aws

Guía del administrador

Decisiones sobre Amazon Connect

Decisiones sobre Amazon Connect: Guía del administrador

Table of Contents

¿Qué es Amazon Connect Decisions?

Amazon Connect Decisions es una solución de planificación e inteligencia de la cadena de suministro con compañeros de equipo de IA que trabajan junto a su equipo armonizando las señales de demanda en previsiones consensuadas, generando planes de suministro sensibles a las restricciones y supervisando activamente sus operaciones para evitar problemas, resolverlos e identificar las causas fundamentales de la mejora continua.

Los compañeros de equipo de IA se adaptan a su forma de trabajar: se guían por sus normas y procedimientos operativos, se integran con sus sistemas actuales y aprenden de las decisiones de sus profesionales. Aprovecha la experiencia en la cadena de suministro de Amazon para ofrecer planes y recomendaciones eficaces desde el primer día.

Diriges un equipo de agentes de IA que se encargan de la coordinación y ejecutan las acciones, lo que te permite centrarte en las decisiones estratégicas que impulsan los niveles de servicio y la eficiencia del capital circulante.

Ventajas

Adáptese a su empresa

Los compañeros de equipo de IA se adaptan a su negocio, sus sistemas y sus decisiones, y transforman rápidamente sus flujos de trabajo actuales. Impulsados por sus procedimientos operativos y normas empresariales, sus compañeros de equipo trabajan con sus sistemas ERP y de planificación existentes. Aprenden de las decisiones de los planificadores, se alinean con sus prioridades e institucionalizan los conocimientos para que sus operaciones mejoren con el tiempo y todos los miembros del equipo sean más eficaces.

Adelántese a lo que viene

Dirija un equipo de agentes de inteligencia artificial que se encargue de la labor de coordinación 24/7: armonice las señales de demanda, genere planes que tengan en cuenta las limitaciones y ejecute las acciones aprobadas. Los compañeros de equipo también detectan patrones invisibles para el análisis manual, como las interrupciones en cascada de los proveedores o la desalineación del inventario en miles de SKU, y descubren lo que importa antes de que se convierta en un problema. Los planificadores pasan de la lucha reactiva a la planificación proactiva, gestionan operaciones más eficaces y mejoran los niveles de servicio mediante decisiones estratégicas que impulsan los resultados empresariales.

Genere confianza desde el primer día

Los compañeros de equipo de IA cuentan con el respaldo de una ciencia perfeccionada durante más de 30 años supervisando más de 400 millones de SKU de Amazon y equipados con herramientas especializadas en la cadena de suministro. Tu equipo se beneficia de la experiencia en el campo desarrollada por una de las redes de cadenas de suministro más complejas del mundo, que ofrece información y recomendaciones prácticas listas para usar con un razonamiento claro y explicable en el que puede confiar y verificar.

Capacidades

Inteligencia adaptativa

Los compañeros de equipo de IA aprenden de cada plan y decisión a través de un ciclo continuo: observan patrones, detectan lo que importa, recomiendan acciones y ejecutan las decisiones aprobadas. Esto institucionaliza el conocimiento: cuando los planificadores se van, la experiencia permanece; los nuevos miembros son productivos desde el primer día y mejoran los resultados sin necesidad de volver a capacitarse manualmente.

Exija inteligencia

Los compañeros de equipo de IA organizan de forma dinámica más de 18 herramientas de previsión y modelos básicos basados en los datos de Amazon, optimizándolos de forma autónoma a nivel de SKU. Genera previsiones precisas desde el primer día, incluso con un historial limitado. Armonice las previsiones estadísticas, los compromisos con los clientes y las aportaciones multifuncionales mediante una planificación consensuada y, al mismo tiempo, supervise continuamente la precisión.

Inteligencia de suministro

Los compañeros de equipo de IA generan planes de suministro con visión de futuro (versión preliminar) y agrupan de forma inteligente las excepciones en decisiones estratégicas clasificadas por impacto. Ejecute modelos de optimización para planificar en toda su red teniendo en cuenta las restricciones. Supervise las operaciones 24/7, descubra lo que importa y, a continuación, ejecute las decisiones aprobadas directamente en los sistemas existentes, reduciendo los ciclos de semanas a horas.

Incorporación de agentes

AI-powered Los agentes de incorporación lo guían durante la configuración mediante una conversación en lenguaje natural. Conecte datos fragmentados a través de JDBC o Amazon S3,

prepárelos para Connect Decisions y señale automáticamente los problemas antes de que afecten a las previsiones. Configure las reglas y políticas empresariales en un lenguaje sencillo con vistas previas en tiempo real y empiece a funcionar en semanas, no en meses.

Introducción

En esta sección, puede aprender a crear una instancia de Amazon Connect Decisions, conceder roles de permisos de usuario e iniciar sesión en la aplicación web Amazon Connect Decisions.

Requisitos previos para usar Amazon Connect Decisions

Antes de crear una instancia de Amazon Connect Decisions, asegúrese de completar los siguientes pasos:

- Tiene una AWS cuenta. Para crear una AWS cuenta, consulte Configuración de una cuenta de AWS.
- Asegúrese de que el Centro de identidades de IAM esté activado. Para activar el Centro de Identidad de IAM, consulte Habilitar el Centro de Identidad de IAM.
- Debe activarse una instancia de IAM Identity Center en la misma región en la que desea crear su instancia de Amazon Connect Decisions. Amazon Connect Decisions solo se admite en las regiones EE.UU. Este (Norte de Virginia) y Europa (Irlanda).
- Si la instancia de Amazon Connect Decisions no se encuentra en la misma región que su región actual del Centro de Identidad de IAM, póngase en contacto con nosotros para obtener más ayuda.
- Debe tener al menos un usuario en la instancia del Centro de Identidad de IAM para asignarlo como administrador de Amazon Connect Decisions. Puede conectar su Active Directory al Centro de Identidad de IAM. Para obtener más información, consulte Conectarse a un directorio de Microsoft AD.
- Añada cualquier usuario adicional que necesite acceder a Amazon Connect Decisions al IAM Identity Center.
- Necesita el servicio de administración de AWS claves (AWS KMS) para crear una instancia. Amazon Connect Decisions utiliza esta clave de AWS KMS para cifrar todos los datos que se incluyen en Amazon Connect Decisions. Para obtener información sobre las claves de AWS KMS, consulte Creación de claves.
- Si desea activar la función de acciones, tendrá que configurar una conexión con el sistema que utiliza para conservar los datos relevantes y proporcionar las credenciales para que las utilice Amazon Connect Decisions. Póngase en contacto con nosotros para obtener más ayuda.

Navegadores compatibles con Amazon Connect Decisions

Antes de trabajar con Amazon Connect Decisions, compruebe que su navegador es compatible con la siguiente tabla.

Navegador	Versiones compatibles
Google Chrome	Tres últimas versiones.
Mozilla Firefox ESR	Las versiones son compatibles hasta la fecha de fin de vida útil de Firefox. Para obtener más información, consulta el calendario de versiones ESR de Firefox.
Mozilla Firefox	Tres últimas versiones.
Microsoft Edge y Edge Chromium	Versión 84 y posteriores.
Safari	Safari 10 o posterior en macOS.

Idiomas compatibles con Amazon Connect Decisions

Amazon Connect Decisions admite los siguientes idiomas:

- English (EE. UU.)

Configuración de una cuenta de AWS

Utilice esta sección para crear una AWS cuenta y un usuario de IAM. Para obtener información sobre las prácticas recomendadas para crear una AWS cuenta, consulte Cómo establecer un AWS entorno de prácticas recomendadas.

Inscríbase en una AWS inscrita

Si no tiene una AWS cuenta, complete los siguientes pasos para crear una.

Para registrarte en una AWS inscrita

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica o mensaje de texto e indicar un código de verificación en el teclado del teléfono.

   Al abrir una AWS cuenta, se crea un usuario raíz de la AWS cuenta. Este usuario tiene acceso a todos los recursos y los servicios de AWS en la cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar Tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando My Account (Mi cuenta).

Creación de un usuario con acceso administrativo

Después de crear una AWS cuenta, proteja el usuario raíz de la AWS cuenta, active el Centro de identidad de AWS IAM y cree un usuario administrativo para no utilizar el usuario raíz en las tareas diarias.

Proteja su AWS usuario raíz de la cuenta

1. Inicie sesión en la consola de administración de AWS como el propietario de la cuenta; para ello, elija Usuario raíz e introduzca la dirección de email de su cuenta de AWS . En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In.
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario raíz de su AWS cuenta (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

Para obtener instrucciones, consulte Habilitar el Centro de Identidad de AWS IAM en la Guía del usuario del Centro de Identidad de AWS IAM.

2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre el uso del directorio del Centro de Identidad de IAM como fuente de identidad, consulte Configurar el acceso de los usuarios con el directorio predeterminado del Centro de Identidad de IAM en la Guía del usuario del Centro de Identidad de AWS IAM.

Inicio de sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, use la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del usuario.AWS Sign-In

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

   Para obtener instrucciones, consulte Crear un conjunto de permisos en la Guía del usuario del AWS IAM Identity Center.

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

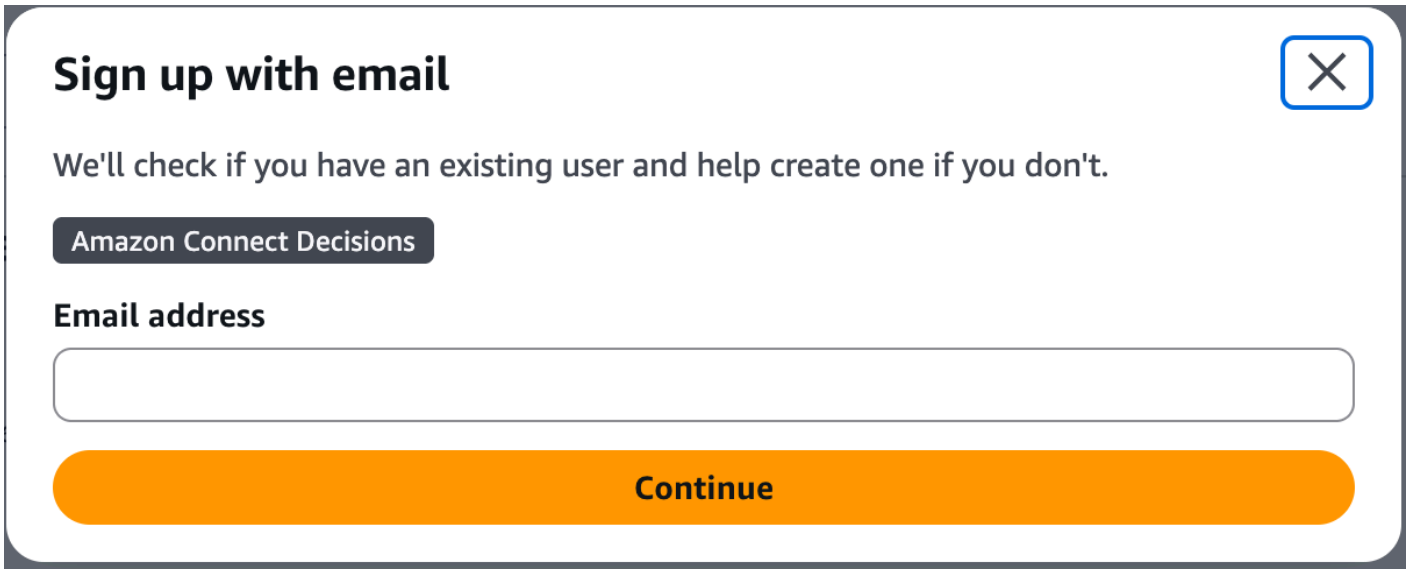
   Para obtener instrucciones, consulte Añadir grupos en la Guía del usuario del AWS IAM Identity Center.

Configuración de la integración de AWS Identity Center

Para crear una instancia y utilizar el servicio Amazon Connect Decisions, debe conectar un perfil de usuario del Centro de identidades de IAM existente o crear uno nuevo.

1. Abra la consola de Amazon Connect Decisions. También puede buscar «Amazon Connect Decisions» en la consola de AWS administración principal.

2. Si es necesario, cambie la región de AWS seleccionando Seleccionar una región en la parte superior de la consola. Elija su región en la lista desplegable.
3. Seleccione Crear instancia de Amazon Connect Decisions. Aparecerá una notificación.



4. Introduce tu dirección de correo electrónico y selecciona Continuar. iDC verificará si el correo electrónico coincide con un usuario existente.
5. Realice una de las siguientes acciones:
   - Si iDC hace coincidir la dirección de correo electrónico con la de un usuario, selecciona Conectar tu fuente de identidad e incorpora a tu equipo.

     > **Note**
     >
     > Esto se puede usar si su organización tiene una instancia de iDC establecida que le gustaría usar para las decisiones de Amazon Connect.

   - Si iDC no encuentra ninguna coincidencia con un usuario existente, aparece una notificación de creación de un nuevo usuario. Continúe con el siguiente paso.
6. En la notificación, introduce lo siguiente y, a continuación, selecciona Continuar:
   - Dirección de correo electrónico
   - Nombre
   - Apellido

   iDC crea el usuario automáticamente y lo añade como administrador de Amazon Connect Decisions.

7. Realice una de las siguientes acciones:
   - Para crear una instancia con la configuración estándar, seleccione Crear. Consulte Usar la configuración estándar.
   - Para crear una instancia con una configuración personalizada, seleccione Editar en la configuración avanzada. Consulte Usar una configuración avanzada.

Cuando se utiliza junto con el Centro de identidad de IAM, Amazon Connect Decisions recupera los campos «nombre de usuario» y «correo electrónico» del directorio del Centro de identidad de IAM. Ninguno de estos atributos se almacena de forma nativa en la instancia de Amazon Connect Decisions y siempre se recupera en tiempo de ejecución. Amazon Connect Decisions cifra estos atributos de identidad en reposo mediante una clave de AWS KMS propia de forma predeterminada. Las claves de KMS gestionadas por el cliente no se admiten en Amazon Connect Decisions. Si eliminas un usuario de tu instancia del Centro de Identidad de AWS IAM, Amazon Connect Decisions también elimina ese usuario de tu instancia.

Gestión de la instancia de Amazon Connect Decisions

Al crear una instancia en Amazon Connect Decisions, se establece un entorno específico para la gestión y el análisis de la cadena de suministro. Para configurar una instancia, debe configurar los detalles básicos, establecer los ajustes y definir los permisos de acceso iniciales de los usuarios.

Solo el administrador de la consola de AWS administración puede crear una instancia. El administrador AWS de Management Console que crea la instancia de Amazon Connect Decisions debe tener todos los permisos enumerados en los ejemplos Identity-based de políticas. Este administrador debe invitar a un usuario de IAM como administrador de Amazon Connect Decisions para gestionar Amazon Connect Decisions.

En las siguientes páginas se describe en detalle el proceso de creación y eliminación de una instancia.

Cómo crear tu instancia

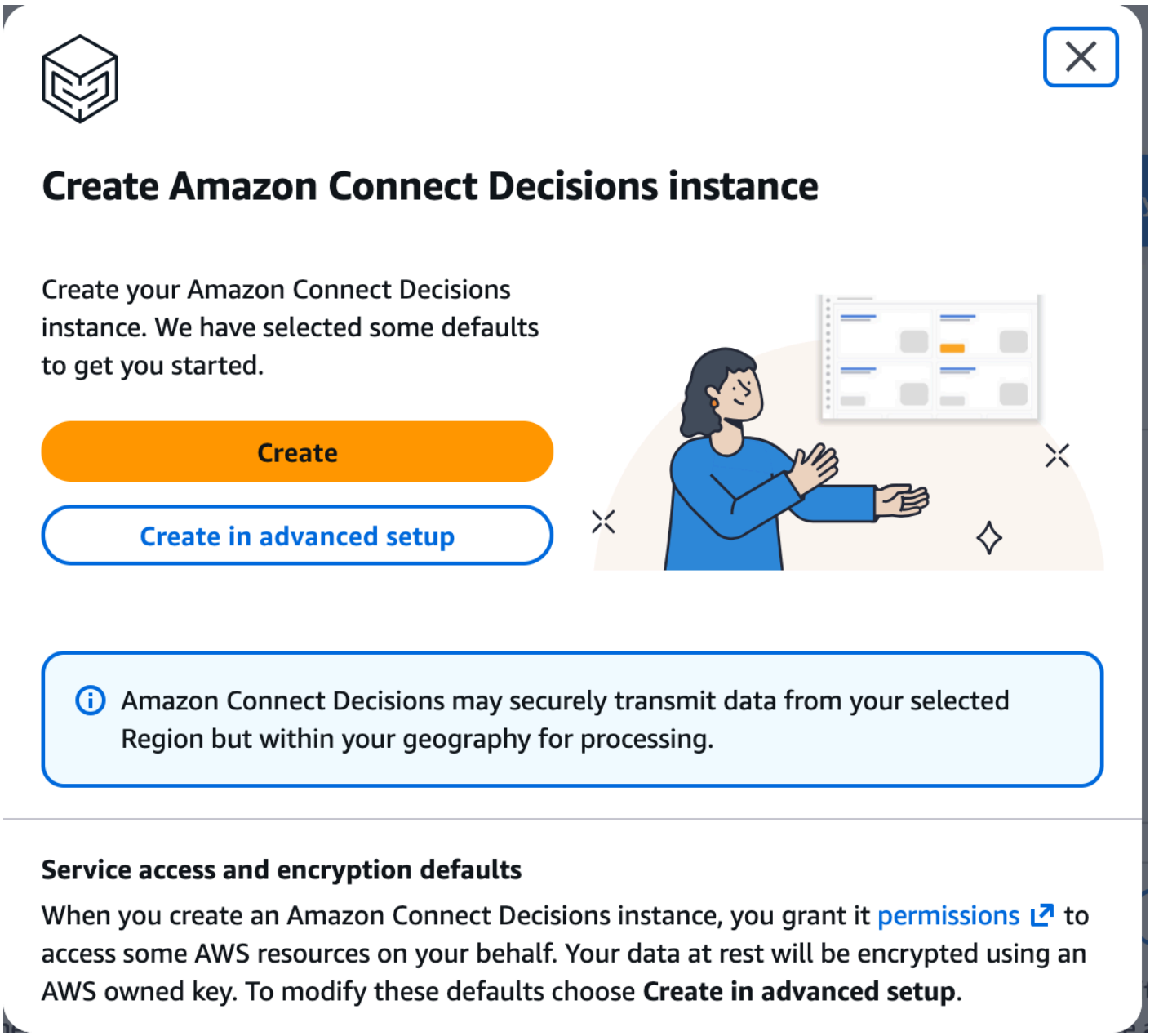
Para crear una instancia, utilice uno de los dos métodos siguientes: configuración estándar o configuración avanzada. La configuración estándar utiliza un proceso automatizado que crea la instancia rápidamente mediante parámetros preestablecidos. La configuración avanzada le permite personalizar la instancia mediante el establecimiento de sus propios parámetros.

Uso de la configuración estándar

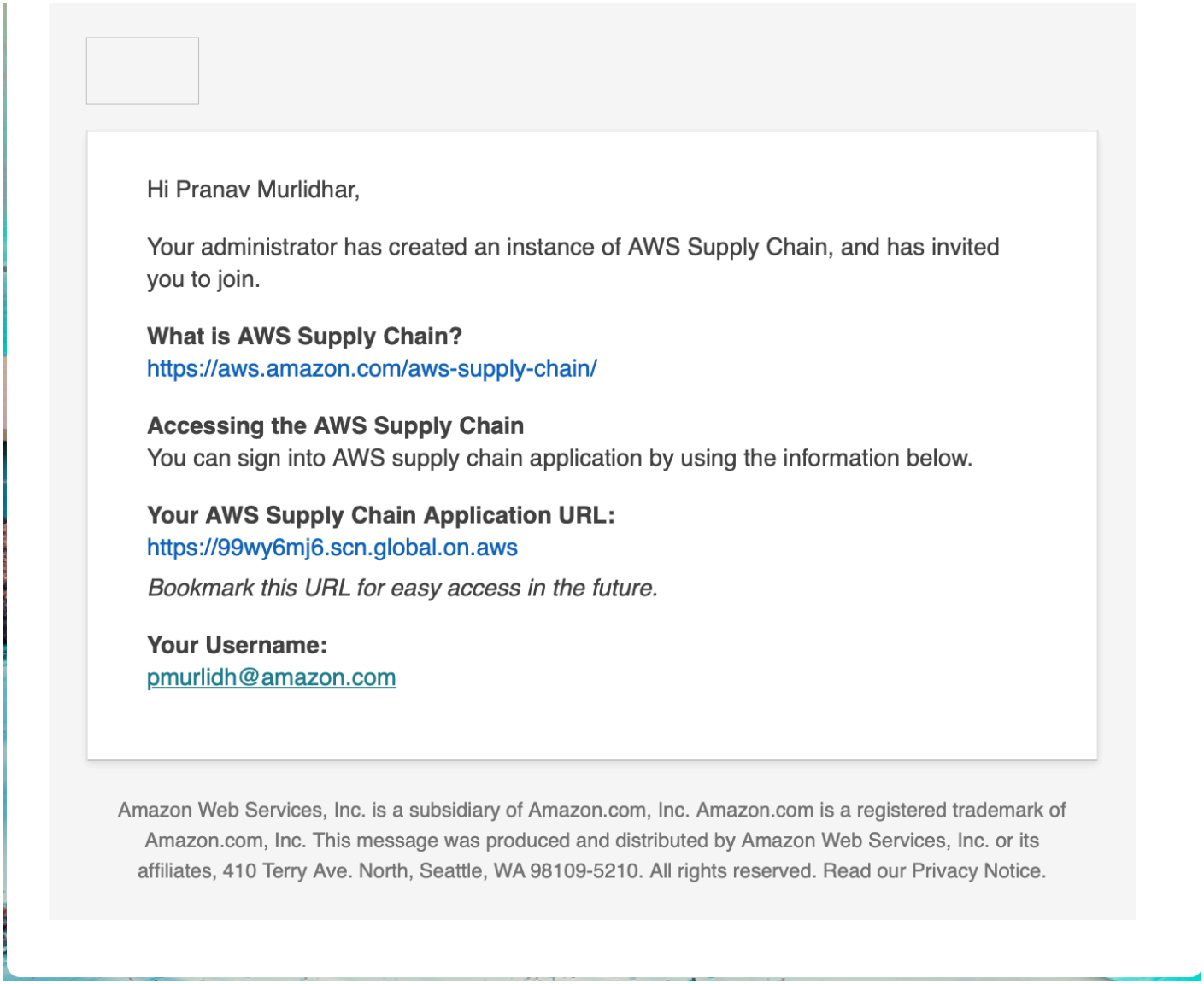
La configuración estándar crea la instancia de Amazon Connect Decisions con la configuración de seguridad y cifrado predeterminada. Las instancias funcionan en regiones AWS geográficas. Para obtener más información sobre las regiones, consulte Regiones y puntos finales en la Guía del usuario de IAM y Puntos finales regionales en la AWS Referencia general.

Para crear una instancia de Amazon Connect Decisions con una configuración estándar de parámetros preestablecidos, siga estos pasos.

1. Seleccione Crear.



2. Compruebe en su correo electrónico lo siguiente:
   - Un correo electrónico del equipo de iDC.
   - Un correo electrónico del equipo de gestión de identidad.



