aws

Guide de l’administrateur

Décisions relatives à Amazon Connect

Décisions relatives à Amazon Connect: Guide de l’administrateur

Table of Contents

Qu'est-ce qu'Amazon Connect Decisions

Amazon Connect Decisions est une solution de planification et d'intelligence de la chaîne d'approvisionnement qui fait appel à des équipes d'intelligence artificielle qui travaillent aux côtés de votre équipe pour harmoniser les signaux de demande en prévisions consensuelles, générer des plans d'approvisionnement tenant compte des contraintes et surveillant activement vos opérations afin de prévenir les problèmes, de les résoudre et d'identifier les causes profondes d'une amélioration continue.

Les équipes d'IA s'adaptent à votre façon de travailler : elles sont guidées par vos procédures et règles opérationnelles, s'intègrent à vos systèmes existants et tirent les leçons des décisions de vos praticiens. Il s'appuie sur l'expertise d'Amazon en matière de chaîne d'approvisionnement pour proposer des plans et des recommandations efficaces dès le premier jour.

Vous dirigez une équipe d'agents IA chargés de la coordination et de l'exécution des actions, ce qui vous permet de vous concentrer sur les décisions stratégiques qui améliorent les niveaux de service et l'efficacité du fonds de roulement.

Avantages

Adaptez-vous à votre entreprise

Les équipes d'IA s'adaptent à votre activité, à vos systèmes et à vos décisions, transformant rapidement vos flux de travail existants. Sur la base de vos procédures opérationnelles et de vos règles commerciales, vos collègues travaillent avec vos systèmes de planification et ERP existants. Ils tirent les leçons des décisions des planificateurs, s'alignent sur vos priorités et institutionnalisent les connaissances afin que vos opérations s'améliorent au fil du temps et que chaque membre de l'équipe soit plus efficace.

Gardez une longueur d'avance sur ce qui vous attend

Dirigez une équipe d'agents d'intelligence artificielle chargée du travail de coordination, en 24/7 harmonisant les signaux de demande, en élaborant des plans tenant compte des contraintes et en exécutant les actions approuvées. Les collègues détectent également des modèles invisibles à l'analyse manuelle, tels que les perturbations en cascade avec les fournisseurs ou les défauts d'alignement des stocks sur des milliers de SKU, et identifient ce qui compte avant qu'il ne devienne un problème. Les planificateurs passent de la lutte réactive contre les incendies à une planification

proactive, en menant des opérations plus efficaces et en améliorant les niveaux de service grâce à des décisions stratégiques qui améliorent les résultats commerciaux.

Instaurez la confiance dès le premier jour

Les membres de l'équipe d'IA s'appuient sur une science affinée au cours des 30 dernières années passées à superviser plus de 400 millions de références Amazon et sont équipés d'outils de chaîne d'approvisionnement spécialisés. Votre équipe bénéficie d'une expertise dans le domaine affinée par l'un des réseaux de chaîne d'approvisionnement les plus complexes au monde, fournissant des informations et des recommandations exploitables prêtes à l'emploi avec un raisonnement clair et explicable auquel vous pouvez faire confiance et que vous pouvez vérifier.

Fonctionnalités

Intelligence adaptative

Les membres de l'équipe d'IA tirent des leçons de chaque plan et de chaque décision grâce à une boucle continue : ils observent des modèles, détectent ce qui compte, recommandent des actions et exécutent les décisions approuvées. Cela institutionnalise les connaissances : lorsque les planificateurs partent, l'expertise demeure ; les nouveaux membres sont productifs dès le premier jour, améliorant ainsi les résultats sans formation manuelle.

Renseignements sur la demande

Les équipes d'IA orchestrent de manière dynamique plus de 18 outils de prévision et modèles de base basés sur les données Amazon, en les optimisant de manière autonome au niveau du SKU. Générez des prévisions précises dès le premier jour, même avec un historique limité. Harmonisez les prévisions statistiques, les engagements des clients et les entrées interfonctionnelles grâce à une planification consensuelle tout en surveillant en permanence la précision.

Renseignements relatifs à l'approvisionnement

Les équipes d'IA élaborent des plans d'approvisionnement prospectifs (version préliminaire) et regroupent intelligemment les exceptions dans les décisions stratégiques classées par impact. Exécutez des modèles d'optimisation pour une planification tenant compte des contraintes sur l'ensemble de votre réseau. Surveillez les opérations 24/7, identifiez ce qui compte, puis exécutez les décisions approuvées directement dans les systèmes existants, réduisant ainsi les cycles de plusieurs semaines à quelques heures.

Intégration agentic

AI-powered les agents d'intégration vous guident tout au long de la configuration par le biais d'une conversation en langage naturel. Connectez des données fragmentées via JDBC ou Amazon S3, préparez-les pour Connect Decisions et signalez automatiquement les problèmes avant qu'ils n'affectent les prévisions. Configurez les règles et politiques commerciales dans un langage clair avec des aperçus en temps réel, pour être opérationnels en quelques semaines, et non en quelques mois.

Démarrage

Dans cette section, vous apprendrez à créer une instance Amazon Connect Decisions, à accorder des rôles d'autorisation aux utilisateurs et à vous connecter à l'application Web Amazon Connect Decisions.

Conditions requises pour utiliser Amazon Connect Decisions

Avant de créer une instance Amazon Connect Decisions, assurez-vous de suivre les étapes suivantes :

- Tu as un AWS compte. Pour créer un AWS compte, consultez Configuration d'un compte AWS.
- Assurez-vous que le centre d'identité IAM est activé. Pour activer IAM Identity Center, consultez la section Activation d'IAM Identity Center.
- Une instance IAM Identity Center doit être activée dans la même région que celle où vous souhaitez créer votre instance Amazon Connect Decisions. Amazon Connect Decisions est uniquement pris en charge dans les régions USA Est (Virginie du Nord) et Europe (Irlande).
- Si l'instance Amazon Connect Decisions ne se trouve pas dans la même région que votre région IAM Identity Center existante, contactez-nous pour obtenir de l'aide.
- Vous devez avoir au moins un utilisateur dans l'instance IAM Identity Center pour être désigné en tant qu'administrateur Amazon Connect Decisions. Vous pouvez connecter votre Active Directory à IAM Identity Center. Pour plus d'informations, voir Se connecter à un annuaire Microsoft AD.
- Ajoutez tous les utilisateurs supplémentaires qui ont besoin d'accéder à Amazon Connect Decisions à IAM Identity Center.
- Vous avez besoin du service de gestion des AWS clés (AWS KMS) pour créer une instance. Amazon Connect Decisions utilise cette clé AWS KMS pour chiffrer toutes les données qui entrent dans Amazon Connect Decisions. Pour plus d'informations sur les clés AWS KMS, consultez la section Création de clés.
- Si vous avez l'intention d'activer la fonctionnalité d'actions, vous devez configurer une connexion au système que vous utilisez pour conserver les données pertinentes et fournir les informations d'identification à utiliser par Amazon Connect Decisions. N'hésitez pas à nous contacter pour obtenir de l'aide supplémentaire.

Navigateurs pris en charge par Amazon Connect Decisions

Avant de travailler avec Amazon Connect Decisions, vérifiez que votre navigateur est compatible à l'aide du tableau suivant.

Navigateur	Versions prises en charge
Google Chrome	Les trois dernières versions.
Mozilla Firefox ESR	Les versions sont prises en charge tant que la date de fin de vie Firefox n'a pas été atteinte. Pour plus de détails, consultez le calendrier de publication de Firefox ESR.
Mozilla Firefox	Les trois dernières versions.
Microsoft Edge et Edge Chromium	Version 84 et versions ultérieures.
Safari	Safari 10 ou version ultérieure sur macOS.

Langues prises en charge par Amazon Connect Decisions

Amazon Connect Decisions prend en charge les langues suivantes :

- Anglais (États-Unis)

Configuration d'un compte AWS

Utilisez cette section pour créer un AWS compte et créer un utilisateur IAM. Pour plus d'informations sur les meilleures pratiques relatives à la création d'un AWS compte, consultez la section Création de votre AWS environnement de bonnes pratiques.

Inscrivez-vous pour un AWS compte

Si vous n'avez pas de AWS compte, suivez les étapes ci-dessous pour en créer un.

Pour vous inscrire à un AWS compte

1. Ouvrir https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d’inscription, vous recevrez un appel téléphonique ou un SMS et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous créez un AWS compte, un AWS utilisateur root est créé. L'utilisateur root a accès à tous les services et ressources AWS du compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l’utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en cliquant sur Mon compte.

Création d’un utilisateur doté d’un accès administratif

Après avoir créé un AWS compte, sécurisez l'utilisateur root de votre AWS compte, activez AWS IAM Identity Center et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre AWS Utilisateur racine d'un compte

1. Connectez-vous à la console de AWS gestion en tant que propriétaire du compte en choisissant Utilisateur root et en saisissant l'adresse e-mail de votre AWS compte. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l’aide pour vous connecter en utilisant l’utilisateur racine, consultez Connexion en tant qu’utilisateur racine dans le Guide de l’utilisateur AWS Sign-In.
2. Activez l’authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, consultez la section Activer un périphérique MFA virtuel pour l'utilisateur root de votre AWS compte (console) dans le guide de l'utilisateur IAM.

Création d’un utilisateur doté d’un accès administratif

1. Activez IAM Identity Center.

Pour obtenir des instructions, consultez la section Activation d' AWS IAM Identity Center dans le guide de l'utilisateur d'AWS IAM Identity Center.

2. Dans IAM Identity Center, octroyez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur avec le répertoire IAM Identity Center par défaut dans le guide de l'utilisateur d'AWS IAM Identity Center.

Connexion en tant qu’utilisateur doté d’un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l’URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l’utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'AWS Sign-In utilisateur.

Attribution d’un accès à d’autres utilisateurs

1. Dans IAM Identity Center, créez un ensemble d’autorisations qui respecte la bonne pratique consistant à appliquer les autorisations de moindre privilège.

   Pour obtenir des instructions, consultez la section Créer un ensemble d'autorisations dans le guide de l'utilisateur d'AWS IAM Identity Center.

2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

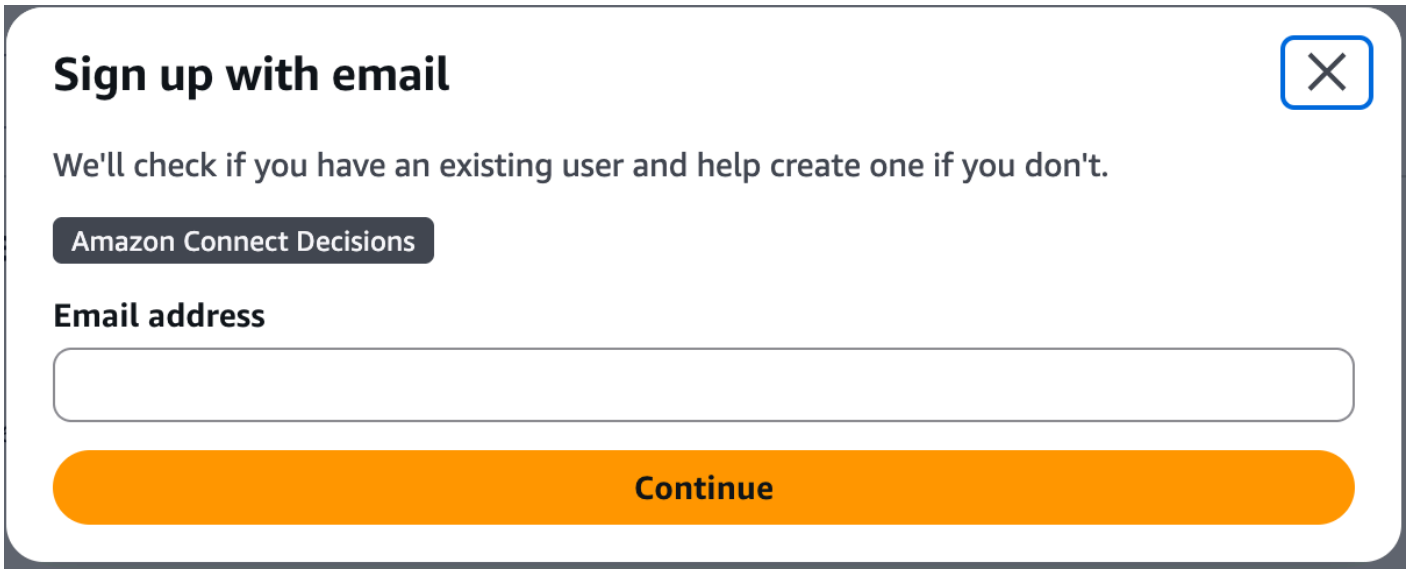
   Pour obtenir des instructions, consultez la section Ajouter des groupes dans le guide de l'utilisateur d'AWS IAM Identity Center.

Configuration de l'intégration d'AWS Identity Center

Pour créer une instance et utiliser le service Amazon Connect Decisions, vous devez soit connecter un profil utilisateur IAM Identity Center existant, soit en créer un nouveau.

1. Ouvrez la console Amazon Connect Decisions. Vous pouvez également rechercher « Amazon Connect Decisions » dans la console de AWS gestion principale.

2. Si nécessaire, modifiez la région AWS en sélectionnant Sélectionner une région en haut de la console. Choisissez votre région dans la liste déroulante.
3. Sélectionnez Créer une instance Amazon Connect Decisions. Une notification s'affichera.



4. Entrez votre adresse e-mail et sélectionnez Continuer. iDC vérifiera si l'e-mail correspond à un utilisateur existant.
5. Effectuez l'une des actions suivantes :
   - Si iDC correspond à l'adresse e-mail d'un utilisateur, sélectionnez Connect your identity source et intégrez votre équipe.

     > **Note**
     >
     > Cela peut être utilisé si votre organisation possède une instance iDC établie que vous souhaitez utiliser pour Amazon Connect Decisions.

   - Si iDC ne trouve aucune correspondance avec un utilisateur existant, une notification de création d'utilisateur apparaît. Passez à l'étape suivante.
6. Dans la notification, saisissez ce qui suit, puis sélectionnez Continuer :
   - Adresse e-mail
   - Prénom
   - Nom

   iDC crée automatiquement l'utilisateur et l'ajoute en tant qu'administrateur Amazon Connect Decisions.

7. Effectuez l’une des actions suivantes :
   - Pour créer une instance à l'aide d'une configuration standard, sélectionnez Créer. Voir Utiliser la configuration standard.
   - Pour créer une instance à l'aide d'une configuration personnalisée, sélectionnez Modifier dans la configuration avancée. Consultez la section Utiliser la configuration avancée.

Lorsqu'il est utilisé conjointement avec IAM Identity Center, Amazon Connect Decisions extrait les champs « nom d'utilisateur » et « e-mail » du répertoire IAM Identity Center. Aucun de ces attributs n'est stocké de manière native dans votre instance Amazon Connect Decisions et est toujours récupéré lors de l'exécution. Amazon Connect Decisions chiffre ces attributs d'identité au repos à l'aide d'une clé KMS AWS détenue par défaut. Les clés KMS gérées par le client ne sont pas prises en charge dans Amazon Connect Decisions. Si vous supprimez un utilisateur dans votre instance AWS IAM Identity Center, Amazon Connect Decisions le supprime également de votre instance.

Gestion de votre instance Amazon Connect Decisions

La création d'une instance dans Amazon Connect Decisions crée un environnement dédié à la gestion et à l'analyse de la chaîne d'approvisionnement. Pour configurer une instance, vous devez configurer les détails de base, établir les paramètres et définir les autorisations d'accès initiales des utilisateurs.

Seul l'administrateur AWS de la console de gestion peut créer une instance. L'administrateur de la console de AWS gestion qui crée l'instance Amazon Connect Decisions doit disposer de toutes les autorisations répertoriées dans les exemples Identity-based de politiques. Cet administrateur doit inviter un utilisateur IAM en tant qu'administrateur Amazon Connect Decisions pour gérer Amazon Connect Decisions.

Les pages suivantes décrivent en détail le processus de création et de suppression d'une instance.

Création de votre instance

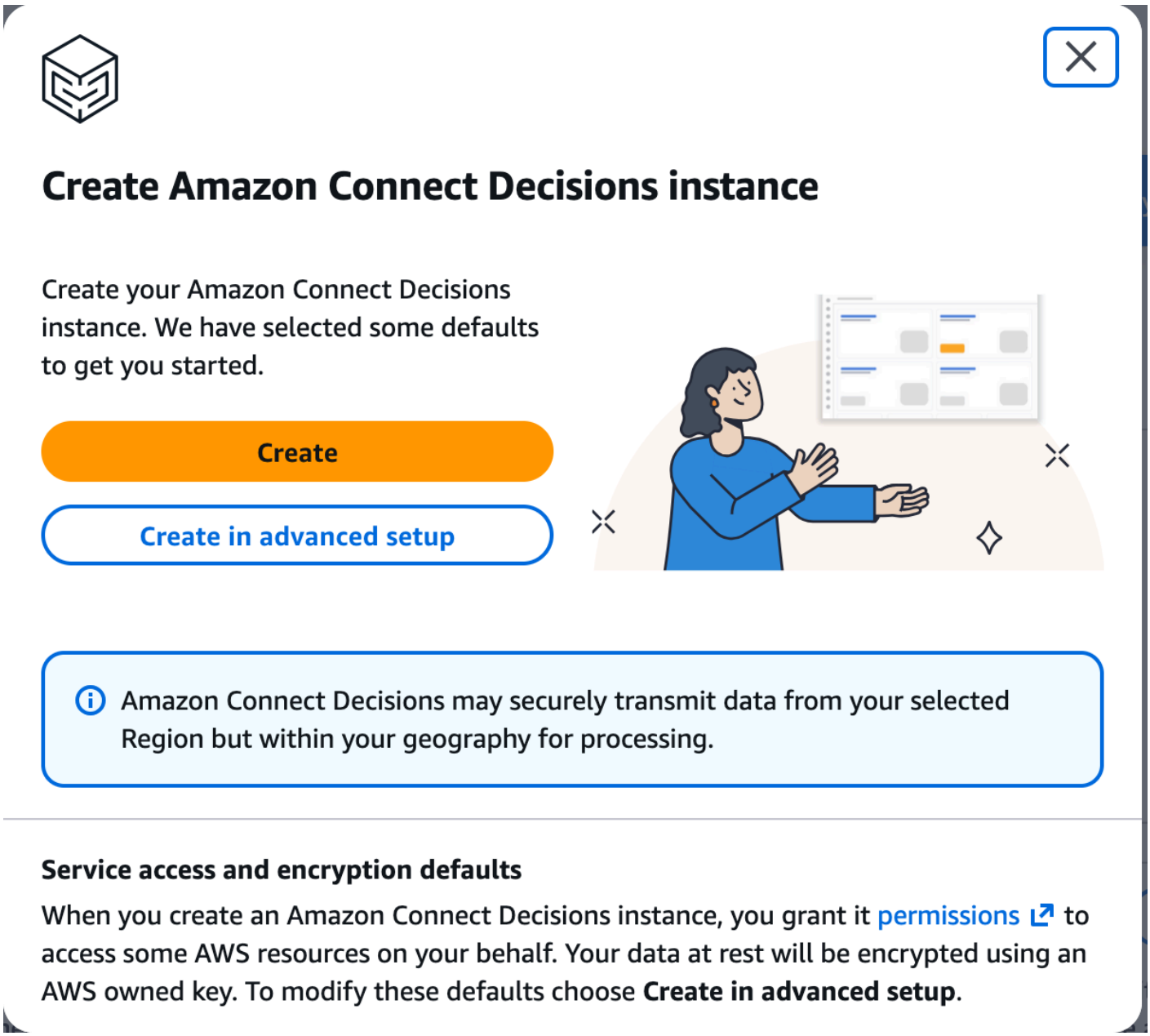
Vous créez une instance à l'aide de l'une des deux méthodes suivantes : configuration standard ou configuration avancée. La configuration standard utilise un processus automatisé qui crée rapidement votre instance à l'aide de paramètres prédéfinis. La configuration avancée vous permet de personnaliser votre instance en définissant vos propres paramètres.

Utilisation de la configuration standard

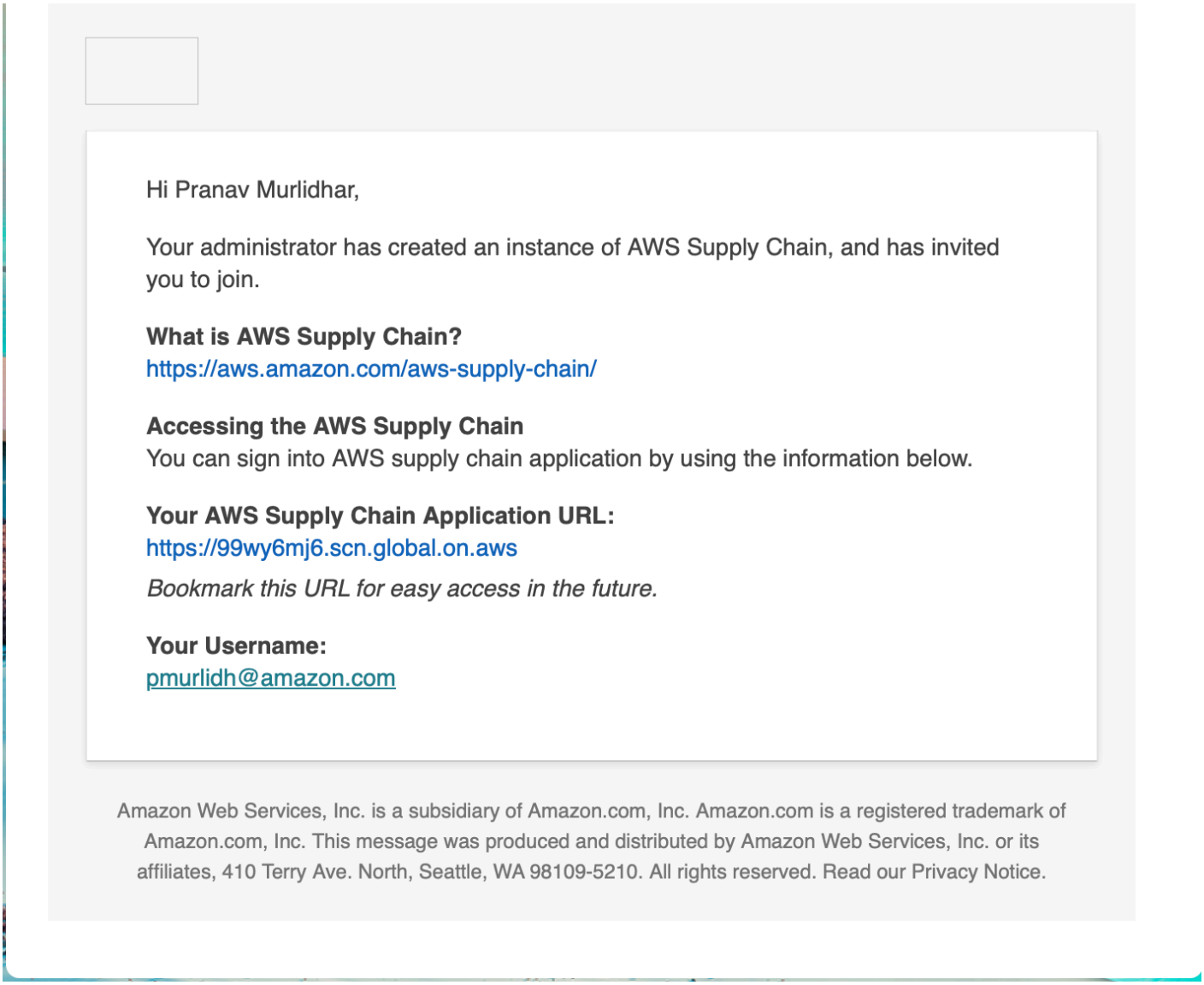
La configuration standard crée votre instance Amazon Connect Decisions à l'aide des paramètres de sécurité et de chiffrement par défaut. Les instances fonctionnent dans des régions AWS géographiques. Pour plus d'informations sur les régions, consultez Régions et points de terminaison dans le guide de l'utilisateur IAM et points de terminaison régionaux dans la AWS référence générale.

Pour créer une instance Amazon Connect Decisions à l'aide d'une configuration standard de paramètres prédéfinis, procédez comme suit.

1. Sélectionnez Créer.



2. Vérifiez vos e-mails pour vérifier les informations suivantes :
   - Un e-mail de l'équipe iDC.
   - Un e-mail de l'équipe de gestion des identités.



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://99wy6mj6.scn.global.on.aws
Bookmark this URL for easy access in the future.

