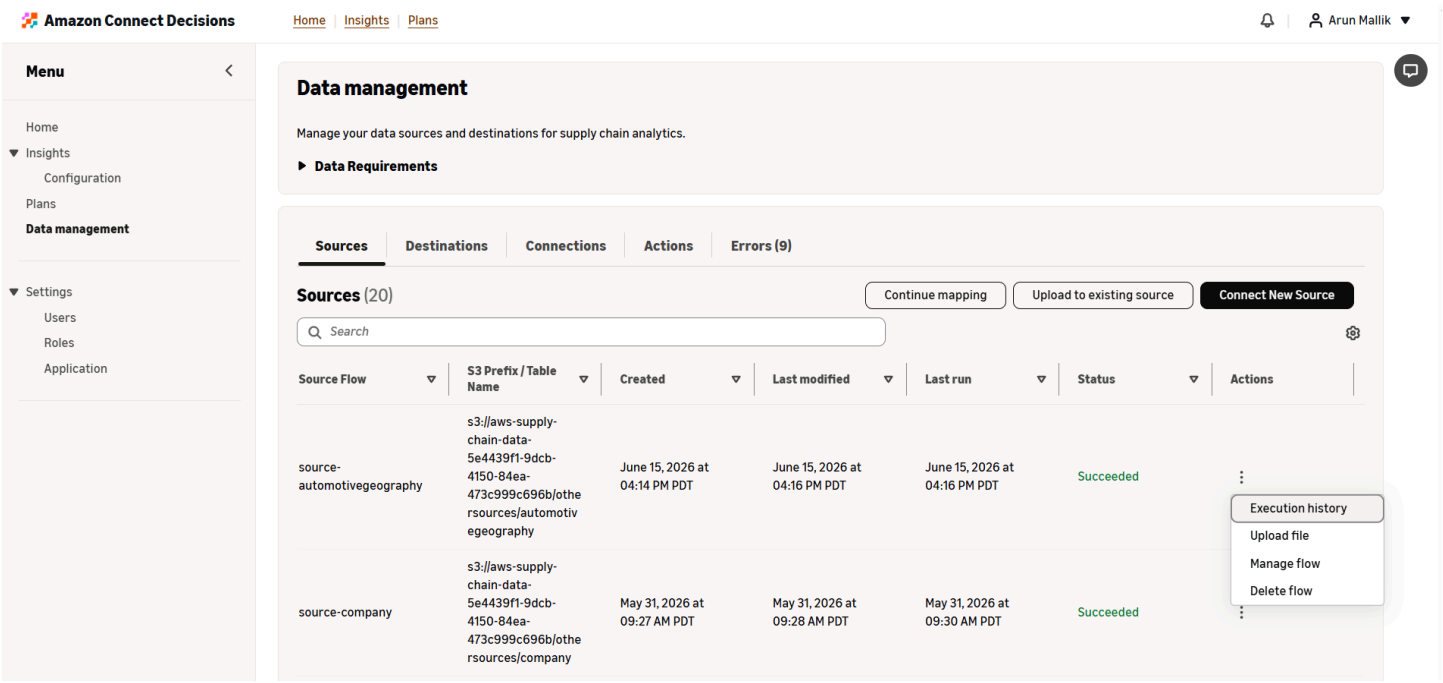
Wenn Sie zurück zum Tab Quellen navigieren, finden Sie:

- Der Quelldatensatz, der erstellt wurde

- Der zugehörige S3-Bucket
- Optionen für:
  - Weitere Quelldaten über einen anderen Datei-Upload anhängen
  - Verwalte den Flow
  - Löschen Sie den Flow
  - Überprüfen Sie die Ausführungen

Wenn Sie „Flow verwalten“ auswählen, gelangen Sie zurück zur Datenzuordnungs-Oberfläche, in der Sie weiterhin mit dem Datenagenten arbeiten können, um die Zuordnungen im Laufe der Zeit zu verfeinern.

Sie haben bei Bedarf auch Zugriff auf „Neue Quelle erstellen“, um den Daten-Onboarding-Prozess für alle neuen Datenquellen neu zu starten.




# Bewährte Methoden

## Datenaufbereitung

- Folgen Sie den Schritten im Abschnitt Voraussetzungen
- Verwenden Sie die UTF-8 Kodierung für alle CSV-Dateien
- Stellen Sie sicher, dass die Dateinamen eindeutig sind

- Überprüfen Sie die Datenqualität vor dem Hochladen

### Mit Data Agent arbeiten

- Seien Sie bei Ihren Anfragen spezifisch
- Bitten Sie um Erklärungen, wenn Sie eine der Entscheidungen nicht verstehen
- Testen Sie alle SQL-Änderungen, bevor Sie sie akzeptieren
- Verwenden Sie die Vorschaufunktion, um Transformationen zu überprüfen

### Laufende Wartung

- Halten Sie Ihre Quelldaten auf dem neuesten Stand
- Überwachen Sie die Flow-Ausführung regelmäßig
- Beheben Sie Datenfehler umgehend, wenn sie benachrichtigt werden
- Dokumentieren Sie benutzerdefinierte Transformationen für Ihr Team

## Mit JDBC eine Verbindung zu Ihrer Datenbank herstellen

Dieser Leitfaden führt Sie durch die Verbindung Ihrer Datenbank mit Amazon Connect Decisions mithilfe von Java Database Connectivity (JDBC). Sie richten eine sichere Verschlüsselung für Ihre Datenbankanmeldedaten ein und stellen eine Verbindung her, über die Amazon Connect Decisions auf Ihre Daten zugreifen kann.

### Was ist eine JDBC-Verbindung und wann sollten Sie sie verwenden?

Durch die JDBC-Verbindung kann Amazon Connect Decisions eine Verbindung zu Ihrer vorhandenen Datenbank herstellen, um Daten zu lesen, anstatt dass Sie CSV-Dateien exportieren und hochladen oder Ihre eigenen Extractions-, Transformations-, Load- (ETL) -Pipelines für S3 einrichten müssen. Dieser Ansatz ist ideal, wenn:

- Ihre Daten sind bereits in einer Glue-compatible relationalen AWS-Datenbank gespeichert. Kompatible Datenbanken und Versionen finden Sie in diesem Handbuch.
- Sie möchten Datenzugriff in Echtzeit oder nahezu in Echtzeit ohne manuelle Dateiexporte
- Ihr Datenvolumen ist groß und wird häufig aktualisiert

- Sie ziehen es vor, Ihre Daten an ihrem aktuellen Standort zu behalten, anstatt sie zu duplizieren
- Wenn Sie mit kleineren Datensätzen arbeiten oder dateibasierte Uploads bevorzugen, ist der standardmäßige CSV-Upload-Prozess für Ihre Bedürfnisse möglicherweise einfacher. Weitere Informationen zu diesem Prozess finden Sie im Data Onboarding-Benutzerhandbuch.

## Voraussetzungen

Stellen Sie vor Beginn sicher, dass Sie über Folgendes verfügen:

- Ein AWS-Konto mit Berechtigungen zum Erstellen von KMS-Schlüsseln und Secrets Manager Manager-Ressourcen
- Ihre AWS-Konto-ID und die Region, in der Amazon Connect Decisions tätig sein wird
- Verbindungsdetails zur Datenbank: Hostname, Port, Datenbankname und Anmeldeinformationen
- Administratorzugriff auf Ihre Datenbank zur Überprüfung der Konnektivität
- Ihre Datenbank ist so konfiguriert, dass sie Verbindungen von AWS-Services akzeptiert

## Erstellen Sie einen Customer-Managed KMS-Schlüssel

Bevor Sie Ihre Datenbank mit Amazon Connect Decisions verbinden, müssen Sie die Verschlüsselung Ihrer Datenbankanmeldedaten einrichten. AWS Key Management Service (KMS) bietet diese Sicherheitsebene und stellt sicher, dass Ihre Verbindungsdetails geschützt bleiben.

### Erstellen Sie Ihren KMS-Schlüssel

1. Navigieren Sie zur AWS KMS KMS-Konsole
   - Öffnen Sie die AWS-Managementkonsole in Ihrem Browser
   - Geben Sie in der Suchleiste oben „KMS“ ein und wählen Sie aus den Ergebnissen „Key Management Service“ aus
   - Dadurch wird das KMS-Dashboard geöffnet, in dem Sie die Verschlüsselungsschlüssel verwalten
2. Initiieren Sie die Schlüsselerstellung
   - Suchen Sie im KMS-Dashboard oben rechts nach der Schaltfläche Schlüssel erstellen und klicken Sie darauf
   - Dadurch wird der Assistent zur Schlüsselerstellung gestartet, der Sie durch den Einrichtungsprozess führt

3. Konfigurieren Sie den Schlüsseltyp und die Verwendung
   - Wählen Sie auf der Seite „Schlüssel konfigurieren“ den Schlüsseltyp Symmetrisch aus (dies ist die Standardoption und die empfohlene Option)
   - Lassen Sie unter Schlüsselverwendung die Option „Verschlüsseln und Entschlüsseln“ ausgewählt
4. Legen Sie die Details zur Schlüsselidentifikation fest
   - Geben Sie im Feld „Alias“ einen aussagekräftigen Namen für Ihren Schlüssel ein, z. B. `aws-supply-chain-database-key`
   - Fügen Sie im Feld „Beschreibung“ einen Kontext wie „Verschlüsselungsschlüssel für Amazon Connect Decisions-Datenbankanmeldedaten“ hinzu
   - Fügen Sie optional Tags hinzu, um Ihre AWS-Ressourcen zu organisieren und nachzuverfolgen (z. B. Key: „Project“, Value: „Amazon Connect Decisions“)
5. Definieren Sie wichtige Administratorberechtigungen
   - Wählen Sie die IAM-Benutzer oder -Rollen aus, die in der Lage sein sollen, diesen Schlüssel zu verwalten (Richtlinien erstellen, löschen, ändern)
   - Fügen Sie mindestens Ihre eigene Admin-Rolle hinzu, um sicherzustellen, dass Sie den Schlüssel später bei Bedarf ändern können
   - Diese Administratoren können den Schlüssel verwalten, haben aber nicht automatisch die Erlaubnis, ihn zu verwenden encryption/decryption
   - Wählen Sie im Bereich „Löschen von Schlüsseln“ die Option Schlüsseladministratoren erlauben, diesen Schlüssel zu löschen. (Dies ist die Standardoption und die empfohlene Option)
6. Definieren Sie die Berechtigungen zur Verwendung von Schlüsseln
   - Auf dieser Seite finden Sie Optionen zur Auswahl von IAM-Benutzern und -Rollen, die den Schlüssel verwenden können
   - Überspringen Sie hier die Auswahl bestimmter Benutzer. Im nächsten Schritt konfigurieren Sie die Serviceberechtigungen
7. Konfigurieren Sie die wichtigsten Richtlinien für die Amazon Connect Decisions-Dienste
   - Es wird ein Richtlinien-Editor mit Standard-JSON angezeigt
   - Fügen Sie im KMS-Schlüsselrichtlinien-Editor die folgende Anweisung an Ihr vorhandenes Array „Statement“ an
   - Diese Richtlinie gewährt Ihrem Konto die volle Kontrolle und ermöglicht es den Diensten von Amazon Connect Decisions (Secrets Manager und Glue), Ihre Datenbankanmeldeinformationen zu entschlüsseln.