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

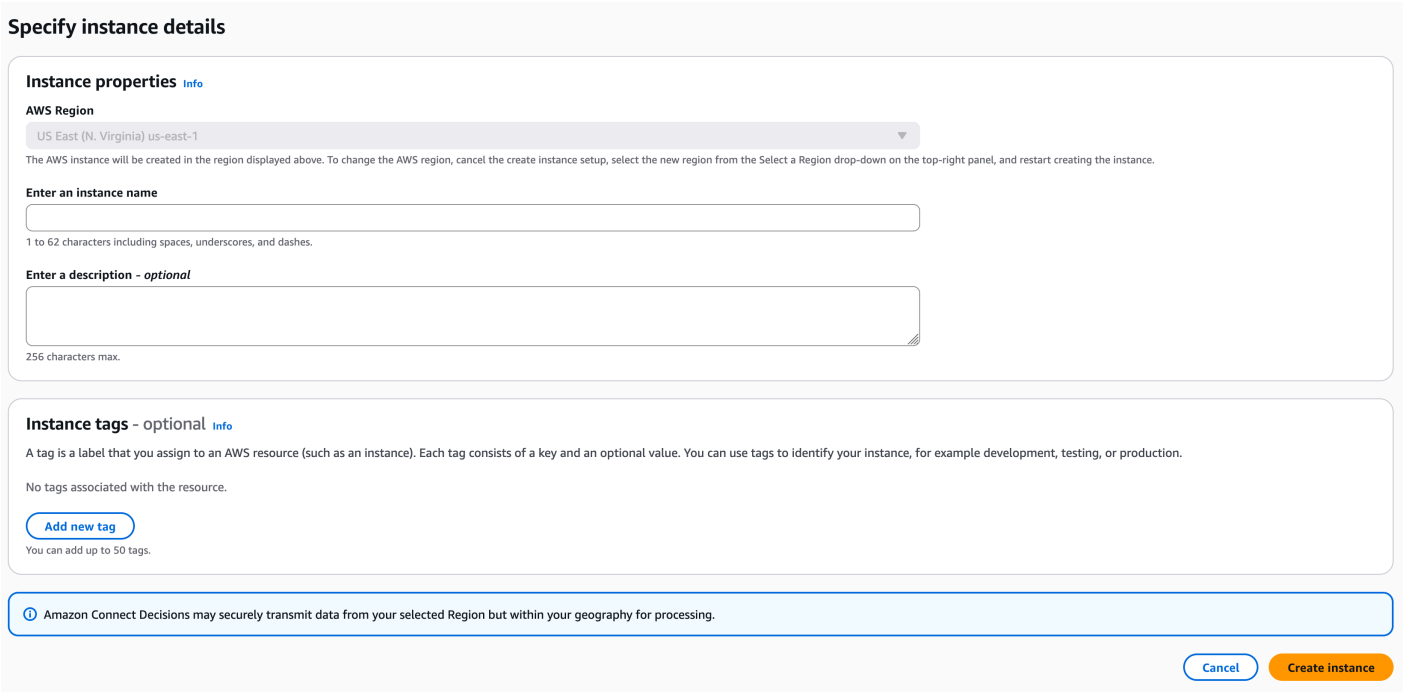
Amazon Web Services, Inc. is a subsidiary of Amazon.com, Inc. Amazon.com is a registered trademark of Amazon.com, Inc. This message was produced and distributed by Amazon Web Services, Inc. or its affiliates, 410 Terry Ave. North, Seattle, WA 98109-5210. All rights reserved. Read our Privacy Notice.

3. Cuando reciba el correo electrónico de invitación, inicie sesión en Amazon Connect Decisions. Consulte Iniciar sesión en la aplicación web Amazon Connect Decisions.

Uso de una configuración avanzada

La configuración avanzada le permite personalizar la instancia mediante el establecimiento de sus propios parámetros. Para crear una instancia de Amazon Connect Decisions mediante una configuración avanzada de parámetros preestablecidos, siga estos pasos.

1. Seleccione Crear en la configuración avanzada.
2. Aparecerá la página de propiedades de la instancia.



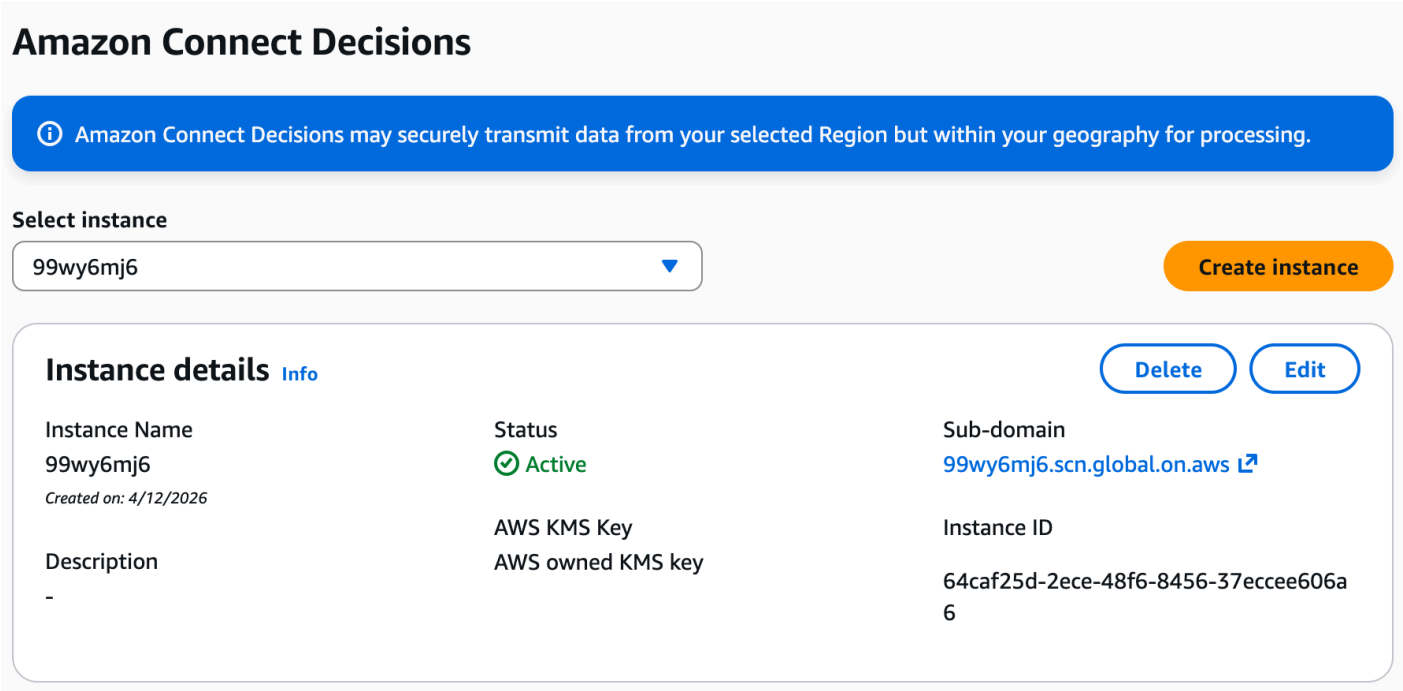
3. Introduzca lo siguiente en la página de propiedades de la instancia:
   - Nombre: introduzca un nombre de instancia.
   - Descripción: introduzca una descripción de su instancia de Amazon Connect Decisions (p. ej., instancia de producción, instancia de prueba, etc.).
   - Etiquetas de instancia: puede añadir etiquetas a su instancia para utilizarlas como identificación. Por ejemplo, puedes añadir una etiqueta para definir el tipo de instancia que vas a crear (p. ej., de producción, de prueba, UAT, etc.).
4. Selecciona Crear instancia.

Eliminación de una instancia

Para eliminar una instancia, sigue estos pasos.

> **Note**
>
> Al eliminar una instancia, la información del bucket de Amazon S3 no se elimina automáticamente.

1. Abra la consola de Amazon Connect Decisions en https://console.aws.amazon.com/scn/home.
2. En el panel de control de la consola Amazon Connect Decisions, en el menú desplegable, selecciona la instancia que quieres eliminar.



3. Elija Eliminar.
4. En la página Eliminar instancia de Amazon Connect Decisions, en Confirmación, escriba `delete` para confirmar que desea eliminar la instancia.
5. Elija Eliminar. Se inicia la eliminación de la instancia y, una vez eliminada, verá un mensaje de confirmación.

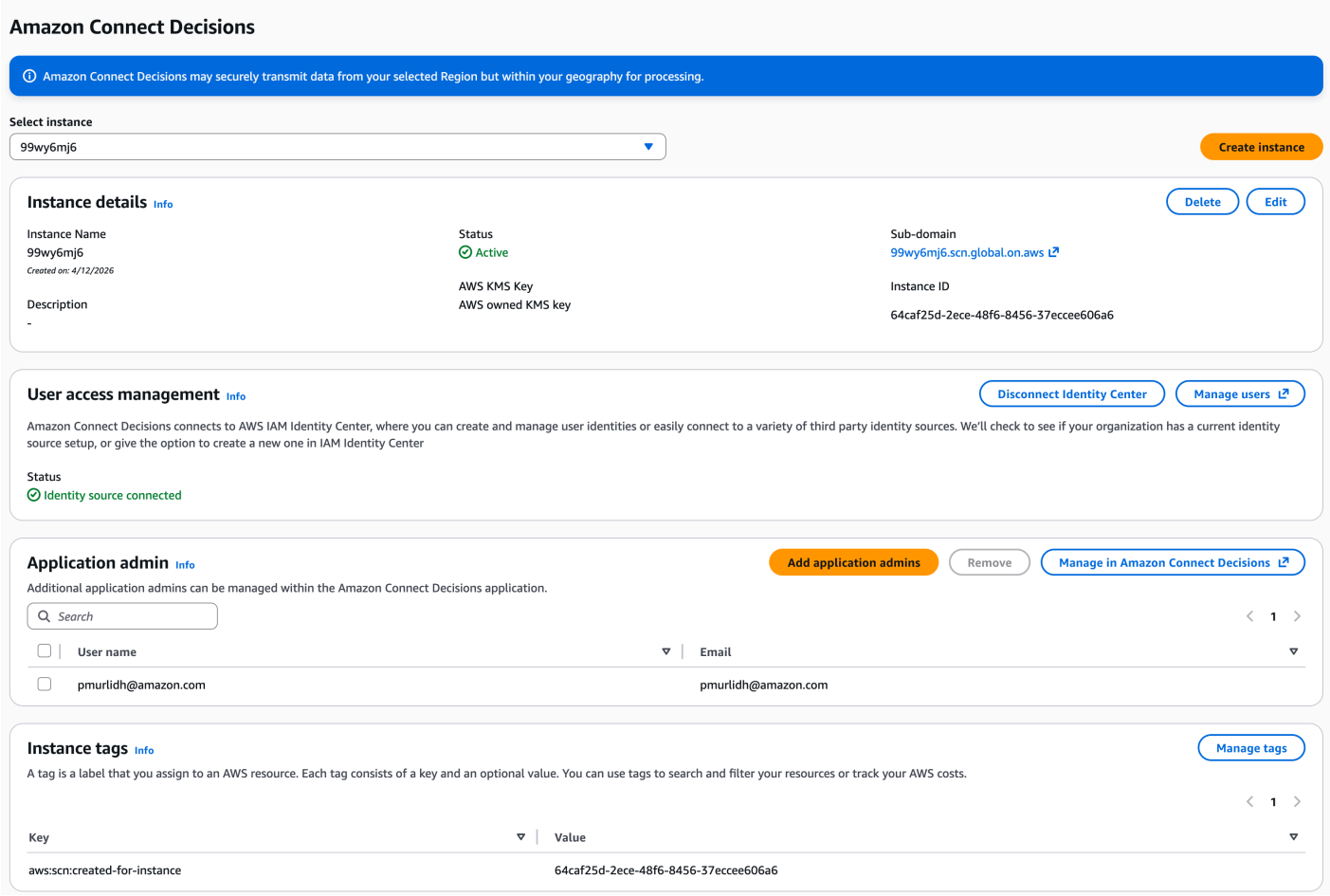
Elige un administrador de la aplicación

Como administrador de AWS la consola, debe elegir un administrador de la aplicación Amazon Connect Decisions para gestionar el acceso a la aplicación web Amazon Connect Decisions. El administrador de la aplicación Amazon Connect Decisions puede añadir o eliminar funciones de permisos de usuario en la aplicación web Amazon Connect Decisions.

Una vez creada la instancia y conectada una fuente de identidad, siga estos pasos para elegir un administrador de la aplicación Amazon Connect Decisions.

1. Abra el panel de control de la consola de Amazon Connect Decisions.

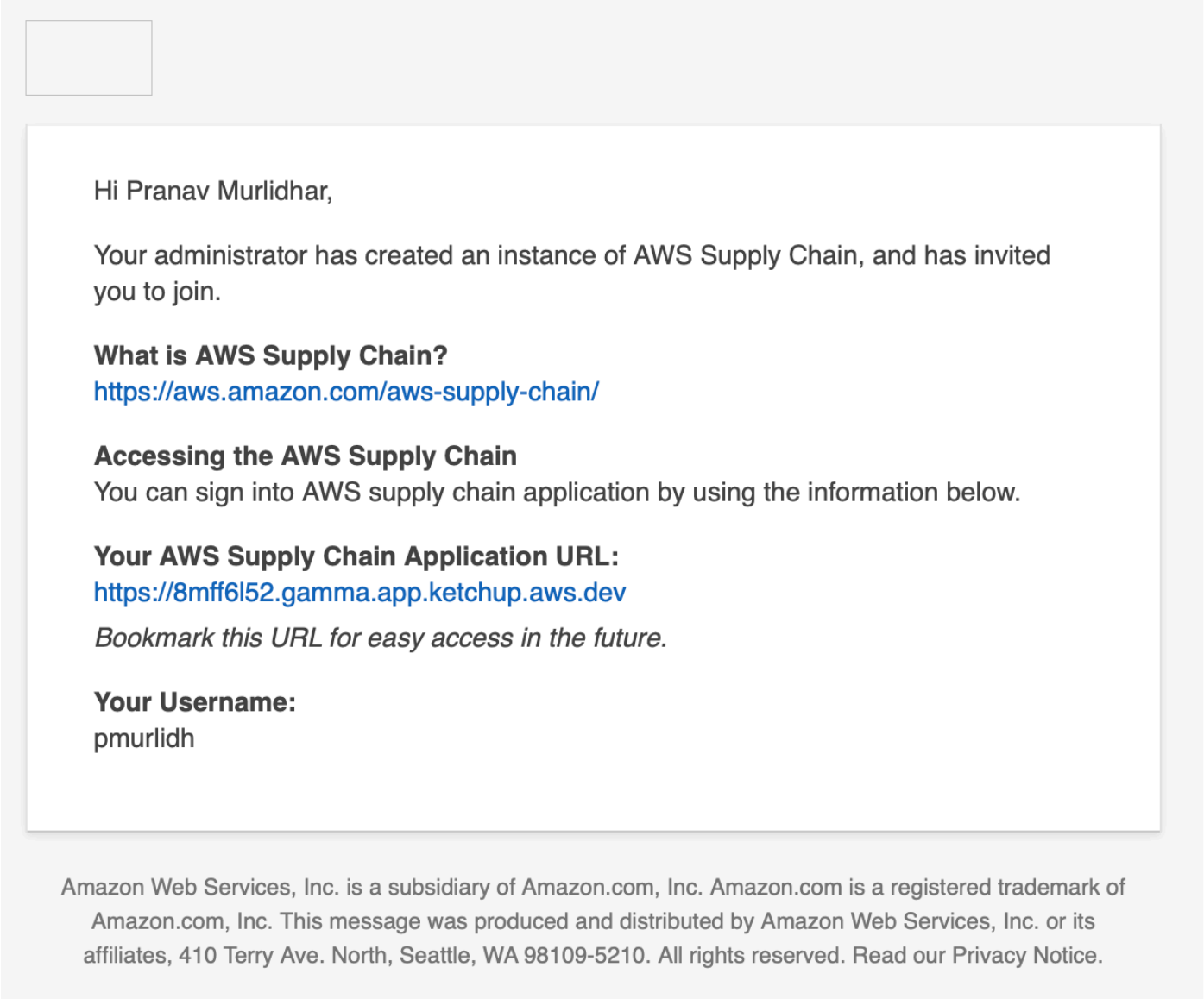
2. Vaya a Select application admin y seleccione un usuario para que sea administrador de la aplicación Amazon Connect Decisions. Los resultados de la búsqueda solo muestran los usuarios que coinciden con los criterios de búsqueda.



3. (Opcional) Seleccione Ir al centro de identidad de IAM para añadir más usuarios. Para obtener más información sobre cómo añadir usuarios, consulte Administrar su fuente de identidad en la Guía del usuario de AWS IAM Identity Center y, para obtener más información sobre las funciones de permisos de usuario, consulte Funciones de permisos de usuario.

> **Note**
>
> Solo puede añadir un usuario a la vez desde la consola de decisiones de Amazon Connect. No puede añadir un grupo como administrador de aplicaciones en Amazon Connect Decisions.

4. Seleccione Enviar invitación. Se envía un correo electrónico al administrador de la aplicación web. Una vez que el administrador de la aplicación web reciba el correo electrónico de invitación, podrá seleccionar la URL de la aplicación e iniciar sesión en 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.

En la aplicación web Amazon Connect Decisions, verá el usuario en la lista Administrador de aplicaciones.

Acceder a su instancia

El uso de la consola es la forma más sencilla de administrar los recursos y las configuraciones del servicio. La consola proporciona una interfaz web intuitiva en la que puede ver, crear, modificar y supervisar sus recursos.

Para acceder a la consola de Amazon Connect Decisions, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de Amazon Connect Decisions de su AWS cuenta. Si crea una política basada en identidades que sea más

restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No necesita conceder permisos mínimos de consola a los usuarios que solo realizan llamadas a la API o a la AWS API. En su lugar, permita el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Como administrador de Amazon Connect Decisions, debería haber recibido una invitación por correo electrónico a la aplicación web Amazon Connect Decisions.

1. Puede elegir el enlace en el correo electrónico o en el panel de control de la consola de Amazon Connect Decisions Sub-domain, en Elija la URL web.
2. Aparece la página de inicio de sesión de la aplicación web Amazon Connect Decisions.
3. Introduzca las credenciales de usuario del AWS IAM Identity Center y seleccione Iniciar sesión.
4. Cada usuario que haya agregado recibirá un mensaje de correo electrónico con un enlace a Amazon Connect Decisions, o puede elegir Copiar enlace y enviar el enlace a los usuarios.

Tras iniciar sesión correctamente, accederá a su página de inicio personalizada. Consulta Cómo entender tu página de inicio en la guía del usuario para entender mejor tu página de inicio.

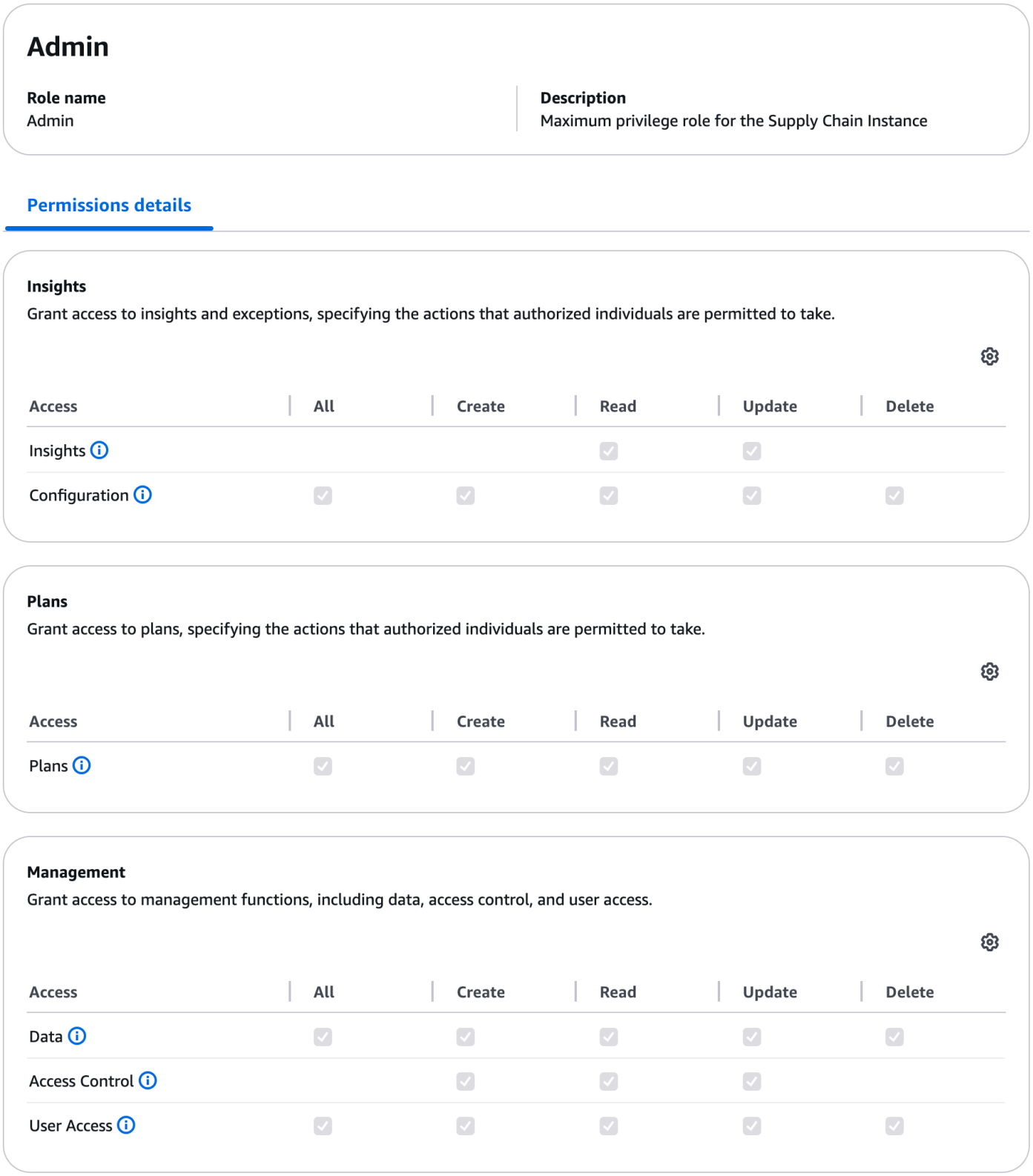
Control de acceso

Amazon Connect Decisions proporciona una gestión de acceso de nivel empresarial que le proporciona un control preciso sobre quién puede acceder a qué datos y realizar qué acciones dentro de su instancia. Esto garantiza que sus usuarios solo vean la información relevante para sus responsabilidades y, al mismo tiempo, mantienen los estándares de seguridad y cumplimiento que exige su organización.

Descripción general de las funciones y los permisos

Como administrador de Amazon Connect Decisions, puede utilizar las funciones de permisos de usuario predeterminadas o crear funciones de permisos personalizadas. Amazon Connect Decisions tiene las siguientes funciones de permisos de usuario predeterminadas:

- Administrador: acceso para crear, ver y administrar todos los datos y permisos de usuario.



