aws

Guida per l'amministratore

Decisioni su Amazon Connect

Decisioni su Amazon Connect: Guida per l'amministratore

Table of Contents

Che cos'è Amazon Connect Decisions

Amazon Connect Decisions è una soluzione di pianificazione e intelligence della catena di approvvigionamento con membri del team di intelligenza artificiale che collaborano con il tuo team per armonizzare i segnali di domanda in previsioni di consenso, generare piani di fornitura consapevoli dei vincoli e monitorare attivamente le tue operazioni per prevenire problemi, risolverli e identificare le cause principali del miglioramento continuo.

I membri del team che si occupano di intelligenza artificiale si adattano al tuo modo di lavorare: si basano sulle tue procedure e regole operative, si integrano con i sistemi esistenti e imparano dalle decisioni dei tuoi professionisti. Sfrutta l'esperienza della catena di fornitura di Amazon per fornire piani e consigli efficaci sin dal primo giorno.

Dirigi un team di agenti di intelligenza artificiale che gestiscono il coordinamento e l'esecuzione delle azioni, consentendoti di concentrarti su decisioni strategiche che promuovono i livelli di servizio e l'efficienza del capitale circolante.

Vantaggi

Adattati alla tua attività

I membri del team di intelligenza artificiale si adattano alla tua azienda, ai tuoi sistemi e alle tue decisioni, apportando rapidamente la trasformazione all'interno dei flussi di lavoro esistenti. Guidati dalle procedure operative e dalle regole aziendali, i colleghi del team lavorano con i sistemi di pianificazione ed ERP esistenti. Imparano dalle decisioni dei pianificatori, allineandosi alle vostre priorità e istituzionalizzando le conoscenze in modo che le vostre operazioni migliorino nel tempo e che ogni membro del team sia più efficace.

Rimani al passo con ciò che sta arrivando

Dirigi un team di agenti di intelligenza artificiale che gestiscono il lavoro di coordinamento, 24/7 armonizzando i segnali di domanda, generando piani consapevoli dei vincoli ed eseguendo azioni approvate. I colleghi del team rilevano anche schemi invisibili all'analisi manuale, come interruzioni a cascata dei fornitori o disallineamenti dell'inventario su migliaia di SKU, e scoprono ciò che conta prima che diventi un problema. I pianificatori passano dalla lotta antincendio reattiva alla pianificazione proattiva, eseguendo operazioni più efficaci e migliorando i livelli di servizio attraverso decisioni strategiche che favoriscono i risultati aziendali.

Crea fiducia sin dal primo giorno

I membri del team di intelligenza artificiale sono supportati da una scienza perfezionata in 30 anni di supervisione di oltre 400 milioni di SKU Amazon e sono dotati di strumenti specializzati per la catena di fornitura. Il tuo team trae vantaggio dall'esperienza di settore acquisita da una delle reti di supply chain più complesse al mondo, in grado di fornire informazioni e consigli utilizzabili pronti all'uso con ragionamenti chiari e spiegabili, affidabili e verificati.

Funzionalità

Intelligenza adattiva

I membri del team di intelligenza artificiale imparano da ogni piano e decisione attraverso un ciclo continuo: osservando i modelli, rilevando ciò che conta, consigliando azioni ed eseguendo le decisioni approvate. In questo modo si istituzionalizza la conoscenza: quando i responsabili della pianificazione se ne vanno, le competenze rimangono invariate; i nuovi membri sono produttivi sin dal primo giorno, migliorando i risultati senza bisogno di riqualificazione manuale.

Richiedete informazioni

I membri del team di intelligenza artificiale orchestrano dinamicamente più di 18 strumenti di previsione e modelli di base formati sui dati di Amazon, ottimizzando in modo autonomo a livello di SKU. Genera previsioni accurate sin dal primo giorno, anche con una cronologia limitata. Armonizza le previsioni statistiche, gli impegni con i clienti e gli input interfunzionali attraverso una pianificazione consensuale e monitorando continuamente l'accuratezza.

Fornisci informazioni

I membri del team di intelligenza artificiale generano piani di fornitura lungimiranti (anteprima) e raggruppano in modo intelligente le eccezioni in decisioni strategiche classificate in base all'impatto. Esegui modelli di ottimizzazione per una pianificazione basata sui vincoli in tutta la tua rete. Monitora le operazioni 24/7, evidenzia ciò che conta, quindi esegui le decisioni approvate direttamente nei sistemi esistenti, riducendo i cicli da settimane a ore.

Inserimento degli agenti

AI-powered Gli agenti di onboarding ti guidano nella configurazione tramite una conversazione in linguaggio naturale. Connetti dati frammentati tramite JDBC o Amazon S3, preparali per Connect Decisions e segnala automaticamente i problemi prima che influiscano sulle previsioni. Configura

le regole e le politiche aziendali in un linguaggio semplice con anteprime in tempo reale: diventa operativo in settimane, non mesi.

Nozioni di base

In questa sezione, puoi imparare a creare un'istanza Amazon Connect Decisions, concedere ruoli di autorizzazione utente e accedere all'applicazione web Amazon Connect Decisions.

Prerequisiti per utilizzare Amazon Connect Decisions

Prima di creare un'istanza Amazon Connect Decisions, assicurati di completare i seguenti passaggi:

- Hai un AWS account. Per creare un AWS account, consulta Configurazione di un account AWS.
- Assicurati che IAM Identity Center sia abilitato. Per abilitare IAM Identity Center, consulta Enabling IAM Identity Center.
- Un'istanza IAM Identity Center deve essere attivata nella stessa regione in cui desideri creare l'istanza Amazon Connect Decisions. Amazon Connect Decisions è supportato solo nella regione Stati Uniti orientali (Virginia settentrionale) ed Europa (Irlanda).
- Se l'istanza Amazon Connect Decisions non si trova nella stessa regione della regione IAM Identity Center esistente, contattaci per ulteriore assistenza.
- È necessario disporre di almeno un utente nell'istanza IAM Identity Center da assegnare come amministratore di Amazon Connect Decisions. Puoi connettere la tua Active Directory a IAM Identity Center. Per ulteriori informazioni, vedere Connect to a Microsoft AD directory.
- Aggiungi eventuali utenti aggiuntivi che devono accedere ad Amazon Connect Decisions a IAM Identity Center.
- È necessario il AWS Key Management Service (AWS KMS) per creare un'istanza. Amazon Connect Decisions utilizza questa chiave AWS KMS per crittografare tutti i dati che entrano in Amazon Connect Decisions. Per informazioni sulle chiavi AWS KMS, consulta Creazione di chiavi.
- Se intendi abilitare la funzionalità delle azioni, dovrai configurare una connessione al sistema che utilizzi per conservare i dati pertinenti e fornire le credenziali da utilizzare per Amazon Connect Decisions. Contattaci per ulteriore assistenza.

Browser supportati da Amazon Connect Decisions

Prima di utilizzare Amazon Connect Decisions, verifica che il tuo browser sia supportato utilizzando la tabella seguente.

Browser	Versioni supportate
Google Chrome	Le ultime tre versioni.
Mozilla Firefox ESR	Sono supportate le versioni fino alla data di fine del ciclo di vita di Firefox. Per informazioni dettagliate, consulta il calendario delle versioni di Firefox ESR.
Mozilla Firefox	Le ultime tre versioni.
Microsoft Edge e Edge Chromium	Versione 84 e successive.
Safari	Safari 10 o versioni successive su macOS.

Lingue supportate da Amazon Connect Decisions

Amazon Connect Decisions supporta le seguenti lingue:

- Inglese (Stati Uniti)

Configurazione di un account AWS

Utilizza questa sezione per creare un AWS account e creare un utente IAM. Per informazioni sulle migliori pratiche per creare un AWS account, consulta Stabilire un AWS ambiente di best practice.

Registrati per un AWS account

Se non disponi di un AWS account, completa i seguenti passaggi per crearne uno.

Per iscriverti a un AWS account

1. Aprire https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata o un messaggio di testo e ti verrà chiesto di inserire un codice di verifica attraverso la tastiera del telefono.

Quando si registra un AWS account, viene creato un AWS account utente root. L'utente root ha accesso a tutte le risorse e i servizi AWS in tale account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. Puoi visualizzare l'attività corrente del tuo account e gestire l'account in qualsiasi momento accedendo a https://aws.amazon.com/ e scegliendo My Account (Il mio account).

Crea un utente con accesso amministrativo

Dopo aver registrato un AWS account, proteggi l'utente root del tuo AWS account, abilita AWS IAM Identity Center e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi AWS Utente root dell'account

1. Accedi alla Console di AWS gestione come proprietario dell'account scegliendo Utente root e inserendo l'indirizzo e-mail AWS del tuo account. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Accedere come utente root nella Guida per l'utente di AWS Sign-In.
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente root (console) dell' AWS account nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita il Centro identità IAM.

   Per istruzioni, consulta Enabling AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center.
2. Nel Centro identità IAM, assegna l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo della directory IAM Identity Center come fonte di identità, consulta Configurare l'accesso utente con la directory IAM Identity Center predefinita nella Guida per l'utente di AWS IAM Identity Center.

Accesso come utente amministratore

- Per accedere come utente del Centro identità IAM, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente del Centro identità IAM.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'AWS Sign-In utente.

Assegnazione dell'accesso ad altri utenti

1. Nel Centro identità IAM, crea un set di autorizzazioni conforme alla best practice per l'applicazione di autorizzazioni con il privilegio minimo.

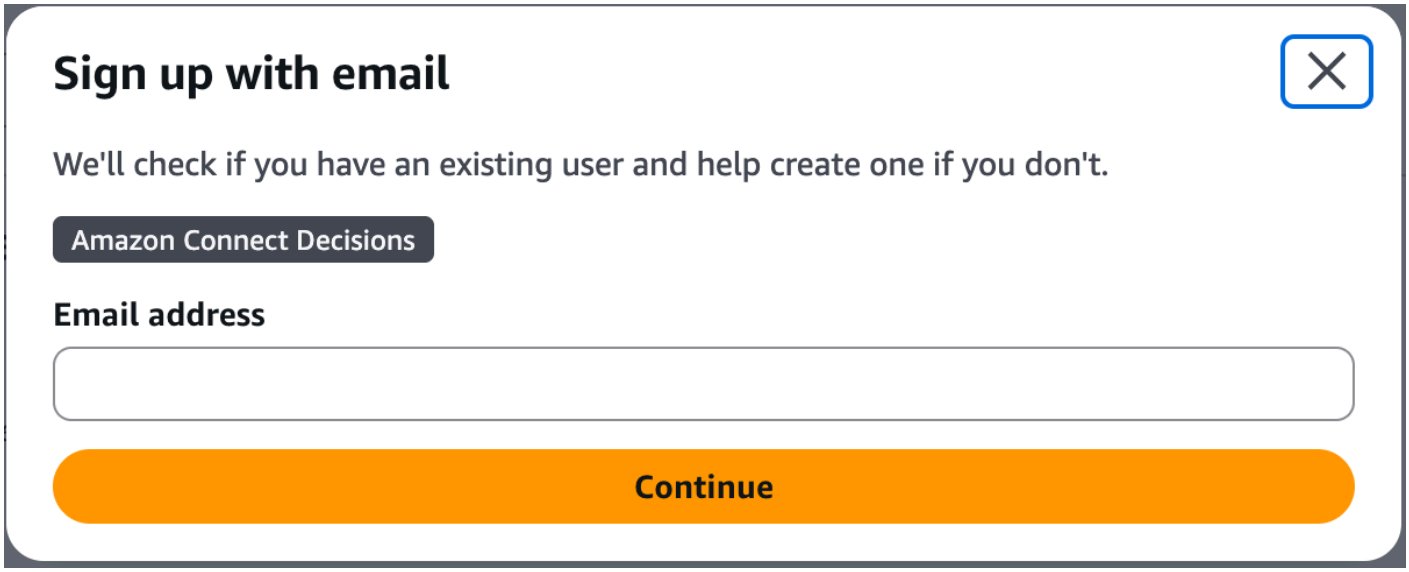
   Per istruzioni, consulta Creare un set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center.
2. Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente di AWS IAM Identity Center.

Configurazione dell'integrazione con AWS Identity Center

Per creare un'istanza e utilizzare il servizio Amazon Connect Decisions, devi connettere un profilo utente IAM Identity Center esistente o crearne uno nuovo.

1. Apri la console Amazon Connect Decisions. Puoi anche cercare «Amazon Connect Decisions» dalla console di AWS gestione principale.
2. Se necessario, modifica la regione AWS selezionando Seleziona una regione nella parte superiore della console. Scegli la tua regione dall'elenco a discesa.
3. Seleziona Crea un'istanza Amazon Connect Decisions. Apparirà una notifica.



4. Inserisci il tuo indirizzo email e seleziona Continua. iDC verificherà se l'e-mail corrisponde a un utente esistente.
5. Esegui una delle seguenti operazioni:
   - Se iDC abbina l'indirizzo email a un utente, seleziona Connect your identity source ed entra a far parte del tuo team.

     > **Note**
     >
     > Può essere usato se la tua organizzazione ha un'istanza iDC consolidata che desideri utilizzare per Amazon Connect Decisions.

   - Se iDC non trova una corrispondenza con un utente esistente, viene visualizzata una notifica Crea un nuovo utente. Passare alla fase successiva.
6. Nella notifica, inserisci quanto segue, quindi seleziona Continua:
   - Indirizzo e-mail
   - Nome
   - Cognome

   iDC crea automaticamente l'utente e lo aggiunge come amministratore di Amazon Connect Decisions.
7. Esegui una delle seguenti operazioni:
   - Per creare un'istanza utilizzando la configurazione standard, seleziona Crea. Vedi Usa la configurazione standard.

- Per creare un'istanza utilizzando una configurazione personalizzata, seleziona Modifica nella configurazione avanzata. Vedi Usa la configurazione avanzata.

Se utilizzato insieme a IAM Identity Center, Amazon Connect Decisions recupera i campi «nome utente» e «email» dalla directory IAM Identity Center. Nessuno di questi attributi viene memorizzato in modo nativo nell'istanza Amazon Connect Decisions e viene sempre recuperato in fase di esecuzione. Amazon Connect Decisions crittografa questi attributi di identità inattivi utilizzando una chiave KMS AWS di proprietà per impostazione predefinita. Le chiavi KMS gestite dal cliente non sono supportate in Amazon Connect Decisions. Se elimini un utente dalla tua istanza AWS IAM Identity Center, Amazon Connect Decisions elimina anche quell'utente dall'istanza.

Gestione dell'istanza Amazon Connect Decisions

La creazione di un'istanza in Amazon Connect Decisions crea un ambiente dedicato per la gestione e l'analisi della catena di fornitura. Per configurare un'istanza, devi configurare i dettagli di base, stabilire le impostazioni e definire le autorizzazioni iniziali di accesso utente.

Solo l'amministratore AWS della console di gestione può creare un'istanza. L'amministratore della Console di AWS gestione che crea l'istanza Amazon Connect Decisions deve disporre di tutte le autorizzazioni elencate negli esempi di Identity-based policy. Questo amministratore deve invitare un utente IAM in qualità di amministratore di Amazon Connect Decisions per gestire Amazon Connect Decisions.

Le pagine seguenti descrivono in dettaglio il processo di creazione ed eliminazione di un'istanza.

Creazione dell'istanza

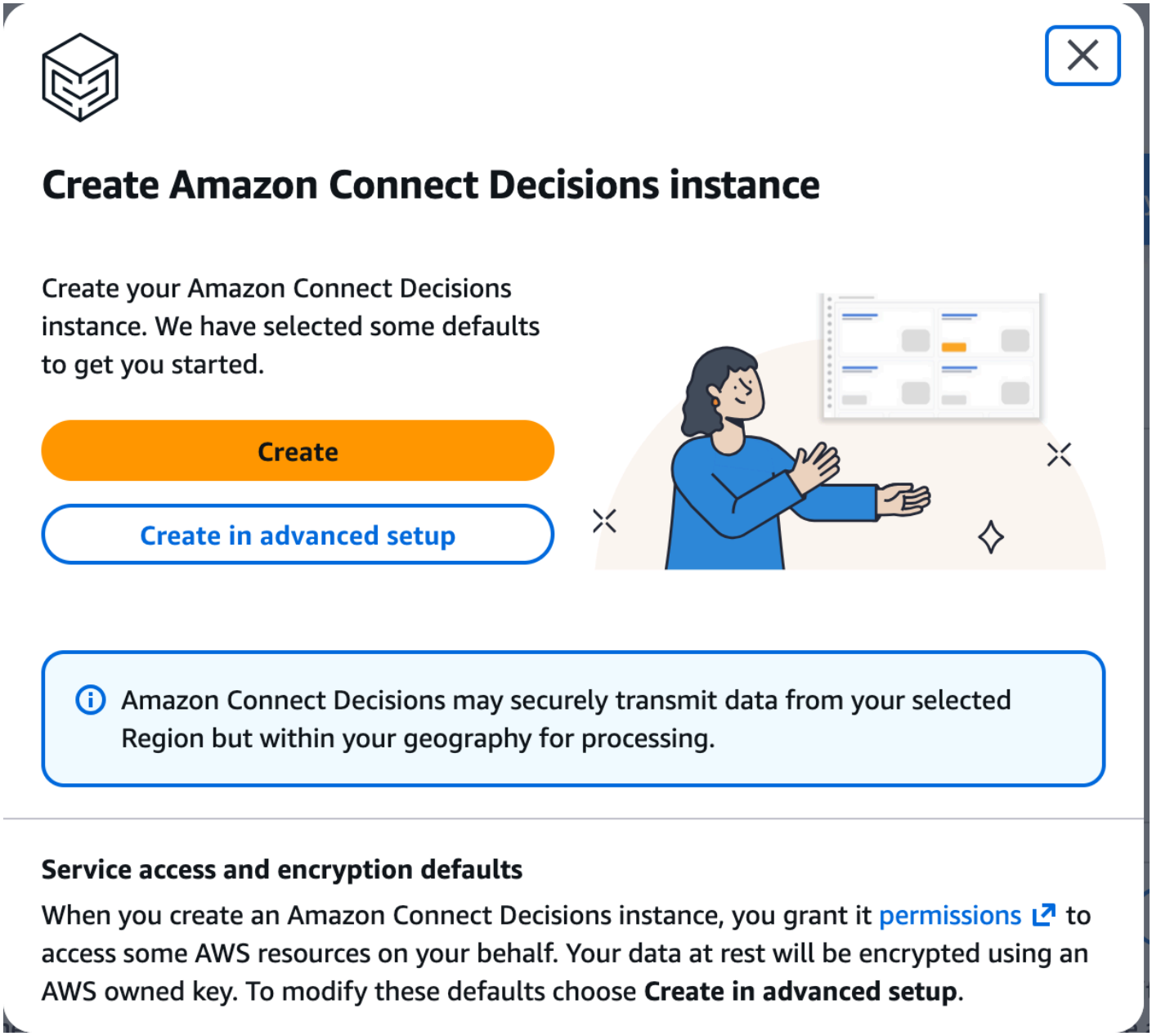
Puoi creare un'istanza utilizzando uno dei due metodi, configurazione standard o configurazione avanzata. La configurazione standard utilizza un processo automatizzato che crea rapidamente l'istanza utilizzando parametri preimpostati. La configurazione avanzata consente di personalizzare l'istanza impostando parametri personalizzati.