Your Username:
pmurlidh@amazon.com

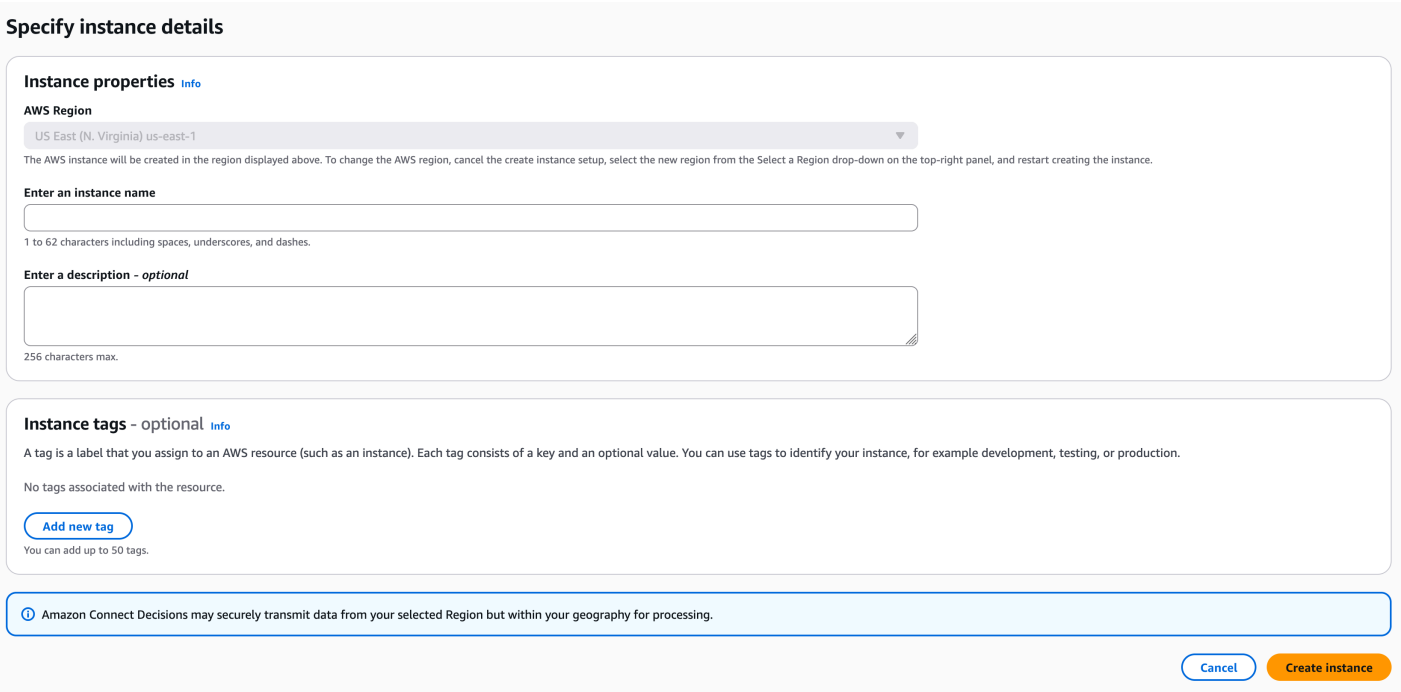
Amazon Web Services, Inc. is a subsidiary of Amazon.com, Inc. Amazon.com is a registered trademark of Amazon.com, Inc. This message was produced and distributed by Amazon Web Services, Inc. or its affiliates, 410 Terry Ave. North, Seattle, WA 98109-5210. All rights reserved. Read our Privacy Notice.

3. Une fois que vous avez reçu l'e-mail d'invitation, connectez-vous à Amazon Connect Decisions. Voir Se connecter à l'application Web Amazon Connect Decisions.

Utilisation de la configuration avancée

La configuration avancée vous permet de personnaliser votre instance en définissant vos propres paramètres. Pour créer une instance Amazon Connect Decisions à l'aide d'une configuration avancée de paramètres prédéfinis, procédez comme suit.

1. Sélectionnez Créer dans la configuration avancée.
2. La page des propriétés de l'instance apparaît.



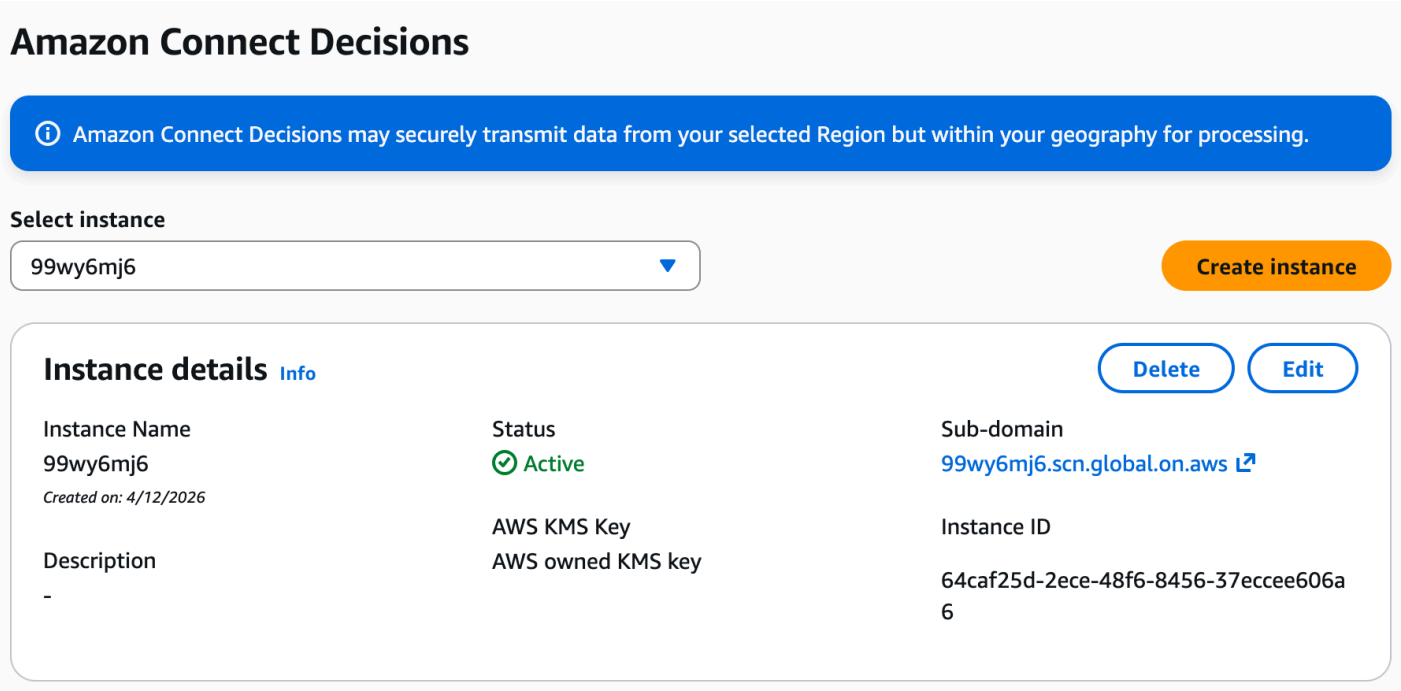
3. Entrez ce qui suit sur la page des propriétés de l'instance :
   - Nom — Entrez le nom de l'instance.
   - Description — Entrez une description de votre instance Amazon Connect Decisions (par exemple, instance de production, instance de test, etc.).
   - Balises d'instance : vous pouvez ajouter des balises à votre instance qui peuvent être utilisées à des fins d'identification. Par exemple, vous pouvez ajouter une balise pour définir le type d'instance que vous créez (par exemple, production, test, UAT, etc.).
4. Sélectionnez Créer une instance.

Suppression d'une instance

Pour supprimer une instance, procédez comme suit.

> **Note**
>
> Lorsque vous supprimez une instance, les informations du compartiment Amazon S3 ne sont pas automatiquement supprimées.

1. Ouvrez la console Amazon Connect Decisions à l'adresse https://console.aws.amazon.com/scn/home.
2. Sur le tableau de bord de la console Amazon Connect Decisions, dans le menu déroulant, sélectionnez l'instance que vous souhaitez supprimer.



3. Sélectionnez Delete (Supprimer).
4. Sur la page Supprimer l'instance Amazon Connect Decisions, sous Confirmation, tapez `delete` pour confirmer que vous souhaitez supprimer l'instance.
5. Sélectionnez Delete (Supprimer). La suppression de l'instance commence et une fois l'instance supprimée, vous verrez un message de confirmation.

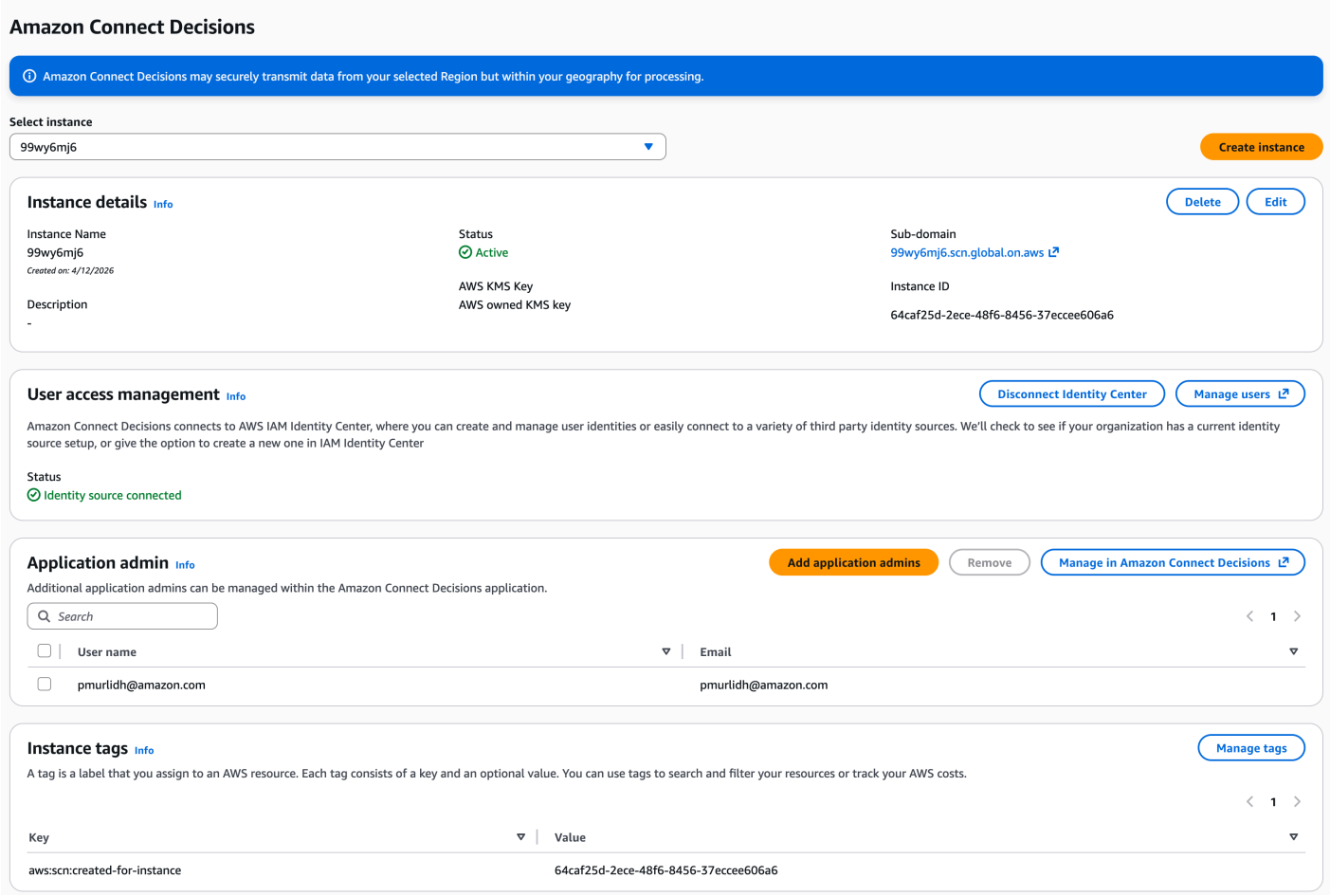
Choisissez un administrateur de l'application

En tant qu'administrateur de AWS console, vous choisissez un administrateur de l'application Amazon Connect Decisions pour gérer l'accès à l'application Web Amazon Connect Decisions. L'administrateur de l'application Amazon Connect Decisions peut ajouter ou supprimer des rôles d'autorisation utilisateur dans l'application Web Amazon Connect Decisions.

Une fois l'instance créée et une source d'identité connectée, procédez comme suit pour choisir un administrateur de l'application Amazon Connect Decisions.

1. Ouvrez le tableau de bord de la console Amazon Connect Decisions.

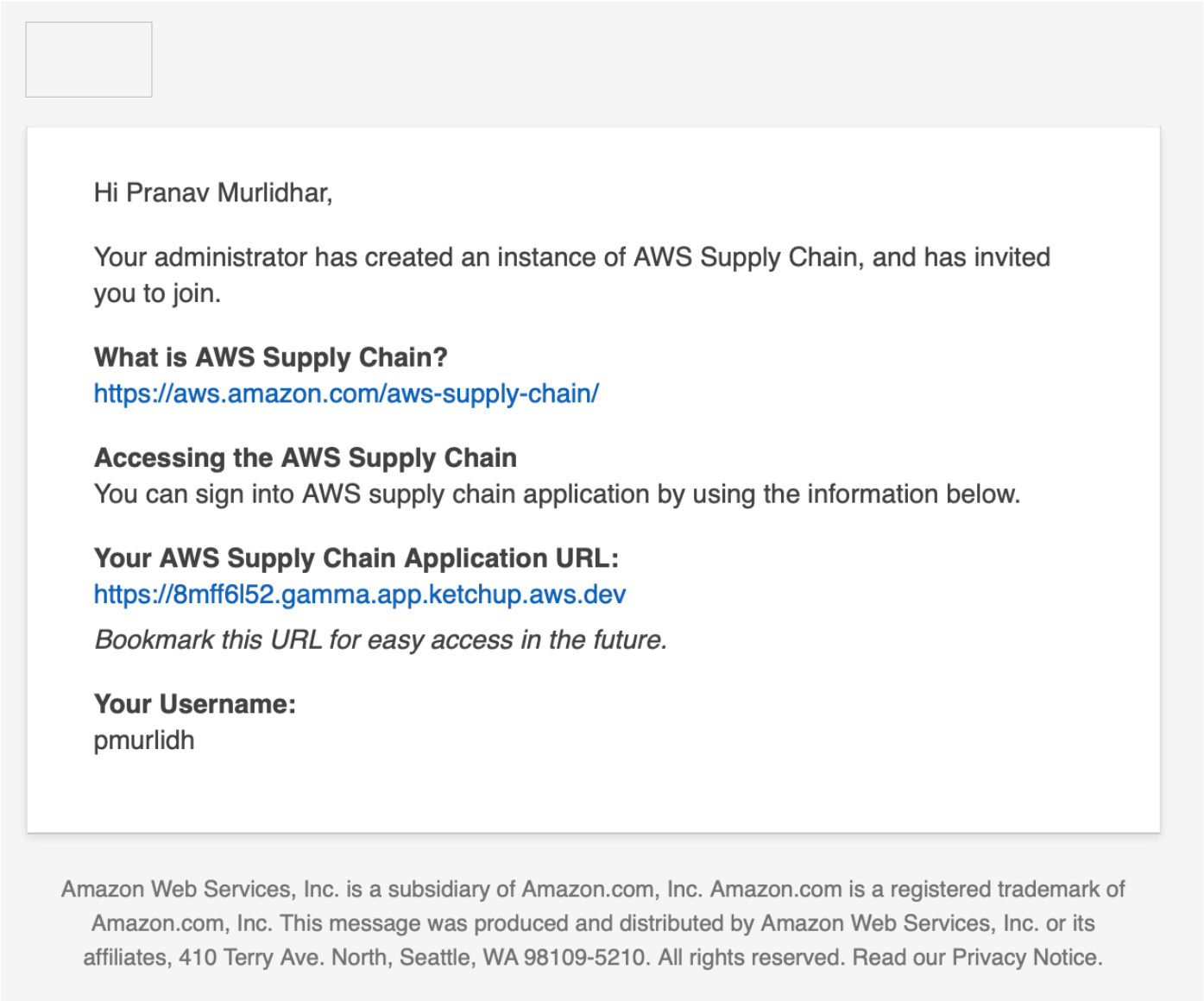
2. Accédez à Sélectionner l'administrateur de l'application et sélectionnez un utilisateur pour être administrateur de l'application Amazon Connect Decisions. Les résultats de recherche n'affichent que les utilisateurs correspondant aux critères de recherche.



3. (Facultatif) Choisissez Accéder au centre d'identité IAM pour ajouter d'autres utilisateurs. Pour plus d'informations sur l'ajout d'utilisateurs, consultez Gérer votre source d'identité dans le guide de l'utilisateur d'AWS IAM Identity Center et pour plus d'informations sur les rôles d'autorisation utilisateur, consultez Rôles d'autorisation utilisateur.

> **Note**
>
> Vous ne pouvez ajouter qu'un seul utilisateur à la fois depuis la console Amazon Connect Decisions. Vous ne pouvez pas ajouter de groupe en tant qu'administrateur d'application dans Amazon Connect Decisions.

4. Choisissez Envoyer une invitation. Un e-mail est envoyé à l'administrateur de l'application Web. Une fois que l'administrateur de l'application Web aura reçu l'e-mail d'invitation, il pourra sélectionner l'URL de l'application et se connecter aux Amazon Connect Decisions.


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.

Dans l'application Web Amazon Connect Decisions, vous verrez l'utilisateur répertorié sous Administration de l'application.

Accès à votre instance

L'utilisation de la console est le moyen le plus simple de gérer les ressources et les configurations de vos services. La console fournit une interface Web intuitive dans laquelle vous pouvez visualiser, créer, modifier et surveiller vos ressources.

Pour accéder à la console Amazon Connect Decisions, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les informations relatives aux ressources Amazon Connect Decisions de votre AWS compte. Si vous

créez une politique basée sur l’identité qui est plus restrictive que l’ensemble minimum d’autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette politique.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API ou l' AWS API. Autorisez plutôt l’accès à uniquement aux actions qui correspondent à l’opération d’API qu’ils tentent d’effectuer.

En tant qu'administrateur Amazon Connect Decisions, vous devriez avoir reçu un e-mail d'invitation à accéder à l'application Web Amazon Connect Decisions.

1. Vous pouvez choisir le lien dans l'e-mail ou sur le tableau de bord de la console Amazon Connect Decisions Sub-domain, sous Choisir une URL Web.
2. La page de connexion à l'application Web Amazon Connect Decisions s'affiche.
3. Entrez les informations d'identification de l'utilisateur AWS IAM Identity Center et choisissez Se connecter.
4. Chaque utilisateur que vous avez ajouté reçoit un e-mail contenant un lien vers Amazon Connect Decisions, ou vous pouvez choisir Copier le lien et envoyer le lien aux utilisateurs.

Une fois connecté avec succès, vous arriverez sur votre page d'accueil personnalisée. Reportez-vous à la section Comprendre votre page d'accueil dans le guide de l'utilisateur pour mieux comprendre votre page d'accueil.

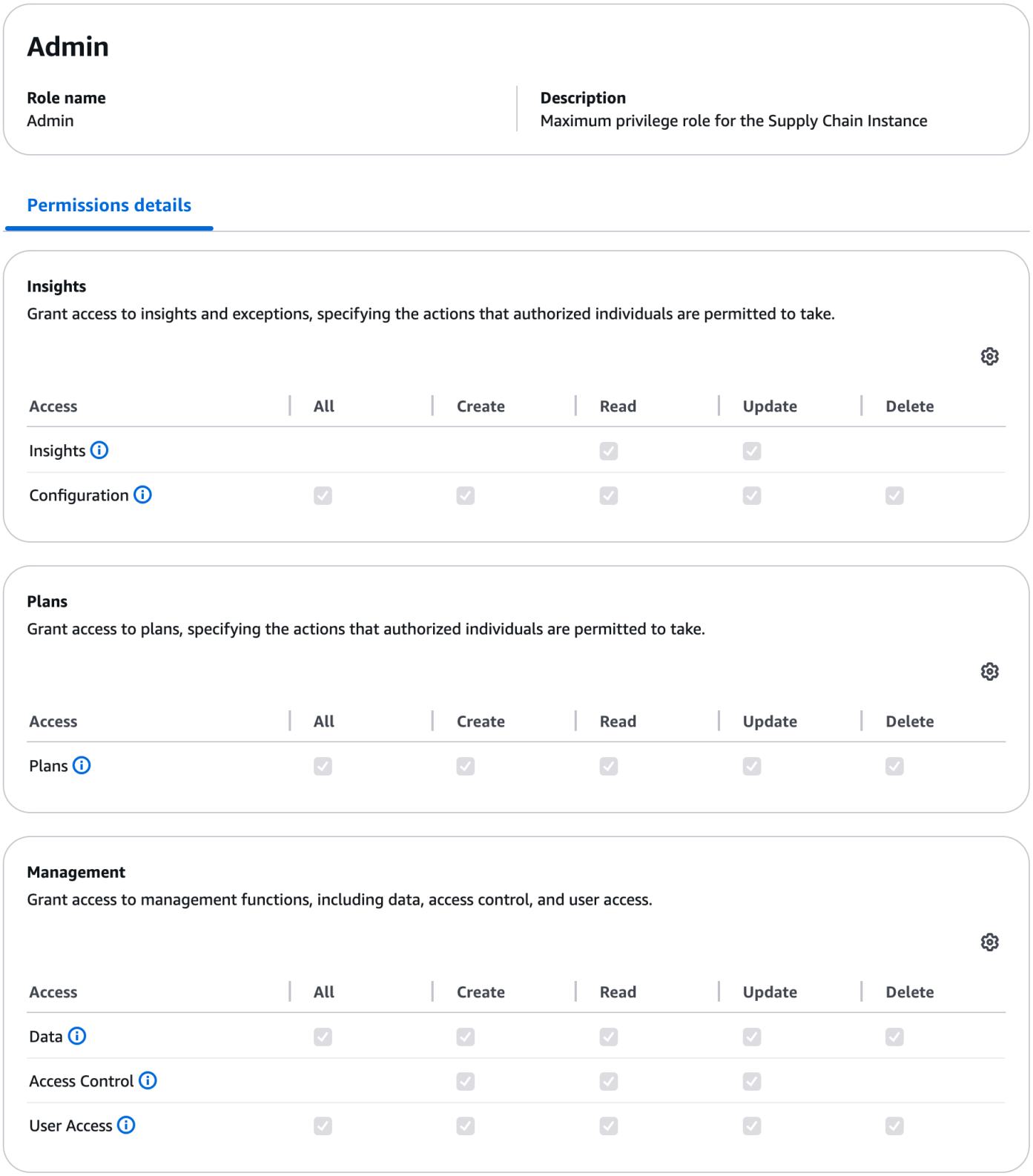
Contrôle d’accès

Amazon Connect Decisions fournit une gestion des accès de niveau entreprise qui vous permet de contrôler précisément qui peut accéder à quelles données et effectuer quelles actions au sein de votre instance. Cela garantit que vos utilisateurs ne voient que les informations pertinentes à leurs responsabilités tout en respectant les normes de sécurité et de conformité requises par votre organisation.