Admin

Role name
Admin

Description
Maximum privilege role for the Supply Chain Instance

Permissions details

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

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

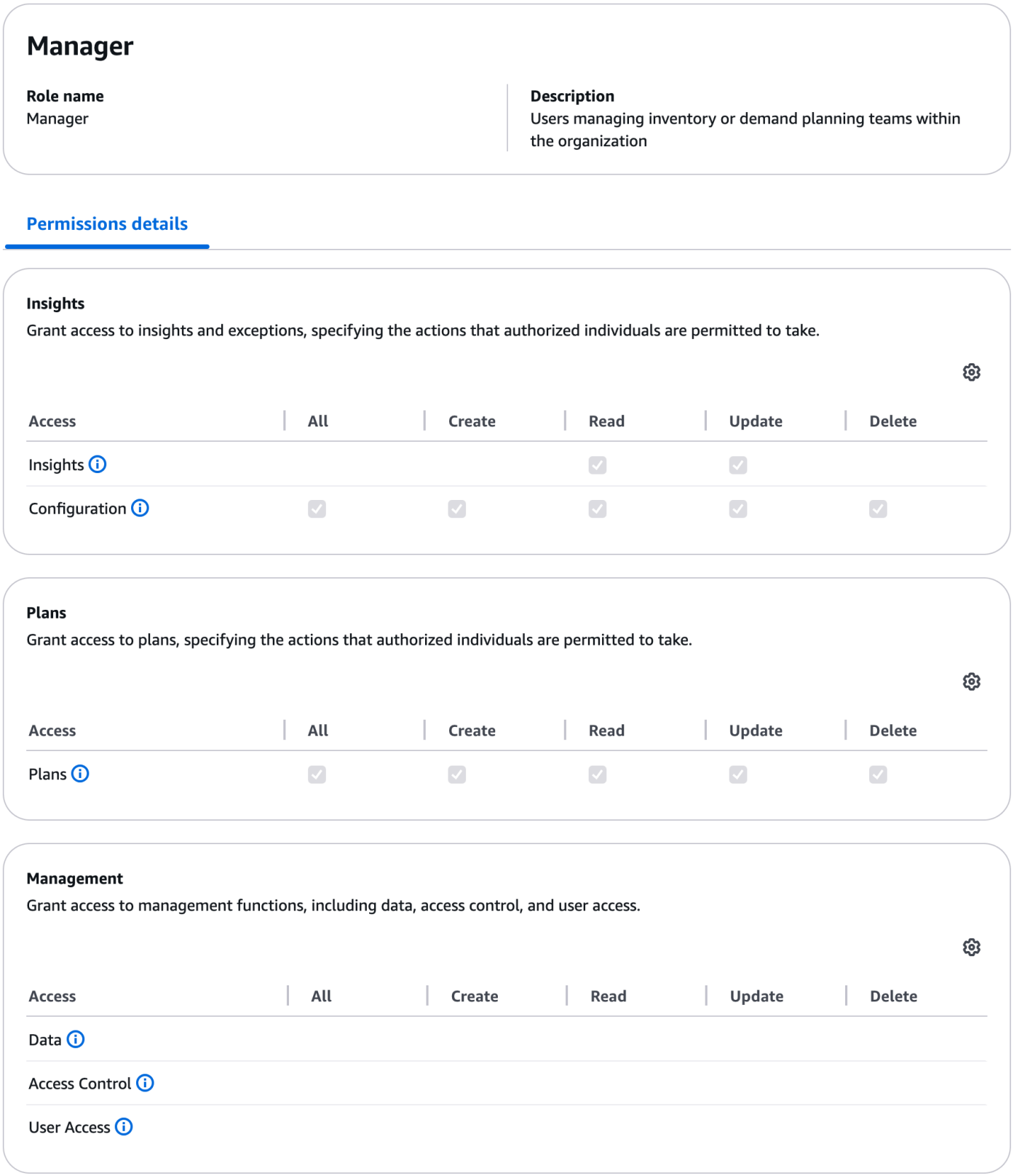
Plans
Grant access to plans, specifying the actions that authorized individuals are permitted to take.

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

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

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

- Administrador: acceso para crear, ver y administrar lo siguiente.



Manager

Role name
Manager

Description
Users managing inventory or demand planning teams 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					

- Planificador: permite crear, ver y gestionar lo siguiente.

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**
>
> Como administrador de Amazon Connect Decisions, antes de añadir usuarios, tenga en cuenta lo siguiente:
>
> - Cada rol de permisos de usuario predeterminado se define con un conjunto de permisos. Puede agregar usuarios a los roles de permisos de usuario predeterminados o crear roles de permisos personalizados.
> - A un usuario solo se le puede asignar un rol de permisos de usuario.
> - Los roles de permisos de usuario predeterminados no se pueden editar.
> - Al editar un rol de permisos personalizado que ha creado, se actualizan los permisos de todos los usuarios del rol de permisos personalizado.
> - Cuando eliminas un rol de permiso personalizado que hayas creado, todos los usuarios del rol de permiso personalizado perderán el acceso a Amazon Connect Decisions.
> - No se admite la adición de grupos en Amazon Connect Decisions.

Administrar las funciones de permisos de usuario

Añadir usuarios

Como administrador de Amazon Connect Decisions, puede añadir usuarios para que accedan a la aplicación web Amazon Connect Decisions. Los usuarios primero deben añadirse al Centro de identidades de IAM (iDC) y, a continuación, pueden añadirse a Amazon Connect Decisions. Para obtener más información sobre cómo añadir usuarios a iDC, consulte Asignar acceso a usuarios.

Una vez que se hayan agregado los usuarios a iDC, siga estos pasos para agregar un usuario.

1. Selecciona la configuración en el cajón del lado izquierdo
2. Selecciona Usuarios. Seleccione Asignar usuarios
3. Busque para identificar al usuario. Puede buscar mediante el nombre para mostrar, el correo electrónico, el nombre, los apellidos y el nombre de usuario
4. Seleccione los usuarios que desee añadir.
5. Asígneles un rol. Consulte la descripción general de las funciones y los permisos para obtener más información sobre las funciones de los usuarios en Amazon Connect Decisions.

6. Seleccione Asignar. Confirme que sus selecciones son correctas.

Actualización de permisos de usuario

Para actualizar el rol de permiso de usuario de los usuarios actuales de Amazon Connect Decisions, siga estos pasos.

1. Selecciona los ajustes en el cajón del lado izquierdo
2. Selecciona Usuarios. Seleccione Asignar usuarios
3. En la lista de usuarios, seleccione el usuario para abrir la página de detalles del usuario.
4. Utilice el menú desplegable del rol para actualizar los permisos del rol del usuario.
5. Confirme que desea cambiar el rol haciendo clic en el botón de cambio de rol

Eliminación de usuarios

Como administrador de Amazon Connect Decisions, puede eliminar usuarios de la aplicación web Amazon Connect Decisions. Siga estos pasos para eliminar usuarios.

1. Selecciona los ajustes en el cajón de la izquierda
2. Selecciona Usuarios. Seleccione Asignar usuarios
3. En la lista de usuarios, seleccione el usuario para abrir la página de detalles del usuario.
4. Seleccione Eliminar.
5. Confirme que desea eliminar el usuario haciendo clic en el botón Eliminar

Configurar el acceso a nivel de atributo

Attribute-Based El control de acceso (ABAC) añade un nivel adicional de precisión al restringir el acceso en función del contexto empresarial. Al utilizar los atributos del producto y del sitio, puede asegurarse de que los planificadores solo vean los detalles de los productos y ubicaciones específicos que administran, mientras que los gerentes mantienen la visibilidad de las áreas de responsabilidad de sus equipos.

Cualquier usuario con el rol de «administrador» puede configurar el acceso por producto y sitio para otros usuarios:

1. Dirígete a la página de usuarios desde la barra de navegación izquierda.
2. En la lista de usuarios de esa instancia, selecciona el usuario que necesita configuración.
3. De forma predeterminada, en la sección Acceso a los datos, los usuarios tendrán habilitada la opción «Conceder acceso total a todos los productos y sitios». Cuando esta opción está activada, proporciona acceso a todos los productos y sitios (tal y como funcionaba antes del lanzamiento).
4. Si desactivas «Otorgar acceso completo a todos los productos y sitios», aparecerá la sección de configuración de los productos y sitios. No se asignará ningún producto o sitio cuando se acceda por primera vez.
5. Haga clic en el Add/Remove botón correspondiente a los productos o sitios en función de lo que necesite configurar. Utilice la búsqueda para buscar y seleccionar los elementos necesarios para ese usuario.
6. A varios usuarios se les puede asignar el mismo producto o sitio. Un usuario puede tener un máximo de 1000 combinaciones de productos y sitios.
7. Los productos o sitios configurados anteriormente se pueden eliminar mediante la misma interfaz.
8. Revise y confirme la lista completa de adiciones y eliminaciones en la última página del asistente para completar la configuración de acceso.

Una vez que se haya configurado el acceso al producto y al sitio, se restringirá el acceso de ese usuario en función de las siguientes asignaciones:

- Todos los usuarios pueden ver cualquier página de excepciones o recomendaciones, independientemente de si se generó para un producto o un sitio incluido en su control de acceso.
- Para realizar acciones mutantes (como descartar una excepción o cambiar el estado de En curso a Completado), los usuarios deben tener el producto o sitio correspondiente configurado en su control de acceso.
- Los usuarios con el control de acceso configurado también pueden utilizar la asignación de usuarios y el conmutador de visualización de acceso.

Asignación de usuarios

La asignación de usuarios es una función que facilita el equilibrio de la información entre varios usuarios. Con la asignación de usuarios, los clientes pueden asignar información específica a los usuarios para reflejar mejor cómo se comparten estas tareas en la vida real. Funciona de la siguiente manera:

- Siempre que se crea una excepción, el sistema compara el producto y el sitio para los que se ha creado la excepción con todos los usuarios que tienen el mismo producto o sitio configurado para su control de acceso
- Si el sistema encuentra un usuario que coincide, el campo Asignado a de esa excepción se actualiza con el nombre de usuario. En los casos en que más de un usuario tiene productos o sitios que coinciden con la excepción, se asigna aleatoriamente a uno de ellos
- Solo se puede asignar un usuario a cada excepción, pero se puede reasignar una excepción a otro usuario si es necesario. Solo se puede reasignar a un usuario con acceso a un producto o sitio
- Auto-assignment ya que la información se produce cuando se crea la excepción por primera vez. La información creada anteriormente no se reasignará automáticamente. Además, si se elimina un usuario o se actualiza su control de acceso, la asignación de usuario no se actualiza automáticamente
- En la página de listados de información, el usuario puede filtrar por la dimensión Asignado a para identificar fácilmente toda la información que se le ha asignado. También pueden usar este mismo filtro para ver la información no asignada. Por el momento, la asignación de usuarios solo está disponible para información

Incorporación de datos

Conectando sus datos

Requisitos previos

Antes de iniciar la incorporación de datos, asegúrese de disponer de lo siguiente:

- Instancia de decisiones de Amazon Connect
  - Su instancia ya debería estar creada con un bucket de S3 asociado
- Datos preparados
  - Trabaje con su homólogo de Amazon Customer Success para determinar qué datos necesita en función de cómo piensa utilizar Amazon Connect Decisions. Los requisitos de datos básicos incluyen:
    - Sales/Order Historial: más de 12 meses de registros de transacciones
    - Detalles del producto: catálogo completo de productos con especificaciones
    - Site/Location Información: almacenes, centros de distribución, puntos de venta
    - Existencias de inventario actuales: On-hand inventario en cada ubicación
  - Todos los datos de origen en formato CSV con UTF-8 codificación

Inicio de sesión por primera vez: cuestionario de incorporación

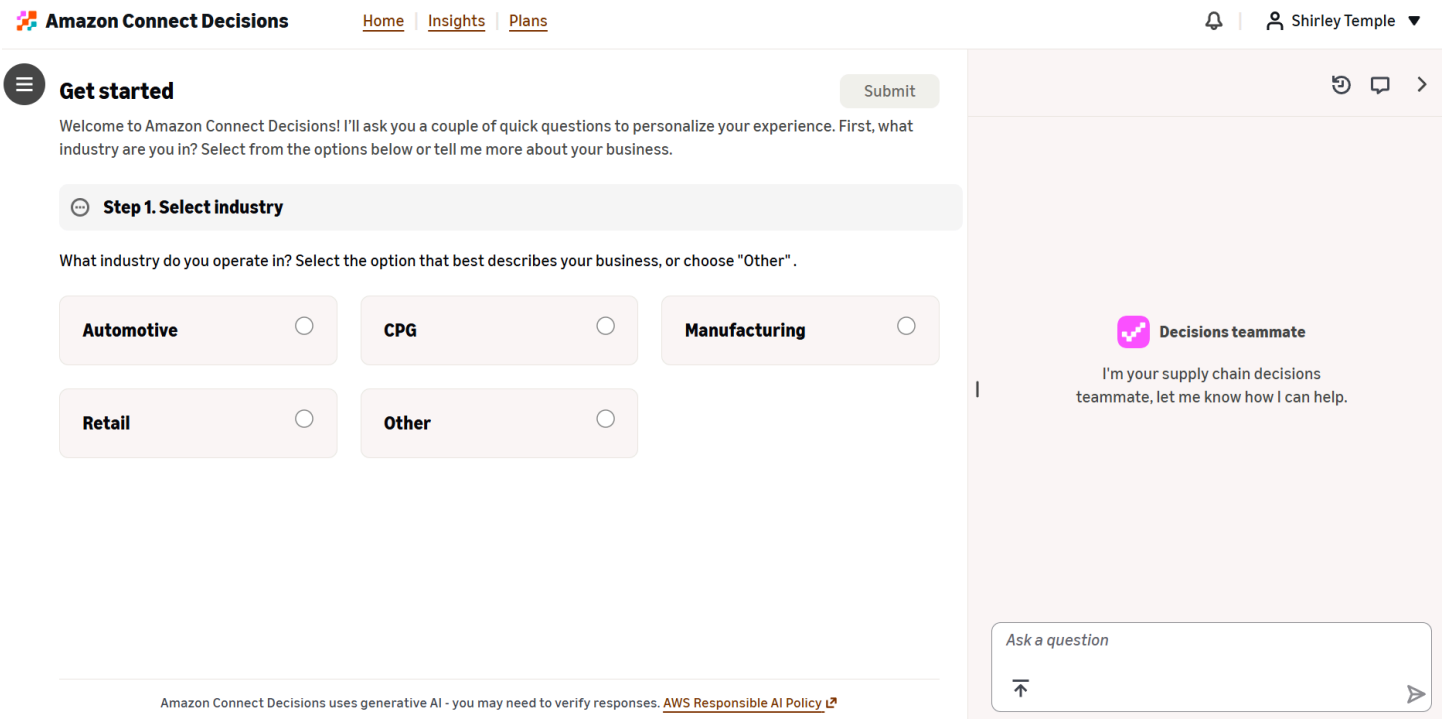
Cuando inicia sesión en Amazon Connect Decisions por primera vez, el sistema presenta un cuestionario de incorporación guiado. Este asistente de personalización ayuda a los compañeros de equipo de Decisions a contextualizar las capacidades más relevantes para su empresa. El cuestionario recopila información sobre su sector, los principales desafíos empresariales y el enfoque preferido de planificación. Sus respuestas ayudarán a optimizar los pasos de incorporación en función de su selección, lo que permitirá al sistema agilizar los flujos de trabajo de configuración posteriores y descubrir las rutas de configuración más relevantes para su empresa. Debe completar todos los pasos antes de acceder a la aplicación completa. El compañero de equipo de Decisions está disponible durante todo el proceso de incorporación a través de la barra lateral derecha para responder a las preguntas en tiempo real.

> **Note**
>
> Esta selección solo se realiza una vez al iniciar sesión por primera vez. Sus respuestas proporcionan un contexto adicional para optimizar las siguientes etapas de incorporación y ayudar a los agentes a entender su entorno empresarial. Todas las capacidades siguen siendo totalmente accesibles, independientemente de sus selecciones.

Paso 1: Seleccione la industria

Lo que ve: un mensaje de bienvenida y un conjunto de botones de radio que le piden que seleccione el sector que mejor describa su negocio.

1. Seleccione el botón de radio que mejor represente a su empresa.
2. Si no se aplica ninguna de las opciones predefinidas, seleccione Otras.



Paso 2: Defina su mayor desafío

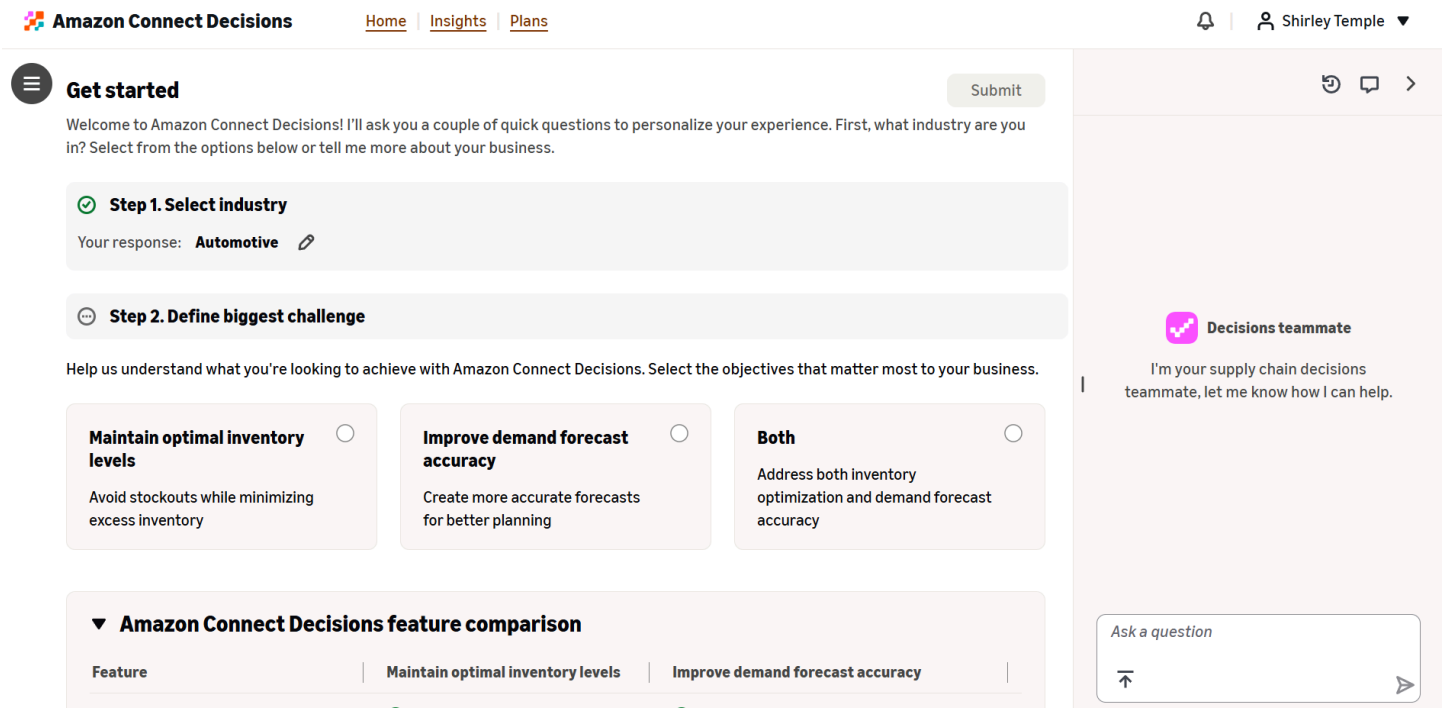
Lo que ves: tu respuesta al paso 1 se muestra con una opción de edición. A continuación, se le pide que identifique su principal desafío empresarial entre tres opciones. Se muestra una tabla de

comparación de características para ayudarle a entender qué capacidades están asociadas a cada selección.

1. Revise las opciones. Consulte la siguiente tabla para ver las opciones disponibles y su significado.
2. Selecciona el botón de radio que represente tu desafío más urgente.
3. Si lo desea, consulte la tabla de comparación de funciones situada debajo de las opciones para comprender qué incluye cada selección.

Opciones para los desafíos empresariales

Opción	Description (Descripción)	Funciones clave habilitadas
Mantenga niveles de inventario óptimos	Elija esta opción si su principal desafío es evitar los desabastecimientos y, al mismo tiempo, minimizar el exceso de inventario.	Optimización del inventario; prevención del agotamiento de existencias; reducción del exceso de inventario; planificación del suministro; seguimiento de los plazos de entrega de los proveedores
Mejore la precisión de las previsiones de demanda	Elija esta opción si su principal desafío es crear previsiones más precisas para tomar mejores decisiones de planificación.	Previsión de referencia; planificación por consenso; seguimiento de la precisión de Forecast
Ambos	Elija esta opción si necesita abordar simultáneamente la optimización del inventario y la precisión de la previsión de la demanda.	Todas las funciones específicas de la oferta y la demanda están habilitadas



Paso 3: Elija su enfoque de planificación de inventario

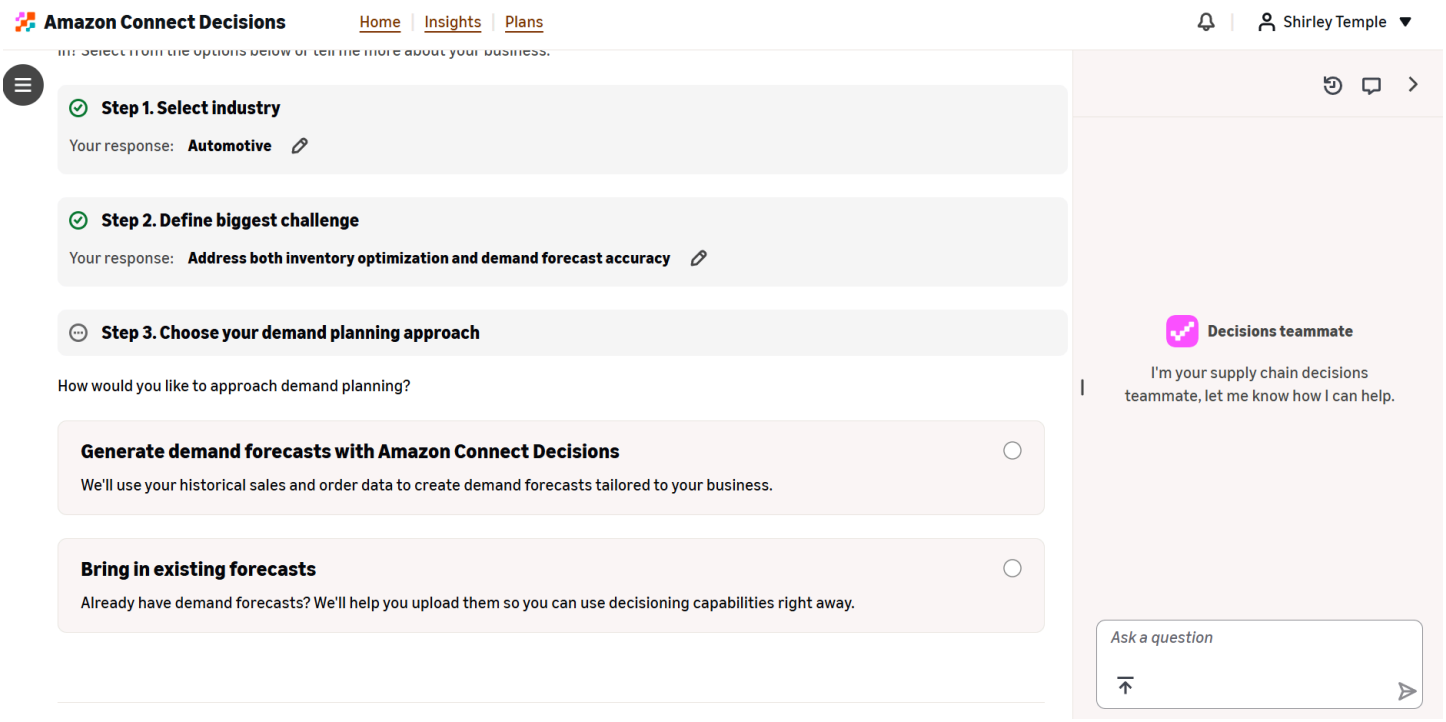
Lo que ves: los pasos 1 y 2 se muestran como completados (se indican con marcas de verificación verdes) y tus respuestas se muestran y se pueden editar. En el paso 3, se pregunta cómo te gustaría enfocar la planificación del inventario, con dos opciones destacadas.

1. Revisa las dos opciones de planificación del inventario. Consulte la siguiente tabla para ver las opciones disponibles y su significado.
2. Seleccione el botón de radio correspondiente al enfoque que se ajuste a su estado actual.

Opciones de enfoque de planificación de inventario

Opción	Description (Descripción)	Recomendada para
Genere planes de inventario con Amazon Connect Decisions	El sistema utiliza sus datos históricos de ventas e inventario para crear planes a la medida de su empresa.	Organizaciones que no tienen una solución de planificación existente o que desean aprovechar los planes generados por IA a partir de sus datos históricos.

Opción	Description (Descripción)	Recomendada para
Incorpore las proyecciones o planes de inventario existentes	Cargue sus planes o proyecciones de inventario actuales para poder utilizar las capacidades de toma de decisiones de forma inmediata. El sistema le ayudará a cargar y mapear sus datos.	Organizaciones que ya tienen procesos de planificación establecidos y desean aprovechar las capacidades de supervisión, generación de información y recomendación sin cambiar la fuente de sus planes.