Utilizzo della configurazione standard

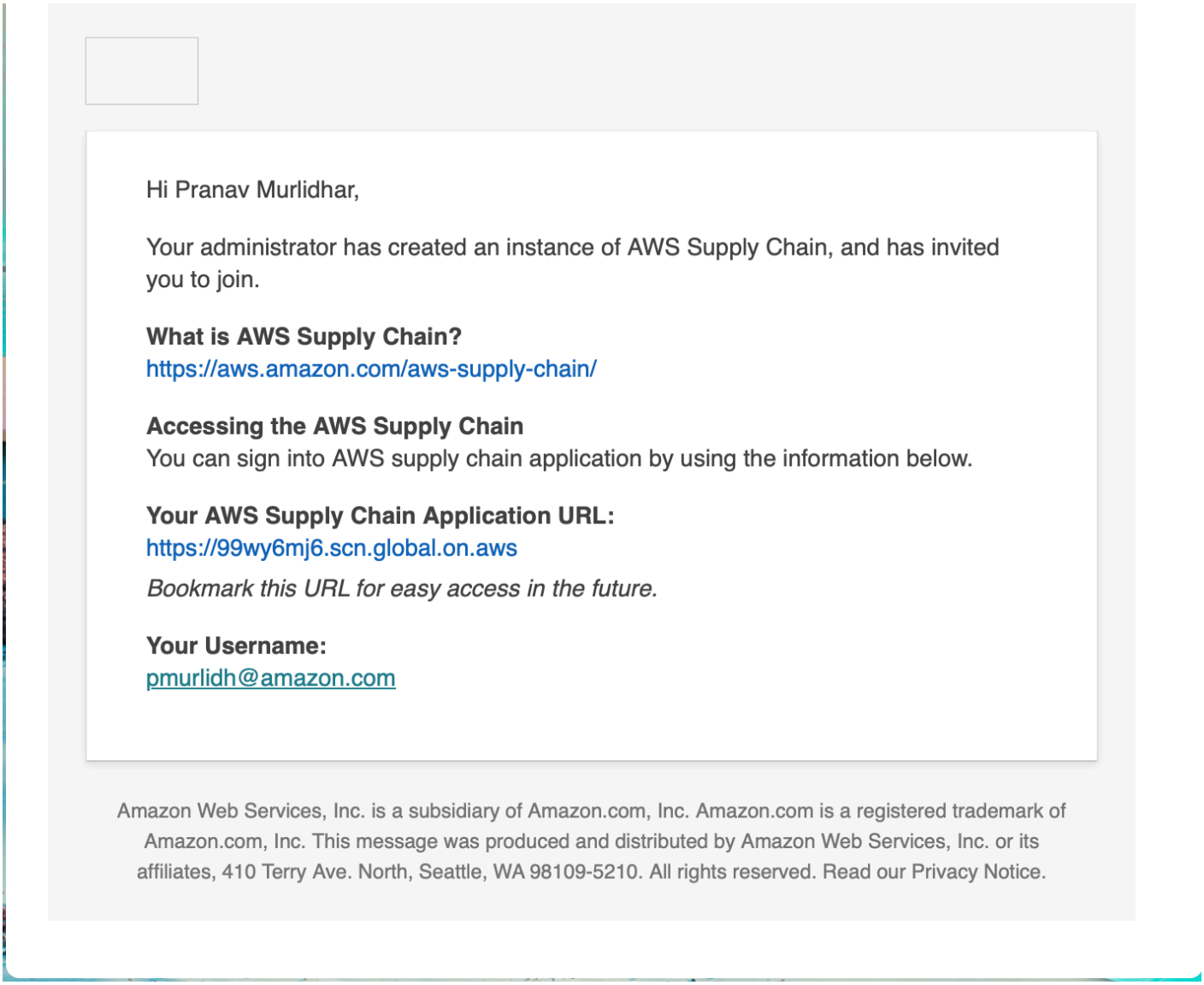
La configurazione standard crea la tua istanza Amazon Connect Decisions utilizzando impostazioni di sicurezza e crittografia predefinite. Le istanze operano in aree AWS geografiche. Per ulteriori informazioni sulle regioni, consulta Regioni ed endpoint nella IAM User Guide e Regional endpoints nel General AWS Reference.

Per creare un'istanza Amazon Connect Decisions utilizzando una configurazione standard di parametri preimpostati, segui questi passaggi.

1. Seleziona Crea.



2. Controlla la tua e-mail per verificare quanto segue:
   - Un'email dal team di iDC.
   - Un'e-mail dal team di Identity Management.

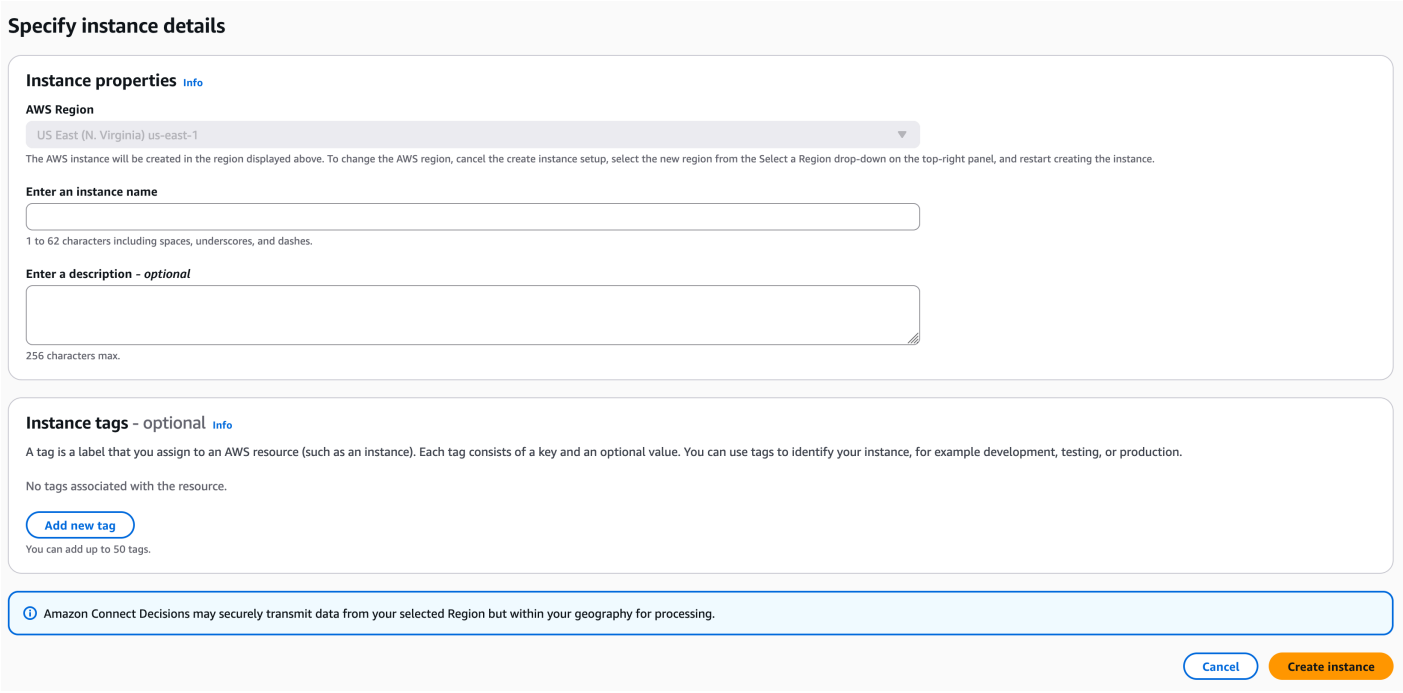


3. Dopo aver ricevuto l'e-mail di invito, accedi ad Amazon Connect Decisions. Vedi Accedere all'applicazione web Amazon Connect Decisions.

Utilizzo della configurazione avanzata

La configurazione avanzata consente di personalizzare l'istanza impostando parametri personalizzati. Per creare un'istanza Amazon Connect Decisions utilizzando una configurazione avanzata di parametri preimpostati, segui questi passaggi.

1. Seleziona Crea in configurazione avanzata.
2. Verrà visualizzata la pagina delle proprietà dell'istanza.



3. Inserisci quanto segue nella pagina delle proprietà dell'istanza:
   - Nome: immettere il nome di un'istanza.
   - Descrizione: inserisci una descrizione della tua istanza Amazon Connect Decisions (ad esempio, istanza di produzione, istanza di test, ecc.).
   - Tag di istanza: puoi aggiungere tag all'istanza che possono essere utilizzati per l'identificazione. Ad esempio, puoi aggiungere un tag per definire il tipo di istanza che stai creando (ad esempio, produzione, test, UAT, ecc.).
4. Seleziona Crea istanza.

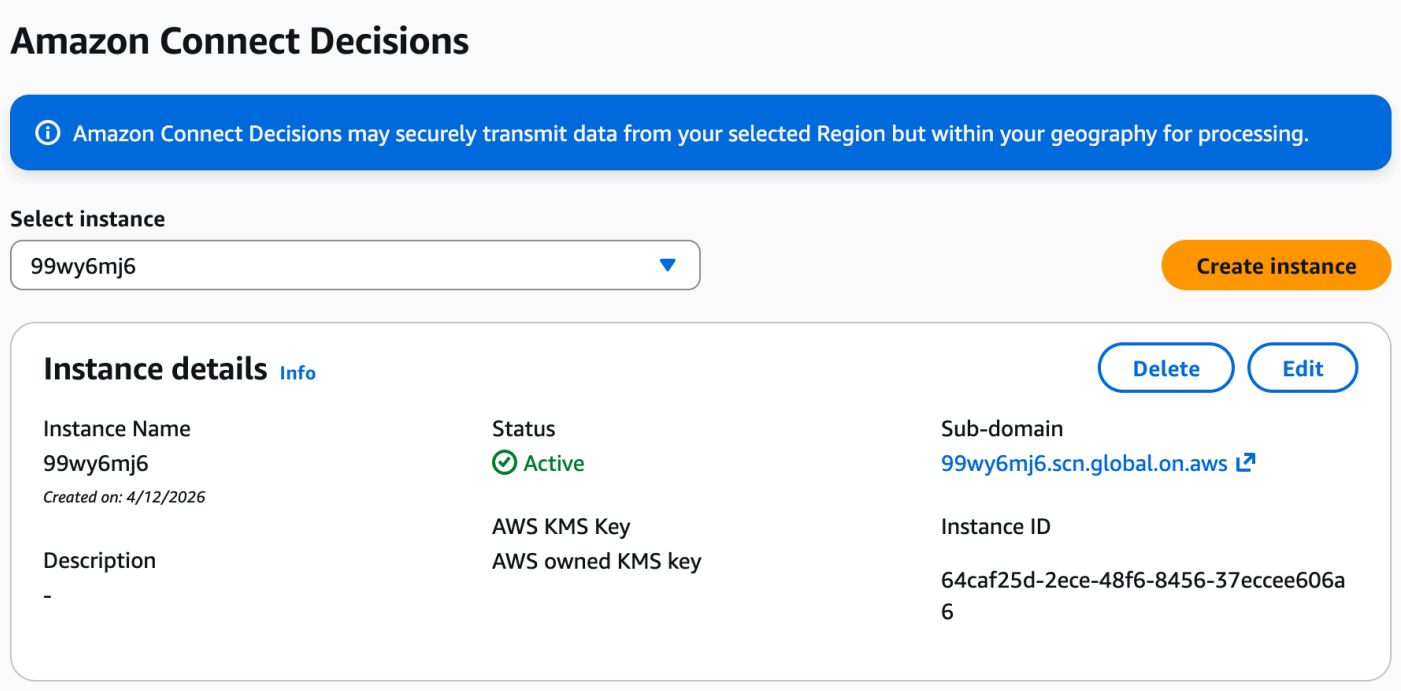
Eliminazione di un'istanza

Per eliminare un'istanza, segui questi passaggi.

> **Note**
>
> Quando elimini un'istanza, le informazioni dal bucket Amazon S3 non vengono eliminate automaticamente.

1. Apri la console Amazon Connect Decisions all'indirizzo https://console.aws.amazon.com/scn/home.

2. Nella dashboard della console Amazon Connect Decisions, dal menu a discesa, seleziona l'istanza che desideri eliminare.



3. Scegli Elimina.
4. Nella pagina Elimina istanza Amazon Connect Decisions, in Conferma, digita `delete` per confermare che desideri eliminare l'istanza.
5. Scegli Elimina. L'eliminazione dell'istanza inizia e, una volta eliminata, vedrai un messaggio di conferma.

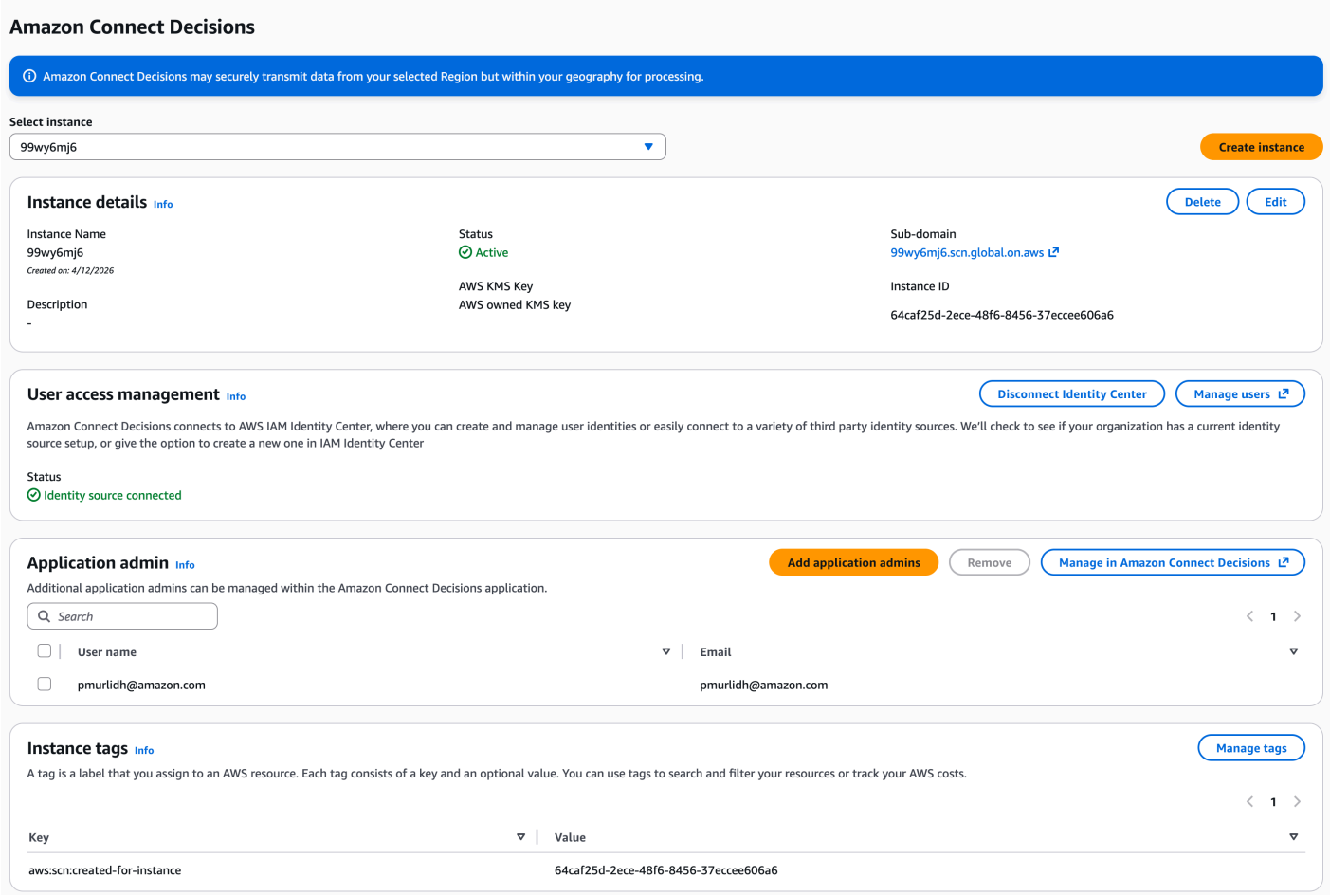
Scegli un amministratore dell'applicazione

In qualità di amministratore AWS della console, scegli un amministratore dell'applicazione Amazon Connect Decisions per gestire l'accesso all'applicazione Web Amazon Connect Decisions. L'amministratore dell'applicazione Amazon Connect Decisions può aggiungere o rimuovere ruoli di autorizzazione utente all'applicazione Web Amazon Connect Decisions.

Dopo aver creato l'istanza e aver collegato una fonte di identità, segui questi passaggi per scegliere un amministratore dell'applicazione Amazon Connect Decisions.

1. Apri la dashboard della console Amazon Connect Decisions.

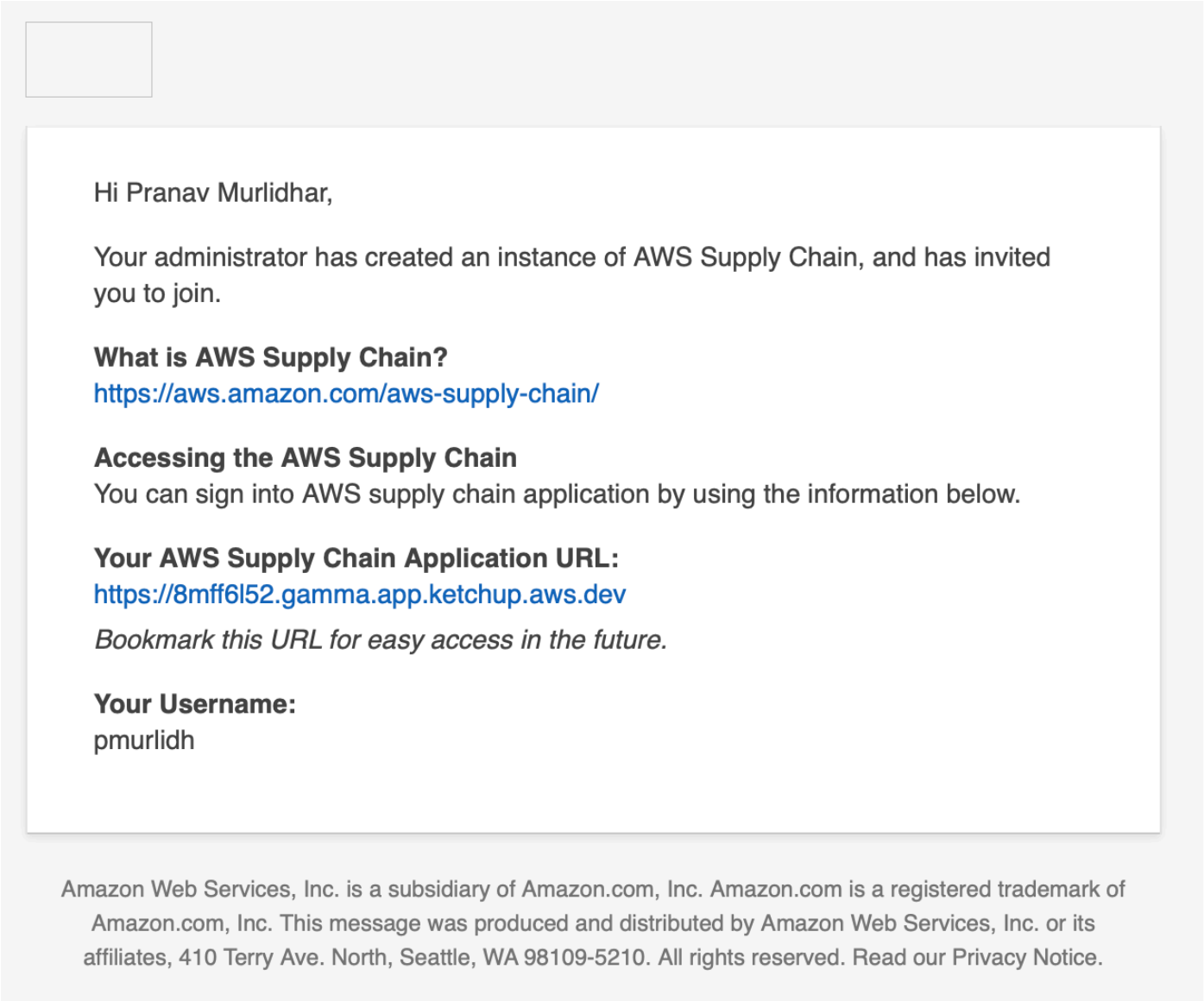
2. Vai a Seleziona amministratore dell'applicazione e seleziona un utente come amministratore dell'applicazione Amazon Connect Decisions. I risultati della ricerca mostrano solo gli utenti che corrispondono ai criteri di ricerca.



3. (Facoltativo) Scegli Vai a IAM Identity Center per aggiungere altri utenti. Per ulteriori informazioni sull'aggiunta di utenti, consulta Manage your identity source in AWS IAM Identity Center User Guide e per ulteriori informazioni sui ruoli di autorizzazione utente, consulta User permission roles.

> **Note**
>
> Puoi aggiungere un solo utente alla volta dalla console Amazon Connect Decisions. Non puoi aggiungere un gruppo come amministratore dell'applicazione in Amazon Connect Decisions.

4. Scegli Invia invito. Viene inviata un'e-mail all'amministratore dell'applicazione Web. Una volta ricevuta l'e-mail di invito, l'amministratore dell'applicazione Web potrà selezionare l'URL dell'applicazione e accedere ad Amazon Connect Decisions.



Nella webapp Amazon Connect Decisions, vedrai l'utente elencato nella sezione Amministratore dell'applicazione.

Accedere alla tua istanza

L'utilizzo della console è il modo più semplice per gestire le risorse e le configurazioni del servizio. La console offre un'interfaccia intuitiva basata sul Web in cui è possibile visualizzare, creare, modificare e monitorare le risorse.

Per accedere alla console Amazon Connect Decisions, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse Amazon Connect Decisions nel tuo AWS account. Se crei una policy basata sull'identità più

restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso o l' AWS API. Al contrario, è opportuno concedere l’accesso solo alle azioni che corrispondono all’operazione API che stanno cercando di eseguire.