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

8. Überprüfen und abschließen
   - Überprüfen Sie alle Ihre Konfigurationseinstellungen auf der Übersichtsseite
   - Vergewissern Sie sich, dass Ihr Alias, Ihre Beschreibung und Ihre Richtlinie korrekt sind
   - Klicken Sie auf Fertig stellen, um den Schlüssel zu erstellen
   - Nach der Erstellung kehren Sie zum KMS-Dashboard zurück, wo Ihr neuer Schlüssel in der Liste erscheint

### Was ist zu erwarten

Die Schlüsselerstellung erfolgt sofort. Nach der Erstellung wird Ihr neuer Schlüssel in der KMS-Konsole mit dem Status „Aktiviert“ aufgeführt. Der Schlüssel ist jetzt bereit, Ihre Datenbankanmeldedaten in Secrets Manager zu verschlüsseln.

## AWS Secrets Manager konfigurieren

Nachdem Sie über einen KMS-Schlüssel verfügen, erstellen Sie einen geheimen Schlüssel in AWS Secrets Manager, um Ihre Datenbankanmeldedaten sicher zu speichern, und konfigurieren dann eine Ressourcenrichtlinie, die Amazon Connect Decisions den Zugriff auf dieses Geheimnis ermöglicht.

### Erstellen Sie Ihr Geheimnis

1. Navigieren Sie zu AWS Secrets Manager
   - Geben Sie in der Suchleiste der AWS-Managementkonsole „Secrets Manager“ ein

- Wählen Sie „Secrets Manager“ aus den Ergebnissen aus, um das Service-Dashboard zu öffnen

2. Fangen Sie an, ein neues Geheimnis zu erstellen
   - Klicken Sie auf die Schaltfläche Neues Geheimnis speichern
   - Wählen Sie auf der Seite „Geheimtyp auswählen“ die Option Anderer Geheimtyp aus (dies gibt Ihnen Flexibilität bei der Strukturierung Ihrer Anmeldeinformationen)
3. Geben Sie Ihre Datenbankanmeldedaten ein
   - Fügen Sie im Abschnitt Schlüssel-Wert-Paare Ihre Datenbankverbindungsdetails als Zeichenfolgen hinzu:

```
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. Wählen Sie Ihren Verschlüsselungsschlüssel
   - Wählen Sie unter „Verschlüsselungsschlüssel“ die Option Wählen Sie einen AWS-KMS-Schlüssel
   - Wählen Sie aus der Dropdownliste den KMS-Schlüssel aus, den Sie in Schritt 1 erstellt haben (z. B.`aws-supply-chain-database-key`)
   - Dadurch wird sichergestellt, dass Ihre Anmeldeinformationen mit Ihrem vom Kunden verwalteten Schlüssel verschlüsselt sind
5. Nennen Sie Ihr Geheimnis
   - Geben Sie einen aussagekräftigen Namen für Ihr Geheimnis ein, z. B. `aws-supply-chain-production-database`
   - Fügen Sie optional eine Beschreibung wie „Datenbankanmeldedaten für die Produktionsumgebung von Amazon Connect Decisions“ hinzu
   - Fügen Sie bei Bedarf Tags für die Organisation hinzu (z. B. Schlüssel: „Umgebung“, Wert: „Produktion“)
6. Fügen Sie Ressourcenberechtigungen hinzu
   - Klicken Sie auf „Berechtigungen bearbeiten“. Fügen Sie im Richtlinien-Editor die folgende Richtlinie ein. Diese Richtlinie ermöglicht es den Diensten von Amazon Connect Decisions, Ihr Geheimnis zu lesen.

```
{
```

```
  "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. Speichern Sie die Richtlinie
   - Klicken Sie auf Speichern, um die Ressourcenrichtlinie anzuwenden
   - Die Richtlinie ist jetzt aktiv und ermöglicht Amazon Connect Decisions, Ihre Datenbankanmeldedaten abzurufen.
8. Rotation konfigurieren (optional)
   - Bei diesem Setup können Sie die automatische Rotation überspringen, indem Sie Automatische Rotation deaktivieren auswählen
   - Sie können die Rotation später aktivieren, wenn Ihre Sicherheitsrichtlinien dies erfordern
9. Überprüfen und erstellen
   - Überprüfe all deine geheimen Daten
   - Klicken Sie auf Speichern, um das Geheimnis zu erstellen
   - Sie werden zum Secrets Manager Manager-Dashboard zurückgeleitet
10. Speichere deinen geheimen ARN
    - Finde dein neu erstelltes Geheimnis in der Geheimnisliste
    - Klicken Sie auf den geheimen Namen, um die zugehörige Detailseite zu öffnen
    - Oben siehst du den Secret ARN
    - Kopieren und speichern Sie diesen ARN
    - Das ARN-Format sieht wie folgt aus: `arn:aws:secretsmanager:us-east-1:123456789012:secret:aws-supply-chain-production-database-AbCdEf`
11. Ressourcenberechtigungen bearbeiten
    - Klicken Sie auf „Berechtigungen bearbeiten“
    - Fügen Sie den kopierten geheimen ARN ein und `<COPY-THE-SECRET-ARN-HERE-AFTER-CREATING>` ersetzen Sie ihn durch Ihren kopierten ARN
    - Klicken Sie auf Speichern, um die Richtlinie anzuhängen

### Was ist zu erwarten

Ihr Geheimnis ist jetzt sicher gespeichert und mit Ihrem KMS-Schlüssel verschlüsselt. Die Dienste von Amazon Connect Decisions sind berechtigt, die Anmeldeinformationen abzurufen, wenn eine Datenbankverbindung hergestellt wird, aber die Anmeldeinformationen bleiben im Ruhezustand und bei der Übertragung verschlüsselt.

## Verbinden Sie Ihre Datenbank mit Amazon Connect Decisions

Nachdem Ihr KMS-Schlüssel und Ihr KMS-Geheimnis konfiguriert sind, können Sie die JDBC-Verbindung in Amazon Connect Decisions einrichten.

### Konfigurieren Sie Ihre JDBC-Verbindung

1. Navigieren Sie zu Amazon Connect Decisions > Data Management
   - Melden Sie sich bei Ihrer Amazon Connect Decisions-Instance an
   - Wählen Sie in der Hauptnavigation „Datenmanagement“
   - Navigieren Sie in der Tab-Navigation zu „Verbindungen“
   - Wählen Sie „Neue Verbindung“, um eine neue Verbindung zu erstellen
2. Geben Sie Ihre Verbindungsdetails ein
   - Verbindungsname (erforderlich): Geben Sie eine eindeutige Kennung für diese Verbindung ein (z. B. „Produktionsdatenbank“)
   - Beschreibung (optional): Fügen Sie Details zum Zweck und zur Verwendung dieser Verbindung hinzu, damit Ihr Team versteht, auf welche Daten es zugreift
   - JDBC-URL (erforderlich): Geben Sie Ihre vollständige JDBC-Verbindungszeichenfolge im folgenden Format ein: (z. B.) `jdbc:<database-type>://<hostname>:<port>/<database>` `jdbc:postgresql://db.example.com:5432/mydb`
   - Schemaname (optional): Geben Sie bei Bedarf das Datenbankschema an (z. B. „public“, „dbo“, „myschema“). Lassen Sie das Feld leer, um das Standardschema Ihrer Datenbank zu verwenden
   - Geheimer ARN (erforderlich): Fügen Sie den geheimen ARN ein, den Sie in Schritt 2 gespeichert haben. Auf diese Weise kann Amazon Connect Decisions Ihre Datenbankanmeldedaten sicher aus Secrets Manager abrufen.
   - SSL-Verbindung erzwingen: Lassen Sie dieses Kontrollkästchen aktiviert (empfohlen), um eine SSL/TLS Verschlüsselung für Ihre Datenbankverbindung zu verlangen

- VPC-Endpunkt-Servicename (erforderlich): Geben Sie Ihren VPC-Endpunkt-Servicenamen für private Konnektivität über AWS ein PrivateLink (Format:) `com.amazonaws.vpce.<region>.vpce-svc-xxxxxxxxx`

3. Connect zu Ihrer Datenbank her
   - Klicken Sie auf „Connect“, um die Verbindung zu testen und herzustellen. Amazon Connect Decisions überprüft, ob es mit den angegebenen Anmeldeinformationen erfolgreich eine Verbindung zu Ihrer Datenbank herstellen kann. Dieser Schritt kann bis zu 2 Minuten dauern. Bitte verlassen Sie diesen Bildschirm nicht, während die Verbindung hergestellt wird.
   - Wenn die Verbindung erfolgreich ist, werden Sie automatisch zur Tabellenauswahl weitergeleitet
   - Wenn die Verbindung fehlschlägt:
     - Überprüfe deine Verbindungsdetails, um sicherzustellen, dass alle Felder korrekt sind:
       - Stellen Sie sicher, dass Ihr geheimer ARN korrekt ist
       - Bestätigen Sie, dass Ihre Datenbankanmeldedaten korrekt sind
       - Vergewissern Sie sich, dass Ihr JDBC-URL-Format korrekt ist
       - Stellen Sie sicher, dass Ihre Datenbank so konfiguriert ist, dass sie Verbindungen von AWS-Services akzeptiert
       - Stellen Sie sicher, dass Ihr KMS-Schlüssel und die Secrets Manager Manager-Richtlinien korrekt konfiguriert sind
     - Sie können das Chat-Erlebnis auch zur Behebung von Verbindungsproblemen nutzen, indem Sie Fragen wie „Warum schlägt meine Datenbankverbindung fehl?“ stellen oder „Hilf mir, meine JDBC-Verbindung zu debuggen“
4. Wählen Sie die zu importierenden Tabellen aus
   - Sobald die Verbindung hergestellt ist, wird der Bildschirm „Tabellen auswählen“ mit allen verfügbaren Tabellen aus Ihrer Datenbank angezeigt
   - Markieren Sie das Kontrollkästchen neben jeder Tabelle, die Sie aufnehmen möchten
5. Konfigurieren Sie den Zeitplan für die Tabellenaktualisierung
   - Klicken Sie für jede ausgewählte Tabelle auf das Dreipunktmenü in der Spalte Aktion und wählen Sie „Aktualisierung planen“
   - Stellen Sie im Dialogfeld „Ladedetails konfigurieren“ Folgendes ein:
     - Schrittfrequenz: Wie oft aktualisiert werden soll (stündlich, täglich, wöchentlich oder Benutzerdefiniert)