Paso 4: Elija su enfoque de planificación de la demanda

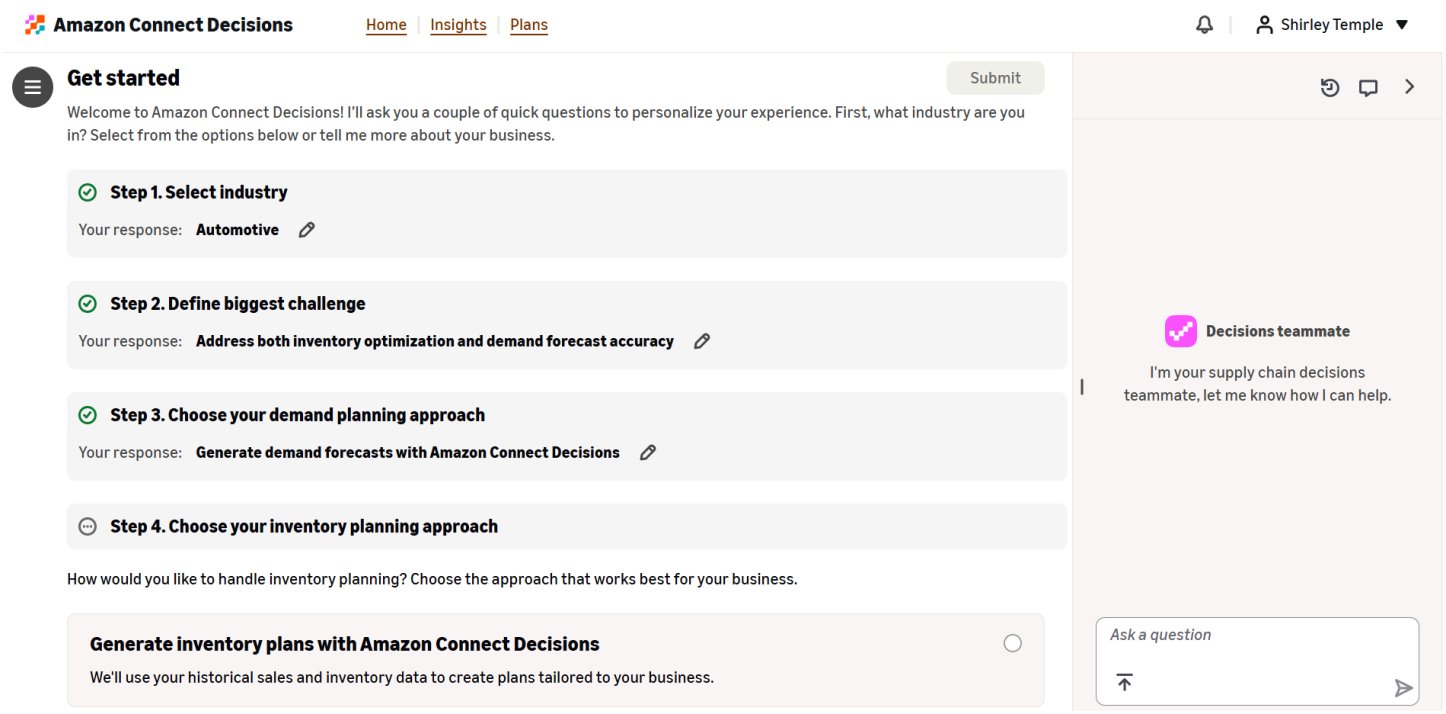
Lo que ve: los pasos 1 a 3 aparecen como completados. En el paso 4 se pregunta cómo le gustaría abordar la planificación de la demanda.

1. Revise las dos opciones de planificación de la demanda. Consulte la siguiente tabla para ver las opciones disponibles y su significado.
2. Seleccione el botón de radio del enfoque que mejor se adapte a su estado actual.
3. Haga clic en Enviar para finalizar el cuestionario de incorporación.

Recuerde: este cuestionario de incorporación es una entrada contextual única que ayuda a optimizar los pasos de incorporación en función de sus selecciones. No altera el comportamiento de los agentes ni restringe el acceso a ninguna funcionalidad. Todas las funciones de Amazon Connect Decisions siguen estando totalmente disponibles para usted.

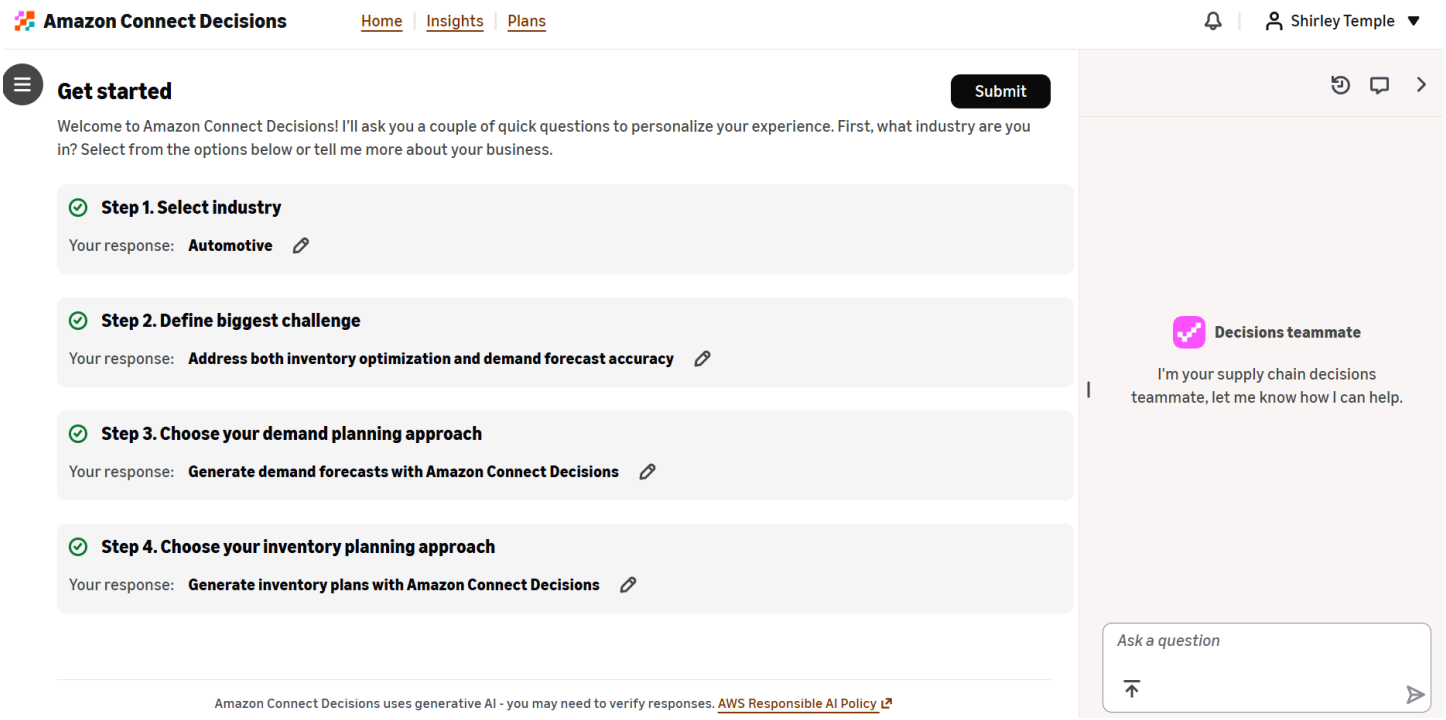
Opciones de enfoque de planificación de la demanda

Opción	Description (Descripción)	Recomendada para
Genere previsiones de demanda con Amazon Connect Decisions	El sistema utiliza sus datos históricos de ventas y pedidos para crear previsiones de demanda adaptadas a su negocio. Amazon Connect Decisions organiza más de 18 herramientas de previsión para producir previsiones de referencia precisas.	Organizaciones que no disponen de una solución de previsión existente o que desean sustituir su enfoque actual por previsiones generadas por IA.
Incorpore las previsiones existentes	Cargue sus previsiones de demanda actuales para poder utilizar las capacidades de toma de decisiones de forma inmediata. El sistema le ayudará a mapear e importar los datos de sus pronósticos.	Organizaciones que ya han establecido procesos de previsión y desean aprovecha r las capacidades de supervisi ón, generación de información y recomendación sin cambiar su fuente de previsión.



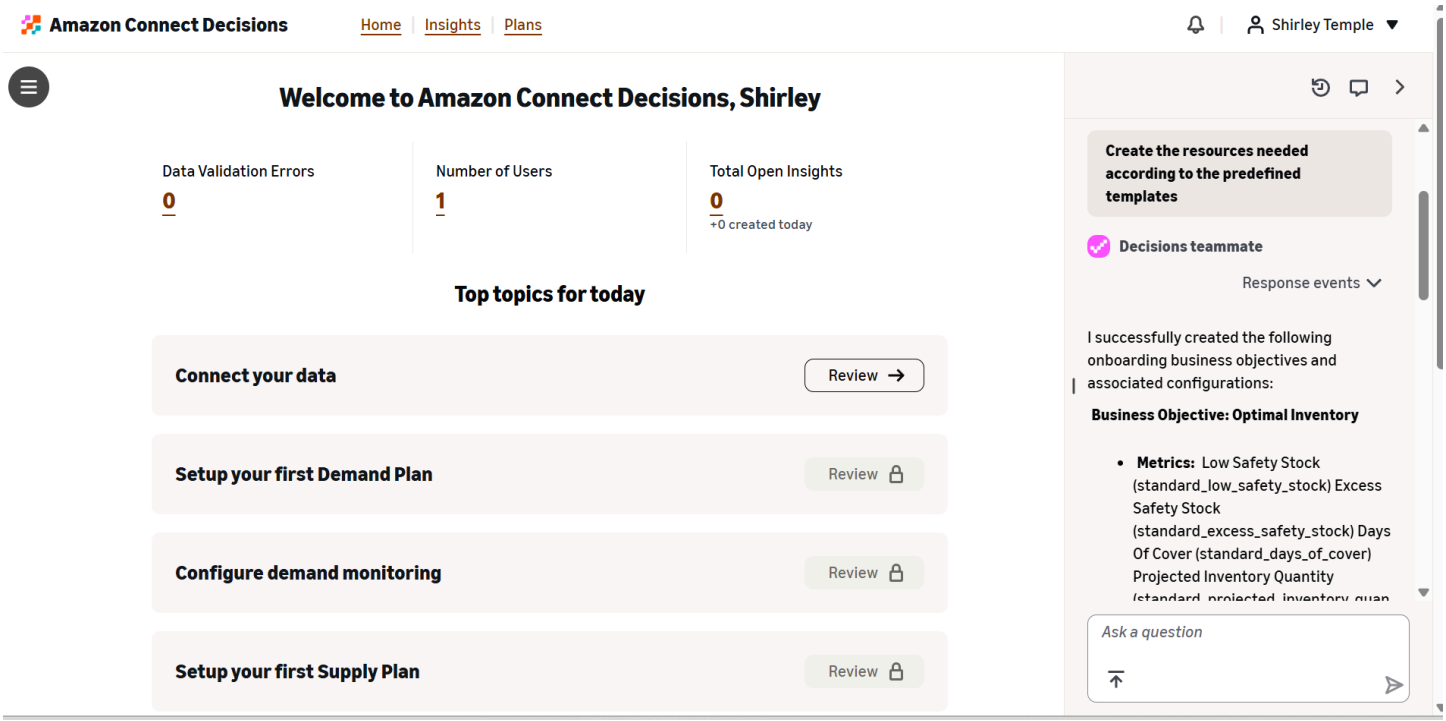
Después de completar el cuestionario

Haga clic en Enviar después de completar los cuatro pasos:



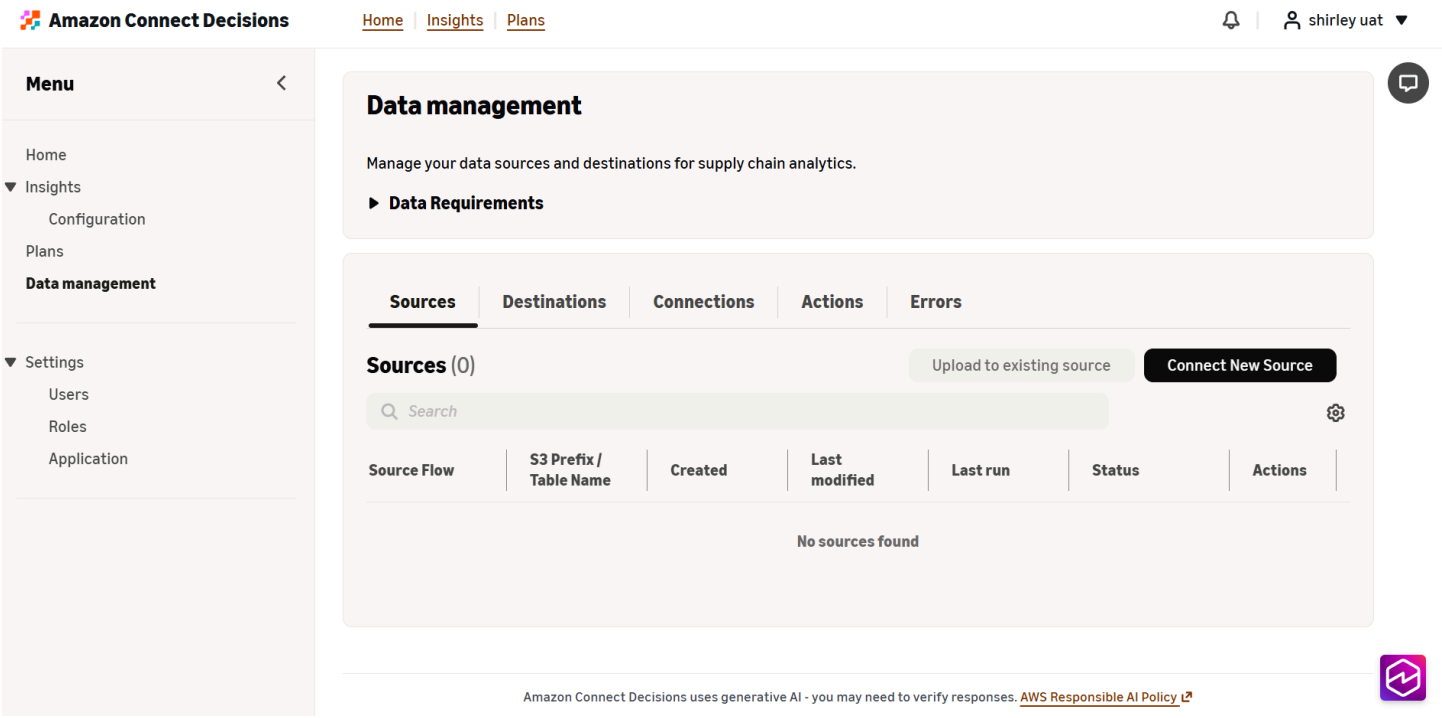
- Se te redirigirá a la página de inicio con un panel de control y tarjetas temáticas diseñadas para guiarte en el resto de los pasos de incorporación.

- El sistema creará automáticamente métricas y reglas dentro de la aplicación en función de sus selecciones. Se crean en estado Borrador y no se activan de forma inmediata.
- Puedes revisar las métricas y reglas creadas automáticamente y, a continuación, activarlas si se ajustan a tus necesidades, o crear tus propias métricas y reglas adaptadas a tus requisitos empresariales específicos.



Cómo crear su primer flujo fuente

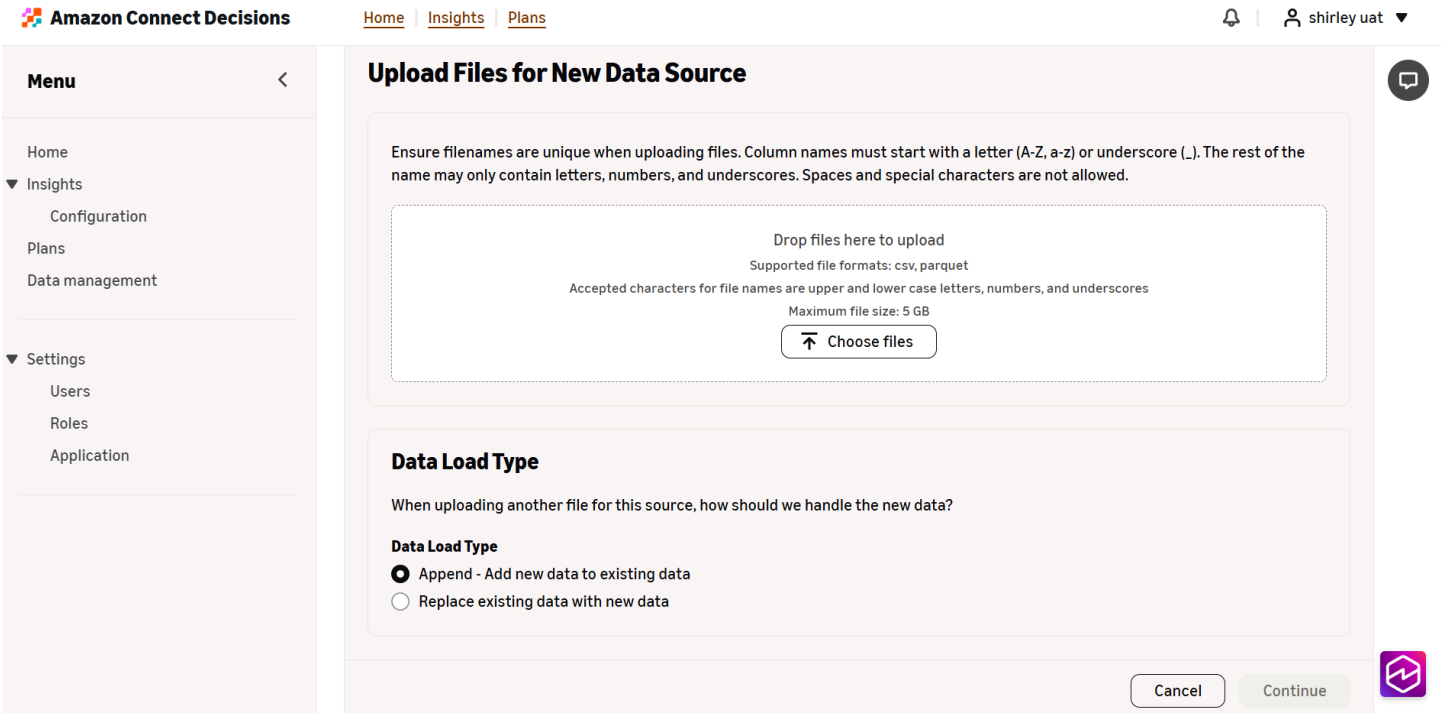
Para empezar a incorporar sus datos, haga clic en Revisar la tarjeta temática Connect your data o vaya a la pestaña Administración de datos en el «Menú Hamburger» de Amazon Connect Decisions. Aquí puede ver todos sus flujos de origen existentes. Si aún no ha configurado uno, haga clic en «Connect New Source» para empezar.



Cargue sus datos de origen

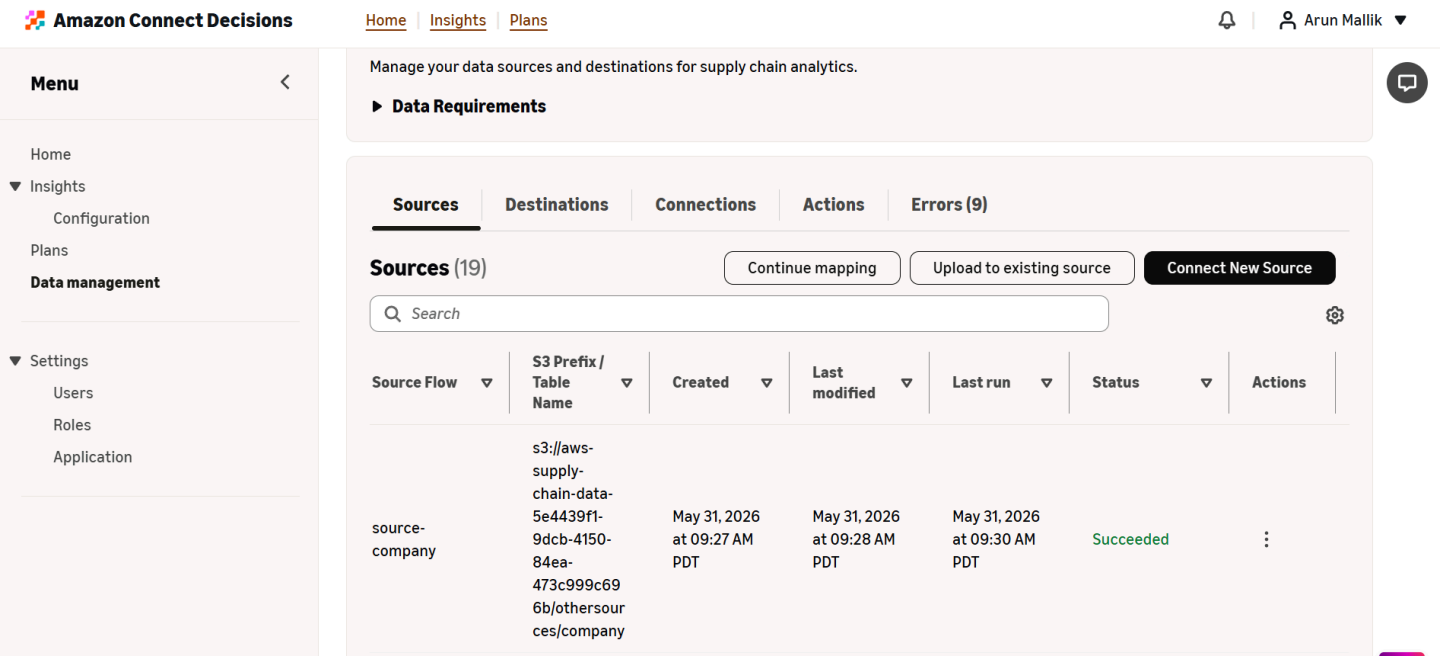
Cargue sus archivos CSV que contengan datos de origen basados en las tablas del CDM requeridas para su caso de uso. Puedes elegir cómo quieres gestionar las actualizaciones de datos:

- Anexar: agrega nuevos datos a los datos existentes
- Reemplazar: reemplaza los datos existentes por datos nuevos



Al cargar archivos, Amazon Connect Decisions crea automáticamente una estructura de carpetas en S3 para esos datos, que incluye:

- Una carpeta principal que lleva el nombre del sistema de origen seleccionado
- Una subcarpeta que lleva el nombre de la tabla de origen seleccionada
- Todos los archivos de una subcarpeta se guardan en la misma tabla de origen
- Esta estructura de archivos también se utiliza para crear la ruta de la carpeta Amazon S3