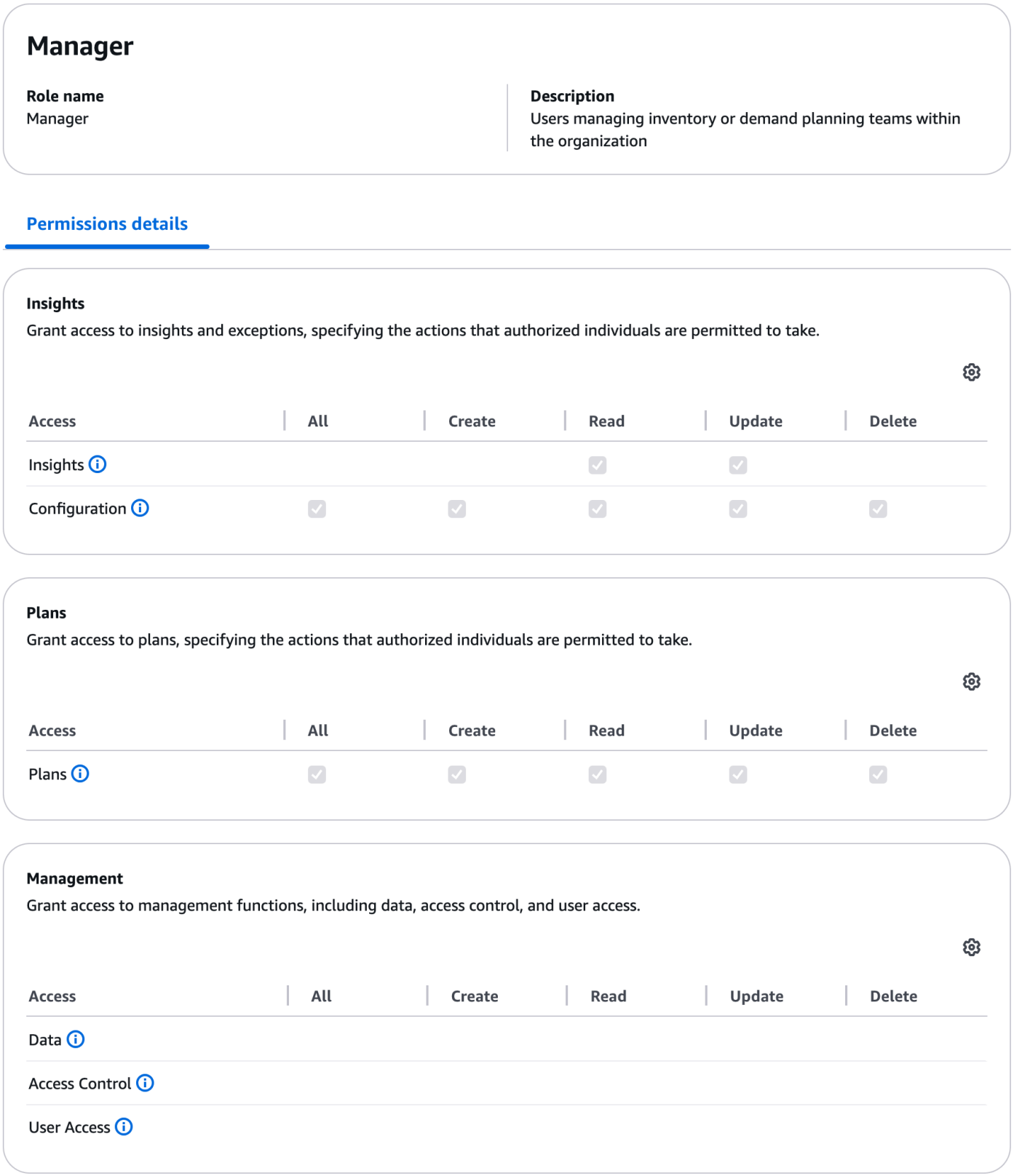
Vue d'ensemble des rôles et des autorisations

En tant qu'administrateur Amazon Connect Decisions, vous pouvez utiliser les rôles d'autorisation utilisateur par défaut ou créer des rôles d'autorisation personnalisés. Amazon Connect Decisions possède les rôles d'autorisation utilisateur par défaut suivants :

- Administrateur : accès permettant de créer, d'afficher et de gérer toutes les données et les autorisations des utilisateurs.



- Gestionnaire : accès permettant de créer, d'afficher et de gérer les éléments suivants.



- Planificateur — Accès pour créer, afficher et gérer les éléments suivants.

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**
>
> En tant qu'administrateur Amazon Connect Decisions, avant d'ajouter des utilisateurs, prenez note des points suivants :
>
> - Chaque rôle d'autorisation utilisateur par défaut est défini avec un ensemble d'autorisations. Vous pouvez ajouter des utilisateurs aux rôles d'autorisation utilisateur par défaut ou créer des rôles d'autorisation personnalisés.
> - Un utilisateur ne peut être affecté qu'à un seul rôle d'autorisation utilisateur.
> - Vous ne pouvez pas modifier ou supprimer les rôles d'autorisation utilisateur par défaut.
> - Lorsque vous modifiez un rôle d'autorisation personnalisé que vous avez créé, les autorisations de tous les utilisateurs du rôle d'autorisation personnalisé sont mises à jour.
> - Lorsque vous supprimez un rôle d'autorisation personnalisé que vous avez créé, tous les utilisateurs associés au rôle d'autorisation personnalisé perdent l'accès à Amazon Connect Decisions.
> - L'ajout de groupes n'est pas pris en charge dans Amazon Connect Decisions.

Gestion des rôles d'autorisation des utilisateurs

Ajout d'utilisateurs

En tant qu'administrateur Amazon Connect Decisions, vous pouvez ajouter des utilisateurs pour accéder à l'application Web Amazon Connect Decisions. Les utilisateurs doivent d'abord être ajoutés à IAM Identity Center (iDC), puis ils peuvent être ajoutés à Amazon Connect Decisions. Pour plus d'informations sur l'ajout d'utilisateurs à iDC, voir Attribuer un accès utilisateur.

Une fois que les utilisateurs ont été ajoutés à iDC, procédez comme suit pour ajouter un utilisateur.

1. Choisissez le tiroir de gauche des paramètres
2. Sélectionnez Utilisateurs. Sélectionnez Attribuer des utilisateurs
3. Effectuez une recherche pour identifier l'utilisateur. Vous pouvez effectuer une recherche en utilisant le nom d'affichage, l'e-mail, le prénom, le nom de famille, le nom d'utilisateur
4. Sélectionnez les utilisateurs que vous souhaitez ajouter.
5. Attribuez-leur un rôle. Consultez la présentation des rôles et des autorisations pour en savoir plus sur les rôles des utilisateurs dans Amazon Connect Decisions.

6. Sélectionnez Attribuer. Vérifiez que vos sélections sont correctes.

Mettre à jour les autorisations des utilisateurs

Pour mettre à jour le rôle d'autorisation utilisateur pour les utilisateurs actuels d'Amazon Connect Decisions, procédez comme suit.

1. Choisissez le tiroir de gauche des paramètres
2. Sélectionnez Utilisateurs. Sélectionnez Attribuer des utilisateurs
3. Dans la liste des utilisateurs, sélectionnez l'utilisateur pour ouvrir la page de détails de l'utilisateur.
4. Utilisez la liste déroulante des rôles pour mettre à jour les autorisations de rôle de l'utilisateur.
5. Confirmez que vous souhaitez modifier le rôle en cliquant sur le bouton de changement de rôle

Suppression des utilisateurs

En tant qu'administrateur Amazon Connect Decisions, vous pouvez supprimer des utilisateurs de l'application Web Amazon Connect Decisions. Pour supprimer des utilisateurs, procédez comme suit.

1. Choisissez le tiroir de gauche des paramètres
2. Sélectionnez Utilisateurs. Sélectionnez Attribuer des utilisateurs
3. Dans la liste des utilisateurs, sélectionnez l'utilisateur pour ouvrir la page de détails de l'utilisateur.
4. Sélectionnez Supprimer
5. Confirmez que vous souhaitez supprimer l'utilisateur en cliquant sur le bouton Supprimer

Configuration de l'accès au niveau des attributs

Attribute-Based Le contrôle d'accès (ABAC) ajoute un niveau de précision supplémentaire en limitant l'accès en fonction du contexte commercial. En utilisant les attributs des produits et des sites, vous pouvez vous assurer que les planificateurs ne voient que les détails des produits et des sites spécifiques qu'ils gèrent, tandis que les responsables conservent une visibilité sur les domaines de responsabilité de leurs équipes.

Tout utilisateur ayant le rôle « Admin » peut configurer l'accès par produit et par site pour les autres utilisateurs :

1. Accédez à la page Utilisateurs dans la barre de navigation de gauche.

2. Dans la liste des utilisateurs de cette instance, sélectionnez celui qui doit être configuré.
3. Par défaut, dans la section Accès aux données, l'option « Accorder l'accès complet à tous les produits et sites » sera activée pour les utilisateurs. Lorsque cette option est activée, elle permet d'accéder à tous les produits et sites (comment cela fonctionnait avant ce lancement).
4. Si vous désactivez « Accorder un accès complet à tous les produits et sites », la section de configuration des produits et des sites sera visible. Aucun produit ou site ne sera attribué lors du premier accès.
5. Cliquez sur le Add/Remove bouton correspondant aux produits ou aux sites en fonction de ce que vous devez configurer. Utilisez la recherche pour trouver et sélectionner les éléments nécessaires à cet utilisateur.
6. Le même produit ou site peut être attribué à plusieurs utilisateurs. Un utilisateur peut disposer d'un maximum de 1 000 combinaisons produit/site.
7. Les produits ou sites précédemment configurés peuvent être supprimés à l'aide de la même interface.
8. Consultez et confirmez la liste complète des ajouts et suppressions dans la dernière page de l'assistant pour terminer la configuration des accès.

Une fois l'accès au produit et au site configuré, l'accès de cet utilisateur sera restreint en fonction des attributions suivantes :

- Tous les utilisateurs peuvent consulter n'importe quelle page d'exception ou de recommandation, qu'elle ait été générée pour un produit ou un site inclus dans leur contrôle d'accès.
- Pour effectuer des actions de mutation (comme ignorer une exception ou changer le statut de En cours à Terminé), les utilisateurs doivent avoir configuré le produit OU le site approprié dans leur contrôle d'accès.
- Les utilisateurs dont le contrôle d'accès est configuré peuvent également utiliser l'attribution d'utilisateurs et le bouton Access View Toggle.

Affectation d'utilisateur

L'attribution d'utilisateurs est une fonctionnalité qui permet d'équilibrer plus facilement les informations entre plusieurs utilisateurs. Grâce à l'affectation des utilisateurs, les clients peuvent attribuer des informations spécifiques aux utilisateurs afin de mieux refléter la manière dont ces tâches sont partagées dans la vie réelle. Elle fonctionne comme suit :

- Chaque fois qu'une exception est créée, le système vérifie le produit et le site pour lesquels l'exception est créée par rapport à tous les utilisateurs dont le contrôle d'accès est configuré pour le même produit OU site
- Si le système trouve un utilisateur correspondant, le champ Affecté à cette exception est mis à jour avec le nom d'utilisateur. Dans les cas où plusieurs utilisateurs ont des produits ou des sites qui correspondent, à l'exception près, celui-ci est attribué au hasard à l'un d'entre eux.
- Un seul utilisateur peut être affecté à chaque exception, mais une exception peut être réaffectée à un autre utilisateur si nécessaire. Il ne peut être réattribué qu'à un utilisateur ayant accès au produit ou au site
- Auto-assignment for insights se produit lorsque l'exception est créée pour la première fois. Les informations créées précédemment ne seront pas réattribuées automatiquement. De plus, si un utilisateur est supprimé ou si son contrôle d'accès est mis à jour, l'attribution de l'utilisateur n'est pas automatiquement mise à jour
- Sur la page de liste des informations, un utilisateur peut filtrer selon la dimension Attribué à afin d'identifier facilement toutes les informations qui lui sont attribuées. Ils peuvent également utiliser ce même filtre pour afficher les informations non attribuées. L'attribution d'utilisateurs n'est actuellement disponible que pour obtenir des informations

Intégration des données

Connecter vos données

Conditions préalables

Avant de commencer l'intégration des données, assurez-vous de disposer des éléments suivants :

- Instance Amazon Connect Decisions
  - Votre instance devrait déjà être créée avec un compartiment S3 associé
- Données préparées
  - Travaillez avec votre homologue Amazon Customer Success pour déterminer les données dont vous avez besoin en fonction de la manière dont vous prévoyez d'utiliser Amazon Connect Decisions. Les exigences relatives aux données de base incluent :
    - Sales/Order Historique : plus de 12 mois d'enregistrements de transactions
    - Détails du produit : Catalogue de produits complet avec spécifications
    - Site/Location Informations : entrepôts, centres de distribution, points de vente
    - Stocks actuels : On-hand inventaire de chaque site
  - Toutes les données sources au format CSV avec UTF-8 encodage

Première connexion : questionnaire d'intégration

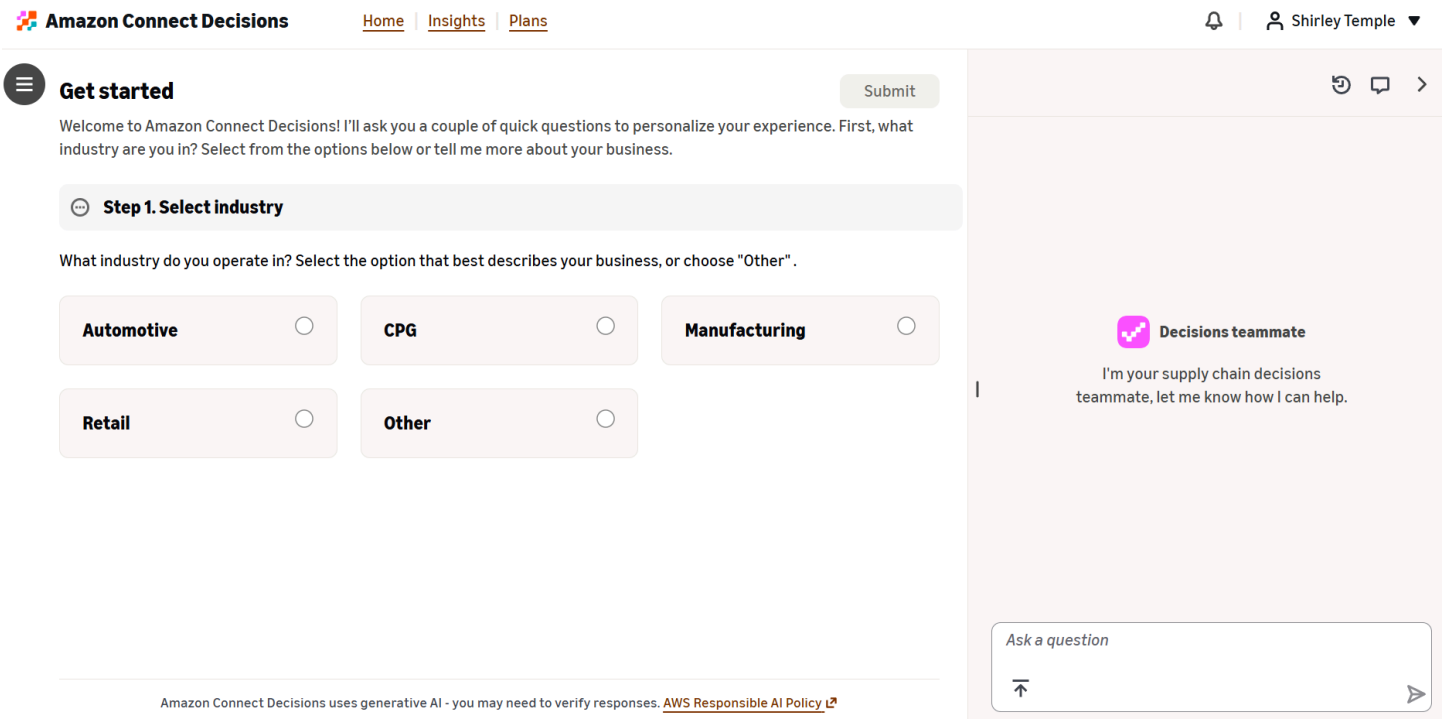
Lorsque vous vous connectez à Amazon Connect Decisions pour la première fois, le système présente un questionnaire d'intégration guidé. Cet assistant de personnalisation aide les collaborateurs de Decisions à contextualiser les fonctionnalités les plus pertinentes pour votre entreprise. Le questionnaire recueille des informations sur votre secteur d'activité, les principaux défis commerciaux et l'approche préférée en matière de planification. Vos réponses aideront à optimiser les étapes d'intégration en fonction de votre sélection, ce qui permettra au système de rationaliser les flux de travail de configuration ultérieurs et de définir les chemins de configuration les plus pertinents pour votre entreprise. Vous devez effectuer toutes les étapes avant d'accéder à l'application complète. The Decisions Teammate est disponible tout au long du processus d'intégration via la barre latérale droite pour répondre aux questions en temps réel.

> **Note**
>
> Il s'agit d'une sélection unique lors de la première connexion uniquement. Vos réponses fournissent un contexte supplémentaire pour optimiser les étapes d'intégration ultérieures et aider les agents à comprendre votre environnement commercial. Toutes les fonctionnalités restent entièrement accessibles, quelles que soient vos sélections.

Étape 1 : Sélectionnez le secteur

Ce que vous voyez : Un message de bienvenue et un ensemble de boutons radio vous invitant à sélectionner le secteur qui décrit le mieux votre activité.

1. Sélectionnez le bouton radio qui représente le mieux votre activité.
2. Si aucune des options prédéfinies ne s'applique, sélectionnez Autre.



Étape 2 : Définissez votre plus grand défi

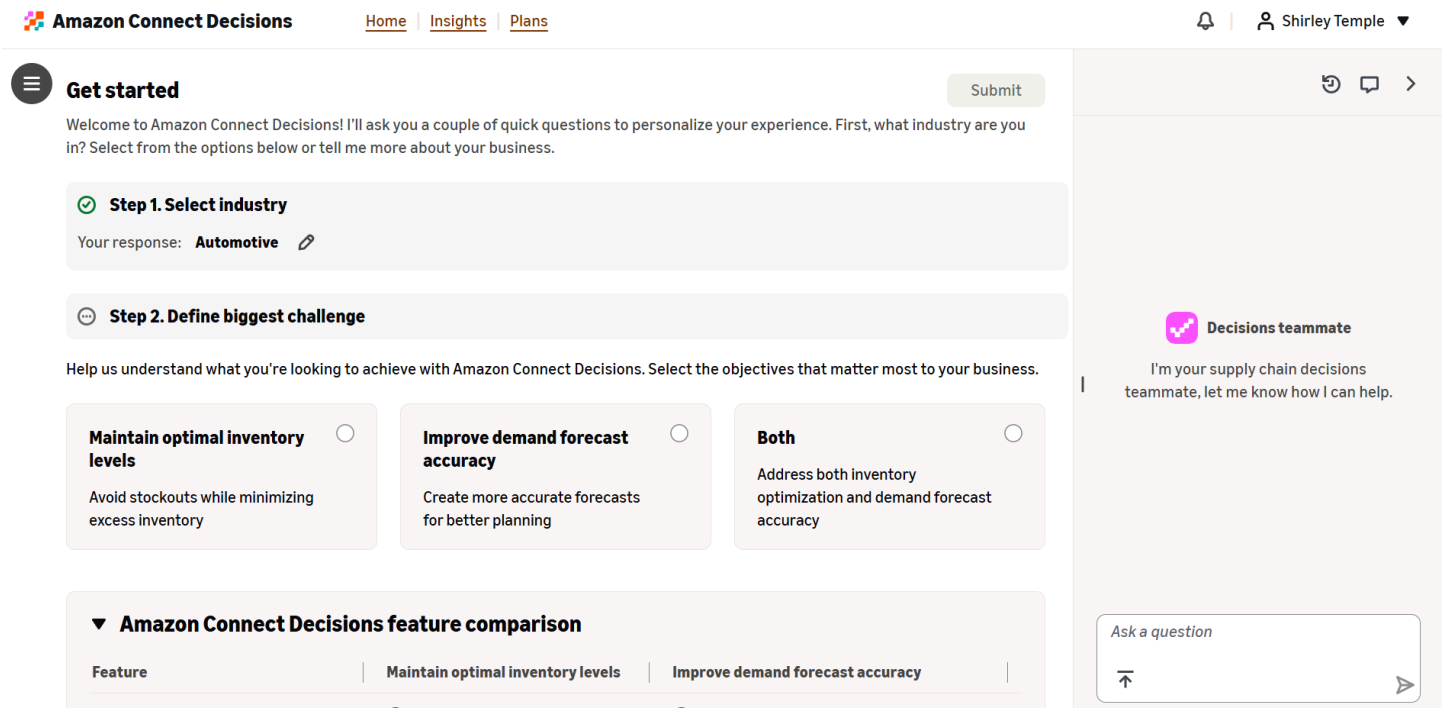
Ce que vous voyez : Votre réponse à l'étape 1 est affichée avec une option de modification. Ci-dessous, vous êtes invité à identifier votre principal défi commercial parmi trois options. Un tableau

de comparaison des fonctionnalités s'affiche pour vous aider à comprendre quelles fonctionnalités sont associées à chaque sélection.

1. Passez en revue les options. Consultez le tableau suivant pour connaître les options disponibles et leur signification.
2. Sélectionnez le bouton radio qui représente votre défi le plus pressant.
3. Consultez éventuellement le tableau de comparaison des fonctionnalités situé sous les options pour comprendre ce qui est inclus dans chaque sélection.

Options de défis commerciaux

Option	Description	Fonctionnalités clés activées
Maintenir des niveaux d'inventaire optimaux	Choisissez cette option si votre principal défi consiste à éviter les ruptures de stock tout en minimisant les stocks excédentaires.	Optimisation des stocks ; Prévention des ruptures de stock ; Réduction des stocks excédentaires ; Planification des approvisionnements ; Suivi des délais de livraison des fournisseurs
Améliorez la précision des prévisions de la demande	Choisissez cette option si votre principal défi consiste à créer des prévisions plus précises pour de meilleures décisions de planification.	Prévisions de base ; planifica tion consensuelle ; suivi de la précision des prévisions
Les deux	Choisissez cette option si vous devez gérer simultanément l'optimisation des stocks et la précision des prévisions de la demande.	Toutes les fonctionnalités spécifiques à l'offre et à la demande sont activées



Étape 3 : Choisissez votre approche de planification des stocks

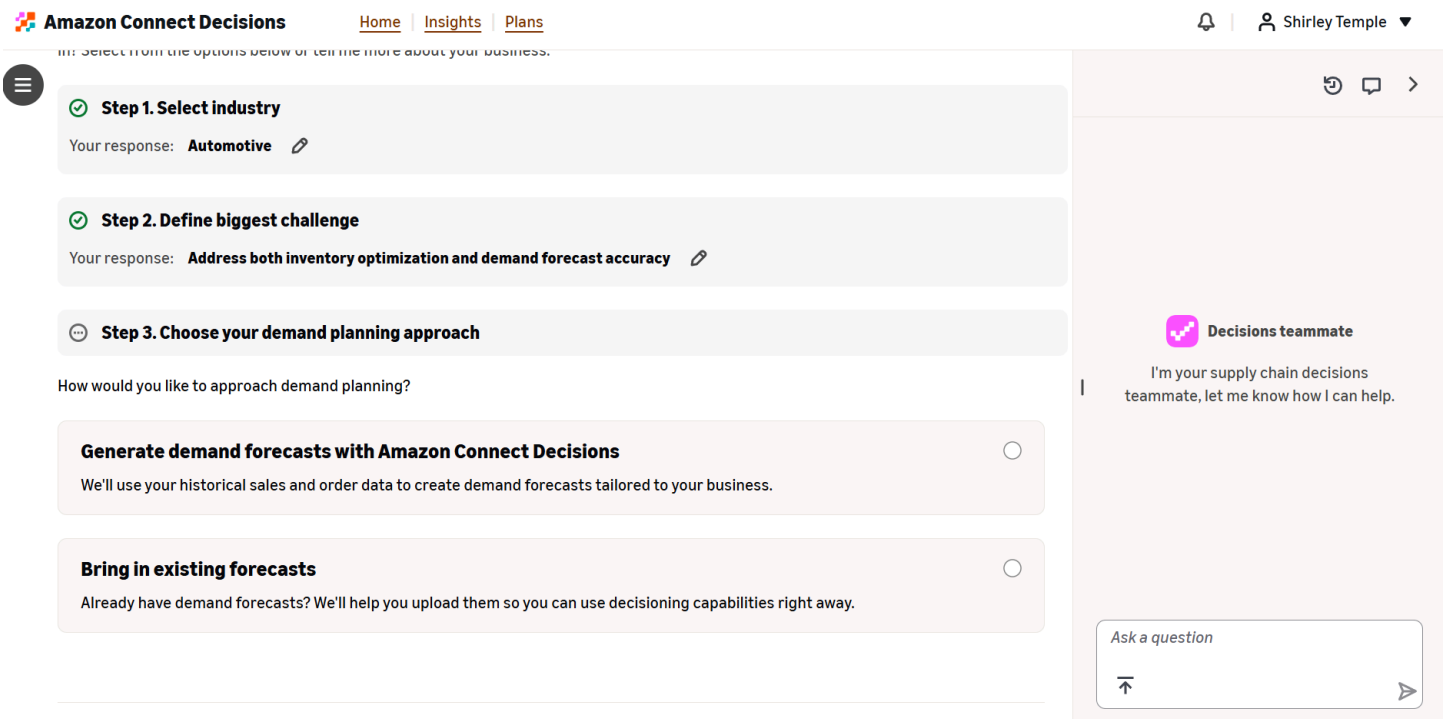
Ce que vous voyez : Les étapes 1 et 2 sont affichées comme terminées (indiquées par des coches vertes) et vos réponses sont affichées et modifiables. L'étape 3 demande comment vous souhaitez aborder la planification des stocks, deux options étant mises en évidence.

1. Passez en revue les deux options de planification des stocks. Consultez le tableau suivant pour connaître les options disponibles et leur signification.
2. Sélectionnez le bouton radio correspondant à l'approche qui correspond à votre état actuel.

Options d'approche de planification des stocks

Option	Description	Idéal pour
Générez des plans d'inventaire avec Amazon Connect Decisions	Le système utilise l'historique de vos ventes et vos données d'inventaire pour créer des plans adaptés à votre entreprise.	Organisations qui ne disposent pas d'une solution de planification existante ou qui souhaitent tirer parti des plans générés par l'IA à partir de leurs données historiques.