    - Startstunde: Die Zeit, zu der die Aktualisierung beginnen soll (wird in UTC mit Ihrem Zeitzonen-Offset angezeigt)
    - Aktualisierungstyp: Wählen Sie Vollständige Aktualisierung (alle Daten ersetzen) oder Inkrementelles Update (neue Daten zu vorhandenen hinzufügen; erfordert die Auswahl einer Spalte mit dem Zeitstempel für Datensätze)
    - Wiederholen Sie den Vorgang nach Bedarf für jede Tabelle
  - Klicken Sie auf Zuordnung starten, wenn alle Tabellen konfiguriert sind
6. Fahren Sie mit der Datenzuordnung fort
  - Ab diesem Zeitpunkt ist die Erfahrung identisch mit unserem Daten-Onboarding-Ablauf
  - Folgen Sie dem Abschnitt Datenzuweisung im Data Onboarding-Benutzerhandbuch, um Ihre Einrichtung abzuschließen

### Was ist zu erwarten

Sobald Ihre Verbindung hergestellt und Tabellen ausgewählt sind, kann Amazon Connect Decisions Daten aus Ihrer Datenbank lesen. Die Verbindung bleibt aktiv und sicher, wobei die Anmeldeinformationen über AWS Secrets Manager verschlüsselt und verwaltet werden. Sie müssen die Anmeldeinformationen in Amazon Connect Decisions nicht manuell aktualisieren. Alle Änderungen, die Sie in Secrets Manager vornehmen, werden automatisch übernommen.

## Bewährte Methoden

### Sicherheits- und Zugriffsmanagement

- Anmeldeinformationen sicher speichern: Verwenden Sie immer AWS Secrets Manager, um Datenbankanmeldedaten zu speichern, niemals hartcodieren Sie Anmeldeinformationen in Verbindungszeichenfolgen oder Konfigurationsdateien
- SSL/TLS Verschlüsselung aktivieren: Lassen Sie die Option „SSL-Verbindung erzwingen“ aktiviert, um sicherzustellen, dass Daten während der Übertragung verschlüsselt werden
- Überprüfen Sie regelmäßig die Richtlinien von KMS und Secrets Manager: Stellen Sie sicher, dass nur autorisierte Dienste und Konten Zugriff auf Ihre Verschlüsselungsschlüssel und Geheimnisse haben
- Zugriff mit geringsten Rechten verwenden: Gewähren Sie Datenbankbenutzern nur die erforderlichen Mindestberechtigungen, die Amazon Connect Decisions für Verbindungen verwendet

## Konfiguration der Verbindung

- Verwenden Sie aussagekräftige Verbindungsnamen: Wählen Sie klare, aussagekräftige Namen, die auf die Umgebung und den Zweck hinweisen (z. B. „production-inventory-db“ statt „db1")
- Dokumentieren Sie Ihre Verbindungen: Verwenden Sie das Feld Beschreibung, um zu notieren, auf welche Daten die Verbindung zugreift, wem sie gehört und welche Besonderheiten zu beachten sind
- Testen Sie die Verbindungen, bevor Sie fortfahren: Stellen Sie immer sicher, dass Ihre Verbindung funktioniert, bevor Sie Tabellen auswählen und Aktualisierungszeitpläne konfigurieren
- Überprüfen Sie das JDBC-URL-Format: Double-check Ihre JDBC-URL-Syntax entspricht Ihrem Datenbanktyp, um Verbindungsfehler zu vermeiden

## Strategie zur Datenaktualisierung

- Wählen Sie den geeigneten Aktualisierungsrhythmus: Wählen Sie die Aktualisierungshäufigkeit auf der Grundlage der Häufigkeit der Änderungen Ihrer Quelldaten und Ihrer Geschäftsanforderungen
- Planen Sie Aktualisierungen in Zeiten geringer Aktivität: Konfigurieren Sie Aktualisierungszeiten, zu denen Ihre Datenbank weniger ausgelastet ist, um die Leistungseinbußen zu minimieren
- Verwenden Sie nach Möglichkeit inkrementelle Aktualisierungen: Bei großen Datensätzen mit häufigen Änderungen sind inkrementelle Aktualisierungen effizienter als vollständige Aktualisierungen
- Wählen Sie aussagekräftige Zeitstempelspalten aus: Wählen Sie bei inkrementellen Aktualisierungen Spalten aus, die genau wiedergeben, wann Datensätze erstellt oder geändert wurden

## Zur Problembehandlung mit dem Chat arbeiten

- Seien Sie bei Ihren Anfragen spezifisch: Geben Sie einen klaren Kontext an, wenn Sie um Hilfe bei der Behebung von Verbindungs- oder Zuordnungsproblemen bitten
- Fragen Sie nach Erläuterungen: Wenn Sie die Empfehlungen oder generierten SQL-Abfragen nicht verstehen, bitten Sie um Klarstellung
- Testen Sie alle SQL-Änderungen, bevor Sie sie akzeptieren: Verwenden Sie die Vorschaufunktion, um zu überprüfen, ob die Transformationen mit Ihren tatsächlichen Daten erwartungsgemäß funktionieren

- Nutzen Sie den Chat zur Problembehandlung: Wenn Verbindungen fehlschlagen oder bei Aktualisierungen Fehler auftreten, stellen Sie Diagnosefragen wie „Warum schlägt meine Verbindung fehl?“ oder „Hilf mir, diesen Aktualisierungsfehler zu verstehen“

### Laufende Wartung

- Überwachen Sie die Ausführung von Aktualisierungen regelmäßig: Überprüfen Sie die Registerkarten Ziele und Quellen in Data Management, um sicherzustellen, dass die Aktualisierungen erfolgreich abgeschlossen werden
- Fehler umgehend beheben: Wenn Amazon Connect Decisions Sie auffordert, Fehler zu aktualisieren, untersuchen und lösen Sie Probleme schnell, um Datenlücken zu vermeiden
- Anmeldeinformationen sicher aktualisieren: Wenn sich Datenbankkennwörter ändern, aktualisieren Sie sie in AWS Secrets Manager. Amazon Connect Decisions verwendet die neuen Anmeldeinformationen automatisch
- Dokumentieren Sie benutzerdefinierte Konfigurationen: Machen Sie sich Notizen zu speziellen Aktualisierungsplänen, Transformationslogik oder Verbindungsanforderungen als Referenz für Ihr Team
- Überprüfen Sie die Tabellenauswahl regelmäßig: Wenn sich Ihre Datenanforderungen ändern, überprüfen Sie erneut, welche Tabellen Sie aufnehmen und ob die Aktualisierungspläne immer noch den Geschäftsanforderungen entsprechen

## Das kanonische Datenmodell (CDM) verstehen

Das Canonical Data Model (CDM) ist die standardisierte Datenstruktur, die von verwendet wird. Wenn Sie Ihre Supply-Chain-Daten integrieren, müssen sie in das CDM-Format umgewandelt werden, damit sie für Planung, Prognose und betriebliche Erkenntnisse verarbeitet werden können.

In diesem Thema wird erklärt, was CDM ist, warum es wichtig ist und welche Dateneinheiten verfügbar sind.

### Was ist das CDM?

Das CDM definiert einen gemeinsamen Satz von Dateneinheiten und Feldern, die Konzepte der Lieferkette wie Produkte, Standorte, Bestellungen, Lieferungen und Inventar repräsentieren. Unabhängig vom Format oder der Struktur Ihrer Quelldaten bietet das CDM ein einziges, konsistentes Schema, das für alle seine Funktionen verwendet wird.

Beim Daten-Onboarding werden Ihre Quelldaten den CDM-Zieltabellen zugeordnet. Der Data Agent kann automatisch Zuordnungen zwischen Ihren Quellfeldern und CDM-Feldern vorschlagen und SQL-Transformationsabfragen zur Konvertierung Ihrer Daten generieren.

## Warum das CDM wichtig ist

- Konsistenz — Alle Funktionen basieren auf derselben Datenstruktur, wodurch ein einheitliches Verhalten bei der Bedarfsplanung, Bestandsoptimierung und Durchlaufzeiterfassung gewährleistet wird.
- Interoperabilität — Daten aus verschiedenen Quellsystemen (ERP, WMS, TMS) werden zu einem einzigen Modell normalisiert, was eine systemübergreifende Analyse ermöglicht.
- Vereinfachtes Onboarding — Der Data Agent verwendet das CDM als Zielschema bei der Generierung automatisierter Mappings, wodurch der manuelle Aufwand reduziert wird.
- Datenqualität — Validierungsprüfungen werden anhand von CDM-Definitionen durchgeführt, um Probleme zu erkennen, bevor die Daten in der Produktion verwendet werden.

## Kategorien von Datenentitäten

CDM-Dateneinheiten lassen sich in zwei Kategorien einteilen:

- Non-transactional Daten — Referenz- oder Stammdaten, die sich selten ändern, wie Produkte, Standorte, Handelspartner und Regionen.
- Transaktionsdaten — Betriebsdaten, die sich häufig ändern, wie Prognosen, Lagerbestände, Bestellungen und Lieferungen.

## Unterstützte Datenentitäten

In der folgenden Tabelle sind alle Datenentitäten aufgeführt, die im CDM unterstützt werden.

Unterstützte CDM-Datenentitäten

| Datenentität | Datentyp | Erforderlich |
|---|---|---|
| Unternehmen | Non-transactional Daten | Ja |
| Produkt | Non-transactional Daten | Ja |

| Datenentität | Datentyp | Erforderlich |
|---|---|---|
| Handelspartner | Non-transactional Daten | Ja |
| Produkt des Anbieters | Non-transactional Daten | Ja |
| Geografie | Non-transactional Daten | Ja |
| Produkthierarchie | Non-transactional Daten | Ja |
| Transportspur | Non-transactional Daten | Ja |
| Vorlaufzeit des Anbieters | Non-transactional Daten | Ja |
| Site | Non-transactional Daten | Ja |
| Feiertag für Verkäufer | Non-transactional Daten | Ja |
| Forecast | Transaktionsdaten | Ja |
| Bestand | Transaktionsdaten | Ja |
| Eingehende Bestellung () PO/STO | Transaktionsdaten | Ja |
| Position für ausgehende Bestellungen | Transaktionsdaten | Ja |
| Versand | Transaktionsdaten | Ja |
| Inventarpolitik | Transaktionsdaten | Ja |
| Zeile für eingehende Bestellungen () PO/STO | Transaktionsdaten | Ja |
| Ausgehender Versand | Transaktionsdaten | Ja |
| Zeitplan für eingehende Bestellungen | Transaktionsdaten | Ja |

# Je nach Funktion erforderliche Entitäten

Nicht für jedes Feature sind alle CDM-Entitäten erforderlich. In den folgenden Abschnitten wird beschrieben, welche Entitäten für jede Funktion erforderlich, optional oder nicht zutreffend sind.