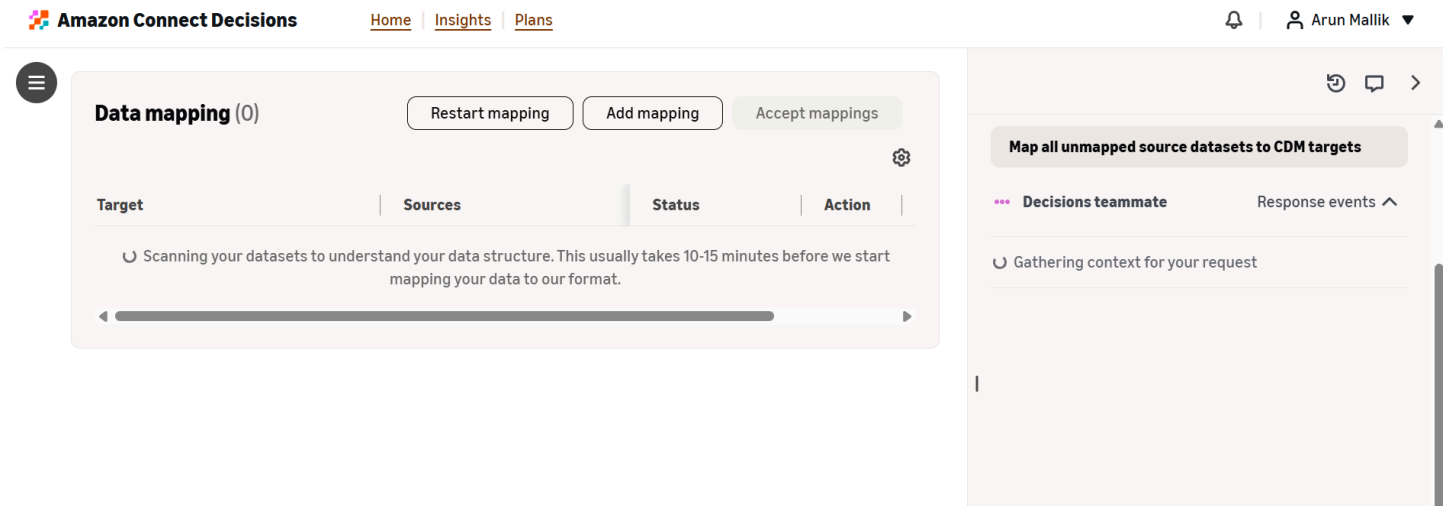


Source-to-CDM Mapeo de destinos

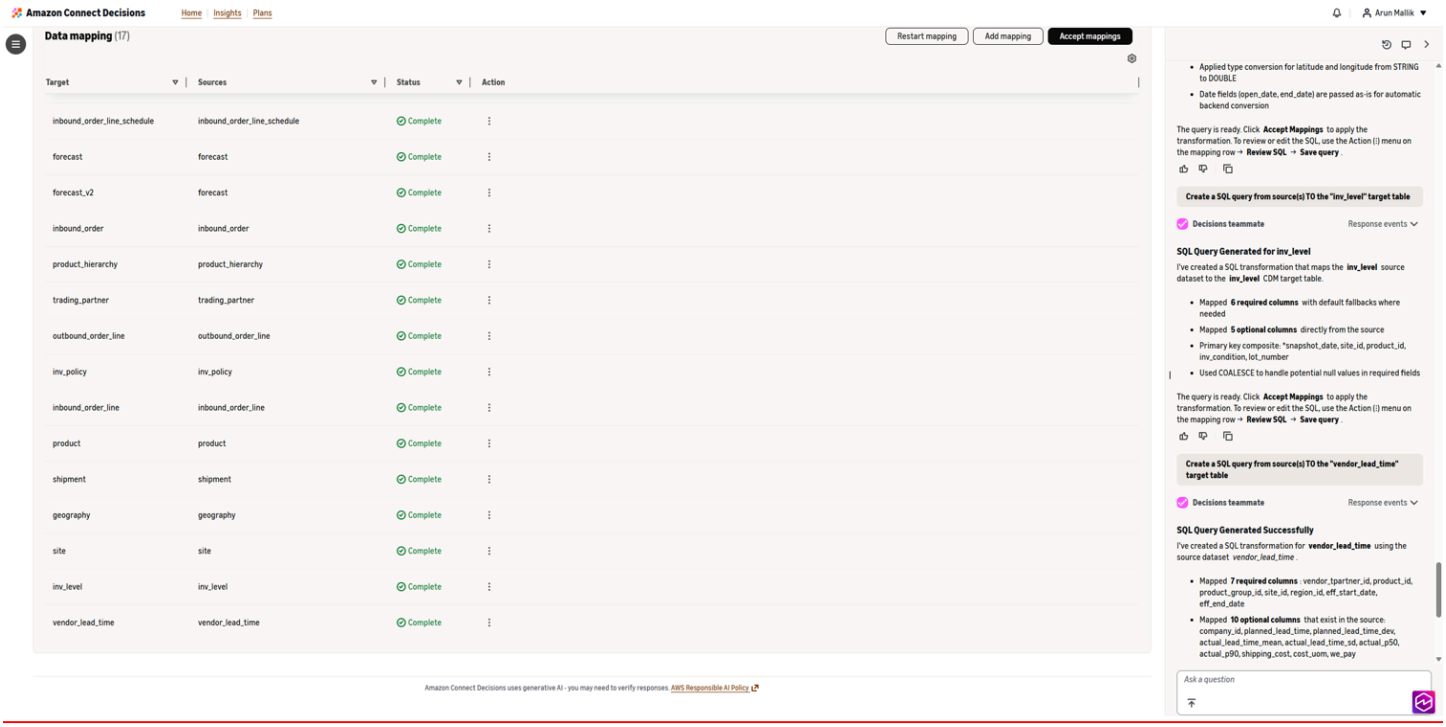
Una vez cargados los archivos, Amazon Connect Decisions comienza a analizar los datos y los asigna automáticamente a una o varias de las tablas de destino de CDM de Amazon Connect Decisions.

¿Qué esperar

- Este paso puede tardar entre 10 y 15 minutos, dependiendo de la cantidad de datos cargados
- El agente de datos trabaja en segundo plano para identificar los mejores conjuntos de datos de destino del CDM para sus datos de origen.
- Si se sale de esta página, se producirá un error en las asignaciones automatizadas. Mientras espera, mantenga abierta la pestaña Amazon Connect Decisions and Data Management para garantizar que se complete el mapeo automatizado.

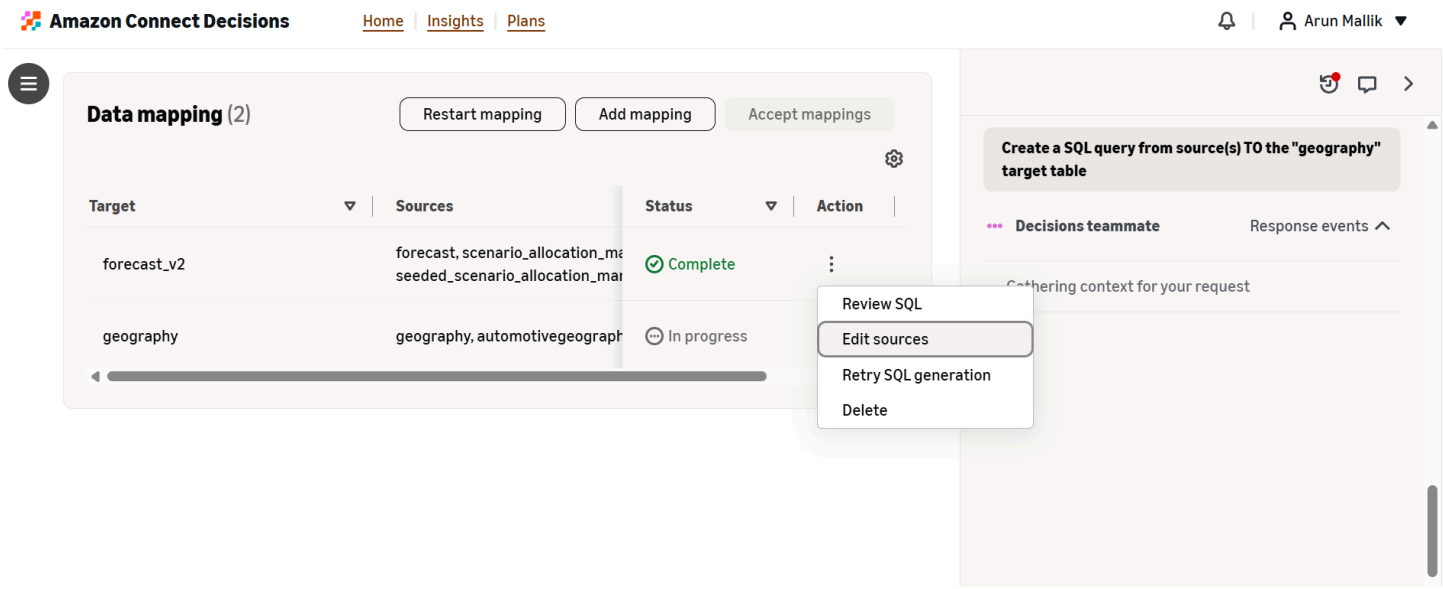


Una vez finalizada, el agente de datos explica los mapeos entre el origen y el destino basándose en la superposición de datos, que usted puede revisar y formular preguntas al agente sobre los resultados del mapeo.



Para revisar y editar las asignaciones de origen, puede:

- Interactúe directamente con el agente de datos mediante un lenguaje natural para actualizar las asignaciones de origen y destino.
- Haga clic en las Acciones y seleccione «Editar fuentes».



Edición de mapeos

Desde aquí, puede:

- Actualice el mapeo de origen y destino manualmente si es necesario
- Haga preguntas utilizando el agente de datos situado en la parte derecha de la pantalla para confirmar los mapeos
- Consulte las guías de usuario para obtener más información sobre conjuntos de datos específicos

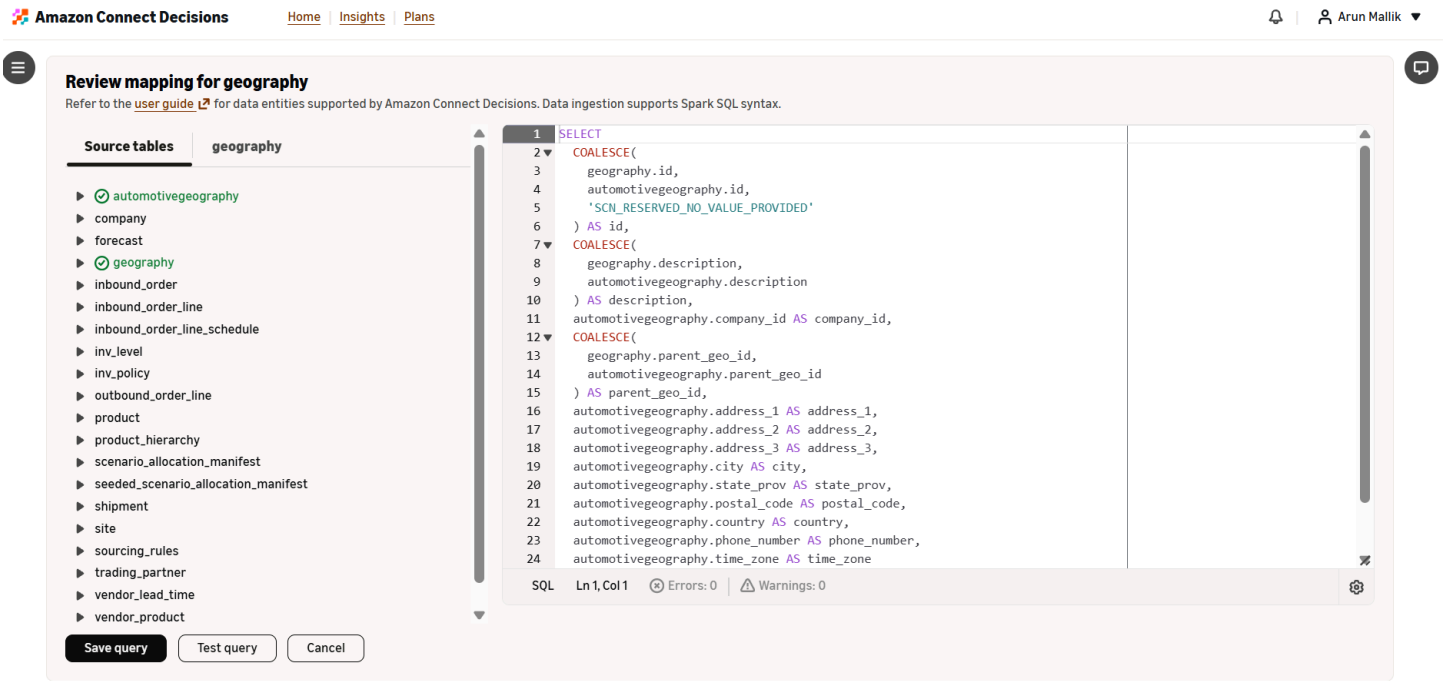
Column/Data Cartografía

Una vez finalizado el mapeo de origen a destino, Amazon Connect Decisions creará automáticamente consultas de transformación SQL desde el conjunto de datos de origen al destino de CDM. Una vez que se complete alguna de sus asignaciones, recibirá una notificación del agente de datos en la que se detallará el resultado de la asignación.

Desde aquí, debe revisar el SQL generado para las asignaciones; para ello, seleccione «Revisar SQL» en el menú de acciones.

Al revisar el mapeo (SQL), verá:

- Columnas del conjunto de datos de origen que ha agregado
- Columnas de la tabla del CDM de destino como referencia
- La transformación SQL que las conecta
- Justificación del mapeo proporcionada por el agente de datos



Edición de mapeos

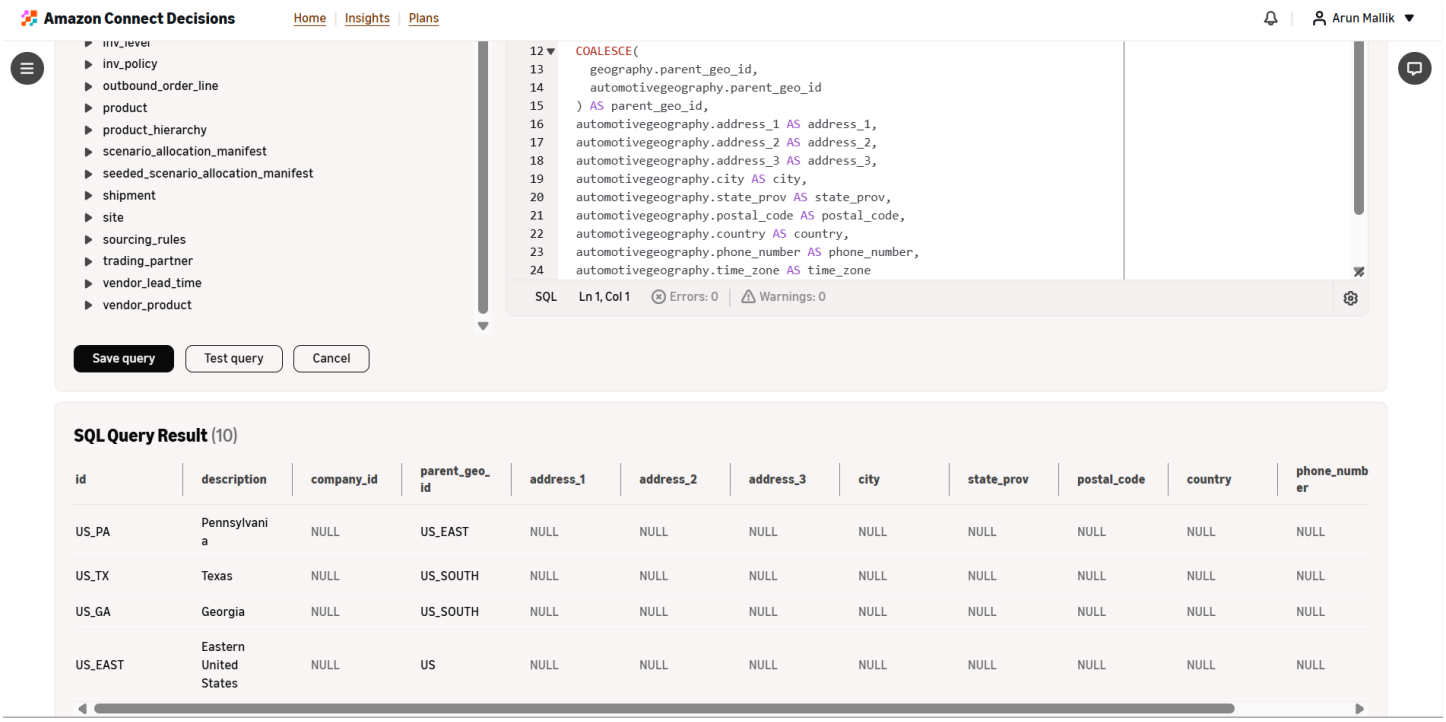
Dispone de dos opciones para editar cualquier mapeo:

- Trabaje con Data Agent: utilice un lenguaje natural para hacer preguntas, administrar y actualizar las asignaciones
- Edite SQL directamente: si está familiarizado con SQL, puede modificar la consulta directamente

Probando sus cambios

A medida que edite la consulta de mapeo, continúe probándola con la función «Probar consulta», que le proporcionará una vista previa desplazable de cómo se están transformando sus datos en el CDM de destino. Utilícela para asegurarse de que la transformación se ejecute correctamente y para validar cualquier actualización adecuada desde el CDM de origen a destino.

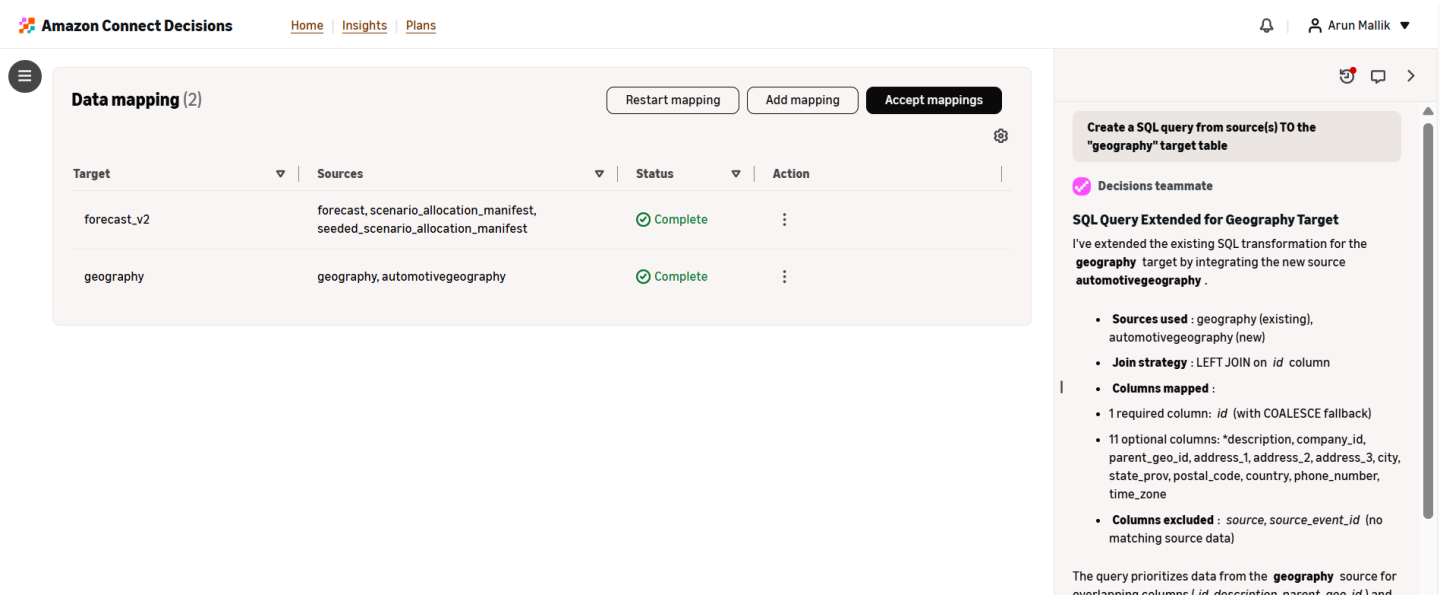
Cuando esté satisfecho con el resultado del mapeo, seleccione «Guardar consulta» para guardar la consulta de transformación para ese par origen-destino.



Revise y acepte los mapeos

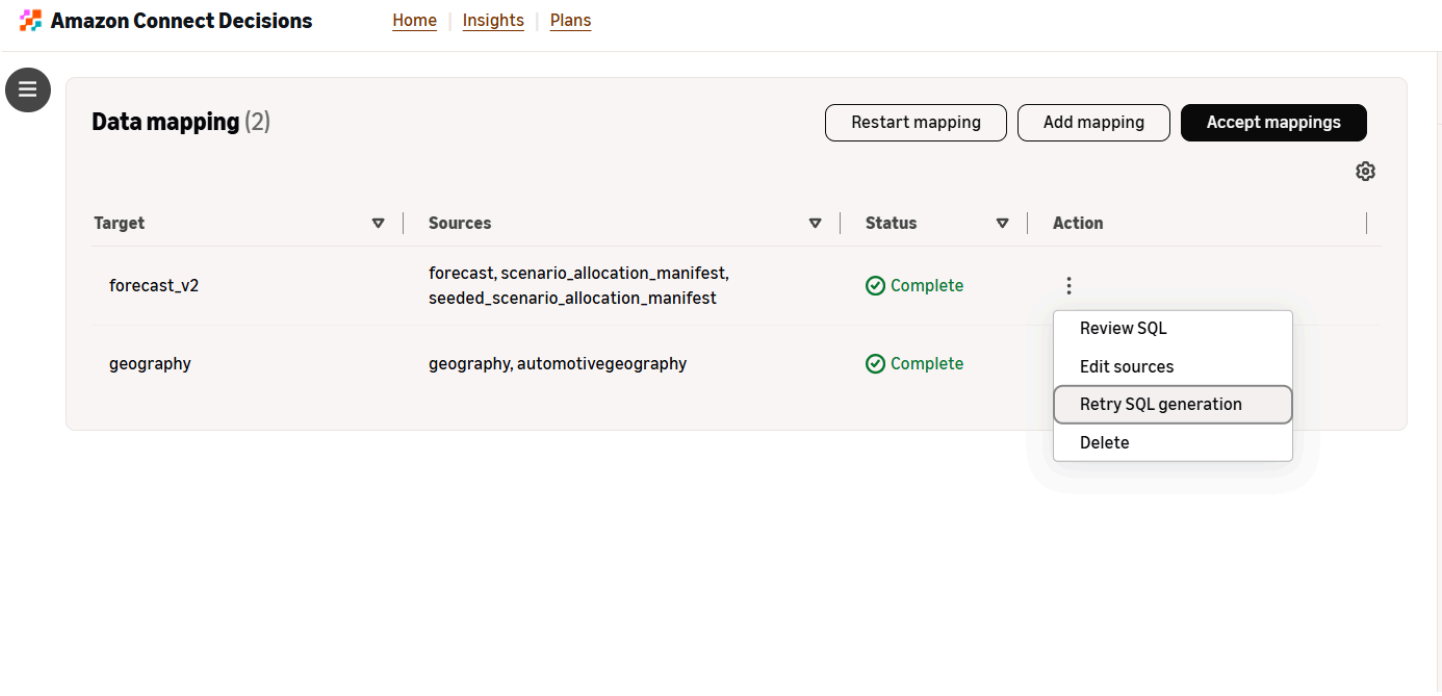
Revise las asignaciones restantes de cada uno de sus conjuntos de datos de origen. El agente de datos permanece en el lado derecho de la pantalla para resolver dudas o ayudar a solucionar problemas.

Cuando esté satisfecho con todos los mapeos, acéptelos para completar la incorporación de datos haciendo clic en Aceptar mapeos.



Gestione los mapeos fallidos

Si alguna asignación ha fallado, puede seleccionar «Reiniciar la asignación» para reiniciar todas las asignaciones o volver a intentar manualmente una sola asignación desde el menú Acciones mediante la opción «Reintentar generar SQL». El agente de datos también puede volver a intentar los mapeos utilizando un lenguaje natural y seguirá ayudándole a identificar y resolver los problemas si los errores persisten.