In qualità di amministratore di Amazon Connect Decisions, dovresti aver ricevuto un invito via e-mail all'applicazione web Amazon Connect Decisions.

1. Puoi scegliere il link nell'e-mail o nella dashboard della console Amazon Connect Decisions, sotto Sub-domain, scegli URL web.
2. Viene visualizzata la pagina di accesso all'applicazione Web Amazon Connect Decisions.
3. Inserisci le credenziali utente di AWS IAM Identity Center e scegli Accedi.
4. Ogni utente che hai aggiunto riceve un messaggio e-mail con un link che rimanda ad Amazon Connect Decisions, oppure puoi scegliere Copia link e inviare il link agli utenti.

Dopo aver effettuato correttamente l'accesso, verrai indirizzato alla tua home page personalizzata. Fai riferimento a Comprendere la tua home page nella guida per l'utente per comprendere meglio la tua home page.

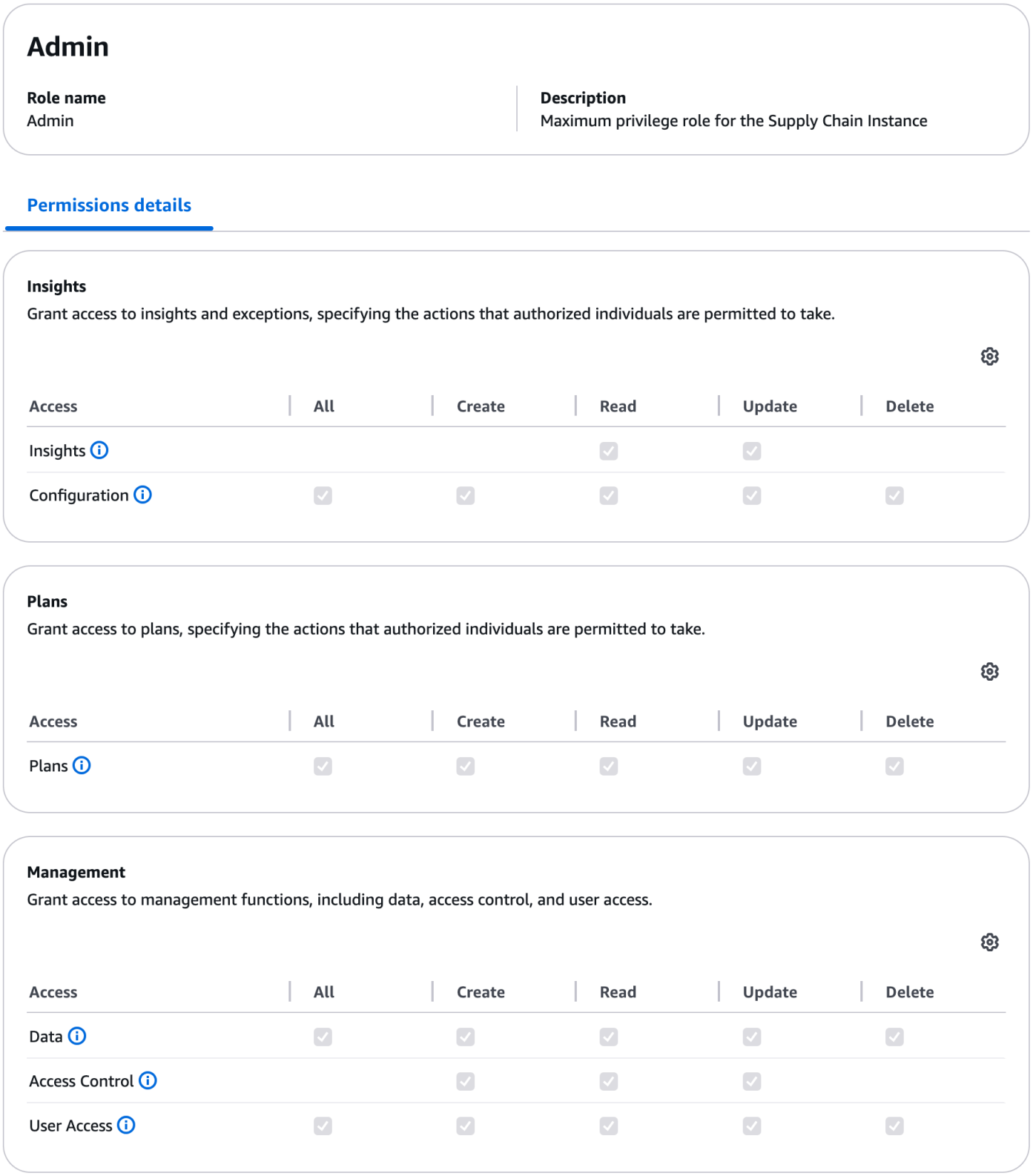
Controllo degli accessi

Amazon Connect Decisions offre una gestione degli accessi di livello aziendale che ti offre un controllo preciso su chi può accedere a quali dati ed eseguire quali azioni all'interno della tua istanza. Ciò garantisce che gli utenti vedano solo le informazioni pertinenti alle loro responsabilità, mantenendo al contempo gli standard di sicurezza e conformità richiesti dalla tua organizzazione.

Panoramica dei ruoli e delle autorizzazioni

In qualità di amministratore di Amazon Connect Decisions, puoi utilizzare i ruoli di autorizzazione utente predefiniti o creare ruoli di autorizzazione personalizzati. Amazon Connect Decisions ha i seguenti ruoli di autorizzazione utente predefiniti:

- Amministratore: accesso per creare, visualizzare e gestire tutti i dati e le autorizzazioni degli utenti.



Admin

Role name
Admin

Description
Maximum privilege role for the Supply Chain Instance

Permissions details

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

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

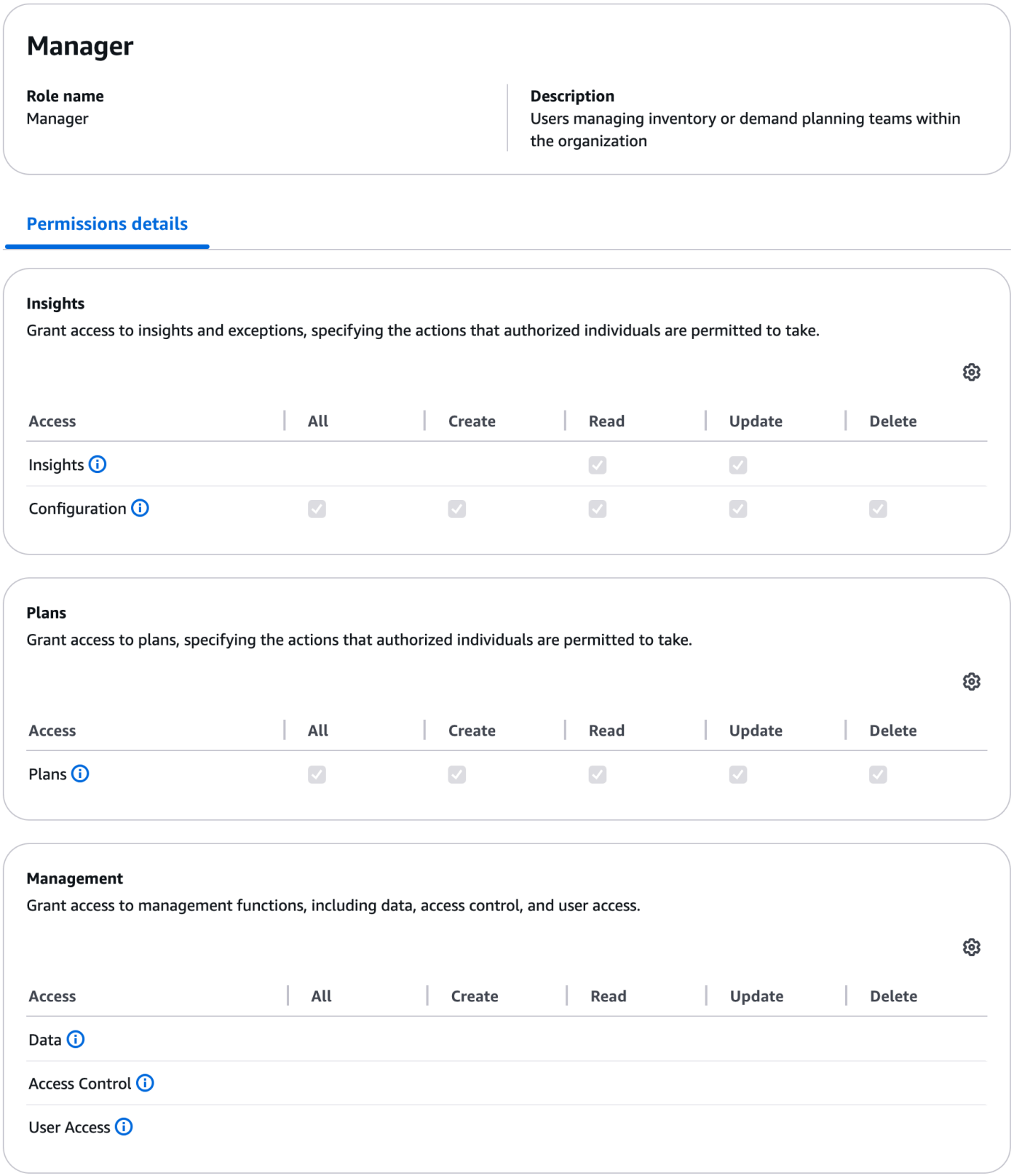
Plans
Grant access to plans, specifying the actions that authorized individuals are permitted to take.

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

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

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

- Manager: accesso per creare, visualizzare e gestire quanto segue.



- Planner: accesso per creare, visualizzare e gestire quanto segue.

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**
>
> In qualità di amministratore di Amazon Connect Decisions, prima di aggiungere utenti, tieni presente quanto segue:
>
> - Ogni ruolo di autorizzazione utente predefinito è definito con una serie di autorizzazioni. È possibile aggiungere utenti ai ruoli di autorizzazione utente predefiniti o creare ruoli di autorizzazione personalizzati.
> - A un utente può essere assegnato un solo ruolo di autorizzazione utente.
> - Non è possibile modificare o eliminare i ruoli di autorizzazione utente predefiniti.
> - Quando modifichi un ruolo di autorizzazione personalizzato che hai creato, le autorizzazioni per tutti gli utenti con il ruolo di autorizzazione personalizzato vengono aggiornate.
> - Quando elimini un ruolo di autorizzazione personalizzato che hai creato, tutti gli utenti con il ruolo di autorizzazione personalizzato perderanno l'accesso ad Amazon Connect Decisions.
> - L'aggiunta di gruppi non è supportata in Amazon Connect Decisions.

Gestione dei ruoli di autorizzazione degli utenti

Aggiunta di utenti

In qualità di amministratore di Amazon Connect Decisions, puoi aggiungere utenti per accedere all'applicazione web Amazon Connect Decisions. Gli utenti devono prima essere aggiunti a IAM Identity Center (iDC), quindi possono essere aggiunti ad Amazon Connect Decisions. Per ulteriori informazioni sull'aggiunta di utenti a iDC, consulta Assegnare l'accesso utente.

Una volta aggiunti gli utenti a iDC, segui questi passaggi per aggiungere un utente.

1. Scegli il cassetto Impostazioni sul lato sinistro
2. Seleziona Utenti. Seleziona Assegna utenti
3. Cerca per identificare l'utente. Puoi cercare utilizzando Nome visualizzato, Email, Nome, Cognome, Nome utente
4. Seleziona gli utenti che desideri aggiungere.
5. Assegna loro un ruolo. Visualizza la panoramica dei ruoli e delle autorizzazioni per ulteriori informazioni sui ruoli utente in Amazon Connect Decisions.

6. Seleziona Assegna. Conferma che le tue selezioni siano accurate.

Aggiornamento delle autorizzazioni degli utenti

Per aggiornare il ruolo di autorizzazione utente per gli attuali utenti di Amazon Connect Decisions, segui questi passaggi.

1. Scegli il cassetto Impostazioni sul lato sinistro
2. Seleziona Utenti. Seleziona Assegna utenti
3. Nell'elenco Utenti, seleziona l'utente per aprire la pagina dei dettagli utente.
4. Utilizza il menu a discesa dei ruoli per aggiornare le autorizzazioni del ruolo per l'utente.
5. Conferma di voler cambiare il ruolo facendo clic sul pulsante Cambia ruolo

Eliminazione di utenti

In qualità di amministratore di Amazon Connect Decisions, puoi eliminare utenti dall'applicazione Web Amazon Connect Decisions. Segui questi passaggi per eliminare gli utenti.

1. Scegli il cassetto Impostazioni sul lato sinistro
2. Seleziona Utenti. Seleziona Assegna utenti
3. Nell'elenco Utenti, seleziona l'utente per aprire la pagina dei dettagli utente.
4. Seleziona Elimina
5. Conferma di voler eliminare l'utente facendo clic sul pulsante Elimina

Configurazione dell'accesso a livello di attributo

Attribute-Based Access Control (ABAC) aggiunge un ulteriore livello di precisione limitando l'accesso in base al contesto aziendale. Utilizzando gli attributi del prodotto e del sito, puoi fare in modo che i responsabili della pianificazione vedano solo i dettagli relativi ai prodotti e alle sedi specifici che gestiscono, mentre i manager mantengano la visibilità su tutte le aree di responsabilità dei loro team.

Qualsiasi utente con il ruolo «Amministratore» può configurare l'accesso per prodotto e siti per altri utenti:

1. Vai alla pagina Utenti dalla barra di navigazione a sinistra.

2. Dall'elenco degli utenti in quell'istanza, seleziona l'utente che necessita della configurazione.
3. Per impostazione predefinita, nella sezione Accesso ai dati, gli utenti avranno l'opzione «Concedi l'accesso completo a tutti i prodotti e i siti». Quando questo interruttore è attivo, fornisce l'accesso a tutti i prodotti e i siti (come funzionava prima di questo lancio).
4. Disattiva «Concedi l'accesso completo a tutti i prodotti e i siti» e la sezione di configurazione dei prodotti e dei siti diventerà visibile. Nessun prodotto o sito verrà assegnato al primo accesso.
5. Fai clic sul Add/Remove pulsante per i prodotti o i siti in base a ciò che devi configurare. Usa la ricerca per trovare e selezionare gli elementi necessari per quell'utente.
6. A più utenti può essere assegnato lo stesso prodotto o sito. Un utente può avere un massimo di 1.000 combinazioni prodotto-sito.
7. I prodotti o i siti configurati in precedenza possono essere rimossi utilizzando la stessa interfaccia.
8. Rivedi e conferma l'elenco completo delle aggiunte e delle rimozioni nella pagina finale della procedura guidata per completare la configurazione di accesso.

Una volta configurato l'accesso al prodotto e al sito, l'accesso per quell'utente verrà limitato in base alle seguenti assegnazioni:

- Tutti gli utenti possono visualizzare qualsiasi pagina di eccezione o raccomandazione, indipendentemente dal fatto che sia stata generata per un prodotto o un sito incluso nel controllo degli accessi.
- Per eseguire azioni di modifica (ad esempio eliminare un'eccezione o modificare lo stato da In corso a Completo), gli utenti devono avere il prodotto O il sito appropriato configurato nel controllo di accesso.
- Gli utenti con controllo di accesso configurato possono anche utilizzare User Assignment e Access View Toggle.

Assegnazione utente

L'assegnazione degli utenti è una funzionalità che semplifica il bilanciamento delle informazioni tra più utenti. Utilizzando User Assignment, i clienti possono assegnare informazioni specifiche agli utenti per riflettere meglio il modo in cui queste attività vengono condivise nella vita reale. Funziona nel seguente modo:

- Ogni volta che viene creata un'eccezione, il sistema verifica il prodotto e il sito per i quali è stata creata l'eccezione confrontandoli con tutti gli utenti che hanno lo stesso prodotto O sito configurato per il controllo degli accessi
- Se il sistema trova un utente corrispondente, il campo Assegnato a per quell'eccezione viene aggiornato con il nome utente. Nei casi in cui più di un utente abbia prodotti o siti che corrispondono all'eccezione, questa viene assegnata in modo casuale a uno di essi
- È possibile assegnare un solo utente a ciascuna eccezione, ma un'eccezione può essere riassegnata a un altro utente, se necessario. Può essere riassegnata solo a un utente con accesso al prodotto o al sito
- Auto-assignment for insights si verifica quando l'eccezione viene creata per la prima volta. Gli approfondimenti creati in precedenza non verranno riassegnati automaticamente. Inoltre, se un utente viene eliminato o il suo controllo di accesso viene aggiornato, l'assegnazione dell'utente non viene aggiornata automaticamente
- Nella pagina di elenco degli approfondimenti, un utente può filtrare in base alla dimensione Assegnato a per identificare facilmente tutti gli approfondimenti a lui assegnati. Possono anche utilizzare lo stesso filtro per visualizzare informazioni non assegnate. L'assegnazione degli utenti è attualmente disponibile solo per gli approfondimenti

Onboarding dei dati

Connessione dei dati

Prerequisiti

Prima di iniziare l'onboarding dei dati, assicurati di avere:

- Istanza Amazon Connect Decisions
  - L'istanza dovrebbe essere già stata creata con un bucket S3 associato
- Dati preparati
  - Collabora con la tua controparte Amazon Customer Success per determinare di quali dati hai bisogno in base a come intendi utilizzare Amazon Connect Decisions. I requisiti relativi ai dati di base includono:
    - Sales/Order Cronologia: oltre 12 mesi di registrazioni delle transazioni
    - Dettagli del prodotto: catalogo completo dei prodotti con specifiche
    - Site/Location Informazioni: magazzini, centri di distribuzione, punti vendita
    - Disponibilità attuale dell'inventario: On-hand inventario in ogni sede
  - Tutti i dati di origine in formato CSV con codifica UTF-8

Primo accesso: questionario di onboarding

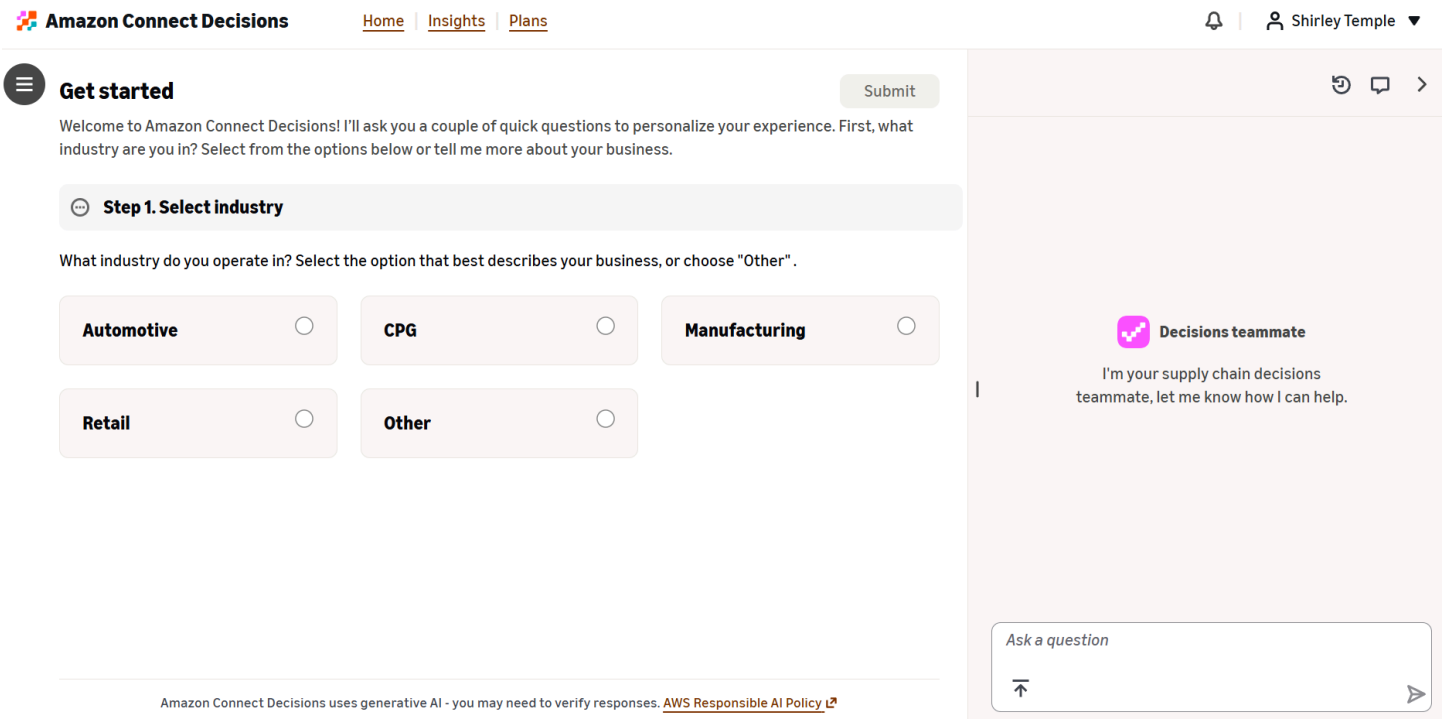
Quando accedi ad Amazon Connect Decisions per la prima volta, il sistema presenta un questionario di onboarding guidato. Questa procedura guidata di personalizzazione aiuta i membri del team di Decisions a contestualizzare le funzionalità più rilevanti per la tua azienda. Il questionario raccoglie informazioni sul settore, sulle principali sfide aziendali e sull'approccio preferito per la pianificazione. Le vostre risposte contribuiranno a ottimizzare le fasi di onboarding in base alla vostra selezione, permettendo al sistema di semplificare i flussi di lavoro di configurazione successivi e di individuare i percorsi di configurazione più pertinenti per la vostra azienda. È necessario completare tutti i passaggi prima di accedere all'applicazione completa. Decisions Teammate è disponibile durante tutto il processo di onboarding tramite la barra laterale destra per rispondere alle domande in tempo reale.