## Sichtbarkeit des Inventars

CDM-Entitäten für die Sichtbarkeit des Inventars

| Datenentität | Datentyp | Erforderlich |
|---|---|---|
| Unternehmen | Non-transactional | Optional |
| Produkt | Non-transactional | Ja |
| Handelspartner | Non-transactional | Optional |
| Produkt des Anbieters | Non-transactional | Nicht zutreffend |
| Geografie | Non-transactional | Optional |
| Produkthierarchie | Non-transactional | Optional |
| Transportspur | Non-transactional | Optional |
| Vorlaufzeit des Anbieters | Non-transactional | Nicht zutreffend |
| Site | Non-transactional | Ja |
| Feiertag des Anbieters | Non-transactional | Nicht zutreffend |
| Forecast | Transaktional | Optional |
| Bestand | Transaktional | Ja |
| Eingehende Bestellung () PO/ STO | Transaktional | Optional |
| Position für ausgehende Bestellungen | Transaktional | Optional |
| Versand | Transaktional | Optional |

| Datenentität | Datentyp | Erforderlich |
|---|---|---|
| Inventarpolitik | Transaktional | Ja |
| Zeile für eingehende Bestellungen | Transaktional | Optional |
| Ausgehender Versand | Transaktional | Optional |
| Zeitplan für eingehende Bestellungen | Transaktional | Optional |

## Einblicke in die Vorlaufzeit

CDM-Einheiten für Einblicke in die Vorlaufzeit

| Datenentität | Datentyp | Erforderlich |
|---|---|---|
| Unternehmen | Non-transactional | Optional |
| Produkt | Non-transactional | Ja |
| Handelspartner | Non-transactional | Ja |
| Produkt des Anbieters | Non-transactional | Ja |
| Geografie | Non-transactional | Optional |
| Produkthierarchie | Non-transactional | Optional |
| Transportspur | Non-transactional | Ja |
| Vorlaufzeit des Anbieters | Non-transactional | Ja |
| Site | Non-transactional | Ja |
| Feiertag des Anbieters | Non-transactional | Optional |
| Forecast | Transaktional | Nicht zutreffend |
| Bestand | Transaktional | Nicht zutreffend |

| Datenentität | Datentyp | Erforderlich |
|---|---|---|
| Eingehende Bestellung () PO/ STO | Transaktional | Ja |
| Position für ausgehende Bestellungen | Transaktional | Nicht zutreffend |
| Versand | Transaktional | Ja |
| Inventarpolitik | Transaktional | Nicht zutreffend |
| Zeile für eingehende Bestellun gen | Transaktional | Ja |
| Ausgehender Versand | Transaktional | Nicht zutreffend |
| Zeitplan für eingehende Bestellungen | Transaktional | Ja |

## Planung der Nachfrage

### CDM-Einheiten für die Bedarfsplanung

| Datenentität | Datentyp | Erforderlich |
|---|---|---|
| Unternehmen | Non-transactional | Optional |
| Produkt | Non-transactional | Ja |
| Handelspartner | Non-transactional | Nicht zutreffend |
| Produkt des Anbieters | Non-transactional | Nicht zutreffend |
| Geografie | Non-transactional | Optional |
| Produkthierarchie | Non-transactional | Optional |
| Transportspur | Non-transactional | Nicht zutreffend |

| Datenentität | Datentyp | Erforderlich |
|---|---|---|
| Vorlaufzeit des Anbieters | Non-transactional | Nicht zutreffend |
| Site | Non-transactional | Ja |
| Feiertag des Anbieters | Non-transactional | Nicht zutreffend |
| Forecast | Transaktional | Nicht zutreffend |
| Bestand | Transaktional | Nicht zutreffend |
| Eingehende Bestellung () PO/ STO | Transaktional | Nicht zutreffend |
| Position für ausgehende Bestellungen | Transaktional | Ja |
| Versand | Transaktional | Nicht zutreffend |
| Inventarpolitik | Transaktional | Nicht zutreffend |
| Zeile für eingehende Bestellun gen | Transaktional | Nicht zutreffend |
| Ausgehender Versand | Transaktional | Nicht zutreffend |
| Zeitplan für eingehende Bestellungen | Transaktional | Nicht zutreffend |

## Wie bezieht sich das CDM auf das Onboarding von Daten

Wenn Sie Daten einbinden, folgt der Prozess diesen Schritten:

1. Upload — Sie laden Ihre Quelldaten als CSV-Dateien auf Amazon S3 hoch.
2. Karte — Der Data Agent analysiert Ihre Quelldatensätze und schlägt vor, welche CDM-Zieltabellen am besten zu Ihren Daten passen.
3. Transformieren — SQL-Transformationsabfragen konvertieren Ihr Quelldatenformat in das CDM-Format.

4. Validieren — Anhand der transformierten Daten werden Qualitätsprüfungen durchgeführt, um sicherzustellen, dass sie den CDM-Anforderungen entsprechen.
5. Aktivieren — Nach der Validierung fließen die Daten in Funktionen ein und stehen für diese zur Verfügung.

Eine schrittweise Anleitung zum Onboarding Ihrer Daten finden Sie im Thema Daten-Onboarding.

# Datenvalidierung und Qualitätsprüfungen

## -Übersicht

Die Datenvalidierung stellt sicher, dass Ihre Daten die Qualitätsanforderungen erfüllen, bevor die Funktionen von Amazon Connect Decisions ausgeführt werden. Das System validiert Daten auf der Grundlage Ihrer konfigurierten Pläne, Kennzahlen und Regeln, um Probleme zu identifizieren, die die Leistung blockieren oder beeinträchtigen könnten.

## So funktioniert die Datenvalidierung

### Auslöser für die Validierung

Die Datenvalidierung wird zu folgenden Zeiten automatisch ausgeführt:

- Änderungen der Insights-Konfiguration: Wenn Sie Metriken, Regeln oder andere Konfigurationen erstellen oder ändern
- Planerstellung: Wenn Sie einen Ad-hoc-Plan oder bei jeder geplanten Planausführung erstellen
- Datenaktualisierung: Nach jeder Datenaktualisierung werden Ihre Zielflüsse aktualisiert
- Ausführung von Fähigkeiten: Vor oder während des Einsatzes von KI-Teamkollegen (z. B. wenn ein Root eine Ausnahme verursacht oder Empfehlungen festgelegt werden)

### Arten der Validierung

Amazon Connect Decisions führt zwei Arten der Validierung durch:

Die Datenpräsenzvalidierung überprüft, ob die erforderlichen Datensätze und Felder auf der Grundlage Ihrer konfigurierten Ressourcen (Metriken, Regeln, Pläne) geladen wurden.

Bei der Validierung der Datenqualität wird anhand Ihrer Einrichtungskonfiguration überprüft, ob die bereitgestellten Daten die Qualitätsanforderungen erfüllen, einschließlich:

- Überprüfung der Einrichtungskriterien: Bestätigt, dass Produkte und Websites Ihren Regelkriterien entsprechen (z. B. Produktkategorien, Standorte der Standorte)
- Überprüfung der Hierarchie: Identifiziert fehlende hierarchische Beziehungen, wenn Sie in Ihrem Setup Hierarchien verwenden
- Gültigkeitsüberprüfung: Bestätigt, dass alle erforderlichen Daten für identifizierte Produkte und Standorte vorhanden sind
- Qualitätsbeurteilung: Bewertet die Datenqualität und Nutzbarkeit im Hinblick auf betriebliche Anforderungen

### Progressive Validierung

Amazon Connect Decisions ermöglicht Funktionen für Produkte und Websites mit gültigen Daten, anstatt Funktionen für Ihren gesamten Datensatz zu blockieren. Wenn Validierungsprobleme bestimmte Produkte oder Websites betreffen, verarbeitet das System weiterhin Produkte und Websites mit gültigen Daten, identifiziert Produkte oder Websites mit Datenproblemen und weist Sie auf die spezifischen Elemente hin, die Ihrer Aufmerksamkeit bedürfen. Auf diese Weise können Sie mit der Nutzung der Funktionen beginnen und gleichzeitig die verbleibenden Datenprobleme lösen.

## Auf Fehler bei der Datenüberprüfung zugreifen

Sie können Fehler bei der Datenüberprüfung über drei Einstiegspunkte anzeigen:

1. Metrik „Fehler bei der Datenvalidierung“ auf der Startseite
2. Themenkarte „Fehler bei der Datenvalidierung“ auf der Startseite
3. „Datenverwaltung“ in der linken Navigationsleiste **>** Registerkarte „Fehler“

## Überprüfung von Validierungsfehlern

Auf der Seite Fehler werden alle offenen und behobenen Validierungsfehler angezeigt. Sie können nach einer der folgenden Spalten suchen und filtern:

- ID: Eindeutiger Bezeichner für den Validierungsfehler
- Status
  - Öffnen: Der Fehler wurde nicht behoben
  - Behoben: Der Fehler wurde behoben und validiert
- Beschreibung: Erklärung des Datenqualitätsproblems

- Art des Problems
  - Fehlende erforderliche Daten: Es wurden keine obligatorischen Daten bereitgestellt, um einen Vorgang auszulösen (z. B. keine Quelltabelle outbound_order_line für den Versorgungsplan)
  - Ungültige Datenwerte: Daten sind vorhanden, enthalten aber falsche Werte (z. B. negative Produktkosten)
  - Fehlende Beziehungen: Erforderliche hierarchische Beziehungen oder Referenzbeziehungen fehlen (z. B. fehlende Produkthierarchien)
  - Unzureichende Daten: Es sind nicht genügend Daten verfügbar, um die erforderlichen Operationen durchzuführen (z. B. erfordert der Bedarfsplan historische Auftragsdaten von 12 Monaten, aber es sind nur 3 Monate vorhanden)
- Fähigkeit: Die betroffene Fähigkeit oder Ressource
  - Versorgungsplan
  - Nachfrageplan
  - Einblick (beinhaltet Ausnahmen, Empfehlungen und RCA für Angebot oder Nachfrage)
- Ziel: Betroffener Zielfluss
- Priorität
  - Kritisch: Mindestens eine Funktion ist vollständig blockiert und kann nicht ausgeführt werden
  - Hoch: Mindestens eine Funktion ist teilweise blockiert (einige Produkte oder Websites können nicht verarbeitet werden)
  - Mittel: Mindestens eine Funktion hat eine verringerte Genauigkeit (läuft, führt aber zu schlechteren Ergebnissen)
- Erstellt am: Zeitstempel, der anzeigt, wann der Fehler zum ersten Mal erkannt wurde

## Fehlerdetails anzeigen

Wählen Sie einen Fehler aus, um detaillierte Informationen anzuzeigen. Auf dem Detailbildschirm werden die oben genannten Informationen zusammen mit einem Zeitstempel, einer zugehörigen Ressource und einem Link (die Metrik, Regel oder der Plan, die die vom Problem betroffene Funktion darstellt) sowie eine Vorschau von bis zu 100 Zeilen mit betroffenen Daten angezeigt, die zeigen, wie sich der Datenvalidierungsfehler äußert.