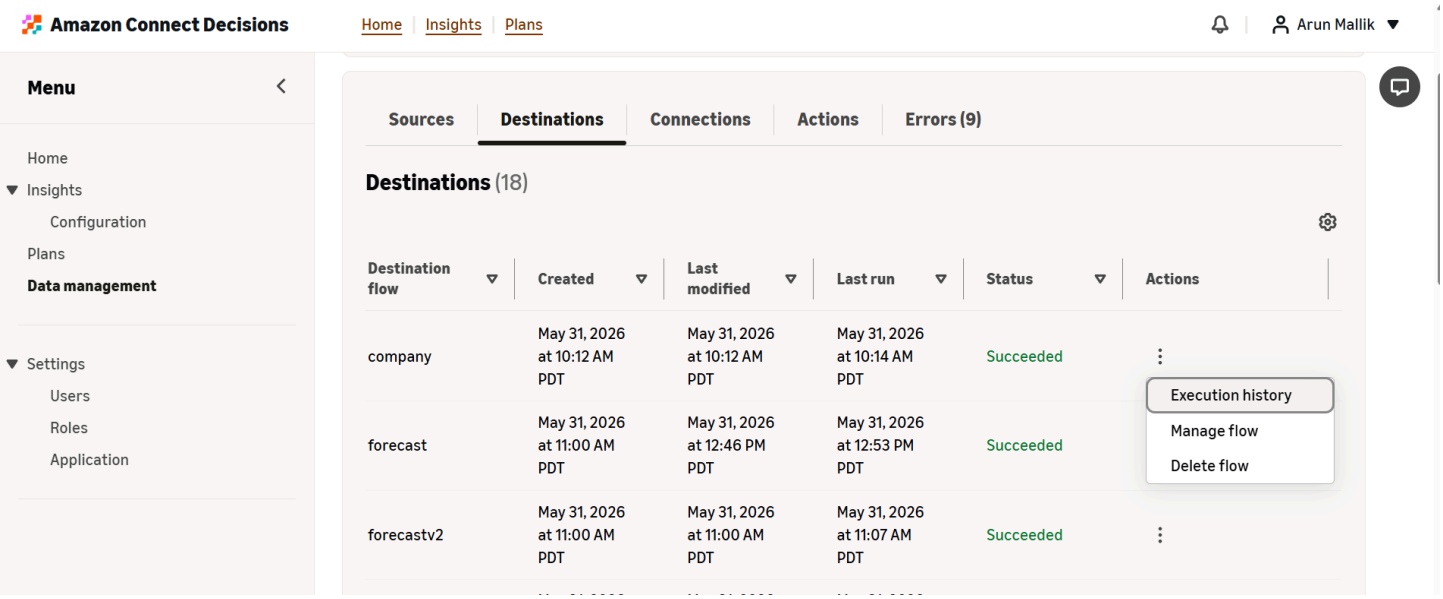


Supervise sus flujos

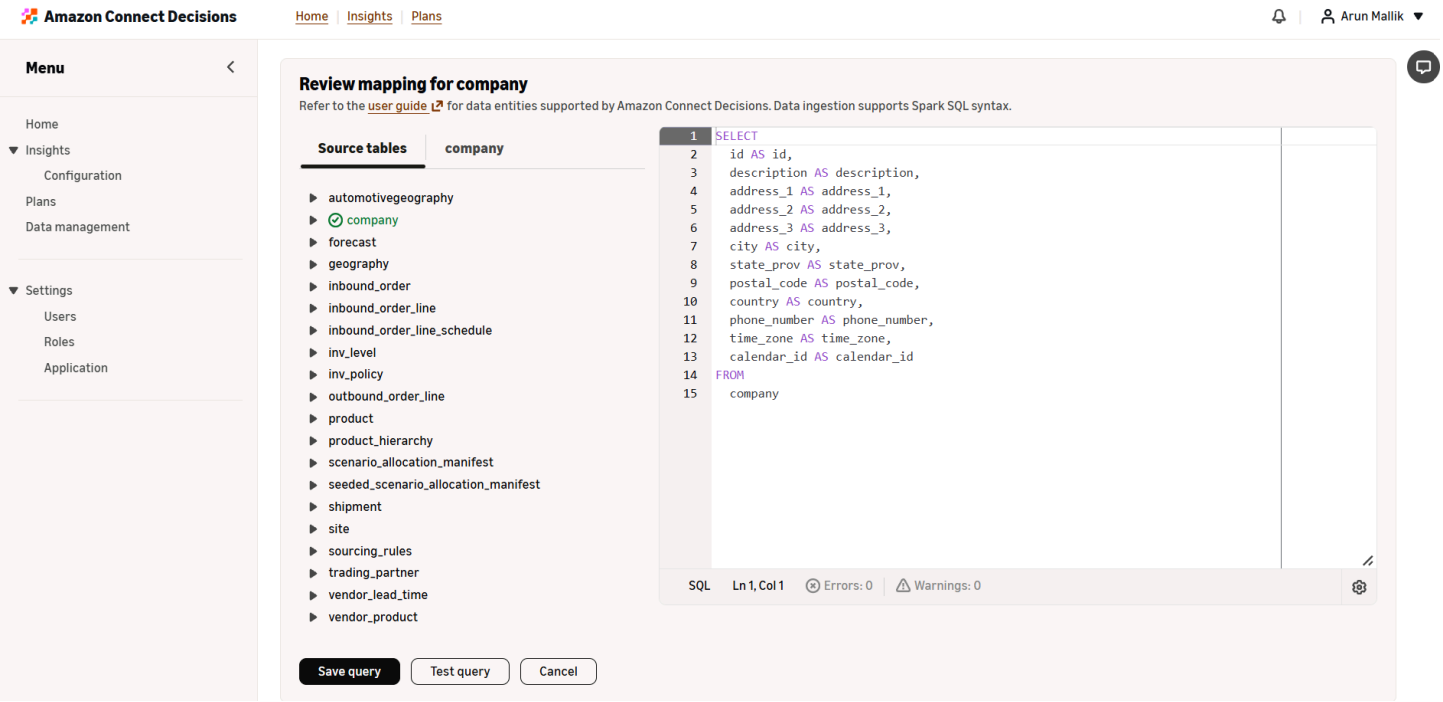
Pestaña de destinos

Al aceptar los mapeos, accederás a la pestaña Destinos de la administración de datos, donde podrás:

- Revise los flujos de destino
- Administre y edite los mapeos («Administrar el flujo»)
- Eliminar flujos obsoletos
- Revise el estado de ejecución de estos flujos



Si selecciona «Administrar flujo», volverá a la experiencia de mapeo de datos, donde podrá seguir trabajando con el agente de datos para refinar los mapeos a lo largo del tiempo.



Pestaña Fuentes

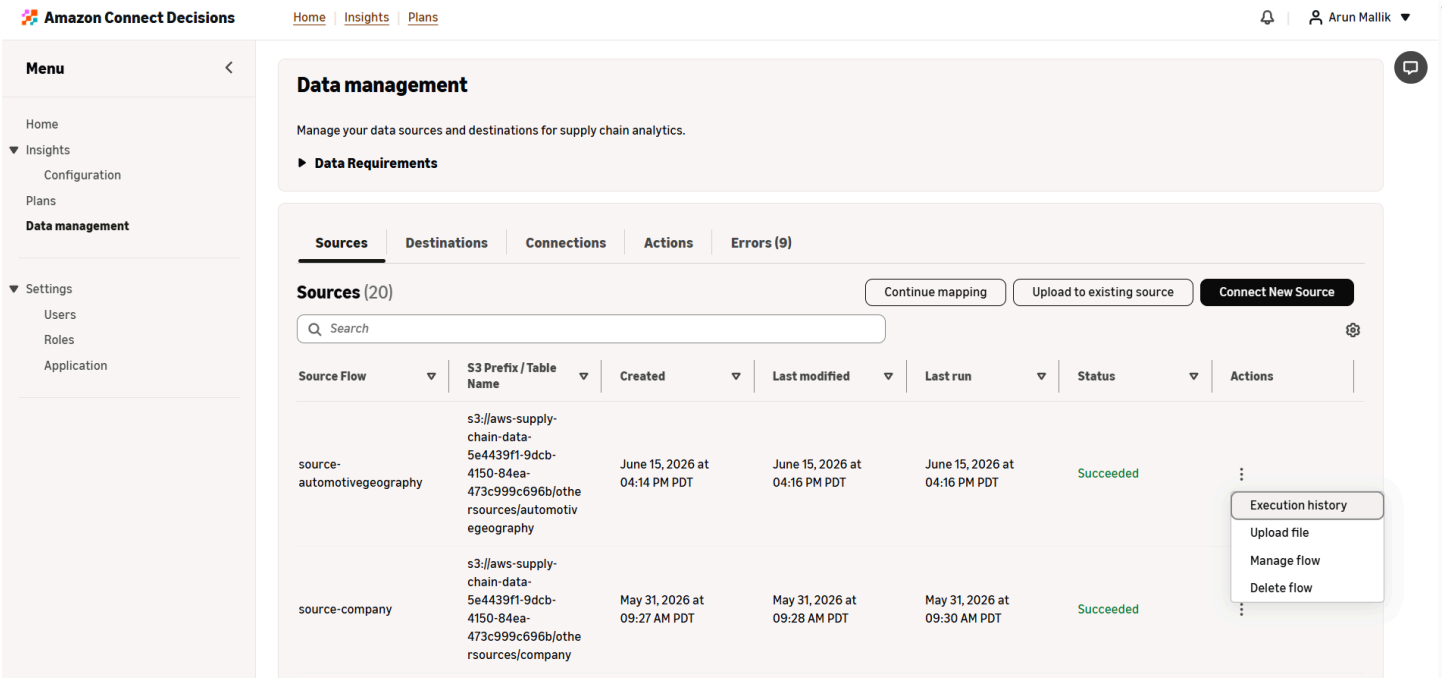
Volviendo a la pestaña Fuentes, encontrarás:

- El conjunto de datos de origen que se ha creado
- Es un bucket de S3 asociado

- Opciones para:
  - Añadir más datos de origen mediante la carga de otro archivo
  - Gestione el flujo
  - Elimine el flujo
  - Revise las ejecuciones

Si selecciona «Administrar flujo», volverá a la experiencia de mapeo de datos, donde podrá seguir trabajando con el agente de datos para refinar los mapeos a lo largo del tiempo.

También tiene acceso a Crear una nueva fuente según sea necesario para reiniciar el proceso de incorporación de datos para cualquier fuente de datos nueva.



Prácticas recomendadas

Preparación de datos

- Siga los pasos de la sección Requisitos previos
- Utilice la UTF-8 codificación para todos los archivos CSV
- Asegúrese de que los nombres de los archivos sean únicos
- Valide la calidad de los datos antes de cargarlos

Trabajando con Data Agent

- Sea específico en sus solicitudes
- Pida explicaciones cuando no comprenda alguna de sus decisiones
- Pruebe todos los cambios de SQL antes de aceptarlos
- Utilice la función de vista previa para verificar las transformaciones

Mantenimiento continuo

- Mantenga sus datos de origen actualizados
- Supervise la ejecución del flujo con regularidad
- Aborde los errores de datos con prontitud cuando se
- Documenta las transformaciones personalizadas para tu equipo

Conexión a su base de datos con JDBC

Esta guía explica cómo conectar la base de datos a Amazon Connect Decisions mediante Java Database Connectivity (JDBC). Configurará un cifrado seguro para las credenciales de su base de datos y establecerá una conexión que Amazon Connect Decisions pueda utilizar para acceder a sus datos.

¿Qué es la conexión JDBC y cuándo debe utilizarla?

La conexión JDBC permite a Amazon Connect Decisions conectarse a su base de datos existente para leer los datos, en lugar de tener que exportar y cargar archivos CSV o configurar sus propias canalizaciones de extracción, transformación y carga (ETL) a S3. Este enfoque es ideal cuando:

- Sus datos ya están almacenados en una base de datos Glue-compatible relacional de AWS. Consulte esta guía para obtener información sobre las bases de datos y las versiones compatibles.
- Desea acceder a los datos en tiempo real o casi en tiempo real sin necesidad de exportar archivos manualmente
- Su volumen de datos es grande y se actualiza con frecuencia
- Prefiere mantener los datos en su ubicación actual en lugar de duplicarlos

- Si trabaja con conjuntos de datos más pequeños o prefiere las cargas basadas en archivos, el proceso de carga de CSV estándar puede ser más sencillo para sus necesidades. Consulta la Guía del usuario de incorporación de datos para obtener más información sobre este proceso.

Requisitos previos

Antes de comenzar, asegúrese de que dispone de lo siguiente:

- Una cuenta de AWS con permisos para crear claves de KMS y recursos de Secrets Manager
- Su ID de cuenta de AWS y la región en la que operará Amazon Connect Decisions
- Detalles de la conexión a la base de datos: nombre de host, puerto, nombre de la base de datos y credenciales
- Acceso administrativo a su base de datos para verificar la conectividad
- Su base de datos configurada para aceptar conexiones desde los servicios de AWS

Cree una clave Customer-Managed KMS

Antes de conectar la base de datos a Amazon Connect Decisions, tendrá que configurar el cifrado de las credenciales de la base de datos. AWS Key Management Service (KMS) proporciona esta capa de seguridad para garantizar que los detalles de su conexión permanezcan protegidos.

Cree su clave KMS

1. Navegue a la consola AWS KMS
   - Abra la consola de administración de AWS en su navegador
   - En la barra de búsqueda de la parte superior, escriba «KMS» y seleccione «Servicio de administración de claves» en los resultados
   - Se abrirá el panel de KMS, donde administrará las claves de cifrado
2. Inicie la creación de la clave
   - En el panel de KMS, localice y haga clic en el botón Crear clave en la esquina superior derecha
   - Esto inicia el asistente de creación de claves que lo guiará a través del proceso de configuración
3. Configure el tipo y el uso de la clave
   - En la página «Configurar clave», selecciona Simétrico como tipo de clave (esta es la opción predeterminada y recomendada)

- Mantenga seleccionada la opción «Cifrar y descifrar» en la sección Uso de claves

4. Establezca los detalles de identificación de la clave
   - En el campo «Alias», introduce un nombre descriptivo para la clave, como `aws-supply-chain-database-key`
   - En el campo «Descripción», añada un contexto como «Clave de cifrado para las credenciales de la base de datos de Amazon Connect Decisions»
   - Si lo desea, añada etiquetas para ayudar a organizar y realizar un seguimiento de sus recursos de AWS (p. ej., clave: «Proyecto», valor: «Amazon Connect Decisions»)
5. Defina los permisos administrativos clave
   - Seleccione los usuarios o roles de IAM que deberían poder administrar esta clave (crear, eliminar o modificar políticas)
   - Como mínimo, incluye tu propia función de administrador para asegurarte de que puedes modificar la clave más adelante si es necesario
   - Estos administradores pueden administrar la clave, pero no tendrán automáticamente permiso para usarla encryption/decryption
   - En la sección «Eliminación de claves», permite a los administradores de claves eliminar esta clave. (esta es la opción predeterminada y recomendada)
6. Defina los permisos de uso clave
   - En esta página, verás opciones para seleccionar los usuarios y roles de IAM que pueden usar la clave
   - Omita la selección de usuarios específicos aquí; configurará los permisos de servicio en el siguiente paso
7. Configurar la política clave para los servicios de Amazon Connect Decisions
   - Verá un editor de políticas con el JSON predeterminado
   - En el editor de políticas clave de KMS, añada la siguiente declaración a su matriz de «Declaración» existente
   - Esta política otorga a su cuenta el control total y permite a los servicios de Amazon Connect Decisions (Secrets Manager y Glue) descifrar las credenciales de su base de datos

```
{
  "Sid": "Allow GDIS service to decrypt",
  "Effect": "Allow",
  "Principal": {
    "Service": "scn.amazonaws.com"
```

```
  },
  "Action": [
    "kms:Decrypt",
    "kms:DescribeKey",
    "kms:CreateGrant",
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource": "*"
}
```

8. Revise y finalice
   - Revise todos los ajustes de configuración en la página de resumen
   - Compruebe que el alias, la descripción y la política son correctos
   - Haga clic en Finalizar para crear la clave
   - Una vez creada, volverá al panel de KMS, donde la nueva clave aparecerá en la lista

¿Qué esperar

La creación de claves es inmediata. Una vez creada, la nueva clave aparecerá en la consola de KMS con el estado «Habilitada». La clave ya está lista para cifrar las credenciales de la base de datos en Secrets Manager.

Configuración de AWS Secrets Manager

Ahora que tiene una clave de KMS, creará un secreto en AWS Secrets Manager para almacenar de forma segura las credenciales de su base de datos y, a continuación, configurará una política de recursos que permita a Amazon Connect Decisions acceder a este secreto.

Cree su secreto

1. Navegue hasta AWS Secrets Manager
   - En la barra de búsqueda de AWS Management Console, escriba «Secrets Manager»
   - Seleccione «Secrets Manager» en los resultados para abrir el panel de servicio
2. Empieza a crear un secreto nuevo
   - Haz clic en el botón Guardar un secreto nuevo
   - En la página «Elegir el tipo de secreto», selecciona Otro tipo de secreto (esto te da flexibilidad a la hora de estructurar tus credenciales)
3. Introduzca las credenciales de su base de datos

- En la sección de pares clave-valor, añada los detalles de la conexión a la base de datos en forma de cadenas:

```
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. Seleccione su clave de cifrado
   - En «Clave de cifrado», selecciona Elegir una clave de AWS KMS
   - En el menú desplegable, seleccione la clave de KMS que creó en el paso 1 (por ejemplo,`aws-supply-chain-database-key`)
   - Esto garantiza que sus credenciales estén cifradas con su clave administrada por el cliente
5. Dime tu secreto
   - Introduce un nombre descriptivo para tu secreto, como `aws-supply-chain-production-database`
   - Si lo desea, añada una descripción como «Credenciales de base de datos para el entorno de producción de Amazon Connect Decisions»
   - Agregue etiquetas si lo desea para la organización (por ejemplo, clave: «Medio ambiente», valor: «Producción»)
6. Agregue permisos de recursos
   - Haga clic en «Editar permisos». En el editor de políticas, pegue la siguiente política. Esta política permite a los servicios de Amazon Connect Decisions leer tu secreto

```
{
  "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. Guarde la política

- Haga clic en Guardar para aplicar la política de recursos
- La política ya está activa y permite a Amazon Connect Decisions recuperar las credenciales de su base de datos.

8. Configure la rotación (opcional)
   - Para esta configuración, puede omitir la rotación automática seleccionando Desactivar la rotación automática
   - Puede habilitar la rotación más adelante si sus políticas de seguridad lo requieren
9. Revisar y crear
   - Revisa todos tus detalles secretos
   - Haz clic en Guardar para crear el secreto
   - Volverás al panel de control de Secrets Manager.
10. Guarda tu ARN secreto
    - Encuentra tu secreto recién creado en la lista de secretos
    - Haz clic en el nombre secreto para abrir su página de detalles
    - En la parte superior, verás el ARN secreto
    - Copia y guarda este ARN
    - El formato ARN tiene el siguiente aspecto: `arn:aws:secretsmanager:us-east-1:123456789012:secret:aws-supply-chain-production-database-AbCdEf`
11. Editar permisos de recursos
    - Haga clic en «Editar permisos»
    - Pegue el ARN secreto copiado y sustitúyalo por el `<COPY-THE-SECRET-ARN-HERE-AFTER-CREATING>` ARN copiado
    - Haga clic en Guardar para adjuntar la política

¿Qué esperar

Su secreto ahora está almacenado y cifrado de forma segura con su clave KMS. Los servicios de Amazon Connect Decisions tienen permiso para recuperar las credenciales al establecer una conexión a la base de datos, pero las credenciales permanecen cifradas en reposo y en tránsito.

Conecte su base de datos a Amazon Connect Decisions

Con la clave y el secreto de KMS configurados, está listo para establecer la conexión JDBC en Amazon Connect Decisions.

Configure su conexión JDBC

1. Vaya a Amazon Connect > Decisiones > Administración de datos
   - Inicie sesión en su instancia de Amazon Connect Decisions
   - En la barra de navegación principal, selecciona «Gestión de datos»
   - En la barra de navegación por pestañas, dirígete a «Conexiones»
   - Seleccione «Nueva conexión» para crear una nueva conexión
2. Introduce los detalles de tu conexión
   - Nombre de conexión (obligatorio): introduce un identificador único para esta conexión (p. ej., «base de datos de producción»)
   - Descripción (opcional): añade detalles sobre el propósito y el uso de esta conexión para ayudar a tu equipo a entender a qué datos accede
   - URL de JDBC (obligatorio): introduce la cadena de conexión JDBC completa en el formato: (por ejemplo,) `jdbc:<database-type>://<hostname>:<port>/<database>` `jdbc:postgresql://db.example.com:5432/mydb`
   - Nombre del esquema (opcional): especifique el esquema de la base de datos si es necesario (por ejemplo, «public», «dbo», «myschema»). Déjelo en blanco para usar el esquema predeterminado de la base de datos
   - ARN secreto (obligatorio): pega el ARN secreto que guardaste en el paso 2. Esto permite a Amazon Connect Decisions recuperar de forma segura las credenciales de su base de datos de Secrets Manager.
   - Exija la conexión SSL: mantenga esta casilla de verificación seleccionada (se recomienda) para requerir el SSL/TLS cifrado de la conexión a la base de datos
   - Nombre del servicio de punto final de VPC (obligatorio): introduzca el nombre de su servicio de punto final de VPC para la conectividad privada a través de AWS PrivateLink (formato:) `com.amazonaws.vpce.<region>.vpce-svc-xxxxxxxxx`
3. Conéctese a su base de datos
   - Haga clic en «Conectar» para probar y establecer la conexión. Amazon Connect Decisions verificará que se puede conectar correctamente a su base de datos con las credenciales

proporcionadas. Este paso puede tardar hasta 2 minutos, así que no abandone esta pantalla durante la conexión.

- Si la conexión se realiza correctamente, accederás automáticamente a la tabla seleccionada
- Si se produce un error en la conexión:
  - Revisa los detalles de tu conexión para asegurarte de que todos los campos son correctos:
    - Comprueba que tu ARN secreto es correcto
    - Confirma que las credenciales de tu base de datos son correctas
    - Compruebe que el formato de la URL de JDBC es correcto
    - Asegúrese de que su base de datos esté configurada para aceptar conexiones de los servicios de AWS
    - Compruebe que la clave de KMS y las políticas de Secrets Manager estén configuradas correctamente
  - También puedes usar la experiencia del chat para solucionar problemas de conexión haciendo preguntas como «¿Por qué falla la conexión de mi base de datos?» o «Ayúdame a depurar mi conexión JDBC»

4. Seleccione las tablas que desee ingerir
   - Una vez conectado, verá la pantalla de selección de tablas, donde se muestran todas las tablas disponibles en su base de datos
   - Selecciona la casilla de verificación situada junto a cada tabla que quieras ingerir
5. Configura el programa de actualización de la tabla
   - Para cada tabla seleccionada, haz clic en el menú de tres puntos de la columna Acción y selecciona «Programar actualización»
   - En el cuadro de diálogo Configurar los detalles de la carga, defina:
     - Cadencia: frecuencia de actualización (por hora, diaria, semanal o personalizada)
     - Hora de inicio: hora a la que comienza la actualización (se muestra en UTC con la diferencia de zona horaria)
     - Tipo de actualización: selecciona Actualización completa (reemplaza todos los datos) o Actualización incremental (agrega nuevos datos a los existentes; requiere seleccionar una columna de registro de fecha y hora)
     - Repita el procedimiento para cada tabla según sea necesario
   - Haga clic en Iniciar el mapeo cuando todas las tablas estén configuradas
6. Continúe con el mapeo de datos

- A partir de ahora, la experiencia es idéntica a nuestro flujo de incorporación de datos
- Siga la sección de mapeo de datos de la guía del usuario de incorporación de datos para completar la configuración

¿Qué esperar

Una vez establecida la conexión y seleccionadas las tablas, Amazon Connect Decisions podrá leer los datos de la base de datos. La conexión permanece activa y segura, con las credenciales cifradas y administradas a través de AWS Secrets Manager. No necesitarás actualizar manualmente las credenciales en Amazon Connect Decisions, ya que cualquier cambio que realices en Secrets Manager se reflejará automáticamente.