> **Note**
>
> Questa è una selezione una tantum solo al primo accesso. Le vostre risposte forniscono un contesto aggiuntivo per ottimizzare le fasi successive di onboarding e aiutano gli agenti a comprendere il vostro ambiente aziendale. Tutte le funzionalità rimangono completamente accessibili indipendentemente dalle selezioni effettuate.

Fase 1: Seleziona il settore

Cosa vedi: un messaggio di benvenuto e una serie di pulsanti radio che ti invitano a selezionare il settore che meglio descrive la tua attività.

1. Seleziona il pulsante radio che meglio rappresenta la tua attività.
2. Se nessuna delle opzioni predefinite si applica, seleziona Altro.



Fase 2: Definite la sfida più grande

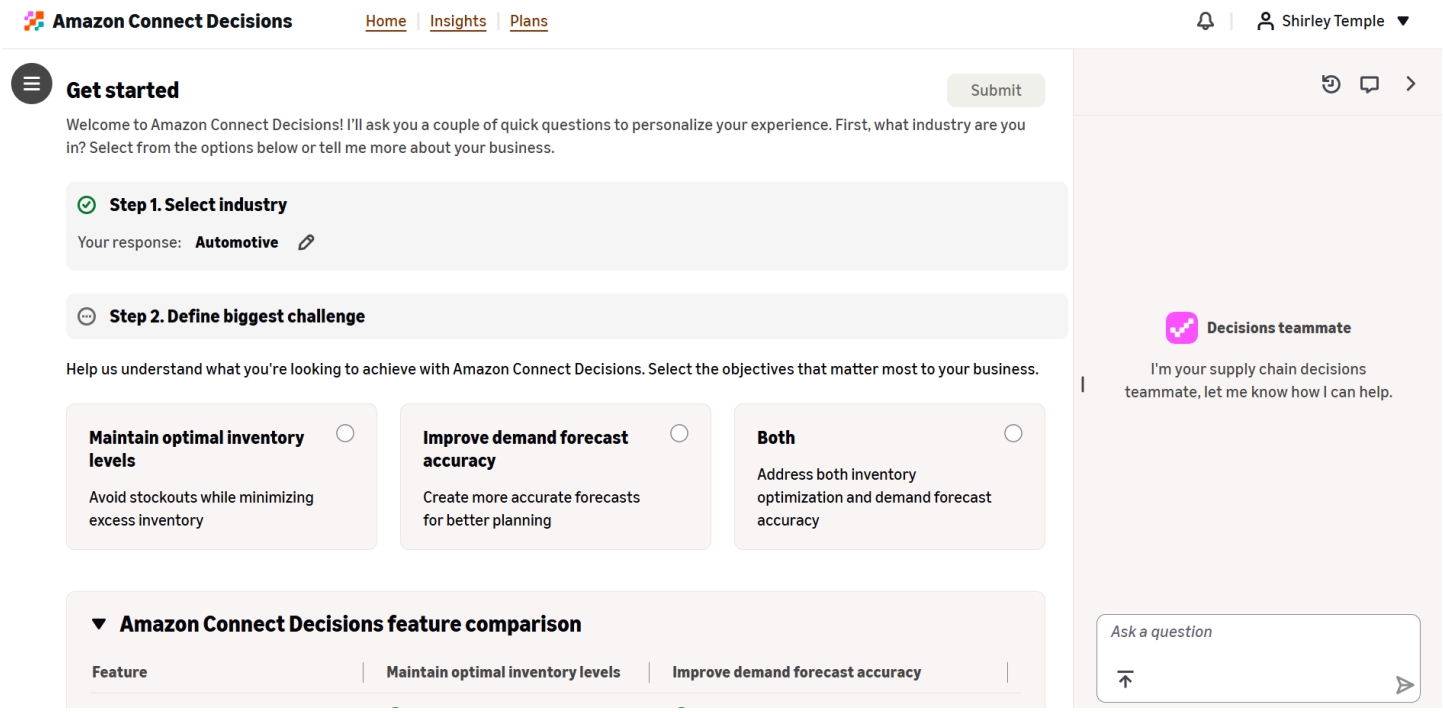
Cosa vedi: la tua risposta alla Fase 1 viene visualizzata con un'opzione di modifica. Di seguito, ti viene chiesto di identificare la sfida aziendale principale tra tre opzioni. Viene visualizzata una

tabella di confronto delle funzionalità per aiutarti a capire quali funzionalità sono associate a ciascuna selezione.

1. Esamina le opzioni. Consulta la tabella seguente per le opzioni disponibili e il loro significato.
2. Seleziona il pulsante radio che rappresenta la sfida più urgente.
3. Facoltativamente, consulta la tabella di confronto delle funzionalità sotto le opzioni per capire cosa è incluso in ciascuna selezione.

Opzioni relative alle sfide aziendali

Opzione	Description	Funzionalità principali abilitate
Mantieni livelli di inventario ottimali	Scegli questa opzione se la tua sfida principale è evitare l'esaurimento delle scorte riducendo al minimo l'inventa rio in eccesso.	Ottimizzazione dell'inventario; prevenzione delle scorte; riduzione delle scorte in eccesso; pianificazione delle forniture; monitoraggio dei tempi di consegna dei fornitori
Migliora l'accuratezza delle previsioni della domanda	Scegli questa opzione se la tua sfida principale è creare previsioni più accurate per decisioni di pianificazione migliori.	Previsione di base; pianifica zione del consenso; monitorag gio dell'accuratezza delle previsioni
Entrambi	Scegli questa opzione se devi occuparti contempor aneamente dell'ottimizzazion e dell'inventario e dell'accu ratezza delle previsioni della domanda.	Tutte le funzionalità specifich e dell'offerta e della domanda sono abilitate



Fase 3: Scegli il tuo approccio alla pianificazione dell'inventario

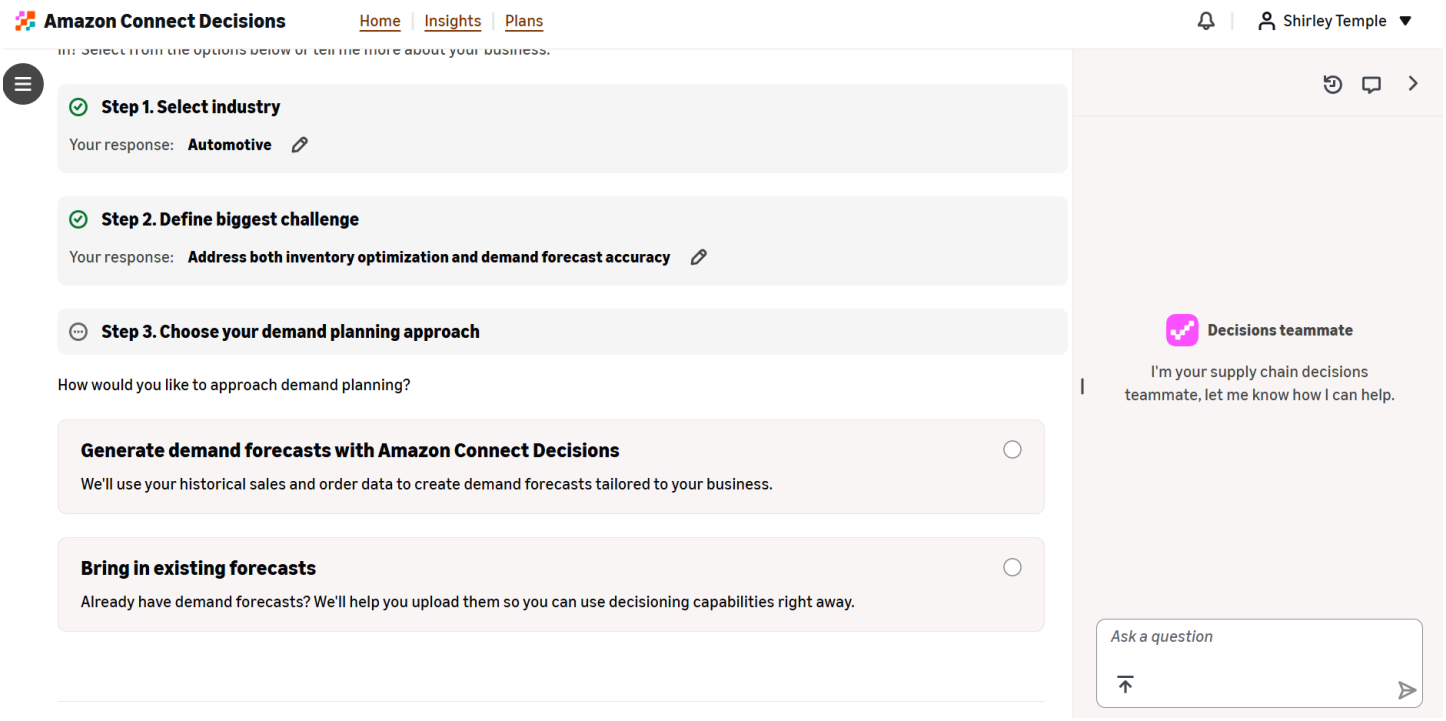
Cosa vedi: i passaggi 1 e 2 vengono visualizzati come completati (indicati da segni di spunta verdi) con le risposte visualizzate e modificabili. La fase 3 chiede come intendi affrontare la pianificazione dell'inventario, con due opzioni evidenziate.

1. Esamina le due opzioni di pianificazione dell'inventario. Consulta la tabella seguente per le opzioni disponibili e il loro significato.
2. Seleziona il pulsante radio per l'approccio che corrisponde al tuo stato attuale.

Opzioni di approccio alla pianificazione dell'inventario

Opzione	Description	Ideale per
Genera piani di inventario con Amazon Connect Decisions	Il sistema utilizza i dati storici delle vendite e dell'inventario per creare piani su misura per la tua attività.	Organizzazioni che non dispongono di una soluzione di pianificazione esistente o che desiderano sfruttare i piani generati dall'intelligenza artificiale a partire dai propri dati storici.

Opzione	Description	Ideale per
Inserisci le proiezioni o i piani di inventario esistenti	Carica i piani o le proiezioni di inventario esistenti in modo da poter utilizzare immediatamente le funzionalità decisionali. Il sistema ti aiuterà a caricare e mappare i tuoi dati.	Organizzazioni che hanno già stabilito processi di pianificazione e desiderano sfruttare le funzionalità di monitoraggio, generazione di informazioni e raccomandazioni senza modificare la fonte del piano.



Fase 4: Scegliete il vostro approccio alla pianificazione della domanda

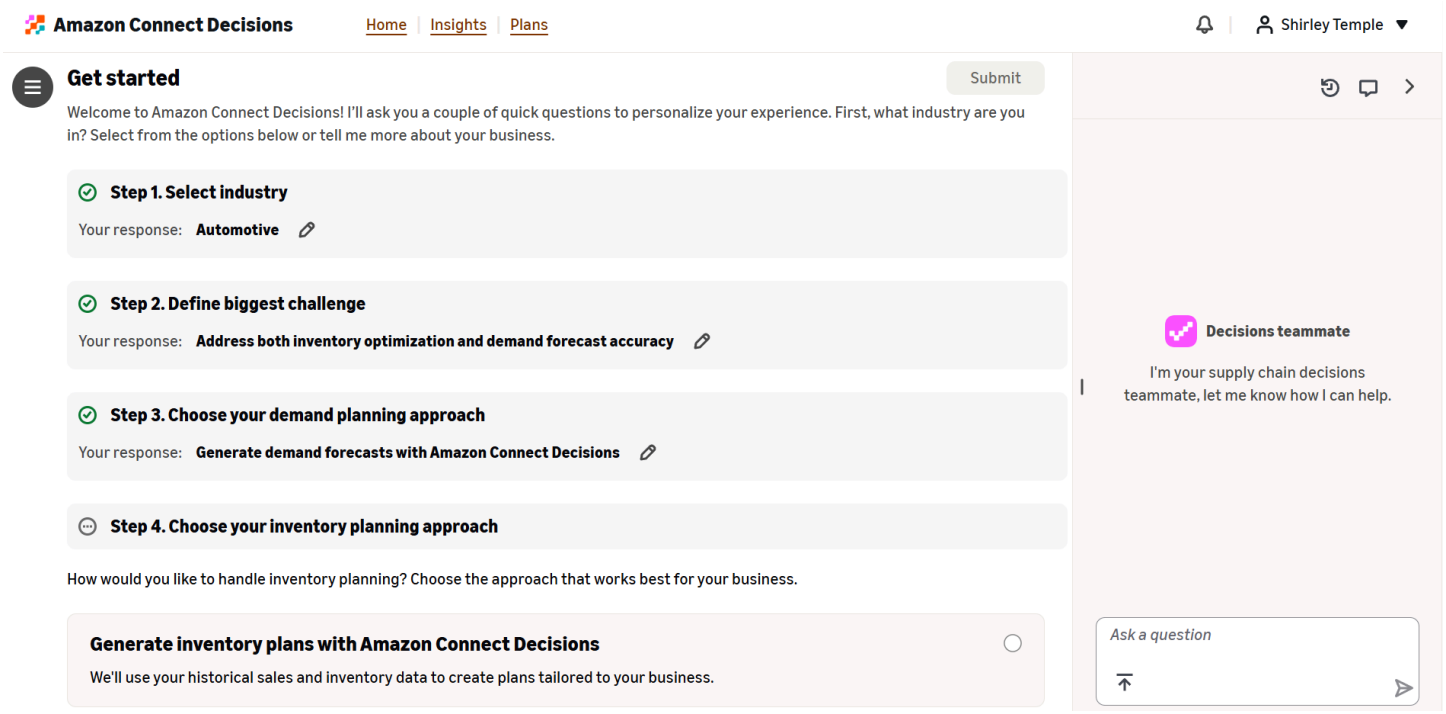
Cosa vedi: i passaggi da 1 a 3 vengono visualizzati come completati. La fase 4 chiede come intendi affrontare la pianificazione della domanda.

1. Esamina le due opzioni di pianificazione della domanda. Vedi la tabella seguente per le opzioni disponibili e il loro significato.
2. Seleziona il pulsante di opzione per l'approccio che corrisponde al tuo stato attuale.
3. Fai clic su Invia per finalizzare il questionario di onboarding.

Ricorda: questo questionario di onboarding è un input contestuale una tantum che aiuta a ottimizzare le fasi di onboarding in base alle tue selezioni. Non altera il comportamento degli agenti né limita l'accesso a nessuna funzionalità. Tutte le funzionalità di Amazon Connect Decisions rimangono completamente disponibili per te.

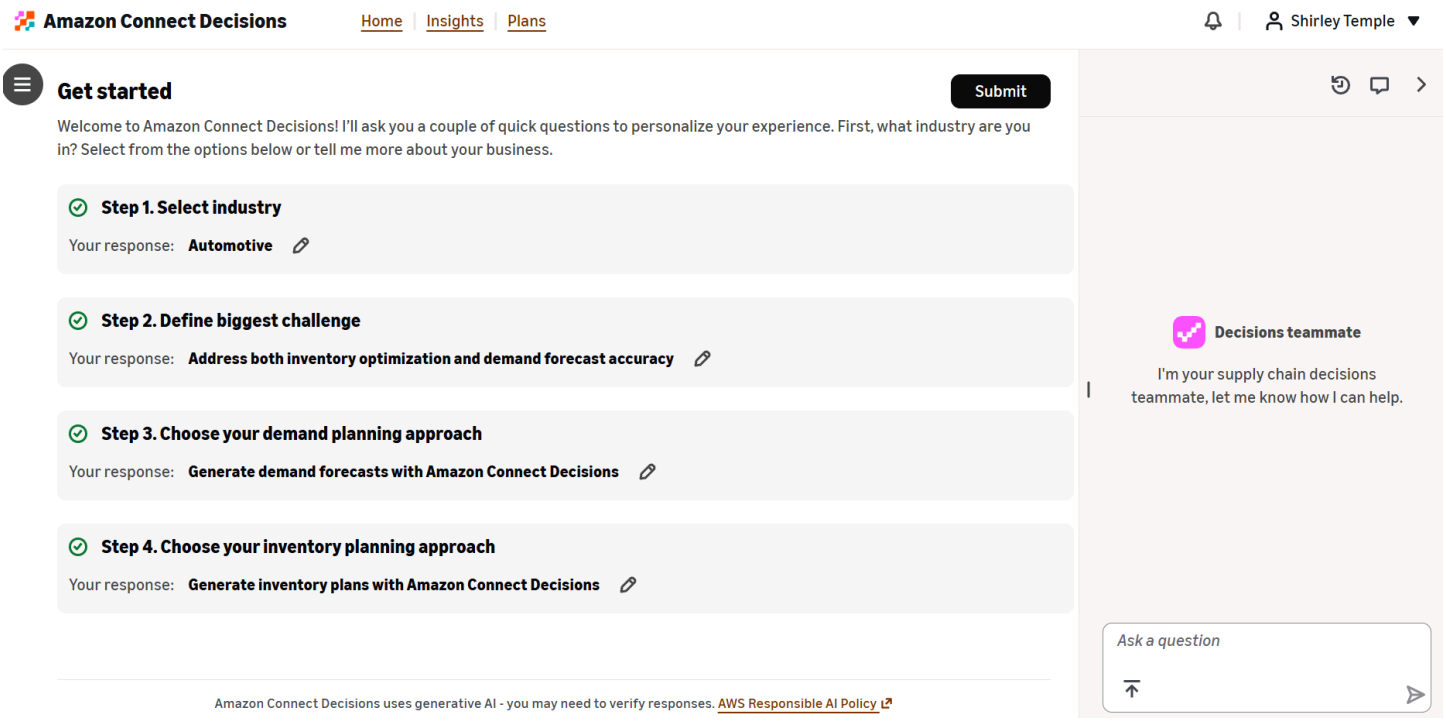
Opzioni di approccio alla pianificazione della domanda

Opzione	Description	Ideale per
Genera previsioni della domanda con Amazon Connect Decisions	Il sistema utilizza i dati storici delle vendite e degli ordini per creare previsioni della domanda su misura per la tua attività. Amazon Connect Decisions orchestra oltre 18 strumenti di previsione per produrre previsioni di base accurate.	Organizzazioni che non dispongono di una soluzione di previsione esistente o che desiderano sostituire il loro approccio attuale con previsioni generate dall'inte lligenza artificiale.
Inserisci le previsioni esistenti	Carica le previsioni della domanda esistenti in modo da poter utilizzare immediata mente le funzionalità decisiona li. Il sistema ti aiuterà a mappare e importare i dati di previsione.	Organizzazioni che hanno già stabilito processi di prevision e e desiderano sfruttare le funzionalità di monitoraggio, generazione di informazioni e raccomandazioni senza modificare la fonte delle previsioni.