### Verfügbare Aktionen

Auf dem Bildschirm mit den Fehlerdetails können Sie:

- Fehlerbehebung: Starten Sie den KI-Teamkollegen, der Sie bei der Problembehebung in natürlicher Sprache unterstützt und detaillierte Anleitungen zur Problembehebung erhält
- Fehler beheben: Markieren Sie den Fehler manuell als behoben, wenn Sie das zugrunde liegende Problem behoben haben
- Herunterladen: Laden Sie den vollständigen betroffenen Datensatz zur detaillierten Analyse und Korrektur herunter

# Behebung von Fehlern bei der Datenvalidierung

## Arbeitsablauf zur Problemlösung

1. Lesen Sie die Fehlerbeschreibung und die Priorität, um die Auswirkungen zu verstehen
2. Sehen Sie sich die Vorschau der betroffenen Daten an, um zu sehen, welche spezifischen Datensätze betroffen sind
3. Folgen Sie den spezifischen Empfehlungen zur Problembehebung
4. Wählen Sie eine geeignete Aktion aus:
   - Bei Konfigurationsproblemen: Arbeiten Sie mit Ihren Managern und Planern zusammen, um die Metrik-, Regel- oder Plankonfiguration anzupassen
   - Bei Zuordnungsproblemen: Korrigieren Sie hochgeladene Quelldaten oder aktualisieren Sie Datentransformationen und -zuordnungen
   - Bei fehlenden oder ungültigen Daten: Laden Sie die korrigierten Daten hoch
5. Markieren Sie den Fehler manuell als behoben, sobald Sie das zugrunde liegende Problem behoben haben

## Ich arbeite mit dem KI-Teamkollegen

Verwenden Sie die Option zur Fehlerbehebung, um Fragen wie „Auf welche Fehler sollte ich mich zuerst konzentrieren?“ zu stellen oder „Welche Fehler blockieren meinen Bedarfsplan?“ , erhalten ausführliche Erläuterungen zu dem Problem und seinen Auswirkungen, erhalten schrittweise Anleitungen zu Lösungsansätzen und erfahren, wie sich der Fehler auf Ihre spezifische Konfiguration auswirkt. Der KI-Teamkollege kann als Leitfaden zur Lösung des Problems in Amazon Connect Connect-Entscheidungen und in Ihren Quelldatensystemen dienen.

# Bewährte Methoden

- Priorisieren Sie nach Schweregrad: Konzentrieren Sie sich zunächst auf kritische Fehler, da diese die Ausführung von Funktionen vollständig blockieren. Behandeln Sie dann Fehler mit hoher Priorität, die die Verarbeitung teilweise blockieren, gefolgt von Problemen mit mittlerer Priorität, die die Genauigkeit beeinträchtigen.
- Lesen Sie die Empfehlungen sorgfältig durch: Jeder Fehler enthält spezifische, umsetzbare Anleitungen, die auf das Problem zugeschnitten sind und auf Ihre Konfiguration zugeschnitten sind.
- Nutzen Sie die progressive Validierung zu Ihrem Vorteil: Warten Sie nicht, bis Sie alle Fehler behoben haben, bevor Sie Funktionen nutzen. Das System aktiviert Funktionen für gültige Produkte und Websites, während Sie an der Lösung von Problemen für andere arbeiten.
- Überwachung nach Datenaktualisierungen: Suchen Sie nach jeder Datenaktualisierung nach neuen Validierungsfehlern, um Probleme frühzeitig zu erkennen, bevor sie sich auf Produktionsabläufe auswirken.
- Laden Sie betroffene Daten strategisch herunter: Verwenden Sie die Download-Option, wenn Sie alle betroffenen Datensätze über die Vorschau hinaus analysieren müssen oder wenn Sie Ihrem Datenteam den kompletten Datensatz zur Verfügung stellen müssen.
- Nutzen Sie den KI-Teamkollegen für komplexe Probleme: Die Option zur Fehlerbehebung bietet kontextuelle Unterstützung, die sich an Ihre spezifische Situation und Konfiguration anpasst.
- Überprüfen Sie die Lösung: Nachdem Sie die Datenprobleme behoben haben, markieren Sie Fehler manuell als behoben, um zu bestätigen, dass Ihre Korrektur erfolgreich war, und entfernen Sie sie aus der Liste „Öffnen“.

# Konfiguration des Systems

Die Einstellungen in Amazon Connect Decisions sind nach Umfang und Zielgruppe geordnet. Einige Einstellungen sind persönlich, sodass jeder Benutzer sein eigenes Erlebnis anpassen kann. Bei anderen handelt es sich um Konfigurationen auf Instanzebene, die von Administratoren verwaltet werden und sich darauf auswirken, wie sich das System für alle Benutzer verhält oder wie es sich mit Ihrer breiteren Technologieumgebung verbindet.

User-level Mithilfe von Einstellungen können Benutzer ihre Kontoinformationen und Benachrichtigungseinstellungen verwalten und festlegen, wie ihr Datenzugriffsbereich auf ihre Ansichten angewendet wird.

Instance-level Mithilfe von Einstellungen können Administratoren das Verhalten der Zugriffskontrollfilter im gesamten Unternehmen konfigurieren, Verbindungen zu Ihrem ERP und anderen externen Systemen herstellen und festlegen, wie das System mit empfohlenen Maßnahmen umgeht.

Zusammen geben diese Einstellungen Ihrem Unternehmen die Flexibilität, Amazon Connect Connect-Entscheidungen an Ihren spezifischen betrieblichen Kontext anzupassen und gleichzeitig die Konsistenz innerhalb Ihres Teams aufrechtzuerhalten.

# Einstellungen des Benutzerprofils

Benutzer können auf ihre Profileinstellungen zugreifen, indem sie ihren Namen in der oberen rechten Ecke der Anwendung auswählen und im Drop-down-Menü Profil auswählen. Auf der Profilseite können Benutzer ihre Kontoinformationen, Benachrichtigungseinstellungen und Datenzugriffseinstellungen verwalten.

## Zugreifen auf die Profileinstellungen

So greifen Sie auf Ihre Profileinstellungen zu:

1. Wähle deinen Namen in der oberen rechten Ecke der Seite
2. Wähle Profil aus dem Drop-down-Menü
3. Auf der Profilseite werden Ihre Kontoinformationen und Einstellungen angezeigt

# Informationen zum Profil

Auf der Profilseite werden die folgenden Kontodetails angezeigt:

Benutzer: Ihr Nutzername

Rolle: Ihre zugewiesene Rolle (Admin, Manager oder Planer)

Zeitzone: Wählen Sie Ihre bevorzugte Zeitzone aus dem Drop-down-Menü aus. Diese Einstellung bestimmt, wie Datum und Uhrzeit in Amazon Connect Connect-Entscheidungen angezeigt werden.

E-Mail: Ihre E-Mail-Adresse, die mit Ihrem Amazon Connect Decisions-Konto verknüpft ist

Erstellt: Datum und Uhrzeit der Erstellung Ihres Kontos

Aktualisiert: Datum und Uhrzeit der letzten Änderung Ihres Profils

Wählen Sie in der oberen rechten Ecke Speichern aus, um alle Änderungen an Ihren Profilinformationen zu speichern.

# Einstellungen für Benachrichtigungen

Auf der Registerkarte Benachrichtigungseinstellungen können Sie konfigurieren, wie Sie Benachrichtigungen für verschiedene Systemereignisse erhalten. Sie können wählen, ob Sie Benachrichtigungen in der Anwendung, per E-Mail oder beides erhalten möchten.

## Plans (Pläne)

Erfolgreiche Planerstellung: Wählen Sie aus, wie Sie benachrichtigt werden möchten, wenn die Planerstellung erfolgreich abgeschlossen wurde. Zu den Optionen gehören In-App-Benachrichtigungen und E-Mail-Benachrichtigungen.

Fehler bei der Plangenerierung: Wählen Sie aus, wie Sie benachrichtigt werden möchten, wenn die Planerstellung fehlschlägt. Zu den Optionen gehören In-App-Benachrichtigungen und E-Mail-Benachrichtigungen.

## Insights-Konfigurationen

Insights-Konfigurationen erfolgreich abgeschlossen: Wählen Sie aus, wie Sie benachrichtigt werden möchten, wenn die Insights-Konfiguration erfolgreich abgeschlossen wurde. Zu den Optionen gehören In-App-Benachrichtigungen.

Fehlgeschlagene Insights-Konfigurationen: Wählen Sie aus, wie Sie benachrichtigt werden möchten, wenn die Insights-Konfiguration fehlschlägt. Zu den Optionen gehören In-App-Benachrichtigungen.

### Datenaufnahme

Datenaufnahme fehlgeschlagen: Wählen Sie aus, wie Sie benachrichtigt werden möchten, wenn die Datenaufnahme fehlschlägt. Zu den Optionen gehören In-App-Benachrichtigungen und E-Mail-Benachrichtigungen.

### Admin-Einstellungen

Administratoren können systemweite Benachrichtigungseinstellungen konfigurieren, die für alle Benutzer gelten.

Aufbewahrung von Benachrichtigungen: Legen Sie die Anzahl der Tage fest, nach denen Benachrichtigungen automatisch aus dem System entfernt werden. Geben Sie einen numerischen Wert ein, um den Aufbewahrungszeitraum anzugeben.

Wählen Sie Speichern, um Ihre Benachrichtigungseinstellungen zu übernehmen.

## Zugewiesener Bereich

Auf der Registerkarte Zugewiesener Bereich werden Ihre Datenzugriffsberechtigungen angezeigt und Sie können konfigurieren, wie Datenansichten anhand des zugewiesenen Bereichs gefiltert werden.