Prácticas recomendadas

Gestión de seguridad y acceso

- Almacene las credenciales de forma segura: utilice siempre AWS Secrets Manager para almacenar las credenciales de las bases de datos, nunca las codifique de forma rígida en las cadenas de conexión o los archivos de configuración
- Habilite el SSL/TLS cifrado: mantenga habilitada la opción «Exigir la conexión SSL» para garantizar que los datos estén cifrados en tránsito
- Revise las políticas de KMS y Secrets Manager con regularidad: asegúrese de que solo los servicios y cuentas autorizados tengan acceso a sus claves y secretos de cifrado
- Utilice el acceso con el mínimo privilegio: conceda solo los permisos mínimos necesarios a los usuarios de la base de datos que Amazon Connect Decisions utilizará para las conexiones

Configuración de conexión

- Utilice nombres de conexión descriptivos: elija nombres claros y significativos que indiquen el entorno y el propósito (por ejemplo, «production-inventory-db» en lugar de «db1")
- Documente sus conexiones: utilice el campo Descripción para anotar a qué datos accede la conexión, quién es su propietario y cualquier consideración especial
- Pruebe las conexiones antes de continuar: compruebe siempre que la conexión funciona antes de seleccionar tablas y configurar los programas de actualización

- Valide el formato de URL de JDBC: la sintaxis de la Double-check URL de JDBC coincide con el tipo de base de datos para evitar errores de conexión

Estrategia de actualización de datos

- Elija la cadencia de actualización adecuada: seleccione la frecuencia de actualización en función de la frecuencia con la que cambien los datos de origen y de las necesidades de su empresa
- Programe actualizaciones durante los períodos de baja actividad: configure los tiempos de actualización cuando la base de datos tenga menos carga para minimizar el impacto en el rendimiento
- Utilice actualizaciones incrementales siempre que sea posible: en el caso de conjuntos de datos grandes con cambios frecuentes, las actualizaciones incrementales son más eficaces que las actualizaciones completas
- Seleccione columnas con fecha y hora significativas: cuando utilice actualizaciones incrementales, elija columnas que reflejen con precisión cuándo se crearon o modificaron los registros

Trabajando con el chat para solucionar problemas

- Sea específico en sus solicitudes: proporcione un contexto claro cuando solicite ayuda para solucionar problemas de conexión o mapeo
- Pide explicaciones: si no entiendes las recomendaciones o las consultas SQL generadas, pide una aclaración
- Pruebe todos los cambios de SQL antes de aceptarlos: utilice la función de vista previa para comprobar que las transformaciones funcionan según lo esperado con sus datos reales
- Aproveche el chat para solucionar problemas: cuando las conexiones fallen o las actualizaciones detecten errores, formule preguntas de diagnóstico como «¿Por qué falla mi conexión?» o «Ayúdame a entender este error de actualización»

Mantenimiento continuo

- Supervise la ejecución de las actualizaciones con regularidad: consulte las pestañas Destinos y Fuentes de la administración de datos para asegurarse de que las actualizaciones se realizan correctamente
- Aborde los errores con prontitud: cuando Amazon Connect Decisions le avise de errores de actualización, investigue y resuelva los problemas rápidamente para evitar brechas de datos

- Actualice las credenciales de forma segura: cuando cambien las contraseñas de las bases de datos, actualícelas en AWS Secrets Manager, Amazon Connect Decisions utilizará automáticamente las nuevas credenciales
- Documente las configuraciones personalizadas: tome nota de los programas de actualización especiales, la lógica de transformación o los requisitos de conexión para que su equipo los pueda consultar
- Revise las tablas seleccionadas periódicamente: a medida que sus necesidades de datos vayan evolucionando, revise qué tablas está incorporando y si los programas de actualización siguen ajustándose a los requisitos empresariales

Comprensión del modelo de datos canónico (CDM)

El modelo de datos canónicos (CDM) es la estructura de datos estandarizada utilizada por. Al incorporar los datos de la cadena de suministro, estos deben transformarse al formato CDM para poder procesarlos con fines de planificación, previsión e información operativa.

En este tema se explica qué es el MDL, por qué es importante y qué entidades de datos están disponibles.

¿Qué es el MDL?

El CDM define un conjunto común de entidades y campos de datos que representan conceptos de la cadena de suministro, como productos, sitios, pedidos, envíos e inventario. Independientemente del formato o la estructura de los datos de origen, el CDM proporciona un esquema único y coherente que utiliza todas sus funciones.

Durante la incorporación de los datos, los datos de origen se asignan a las tablas de destino del CDM. El agente de datos puede sugerir automáticamente mapeos entre los campos de origen y los campos de CDM, y generar consultas de transformación de SQL para convertir los datos.

Por qué es importante el CDM

- Coherencia: todas las funciones funcionan en la misma estructura de datos, lo que garantiza un comportamiento uniforme en la planificación de la demanda, la optimización del inventario y la información sobre los plazos de entrega.
- Interoperabilidad: los datos de diferentes sistemas de origen (ERP, WMS, TMS) se normalizan en un único modelo, lo que permite el análisis entre sistemas.

- Integración simplificada: el agente de datos utiliza el CDM como esquema de destino al generar mapeos automatizados, lo que reduce el esfuerzo manual.
- Calidad de los datos: las comprobaciones de validación se comparan con las definiciones del MDL para detectar los problemas antes de que los datos se utilicen en la producción.

Categorías de entidades de datos

Las entidades de datos del MDL se dividen en dos categorías:

- Non-transactional datos: datos maestros o de referencia que cambian con poca frecuencia, como productos, sitios, socios comerciales y ubicaciones geográficas.
- Datos transaccionales: datos operativos que cambian con frecuencia, como las previsiones, los niveles de inventario, los pedidos y los envíos.

Entidades de datos compatibles

En la siguiente tabla se enumeran todas las entidades de datos compatibles con el CDM.

Entidades de datos del CDM compatibles

Entidad de datos	Tipo de datos	Obligatorio
Empresa	Non-transactional datos	Sí
Producto	Non-transactional datos	Sí
Socio comercial	Non-transactional datos	Sí
Producto de proveedor	Non-transactional datos	Sí
Geography	Non-transactional datos	Sí
Jerarquía de productos	Non-transactional datos	Sí
Carril de transporte	Non-transactional datos	Sí
Plazo de entrega del proveedor	Non-transactional datos	Sí

Entidad de datos	Tipo de datos	Obligatorio
Sitio	Non-transactional datos	Sí
Día festivo para vendedores	Non-transactional datos	Sí
Forecast	Datos transaccionales	Sí
Inventario	Datos transaccionales	Sí
Pedido entrante () PO/STO	Datos transaccionales	Sí
Línea de pedido saliente	Datos transaccionales	Sí
Shipment	Datos transaccionales	Sí
Política de inventario	Datos transaccionales	Sí
Línea de pedido entrante () PO/STO	Datos transaccionales	Sí
Envío saliente	Datos transaccionales	Sí
Calendario de líneas de pedidos entrantes	Datos transaccionales	Sí

Entidades requeridas por función

No todas las funciones requieren todas las entidades del CDM. Las siguientes secciones describen qué entidades son obligatorias, opcionales o no aplicables a cada función.

Visibilidad del inventario

Entidades de MDL para la visibilidad del inventario

Entidad de datos	Tipo de datos	Obligatorio
Empresa	Non-transactional	Opcional
Producto	Non-transactional	Sí

Entidad de datos	Tipo de datos	Obligatorio
Socio comercial	Non-transactional	Opcional
Producto de proveedor	Non-transactional	No aplicable
Geography	Non-transactional	Opcional
Jerarquía de productos	Non-transactional	Opcional
Carril de transporte	Non-transactional	Opcional
Plazo de entrega del proveedor	Non-transactional	No aplicable
Sitio	Non-transactional	Sí
Día festivo para vendedores	Non-transactional	No aplicable
Forecast	Transactional	Opcional
Inventario	Transactional	Sí
Pedido entrante () PO/STO	Transactional	Opcional
Línea de pedido saliente	Transactional	Opcional
Shipment	Transactional	Opcional
Política de inventario	Transactional	Sí
Línea de pedidos entrantes	Transactional	Opcional
Envío saliente	Transactional	Opcional
Calendario de líneas de pedidos entrantes	Transactional	Opcional

Información sobre los plazos de entrega

Entidades del MDL para obtener información sobre los plazos de entrega

Entidad de datos	Tipo de datos	Obligatorio
Empresa	Non-transactional	Opcional
Producto	Non-transactional	Sí
Socio comercial	Non-transactional	Sí
Producto de proveedor	Non-transactional	Sí
Geography	Non-transactional	Opcional
Jerarquía de productos	Non-transactional	Opcional
Carril de transporte	Non-transactional	Sí
Plazo de entrega del proveedor	Non-transactional	Sí
Sitio	Non-transactional	Sí
Día festivo para vendedores	Non-transactional	Opcional
Forecast	Transactional	No aplicable
Inventario	Transactional	No aplicable
Pedido entrante () PO/STO	Transactional	Sí
Línea de pedido saliente	Transactional	No aplicable
Shipment	Transactional	Sí
Política de inventario	Transactional	No aplicable
Línea de pedidos entrantes	Transactional	Sí
Envío saliente	Transactional	No aplicable

Entidad de datos	Tipo de datos	Obligatorio
Calendario de líneas de pedidos entrantes	Transactional	Sí

Planificación de la demanda

Entidades del MDL para la planificación de la demanda

Entidad de datos	Tipo de datos	Obligatorio
Empresa	Non-transactional	Opcional
Producto	Non-transactional	Sí
Socio comercial	Non-transactional	No aplicable
Producto de proveedor	Non-transactional	No aplicable
Geography	Non-transactional	Opcional
Jerarquía de productos	Non-transactional	Opcional
Carril de transporte	Non-transactional	No aplicable
Plazo de entrega del proveedor	Non-transactional	No aplicable
Sitio	Non-transactional	Sí
Día festivo para vendedores	Non-transactional	No aplicable
Forecast	Transactional	No aplicable
Inventario	Transactional	No aplicable
Pedido entrante () PO/STO	Transactional	No aplicable
Línea de pedido saliente	Transactional	Sí
Shipment	Transactional	No aplicable

Entidad de datos	Tipo de datos	Obligatorio
Política de inventario	Transactional	No aplicable
Línea de pedidos entrantes	Transactional	No aplicable
Envío saliente	Transactional	No aplicable
Calendario de líneas de pedidos entrantes	Transactional	No aplicable

Cómo se relaciona el CDM con la incorporación de datos

Al incorporar datos, el proceso sigue estos pasos:

1. Cargar: los datos de origen se cargan como archivos CSV en Amazon S3.
2. Mapa: el agente de datos analiza los conjuntos de datos de origen y sugiere qué tablas de destino del CDM se ajustan mejor a sus datos.
3. Transformación: las consultas de transformación de SQL convierten el formato de datos de origen en formato CDM.
4. Validación: se realizan controles de calidad con los datos transformados para comprobar que cumplen con los requisitos del CDM.
5. Activar: una vez validados, los datos fluyen hacia las funciones y están disponibles para ellas.

Para obtener instrucciones paso a paso sobre la incorporación de sus datos, consulte el tema Incorporación de datos.

Validación de datos y controles de calidad

Descripción general de

La validación de datos garantiza que sus datos cumplan los requisitos de calidad antes de que se ejecuten las capacidades de Amazon Connect Decisions. El sistema valida los datos en función de sus planes, métricas y reglas configurados para identificar los problemas que podrían bloquear o degradar el rendimiento.

Cómo funciona la validación de datos

Activadores de validación

La validación de datos se ejecuta automáticamente en los siguientes momentos:

- Cambios en la configuración de Insights: al crear o modificar métricas, reglas u otras configuraciones
- Creación de planes: al crear un plan ad hoc o cada vez que se ejecute un plan programado
- Actualización de datos: después de cada actualización de datos en sus flujos de destino
- Ejecución de la capacidad: antes o durante las operaciones de un compañero de equipo de IA (por ejemplo, al provocar una excepción o determinar recomendaciones)

Tipos de validación

Amazon Connect Decisions realiza dos tipos de validación:

La validación de presencia de datos verifica que los campos y conjuntos de datos necesarios se carguen en función de los recursos configurados (métricas, reglas, planes).

La validación de la calidad de los datos valida si los datos proporcionados cumplen los requisitos de calidad en función de la configuración de la configuración, que incluyen:

- Validación de los criterios de configuración: confirma que los productos y los sitios cumplen los criterios de las reglas (p. ej., categorías de productos o ubicaciones de sitios)
- Validación de jerarquías: identifica las relaciones jerárquicas que faltan si utiliza jerarquías en la configuración
- Validación del alcance: confirma que existen todos los datos necesarios para los productos y sitios identificados
- Evaluación de la calidad: evalúa la calidad y la usabilidad de los datos en función de los requisitos operativos

Validación progresiva

Amazon Connect Decisions habilita capacidades para productos y sitios con datos válidos en lugar de bloquear la funcionalidad de todo el conjunto de datos. Cuando los problemas de validación afectan a productos o sitios específicos, el sistema continúa procesando los productos y sitios con

datos válidos, identifica los productos o sitios con problemas de datos y le avisa sobre los elementos específicos que requieren atención. Esto le permite empezar a utilizar las capacidades y, al mismo tiempo, resolver los problemas de datos pendientes.

Errores de validación de datos al acceder

Puede ver los errores de validación de datos a través de tres puntos de entrada:

1. La métrica «errores de validación de datos» aparece en la página de inicio
2. Tarjeta temática sobre errores de validación de datos en la página de inicio
3. «Gestión de datos» en la pestaña de navegación izquierda **>** «Errores»

Revisión de los errores de validación

La página de errores muestra todos los errores de validación abiertos y resueltos. Puede buscar y filtrar por cualquiera de las siguientes columnas:

- ID: identificador único del error de validación
- Estado
  - Abierto: el error no se ha resuelto
  - Resuelto: se ha corregido y validado el error
- Descripción: Explicación del problema de calidad de los datos
- Tipo de problema
  - Faltan datos obligatorios: no se proporcionan datos obligatorios para activar una operación (por ejemplo, no hay una tabla fuente de outbound_order_line para el plan de suministro)
  - Valores de datos no válidos: los datos existen pero contienen valores incorrectos (por ejemplo, un coste negativo del producto)
  - Relaciones faltantes: faltan las relaciones jerárquicas o de referencia requeridas (por ejemplo, faltan jerarquías de productos)
  - Datos insuficientes: no hay suficientes datos disponibles para realizar las operaciones requeridas (por ejemplo, el plan de demanda requiere 12 meses de datos históricos de pedidos, pero solo existen 3 meses)
- Capacidad: la capacidad o el recurso afectados
  - Plan de suministro
  - Plan de demanda

  - Perspectiva (incluye excepciones, recomendaciones y un RCA para la oferta o la demanda)
- Destino: flujo de destino afectado
- Priority (Prioridad)
  - Crítico: al menos una capacidad está completamente bloqueada y no se puede ejecutar
  - Alto: al menos una capacidad está parcialmente bloqueada (algunos productos o sitios no se pueden procesar)
  - Medio: al menos una capacidad tiene una precisión reducida (se ejecutará pero con resultados degradados)
- Creado en: marca de tiempo que muestra cuándo se detectó el error por primera vez

Visualización de los detalles del error

Seleccione cualquier error para ver información detallada. La pantalla de detalles muestra la información anterior junto con la fecha y hora en que se produjo por última vez, el recurso y el enlace relacionados (la métrica, la regla o el plan que representa la capacidad afectada por el problema) y una vista previa de hasta 100 filas de datos afectados que muestran cómo se está manifestando el error de validación de datos.

Acciones disponibles

Desde la pantalla de detalles del error, puede:

- Solución de problemas: lanza un compañero de equipo de IA para que te ayude a solucionar el problema en lenguaje natural y reciba instrucciones detalladas sobre cómo solucionarlo
- Resolver el error: marca manualmente el error como resuelto si has solucionado el problema subyacente
- Descargar: descargue el conjunto de datos afectado completo para un análisis y una corrección detallados

Resolución de errores de validación de datos

flujo de trabajo de resolución

1. Revise la descripción y la prioridad del error para comprender el impacto
2. Consulte la vista previa de los datos afectados para ver qué registros específicos están afectados

3. Siga la recomendación específica proporcionada para la remediación
4. Elija una acción adecuada:
   - Para problemas de configuración: trabaje con sus gerentes y planificadores para ajustar la configuración de la métrica, la regla o el plan
   - Para problemas de mapeo: corrija los datos de origen cargados o actualice las transformaciones y mapeos de datos
   - En caso de datos faltantes o no válidos: cargue los datos corregidos
5. Marque manualmente el error como resuelto una vez que haya solucionado el problema subyacente

Trabajando con el compañero de equipo de IA

Usa la opción Solucionar problemas para hacer preguntas como «¿En qué errores debo centrarme primero?» o «¿Qué errores bloquean mi plan de demanda?» , reciba explicaciones detalladas del problema y su impacto, reciba instrucciones paso a paso sobre los enfoques de resolución y comprenda cómo afecta el error a su configuración específica. El compañero de equipo de IA puede servir de guía para resolver el problema en Amazon Connect Decisions y en sus sistemas de datos de origen.

Prácticas recomendadas

- Priorice por gravedad: concéntrese primero en los errores críticos, ya que impiden por completo la ejecución de las funcionalidades. A continuación, aborde los errores de prioridad alta que bloquean parcialmente el procesamiento, seguidos de los problemas de prioridad media que reducen la precisión.
- Revise las recomendaciones detenidamente: cada error incluye una guía específica y práctica adaptada al problema en función de su configuración.
- Utilice la validación progresiva a su favor: no espere a resolver todos los errores antes de utilizar las funciones. El sistema habilita la funcionalidad de productos y sitios válidos mientras usted trabaja para resolver problemas para otros.
- Supervise después de la actualización de los datos: compruebe si hay nuevos errores de validación después de cada actualización de datos para detectar los problemas antes de que afecten a los flujos de trabajo de producción.

- Descargue los datos afectados de forma estratégica: utilice la opción de descarga cuando necesite analizar todos los registros afectados más allá de la vista previa o cuando necesite proporcionar el conjunto de datos completo a su equipo de datos.
- Utilice a un compañero de equipo de IA para problemas complejos: la opción de solución de problemas proporciona asistencia contextual que se adapta a su situación y configuración específicas.
- Verifica la resolución: después de corregir los problemas de datos, marca manualmente los errores como resueltos para confirmar que la solución se ha realizado correctamente y elimínalos de la lista abierta.

Configuración del sistema

La configuración de Amazon Connect Decisions está organizada por ámbito y público. Algunos ajustes son personales, lo que permite a cada usuario personalizar su propia experiencia. Otras son configuraciones a nivel de instancia administradas por los administradores que afectan al comportamiento del sistema para todos los usuarios o a la forma en que se conecta a un entorno tecnológico más amplio.

User-level La configuración permite a las personas administrar la información de su cuenta, las preferencias de notificación y la forma en que el alcance de acceso a los datos se aplica a sus puntos de vista.

Instance-level Los ajustes permiten a los administradores configurar el comportamiento de los filtros de control de acceso en toda la organización, establecer conexiones con su ERP y otros sistemas externos y definir la forma en que el sistema gestiona las acciones recomendadas.

En conjunto, estas configuraciones proporcionan a su organización la flexibilidad necesaria para adaptar las decisiones de Amazon Connect a su contexto operativo específico y, al mismo tiempo, mantener la coherencia en todo el equipo.

Configuración del perfil de usuario

Los usuarios pueden acceder a la configuración de su perfil seleccionando su nombre en la esquina superior derecha de la aplicación y eligiendo Perfil en el menú desplegable. La página de perfil permite a los usuarios administrar la información de su cuenta, las preferencias de notificación y la configuración de acceso a los datos.

Acceder a la configuración del perfil

Para acceder a la configuración de tu perfil:

1. Selecciona tu nombre en la esquina superior derecha de la página
2. Selecciona Perfil en el menú desplegable
3. La página de perfil muestra la información y la configuración de tu cuenta

Información de perfil

La página de perfil muestra los siguientes detalles de la cuenta:

Usuario: su nombre de usuario

Función: su función asignada (administrador, gerente o planificador)

Zona horaria: selecciona la zona horaria que prefieras en el menú desplegable. Esta configuración determina cómo se muestran las fechas y las horas en las decisiones de Amazon Connect.

Correo electrónico: su dirección de correo electrónico asociada a su cuenta de Amazon Connect Decisions

Creada: la fecha y la hora en que se creó su cuenta

Actualizado: fecha y hora en que se modificó tu perfil por última vez

Selecciona Guardar en la esquina superior derecha para guardar cualquier cambio en la información de tu perfil.

Preferencias de notificación

La pestaña Preferencias de notificación le permite configurar la forma en que recibe las notificaciones de varios eventos del sistema. Puede elegir entre recibir las notificaciones en la aplicación, por correo electrónico o ambas.

Planes

Éxito en la generación del plan: elija cómo desea que se le notifique cuando la generación del plan se complete correctamente. Las opciones incluyen notificaciones integradas en la aplicación y notificaciones por correo electrónico.

Fallo en la generación del plan: elija cómo desea que se le notifique cuando se produzca un error en la generación del plan. Las opciones incluyen notificaciones integradas en la aplicación y notificaciones por correo electrónico.

Configuraciones de Insights

Las configuraciones de Insights se realizaron correctamente: elija cómo quiere que se le notifique cuando la configuración de Insights se complete correctamente. Entre las opciones se incluyen las notificaciones integradas en la aplicación.

Falló la configuración de Insights: elija cómo quiere que se le notifique cuando se produzca un error en la configuración de Insights. Entre las opciones se incluyen las notificaciones integradas en la aplicación.

Ingesta de datos

Error en la ingesta de datos: elija cómo desea que se le notifique cuando se produzca un error en la ingesta de datos. Las opciones incluyen notificaciones integradas en la aplicación y notificaciones por correo electrónico.

Configuración de administrador

Los administradores pueden configurar los ajustes de notificación de todo el sistema que se apliquen a todos los usuarios.

Retención de notificaciones: establezca el número de días después de los cuales las notificaciones se eliminarán automáticamente del sistema. Introduzca un valor numérico para especificar el período de retención.

Seleccione Guardar para aplicar sus preferencias de notificación.

Ámbito asignado

La pestaña Ámbito asignado muestra sus permisos de acceso a los datos y le permite configurar cómo se filtran las vistas de datos en función del ámbito asignado.

Acceso a los datos

En esta sección se muestra su nivel de acceso a los datos actual. Si tiene acceso a todos los sitios y productos, verá el mensaje «Tiene acceso a todos los sitios y productos».

Filtro de visualización predeterminado

Filtrar las vistas según el ámbito que se me haya asignado: cuando están activadas, las vistas de datos se filtran automáticamente para mostrar solo los artículos de los productos y sitios que tengas asignados. Activa o desactiva esta configuración según tus preferencias.

Cuando este filtro esté activado, solo verá las excepciones, los planes y otros datos relevantes para el ámbito asignado. Si está deshabilitado, es posible que veas datos fuera del ámbito asignado, en función de los permisos de tu función.

Selecciona Guardar para aplicar tus preferencias de filtro.

Alternar el filtro de control de acceso

Como se indicó anteriormente, todos los usuarios pueden ver todas las excepciones, independientemente de si han configurado los productos y sitios adecuados (las acciones de mutación siguen requiriendo el acceso adecuado). Si bien esto facilita el intercambio de conocimientos, los usuarios que se centran únicamente en productos y sitios específicos pueden verse abrumados por las excepciones o las recomendaciones de otros productos y sitios. Para ayudar a los usuarios a centrarse en las excepciones y recomendaciones que les interesan, pueden utilizar la opción de visualización de acceso de la siguiente manera:

- En primer lugar, un usuario con el rol de «administrador» debe habilitar la función en esa instancia. Ve a la página de configuración de la instancia desde la barra de navegación izquierda
- De forma predeterminada, verán una palanca que establece el filtro de vista de acceso predeterminado para toda la instancia. El «administrador» puede decidir tener una configuración unificada para todos los usuarios de la instancia o dejar que los usuarios decidan sus preferencias
- Si elige la configuración de la vista de acceso unificado, el «administrador» también puede decidir si la opción debe estar habilitada o deshabilitada para todos los usuarios
- Si decide permitir que cada usuario seleccione sus propias preferencias, cada usuario tendrá la opción de cambiar el filtro de la vista de acceso por sí mismo. Cada usuario puede ir a la página de preferencias del usuario desde el menú desplegable Usuario situado en la esquina superior derecha de la pantalla

Cambia la palanca de control de acceso de tu instancia:

1. Selecciona el cajón de la izquierda de Ajustes
2. Seleccione la aplicación
3. Actualice el conmutador y haga clic en guardar la configuración

Si la configuración está habilitada, el sistema filtrará automáticamente las páginas de listas de excepciones y recomendaciones para mostrar solo las que se hayan generado para un producto o sitio que coincida con la configuración de control de acceso.