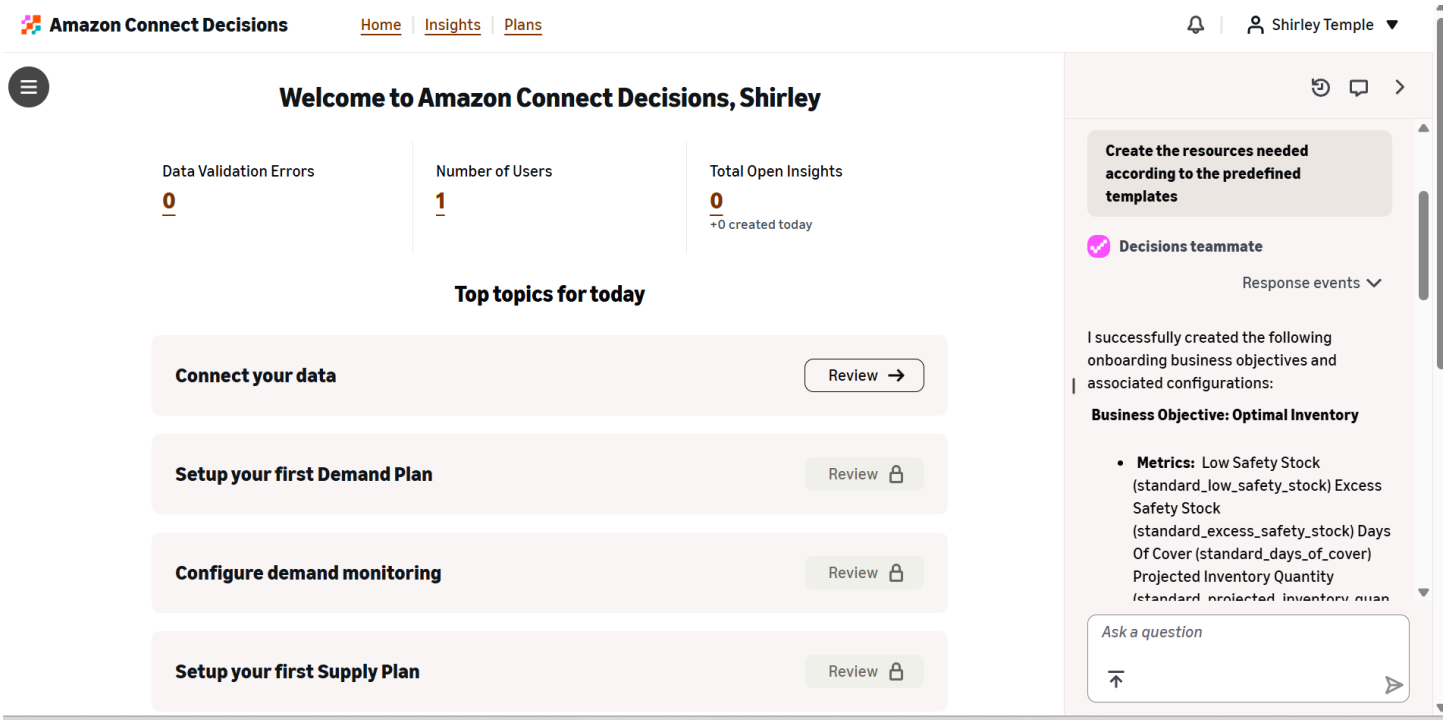
Dopo aver completato il questionario

Fai clic su Invia dopo aver completato tutti e quattro i passaggi:



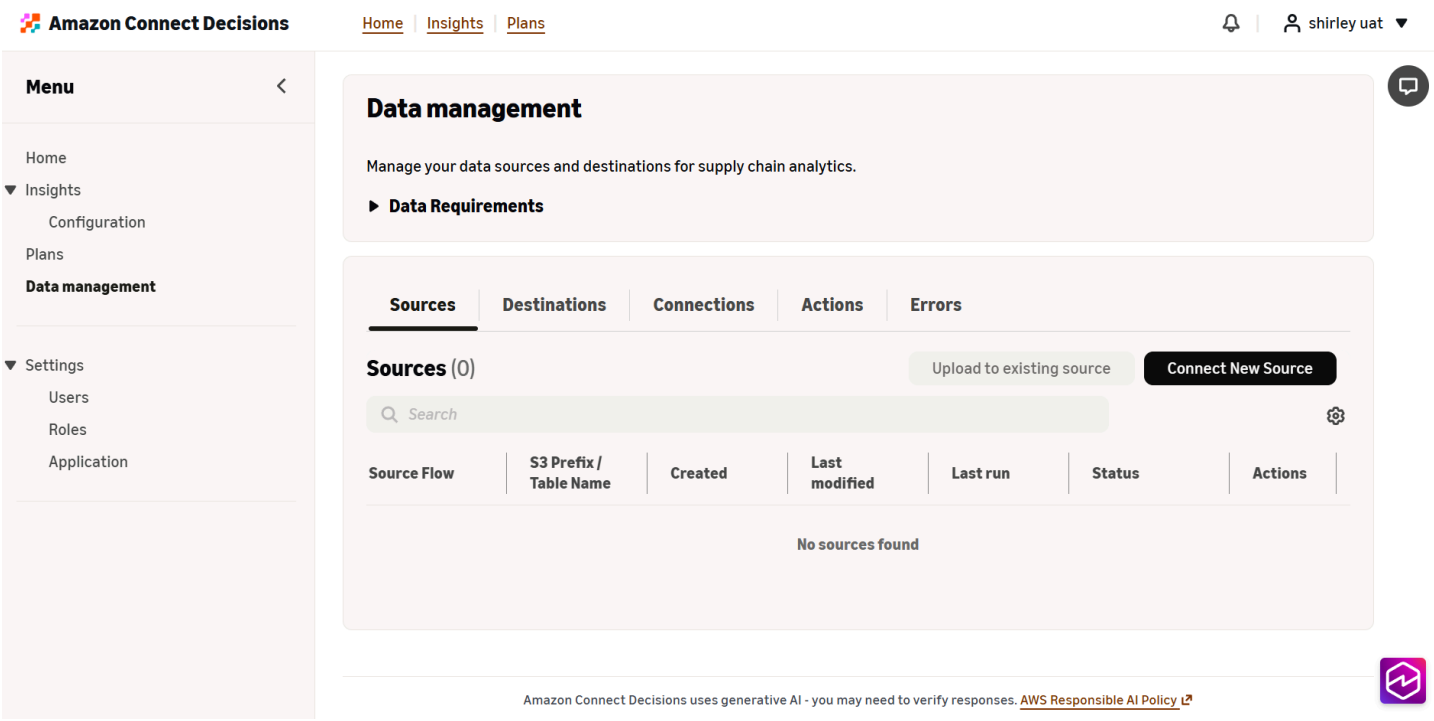
- Verrai reindirizzato alla home page con dashboard e schede tematiche progettate per guidarti attraverso le fasi di onboarding rimanenti.

- Il sistema creerà automaticamente metriche e regole all'interno dell'applicazione in base alle selezioni effettuate. Queste vengono create nello stato Bozza e non sono immediatamente attive.
- Puoi rivedere le metriche e le regole create automaticamente, quindi attivarle se soddisfano le tue esigenze o creare metriche e regole personalizzate su misura per i tuoi requisiti aziendali specifici.



Creazione del primo Source Flow

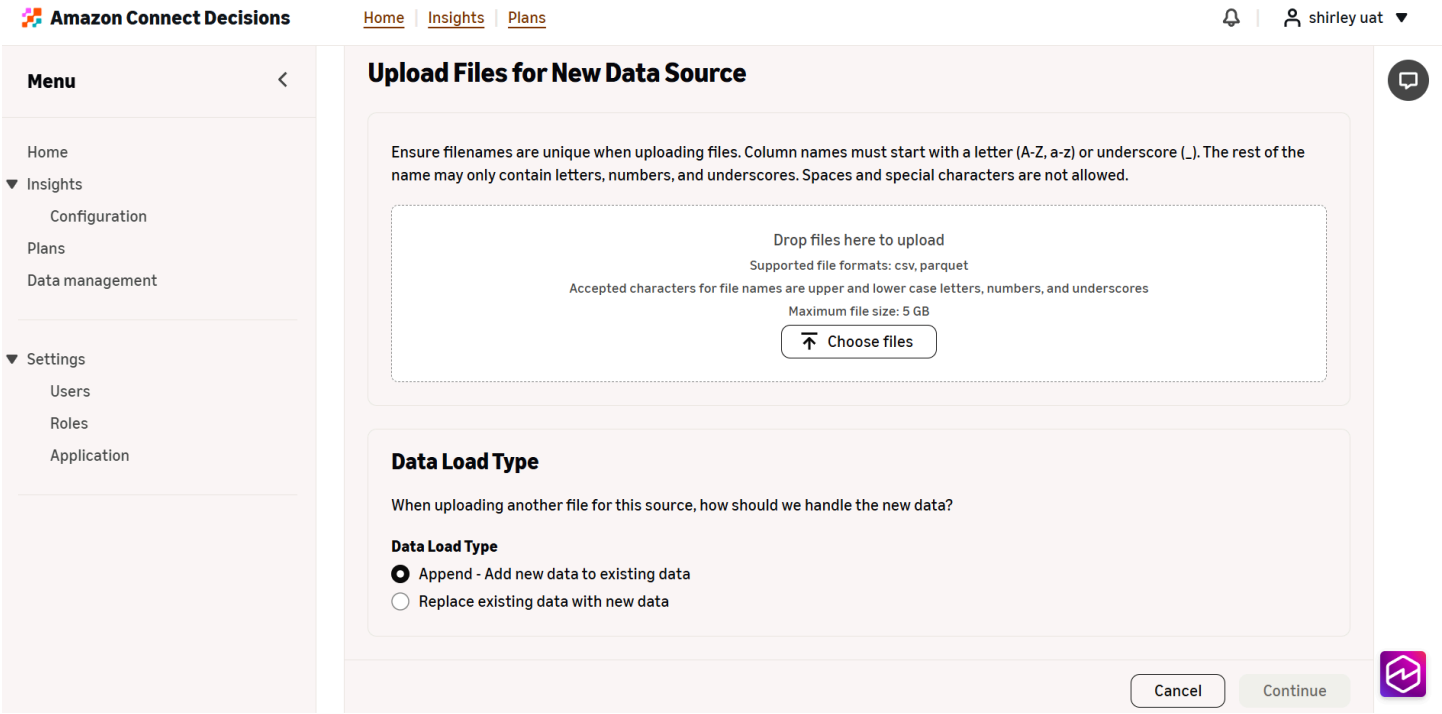
Per iniziare l'onboarding dei tuoi dati, fai clic su Rivedi nella scheda tematica Connetti i tuoi dati o vai alla scheda Gestione dati nel «Menu Hamburger» in Amazon Connect Decisions. Qui puoi vedere tutti i flussi di origine esistenti. Se non ne hai ancora configurato uno, fai clic su «Connect New Source» per iniziare.



Carica i tuoi dati di origine

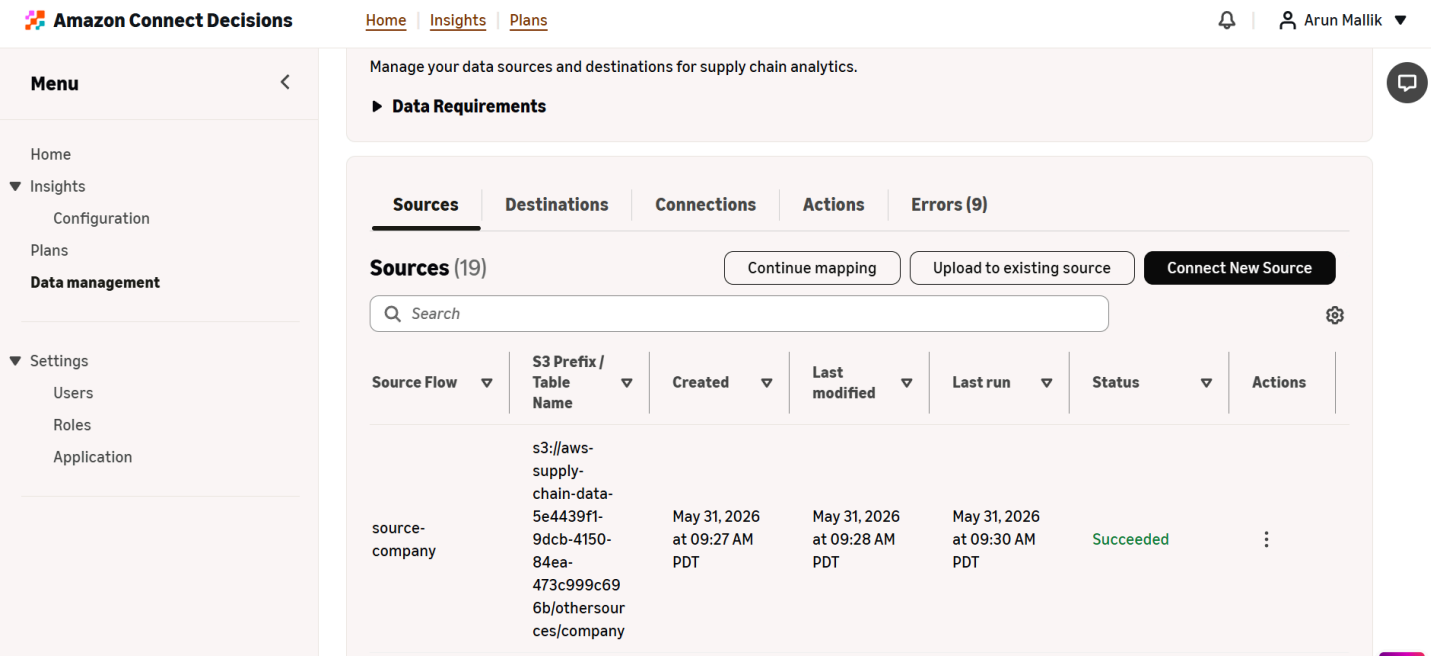
Carica i tuoi file CSV contenenti i dati di origine in base alle tabelle CDM richieste per il tuo caso d'uso. Puoi scegliere come gestire gli aggiornamenti dei dati:

- Aggiungi: aggiungi nuovi dati ai dati esistenti
- Sostituisci: sostituisci i dati esistenti con nuovi dati



Quando carichi file, Amazon Connect Decisions crea automaticamente una struttura di cartelle in S3 per quei dati, tra cui:

- Una cartella principale che prende il nome dal sistema di origine selezionato
- Una sottocartella denominata in base al nome della tabella di origine selezionata
- Tutti i file contenuti in una sottocartella vengono salvati nella stessa tabella di origine
- Questa struttura di file viene utilizzata anche per creare il percorso della cartella Amazon S3

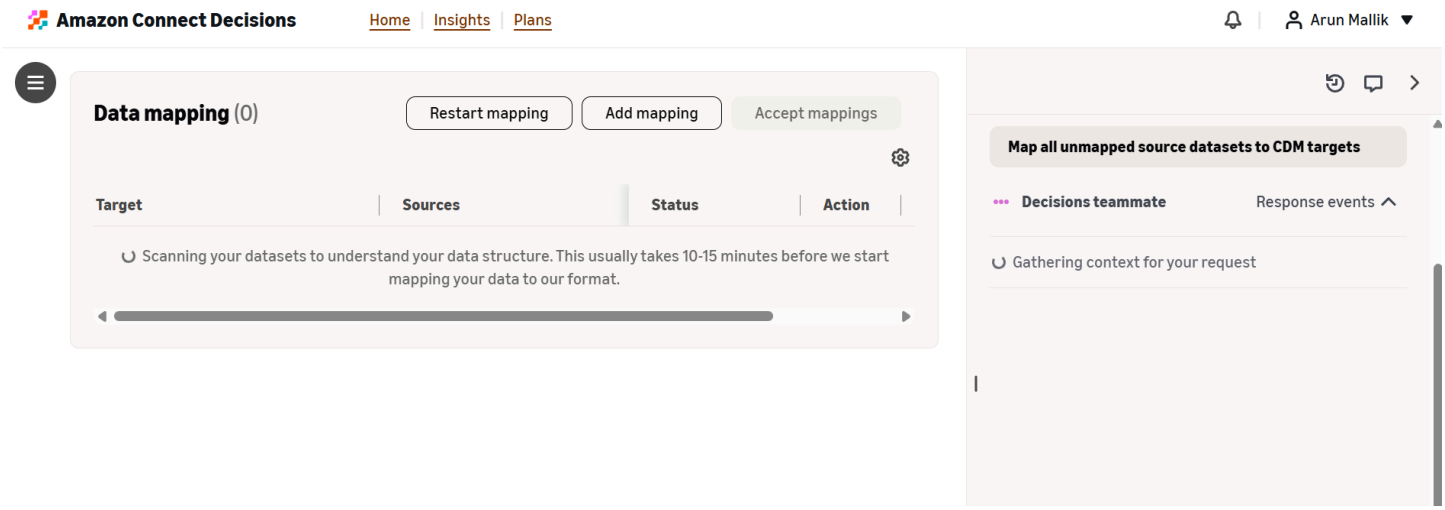


Source-to-CDM Mappatura della destinazione

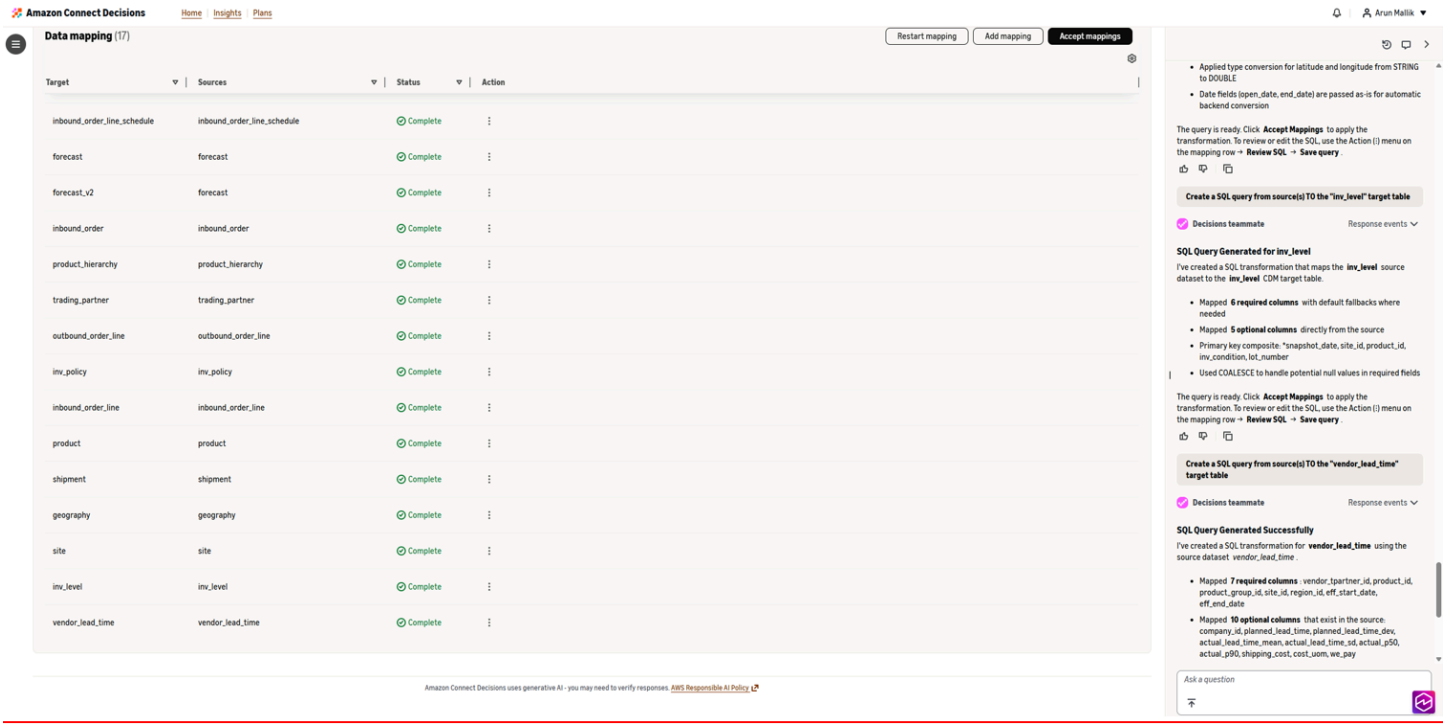
Una volta caricati i file, Amazon Connect Decisions inizia ad analizzare i dati e li mappa automaticamente su una o più tabelle di destinazione CDM di Amazon Connect Decisions.

Cosa aspettarsi

- Questo passaggio può richiedere tra 10-15 minuti a seconda della quantità di dati caricati
- Il Data Agent lavora in background per identificare i migliori set di dati di destinazione CDM per i dati di origine.
- Se si esce da questa pagina, le mappature automatiche non funzioneranno. Durante l'attesa, tieni aperta la scheda Amazon Connect Decisions and Data Management per garantire il completamento della mappatura automatica.