Option	Description	Idéal pour
Intégrez les projections ou les plans d'inventaire existants	Téléchargez vos plans d'inventaire ou vos projections existants afin de pouvoir utiliser immédiatement les fonctionnalités de prise de décision. Le système vous aidera à télécharger et à cartographier vos données.	Organisations qui ont déjà établi des processus de planification et qui souhaitent tirer parti des fonctionnalités de surveillance, de génération d'informations et de recommandation sans modifier la source de leur plan.



Étape 4 : Choisissez votre approche de planification de la demande

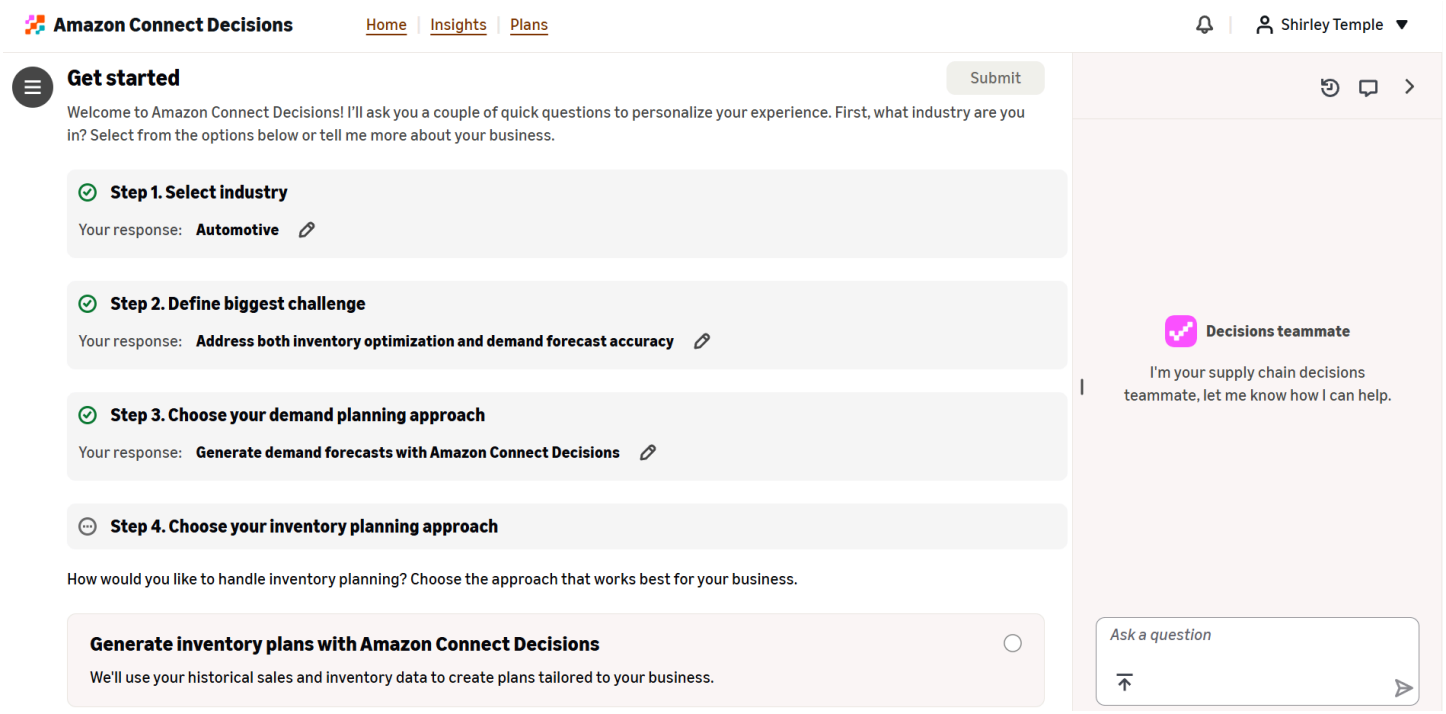
Ce que vous voyez : Les étapes 1 à 3 sont affichées comme terminées. L'étape 4 demande comment vous souhaitez aborder la planification de la demande.

1. Passez en revue les deux options de planification de la demande. Consultez le tableau suivant pour connaître les options disponibles et leur signification.
2. Sélectionnez le bouton radio correspondant à l'approche qui correspond à votre état actuel.
3. Cliquez sur Soumettre pour finaliser le questionnaire d'intégration.

N'oubliez pas : ce questionnaire d'intégration est une saisie contextuelle unique qui permet d'optimiser les étapes d'intégration en fonction de vos sélections. Il ne modifie pas le comportement de l'agent et ne restreint pas l'accès à ses fonctionnalités. Vous pouvez toujours accéder à toutes les fonctionnalités d'Amazon Connect Decisions.

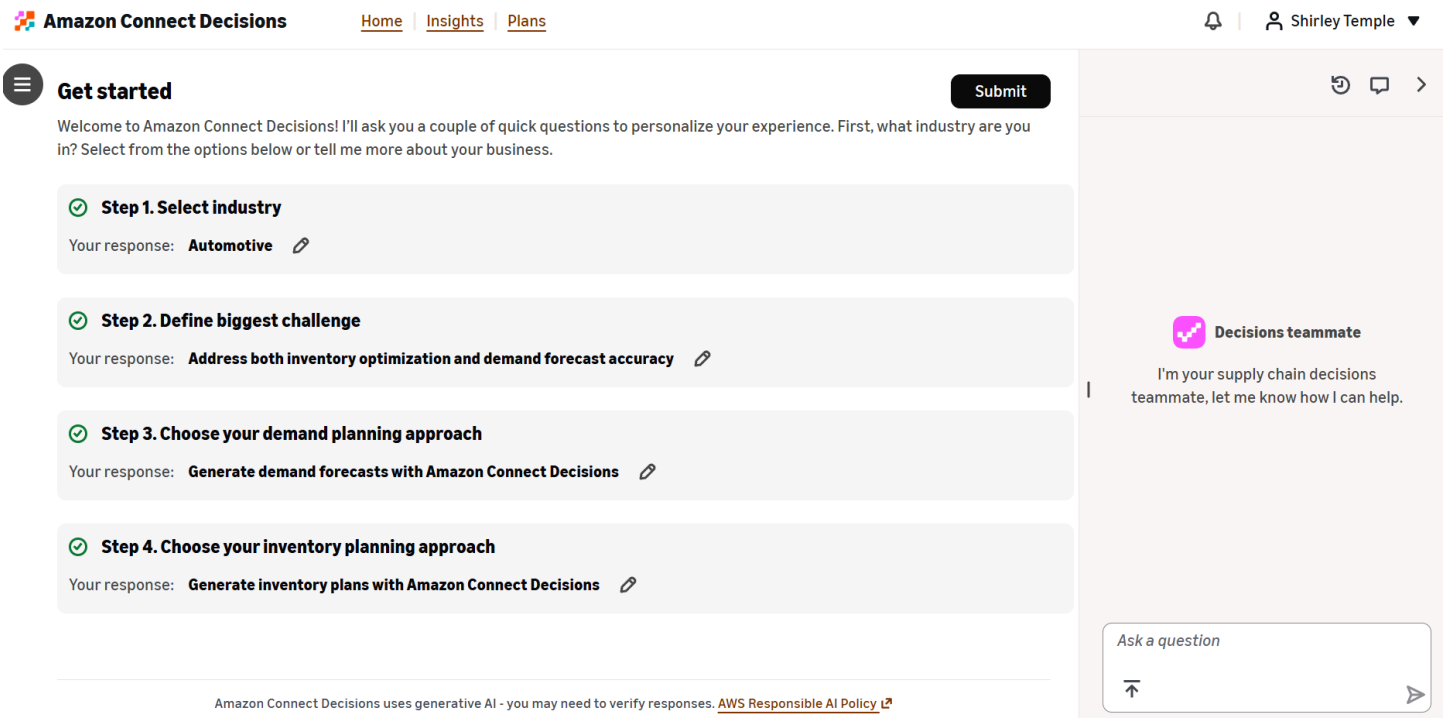
Options d'approche de planification de la demande

Option	Description	Idéal pour
Générez des prévisions de demande avec Amazon Connect Decisions	Le système utilise l'histori que de vos ventes et de vos commandes pour créer des prévisions de demande adaptées à votre activité. Amazon Connect Decisions orchestre plus de 18 outils de prévision pour produire des prévisions de référence précises.	Organisations qui ne disposent pas d'une solution de prévision existante ou qui souhaitent remplacer leur approche actuelle par des prévisions générées par l'IA.
Intégrez les prévisions existantes	Téléchargez vos prévisions de demande existantes afin de pouvoir utiliser immédiate ment les fonctionnalités de prise de décision. Le système vous aidera à cartographier et à importer vos données de prévision.	Organisations qui ont déjà établi des processus de prévision et qui souhaiten t tirer parti des fonctionn alités de surveillance, de génération d'informations et de recommandation sans modifier leur source de prévisions.



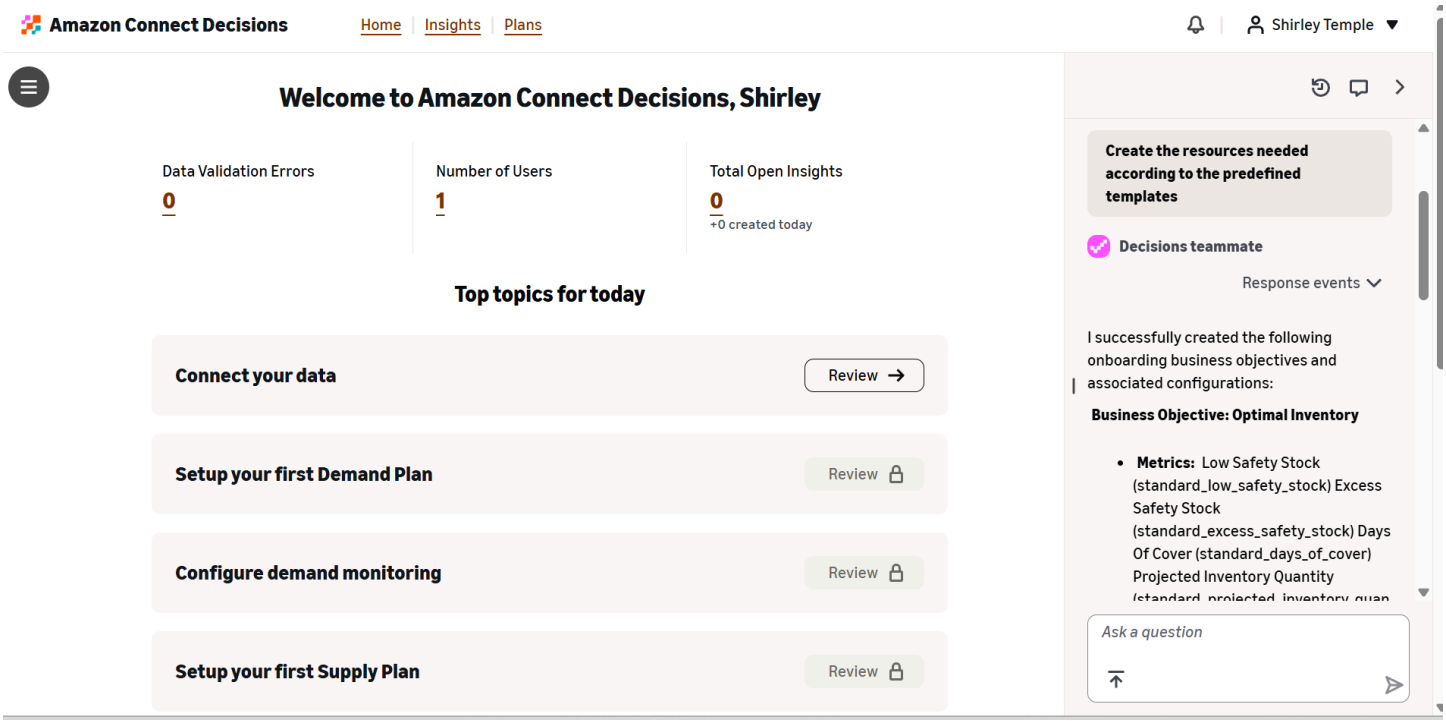
Après avoir rempli le questionnaire

Cliquez sur Soumettre après avoir effectué les quatre étapes :



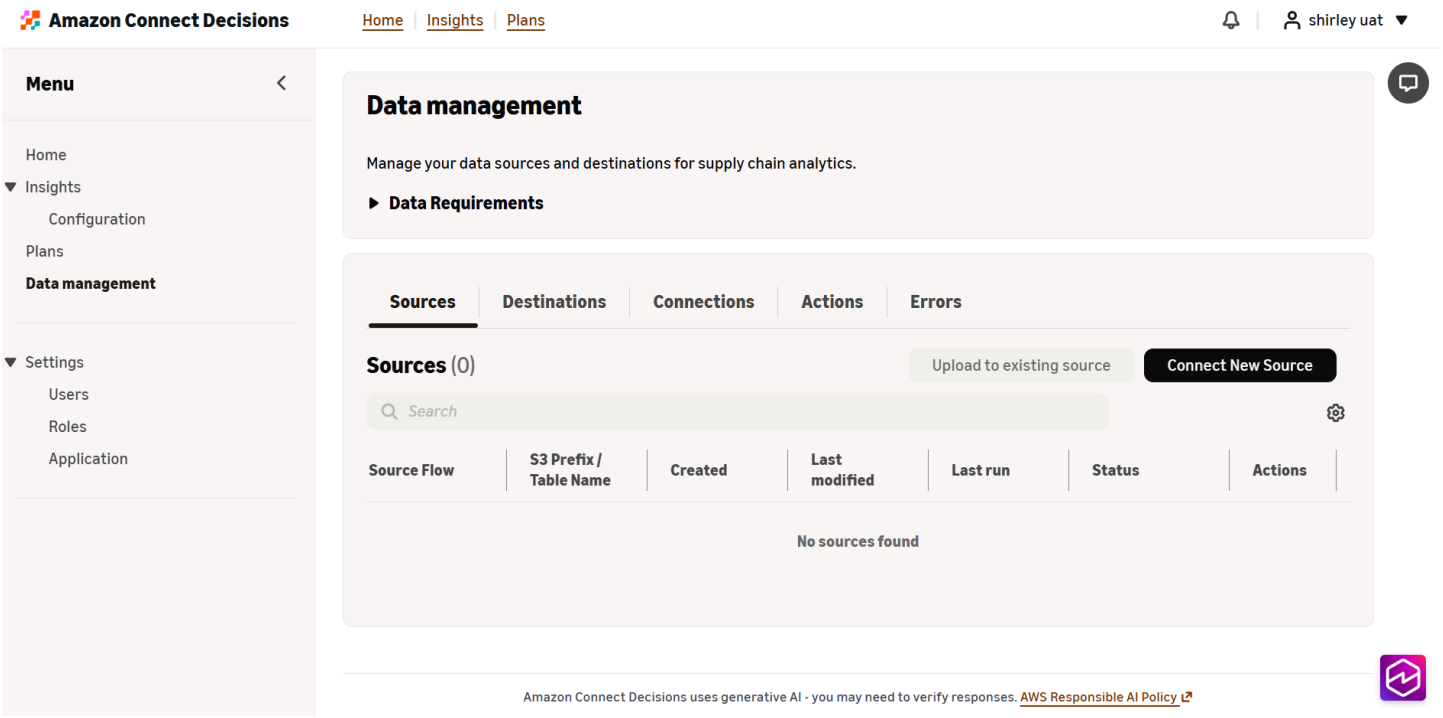
- Vous serez redirigé vers la page d'accueil avec un tableau de bord et des fiches thématiques conçues pour vous guider dans les étapes d'intégration restantes.

- Le système créera automatiquement des métriques et des règles dans l'application en fonction de vos sélections. Ils sont créés dans le statut Brouillon et ne sont pas immédiatement actifs.
- Vous pouvez consulter les mesures et règles créées automatiquement, puis les activer si elles répondent à vos besoins, ou créer vos propres mesures et règles adaptées aux besoins spécifiques de votre entreprise.



Création de votre premier flux source

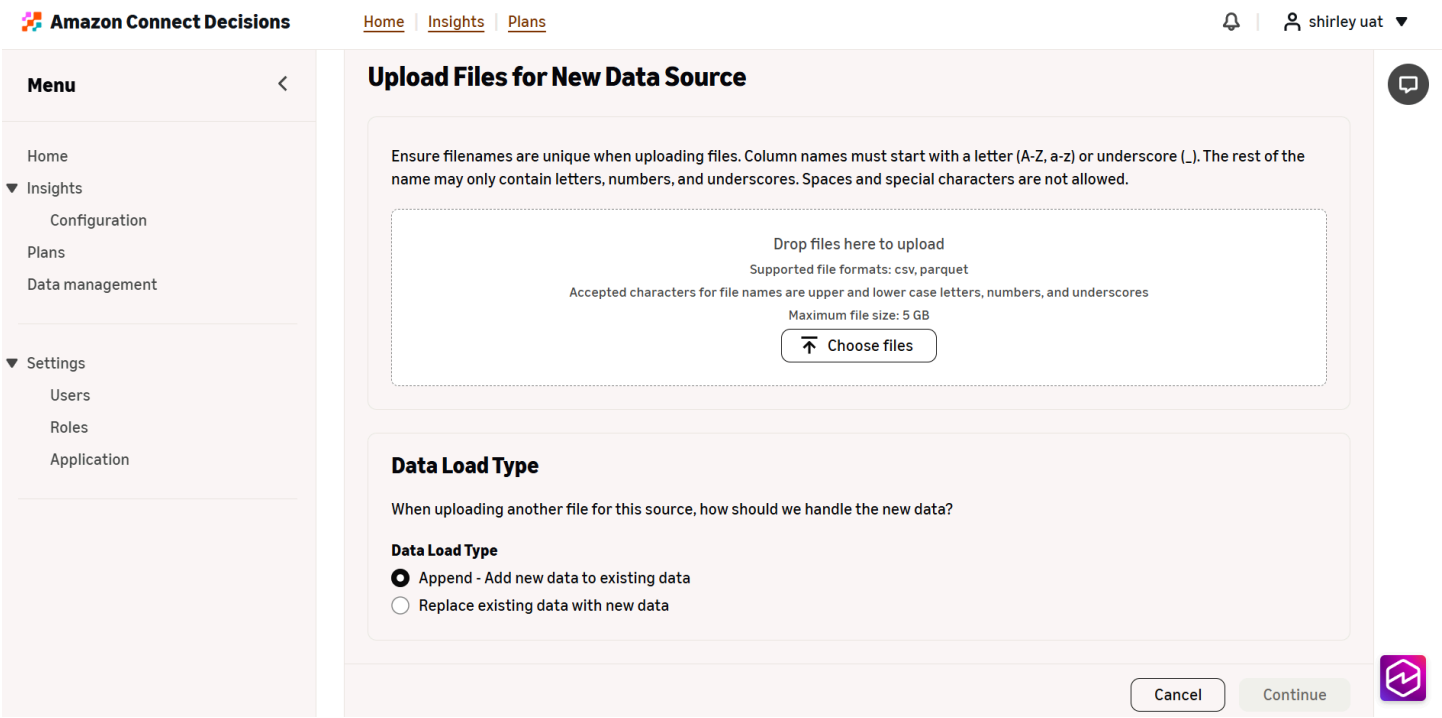
Pour commencer à intégrer vos données, cliquez sur Réviser pour la fiche thématique Connect your data ou accédez à l'onglet Gestion des données dans le « Menu Hamburger » d'Amazon Connect Decisions. Vous pouvez voir ici tous vos flux source existants. Si vous n'en avez pas encore configuré, cliquez sur « Connect New Source » pour commencer.



Téléchargez vos données sources

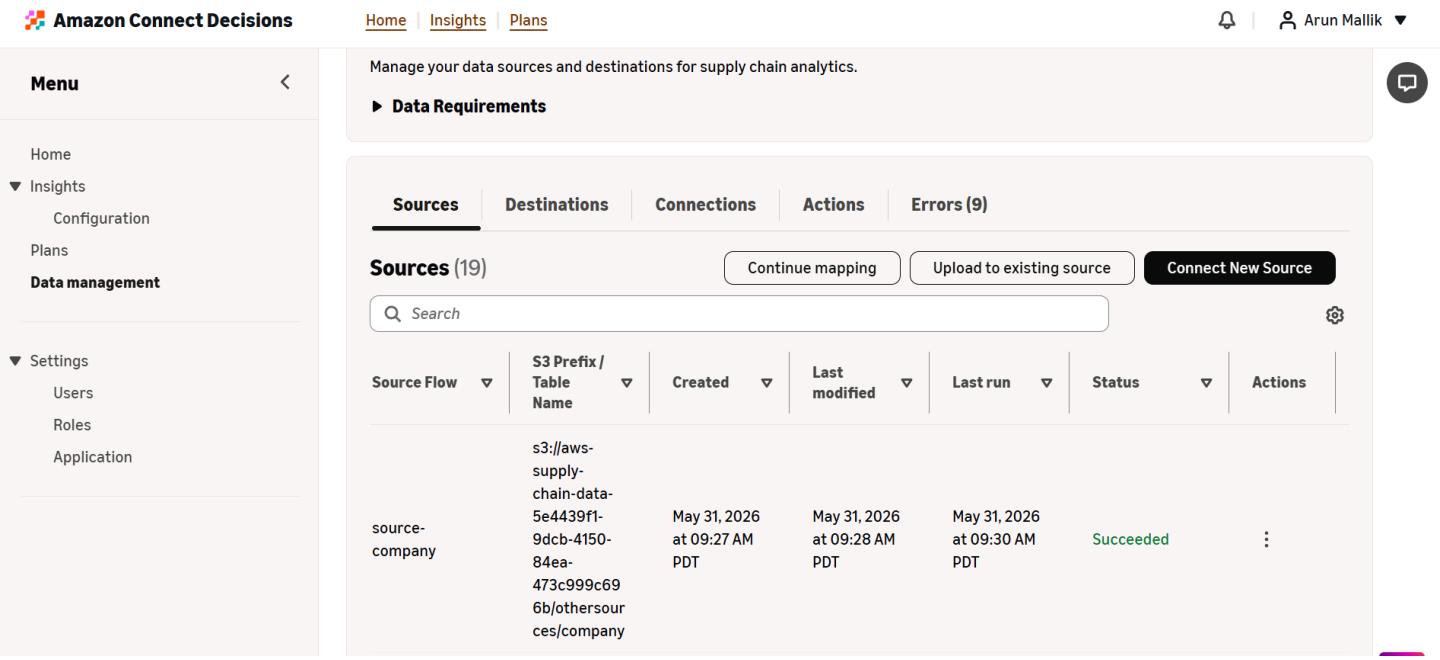
Téléchargez vos fichiers CSV contenant des données sources basées sur les tableaux CDM requis pour votre cas d'utilisation. Vous pouvez choisir la manière dont vous souhaitez gérer les mises à jour des données :

- Ajouter : ajouter de nouvelles données aux données existantes
- Remplacer : remplacer les données existantes par de nouvelles données



Lorsque vous chargez des fichiers, Amazon Connect Decisions crée automatiquement une structure de dossiers dans S3 pour ces données, notamment :

- Un dossier parent nommé d'après le système source que vous avez sélectionné
- Un sous-dossier nommé d'après le nom de la table source que vous avez sélectionnée
- Tous les fichiers d'un sous-dossier sont enregistrés dans la même table source
- Cette structure de fichier est également utilisée pour créer le chemin du dossier Amazon S3