### Datenzugriff

In diesem Abschnitt wird Ihre aktuelle Datenzugriffsebene angezeigt. Wenn Sie Zugriff auf alle Websites und Produkte haben, wird die Meldung „Sie haben Zugriff auf alle Websites und Produkte“ angezeigt.

### Standardansichtsfilter

Ansichten nach meinem zugewiesenen Bereich filtern: Wenn diese Option aktiviert ist, werden Datenansichten automatisch so gefiltert, dass nur Artikel innerhalb der von Ihnen zugewiesenen Produkte und Websites angezeigt werden. Schalten Sie diese Einstellung je nach Ihren Wünschen ein oder aus.

Wenn dieser Filter aktiviert ist, werden Ihnen nur Ausnahmen, Pläne und andere Daten angezeigt, die für Ihren zugewiesenen Bereich relevant sind. Wenn diese Option deaktiviert ist, werden je nach Ihren Rollenberechtigungen möglicherweise Daten außerhalb Ihres zugewiesenen Bereichs angezeigt.

Wählen Sie Speichern aus, um Ihre Filtereinstellungen anzuwenden.

# Zugriffskontrolle, Filter umschalten

Wie bereits erwähnt, können alle Benutzer alle Ausnahmen einsehen, unabhängig davon, ob sie die entsprechenden Produkte und Websites konfiguriert haben (für Mutationsaktionen ist weiterhin der entsprechende Zugriff erforderlich). Dies erleichtert zwar den Wissensaustausch, Benutzer, die sich nur auf bestimmte Produkte und Websites konzentrieren, können jedoch mit Ausnahmen oder Empfehlungen für andere Produkte und Websites überfordert werden. Um Benutzern zu helfen, sich auf die Ausnahmen und Empfehlungen zu konzentrieren, die für sie wichtig sind, können sie den Schalter für die Zugriffsansicht wie folgt verwenden:

- Zunächst muss ein Benutzer mit der Rolle „Admin“ die Funktion auf dieser Instanz aktivieren. Navigieren Sie von der linken Navigationsleiste zur Seite mit den Instanzeinstellungen
- Standardmäßig wird ihnen ein Schalter angezeigt, mit dem der Standardfilter für die Zugriffsansicht für die gesamte Instanz festgelegt wird. Der „Administrator“ kann sich entweder dafür entscheiden, eine einheitliche Einstellung für alle Benutzer in der Instanz zu verwenden, oder die Benutzer selbst über ihre Präferenzen entscheiden lassen
- Wenn er die Einstellung zum Umschalten der Ansicht mit einheitlichem Zugriff wählt, kann der „Administrator“ auch entscheiden, ob der Umschalter für alle Benutzer aktiviert oder deaktiviert werden soll
- Wenn er sich dafür entscheidet, dass jeder Benutzer seine eigenen Einstellungen wählen kann, hat jeder Benutzer die Möglichkeit, den Filter für die Zugriffsansicht für sich selbst umzuschalten. Jeder Benutzer kann über das Drop-down-Menü „Benutzer“ in der oberen rechten Ecke des Bildschirms zur Seite mit den Benutzereinstellungen navigieren

## Ändern Sie den Schalter für die Zugriffskontrolle für Ihre Instanz:

1. Wählen Sie auf der linken Seite die Menüleiste „Einstellungen“
2. Wählen Sie Anwendung
3. Aktualisieren Sie den Schalter und klicken Sie auf Einstellungen speichern

Wenn die Einstellung aktiviert ist, filtert das System automatisch Ausnahmen und Empfehlungen, sodass nur die Seiten angezeigt werden, die für ein Produkt ODER eine Website generiert wurden, die der Konfiguration für die Zugriffskontrolle entsprechen

Für Benutzer, für die die Option „Vollzugriff auf alle Produkte und Websites gewähren“ aktiviert ist, werden beim Umschalten der Zugriffsansicht weiterhin alle Ausnahmen und Empfehlungen angezeigt. Wenn ein Benutzer diesen Schalter deaktiviert hat, aber keine Produkte oder Websites konfiguriert hat, interpretiert das System dies so, als ob er Zugriff auf kein Produkt und keine Website hat, sodass dem Benutzer nichts angezeigt wird

Der Zugriffsansichtsfilter wird als ein anderer Filtertyp betrachtet und wird daher nicht in den Filterchips auf der Ausnahme- und Empfehlungsseite angezeigt. Benutzer können weiterhin auf die gleiche Weise wie zuvor andere Filter anwenden, einschließlich anderer Produkt- und Seitenfilter

Benutzer können weiterhin auf Ausnahmen und Empfehlungen für andere Produkte ODER Websites zugreifen, wenn sie den Schalter für die Zugriffsansicht deaktivieren oder wenn sie den direkten Hyperlink zu ihnen haben

# Verbindungen zu Ihrem ERP konfigurieren

Damit Amazon Connect Decisions in Ihrem Namen Operationen in Ihrem Enterprise Resource Planning (ERP) -System ausführen kann, müssen Sie eine Verbindung konfigurieren, die die erforderlichen Verbindungsparameter und die Anmeldeinformationen angibt, die Amazon Connect Decisions während des Vorgangs verwenden soll.

Unterstützte ERP-Systeme:

- SAP S/4HANA

## Konfigurieren Sie die Anmeldeinformationen in Secrets Manager

1. Verwenden Sie Ihr Konto und verwenden Sie Secrets Manager, um ein Secrets Manager Manager-Geheimnis zu erstellen
   - Wenn Sie die Anmeldeinformationen in Secrets Manager eingeben, ersetzen Sie die Platzhalterwerte unten (<username>und<password>) durch den tatsächlichen Benutzernamen und das Passwort, die Amazon Connect Decisions verwenden soll
   - Wenn Sie die Konsole verwenden, wählen Sie `Other type of secret` für `Secret Type`
   - Wenn Sie die Details über die `Key/value pairs` Registerkarte in der Konsole eingeben, geben Sie 2 Paare ein:
     - Schlüssel:`username`; Wert: <*username*>
     - Schlüssel:`password`; Wert: <*password*>

- Wenn Sie die `Plaintext` Registerkarte verwenden, um das Geheimnis in der Konsole einzugeben, geben Sie ein JSON-Objekt mit den beiden Paaren ein:

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

2. Verschlüsseln Sie Ihr Geheimnis mit einem AWS KMS-Schlüssel. Notieren Sie sich die ID des Schlüssels, da Sie sie in den nachfolgenden Schritten benötigen
3. Notieren Sie sich nach der Erstellung Ihres Geheimnisses seinen Amazon-Ressourcennamen (ARN), da Sie ihn in den nachfolgenden Schritten benötigen
   - z. B.: `arn:aws:secretsmanager:<Region>:<AccountId>:secret:<SecretName>-<SixRandomCharacters>`

## Konfigurieren Sie die Berechtigungen für den KMS-Schlüssel

Sie müssen die erforderlichen Berechtigungen bereitstellen, damit Amazon Connect Decisions darauf zugreifen und es verwenden kann.

1. Aktualisieren Sie Ihre KMS-Richtlinie, damit Amazon Connect Decisions über die Instance-Rolle auf Ihren Schlüssel zugreifen kann
   - Hinweis: Ersetzen Sie `<YourAccountNumber>` und `<YourInstanceID>` durch Ihr AWS Konto und Ihre Amazon Connect Decisions-Instance-ID.

```
{
    "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. Aktualisieren Sie die Inline-Richtlinie für Ihre Instance-Rolle, um die Berechtigung für den Schlüssel zu erteilen
   - Hinweis: Ersetzen <YourSecretArn> Sie <YourAccountNumber> und <YourInstanceID> durch Ihren geheimen ARN, Ihr AWS Konto und Ihre AWS Supply Chain Instance-ID.

```
{
    "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"
        }
    ]
}
```

## Aktualisieren Sie die Secrets Manager Manager-Ressourcenrichtlinie für Ihr Secret

1. Aktualisieren Sie die Secrets Manager Manager-Ressourcenrichtlinie für Ihr Secret
   - Hinweis: Ersetze es <YourSecretArn> durch den ARN deines Secrets