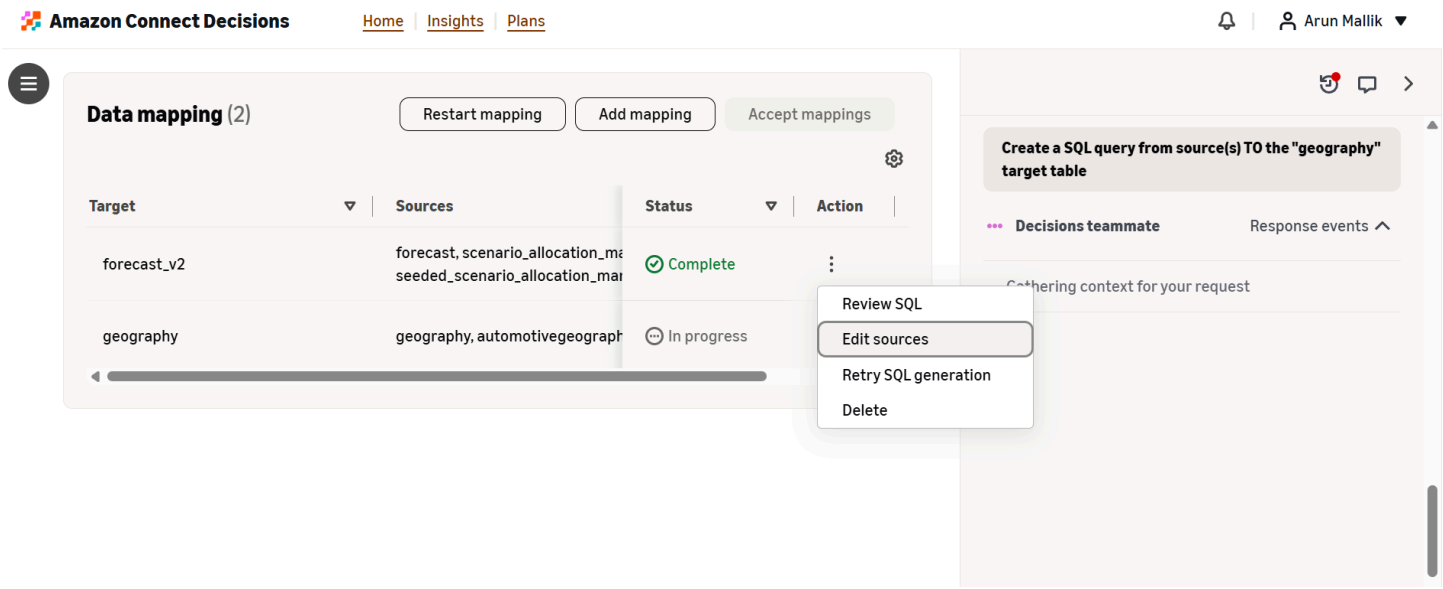


Una volta completata, Data Agent fornisce una spiegazione logica sulle mappature da origine a destinazione basate su dati sovrapposti, che puoi esaminare e porre domande all'agente su qualsiasi risultato di mappatura.



Per rivedere e modificare le mappature delle sorgenti, puoi:

- Interagisci direttamente con il Data Agent utilizzando il linguaggio naturale per aggiornare le mappature sorgente-destinazione.
- Fai clic sulle azioni e seleziona «Modifica sorgenti».



Modifica delle mappature

Da qui, puoi:

- Se necessario, aggiornare manualmente la mappatura di origine e destinazione
- Poni domande utilizzando il Data Agent sul lato destro dello schermo per confermare le mappature
- Consulta le guide utente per saperne di più su set di dati specifici

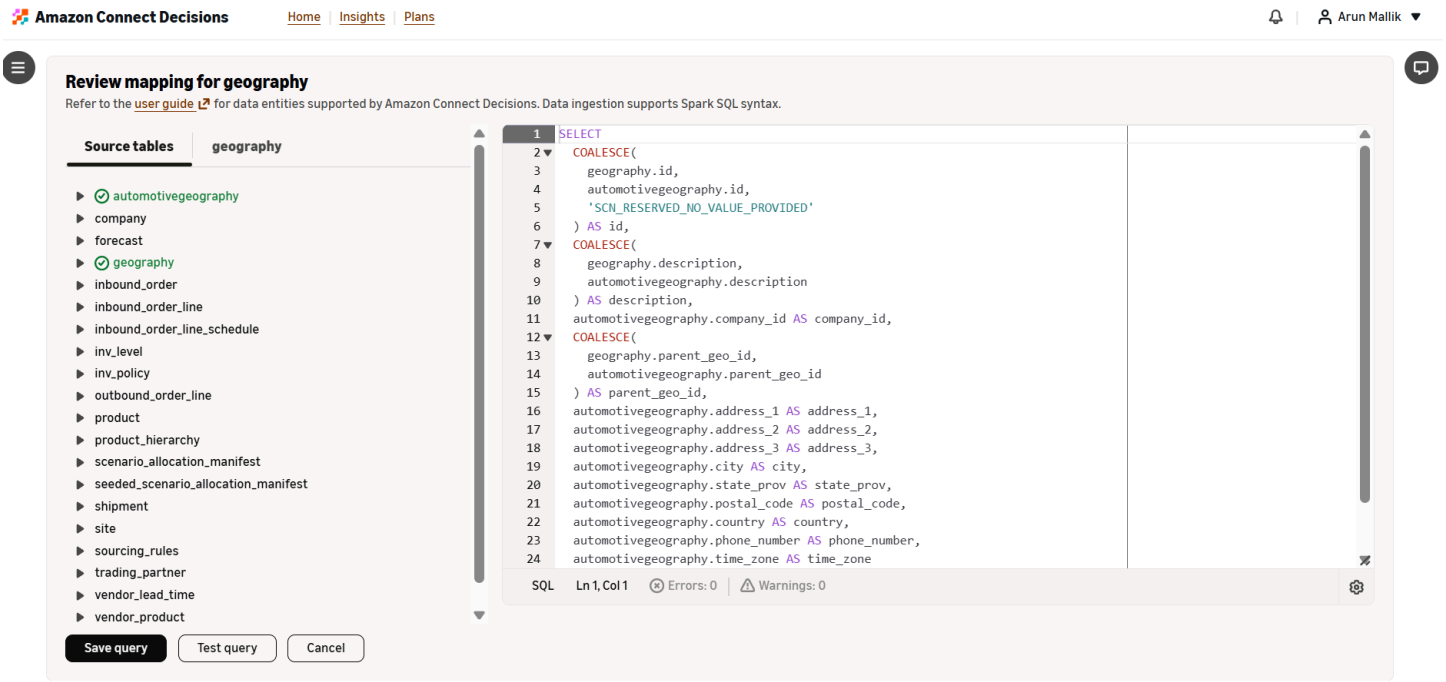
Column/Data Mappatura

Una volta completata la mappatura da origine a destinazione, Amazon Connect Decisions creerà automaticamente query di trasformazione SQL dal set di dati di origine alla destinazione CDM. Una volta completata una mappatura, riceverai una notifica dal Data Agent con i dettagli del risultato della mappatura.

Da qui, dovresti esaminare l'SQL generato per le mappature selezionando «Review SQL» dal menu Azione.

Esaminando la mappatura (SQL), vedrai:

- Colonne del set di dati di origine che hai aggiunto
- Colonne di riferimento della tabella CDM di destinazione
- L'SQL di trasformazione che le collega
- Motivazione della mappatura fornita dal Data Agent



Modifica delle mappature

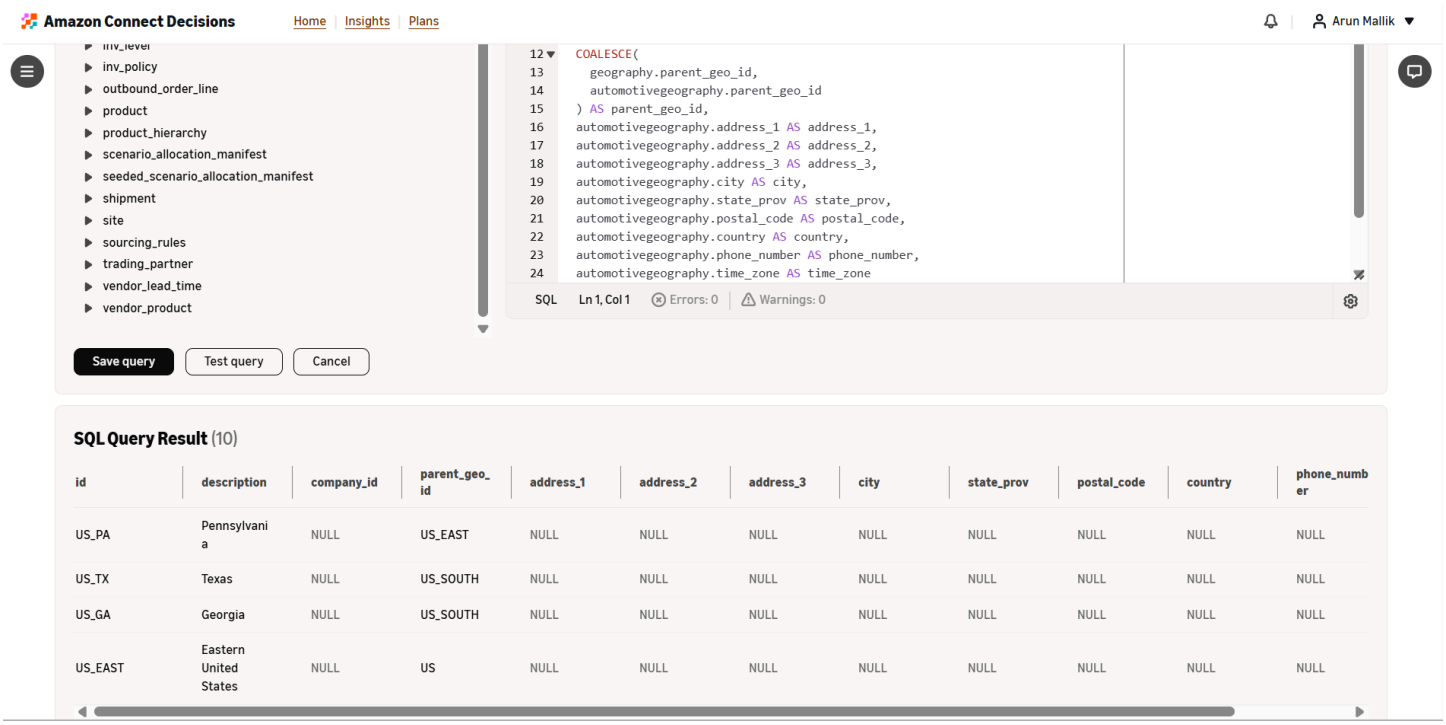
Sono disponibili due opzioni per modificare qualsiasi mappatura:

- Lavora con Data Agent: utilizza il linguaggio naturale per porre domande, gestire e aggiornare le mappature
- Modifica SQL direttamente: se hai familiarità con SQL, puoi modificare direttamente la query

Verifica delle modifiche

Mentre modifichi la query di mappatura, continua a testarla utilizzando la funzionalità «Test Query», che ti fornirà un'anteprima scorrevole di come un esempio di come i tuoi dati vengono trasformati in CDM di destinazione. Utilizzatela per assicurarvi che la trasformazione venga eseguita correttamente e per convalidare eventuali aggiornamenti appropriati dal CDM dall'origine alla destinazione.

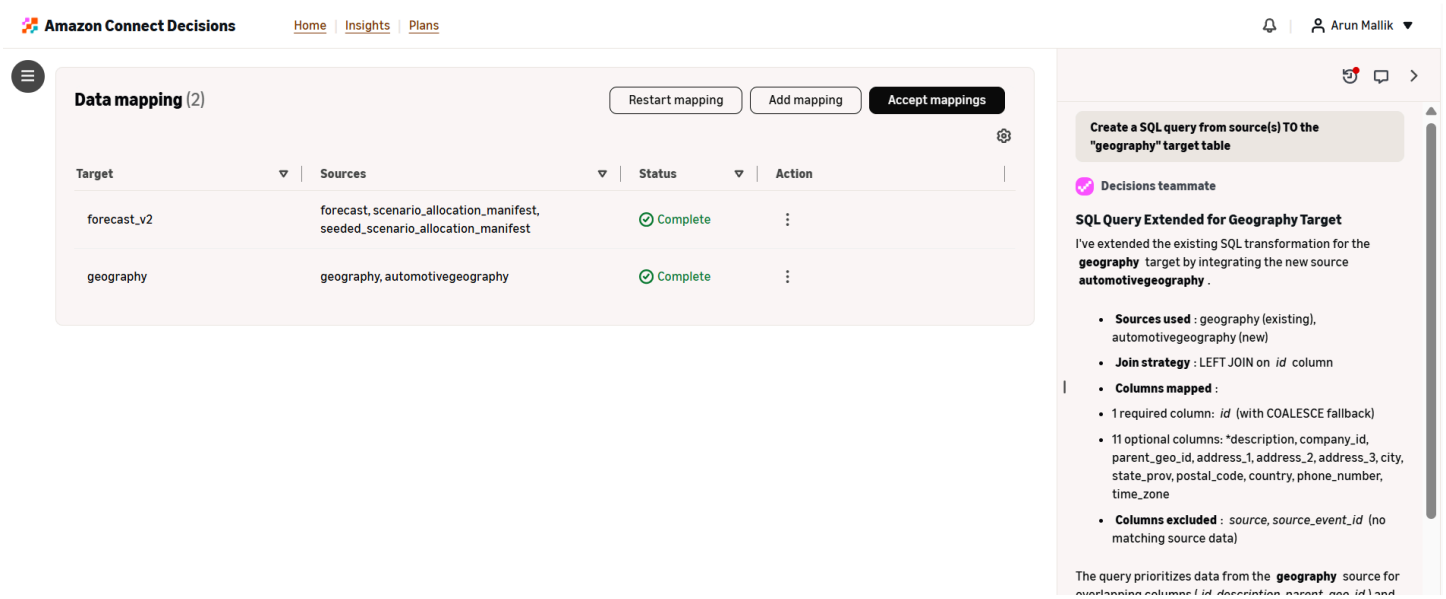
Quando sei soddisfatto dell'output della mappatura, seleziona "Salva interrogazione" per salvare la query di trasformazione per quella coppia origine-destinazione.



Rivedi e accetta le mappature

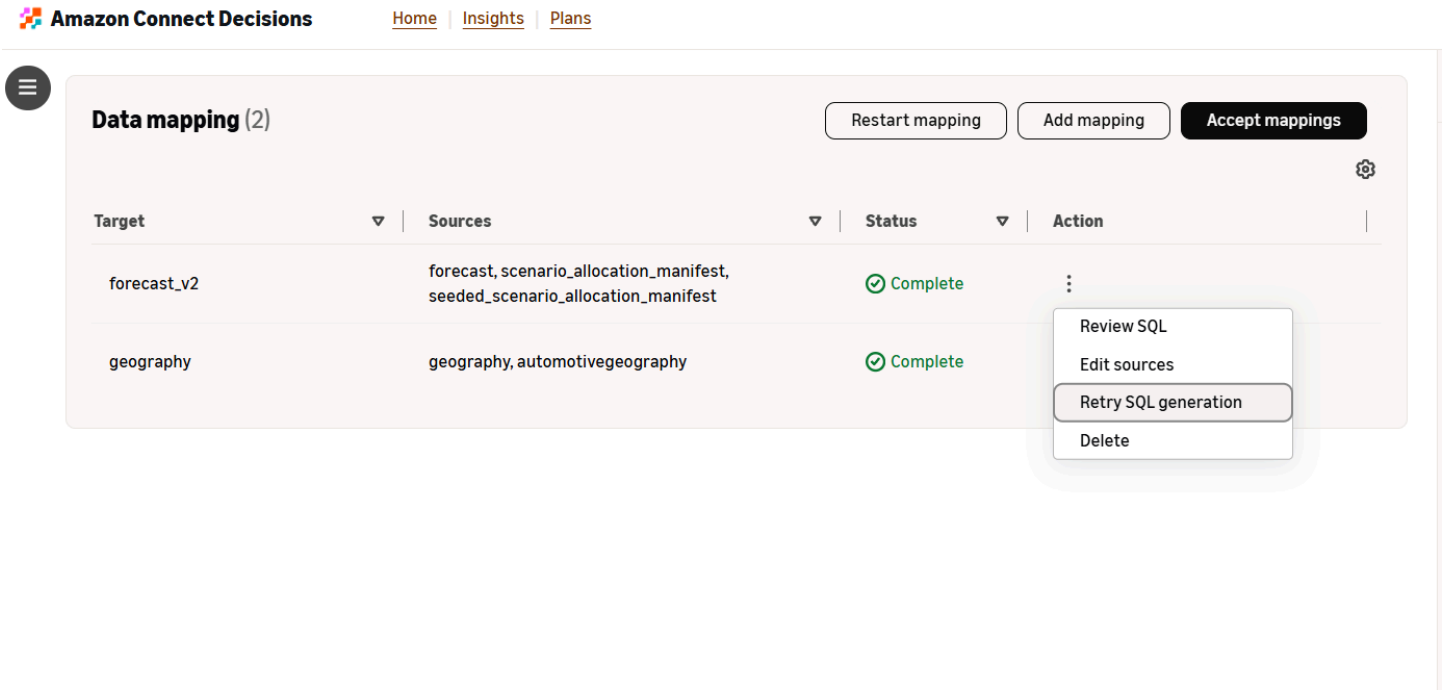
Esamina le mappature rimanenti per ciascuno dei tuoi set di dati di origine. Il Data Agent rimane persistente sul lato destro dello schermo per domande o assistenza alla risoluzione dei problemi.

Quando sei soddisfatto di tutte le mappature, accettale per completare l'onboarding dei dati facendo clic su Accetta mappature.



Gestisci le mappature non riuscite

Se una mappatura fallisce, puoi selezionare «Riavvia mappatura» per riavviare tutte le mappature o riprovare manualmente una singola mappatura dal menu Azioni tramite «Riprova la generazione SQL». Il Data Agent può anche riprovare le mappature utilizzando il linguaggio naturale e continuerà ad aiutarti a identificare e risolvere i problemi se gli errori continuano a persistere.

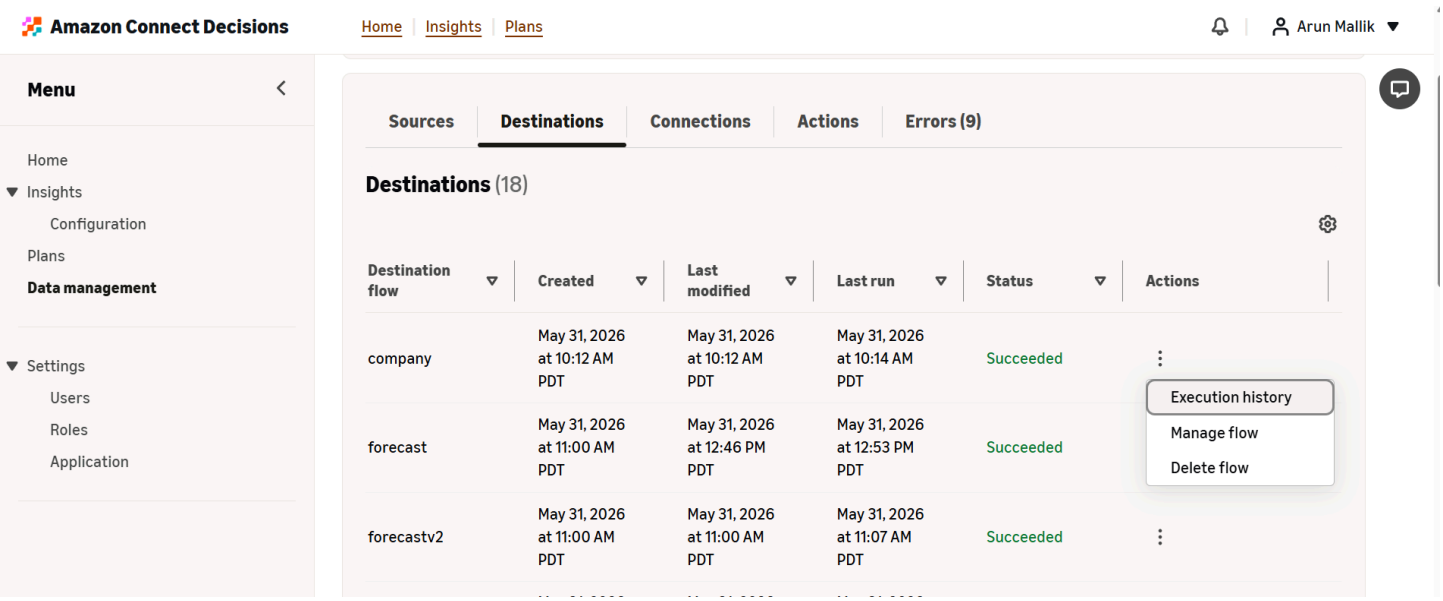


Monitora i tuoi flussi

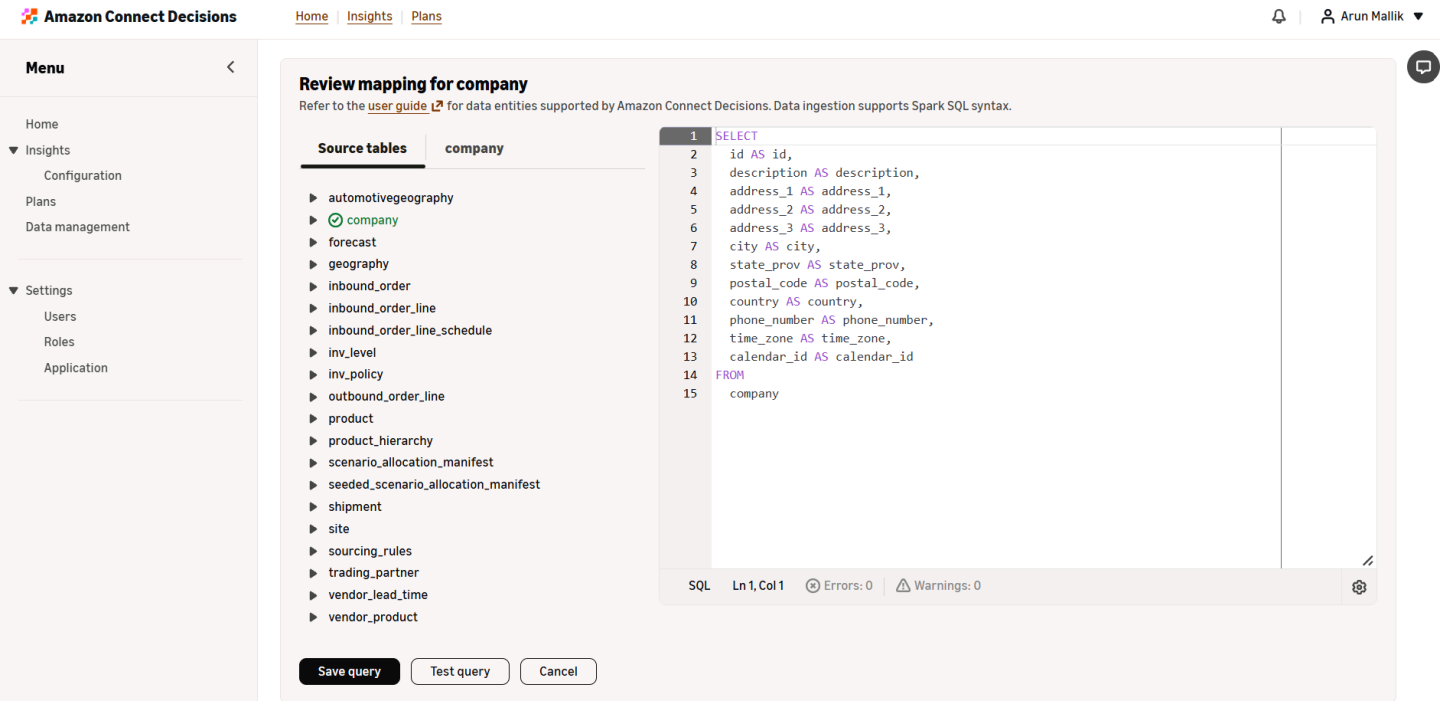
Scheda Destinazioni

Dopo aver accettato le mappature, verrai indirizzato alla scheda Destinazioni all'interno di Gestione dei dati, dove potrai:

- Rivedi i flussi di destinazione
- Gestisci e modifica le mappature («Gestisci flusso»)
- Elimina i flussi obsoleti
- Verifica lo stato di esecuzione di questi flussi



Selezionando «Manage Flow» tornerai all'esperienza di Data Mapping, dove potrai continuare a lavorare con Data Agent per perfezionare le mappature nel tempo.



Scheda Sorgenti

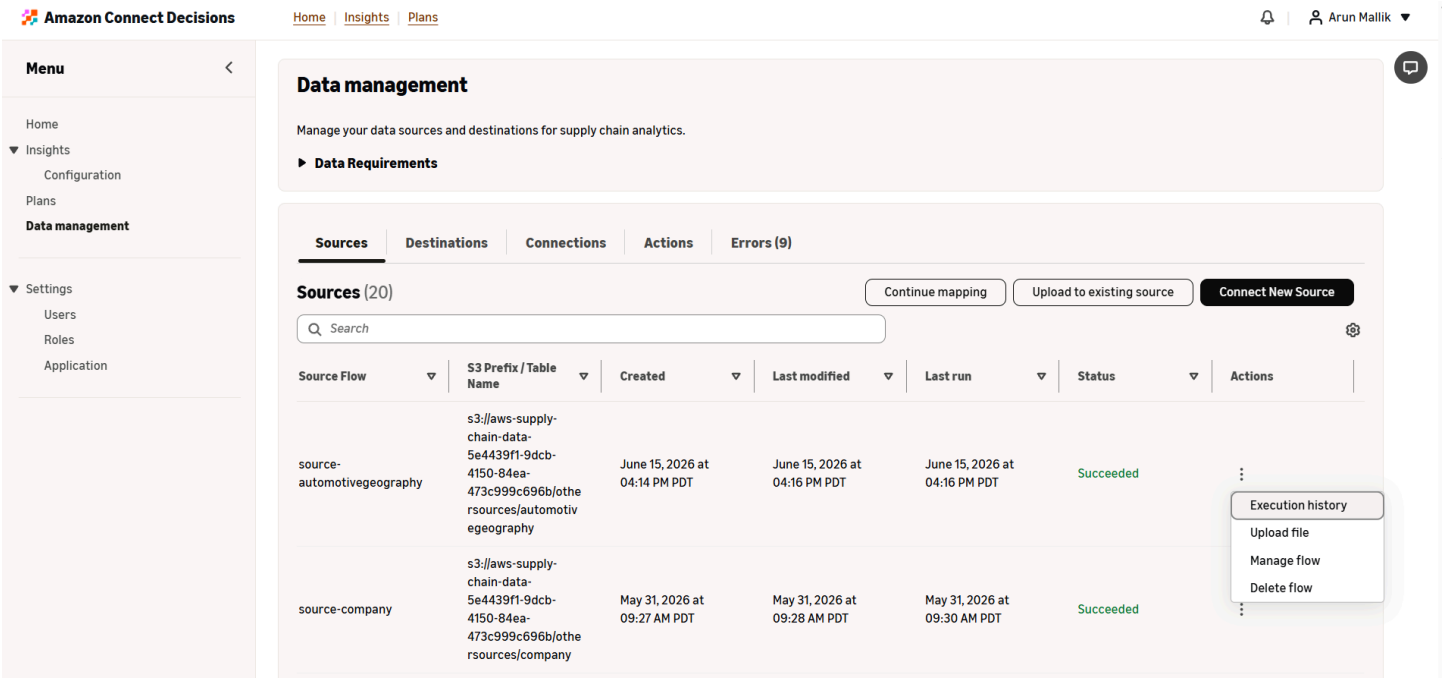
Tornando alla scheda Sorgenti puoi trovare:

- Il set di dati di origine che è stato creato
- È un bucket S3 associato

- Opzioni per:
  - Aggiungi altri dati di origine tramite un altro caricamento di file
  - Gestisci il flusso
  - Eliminare il flusso
  - Rivedi le esecuzioni

Selezionando «Manage Flow» tornerai all'esperienza di Data Mapping, dove potrai continuare a lavorare con Data Agent per perfezionare le mappature nel tempo.

Hai anche accesso a Crea una nuova fonte, se necessario, per riavviare il processo di data onboarding per qualsiasi nuova fonte di dati.



Best practice

Preparazione dei dati

- Segui i passaggi indicati nella sezione Prerequisiti
- Usa la UTF-8 codifica per tutti i file CSV
- Assicurati che i nomi dei file siano unici
- Convalida la qualità dei dati prima del caricamento

Lavorare con Data Agent

- Sii specifico nelle tue richieste
- Chiedi spiegazioni quando non comprendi nessuna delle sue decisioni
- Verifica tutte le modifiche SQL prima di accettarle
- Utilizzate la funzione di anteprima per verificare le trasformazioni

Manutenzione continua

- Mantieni aggiornati i dati di origine
- Monitora regolarmente l'esecuzione del flusso
- Risolvi tempestivamente gli errori nei dati quando vengono notificati
- Documenta le trasformazioni personalizzate per il tuo team

Connessione al database con JDBC

Questa guida illustra come connettere il database ad Amazon Connect Decisions utilizzando Java Database Connectivity (JDBC). Configurerai una crittografia sicura per le credenziali del tuo database e stabilirai una connessione che Amazon Connect Decisions può utilizzare per accedere ai tuoi dati.

Cos'è la connessione JDBC e quando dovresti usarla?

La connessione JDBC consente ad Amazon Connect Decisions di connettersi al tuo database esistente per leggere i dati, anziché richiedere di esportare e caricare file CSV o configurare le tue pipeline di estrazione, trasformazione, caricamento (ETL) su S3. Questo approccio è ideale quando:

- I tuoi dati sono già archiviati in un database Glue-compatible relazionale AWS. Consulta questa guida per database e versioni compatibili.
- Desiderate un accesso ai dati in tempo reale o quasi reale senza esportazioni manuali di file
- Il volume dei dati è elevato e viene aggiornato frequentemente
- Preferisci conservare i dati nella posizione corrente anziché duplicarli
- Se lavori con set di dati più piccoli o preferisci i caricamenti basati su file, il processo di caricamento CSV standard potrebbe essere più semplice per le tue esigenze. Consulta la Guida per l'utente di Data Onboarding per maggiori dettagli su questo processo.

Prerequisiti

Prima di iniziare, assicurati di disporre dei seguenti elementi:

- Un account AWS con autorizzazioni per creare chiavi KMS e risorse Secrets Manager
- L'ID del tuo account AWS e la regione in cui opererà Amazon Connect Decisions
- Dettagli di connessione al database: nome host, porta, nome del database e credenziali
- Accesso amministrativo al database per verificare la connettività
- Il tuo database è configurato per accettare connessioni dai servizi AWS

Crea una chiave Customer-Managed KMS

Prima di connettere il database ad Amazon Connect Decisions, dovrai configurare la crittografia per le credenziali del database. AWS Key Management Service (KMS) fornisce questo livello di sicurezza, garantendo la protezione dei dettagli della connessione.

Crea la tua chiave KMS

1. Passa alla console AWS KMS
   - Apri la Console di gestione AWS nel tuo browser
   - Nella barra di ricerca in alto, digita «KMS» e seleziona «Key Management Service» dai risultati
   - Si apre la dashboard KMS in cui gestirai le chiavi di crittografia
2. Avvia la creazione delle chiavi
   - Nella dashboard KMS, individua e fai clic sul pulsante Crea chiave in alto a destra
   - Questo avvia la procedura guidata per la creazione delle chiavi che ti guiderà attraverso il processo di configurazione
3. Configura il tipo e l'utilizzo della chiave
   - Nella pagina «Configura chiave», seleziona Symmetric come tipo di chiave (questa è l'opzione predefinita e consigliata)
   - Mantieni selezionato «Crittografa e decrittografa» nella sezione Utilizzo della chiave
4. Imposta i dettagli di identificazione delle chiavi
   - Nel campo «Alias», inserisci un nome descrittivo per la tua chiave, ad esempio `aws-supply-chain-database-key`

- Nel campo «Descrizione», aggiungi un contesto come «Chiave di crittografia per le credenziali del database Amazon Connect Decisions»
- Facoltativamente, aggiungi tag per organizzare e tracciare le tue risorse AWS (ad esempio, Key: «Project», Value: «Amazon Connect Decisions»)

5. Definisci le autorizzazioni amministrative chiave
   - Seleziona gli utenti o i ruoli IAM che dovrebbero essere in grado di gestire questa chiave (creare, eliminare, modificare le politiche)
   - Come minimo, includi il tuo ruolo di amministratore per assicurarti di poter modificare la chiave in un secondo momento, se necessario
   - Questi amministratori possono gestire la chiave ma non avranno automaticamente l'autorizzazione per usarla encryption/decryption
   - Nella sezione «Eliminazione chiave», consenti agli amministratori chiave di eliminare questa chiave. (questa è l'opzione predefinita e consigliata)
6. Definire le autorizzazioni di utilizzo delle chiavi
   - In questa pagina, vedrai le opzioni per selezionare gli utenti e i ruoli IAM che possono utilizzare la chiave
   - Salta la selezione di utenti specifici qui, configurerai le autorizzazioni di servizio nel passaggio successivo
7. Configura la policy chiave per i servizi Amazon Connect Decisions
   - Vedrai un editor di policy con JSON predefinito
   - Nell'editor delle politiche chiave KMS, aggiungi la seguente dichiarazione all'array «Statement» esistente
   - Questa politica garantisce il pieno controllo del tuo account e consente ai servizi di Amazon Connect Decisions (Secrets Manager e Glue) di decrittografare le credenziali del database.

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

```
    "kms:GenerateDataKeyWithoutPlaintext"
  ],
  "Resource": "*"
}
```

8. Rivedi e finalizza
   - Controlla tutte le impostazioni di configurazione nella pagina di riepilogo
   - Verifica che l'alias, la descrizione e la policy siano corretti
   - Fai clic su Fine per creare la chiave
   - Una volta creata, verrai reindirizzato alla dashboard KMS dove la tua nuova chiave apparirà nell'elenco

Cosa aspettarsi

La creazione delle chiavi è immediata. Una volta creata, vedrai la tua nuova chiave elencata nella console KMS con lo stato «Abilitato». La chiave è ora pronta per crittografare le credenziali del database in Secrets Manager.

Configurazione di AWS Secrets Manager

Ora che disponi di una chiave KMS, creerai un segreto in AWS Secrets Manager per archiviare in modo sicuro le credenziali del database, quindi configurerai una policy di risorse che consenta ad Amazon Connect Decisions di accedere a questo segreto.

Crea il tuo segreto

1. Accedi ad AWS Secrets Manager
   - Nella barra di ricerca della Console di gestione AWS, digita «Secrets Manager»
   - Seleziona «Secrets Manager» dai risultati per aprire la dashboard del servizio
2. Inizia a creare un nuovo segreto
   - Fai clic sul pulsante Memorizza un nuovo segreto
   - Nella pagina «Scegli il tipo di segreto», seleziona Altro tipo di segreto (questo ti dà la flessibilità di strutturare le tue credenziali)
3. Inserisci le credenziali del database
   - Nella sezione coppie chiave-valore, aggiungi i dettagli della connessione al database come stringhe:

```
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. Seleziona la tua chiave di crittografia
   - In «Chiave di crittografia», seleziona Scegli una chiave AWS KMS
   - Dal menu a discesa, seleziona la chiave KMS che hai creato nella fase 1 (ad esempio,) `aws-supply-chain-database-key`
   - Ciò garantisce che le tue credenziali siano crittografate con la chiave gestita dal cliente
5. Dai un nome al tuo segreto
   - Inserisci un nome descrittivo per il tuo segreto, ad esempio `aws-supply-chain-production-database`
   - Facoltativamente, aggiungi una descrizione come «Credenziali del database per l'ambiente di produzione Amazon Connect Decisions»
   - Se lo desideri, aggiungi tag per l'organizzazione (ad esempio, Chiave: «Ambiente», Valore: «Produzione»)
6. Aggiungi le autorizzazioni per le risorse
   - Fai clic su «Modifica autorizzazioni». Nell'editor delle politiche, incolla la seguente politica. Questa politica consente ai servizi di Amazon Connect Decisions di leggere il tuo segreto.

```
{
  "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. Salva la politica
   - Fai clic su Salva per applicare la politica sulle risorse

- La policy è ora attiva e consente ad Amazon Connect Decisions di recuperare le credenziali del database.

8. Configura la rotazione (opzionale)
   - Per questa configurazione, puoi saltare la rotazione automatica selezionando Disabilita la rotazione automatica
   - Puoi abilitare la rotazione in un secondo momento se le tue politiche di sicurezza lo richiedono
9. Revisione e creazione
   - Rivedi tutti i tuoi dati segreti
   - Fai clic su Store per creare il segreto
   - Verrai reindirizzato alla dashboard di Secrets Manager
10. Salva il tuo ARN segreto
    - Trova il tuo segreto appena creato nell'elenco dei segreti
    - Fai clic sul nome del segreto per aprirne la pagina dei dettagli
    - In alto, vedrai l'ARN segreto
    - Copia e salva questo ARN
    - Il formato ARN ha il seguente aspetto: `arn:aws:secretsmanager:us-east-1:123456789012:secret:aws-supply-chain-production-database-AbCdEf`
11. Modifica le autorizzazioni delle risorse
    - Fai clic su «Modifica autorizzazioni»
    - Incolla l'ARN segreto copiato e `<COPY-THE-SECRET-ARN-HERE-AFTER-CREATING>` sostituiscilo con l'ARN copiato
    - Fai clic su Salva per allegare la politica

Cosa aspettarsi

Il tuo segreto è ora archiviato in modo sicuro e crittografato con la tua chiave KMS. I servizi di Amazon Connect Decisions sono autorizzati a recuperare le credenziali quando stabiliscono una connessione al database, ma le credenziali rimangono crittografate quando sono inutilizzate e in transito.

Connetti il tuo database ad Amazon Connect Decisions

Con la chiave KMS e il segreto configurati, sei pronto per stabilire la connessione JDBC in Amazon Connect Decisions.

Configura la tua connessione JDBC

1. Passa ad Amazon Connect Decisions > Gestione dei dati
   - Accedi alla tua istanza Amazon Connect Decisions
   - Dalla navigazione principale, seleziona «Gestione dei dati»
   - Nella scheda di navigazione, vai a «Connessioni»
   - Seleziona «Nuova connessione» per creare una nuova connessione
2. Inserisci i dettagli della connessione
   - Nome della connessione (richiesto): inserisci un identificatore univoco per questa connessione (ad esempio, «database di produzione»)
   - Descrizione (opzionale): aggiungi dettagli sullo scopo e sull'utilizzo di questa connessione per aiutare il team a capire a quali dati accede
   - URL JDBC (richiesto): inserisci la stringa di connessione JDBC completa nel formato: (ad es.) `jdbc:<database-type>://<hostname>:<port>/<database>` `jdbc:postgresql://db.example.com:5432/mydb`
   - Nome dello schema (opzionale): Specificate lo schema del database, se necessario (ad esempio, «public», «dbo», «myschema»). Lascia vuoto per utilizzare lo schema predefinito del database
   - ARN segreto (obbligatorio): incolla l'ARN segreto salvato dal passaggio 2. Ciò consente ad Amazon Connect Decisions di recuperare in modo sicuro le credenziali del database da Secrets Manager.
   - Applica la connessione SSL: mantieni questa casella di controllo selezionata (scelta consigliata) per richiedere la crittografia per la connessione al database SSL/TLS
   - Nome del servizio endpoint VPC (richiesto): inserisci il nome del servizio endpoint VPC per la connettività privata tramite AWS (formato:) PrivateLink `com.amazonaws.vpce.<region>.vpce-svc-xxxxxxxxx`
3. Connect al database
   - Fai clic su «Connetti» per testare e stabilire la connessione. Amazon Connect Decisions verificherà che sia in grado di connettersi correttamente al tuo database utilizzando le

credenziali fornite. Questo passaggio può richiedere fino a 2 minuti, quindi ti preghiamo di non lasciare questa schermata durante la connessione.

- Se la connessione riesce, verrai indirizzato automaticamente alla selezione della tabella
- Se la connessione fallisce:
  - Controlla i dettagli della connessione per assicurarti che tutti i campi siano corretti:
    - Verifica che il tuo Secret ARN sia corretto
    - Conferma che le credenziali del database siano corrette
    - Verifica che il formato dell'URL JDBC sia corretto
    - Assicurati che il tuo database sia configurato per accettare connessioni dai servizi AWS
    - Verifica che la chiave KMS e le politiche di Secrets Manager siano configurate correttamente
  - Puoi anche utilizzare l'esperienza di chat per risolvere i problemi di connessione ponendo domande come «Perché la mia connessione al database non funziona?» o «Aiutami a eseguire il debug della mia connessione JDBC»

4. Seleziona le tabelle da importare
   - Una volta connesso, vedrai la schermata Seleziona tabelle che mostra tutte le tabelle disponibili dal tuo database
   - Seleziona la casella di controllo accanto a ciascuna tabella che desideri importare
5. Configura la pianificazione dell'aggiornamento della tabella
   - Per ogni tabella selezionata, fai clic sul menu a tre punti nella colonna Azione e seleziona «Pianifica l'aggiornamento»
   - Nella finestra di dialogo Configura i dettagli del caricamento, imposta:
     - Cadenza: con quale frequenza di aggiornamento (oraria, giornaliera, settimanale o personalizzata)
     - Ora di inizio: l'ora di inizio dell'aggiornamento (visualizzata in UTC con lo scostamento del fuso orario)
     - Tipo di aggiornamento: scegli Aggiornamento completo (sostituisci tutti i dati) o Aggiornamento incrementale (aggiungi nuovi dati a quelli esistenti; richiede la selezione di una colonna Record timestamp)
     - Ripetete l'operazione per ogni tabella, se necessario
   - Fai clic su Avvia mappatura quando tutte le tabelle sono configurate
6. Continua con la mappatura dei dati

- Da questo momento in poi, l'esperienza è identica al nostro flusso di Data Onboarding
- Segui la sezione Data Mapping della Data Onboarding User Guide per completare la configurazione

Cosa aspettarsi

Una volta stabilita la connessione e selezionate le tabelle, Amazon Connect Decisions può leggere i dati dal tuo database. La connessione rimane attiva e sicura, con credenziali crittografate e gestite tramite AWS Secrets Manager. Non sarà necessario aggiornare manualmente le credenziali in Amazon Connect Decisions, tutte le modifiche apportate in Secrets Manager verranno riflesse automaticamente.