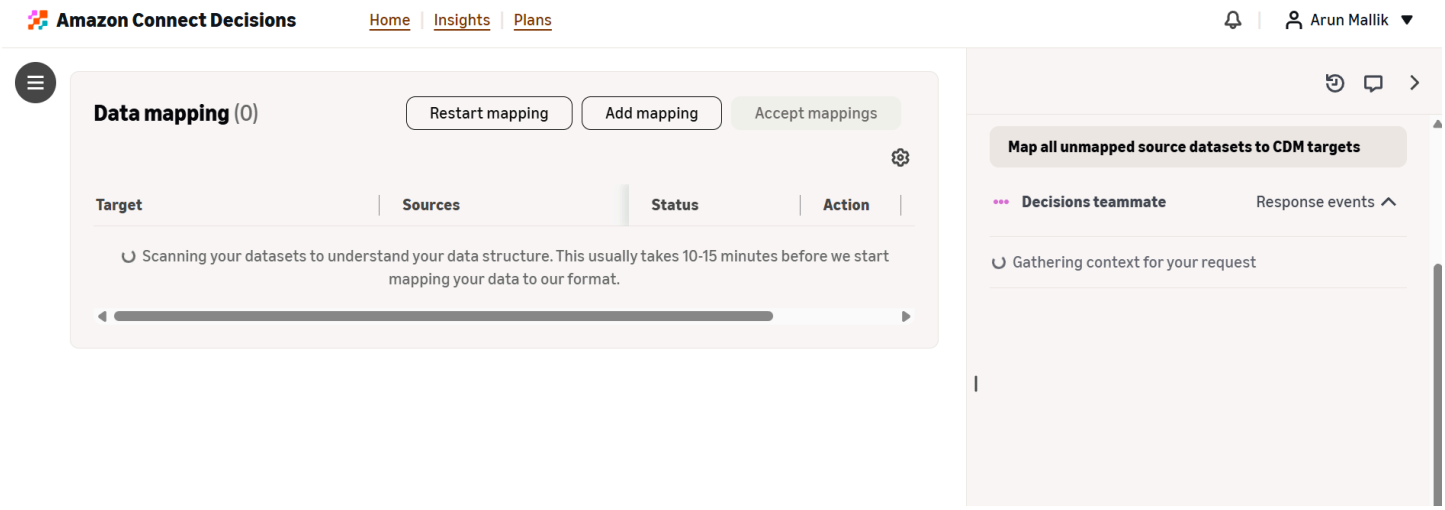


Source-to-CDM Cartographie des destinations

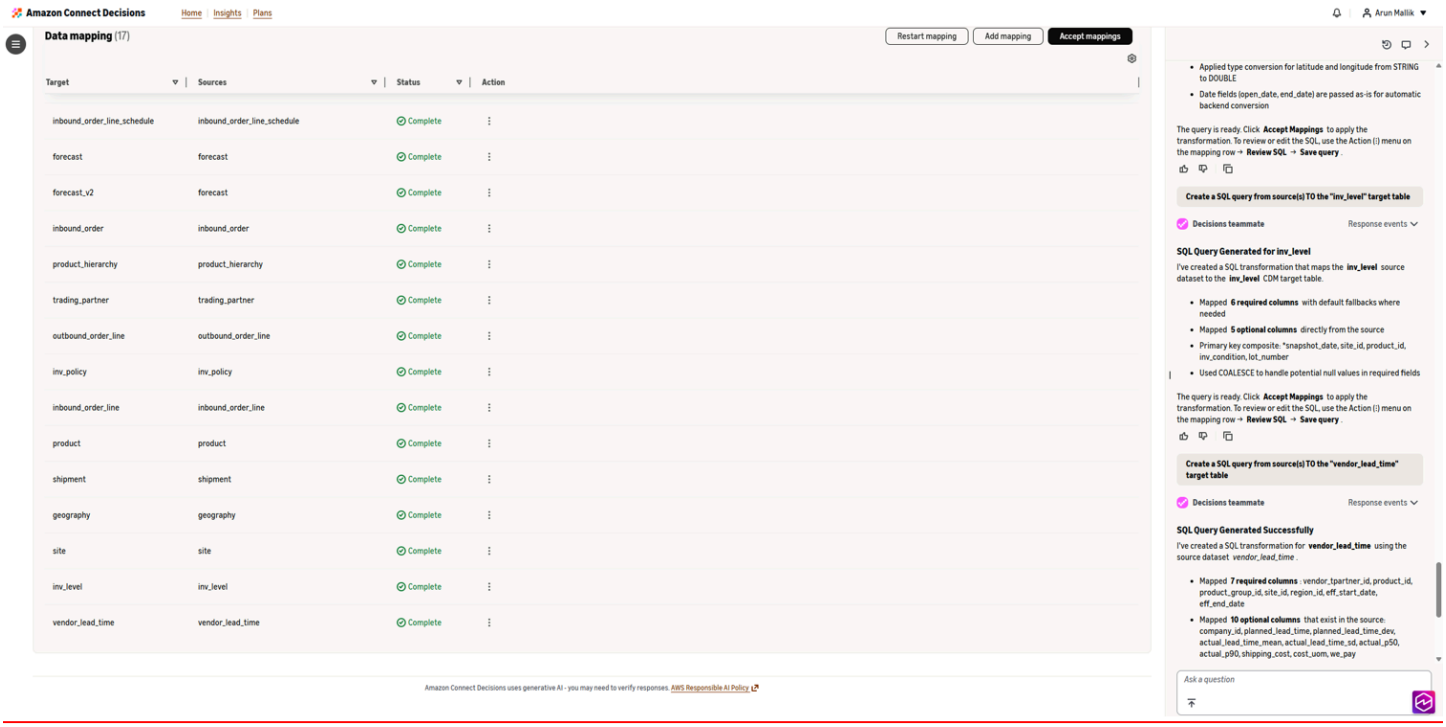
Une fois vos fichiers chargés, Amazon Connect Decisions commence à analyser vos données et à les mapper automatiquement à une ou plusieurs tables de destination CDM d'Amazon Connect Decisions.

À quoi s'attendre

- Cette étape peut prendre entre 10 et 15 minutes en fonction de la quantité de données téléchargées
- L'agent de données fonctionne en arrière-plan pour identifier les meilleurs ensembles de données de destination CDM pour vos données sources.
- Si vous quittez cette page, les mappages automatisés échoueront. Pendant que vous attendez, laissez l'onglet Amazon Connect Decisions and Data Management ouvert pour vous assurer que le mappage automatique est terminé.

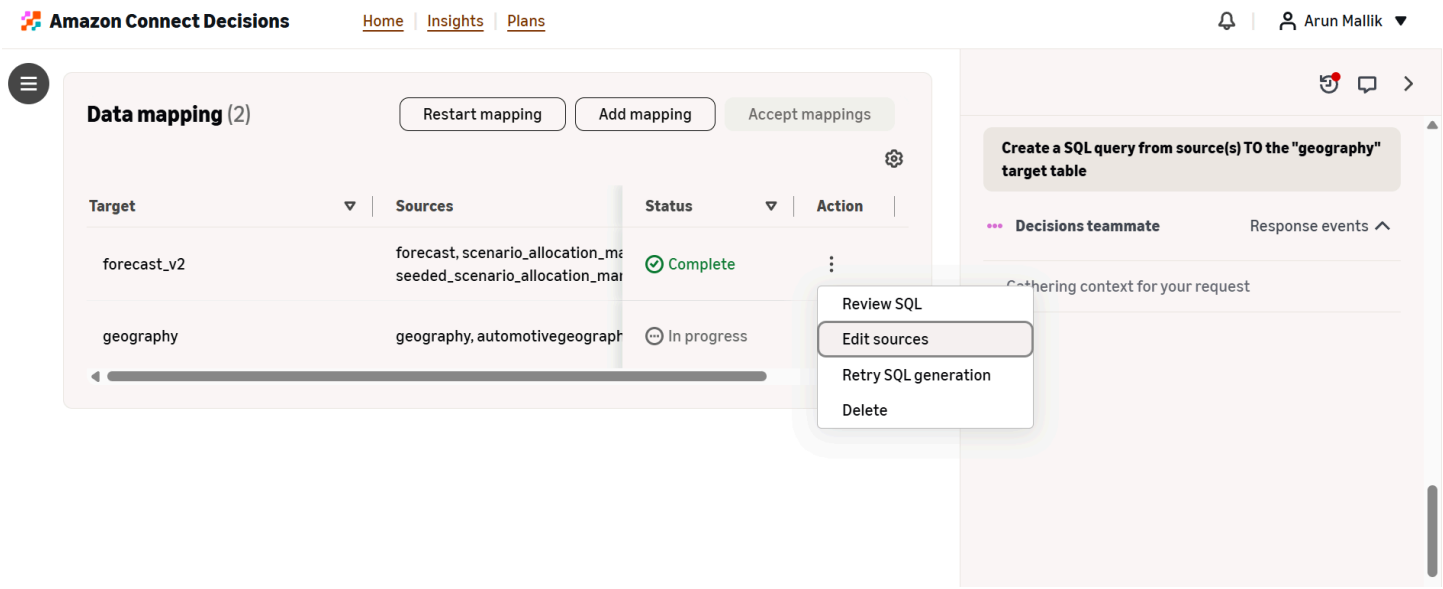


Une fois terminé, l'agent de données fournit une justification des mappages source-destination sur la base de données qui se chevauchent, que vous pouvez examiner et poser des questions à l'agent sur tous les résultats de mappage.



Pour consulter et modifier les mappages de sources, vous pouvez :

- Interagissez directement avec l'agent de données en langage naturel pour mettre à jour les mappages source-destination.
- Cliquez sur Actions et sélectionnez « Modifier les sources ».



Modification des mappages

À partir de là, vous pouvez :

- Mettez à jour le mappage de la source et de la destination manuellement si nécessaire
- Posez des questions à l'aide de l'agent de données situé sur le côté droit de l'écran pour confirmer les mappages
- Consultez les guides de l'utilisateur pour en savoir plus sur des ensembles de données spécifiques

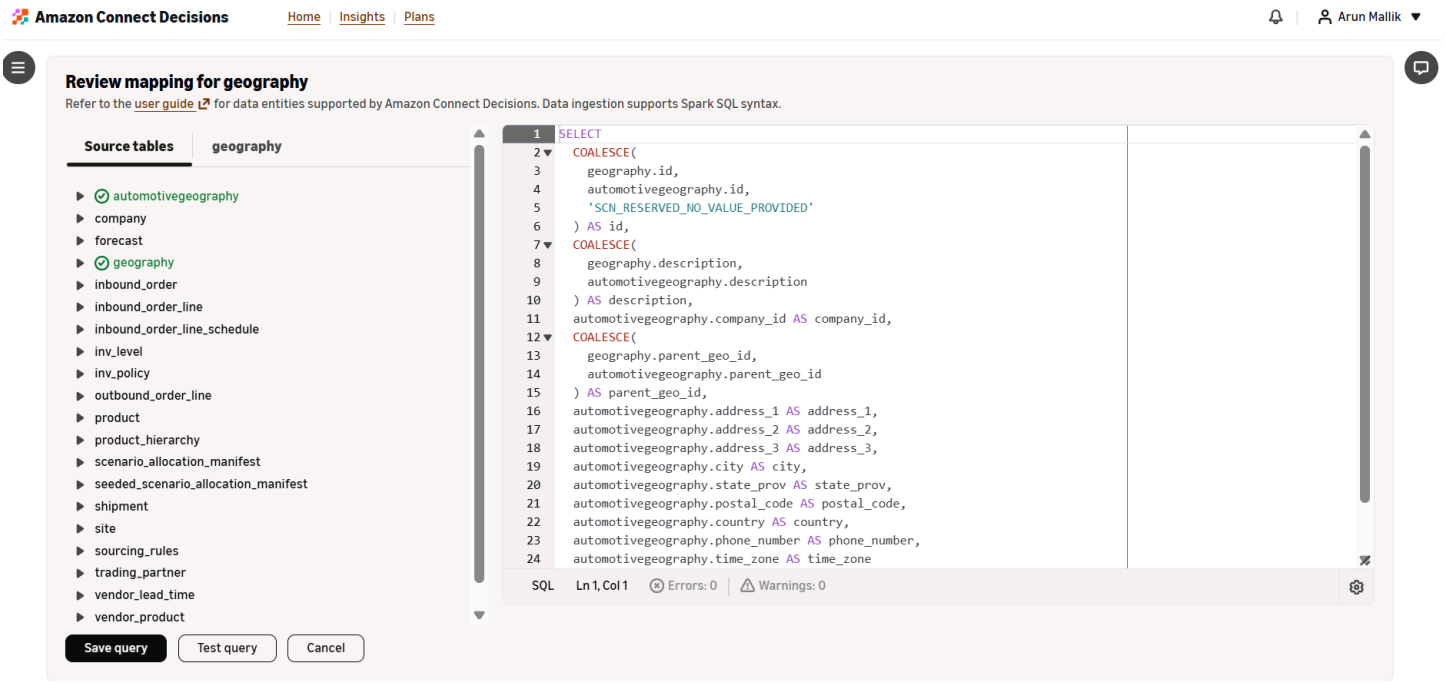
Column/Data Cartographie

Une fois le mappage source-destination terminé, Amazon Connect Decisions crée automatiquement des requêtes de transformation SQL depuis votre ensemble de données source vers la destination CDM. Une fois l'un de vos mappages terminé, vous recevrez une notification de l'agent de données détaillant le résultat du mappage.

À partir de là, vous devez examiner le code SQL généré pour les mappages en sélectionnant « Réviser le code SQL » dans le menu Action.

En examinant le mappage (SQL), vous verrez :

- Colonnes du jeu de données source que vous avez ajoutées
- Colonnes du tableau CDM de destination à titre de référence
- Le SQL de transformation qui les connecte
- Justification de la cartographie fournie par l'agent de données



Modification des mappages

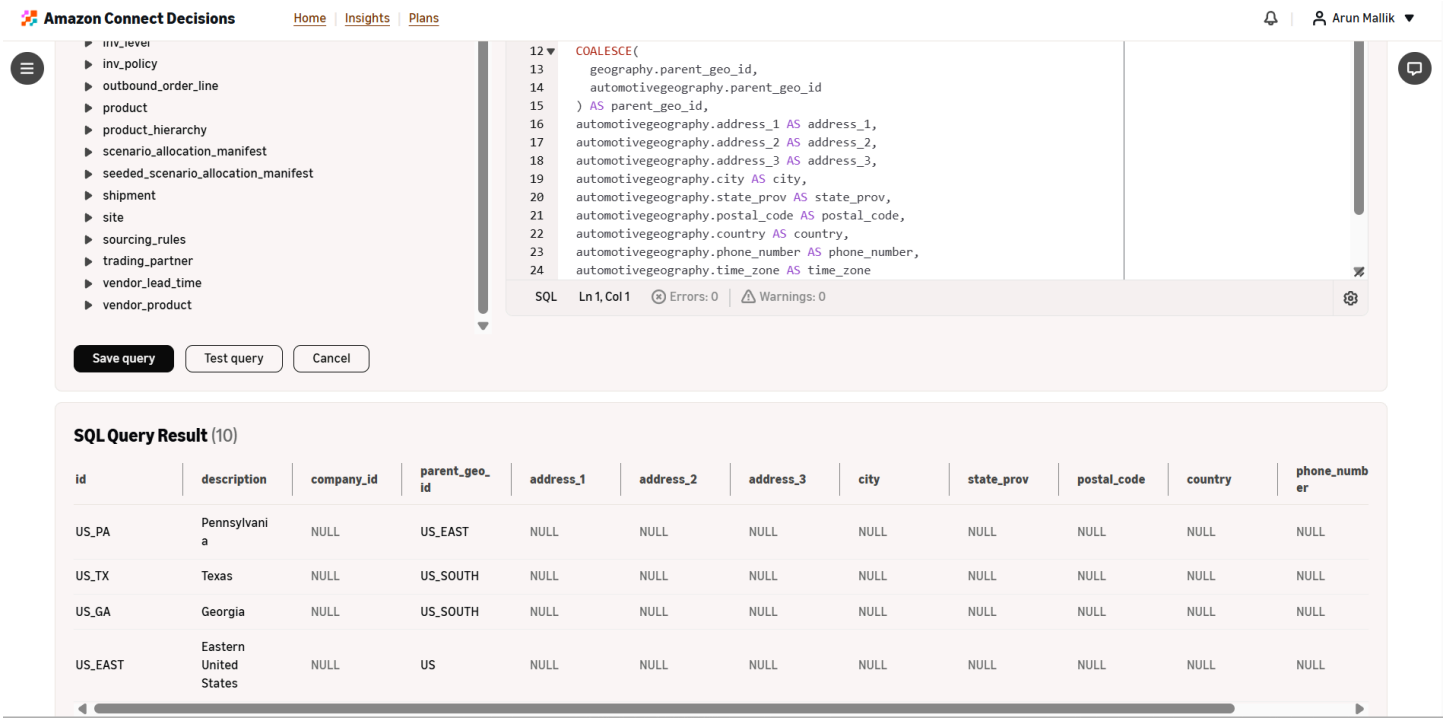
Deux options s'offrent à vous pour modifier les mappages :

- Utilisation de l'agent de données : utilisez le langage naturel pour poser des questions, gérer et mettre à jour les mappages
- Modifier directement le code SQL : si vous connaissez le langage SQL, vous pouvez modifier directement la requête

Tester vos modifications

Lorsque vous modifiez la requête de mappage, continuez à la tester à l'aide de la fonctionnalité « Test Query » qui vous donnera un aperçu défilant de la façon dont un échantillon de la façon dont vos données sont transformées en CDM de destination. Utilisez-le pour vous assurer que votre transformation s'exécute correctement et pour valider les mises à jour appropriées depuis votre CDM de la source vers la destination.

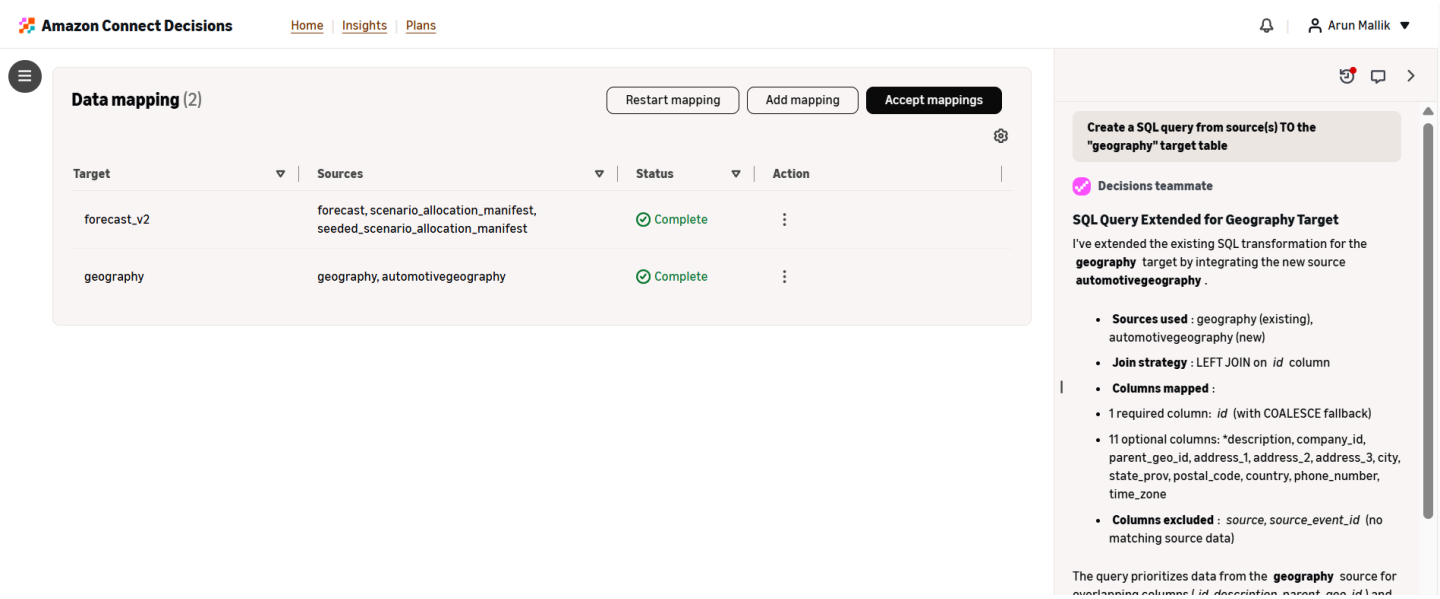
Une fois que vous êtes satisfait de la sortie de mappage, sélectionnez « Enregistrer la requête » pour enregistrer la requête de transformation pour cette paire source-destination.



Vérifier et accepter les mappages

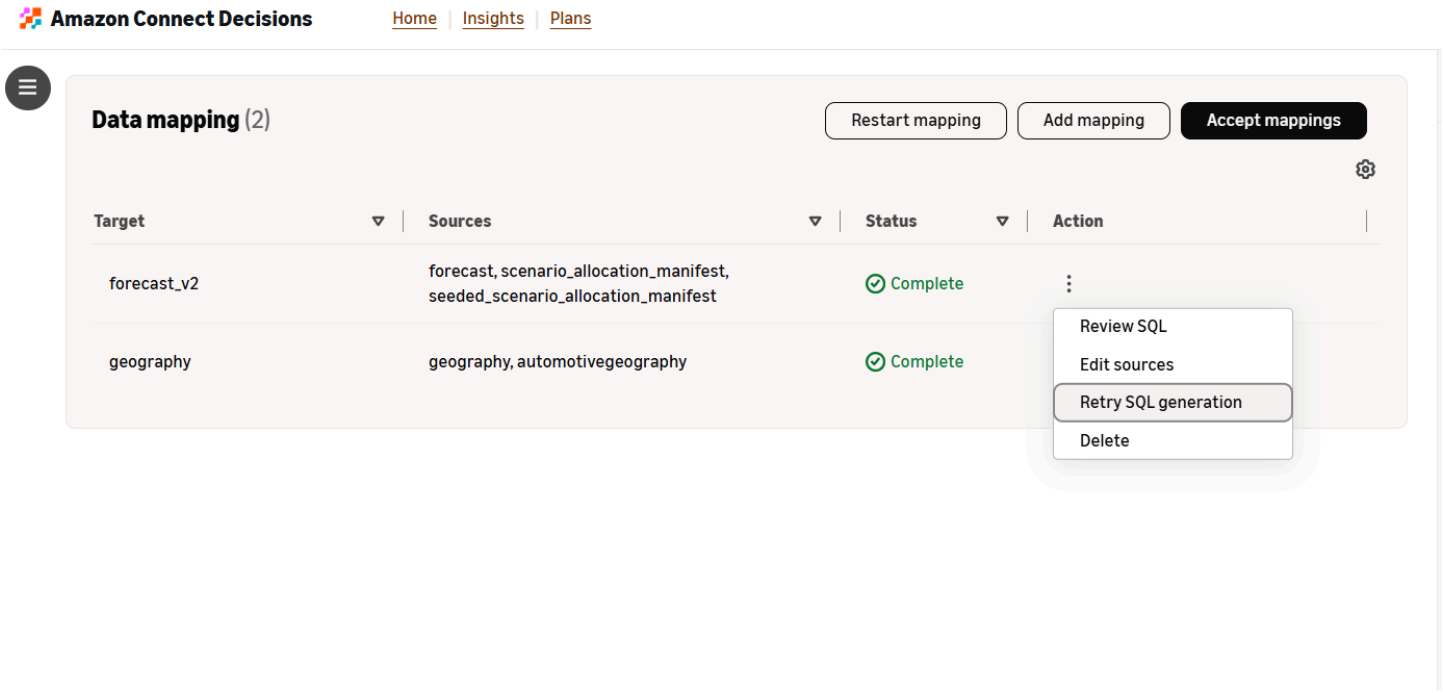
Passez en revue les mappages restants pour chacun de vos ensembles de données sources. L'agent de données reste présent sur le côté droit de l'écran pour répondre aux questions ou obtenir de l'aide pour résoudre les problèmes.

Une fois que vous êtes satisfait de tous les mappages, acceptez-les pour terminer l'intégration des données en cliquant sur Accepter les mappages.



Gérer les mappages ayant échoué

Si un mappage échoue, vous pouvez sélectionner « Redémarrer le mappage » pour redémarrer tous les mappages, ou réessayer manuellement un seul mappage dans le menu Actions via « Réessayer la génération SQL ». L'agent de données peut également réessayer les mappages en langage naturel et continuera à vous aider à identifier et à résoudre les problèmes si les erreurs persistent.