En el caso de los usuarios que tengan activada la opción «Conceder acceso total a todos los productos y sitios», la barra de visualización de acceso seguirá mostrando todas las excepciones y recomendaciones. Si un usuario tiene esa opción desactivada pero no tiene ningún producto o sitio

configurado, el sistema interpretará que no tiene acceso a ningún producto o sitio y, por lo tanto, el usuario no verá nada

El filtro de visualización de acceso se considera un tipo de filtro diferente y, por lo tanto, no se mostrará en las fichas de filtro de la página de excepciones y recomendaciones. Los usuarios pueden seguir aplicando otros filtros de la misma forma que antes, incluidos otros filtros de productos y sitios

Los usuarios pueden seguir accediendo a las excepciones y recomendaciones de otros productos o sitios si desactivan la opción de visualización de acceso o si tienen el hipervínculo directo a ellos

Configuración de las conexiones a su ERP

Para permitir que Amazon Connect Decisions realice operaciones en su nombre en su sistema de planificación de recursos empresariales (ERP), debe configurar una conexión que especifique los parámetros de conexión necesarios y las credenciales que Amazon Connect Decisions debe utilizar durante la operación.

Sistemas ERP compatibles:

- SAP S/4HANA

Configurar las credenciales en Secrets Manager

1. Con tu cuenta, usa Secrets Manager para crear un secreto de Secrets Manager
   - Al introducir las credenciales en Secrets Manager, sustituya los valores de los marcadores de posición que aparecen a continuación (`<username>` y `<password>`) por el nombre de usuario y la contraseña reales que debe utilizar Amazon Connect Decisions
   - Si utiliza la consola, elija `Other type of secret` `Secret Type`
   - Si introduce los detalles a través de la `Key/value pairs` pestaña de la consola, introduzca 2 pares:
     - Clave:`username`; Valor: <*`username`*>
     - Clave:`password`; Valor: <*`password`*>
   - Si utilizas la `Plaintext` pestaña para introducir el secreto en la consola, introduce un objeto JSON con los dos pares:

     ```
     {
     ```

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

2. Cifra tu secreto con una clave AWS KMS y anota el identificador de la clave, ya que lo necesitarás en los pasos siguientes
3. Una vez creado tu secreto, anota su nombre de recurso de Amazon (ARN), ya que lo necesitarás en los pasos siguientes
   - p. ej.: `arn:aws:secretsmanager:<Region>:<AccountId>:secret:<SecretName>-<SixRandomCharacters>`

Configure los permisos en la clave KMS

Debe proporcionar los permisos necesarios para que Amazon Connect Decisions pueda acceder a él y utilizarlo.

1. Actualice su política de KMS para permitir que Amazon Connect Decisions acceda a su clave a través del rol de instancia
   - Nota: Sustituya `<YourAccountNumber>` y `<YourInstanceID>` por su AWS cuenta y el ID de instancia de 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. Actualiza la política interna de tu rol de instancia para conceder permisos sobre la clave

   - Nota: Sustituya <YourSecretArn> <YourAccountNumber> y <YourInstanceID> por su ARN secreto, AWS cuenta e ID de instancia de la cadena AWS de suministro.

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

Actualiza la política de recursos de Secrets Manager para tu secreto

1. Actualiza la política de recursos de Secrets Manager para tu secreto

   - Nota: <YourSecretArn> Sustitúyalo por el ARN de su secreto

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

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

Configurar la conexión de Amazon Connect Decisions

1. En su instancia de Amazon Connect Decisions, vaya a la página de administración de datos
2. Seleccione la `Connections` pestaña
3. Haga clic en el `Create Connection` botón
4. En la `Create Connector` página, haga clic en el `Select` botón de la fila correspondiente al tipo de `SAP S/4HANA` conector
5. En la `Configure SAP S/4HANA API Connector` página, introduzca la información necesaria:
   - `Connection Name`: nombre de conexión único
   - `API Endpoint URL`: la URL del punto final de la API de OData de su S/4HANA instancia de SAP (por ejemplo:`https://<hostname>:<port>`)
   - `Client Number`: el número de cliente de SAP de 3 dígitos (por ejemplo:) `100`
   - `Secret ARN`: el nombre de recurso de Amazon (ARN) del secreto de Secrets Manager, donde se almacenan las credenciales que utilizará Amazon Connect Decisions
6. Haga clic en el `Create Connector` botón

Configuración de los ajustes de acción

Amazon Connect Decisions le permite controlar los tipos de acciones que debe ofrecer para realizar operaciones en su nombre en su sistema de planificación de recursos empresariales (ERP). De forma predeterminada, todos los tipos de acciones están deshabilitados y debe habilitar esta función para cada tipo de acción que desee.

> **Note**
>
> Al habilitar la compatibilidad con un tipo de acción determinado, se controla si la opción de que Amazon Connect Decisions lleve a cabo la acción en su nombre se presentará en todo el sistema (por ejemplo, al revisar un Insight con una recomendación del tipo determinado).

Amazon Connect Decisions no realizará estas acciones (incluso cuando el soporte esté activado) hasta que usted acepte la recomendación específica.

Tipos de acciones compatibles:

- Crear pedido de compra
- Actualizar la orden de compra
- Cancelar la orden de compra

Configure el soporte de acciones para cada tipo de acción:

1. En su instancia de Amazon Connect Decisions, vaya a la página de administración de datos
2. Seleccione la `Actions` pestaña
3. Busque el tipo de acción que desea configurar en la lista
4. Para habilitar la compatibilidad con el tipo de acción:
   - Seleccione una de las conexiones que aparecen en el menú desplegable para ese tipo de acción
   - Nota: el menú desplegable mostrará solo las conexiones disponibles que se hayan configurado de un tipo que admita esa `Actions` capacidad (por ejemplo:) `SAP S/4HANA`
5. Para deshabilitar la compatibilidad con el tipo de acción:
   - Selecciona `No connection` ese tipo de acción en el menú desplegable
6. Haz clic `Save` para guardar los cambios

Seguridad

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Third-party los auditores prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los programas de conformidad de AWS. Para obtener más información sobre los programas de conformidad que se aplican a las decisiones de Amazon Connect, consulte AWS Services in Scope by Compliance Program.
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación sirve de ayuda para comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Amazon Connect. Los siguientes temas muestran cómo configurar Amazon Connect Decisions para cumplir sus objetivos de seguridad y conformidad.

Protección de los datos

El modelo de responsabilidad AWS compartida se aplica a la protección de datos en Amazon Connect Decisions. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se basa toda la AWS nube. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También es responsable de las tareas de configuración y administración de la seguridad de AWS los servicios que utiliza. Para obtener más información sobre la privacidad de datos, consulte Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la entrada del blog sobre el modelo de responsabilidad compartida de AWS y el RGPD en el blog sobre seguridad de AWS.

Para proteger los datos, le recomendamos que proteja las credenciales de la AWS cuenta y configure los usuarios individuales con AWS Identity and Access Management (IAM). De esta

manera, cada usuario recibe únicamente los permisos necesarios para cumplir con sus obligaciones laborales. También recomendamos proteger sus datos de las siguientes maneras:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Se utiliza SSL/TLS para comunicarse con AWS los recursos. Recomendamos TLS 1.2 o una versión posterior.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados de AWS los servicios.
- Utilice servicios de seguridad gestionados avanzados, como Amazon Macie, que ayudan a descubrir y proteger los datos confidenciales almacenados en Amazon Simple Storage Service.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no introducir nunca información confidencial, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, como, por ejemplo, el campo Nombre. Esto incluye cuando trabaja con Amazon Connect Decisions u otros AWS servicios mediante la consola AWS de administración, la API, AWS Command Line Interface (AWS CLI) o AWS los SDK. Cualquier dato que ingrese en etiquetas o campos de texto de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico.

Cifrado de datos

En este tema se proporciona información específica sobre las decisiones de Amazon Connect sobre el cifrado en tránsito y el cifrado en reposo.

Cifrado en tránsito

Toda la comunicación entre los clientes y Amazon Connect Decisions y entre Amazon Connect Decisions y sus dependencias descendentes está protegida mediante conexiones TLS 1.2 o superior.

Cifrado en reposo

Amazon Connect Decisions almacena los datos en reposo mediante DynamoDB y Amazon Simple Storage Service (Amazon S3). Los datos en reposo se cifran mediante soluciones de AWS cifrado de

forma predeterminada. Amazon Connect Decisions cifra sus datos mediante claves AWS de cifrado propias de AWS Key Management Service (AWS KMS). No tiene que tomar ninguna medida para proteger las claves AWS administradas que cifran sus datos. Para obtener más información, consulte las claves propiedad de AWS en la Guía para desarrolladores de AWS KMS .

Si cambias la clave de KMS utilizada para cifrar los datos de tu instancia de Amazon Connect Decisions en la AWS consola, debes crear una nueva instancia para empezar a usar la nueva clave para cifrar los datos. Los datos que se hayan cifrado con la clave anterior no se conservarán y solo los datos se cifrarán con la clave actualizada. Si quieres conservar los datos de un método de cifrado anterior, puedes volver a la clave que utilizaste durante esas conversaciones.

Sus conversaciones con Amazon Connect Decisions en la aplicación web y en las aplicaciones de chat solo se cifran con AWS-owned claves.

Cross-region procesamiento

Amazon Connect Decisions cuenta con la tecnología de Amazon Bedrock y utiliza la inferencia entre regiones (CRIS) para distribuir el tráfico entre distintas AWS regiones a fin de mejorar el rendimiento y la fiabilidad de las inferencias del modelo de lenguaje grande (LLM). Con la inferencia entre regiones, obtendrá:

- Un mayor rendimiento y resiliencia durante los periodos de alta demanda
- Un mayor rendimiento
- Acceso a las funciones y funciones de Amazon Connect Decisions, recientemente lanzadas, que se basan en los LLM más potentes alojados en Amazon Bedrock

Cross-region La inferencia funciona de forma diferente en función de la AWS región en la que se cree la instancia de Amazon Connect Decisions.

Para todas las instancias creadas en la región geográfica de EE. UU., Amazon Connect Decisions utilizará Global CRIS. Esto significa que las solicitudes de inferencia se enviarán a las AWS regiones comerciales compatibles de todo el mundo, lo que optimizará los recursos disponibles y permitirá un mayor rendimiento del modelo. Consulte la guía del usuario de Amazon Bedrock para obtener más información sobre Global CRIS.

Para todas las instancias creadas en la región geográfica de la UE, Amazon Connect Decisions utilizará el CRIS geográfico. Esto significa que las solicitudes de inferencia se guardan dentro de las AWS regiones que forman parte de la zona geográfica en la que residen originalmente los datos.

Consulte la guía del usuario de Amazon Bedrock para obtener más información sobre Geographic CRIS.

Por ejemplo, una solicitud realizada desde una instancia de Amazon Connect Decisions creada en la región EE.UU. Este (Virginia del Norte) (us-east-1) puede enviarse a AWS cualquier región del mundo, como Asia Pacífico (Sídney) (ap-southeast-2). Sin embargo, si una solicitud se realiza desde una instancia de Amazon Connect Decisions creada en la región Europa (Irlanda) (eu-west-1), se redirige AWS a una región de la UE, como Europa (Fráncfort) (eu-central-1). Para obtener más información, consulte Regiones compatibles para las decisiones de Amazon Connect.

Si bien las inferencias entre regiones no cambian el lugar donde se almacenan los datos, es posible que sus solicitudes y los resultados de salida se trasladen fuera de la región en la que residen originalmente los datos. Todos los datos se cifran mientras se transmiten a través de la red segura de Amazon. El uso de la inferencia entre regiones no conlleva ningún costo adicional. Para obtener información sobre dónde se almacenan los datos cuando utiliza Amazon Connect Decisions, consulte Protección de datos en Amazon Connect Decisions.

Decisiones sobre IAM para Amazon Connect

AWS Identity and Access Management (IAM) es un servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos de Amazon Connect Decisions. IAM es un servicio de AWS que puede utilizar sin cargo adicional.

¿Cómo funciona IAM con Amazon Connect Decisions?

Antes de utilizar IAM para gestionar el acceso a Amazon Connect Decisions, conozca qué funciones de IAM están disponibles para su uso con Amazon Connect Decisions. Para obtener una visión general de cómo funcionan Amazon Connect Decisions y otros AWS servicios con la mayoría de las funciones de IAM, consulte los servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Identity-based políticas para Amazon Connect Decisions

Compatibilidad con las políticas basadas en identidad: sí

Identity-based las políticas son documentos de política de permisos de JSON que puede adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. Estas políticas controlan

qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de la política de JSON de IAM en la Guía del usuario de IAM.

Resource-based políticas incluidas en Amazon Connect Decisions

Admite políticas basadas en recursos: no

Resource-based las políticas son documentos de política JSON que se adjuntan a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política basada en recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o AWS servicios.

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones políticas para las decisiones de Amazon Connect

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Las acciones políticas en Amazon Connect Decisions utilizan el siguiente prefijo antes de la acción:

```
scn
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

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

Recursos de políticas para Amazon Connect Decisions

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). En el caso de las acciones que no admiten permisos por recurso, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Claves de condición de la política para Amazon Connect Decisions

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puede crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición globales de AWS en la Guía del usuario de IAM.

Uso de credenciales temporales con Amazon Connect Decisions

Compatibilidad con credenciales temporales: sí

Las credenciales temporales proporcionan acceso a AWS los recursos a corto plazo y se crean automáticamente cuando se utiliza una federación o se cambia de rol. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en los servicios de IAM y AWS que funcionan con IAM en la Guía del usuario de IAM.

Sesiones de acceso directo para Amazon Connect Decisions

Admite sesiones de acceso directo (FAS): sí

Las sesiones de acceso directo (FAS) utilizan los permisos del principal que llama a un AWS servicio, junto con los del AWS servicio solicitante, para realizar solicitudes a los servicios descendentes. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Sesiones de acceso directo.

Funciones de servicio para Amazon Connect Decisions

Compatible con roles de servicio: sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puedes crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Crear un rol para delegar permisos a un AWS servicio en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de Amazon Connect Decisions. Edite las funciones de servicio solo cuando Amazon Connect Decisions proporcione orientación para hacerlo.

Identity-based ejemplos de políticas

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de Amazon Connect Decisions. Tampoco pueden realizar tareas mediante la consola de AWS administración, la interfaz de línea de AWS comandos (AWS CLI) o la AWS API. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Política de administración de instancias (IAM)

A continuación, se muestra la política de IAM necesaria para crear, actualizar o eliminar instancias a través de la consola o la API pública (se excluyen todas las operaciones de la aplicación web).

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

Prácticas recomendadas sobre las políticas

Identity-based las políticas determinan si alguien puede crear, acceder o eliminar los recursos de Amazon Connect Decisions de su cuenta. Estas acciones pueden generar costos adicionales para su cuenta de AWS . Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para comenzar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas administradas de AWS que otorgan permisos para muchos casos de uso comunes. Están disponibles en su cuenta de AWS . Se recomienda definir políticas administradas por el cliente de AWS específicas para sus casos de uso a fin de reducir aún más los permisos. Para obtener más información, consulte Políticas administradas por AWS o Políticas administradas por AWS para funciones laborales en la Guía del usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puede utilizar condiciones para conceder acceso a las acciones de servicio si se utilizan a través de un AWS servicio específico, por ejemplo. CloudFormation Para

obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.

- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesita un usuario raíz o usuarios de IAM en su cuenta de AWS , active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Solución de problemas de IAM

Utilice la siguiente información para ayudarle a diagnosticar y solucionar los problemas habituales que puede encontrar al trabajar con Amazon Connect Decisions e IAM.

No estoy autorizado a realizar ninguna acción en Amazon Connect Decisions

Si la consola AWS de administración no está autorizado a realizar una acción, debe ponerse en contacto con su administrador para obtener ayuda. El administrador es la persona que le facilitó el nombre de usuario y la contraseña.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio `my-example-widget`, pero no tiene los permisos ficticios `scn:GetWidget`.

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

En este caso, Mateo pide a su administrador que actualice sus políticas de forma que pueda obtener acceso al recurso `my-example-widget` mediante la acción `scn:GetWidget`.

No estoy autorizado a realizar lo siguiente: PassRole

Si recibe un error que indica que no está autorizado a realizar la `iam:PassRole` acción, sus políticas deben actualizarse para que pueda transferir una función a Amazon Connect Decisions.

Algunos AWS servicios le permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada al servicio. Para ello, debe tener permisos para transferir la función al servicio.

El siguiente ejemplo de error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Amazon Connect Decisions. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir la función al servicio.

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

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mi AWS cuenta para acceder a mis recursos de Amazon Connect Decisions

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si Amazon Connect Decisions admite estas funciones, consulte Cómo funciona Amazon Connect Decisions con IAM.
- Para obtener información sobre cómo proporcionar acceso a sus recursos en todas AWS las cuentas de su propiedad, consulte Proporcionar acceso a un usuario de IAM en otra AWS cuenta de su propiedad en la Guía del usuario de IAM.

- Para obtener información sobre cómo proporcionar acceso a tus recursos a AWS cuentas de terceros, consulta Cómo proporcionar acceso a AWS cuentas propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Third-party subprocesadores

Amazon Connect Decisions utiliza Boomi, una API de terceros, para permitir que se tomen medidas en su nombre en sistemas externos. Cuando utilizas una función de Amazon Connect Decisions que se conecta a tus sistemas de terceros, nos autorizas a utilizar Boomi como nuestro middleware de integración para transmitir y procesar tus datos cifrados; tus datos no se almacenan por separado en Boomi.

Para obtener más información sobre Boomi y cómo funciona, consulta la documentación pública de Boomi.

Regiones admitidas

En esta página se describen las AWS regiones en las que puede utilizar Amazon Connect Decisions. Para obtener más información sobre AWS las regiones, consulte Especificar qué AWS regiones puede usar su cuenta en la Guía de referencia de administración de AWS cuentas.

Es posible que sus datos se procesen en una región diferente de la región en la que utiliza Amazon Connect Decisions. Para obtener información sobre el procesamiento entre regiones en Amazon Connect Decisions, consulte Cross-region Procesamiento. Para obtener información sobre dónde se almacenan los datos durante el procesamiento, consulte Protección de datos.

Regiones admitidas

Amazon Connect Decisions está disponible en la consola de AWS administración, la aplicación AWS Console Mobile Application, el AWS sitio web y el sitio web de AWS documentación en las siguientes AWS regiones. Estas regiones están habilitadas de forma predeterminada, lo que significa que no es

necesario habilitarlas antes de usarlas. Para obtener más información, consulte Regiones que están habilitadas de forma predeterminada.

Utiliza Amazon Connect Decisions en las siguientes regiones.

Nombre de la región de AWS	Nombre en clave	Geografía (EE. UU., UE, etc.)
Este de EE. UU. (Norte de Virginia)	us-east-1	EE. UU.
Europa (Irlanda)	eu-west-1	UE

Resolución de problemas

Cuando surjan problemas durante la configuración o el uso diario de Amazon Connect Decisions, en esta sección se proporcionan instrucciones para ayudarle a diagnosticar y resolver los problemas más comunes. Comience por identificar la categoría que mejor se adapte al problema que tiene y, a continuación, siga los pasos de solución de problemas de la página correspondiente. Si no está seguro de qué categoría corresponde, comience por Problemas comunes de configuración, que cubre la gama más amplia de problemas de configuración inicial.

Problemas comunes de configuración

Errores de integridad referencial: «Los valores del product_id no coinciden con ningún identificador del conjunto de datos del producto»

La causa más común son los espacios en blanco que aparecen al final de los campos de ID. Los sistemas de origen que exportan desde bases de datos de ancho fijo suelen rellenar los campos de cadenas con espacios. El producto maestro puede tener identificadores limpios («MAT604"), mientras que el archivo de la línea de pedido tiene identificadores rellenados («MAT604»). El sistema hace coincidir estrictamente las cadenas, por lo que no se unirán.

Solución: añada TRIM () a todos los campos de ID de cadena de las transformaciones SQL de su flujo de datos. Aplícala a product_id, ship_from_site_id, customer_tpartner_id y cualquier otra clave de unión. Compruebe también si hay inconsistencias entre comillas entre archivos. Al volver a exportar los CSV, utilice QUOTE_ALL para evitar problemas de inferencia de tipos en los que los identificadores con aspecto numérico (p. ej., «111613") se traten como enteros en un archivo y como cadenas en otro.

Prevención: recorta siempre todos los campos de ID de tus transformaciones de SQL como práctica predeterminada, incluso si no ves el problema en la actualidad. Los datos de origen pueden cambiar de una exportación a otra.

Faltan productos en el historial de pedidos en el producto maestro

Tu historial de pedidos suele incluir productos que no figuran en el catálogo de productos actual (productos descontinuados, artículos de un solo uso, SKU de prueba). El sistema rechazará todo el fichero de pedido si algún product_id no tiene un registro maestro de producto coincidente.

Solución: (a) crea filas auxiliares en el producto maestro para los productos faltantes con un mínimo de campos obligatorios (id, descripción, base_uom) o (b) filtra el historial de pedidos para incluir solo los productos presentes en el producto maestro. Se prefiere la opción (a) porque conserva el historial de demanda, que puede resultar útil para detectar linajes y tendencias.

Errores de análisis del CSV al subir la versión maestra del producto

Las descripciones de los productos que contienen comas, comillas o caracteres especiales pueden interrumpir el análisis del CSV. Es posible que veas errores como «Se esperaban 17 campos, vi 19» en filas específicas.

Solución: Re-export el archivo con las comillas adecuadas (QUOTE_ALL). Compruebe las filas específicas que fallan para ver si hay comas incrustadas en los campos de descripción.

Los datos no aparecen después de subirlos

- Comprueba que el formato del archivo no haya cambiado (extensión, encabezados de columna, codificación).
- Comprueba que los nombres y las extensiones de los archivos coincidan con el patrón esperado: si cambias el nombre de .csv a .csv000 o similar, se interrumpirá la ingestión.
- Tras la carga, espere hasta 30 minutos para que se complete la ingesta de datos.
- Si los encabezados de las columnas cambian de una carga a otra (por ejemplo, si las columnas tienen un nombre month/year), es necesario realizar un paso previo al procesamiento antes de cargarlas.

El PIV no se actualiza después de actualizar los datos

- El PIV se activa aproximadamente 15 minutos después de que se complete la ingestión y tarda entre 20 y 30 minutos en ejecutarse.
- End-to-end desde la carga de los datos hasta la nueva PIV: aproximadamente de 1 a 1,5 horas.
- Si el PIV no se ha actualizado en más de 24 horas, ponte en contacto con el servicio de asistencia.

Los recuentos de excepciones parecen demasiado altos o demasiado bajos

- Demasiado alto: es posible que el umbral sea demasiado bajo o que un solo producto y sitio estén generando varias excepciones para fechas diferentes. Ponte en contacto con el soporte técnico para revisar la configuración de las reglas.
- Demasiado bajo: es posible que el umbral sea demasiado restrictivo o que falten datos obligatorios (por ejemplo, previsiones o niveles de inventario) para algunos productos.

Spot-check conoce bien algunos productos y compara lo que muestra el sistema con lo que muestra tu sistema original.

No se muestra ningún impacto financiero en las excepciones

El impacto financiero requiere que el coste unitario se incluya en los datos del producto. Si falta el costo de un producto o es cero, no se mostrará el valor en dólares. Consulta con tu equipo de soporte la cobertura de los datos de costes: un enfoque en cascada que abarque varios campos de costes suele ofrecer la mejor cobertura.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.