```
{
   "Version":"2012-10-17",
   "Statement":[
```

```
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"scn.amazonaws.com"
         },
         "Action":[
            "secretsmanager:GetSecretValue",
            "secretsmanager:DescribeSecret"
         ],
         "Resource":"YourSecretArn"
      }
   ]
}
```

## Konfiguration der Amazon Connect Decisions-Verbindung

1. Navigieren Sie in Ihrer Instanz von Amazon Connect Decisions zur Datenverwaltungsseite
2. Wählen Sie die `Connections` Registerkarte
3. Klicken Sie auf die Schaltfläche `Create Connection`.
4. Klicken Sie auf der `Create Connector` Seite auf die `Select` Schaltfläche in der Zeile für den `SAP S/4HANA` Steckertyp
5. Geben Sie `Configure SAP S/4HANA API Connector` auf der Seite die erforderlichen Informationen ein:
   - `Connection Name`: eindeutiger Verbindungsname
   - `API Endpoint URL`: die OData-API-Endpunkt-URL Ihrer S/4HANA SAP-Instanz (z. B.:`https://<hostname>:<port>`)
   - `Client Number`: die dreistellige SAP-Kundennummer (z. B.:) `100`
   - `Secret ARN`: der Amazon-Ressourcenname (ARN) des Secrets in Secrets Manager, in dem die von Amazon Connect Decisions zu verwendenden Anmeldeinformationen gespeichert sind
6. Klicken Sie auf die `Create Connector` Schaltfläche

# Aktionseinstellungen konfigurieren

Mit Amazon Connect Decisions können Sie steuern, für welche Aktionstypen es anbieten soll, um in Ihrem Namen Operationen in Ihrem Enterprise Resource Planning (ERP) -System durchzuführen.

Standardmäßig sind alle Aktionstypen deaktiviert, und Sie müssen diese Funktion für jeden gewünschten Aktionstyp aktivieren.

> **Note**
>
> Durch die Aktivierung der Unterstützung für einen bestimmten Aktionstyp wird gesteuert, ob die Option, dass Amazon Connect Decisions die Aktion in Ihrem Namen durchführt, im gesamten System angezeigt wird (z. B. bei der Überprüfung eines Insights mit einer Empfehlung des angegebenen Typs). Amazon Connect Decisions führt diese Aktionen erst durch (auch wenn der Support aktiviert ist), wenn Sie die spezifische Empfehlung akzeptieren.

Unterstützte Aktionstypen:

- Bestellung erstellen
- Bestellung aktualisieren
- Bestellung stornieren

Konfigurieren Sie die Aktionsunterstützung für jeden Aktionstyp:

1. Navigieren Sie in Ihrer Instanz von Amazon Connect Decisions zur Datenverwaltungsseite
2. Wählen Sie die `Actions` Registerkarte
3. Suchen Sie in der Liste nach dem Aktionstyp, den Sie konfigurieren möchten
4. Um die Unterstützung für den Aktionstyp zu aktivieren:
   - Wählen Sie eine der Verbindungen aus, die im Dropdownmenü für diesen Aktionstyp aufgeführt sind
   - Hinweis: In der Dropdownliste werden nur die verfügbaren Verbindungen angezeigt, für die ein Typ konfiguriert wurde, der die `Actions` Funktion unterstützt (z. B.:) `SAP S/4HANA`
5. Um die Unterstützung für den Aktionstyp zu deaktivieren:
   - Wählen Sie `No connection` im Dropdownmenü diesen Aktionstyp aus
6. Klicken Sie hier`Save`, um Ihre Änderungen zu speichern

# Sicherheit

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Third-party Auditoren testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheit im Rahmen der AWS-Compliance-Programme. Weitere Informationen zu den Compliance-Programmen, die für Amazon Connect Connect-Entscheidungen gelten, finden Sie unter AWS-Services in Umfang nach Compliance-Programmen.
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation zeigt Ihnen, wie Sie das Modell der geteilten Verantwortung bei der Verwendung von Amazon Connect einsetzen können. In den folgenden Themen erfahren Sie, wie Sie Amazon Connect Decisions konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen.

# Datenschutz

Das Modell der AWS gemeinsamen Verantwortung gilt für den Datenschutz in Amazon Connect Connect-Entscheidungen. AWS Ist, wie in diesem Modell beschrieben, für den Schutz der globalen Infrastruktur verantwortlich, auf der die gesamte AWS Cloud läuft. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben der von Ihnen verwendeten AWS Dienste verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im AWS Shared Responsibility Model und im DSGVO-Blogbeitrag im AWS-Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, die AWS Kontoanmeldedaten zu schützen und einzelne Benutzer mit AWS Identity and Access Management (IAM) einzurichten. So erhält jeder Benutzer nur

die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem sollten Sie die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir empfehlen TLS 1.2 oder höher.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen innerhalb der AWS Dienste.
- Verwenden Sie fortschrittliche verwaltete Sicherheitsdienste wie Amazon Macie, die Sie bei der Erkennung und Sicherung sensibler Daten unterstützen, die in Amazon Simple Storage Service gespeichert sind.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Tags oder Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Amazon Connect Decisions oder anderen AWS Services über die AWS Management Console, API, AWS Command Line Interface (AWS CLI) oder AWS SDKs arbeiten. Alle Daten, die Sie in Tags oder frei formatierte Textfelder für Namen eingeben, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden.

## Datenverschlüsselung

Dieses Thema enthält spezifische Informationen zu Amazon Connect Connect-Entscheidungen zur Verschlüsselung bei der Übertragung und Verschlüsselung im Ruhezustand.

### Verschlüsselung während der Übertragung

Die gesamte Kommunikation zwischen Kunden und Amazon Connect Decisions sowie zwischen Amazon Connect Decisions und seinen nachgelagerten Abhängigkeiten ist durch Verbindungen mit TLS 1.2 oder höher geschützt.

### Verschlüsselung im Ruhezustand

Amazon Connect Decisions speichert Daten im Ruhezustand mithilfe von DynamoDB und Amazon Simple Storage Service (Amazon S3). Die ruhenden Daten werden standardmäßig mithilfe von AWS Verschlüsselungslösungen verschlüsselt. Amazon Connect Decisions verschlüsselt Ihre Daten mit AWS eigenen Verschlüsselungsschlüsseln von AWS Key Management Service (AWS KMS). Sie müssen keine Maßnahmen ergreifen, um die AWS verwalteten Schlüssel, die Ihre Daten verschlüsseln, zu schützen. Weitere Informationen finden Sie unter AWS-eigene Schlüssel im AWS KMS Entwicklerhandbuch.

Wenn Sie den KMS-Schlüssel, der zum Verschlüsseln von Daten auf Ihrer Amazon Connect Decisions-Instance verwendet wird, in der AWS Konsole ändern, müssen Sie eine neue Instance erstellen, um mit dem neuen Schlüssel Ihre Daten zu verschlüsseln. Alle Daten, die mit dem vorherigen Schlüssel verschlüsselt wurden, werden nicht beibehalten, und nur Daten werden mit dem aktualisierten Schlüssel verschlüsselt. Wenn Sie Ihre Daten aus einer früheren Verschlüsselungsmethode beibehalten möchten, können Sie zu dem Schlüssel zurückkehren, den Sie während dieser Konversationen verwendet haben.

Ihre Konversationen mit Amazon Connect Decisions in der Webapp und in Chat-Anwendungen werden nur mit AWS-owned Schlüsseln verschlüsselt.

## Cross-region Verarbeitung

Amazon Connect Decisions wird von Amazon Bedrock unterstützt und verwendet Cross-Region-Inference (CRIS), um den Traffic auf verschiedene AWS Regionen zu verteilen und so die Leistung und Zuverlässigkeit von Large Language Model (LLM) -Inferenzen zu verbessern. Regionsübergreifende Inferenz bietet folgende Vorteile:

- Höherer Durchsatz und größere Stabilität in Zeiten hoher Nachfrage
- Verbesserte Leistung
- Zugriff auf die neu eingeführten Funktionen und Funktionen von Amazon Connect Decisions, die auf den leistungsstärksten LLMs basieren, die auf Amazon Bedrock gehostet werden

Cross-region Die Inferenzierung funktioniert je nach AWS Region, in der Ihre Amazon Connect Decisions-Instance erstellt wurde, unterschiedlich.

Für alle Instances, die in der geografischen Region USA erstellt wurden, verwendet Amazon Connect Decisions Global CRIS. Das bedeutet, dass Inferenzanfragen an unterstützte kommerzielle AWS

Regionen weltweit weitergeleitet werden, wodurch die verfügbaren Ressourcen optimiert und ein höherer Modelldurchsatz ermöglicht wird. Weitere Informationen zu Global CRIS finden Sie im Amazon Bedrock-Benutzerhandbuch.

Für alle Instances, die in der geografischen Region EU erstellt wurden, verwendet Amazon Connect Decisions Geographic CRIS. Das bedeutet, dass Inferenzanfragen in den AWS Regionen aufbewahrt werden, die Teil der Region sind, in der sich die Daten ursprünglich befinden. Weitere Informationen zu Geographic CRIS finden Sie im Amazon Bedrock-Benutzerhandbuch.

Beispielsweise kann eine Anfrage von einer Amazon Connect Decisions-Instance, die in der Region USA Ost (Nord-Virginia) (us-east-1) erstellt wurde, an jede AWS Region weltweit weitergeleitet werden, z. B. Asien-Pazifik (Sydney) (ap-southeast-2). Eine Anfrage von einer Amazon Connect Decisions-Instance, die in der Region Europa (Irland) (eu-west-1) erstellt wurde, wird jedoch an eine AWS Region innerhalb der EU wie Europa (Frankfurt) (eu-central-1) weitergeleitet. Weitere Informationen finden Sie unter Unterstützte Regionen für Amazon Connect Connect-Entscheidungen.

Regionsübergreifende Inferenzen ändern zwar nicht, wo Ihre Daten gespeichert werden, aber Ihre Anfragen und Ausgabeergebnisse können sich außerhalb der Region bewegen, in der sich die Daten ursprünglich befinden. Alle Daten werden bei der Übertragung über das sichere Netzwerk von Amazon verschlüsselt. Für die Nutzung von regionsübergreifender Inferenz fallen keine zusätzlichen Kosten an. Informationen darüber, wo Daten gespeichert werden, wenn Sie Amazon Connect Decisions verwenden, finden Sie unter Datenschutz in Amazon Connect Decisions.

# Entscheidungen über IAM für Amazon Connect

AWS Identity and Access Management (IAM) ist ein AWS-Service, der es einem Administrator ermöglicht, den Zugriff auf AWS-Ressourcen sicher zu steuern. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um die Ressourcen von Amazon Connect Decisions zu nutzen. IAM ist ein AWS-Service, die Sie ohne zusätzliche Kosten verwenden können.

## Wie funktioniert IAM mit Amazon Connect Decisions

Bevor Sie IAM verwenden, um den Zugriff auf Amazon Connect Decisions zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen für Amazon Connect Decisions verfügbar sind. Einen umfassenden Überblick darüber, wie Amazon Connect Decisions und andere AWS Services mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS-Services, die mit IAM funktionieren.

## Identity-based Richtlinien für Amazon Connect Connect-Entscheidungen

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identity-based Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität anhängen können, z. B. an einen IAM-Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

## Resource-based Richtlinien innerhalb von Amazon Connect Connect-Entscheidungen

Unterstützt ressourcenbasierte Richtlinien: Nein

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

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

## Politische Maßnahmen für Amazon Connect Connect-Entscheidungen

Unterstützt Richtlinienaktionen: Ja

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

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs zu erteilen.

Richtlinienaktionen in Amazon Connect Connect-Entscheidungen verwenden das folgende Präfix vor der Aktion:

```
scn
```

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

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

## Richtlinienressourcen für Amazon Connect Connect-Entscheidungen

Unterstützt Richtlinienressourcen: Ja

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

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Als Best Practice geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

## Schlüssel zu den Richtlinienbedingungen für Amazon Connect Connect-Entscheidungen

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

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

Das Element `Condition` gibt an, wann Anweisungen auf der Grundlage definierter Kriterien ausgeführt werden. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter AWS-Kontextschlüssel für globale Bedingungen im IAM-Benutzerhandbuch.

## Temporäre Anmeldeinformationen mit Amazon Connect Decisions verwenden

Unterstützt temporäre Anmeldeinformationen: Ja

Temporäre Anmeldeinformationen ermöglichen kurzfristigen Zugriff auf AWS Ressourcen und werden automatisch erstellt, wenn Sie den Verbund verwenden oder die Rollen wechseln. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldedaten in IAM - und AWS-Services, die mit IAM funktionieren, im IAM-Benutzerhandbuch.

## Zugriffssitzungen für Amazon Connect Connect-Entscheidungen weiterleiten

Unterstützt Forward Access Sessions (FAS): Ja

Forward-Access-Sitzungen (FAS) verwenden die Berechtigungen des Prinzipals, der einen AWS Service aufruft, in Kombination mit dem anfragenden AWS Service, um Anfragen an nachgelagerte Dienste zu stellen. Einzelheiten zu den Richtlinien für FAS-Anforderungen finden Sie unter Zugriffssitzungen weiterleiten.

## Servicerollen für Amazon Connect Connect-Entscheidungen

Unterstützt Servicerollen: Ja

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

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle kann die Funktionalität von Amazon Connect Decisions beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn Amazon Connect Decisions Sie dazu anleitet.

## Identity-based Beispiele für Richtlinien

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

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

### IAM-Richtlinie für die Instanzverwaltung

Im Folgenden finden Sie die IAM-Richtlinie, die zum Erstellen, Aktualisieren oder Löschen von Instanzen über die Konsole oder die öffentliche API erforderlich ist (ausgenommen sind alle Webapp-Operationen).