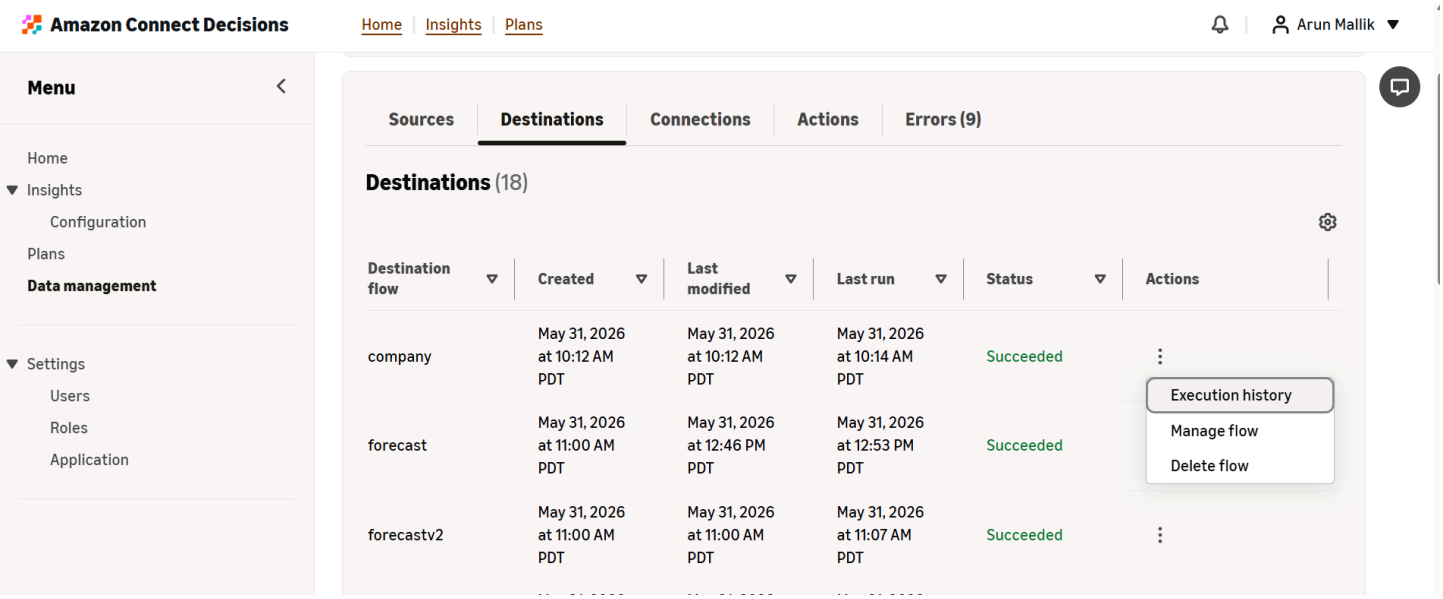


Surveillez vos flux

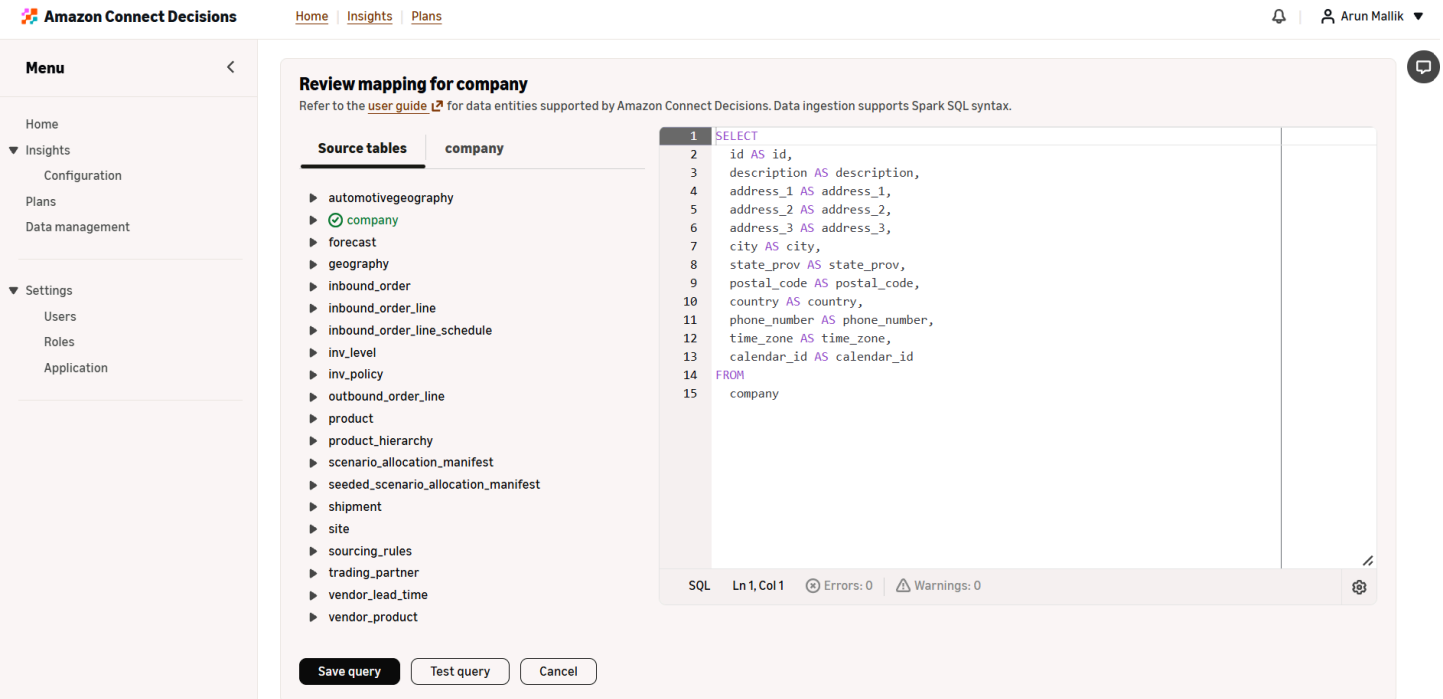
Onglet Destinations

Après avoir accepté les mappages, vous serez dirigé vers l'onglet Destinations de la gestion des données, où vous pourrez :

- Passez en revue les flux de destination
- Gérer et modifier les mappages (« Gérer le flux »)
- Supprimer les flux obsolètes
- Vérifiez l'état d'exécution de ces flux



La sélection de « Gérer le flux » vous ramènera à l'expérience de mappage des données, dans laquelle vous pourrez continuer à travailler avec l'agent de données pour affiner les mappages au fil du temps.



Onglet Sources

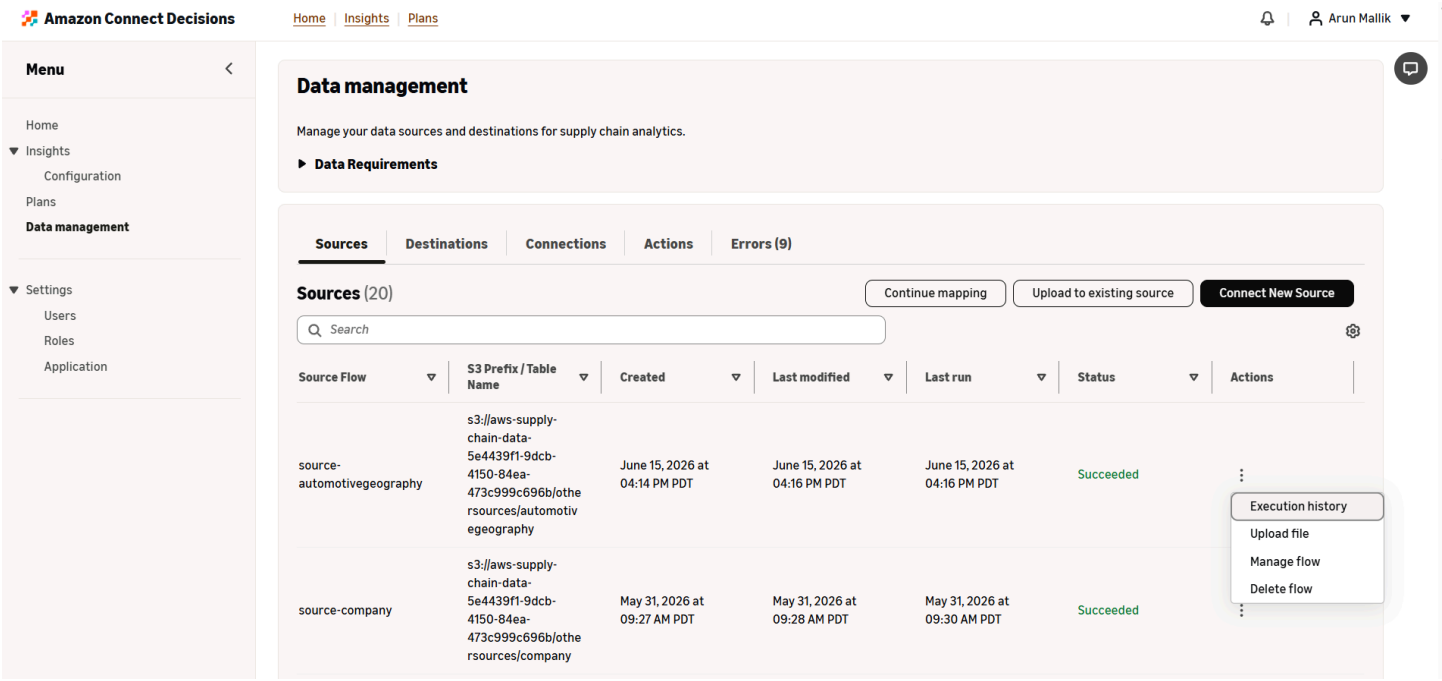
En revenant à l'onglet Sources, vous trouverez :

- Le jeu de données source qui a été créé

- Son compartiment S3 associé
- Options pour :
  - Ajouter des données sources supplémentaires via un autre téléchargement de fichier
  - Gérez le flux
  - Supprimer le flux
  - Examiner les exécutions

La sélection de « Gérer le flux » vous ramènera à l'expérience de mappage des données, dans laquelle vous pourrez continuer à travailler avec l'agent de données pour affiner les mappages au fil du temps.

Vous avez également accès à la fonction Créer une nouvelle source si nécessaire pour redémarrer le processus d'intégration des données pour toute nouvelle source de données.



Bonnes pratiques

Préparation des données

- Suivez les étapes décrites dans la section Prérequis
- Utiliser le UTF-8 codage pour tous les fichiers CSV
- Assurez-vous que les noms de fichiers sont uniques

- Valider la qualité des données avant de les télécharger

Utilisation de l'agent de données

- Soyez précis dans vos demandes
- Demandez des explications lorsque vous ne comprenez aucune de ses décisions
- Testez toutes les modifications SQL avant de les accepter
- Utilisez la fonction d'aperçu pour vérifier les transformations

Maintenance continue

- Maintenez vos données sources à jour
- Surveillez régulièrement l'exécution du flux
- Corrigez rapidement les erreurs de données dès qu'elles sont signalées
- Documentez les transformations personnalisées pour votre équipe

Connexion à votre base de données avec JDBC

Ce guide explique comment connecter votre base de données à Amazon Connect Decisions à l'aide de Java Database Connectivity (JDBC). Vous allez configurer un chiffrement sécurisé pour les informations d'identification de votre base de données et établir une connexion qu'Amazon Connect Decisions pourra utiliser pour accéder à vos données.

Qu'est-ce que la connexion JDBC et quand devriez-vous l'utiliser ?

La connexion JDBC permet à Amazon Connect Decisions de se connecter à votre base de données existante pour lire les données, au lieu de vous obliger à exporter et à télécharger des fichiers CSV ou à configurer vos propres pipelines d'extraction, de transformation, de chargement (ETL) vers S3. Cette approche est idéale lorsque :

- Vos données sont déjà stockées dans une base de données Glue-compatible relationnelle AWS. Consultez ce guide pour connaître les bases de données et les versions compatibles.
- Vous souhaitez accéder aux données en temps réel ou quasi réel sans exportation manuelle de fichiers
- Votre volume de données est important et fréquemment mis à jour

- Vous préférez conserver vos données à leur emplacement actuel plutôt que de les dupliquer
- Si vous travaillez avec des ensembles de données plus petits ou si vous préférez les téléchargements basés sur des fichiers, le processus de téléchargement CSV standard peut être plus simple pour répondre à vos besoins. Reportez-vous au guide de l'utilisateur sur l'intégration des données pour plus de détails sur ce processus.

Conditions préalables

Avant de commencer, assurez-vous de disposer des éléments suivants :

- Un compte AWS autorisé à créer des clés KMS et des ressources Secrets Manager
- Votre identifiant de compte AWS et la région dans laquelle Amazon Connect Decisions exercera ses activités
- Détails de connexion à la base de données : nom d'hôte, port, nom de base de données et informations d'identification
- Accès administratif à votre base de données pour vérifier la connectivité
- Votre base de données est configurée pour accepter les connexions depuis les services AWS

Création d'une clé Customer-Managed KMS

Avant de connecter votre base de données à Amazon Connect Decisions, vous devez configurer le chiffrement des informations d'identification de votre base de données. AWS Key Management Service (KMS) fournit cette couche de sécurité, garantissant ainsi la protection de vos informations de connexion.

Créez votre clé KMS

1. Accédez à la console AWS KMS
   - Ouvrez la console de gestion AWS dans votre navigateur
   - Dans la barre de recherche en haut, tapez « KMS » et sélectionnez « Key Management Service » dans les résultats
   - Cela ouvre le tableau de bord KMS dans lequel vous allez gérer les clés de chiffrement
2. Lancer la création de clés
   - Sur le tableau de bord KMS, recherchez et cliquez sur le bouton Créer une clé en haut à droite

- Cela lance l'assistant de création de clés qui vous guidera tout au long du processus de configuration

3. Configuration du type de clé et de son utilisation
   - Sur la page « Configurer la clé », sélectionnez Symétrique comme type de clé (il s'agit de l'option recommandée par défaut)
   - Gardez l'option « Chiffrer et déchiffrer » sélectionnée sous Utilisation des clés
4. Définissez les informations d'identification clés
   - Dans le champ « Alias », entrez un nom descriptif pour votre clé, tel que `aws-supply-chain-database-key`
   - Dans le champ « Description », ajoutez un contexte tel que « Clé de chiffrement pour les informations d'identification de la base de données Amazon Connect Decisions »
   - Ajoutez éventuellement des balises pour vous aider à organiser et à suivre vos ressources AWS (par exemple, clé : « Projet », valeur : « Amazon Connect Decisions »)
5. Définissez les principales autorisations administratives
   - Sélectionnez les utilisateurs ou les rôles IAM qui devraient être en mesure de gérer cette clé (créer, supprimer, modifier les politiques)
   - Incluez au minimum votre propre rôle d'administrateur pour pouvoir modifier la clé ultérieurement si nécessaire
   - Ces administrateurs peuvent gérer la clé mais ne seront pas automatiquement autorisés à l'utiliser pour encryption/decryption
   - Dans la section « Suppression de la clé », autorisez les administrateurs des clés à supprimer cette clé. (il s'agit de l'option par défaut et recommandée)
6. Définissez les autorisations d'utilisation clés
   - Sur cette page, vous verrez des options permettant de sélectionner les utilisateurs et les rôles IAM autorisés à utiliser la clé
   - Ignorez la sélection d'utilisateurs spécifiques ici, vous configurerez les autorisations de service à l'étape suivante
7. Configuration de la politique clé pour les services Amazon Connect Decisions
   - Vous verrez un éditeur de politiques avec le JSON par défaut
   - Dans l'éditeur de politique de clés KMS, ajoutez l'instruction suivante à votre tableau « Statement » existant

- Cette politique accorde à votre compte un contrôle total et permet aux services d'Amazon Connect Decisions (Secrets Manager et Glue) de déchiffrer les informations d'identification de votre base de données

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

8. Réviser et finaliser
   - Vérifiez tous vos paramètres de configuration sur la page de résumé
   - Vérifiez que votre alias, votre description et votre politique sont corrects
   - Cliquez sur Terminer pour créer la clé
   - Une fois créée, vous serez redirigé vers le tableau de bord KMS où votre nouvelle clé apparaîtra dans la liste

À quoi s'attendre

La création des clés est immédiate. Une fois créée, votre nouvelle clé sera répertoriée dans la console KMS avec le statut « Activé ». La clé est maintenant prête à chiffrer les informations d'identification de votre base de données dans Secrets Manager.

Configuration d'AWS Secrets Manager

Maintenant que vous disposez d'une clé KMS, vous allez créer un secret dans AWS Secrets Manager pour stocker en toute sécurité les informations d'identification de votre base de données, puis configurer une politique de ressources qui autorise Amazon Connect Decisions à accéder à ce secret.

Créez votre secret

1. Accédez à AWS Secrets Manager
   - Dans la barre de recherche de l'AWS Management Console, saisissez « Secrets Manager »
   - Sélectionnez « Secrets Manager » dans les résultats pour ouvrir le tableau de bord du service
2. Commencez à créer un nouveau secret
   - Cliquez sur le bouton Enregistrer un nouveau secret
   - Sur la page « Choisir le type de secret », sélectionnez Autre type de secret (cela vous donne la flexibilité de structurer vos informations d'identification)
3. Entrez vos informations d'identification de base de données
   - Dans la section paires clé-valeur, ajoutez les détails de votre connexion à la base de données sous forme de chaînes :

```
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. Sélectionnez votre clé de chiffrement
   - Sous « Clé de chiffrement », sélectionnez Choisir une clé AWS KMS
   - Dans le menu déroulant, sélectionnez la clé KMS que vous avez créée à l'étape 1 (par exemple,`aws-supply-chain-database-key`)
   - Cela garantit que vos informations d'identification sont cryptées avec votre clé gérée par le client
5. Donnez un nom à votre secret
   - Entrez un nom descriptif pour votre secret, tel que `aws-supply-chain-production-database`
   - Ajoutez éventuellement une description telle que « Informations d'identification de base de données pour l'environnement de production Amazon Connect Decisions »
   - Ajoutez des balises si vous le souhaitez pour l'organisation (par exemple, clé : « environnement », valeur : « production »)
6. Ajouter des autorisations sur les ressources
   - Cliquez sur « Modifier les autorisations ». Dans l'éditeur de stratégie, collez la politique suivante. Cette politique permet aux services d'Amazon Connect Decisions de lire votre secret

```
{
  "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. Enregistrez la politique
   - Cliquez sur Enregistrer pour appliquer la politique de ressources
   - La politique est désormais active et permet à Amazon Connect Decisions de récupérer les informations d'identification de votre base de données
8. Configurer la rotation (facultatif)
   - Pour cette configuration, vous pouvez ignorer la rotation automatique en sélectionnant Désactiver la rotation automatique
   - Vous pouvez activer la rotation ultérieurement si vos politiques de sécurité l'exigent.
9. Vérifier et créer
   - Passez en revue tous vos détails secrets
   - Cliquez sur Store pour créer le secret
   - Vous serez redirigé vers le tableau de bord de Secrets Manager
10. Enregistrez votre ARN secret
    - Trouvez le secret que vous venez de créer dans la liste des secrets
    - Cliquez sur le nom du secret pour ouvrir sa page de détails
    - En haut, vous verrez l'ARN secret
    - Copiez et enregistrez cet ARN
    - Le format ARN ressemble à ceci : `arn:aws:secretsmanager:us-east-1:123456789012:secret:aws-supply-chain-production-database-AbCdEf`
11. Modifier les autorisations relatives aux ressources
    - Cliquez sur « Modifier les autorisations »

- Collez l'ARN secret copié et remplacez-le <COPY-THE-SECRET-ARN-HERE-AFTER-CREATING> par votre ARN copié
- Cliquez sur Enregistrer pour joindre la politique

À quoi s'attendre

Votre secret est désormais stocké en toute sécurité et crypté avec votre clé KMS. Les services d'Amazon Connect Decisions sont autorisés à récupérer les informations d'identification lors de l'établissement d'une connexion à la base de données, mais les informations d'identification restent cryptées au repos et en transit.

Connectez votre base de données à Amazon Connect Decisions

Une fois votre clé et votre secret KMS configurés, vous êtes prêt à établir la connexion JDBC dans Amazon Connect Decisions.

Configurez votre connexion JDBC

1. Accédez à Amazon Connect Decisions > Gestion des données
   - Connectez-vous à votre instance Amazon Connect Decisions
   - Dans la navigation principale, sélectionnez « Gestion des données »
   - Dans l'onglet de navigation, accédez à « Connexions »
   - Sélectionnez « Nouvelle connexion » pour créer une nouvelle connexion
2. Entrez vos informations de connexion
   - Nom de la connexion (obligatoire) : entrez un identifiant unique pour cette connexion (par exemple, « base de données de production »)
   - Description (facultatif) : Ajoutez des détails sur l'objectif et l'utilisation de cette connexion pour aider votre équipe à comprendre à quelles données elle accède
   - URL JDBC (obligatoire) : Entrez votre chaîne de connexion JDBC complète au format : `jdbc:<database-type>://<hostname>:<port>/<database>` (par exemple,) `jdbc:postgresql://db.example.com:5432/mydb`
   - Nom du schéma (facultatif) : Spécifiez le schéma de base de données si nécessaire (par exemple, « public », « dbo », « myschema »). Laissez ce champ vide pour utiliser le schéma par défaut de votre base de données

- ARN secret (obligatoire) : collez l'ARN secret que vous avez enregistré à l'étape 2. Cela permet à Amazon Connect Decisions de récupérer en toute sécurité les informations d'identification de votre base de données auprès de Secrets Manager.
- Appliquer la connexion SSL : maintenez cette case cochée (recommandé) pour exiger le SSL/TLS chiffrement de votre connexion à la base de données
- Nom du service de point de terminaison VPC (obligatoire) : entrez le nom de votre service de point de terminaison VPC pour une connectivité privée via AWS PrivateLink (format :) `com.amazonaws.vpce.<region>.vpce-svc-xxxxxxxxx`

3. Connect à votre base de données
   - Cliquez sur « Connect » pour tester et établir la connexion. Amazon Connect Decisions vérifiera qu'il peut se connecter correctement à votre base de données à l'aide des informations d'identification fournies. Cette étape peut prendre jusqu'à 2 minutes. Veuillez donc ne pas quitter cet écran pendant la connexion.
   - Si la connexion aboutit, vous serez automatiquement dirigé vers la sélection de la table
   - En cas d'échec de la connexion :
     - Vérifiez vos informations de connexion pour vous assurer que tous les champs sont exacts :
       - Vérifiez que votre ARN secret est correct
       - Vérifiez que les informations d'identification de votre base de données sont exactes
       - Vérifiez que le format de votre URL JDBC est correct
       - Assurez-vous que votre base de données est configurée pour accepter les connexions provenant des services AWS
       - Vérifiez que votre clé KMS et les politiques de Secrets Manager sont correctement configurées
     - Vous pouvez également utiliser l'expérience de chat pour résoudre les problèmes de connexion en posant des questions telles que « Pourquoi ma connexion à la base de données échoue-t-elle ? » ou « Aidez-moi à déboguer ma connexion JDBC »
4. Sélectionnez les tables à ingérer
   - Une fois connecté, vous verrez l'écran Select Tables affichant toutes les tables disponibles dans votre base de données
   - Cochez la case à côté de chaque table que vous souhaitez ingérer
5. Configurer le calendrier d'actualisation des tables
   - Pour chaque tableau sélectionné, cliquez sur le menu à trois points dans la colonne Action et sélectionnez « Planifier l'actualisation »

- Dans la boîte de dialogue Configurer les détails du chargement, définissez :
  - Cadence : fréquence d'actualisation (horaire, quotidienne, hebdomadaire ou personnalisée)
  - Heure de début : heure à laquelle l'actualisation doit commencer (affichée en UTC avec le décalage de votre fuseau horaire)
  - Type d'actualisation : choisissez Actualisation complète (remplacement de toutes les données) ou Mise à jour incrémentielle (ajout de nouvelles données aux données existantes ; nécessite la sélection d'une colonne d'horodatage des enregistrements)
  - Répétez l'opération pour chaque table selon les besoins
- Cliquez sur Démarrer le mappage lorsque toutes les tables sont configurées

6. Poursuivre le mappage des données
   - À partir de maintenant, l'expérience est identique à celle de notre flux d'onboarding des données
   - Suivez la section Cartographie des données du guide de l'utilisateur sur l'intégration des données pour terminer votre configuration

À quoi s'attendre

Une fois votre connexion établie et les tables sélectionnées, Amazon Connect Decisions peut lire les données de votre base de données. La connexion reste active et sécurisée, les informations d'identification étant cryptées et gérées via AWS Secrets Manager. Vous n'avez pas besoin de mettre à jour manuellement les informations d'identification dans Amazon Connect Decisions, toutes les modifications que vous apportez dans Secrets Manager seront automatiquement prises en compte.

Bonnes pratiques

Gestion de la sécurité et des accès

- Stockez les informations d'identification en toute sécurité : utilisez toujours AWS Secrets Manager pour stocker les informations d'identification de base de données, ne les codez jamais en dur dans des chaînes de connexion ou des fichiers de configuration
- Activer le SSL/TLS chiffrement : maintenez l'option « Appliquer la connexion SSL » activée pour vous assurer que les données sont cryptées pendant le transfert
- Passez régulièrement en revue les politiques de KMS et de Secrets Manager : assurez-vous que seuls les services et comptes autorisés ont accès à vos clés de chiffrement et à vos secrets

- Utiliser l'accès avec le moindre privilège : accordez uniquement les autorisations minimales nécessaires aux utilisateurs de la base de données qu'Amazon Connect Decisions utilisera pour les connexions

Configuration de connexion

- Utilisez des noms de connexion descriptifs : choisissez des noms clairs et significatifs qui indiquent l'environnement et le but (par exemple, « production-inventory-db » plutôt que « db1 »)
- Documentez vos connexions : utilisez le champ Description pour noter les données auxquelles la connexion accède, son propriétaire et toute considération particulière
- Testez les connexions avant de continuer : vérifiez toujours que votre connexion fonctionne avant de sélectionner des tables et de configurer des programmes d'actualisation
- Validez le format d'URL JDBC : la syntaxe de Double-check votre URL JDBC correspond au type de votre base de données pour éviter les erreurs de connexion

Stratégie d'actualisation des données

- Choisissez la cadence d'actualisation appropriée : sélectionnez la fréquence d'actualisation en fonction de la fréquence à laquelle vos données sources changent et des besoins de votre entreprise
- Planifiez des actualisations pendant les périodes de faible activité : configurez les heures d'actualisation lorsque la charge de votre base de données est plus faible afin de minimiser l'impact sur les performances
- Utilisez des mises à jour incrémentielles lorsque cela est possible : pour les grands ensembles de données soumis à des modifications fréquentes, les mises à jour incrémentielles sont plus efficaces que les actualisations complètes
- Sélectionnez des colonnes d'horodatage significatives : lorsque vous utilisez des mises à jour incrémentielles, choisissez des colonnes qui reflètent précisément le moment où les enregistrements ont été créés ou modifiés

Utilisation du chat pour résoudre les problèmes

- Soyez précis dans vos demandes : fournissez un contexte clair lorsque vous demandez de l'aide pour résoudre des problèmes de connexion ou de mappage

- Demandez des explications : si vous ne comprenez pas les recommandations ou les requêtes SQL générées, demandez des éclaircissements
- Testez toutes les modifications SQL avant de les accepter : utilisez la fonction d'aperçu pour vérifier que les transformations fonctionnent comme prévu avec vos données réelles
- Utilisez le chat pour résoudre les problèmes : lorsque les connexions échouent ou que les actualisations rencontrent des erreurs, posez des questions de diagnostic telles que « Pourquoi ma connexion échoue-t-elle ? » ou « Aidez-moi à comprendre cette erreur d'actualisation »

Maintenance continue

- Surveillez régulièrement l'exécution des actualisations : vérifiez les onglets Destinations et Sources dans la gestion des données pour vous assurer que les actualisations se terminent correctement
- Corrigez rapidement les erreurs : lorsqu'Amazon Connect Decisions vous alerte en cas d'échec d'actualisation, étudiez et résolvez rapidement les problèmes afin d'éviter les lacunes dans les données
- Mettez à jour les informations d'identification en toute sécurité : lorsque les mots de passe de base de données changent, mettez-les à jour dans AWS Secrets Manager, Amazon Connect Decisions utilisera automatiquement les nouvelles informations d'identification
- Documentez les configurations personnalisées : notez les calendriers d'actualisation spéciaux, la logique de transformation ou les exigences de connexion à des fins de référence pour votre équipe
- Passez régulièrement en revue les sélections de tables : au fur et à mesure de l'évolution de vos besoins en données, revoyez les tables que vous ingérez et vérifiez si les calendriers d'actualisation répondent toujours aux exigences de l'entreprise

Comprendre le modèle de données canonique (CDM)

Le modèle de données canonique (CDM) est la structure de données standardisée utilisée par. Lorsque vous intégrez les données de votre chaîne d'approvisionnement, elles doivent être transformées au format CDM afin de pouvoir les traiter à des fins de planification, de prévision et d'informations opérationnelles.

Cette rubrique explique ce qu'est le CDM, pourquoi il est important et quelles entités de données sont disponibles.

Qu'est-ce que le MDP ?

Le CDM définit un ensemble commun d'entités de données et de champs qui représentent des concepts de chaîne d'approvisionnement tels que les produits, les sites, les commandes, les expéditions et les stocks. Quel que soit le format ou la structure de vos données sources, le CDM fournit un schéma unique et cohérent qui utilise toutes ses fonctionnalités.

Lors de l'intégration des données, vos données sources sont mappées aux tables de destination CDM. L'agent de données peut automatiquement suggérer des mappages entre vos champs source et vos champs CDM, et générer des requêtes de transformation SQL pour convertir vos données.

Pourquoi le MDP est important

- Cohérence — Toutes les fonctionnalités fonctionnent sur la même structure de données, ce qui garantit un comportement uniforme en matière de planification de la demande, d'optimisation des stocks et d'analyse des délais.
- Interopérabilité — Les données provenant de différents systèmes sources (ERP, WMS, TMS) sont normalisées dans un modèle unique, ce qui permet une analyse intersystème.
- Intégration simplifiée : l'agent de données utilise le CDM comme schéma cible lors de la génération de mappages automatisés, ce qui réduit les efforts manuels.
- Qualité des données — Les contrôles de validation sont exécutés par rapport aux définitions du CDM pour détecter les problèmes avant que les données ne soient utilisées en production.

Catégories d'entités de données

Les entités de données CDM se répartissent en deux catégories :

- Non-transactional données : données de référence ou de référence qui changent rarement, telles que les produits, les sites, les partenaires commerciaux et les zones géographiques.
- Données transactionnelles : données opérationnelles qui changent fréquemment, telles que les prévisions, les niveaux de stock, les commandes et les expéditions.

Entités de données prises en charge

Le tableau suivant répertorie toutes les entités de données prises en charge dans le CDM.

Entités de données CDM prises en charge

Entité de données	Type de données	Obligatoire
Société	Non-transactional données	Oui
Produit (langue française non garantie)	Non-transactional données	Oui
Partenaire commercial	Non-transactional données	Oui
Produit du fournisseur	Non-transactional données	Oui
Géographie	Non-transactional données	Oui
Hiérarchie des produits	Non-transactional données	Oui
Voie de transport	Non-transactional données	Oui
Délai de livraison du fournisseur	Non-transactional données	Oui
Site	Non-transactional données	Oui
Vacances du vendeur	Non-transactional données	Oui
Forecast	Données transactionnelles	Oui
Inventory	Données transactionnelles	Oui
Commande entrante () PO/STO	Données transactionnelles	Oui
Ligne de commande sortante	Données transactionnelles	Oui
Expédition	Données transactionnelles	Oui
Politique d'inventaire	Données transactionnelles	Oui
Ligne de commande entrante () PO/STO	Données transactionnelles	Oui

Entité de données	Type de données	Obligatoire
Expédition sortante	Données transactionnelles	Oui
Calendrier des lignes de commande entrantes	Données transactionnelles	Oui

Entités requises par fonctionnalité

Toutes les fonctionnalités de ne nécessitent pas toutes les entités CDM. Les sections suivantes décrivent les entités obligatoires, facultatives ou non applicables pour chaque fonctionnalité.

Visibilité de l'inventaire

Entités CDM pour la visibilité des stocks

Entité de données	Type de données	Obligatoire
Société	Non-transactional	Facultatif
Produit (langue française non garantie)	Non-transactional	Oui
Partenaire commercial	Non-transactional	Facultatif
Produit du fournisseur	Non-transactional	Non applicable
Géographie	Non-transactional	Facultatif
Hiérarchie des produits	Non-transactional	Facultatif
Voie de transport	Non-transactional	Facultatif
Délai de livraison du fournisseur	Non-transactional	Non applicable
Site	Non-transactional	Oui
Vacances du vendeur	Non-transactional	Non applicable

Entité de données	Type de données	Obligatoire
Forecast	Transactionnel	Facultatif
Inventory	Transactionnel	Oui
Commande entrante () PO/ STO	Transactionnel	Facultatif
Ligne de commande sortante	Transactionnel	Facultatif
Expédition	Transactionnel	Facultatif
Politique d'inventaire	Transactionnel	Oui
Ligne de commande entrante	Transactionnel	Facultatif
Expédition sortante	Transactionnel	Facultatif
Calendrier des lignes de commande entrantes	Transactionnel	Facultatif

Informations sur les délais

Entités CDM pour des informations sur les délais

Entité de données	Type de données	Obligatoire
Société	Non-transactional	Facultatif
Produit (langue française non garantie)	Non-transactional	Oui
Partenaire commercial	Non-transactional	Oui
Produit du fournisseur	Non-transactional	Oui
Géographie	Non-transactional	Facultatif
Hiérarchie des produits	Non-transactional	Facultatif

Entité de données	Type de données	Obligatoire
Voie de transport	Non-transactional	Oui
Délai de livraison du fournisseur	Non-transactional	Oui
Site	Non-transactional	Oui
Vacances du vendeur	Non-transactional	Facultatif
Forecast	Transactionnel	Non applicable
Inventory	Transactionnel	Non applicable
Commande entrante () PO/STO	Transactionnel	Oui
Ligne de commande sortante	Transactionnel	Non applicable
Expédition	Transactionnel	Oui
Politique d'inventaire	Transactionnel	Non applicable
Ligne de commande entrante	Transactionnel	Oui
Expédition sortante	Transactionnel	Non applicable
Calendrier des lignes de commande entrantes	Transactionnel	Oui

Planification de la demande

Entités CDM pour la planification de la demande

Entité de données	Type de données	Obligatoire
Société	Non-transactional	Facultatif

Entité de données	Type de données	Obligatoire
Produit (langue française non garantie)	Non-transactional	Oui
Partenaire commercial	Non-transactional	Non applicable
Produit du fournisseur	Non-transactional	Non applicable
Géographie	Non-transactional	Facultatif
Hiérarchie des produits	Non-transactional	Facultatif
Voie de transport	Non-transactional	Non applicable
Délai de livraison du fournisseur	Non-transactional	Non applicable
Site	Non-transactional	Oui
Vacances du vendeur	Non-transactional	Non applicable
Forecast	Transactionnel	Non applicable
Inventory	Transactionnel	Non applicable
Commande entrante () PO/STO	Transactionnel	Non applicable
Ligne de commande sortante	Transactionnel	Oui
Expédition	Transactionnel	Non applicable
Politique d'inventaire	Transactionnel	Non applicable
Ligne de commande entrante	Transactionnel	Non applicable
Expédition sortante	Transactionnel	Non applicable
Calendrier des lignes de commande entrantes	Transactionnel	Non applicable

Comment le CDM est lié à l'intégration des données

Lorsque vous intégrez des données, le processus suit les étapes suivantes :

1. Chargement : vous chargez vos données sources sous forme de fichiers CSV sur Amazon S3.
2. Carte : l'agent de données analyse vos ensembles de données sources et suggère les tables de destination CDM qui correspondent le mieux à vos données.
3. Transformation : les requêtes de transformation SQL convertissent le format de vos données source au format CDM.
4. Valider — Des contrôles de qualité sont effectués sur les données transformées pour vérifier leur conformité aux exigences du CDM.
5. Activer — Une fois validées, les données entrent dans les fonctionnalités et deviennent disponibles pour celles-ci.

Pour obtenir des instructions détaillées sur l'intégration de vos données, consultez la rubrique Intégration des données.

Validation des données et contrôles de qualité

Présentation de

La validation des données garantit que vos données répondent aux exigences de qualité avant que les fonctionnalités d'Amazon Connect Decisions ne soient exécutées. Le système valide les données en fonction des plans, des mesures et des règles que vous avez configurés pour identifier les problèmes susceptibles de bloquer ou de dégrader les performances.

Comment fonctionne la validation des données

Éléments déclencheurs de validation

La validation des données s'exécute automatiquement aux heures suivantes :

- Modifications de configuration d'Insights : lorsque vous créez ou modifiez des métriques, des règles ou d'autres configurations
- Création d'un plan : lorsque vous créez un plan ad hoc ou à chaque exécution planifiée
- Actualisation des données : après chaque actualisation des données dans vos flux de destination

- Exécution des capacités : avant ou pendant les opérations d'un coéquipier basé sur l'IA (par exemple, lors de la détection d'une exception ou de l'établissement de recommandations)

Types de validation

Amazon Connect Decisions effectue deux types de validation :

La validation de présence des données vérifie que les ensembles de données et les champs requis sont chargés en fonction de vos ressources configurées (métriques, règles, plans).

La validation de la qualité des données confirme que les données fournies répondent aux exigences de qualité en fonction de votre configuration de configuration, notamment :

- Validation des critères de configuration : confirme que les produits et les sites correspondent à vos critères de règles (par exemple, catégories de produits, emplacements des sites)
- Validation hiérarchique : identifie les relations hiérarchiques manquantes si vous utilisez des hiérarchies dans votre configuration
- Validation du champ d'application : confirme que toutes les données nécessaires existent pour les produits et sites identifiés
- Évaluation de la qualité : évalue la qualité et la facilité d'utilisation des données en fonction des exigences opérationnelles

Validation progressive

Amazon Connect Decisions active des fonctionnalités pour les produits et les sites contenant des données valides plutôt que de bloquer les fonctionnalités pour l'ensemble de votre ensemble de données. Lorsque des problèmes de validation concernent des produits ou des sites spécifiques, le système continue de traiter les produits et les sites contenant des données valides, identifie les produits ou sites présentant des problèmes de données et vous avertit des éléments spécifiques nécessitant une attention particulière. Cela vous permet de commencer à utiliser les fonctionnalités tout en résolvant les problèmes de données restants.

Erreurs d'accès à la validation des données

Vous pouvez visualiser les erreurs de validation des données via trois points d'entrée :

1. Métrique « Erreurs de validation des données » sur la page d'accueil

2. Carte thématique sur les erreurs de validation des données sur la page d'accueil
3. « Gestion des données » dans le menu de navigation de gauche **>** onglet « Erreurs »

Révision des erreurs de validation

La page Erreurs affiche toutes les erreurs de validation ouvertes et résolues. Vous pouvez effectuer une recherche et filtrer selon l'une des colonnes suivantes :

- ID : identifiant unique pour l'erreur de validation
- Statut
  - Ouvert : l'erreur n'a pas été résolue
  - Résolu : L'erreur a été corrigée et validée
- Description : Explication du problème de qualité des données
- Type de problème
  - Données obligatoires manquantes : les données obligatoires ne sont pas fournies pour déclencher une opération (par exemple, aucune table source outbound_order_line pour le plan d'approvisionnement)
  - Valeurs de données non valides : les données existent mais contiennent des valeurs incorrectes (par exemple, un coût de produit négatif)
  - Relations manquantes : les relations hiérarchiques ou de référence requises sont manquantes (par exemple, des hiérarchies de produits manquantes)
  - Données insuffisantes : données disponibles insuffisantes pour effectuer les opérations requises (par exemple, le plan de demande nécessite 12 mois d'historique des données de commande, mais il n'en existe que 3 mois)
- Capacité : capacité ou ressource affectée
  - Plan d'approvisionnement
  - Plan de demande
  - Aperçu (inclut les exceptions, les recommandations et le RCA pour l'offre ou la demande)
- Destination : flux de destination impacté
- Priorité
  - Critique : au moins une fonctionnalité est complètement bloquée et ne peut pas être exécutée
  - Élevé : au moins une fonctionnalité est partiellement bloquée (certains produits ou sites ne peuvent pas être traités)

  - Moyen : au moins une fonctionnalité présente une précision réduite (elle fonctionnera mais avec des résultats dégradés)
- Créé à : Horodatage indiquant la date à laquelle l'erreur a été détectée pour la première fois

Affichage des détails de l'erreur

Sélectionnez une erreur pour afficher des informations détaillées. L'écran détaillé affiche les informations ci-dessus ainsi que l'horodatage du dernier événement, la ressource et le lien associés (la métrique, la règle ou le plan représentant la fonctionnalité affectée par le problème), ainsi qu'un aperçu d'un maximum de 100 lignes de données concernées indiquant comment se manifeste l'erreur de validation des données.

Actions disponibles

À partir de l'écran détaillé des erreurs, vous pouvez :

- Résolution des problèmes : lancez l'IA Teammate pour vous aider à résoudre le problème en langage naturel et recevoir des conseils de résolution détaillés
- Résoudre l'erreur : marquez manuellement l'erreur comme résolue si vous avez résolu le problème sous-jacent
- Téléchargement : Téléchargez le jeu de données concerné complet pour une analyse et une correction détaillées

Résolution des erreurs de validation des données

Flux de travail de résolution

1. Consultez la description et la priorité de l'erreur pour comprendre son impact
2. Consultez l'aperçu des données concernées pour voir quels enregistrements spécifiques sont concernés
3. Suivez les recommandations spécifiques fournies pour la correction
4. Choisissez une action appropriée :
   - Pour les problèmes de configuration : collaborez avec vos responsables et planificateurs pour ajuster la configuration des métriques, des règles ou des plans
   - Pour les problèmes de mappage : corrigez les données source téléchargées ou mettez à jour les transformations de données et les mappages

- Pour les données manquantes ou non valides : téléchargez les données corrigées

5. Marquez manuellement l'erreur comme résolue une fois que vous avez résolu le problème sous-jacent

Travailler avec l'IA Teammate

Utilisez l'option Dépannage pour poser des questions telles que « Sur quelles erreurs dois-je me concentrer en premier ? » ou « Quelles sont les erreurs qui bloquent mon plan de demande ? » , recevez des explications détaillées sur le problème et son impact, obtenez des conseils étape par étape sur les approches de résolution et comprenez comment l'erreur affecte votre configuration spécifique. L'équipier IA peut vous aider à résoudre le problème dans Amazon Connect Decisions et dans vos systèmes de données sources.

Bonnes pratiques

- Hiérarchisez en fonction de leur gravité : concentrez-vous d'abord sur les erreurs critiques, car elles bloquent totalement l'exécution des fonctionnalités. Corrigez ensuite les erreurs de priorité élevée qui bloquent partiellement le traitement, puis les erreurs de priorité moyenne qui réduisent la précision.
- Lisez attentivement les recommandations : chaque erreur inclut des conseils spécifiques et exploitables adaptés au problème en fonction de votre configuration.
- Utilisez la validation progressive à votre avantage : n'attendez pas de résoudre chaque erreur avant d'utiliser les fonctionnalités. Le système active le fonctionnement de produits et de sites valides pendant que vous vous efforcez de résoudre des problèmes pour d'autres utilisateurs.
- Surveillance après l'actualisation des données : vérifiez l'absence de nouvelles erreurs de validation après chaque mise à jour des données afin de détecter les problèmes à un stade précoce avant qu'ils n'aient un impact sur les flux de production.
- Téléchargez les données concernées de manière stratégique : utilisez l'option de téléchargement lorsque vous devez analyser tous les enregistrements concernés au-delà de l'aperçu ou lorsque vous devez fournir l'ensemble de données complet à votre équipe chargée des données.
- Utilisez l'IA Teammate pour les problèmes complexes : l'option Dépannage fournit une assistance contextuelle qui s'adapte à votre situation et à votre configuration spécifiques.
- Vérifier la résolution : après avoir résolu les problèmes de données, marquez manuellement les erreurs comme résolues pour confirmer que le correctif a été correctement résolu et supprimez-les de la liste ouverte.

Configuration du système

Les paramètres d'Amazon Connect Decisions sont organisés par champ d'application et par public. Certains paramètres sont personnels, ce qui permet à chaque utilisateur de personnaliser sa propre expérience. D'autres sont des configurations au niveau de l'instance gérées par des administrateurs qui affectent le comportement du système pour tous les utilisateurs ou la manière dont il se connecte à votre environnement technologique plus large.

User-level les paramètres permettent aux utilisateurs de gérer les informations de leur compte, leurs préférences de notification et la manière dont leur champ d'accès aux données est appliqué à leurs vues.

Instance-level les paramètres permettent aux administrateurs de configurer le comportement des filtres de contrôle d'accès au sein de l'organisation, d'établir des connexions avec votre ERP et d'autres systèmes externes, et de définir la manière dont le système gère les actions recommandées.

Ensemble, ces paramètres donnent à votre organisation la flexibilité nécessaire pour adapter les décisions Amazon Connect à votre contexte opérationnel spécifique tout en préservant la cohérence au sein de votre équipe.

Paramètres du profil utilisateur

Les utilisateurs peuvent accéder aux paramètres de leur profil en sélectionnant leur nom dans le coin supérieur droit de l'application et en choisissant Profil dans le menu déroulant. La page de profil permet aux utilisateurs de gérer les informations de leur compte, leurs préférences de notification et leurs paramètres d'accès aux données.

Accès aux paramètres du profil

Pour accéder aux paramètres de votre profil :

1. Sélectionnez votre nom dans le coin supérieur droit de la page
2. Choisissez Profil dans le menu déroulant
3. La page de profil affiche les informations et les paramètres de votre compte

Informations sur le profil

La page de profil affiche les informations de compte suivantes :

Utilisateur : Votre nom d'utilisateur

Rôle : le rôle qui vous est assigné (administrateur, responsable ou planificateur)

Fuseau horaire : sélectionnez votre fuseau horaire préféré dans le menu déroulant. Ce paramètre détermine la manière dont les dates et heures sont affichées dans Amazon Connect Decisions.

E-mail : votre adresse e-mail associée à votre compte Amazon Connect Decisions

Création : date et heure de création de votre compte

Mise à jour : date et heure de dernière modification de votre profil

Sélectionnez Enregistrer dans le coin supérieur droit pour enregistrer les modifications apportées aux informations de votre profil.

Préférences de notification

L'onglet Préférences de notification vous permet de configurer la façon dont vous recevez les notifications relatives aux différents événements du système. Vous pouvez choisir de recevoir des notifications dans l'application, par e-mail ou par les deux.

Plans

Succès de la génération du plan : choisissez comment vous souhaitez être averti lorsque la génération du plan est terminée avec succès. Les options incluent les notifications intégrées à l'application et les notifications par e-mail.

Échec de génération du plan : choisissez comment vous souhaitez être averti en cas d'échec de la génération du plan. Les options incluent les notifications intégrées à l'application et les notifications par e-mail.

Configurations Insights

Configurations d'Insights réussies : choisissez comment vous souhaitez être averti lorsque la configuration d'Insights est terminée avec succès. Les options incluent les notifications intégrées à l'application.

Échec des configurations Insights : choisissez comment vous souhaitez être averti en cas d'échec de la configuration d'Insights. Les options incluent les notifications intégrées à l'application.

Ingestion de données

Échec de l'ingestion des données : choisissez comment vous souhaitez être averti en cas d'échec de l'ingestion des données. Les options incluent les notifications intégrées à l'application et les notifications par e-mail.

Paramètres d'administration

Les administrateurs peuvent configurer des paramètres de notification à l'échelle du système qui s'appliquent à tous les utilisateurs.

Conservation des notifications : définissez le nombre de jours après lesquels les notifications sont automatiquement supprimées du système. Entrez une valeur numérique pour spécifier la période de conservation.

Sélectionnez Enregistrer pour appliquer vos préférences de notification.

Étendue assignée

L'onglet Étendue assignée affiche vos autorisations d'accès aux données et vous permet de configurer la manière dont les vues de données sont filtrées en fonction de l'étendue qui vous est attribuée.

Accès aux données

Cette section affiche votre niveau actuel d'accès aux données. Si vous avez accès à tous les sites et produits, le message « Vous avez accès à tous les sites et produits » s'affichera.

Filtre de vue par défaut

Filtrer les vues en fonction de l'étendue qui m'est attribuée : lorsqu'elles sont activées, les vues de données sont automatiquement filtrées pour n'afficher que les éléments des produits et sites qui vous ont été attribués. Activez ou désactivez ce paramètre selon vos préférences.

Lorsque ce filtre est activé, vous ne verrez que les exceptions, les plans et les autres données correspondant à l'étendue qui vous a été attribuée. Lorsque cette option est désactivée, vous pouvez voir des données en dehors de la zone qui vous est assignée en fonction des autorisations de votre rôle.

Sélectionnez Enregistrer pour appliquer vos préférences de filtre.

Filtre de contrôle d'accès Toggle

Comme indiqué précédemment, tous les utilisateurs peuvent consulter toutes les exceptions, qu'ils aient ou non configuré les produits et sites appropriés (les actions de mutation nécessitent toujours un accès approprié). Bien que cela facilite le partage des connaissances, les utilisateurs qui se concentrent uniquement sur des produits et des sites spécifiques peuvent être submergés par des exceptions ou des recommandations pour d'autres produits et sites. Pour aider les utilisateurs à se concentrer sur les exceptions et les recommandations qui leur tiennent à cœur, ils peuvent utiliser le bouton d'affichage des accès comme suit :

- Tout d'abord, un utilisateur ayant le rôle « Admin » doit activer la fonctionnalité sur cette instance. Accédez à la page Paramètres de l'instance depuis la barre de navigation de gauche
- Par défaut, ils verront une bascule qui définit le filtre de vue d'accès par défaut pour l'ensemble de l'instance. L' « administrateur » peut soit décider d'avoir un seul paramètre unifié pour tous les utilisateurs de l'instance, soit laisser les utilisateurs décider de leurs préférences
- S'ils choisissent le paramètre de basculement de la vue d'accès unifié, l' « administrateur » peut également décider si le basculement doit être activé ou désactivé pour tous les utilisateurs
- S'ils choisissent de laisser chaque utilisateur sélectionner ses propres préférences, chaque utilisateur aura la possibilité d'activer lui-même le filtre d'affichage des accès. Chaque utilisateur peut accéder à la page des préférences utilisateur à partir de la liste déroulante des utilisateurs située dans le coin supérieur droit de l'écran.