```
{
    "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"
        }
    ]
}
```

## Best Practices für Richtlinien

Identity-based Richtlinien legen fest, ob jemand Amazon Connect Decisions-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder diese löschen kann. Dies kann zusätzliche Kosten für Ihr AWS -Konto verursachen. Wenn Sie identitätsbasierte Richtlinien erstellen oder bearbeiten, befolgen Sie diese Richtlinien und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die verwalteten AWS-Richtlinien, die Berechtigungen

für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem AWS -Konto verfügbar. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete AWS -Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS-verwaltete Richtlinien oder AWS-verwaltete Richtlinien für Jobfunktionen im IAM-Benutzerhandbuch.

- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese über einen bestimmten AWS Service genutzt werden, z. B. CloudFormation Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.
- Anforderung einer Multi-Faktor-Authentifizierung (MFA) – Wenn Sie ein Szenario haben, das IAM-Benutzer oder Root-Benutzer in Ihrem AWS -Konto erfordert, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

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

# Fehlersuche bei IAM

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Amazon Connect Decisions und IAM auftreten können.

## Ich bin nicht berechtigt, eine Aktion in Amazon Connect Decisions durchzuführen

Wenn Sie in der AWS Management-Konsole nicht berechtigt sind, eine Aktion durchzuführen, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator ist die Person, die Ihnen Ihren Benutzernamen und Ihr Passwort zur Verfügung gestellt hat.

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

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

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

## Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion durchzuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Amazon Connect Decisions übergeben können.

Bei einigen AWS Diensten können Sie eine bestehende Rolle an diesen Service übergeben, anstatt eine neue Servicerolle oder eine dienstbezogene Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Amazon Connect Decisions auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

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

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

### Ich möchte Personen außerhalb meines AWS Konto für den Zugriff auf meine Amazon Connect Decisions-Ressourcen

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

Weitere Informationen dazu finden Sie hier:

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

## Third-party Unterauftragsverarbeiter

Amazon Connect Decisions verwendet Boomi, eine Drittanbieter-API, damit in Ihrem Namen Maßnahmen in externen Systemen ergriffen werden können. Wenn Sie eine Funktion von Amazon Connect Decisions verwenden, die eine Verbindung zu Ihren Drittanbietersystemen herstellt,

autorisieren Sie uns, Boomi als unsere Integrations-Middleware für die Übertragung und Verarbeitung Ihrer verschlüsselten Daten zu verwenden. Ihre Daten werden nicht separat in Boomi gespeichert.

Weitere Informationen über Boomi und seine Funktionsweise finden Sie in der öffentlichen Dokumentation von Boomi.

# Unterstützte Regionen

Auf dieser Seite werden die AWS Regionen beschrieben, in denen Sie Amazon Connect Decisions verwenden können. Weitere Informationen zu AWS Regionen finden Sie im Referenzhandbuch zur Kontoverwaltung unter „Geben Sie an, welche AWS Regionen Ihr AWS Konto verwenden kann“.

Ihre Daten werden möglicherweise in einer anderen Region als der Region verarbeitet, in der Sie Amazon Connect Decisions verwenden. Informationen zur regionsübergreifenden Verarbeitung in Amazon Connect Connect-Entscheidungen finden Sie unter Cross-region Verarbeitung. Informationen darüber, wo Daten während der Verarbeitung gespeichert werden, finden Sie unter Datenschutz.

## Unterstützte Regionen

Amazon Connect Decisions ist in den folgenden AWS Regionen in der AWS Management AWS Console, der mobilen Konsolenanwendung, AWS der Website und der AWS Dokumentationswebsite verfügbar. Diese Regionen sind standardmäßig aktiviert, sodass Sie sie vor der Verwendung nicht aktivieren müssen. Weitere Informationen erhalten Sie unter Regionen, die standardmäßig aktiviert sind.

Sie verwenden Amazon Connect Decisions in den folgenden Regionen.

| AWS Name der Region | Codename | Geografie (USA, EU usw.) |
|---|---|---|
| USA Ost (Nord-Virginia) | us-east-1 | US |
| Europa (Irland) | eu-west-1 | EU |

# Fehlerbehebung

Wenn bei der Einrichtung oder der täglichen Nutzung von Amazon Connect Decisions Probleme auftreten, finden Sie in diesem Abschnitt Anleitungen zur Diagnose und Lösung der häufigsten Probleme. Identifizieren Sie zunächst die Kategorie, die dem aufgetretenen Problem am besten entspricht, und folgen Sie dann den Schritten zur Fehlerbehebung auf der entsprechenden Seite. Wenn Sie sich nicht sicher sind, welche Kategorie zutrifft, beginnen Sie mit „Allgemeine Probleme bei der Installation“, die das breiteste Spektrum an Problemen bei der Erstkonfiguration abdeckt.

## Allgemeine Probleme bei der Installation

### Fehler bei der referenziellen Integrität: „Die Werte von product_id stimmen mit keiner ID im Produktdatensatz überein“

Die häufigste Ursache sind Leerzeichen am Ende in ID-Feldern. Quellsysteme, die aus Datenbanken mit fester Breite exportieren, füllen Zeichenkettenfelder häufig mit Leerzeichen auf. Der Produktmaster hat möglicherweise leere IDs („MAT604"), während die Bestellzeilendatei aufgefüllte IDs („MAT604“) hat. Das System führt einen strikten Zeichenfolgenabgleich durch, sodass diese nicht zusammengefügt werden können.

Behebung: Fügen Sie TRIM () zu allen Zeichenketten-ID-Feldern in Ihren Datenfluss-SQL-Transformationen hinzu. Wenden Sie es auf product_id, ship_from_site_id, customer_tpartner_id und jeden anderen Join-Schlüssel an. Prüfen Sie auch, ob es zwischen den Dateien Inkonsistenzen bei der Angabe von Anführungszeichen gibt. Verwenden Sie beim erneuten Exportieren von CSVs QUOTE_ALL, um Typinferenzprobleme zu vermeiden, bei denen numerisch aussehende IDs (z. B. „111613") in einer Datei als Ganzzahlen und in einer anderen als Zeichenketten behandelt werden.

Prävention: Standardmäßig werden alle ID-Felder in Ihren SQL-Transformationen immer TRIM gekürzt, auch wenn Sie das Problem heute nicht sehen. Quelldaten können sich zwischen Exporten ändern.

### Produkte in der Bestellhistorie fehlen im Produktmaster

Ihre Bestellhistorie enthält häufig Produkte, die nicht im aktuellen Produktmaster enthalten sind (Auslaufprodukte, Einmalartikel, Test-SKUs). Das System lehnt die gesamte Bestelldatei ab, wenn für eine Product_ID kein passender Produktstammdatensatz vorhanden ist.

Lösung: Erstellen Sie entweder (a) Stubzeilen im Produktmaster für fehlende Produkte mit minimalen Pflichtfeldern (id, description, base_uom), oder (b) filtern Sie die Bestellhistorie so, dass sie nur Produkte enthält, die im Produktmaster vorhanden sind. Option (a) wird bevorzugt, da sie den Nachfrageverlauf beibehält, der für die Herkunfts- und Trenderkennung nützlich sein kann.

## Fehler bei der CSV-Analyse beim Upload des Produktmasters

Produktbeschreibungen, die Kommas, Anführungszeichen oder Sonderzeichen enthalten, können die CSV-Analyse unterbrechen. Möglicherweise werden in bestimmten Zeilen Fehler wie „17 Felder erwartet, 19 wurden gefunden“ angezeigt.

Fix: Re-export Die Datei mit den richtigen Anführungszeichen (QUOTE_ALL). Überprüfen Sie die spezifischen fehlerhaften Zeilen auf eingebettete Kommas in den Beschreibungsfeldern.

## Daten werden nach dem Upload nicht angezeigt

- Stellen Sie sicher, dass sich Ihr Dateiformat nicht geändert hat (Erweiterung, Spaltenüberschriften, Kodierung).
- Vergewissern Sie sich, dass die Dateinamen und Erweiterungen dem erwarteten Muster entsprechen. Wenn Sie „.csv“ in „.csv000“ oder etwas Ähnliches umbenennen, wird die Aufnahme unterbrochen.
- Warten Sie bis zu 30 Minuten, bis die Datenaufnahme nach dem Upload abgeschlossen ist.
- Wenn sich die Spaltenüberschriften zwischen den Ladevorgängen ändern (z. B. Spalten, die nach benannt sind month/year), ist vor dem Hochladen ein Vorverarbeitungsschritt erforderlich.

## PIV wird nach der Datenaktualisierung nicht aktualisiert

- PIV wird etwa 15 Minuten nach Abschluss der Aufnahme ausgelöst und die Ausführung dauert etwa 20 bis 30 Minuten.
- End-to-end vom Datenupload bis zum neuen PIV: ca. 1—1,5 Stunden.
- Wenn PIV innerhalb von mehr als 24 Stunden nicht aktualisiert wurde, wenden Sie sich an den Support.

## Die Anzahl der Ausnahmen scheint zu hoch oder zu niedrig

- Zu hoch: Der Schwellenwert ist möglicherweise zu locker, oder ein einzelnes Produkt+eine einzelne Website generiert möglicherweise mehrere Ausnahmen für unterschiedliche Daten. Wenden Sie sich an den Support, um die Regelkonfiguration zu überprüfen.
- Zu niedrig: Der Schwellenwert ist möglicherweise zu restriktiv, oder für einige Produkte fehlen erforderliche Daten (z. B. Prognosen, Lagerbestände).

Spot-check einige Produkte, die Sie gut kennen, und vergleichen Sie, was das System anzeigt, mit denen Ihres Quellsystems.

## Keine finanziellen Auswirkungen, keine Ausnahmen

Finanzielle Auswirkungen erfordern, dass die Stückkosten in den Produktdaten angegeben werden. Wenn die Kosten für ein Produkt fehlen oder Null sind, wird kein Dollarwert angezeigt. Erkundigen Sie sich bei Ihrem Support-Team nach der Deckung der Kostendaten. Ein Wasserfall-Ansatz, der mehrere Kostenfelder umfasst, bietet in der Regel die beste Abdeckung.

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