Modifiez le bouton de contrôle d'accès pour votre instance :

1. Choisissez le tiroir de gauche des paramètres
2. Sélectionnez une application
3. Mettez à jour le bouton et cliquez sur Enregistrer les paramètres

Si le paramètre est activé, le système filtre automatiquement les pages répertoriant les exceptions et les recommandations pour n'afficher que celles qui ont été générées pour un produit OU un site correspondant à la configuration du contrôle d'accès

Pour les utilisateurs dont l'option « Accorder l'accès complet à tous les produits et sites » est activée, le bouton d'affichage des accès affichera toujours toutes les exceptions et recommandations. Si un utilisateur a désactivé cette option mais qu'aucun produit ou site n'est configuré, le système l'interprète comme n'ayant accès à aucun produit ou site et l'utilisateur ne verra donc rien

Le filtre de vue d'accès est considéré comme un type de filtre différent et n'apparaîtra donc pas dans les puces de filtre de la page des exceptions et des recommandations. Les utilisateurs peuvent toujours appliquer d'autres filtres de la même manière qu'auparavant, y compris les filtres d'autres produits et sites

Les utilisateurs peuvent toujours accéder aux exceptions et aux recommandations pour d'autres produits OU sites s'ils désactivent le bouton d'affichage d'accès ou s'ils disposent d'un lien hypertexte direct vers celles-ci

Configuration des connexions à votre ERP

Pour permettre à Amazon Connect Decisions d'effectuer des opérations en votre nom dans votre système de planification des ressources d'entreprise (ERP), vous devez configurer une connexion qui spécifie les paramètres de connexion nécessaires et les informations d'identification qu'Amazon Connect Decisions doit utiliser pendant l'opération.

Systèmes ERP pris en charge :

- SAP S/4HANA

Configurer les informations d'identification dans Secrets Manager

1. À l'aide de votre compte, utilisez Secrets Manager pour créer un secret Secrets Manager
   - Lorsque vous saisissez les informations d'identification dans Secrets Manager, remplacez les valeurs d'espace réservé ci-dessous (`<username>`et`<password>`) par le nom d'utilisateur et le mot de passe réels qu'Amazon Connect Decisions doit utiliser
   - Si vous utilisez la console, choisissez `Other type of secret` `Secret Type`
   - Si vous entrez les détails via l'`Key/value pairs`onglet de la console, entrez 2 paires :
     - Clé : `username` ; Valeur : <*username*>
     - Clé : `password` ; Valeur : <*password*>
   - Si vous utilisez l'`Plaintext`onglet pour saisir le secret dans la console, entrez un objet JSON avec les deux paires suivantes :

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

2. Chiffrez votre secret avec une clé AWS KMS, notez l'identifiant de la clé, car vous en aurez besoin dans les étapes suivantes
3. Une fois votre secret créé, prenez note de son Amazon Resource Name (ARN), car vous en aurez besoin lors des étapes suivantes
   - par exemple : `arn:aws:secretsmanager:<Region>:<AccountId>:secret:<SecretName>-<SixRandomCharacters>`

Configurer les autorisations sur la clé KMS

Vous devez fournir les autorisations nécessaires pour qu'Amazon Connect Decisions puisse y accéder et l'utiliser.

1. Mettez à jour votre politique KMS pour permettre à Amazon Connect Decisions d'accéder à votre clé via le rôle d'instance
   - Remarque : remplacez `<YourAccountNumber>` et `<YourInstanceID>` par votre AWS compte et l'ID d'instance Amazon Connect Decisions.

```
{
    "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. Mettez à jour la politique intégrée pour votre rôle d'instance afin d'accorder l'autorisation sur la clé

- Remarque : remplacez <YourSecretArn> <YourAccountNumber> et <YourInstanceID> par votre ARN secret, votre AWS compte et votre ID d'instance de chaîne AWS d'approvisionnement.

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

Mettez à jour la politique de ressources du Gestionnaire de secrets pour votre secret

1. Mettez à jour la politique de ressources du Gestionnaire de secrets pour votre secret

- Remarque : remplacez-le <YourSecretArn> par l'ARN de votre secret

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"scn.amazonaws.com"
         },
         "Action":[
```

```
            "secretsmanager:GetSecretValue",
            "secretsmanager:DescribeSecret"
         ],
         "Resource":"YourSecretArn"
      }
   ]
}
```

Configuration de la connexion Amazon Connect Decisions

1. Dans votre instance d'Amazon Connect Decisions, accédez à la page de gestion des données
2. Sélectionnez l'`Connections`onglet
3. Cliquez sur le bouton `Create Connection`.
4. Sur la `Create Connector` page, cliquez sur le `Select` bouton sur la ligne correspondant au type de `SAP S/4HANA` connecteur
5. Dans la `Configure SAP S/4HANA API Connector` page, entrez les informations nécessaires :
   - `Connection Name`: nom de connexion unique
   - `API Endpoint URL`: l'URL du point de terminaison de l'API OData de votre S/4HANA instance SAP (par exemple :`https://<hostname>:<port>`)
   - `Client Number`: le numéro de client SAP à 3 chiffres (par exemple :`100`)
   - `Secret ARN`: le nom de ressource Amazon (ARN) du secret dans Secrets Manager où sont stockées les informations d'identification à utiliser par Amazon Connect Decisions
6. Cliquez sur le `Create Connector` bouton

Configuration des paramètres d'action

Amazon Connect Decisions vous permet de contrôler les types d'actions qu'il doit proposer pour effectuer des opérations en votre nom dans votre système de planification des ressources d'entreprise (ERP). Par défaut, tous les types d'action sont désactivés et vous devez activer cette fonctionnalité pour chaque type d'action souhaité.

> **Note**
>
> L'activation de la prise en charge d'un type d'action donné permet de contrôler si l'option permettant à Amazon Connect Decisions d'effectuer l'action en votre nom sera présentée dans l'ensemble du système (par exemple, lors de la révision d'un Insight contenant une recommandation du type donné). Amazon Connect Decisions n'effectuera pas ces actions (même lorsque le support est activé) tant que vous n'aurez pas accepté la recommandation spécifique.

Types d'actions pris en charge :

- Créer un bon de commande
- Mettre à jour le bon de commande
- Annuler le bon de commande

Configurez le support des actions pour chaque type d'action :

1. Dans votre instance d'Amazon Connect Decisions, accédez à la page de gestion des données
2. Sélectionnez l'`Actions`onglet
3. Trouvez le type d'action que vous souhaitez configurer dans la liste
4. Pour activer la prise en charge du type d'action :
   - Sélectionnez l'une des connexions répertoriées dans le menu déroulant pour ce type d'action
   - Remarque : le menu déroulant n'affichera que les connexions disponibles qui ont été configurées d'un type compatible avec cette `Actions` fonctionnalité (par exemple :`SAP S/4HANA`)
5. Pour désactiver la prise en charge du type d'action :
   - Sélectionnez `No connection` ce type d'action dans le menu déroulant
6. Cliquez `Save` pour enregistrer vos modifications

Sécurité

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Third-party des auditeurs testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de conformité d'AWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent aux décisions relatives à Amazon Connect, consultez la section Services AWS concernés par chaque programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d’autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l’utilisation d’Amazon Connect. Les rubriques suivantes expliquent comment configurer Amazon Connect Decisions pour répondre à vos objectifs de sécurité et de conformité.

Protection des données

Le modèle de responsabilité AWS partagée s'applique à la protection des données dans Amazon Connect Decisions. Comme décrit dans ce modèle, AWS est responsable de la protection de l'infrastructure mondiale qui gère l'ensemble du AWS cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable de la configuration de la sécurité et des tâches de gestion des AWS services que vous utilisez. Pour plus d’informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) relatives à la confidentialité des données. Pour plus d'informations sur la protection des données en Europe, consultez le modèle de responsabilité partagée d'AWS et le billet de blog sur le RGPD sur le blog de sécurité AWS.

À des fins de protection des données, nous vous recommandons de protéger les informations d'identification du AWS compte et de configurer les utilisateurs individuels avec Gestion des identités

et des accès AWS (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l’authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous vous recommandons le certificat TLS 1.2 ou une version ultérieure.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut au sein AWS des services.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui vous aident à découvrir et à sécuriser les données sensibles stockées dans Amazon Simple Storage Service.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d’informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l’information fédérale).

Nous vous recommandons vivement de ne jamais placer d’informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec Amazon Connect Decisions ou d'autres AWS services à l'aide de la console de AWS gestion, de l'API AWS Command Line Interface (AWS CLI) ou AWS des SDK. Toutes les données que vous saisissez dans des balises ou des champs de texte libre utilisés pour les noms peuvent être utilisées pour les journaux de facturation ou de diagnostic.

Chiffrement des données

Cette rubrique fournit des informations spécifiques à Amazon Connect Decisions concernant le chiffrement en transit et le chiffrement au repos.

Chiffrement en transit

Toutes les communications entre les clients et Amazon Connect Decisions et entre Amazon Connect Decisions et ses dépendances en aval sont protégées à l'aide de connexions TLS 1.2 ou supérieures.

Chiffrement au repos

Amazon Connect Decisions stocke les données au repos à l'aide de DynamoDB et d'Amazon Simple Storage Service (Amazon S3). Les données au repos sont cryptées par défaut à l'aide de solutions de AWS chiffrement. Amazon Connect Decisions chiffre vos données à l'aide des clés de chiffrement AWS détenues par AWS Key Management Service (AWS KMS). Vous n'avez aucune action à entreprendre pour protéger les clés AWS gérées qui chiffrent vos données. Pour plus d'informations, consultez les clés détenues par AWS dans le manuel du AWS KMS développeur.

Si vous modifiez la clé KMS utilisée pour chiffrer les données de votre instance Amazon Connect Decisions dans la AWS console, vous devez créer une nouvelle instance pour commencer à utiliser la nouvelle clé pour chiffrer vos données. Les données chiffrées avec la clé précédente ne seront pas conservées, et seules les données seront chiffrées avec la clé mise à jour. Si vous souhaitez conserver les données d'une méthode de chiffrement précédente, vous pouvez revenir à la clé que vous utilisiez lors de ces conversations.

Vos conversations avec Amazon Connect Decisions sur l'application Web et dans les applications de chat sont chiffrées uniquement à l'aide de AWS-owned clés.

Cross-region traitement

Amazon Connect Decisions est alimenté par Amazon Bedrock et utilise l'inférence interrégionale (CRIS) pour répartir le trafic entre différentes AWS régions afin d'améliorer les performances et la fiabilité de l'inférence par modèle de langage étendu (LLM). Grâce à l’inférence entre régions, vous obtenez :

- Débit et résilience accrus pendant les périodes de forte demande
- Amélioration des performances
- Accès aux nouvelles fonctionnalités et fonctionnalités d'Amazon Connect Decisions qui s'appuient sur les LLM les plus puissants hébergés sur Amazon Bedrock

Cross-region l'inférence fonctionne différemment en fonction de la AWS région dans laquelle votre instance Amazon Connect Decisions est créée.

Pour toutes les instances créées dans la région géographique des États-Unis, Amazon Connect Decisions utilisera Global CRIS. Cela signifie que les demandes d'inférence seront acheminées vers les AWS régions commerciales prises en charge dans le monde entier, ce qui optimisera les

ressources disponibles et permettra d'augmenter le débit des modèles. Reportez-vous au guide de l'utilisateur d'Amazon Bedrock pour en savoir plus sur Global CRIS.

Pour toutes les instances créées dans la région géographique de l'UE, Amazon Connect Decisions utilisera Geographic CRIS. Cela signifie que les demandes d'inférence sont conservées dans les AWS régions qui font partie de la zone géographique où les données se trouvent à l'origine. Reportez-vous au guide de l'utilisateur d'Amazon Bedrock pour en savoir plus sur Geographic CRIS.

Par exemple, une demande effectuée depuis une instance Amazon Connect Decisions créée dans la région USA Est (Virginie du Nord) (us-east-1) peut être acheminée vers AWS n'importe quelle région du monde, telle que l'Asie-Pacifique (Sydney) (ap-southeast-2). Toutefois, pour une demande effectuée depuis une instance Amazon Connect Decisions créée dans la région Europe (Irlande) (eu-west-1), elle est acheminée AWS vers une région de l'UE telle que l'Europe (Francfort) (eu-central-1). Pour plus d'informations, consultez la section Régions prises en charge par Amazon Connect Decisions.

Bien que l'inférence entre régions ne modifie pas l'endroit où vos données sont stockées, vos demandes et les résultats de sortie peuvent être déplacés en dehors de la région dans laquelle les données se trouvent à l'origine. Toutes les données sont chiffrées lors de leur transmission sur le réseau sécurisé d'Amazon. L'utilisation de l'inférence entre régions n'entraîne aucun coût supplémentaire. Pour plus d'informations sur l'endroit où les données sont stockées lorsque vous utilisez Amazon Connect Decisions, consultez la section Protection des données dans Amazon Connect Decisions.

Décisions relatives à l'IAM pour Amazon Connect

AWS Identity and Access Management (IAM) est un service AWS qui permet à un administrateur de contrôler l'accès aux ressources AWS en toute sécurité. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources Amazon Connect Decisions. IAM est un service AWS que vous pouvez utiliser sans frais supplémentaires.

Comment fonctionne IAM avec Amazon Connect Decisions

Avant d'utiliser IAM pour gérer l'accès à Amazon Connect Decisions, découvrez quelles fonctionnalités IAM peuvent être utilisées avec Amazon Connect Decisions. Pour obtenir une vue d'ensemble de la façon dont Amazon Connect Decisions et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez les services AWS compatibles avec IAM dans le guide de l'utilisateur IAM.

Identity-based politiques relatives aux décisions relatives à Amazon Connect

Prend en charge les politiques basées sur l’identité : oui

Identity-based les politiques sont des documents de politique d'autorisation JSON que vous pouvez associer à une identité, telle qu'un utilisateur IAM, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d’actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l’identité, consultez Définition d’autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l’utilisateur IAM.

Avec les politiques IAM basées sur l’identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l’utilisateur IAM.

Resource-based politiques au sein d'Amazon Connect Decisions

Prend en charge les politiques basées sur les ressources : non

Resource-based les politiques sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l’accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d’actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou AWS des services.

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. Pour plus d’informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l’utilisateur IAM.

Actions politiques pour Amazon Connect Decisions

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Les actions politiques dans Amazon Connect Decisions utilisent le préfixe suivant avant l'action :

```
scn
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

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

Ressources relatives aux politiques pour Amazon Connect Decisions

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

Clés de conditions de politique pour Amazon Connect Decisions

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` indique à quel moment les instructions s'exécutent en fonction de critères définis. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande. Pour voir toutes les clés de condition AWS globales, consultez les clés de contexte de condition globale AWS dans le guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec Amazon Connect Decisions

Prend en charge les informations d'identification temporaires : oui

Les informations d'identification temporaires fournissent un accès à court terme aux AWS ressources et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez la section Informations d'identification de sécurité temporaires dans les services IAM et AWS qui fonctionnent avec IAM dans le guide de l'utilisateur IAM.

Transférer les sessions d'accès pour Amazon Connect Decisions

Prend en charge les sessions d'accès direct (FAS) : oui

Les sessions d'accès direct (FAS) utilisent les autorisations du principal appelant un AWS service, combinées au AWS service demandeur pour adresser des demandes aux services en aval. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez la section Sessions de transmission d'accès.

Rôles de service pour Amazon Connect Decisions

Prend en charge les rôles de service : oui

Un rôle de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez la section Créer un rôle pour déléguer des autorisations à un AWS service dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut perturber les fonctionnalités d'Amazon Connect Decisions. Modifiez les rôles de service uniquement lorsque Amazon Connect Decisions fournit des instructions à cet effet.

Identity-based exemples de politiques

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier les ressources Amazon Connect Decisions. Ils ne peuvent pas non plus effectuer de tâches à l'aide de la console AWS de gestion, de l'interface de ligne de AWS commande (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour savoir comment créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de stratégie JSON, consultez la section Création de politiques IAM dans le guide de l'utilisateur IAM.

Politique IAM de gestion des instances

Vous trouverez ci-dessous la politique IAM nécessaire pour créer, mettre à jour ou supprimer des instances via la console ou l'API publique (à l'exclusion de toutes les opérations Webapp).

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

Bonnes pratiques en matière de politiques

Identity-based les politiques déterminent si quelqu'un peut créer, accéder ou supprimer les ressources Amazon Connect Decisions de votre compte. Ces actions peuvent entraîner des frais pour votre compte AWS . Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques gérées par AWS qui accordent des autorisations pour de nombreux cas d'utilisation courants. Elles sont disponibles dans votre compte AWS . Nous vous recommandons de réduire encore les autorisations en définissant des politiques AWS gérées par le client qui sont propres à vos cas d'utilisation. Pour plus d'informations, consultez les politiques gérées par AWS ou les politiques gérées par AWS pour les fonctions professionnelles dans le guide de l'utilisateur IAM.
- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule

tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.

- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un AWS service spécifique, tel que CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politiques avec IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exigez l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur racine dans votre compte AWS , activez la MFA pour plus de sécurité. Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Dépannage IAM

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lors de l'utilisation d'Amazon Connect Decisions et d'IAM.

Je ne suis pas autorisé à effectuer une action dans Amazon Connect Decisions

Si vous n'êtes pas autorisé à effectuer une action sur la console de AWS gestion, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni votre nom d'utilisateur et votre mot de passe.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource `my-example-widget` fictive, mais ne dispose pas des autorisations `scn:GetWidget` fictives.

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

Dans ce cas, Mateo demande à son administrateur de mettre à jour ses politiques pour lui permettre d'accéder à la ressource `my-example-widget` à l'aide de l'action `scn:GetWidget`.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à Amazon Connect Decisions.

Certains AWS services vous permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, vous devez disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans Amazon Connect Decisions. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary n'est pas autorisée à transmettre le rôle au service.

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

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à mon AWS compte pour accéder à mes ressources Amazon Connect Decisions

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques

basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si Amazon Connect Decisions prend en charge ces fonctionnalités, consultez Comment Amazon Connect Decisions fonctionne avec IAM.
- Pour savoir comment fournir un accès à vos ressources sur les AWS comptes que vous possédez, consultez la section Fournir un accès à un utilisateur IAM sur un autre AWS compte que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des AWS comptes tiers, consultez la section Fournir un accès aux AWS comptes détenus par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Third-party sous-processeurs

Amazon Connect Decisions utilise Boomi, une API tierce, pour permettre d'effectuer des actions en votre nom dans des systèmes externes. Lorsque vous utilisez une fonctionnalité d'Amazon Connect Decisions qui se connecte à vos systèmes tiers, vous nous autorisez à utiliser Boomi comme intergiciel d'intégration pour transmettre et traiter vos données chiffrées ; vos données ne sont pas stockées séparément dans Boomi.

Pour en savoir plus sur Boomi et son fonctionnement, consultez la documentation publique de Boomi.

Régions prises en charge

Cette page décrit les AWS régions dans lesquelles vous pouvez utiliser Amazon Connect Decisions. Pour plus d'informations sur AWS les régions, voir Spécifier les AWS régions que votre compte peut utiliser dans le Guide de référence sur la gestion des AWS comptes.

Vos données peuvent être traitées dans une région différente de celle dans laquelle vous utilisez Amazon Connect Decisions. Pour plus d'informations sur le traitement interrégional dans Amazon

Connect Decisions, consultez la section Cross-region Traitement. Pour en savoir plus sur l'endroit où les données sont stockées pendant le traitement, consultez Protection des données.

Régions prises en charge

Amazon Connect Decisions est disponible sur la console de AWS gestion, l'application mobile de AWS la console, le AWS site Web et le site Web de AWS documentation dans les AWS régions suivantes. Ces régions sont activées par défaut, ce qui signifie que vous n'avez pas besoin de les activer avant de les utiliser. Pour plus d'informations, consultez Regions that are enabled by default.

Vous utilisez Amazon Connect Decisions dans les régions suivantes.

AWS Nom de la région	Nom du code	Géographie (États-Unis, UE, etc.)
USA Est (Virginie du Nord)	us-east-1	ETATS-UNIS
Europe (Irlande)	eu-west-1	UE

Résolution des problèmes

Lorsque des problèmes surviennent lors de la configuration ou de l'utilisation quotidienne d'Amazon Connect Decisions, cette section fournit des conseils pour vous aider à diagnostiquer et à résoudre les problèmes les plus courants. Commencez par identifier la catégorie qui correspond le mieux au problème que vous rencontrez, puis suivez les étapes de résolution des problèmes indiquées sur la page correspondante. Si vous ne savez pas quelle catégorie s'applique, commencez par les problèmes d'installation courants, qui couvre le plus large éventail de problèmes de configuration initiale.

Problèmes de configuration courants

Erreurs d'intégrité référentielle : « les valeurs product_id ne correspondent à aucun identifiant dans l'ensemble de données du produit »

La cause la plus courante est la présence d'espaces blancs à la fin des champs d'identification. Les systèmes source qui exportent à partir de bases de données à largeur fixe comportent souvent des espaces dans les champs de chaînes. Le product master peut avoir des identifiants propres (« MAT604 ») alors que le fichier de ligne de commande contient des identifiants complétés (« MAT604 »). Le système fait une correspondance stricte entre les chaînes, de sorte que celles-ci ne se rejoignent pas.

Correctif : ajoutez TRIM () à tous les champs d'ID de chaîne dans les transformations SQL de votre flux de données. Appliquez-le à product_id, ship_from_site_id, customer_tpartner_id et à toute autre clé de jointure. Vérifiez également les incohérences entre les citations entre les fichiers. Lorsque vous réexportez des fichiers CSV, utilisez QUOTE_ALL pour éviter les problèmes d'inférence de type dans lesquels les identifiants d'apparence numérique (par exemple, « 111613 ») sont traités comme des entiers dans un fichier et des chaînes dans un autre.

Prévention : par défaut, supprimez toujours tous les champs d'ID de vos transformations SQL, même si vous ne voyez pas le problème aujourd'hui. Les données source peuvent changer entre les exportations.

Les produits figurant dans l'historique des commandes sont absents de la liste des produits

L'historique de vos commandes contient souvent des produits qui ne figurent pas dans le catalogue de produits actuel (produits abandonnés, articles uniques, SKU de test). Le système rejettera l'intégralité du fichier de commande si aucun product_id ne correspond à un enregistrement principal de produit.

Correctif : soit (a) créez des lignes souches dans le référentiel de produits pour les produits manquants avec un minimum de champs obligatoires (id, description, base_uom), soit (b) filtrez l'historique des commandes pour n'inclure que les produits présents dans le référentiel de produits. L'option (a) est préférée car elle préserve l'historique de la demande qui peut être utile pour la détection du lignage et des tendances.

Erreurs d'analyse CSV lors du téléchargement du produit principal

Les descriptions de produits contenant des virgules, des guillemets ou des caractères spéciaux peuvent interrompre l'analyse CSV. Des erreurs telles que « 17 champs attendus, 19 champs visibles » peuvent s'afficher sur des lignes spécifiques.

Correctif : Re-export le fichier avec les guillemets appropriés (QUOTE_ALL). Vérifiez que les lignes défaillantes spécifiques ne contiennent pas de virgules incorporées dans les champs de description.

Les données ne s'affichent pas après le téléchargement

- Vérifiez que le format de votre fichier n'a pas changé (extension, en-têtes de colonne, encodage).
- Vérifiez que les noms de fichiers et les extensions correspondent au modèle attendu : renommer .csv en .csv000 ou similaire interrompra l'ingestion.
- Attendez jusqu'à 30 minutes pour que l'ingestion des données soit terminée après le téléchargement.
- Si les en-têtes de colonne changent entre les chargements (par exemple, les colonnes nommées par month/year), une étape de prétraitement est requise avant le téléchargement.

Le PIV ne se met pas à jour après l'actualisation des données

- Le PIV se déclenche environ 15 minutes après la fin de l'ingestion et prend environ 20 à 30 minutes pour s'écouler.

- End-to-end du téléchargement des données au nouveau PIV : environ 1 à 1,5 heure.
- Si PIV n'a pas été mis à jour depuis plus de 24 heures, contactez le support.

Le nombre d'exceptions semble trop élevé ou trop faible

- Trop élevé : le seuil est peut-être trop faible ou un seul produit+site peut générer plusieurs exceptions pour des dates différentes. Contactez le support pour vérifier la configuration des règles.
- Trop bas : le seuil peut être trop restrictif ou les données requises (par exemple, prévisions, niveaux de stock) peuvent être manquantes pour certains produits.

Spot-check quelques produits que vous connaissez bien et comparez ce que le système affiche par rapport à votre système source.

Aucune incidence financière visible sur les exceptions

L'impact financier nécessite que le coût unitaire soit renseigné dans les données du produit. Si le coût d'un produit est absent ou nul, aucune valeur monétaire ne sera affichée. Renseignez-vous auprès de votre équipe d'assistance sur la couverture des données sur les coûts : une approche en cascade couvrant plusieurs domaines de coûts fournit généralement la meilleure couverture.

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.