Best practice

Gestione della sicurezza e degli accessi

- Archivia le credenziali in modo sicuro: utilizza sempre AWS Secrets Manager per archiviare le credenziali del database, non codificare mai le credenziali nelle stringhe di connessione o nei file di configurazione
- Abilita SSL/TLS la crittografia: mantieni abilitata l'opzione «Enforce SSL connection» per garantire che i dati siano crittografati in transito
- Rivedi regolarmente le politiche di KMS and Secrets Manager: assicurati che solo i servizi e gli account autorizzati abbiano accesso alle tue chiavi e ai tuoi segreti di crittografia
- Usa l'accesso con privilegi minimi: concedi solo le autorizzazioni minime necessarie agli utenti del database che Amazon Connect Decisions utilizzerà per le connessioni

Configurazione della connessione

- Usa nomi di connessione descrittivi: scegli nomi chiari e significativi che indichino l'ambiente e lo scopo (ad esempio, «production-inventory-db» anziché «db1")
- Documenta le tue connessioni: utilizza il campo Descrizione per annotare a quali dati accede la connessione, chi ne è il proprietario ed eventuali considerazioni speciali
- Verifica le connessioni prima di procedere: verifica sempre che la connessione funzioni prima di selezionare le tabelle e configurare le pianificazioni di aggiornamento

- Convalida il formato dell'URL JDBC: la sintassi dell'URL JDBC Double-check corrisponde al tipo di database per evitare errori di connessione

Strategia di aggiornamento dei dati

- Scegli la cadenza di aggiornamento appropriata: seleziona la frequenza di aggiornamento in base alla frequenza con cui cambiano i dati di origine e alle esigenze aziendali
- Pianifica gli aggiornamenti durante i periodi di bassa attività: configura gli orari di aggiornamento quando il carico del database è inferiore per ridurre al minimo l'impatto sulle prestazioni
- Utilizza gli aggiornamenti incrementali quando possibile: per set di dati di grandi dimensioni con modifiche frequenti, gli aggiornamenti incrementali sono più efficienti degli aggiornamenti completi
- Seleziona colonne con timestamp significative: quando utilizzi gli aggiornamenti incrementali, scegli colonne che riflettano accuratamente quando i record sono stati creati o modificati

Utilizzo della chat per la risoluzione dei problemi

- Sii specifico nelle tue richieste: fornisci un contesto chiaro quando chiedi aiuto per la risoluzione dei problemi di connessione o mappatura
- Chiedi spiegazioni: se non comprendi i consigli o le query SQL generate, chiedi chiarimenti
- Verifica tutte le modifiche SQL prima di accettarle: utilizza la funzionalità di anteprima per verificare che le trasformazioni funzionino come previsto con i dati effettivi
- Sfrutta la chat per la risoluzione dei problemi: quando le connessioni falliscono o gli aggiornamenti riscontrano errori, fai domande diagnostiche come «Perché la mia connessione non funziona?» o «Aiutami a capire questo errore di aggiornamento»

Manutenzione continua

- Monitora regolarmente l'esecuzione degli aggiornamenti: controlla le schede Destinazioni e Fonti in Gestione dei dati per assicurarti che gli aggiornamenti vengano completati correttamente
- Risolvi tempestivamente gli errori: quando Amazon Connect Decisions ti avvisa degli errori di aggiornamento, analizza e risolvi rapidamente i problemi per evitare lacune nei dati
- Aggiorna le credenziali in modo sicuro: quando le password del database cambiano, aggiornale in AWS Secrets Manager, Amazon Connect Decisions utilizzerà automaticamente le nuove credenziali

- Documenta configurazioni personalizzate: prendi nota di eventuali pianificazioni di aggiornamento speciali, logica di trasformazione o requisiti di connessione come riferimento per il tuo team
- Rivedi periodicamente le selezioni delle tabelle: man mano che le tue esigenze in materia di dati evolvono, rivedi le tabelle che stai importando e verifica se le pianificazioni di aggiornamento sono ancora in linea con i requisiti aziendali

Comprensione del Canonical Data Model (CDM)

Il Canonical Data Model (CDM) è la struttura dati standardizzata utilizzata da. Quando si integrano i dati della catena di fornitura, questi devono essere trasformati in formato CDM in modo da poterli elaborare per la pianificazione, la previsione e le informazioni operative.

Questo argomento spiega cos'è il CDM, perché è importante e quali entità di dati sono disponibili.

Cos'è il CDM?

Il CDM definisce un insieme comune di entità e campi di dati che rappresentano i concetti della catena di approvvigionamento come prodotti, siti, ordini, spedizioni e inventario. Indipendentemente dal formato o dalla struttura dei dati di origine, il CDM fornisce uno schema unico e coerente che utilizza tutte le sue funzionalità.

Durante l'onboarding dei dati, i dati di origine vengono mappati sulle tabelle di destinazione CDM. Il Data Agent può suggerire automaticamente mappature tra i campi di origine e i campi CDM e generare query di trasformazione SQL per convertire i dati.

Perché il CDM è importante

- Coerenza: tutte le funzionalità funzionano sulla stessa struttura di dati, garantendo un comportamento uniforme in termini di pianificazione della domanda, ottimizzazione dell'inventario e analisi dei tempi di consegna.
- Interoperabilità: i dati provenienti da diversi sistemi di origine (ERP, WMS, TMS) vengono normalizzati in un unico modello, che consente l'analisi tra sistemi.
- Onboarding semplificato: Data Agent utilizza il CDM come schema di destinazione per generare mappature automatiche, riducendo il lavoro manuale.
- Qualità dei dati: i controlli di convalida vengono eseguiti rispetto alle definizioni CDM per individuare eventuali problemi prima che i dati vengano utilizzati nella produzione.

Categorie di entità dati

Le entità di dati CDM si dividono in due categorie:

- Non-transactional dati: dati di riferimento o anagrafici che cambiano raramente, come prodotti, siti, partner commerciali e aree geografiche.
- Dati transazionali: dati operativi che cambiano frequentemente, come previsioni, livelli di inventario, ordini e spedizioni.

Entità di dati supportate

La tabella seguente elenca tutte le entità di dati supportate nel CDM.

Entità di dati CDM supportate

Entità dati	Tipo di dato	Richiesto
Azienda	Non-transactional dati	Sì
Prodotto	Non-transactional dati	Sì
Partner commerciale	Non-transactional dati	Sì
Prodotto del fornitore	Non-transactional dati	Sì
geografia	Non-transactional dati	Sì
Gerarchia dei prodotti	Non-transactional dati	Sì
corsia di trasporto	Non-transactional dati	Sì
lead time del fornitore	Non-transactional dati	Sì
Site	Non-transactional dati	Sì
festività del fornitore	Non-transactional dati	Sì
Previsione	Dati transazionali	Sì
Inventory	Dati transazionali	Sì

Entità dati	Tipo di dato	Richiesto
Ordine in entrata () PO/STO	Dati transazionali	Sì
Linea d'ordine in uscita	Dati transazionali	Sì
Spedizione	Dati transazionali	Sì
Politica di inventario	Dati transazionali	Sì
Riga d'ordine in entrata () PO/STO	Dati transazionali	Sì
Spedizione in uscita	Dati transazionali	Sì
Pianificazione della linea degli ordini in entrata	Dati transazionali	Sì

Entità richieste dalla funzionalità

Non tutte le funzionalità incluse richiedono tutte le entità CDM. Le sezioni seguenti descrivono quali entità sono obbligatorie, facoltative o non applicabili per ciascuna funzionalità.

Visibilità dell'inventario

Entità CDM per la visibilità dell'inventario

Entità dei dati	Tipo di dato	Richiesto
Azienda	Non-transactional	Facoltativo
Prodotto	Non-transactional	Sì
Partner commerciale	Non-transactional	Facoltativo
Prodotto del fornitore	Non-transactional	Non applicabile
Geografia	Non-transactional	Facoltativo
Gerarchia dei prodotti	Non-transactional	Facoltativo

Entità dei dati	Tipo di dato	Richiesto
Corsia di trasporto	Non-transactional	Facoltativo
Tempi di consegna del fornitore	Non-transactional	Non applicabile
Site	Non-transactional	Sì
Festa del fornitore	Non-transactional	Non applicabile
Previsione	Transazionale	Facoltativo
Inventory	Transazionale	Sì
Ordine in entrata () PO/STO	Transazionale	Facoltativo
Linea d'ordine in uscita	Transazionale	Facoltativo
Spedizione	Transazionale	Facoltativo
Politica di inventario	Transazionale	Sì
Linea d'ordine in entrata	Transazionale	Facoltativo
Spedizione in uscita	Transazionale	Facoltativo
Pianificazione della linea degli ordini in entrata	Transazionale	Facoltativo

Informazioni sui tempi di consegna

Entità CDM per informazioni dettagliate sui tempi di consegna

Entità dei dati	Tipo di dato	Richiesto
Azienda	Non-transactional	Facoltativo
Prodotto	Non-transactional	Sì
Partner commerciale	Non-transactional	Sì

Entità dei dati	Tipo di dato	Richiesto
Prodotto del fornitore	Non-transactional	Sì
Geografia	Non-transactional	Facoltativo
Gerarchia dei prodotti	Non-transactional	Facoltativo
Corsia di trasporto	Non-transactional	Sì
Tempi di consegna del fornitore	Non-transactional	Sì
Site	Non-transactional	Sì
Festa del fornitore	Non-transactional	Facoltativo
Previsione	Transazionale	Non applicabile
Inventory	Transazionale	Non applicabile
Ordine in entrata () PO/STO	Transazionale	Sì
Linea d'ordine in uscita	Transazionale	Non applicabile
Spedizione	Transazionale	Sì
Politica di inventario	Transazionale	Non applicabile
Linea d'ordine in entrata	Transazionale	Sì
Spedizione in uscita	Transazionale	Non applicabile
Pianificazione della linea degli ordini in entrata	Transazionale	Sì

Pianificazione della domanda

Entità CDM per la pianificazione della domanda

Entità dei dati	Tipo di dato	Richiesto
Azienda	Non-transactional	Facoltativo
Prodotto	Non-transactional	Sì
Partner commerciale	Non-transactional	Non applicabile
Prodotto del fornitore	Non-transactional	Non applicabile
Geografia	Non-transactional	Facoltativo
Gerarchia dei prodotti	Non-transactional	Facoltativo
Corsia di trasporto	Non-transactional	Non applicabile
Tempi di consegna del fornitore	Non-transactional	Non applicabile
Site	Non-transactional	Sì
Festa del fornitore	Non-transactional	Non applicabile
Previsione	Transazionale	Non applicabile
Inventory	Transazionale	Non applicabile
Ordine in entrata () PO/STO	Transazionale	Non applicabile
Linea d'ordine in uscita	Transazionale	Sì
Spedizione	Transazionale	Non applicabile
Politica di inventario	Transazionale	Non applicabile
Linea d'ordine in entrata	Transazionale	Non applicabile
Spedizione in uscita	Transazionale	Non applicabile

Entità dei dati	Tipo di dato	Richiesto
Pianificazione della linea degli ordini in entrata	Transazionale	Non applicabile

In che modo il CDM si relaziona all'onboarding dei dati

Quando si effettuano l'onboarding dei dati, il processo segue questi passaggi:

1. Caricamento: carichi i dati di origine come file CSV su Amazon S3.
2. Mappa: Data Agent analizza i set di dati di origine e suggerisce quali tabelle di destinazione CDM si adattano meglio ai dati.
3. Trasforma: le query di trasformazione SQL convertono il formato dei dati di origine in formato CDM.
4. Convalida: vengono eseguiti controlli di qualità sui dati trasformati per verificarne la conformità ai requisiti CDM.
5. Attiva: una volta convalidati, i dati confluiscono e diventano disponibili per le funzionalità.

Per istruzioni dettagliate sull'onboarding dei dati, consulta l'argomento Data Onboarding.

Convalida dei dati e controlli di qualità

Panoramica di

La convalida dei dati garantisce che i dati soddisfino i requisiti di qualità prima dell'esecuzione delle funzionalità di Amazon Connect Decisions. Il sistema convalida i dati in base ai piani, alle metriche e alle regole configurati per identificare i problemi che potrebbero bloccare o ridurre le prestazioni.

Come funziona la convalida dei dati

Trigger di convalida

La convalida dei dati viene eseguita automaticamente nei seguenti orari:

- Modifiche alla configurazione di Insights: quando crei o modifichi metriche, regole o altre configurazioni

- Creazione del piano: quando crei un piano ad hoc o in occasione di ogni esecuzione del piano pianificato
- Aggiornamento dei dati: dopo ogni aggiornamento dei dati nei flussi di destinazione
- Esecuzione delle capacità: prima o durante le operazioni dei membri del team AI (ad esempio, quando si causa un'eccezione come root o si determinano raccomandazioni)

Tipi di convalida

Amazon Connect Decisions esegue due tipi di convalida:

Data Presence Validation verifica che i set di dati e i campi richiesti vengano caricati in base alle risorse configurate (metriche, regole, piani).

La convalida della qualità dei dati verifica che i dati forniti soddisfino i requisiti di qualità in base alla configurazione di configurazione, tra cui:

- Convalida dei criteri di configurazione: conferma che i prodotti e i siti soddisfano i criteri delle regole (ad esempio, categorie di prodotti, sedi dei siti)
- Convalida della gerarchia: identifica le relazioni gerarchiche mancanti se si utilizzano gerarchie nella configurazione
- Convalida dell'ambito: conferma l'esistenza di tutti i dati necessari per i prodotti e i siti identificati
- Valutazione della qualità: valuta la qualità e l'usabilità dei dati per i requisiti operativi

Validazione progressiva

Amazon Connect Decisions abilita funzionalità per prodotti e siti con dati validi anziché bloccare le funzionalità per l'intero set di dati. Quando i problemi di convalida riguardano prodotti o siti specifici, il sistema continua a elaborare prodotti e siti con dati validi, identifica i prodotti o i siti con problemi di dati e ti avvisa degli elementi specifici che richiedono attenzione. Ciò consente di iniziare a utilizzare le funzionalità risolvendo al contempo i restanti problemi relativi ai dati.

Accesso agli errori di convalida dei dati

È possibile visualizzare gli errori di convalida dei dati tramite tre punti di ingresso:

1. Metrica «Errori di convalida dei dati» nella home page
2. Scheda tematica degli errori di convalida dei dati nella home page

3. «Gestione dei dati» nella barra di navigazione a sinistra > scheda «Errori»

Revisione degli errori di convalida

La pagina Errori mostra tutti gli errori di convalida aperti e risolti. È possibile cercare e filtrare in base a una delle seguenti colonne:

- ID: identificatore univoco per l'errore di convalida
- Stato
  - Aperto: l'errore non è stato risolto
  - Risolto: l'errore è stato corretto e convalidato
- Descrizione: spiegazione del problema relativo alla qualità dei dati
- Tipo di problema
  - Dati obbligatori mancanti: non vengono forniti dati obbligatori per avviare un'operazione (ad esempio, nessuna tabella di origine outbound_order_line per Supply Plan)
  - Valori dati non validi: i dati esistono ma contengono valori errati (ad esempio, costo negativo del prodotto)
  - Relazioni mancanti: mancano le relazioni gerarchiche o di riferimento richieste (ad esempio, gerarchie di prodotti mancanti)
  - Dati insufficienti: i dati disponibili non sono sufficienti per eseguire le operazioni richieste (ad esempio, il piano della domanda richiede 12 mesi di dati storici sugli ordini, ma esistono solo 3 mesi)
- Capacità: la capacità o la risorsa interessata
  - Piano di fornitura
  - Piano della domanda
  - Informazioni approfondite (include eccezioni, raccomandazioni e RCA per la domanda o l'offerta)
- Destinazione: flusso di destinazione interessato
- Priorità
  - Critico: almeno una funzionalità è completamente bloccata e non può essere eseguita
  - Alto: almeno una funzionalità è parzialmente bloccata (alcuni prodotti o siti non possono essere elaborati)
  - Medio: almeno una funzionalità ha una precisione ridotta (funzionerà ma con risultati scadenti)
- Creato in: Timestamp che mostra quando l'errore è stato rilevato per la prima volta

Visualizzazione dei dettagli dell'errore

Seleziona un errore per visualizzare informazioni dettagliate. La schermata di dettaglio mostra le informazioni di cui sopra insieme a un timestamp dell'ultima volta che si è verificato, una risorsa e un link correlati (la metrica, la regola o il piano che rappresenta la capacità interessata dal problema) e un'anteprima di un massimo di 100 righe di dati interessati che mostrano come si manifesta l'errore di convalida dei dati.

Operazioni disponibili

Dalla schermata dei dettagli dell'errore, puoi:

- Risoluzione dei problemi: avvia l'AI Teammate per aiutarti a risolvere il problema in linguaggio naturale e ricevi una guida dettagliata sulla risoluzione
- Risolvi errore: contrassegna manualmente l'errore come risolto se hai risolto il problema sottostante
- Scarica: scarica il set di dati interessato completo per un'analisi e una correzione dettagliate

Risoluzione degli errori di convalida dei dati

Workflow di risoluzione

1. Esamina la descrizione e la priorità dell'errore per comprenderne l'impatto
2. Controlla l'anteprima dei dati interessati per vedere quali record specifici sono interessati
3. Segui la raccomandazione specifica fornita per la correzione
4. Scegli un'azione appropriata:
   - Per problemi di configurazione: collabora con i tuoi manager e pianificatori per modificare la configurazione di metriche, regole o piani
   - Per problemi di mappatura: correggi i dati di origine caricati o aggiorna le trasformazioni e le mappature dei dati
   - Per dati mancanti o non validi: carica i dati corretti
5. Contrassegna manualmente l'errore come risolto dopo aver risolto il problema sottostante

Lavorare con AI Teammate

Usa l'opzione Risoluzione dei problemi per porre domande come «Su quali errori devo concentrarmi per primi?» o «Quali errori bloccano il mio piano di domanda?» , ricevi spiegazioni dettagliate del problema e del suo impatto, ottieni indicazioni dettagliate sugli approcci di risoluzione e scopri in che modo l'errore influisce sulla tua configurazione specifica. Il collega del team AI può fungere da guida per risolvere il problema all'interno di Amazon Connect Decisions e all'interno dei tuoi sistemi di dati di origine.

Best practice

- Assegna priorità in base alla gravità: concentrati innanzitutto sugli errori critici, poiché bloccano completamente l'esecuzione delle funzionalità. Quindi risolvi gli errori ad alta priorità che bloccano parzialmente l'elaborazione, seguiti da quelli a priorità media che riducono la precisione.
- Esamina attentamente i consigli: ogni errore include indicazioni specifiche e attuabili, adattate al problema in base alla configurazione.
- Sfruttate la convalida progressiva a vostro vantaggio: non aspettate di risolvere ogni errore prima di utilizzare le funzionalità. Il sistema abilita la funzionalità di prodotti e siti validi mentre tu lavori alla risoluzione dei problemi per altri.
- Monitoraggio dopo l'aggiornamento dei dati: verifica la presenza di nuovi errori di convalida dopo ogni aggiornamento dei dati per individuare tempestivamente i problemi prima che influiscano sui flussi di lavoro di produzione.
- Scarica i dati interessati in modo strategico: utilizza l'opzione di download quando devi analizzare tutti i record interessati oltre all'anteprima o quando devi fornire il set di dati completo al tuo team di dati.
- Usa AI teammate per problemi complessi: l'opzione Risoluzione dei problemi fornisce un'assistenza contestuale che si adatta alla situazione e alla configurazione specifiche.
- Verifica la risoluzione: dopo aver risolto i problemi relativi ai dati, contrassegna manualmente gli errori come risolti per confermare che la correzione è avvenuta correttamente e rimuovili dall'elenco Apri.

Configurazione del sistema

Le impostazioni in Amazon Connect Decisions sono organizzate per ambito e pubblico. Alcune impostazioni sono personali e consentono a ciascun utente di personalizzare la propria esperienza. Altre sono configurazioni a livello di istanza gestite dagli amministratori che influiscono sul comportamento del sistema per tutti gli utenti o sulla sua connessione all'ambiente tecnologico più ampio.

User-level le impostazioni consentono agli utenti di gestire le informazioni relative all'account, le preferenze di notifica e il modo in cui l'ambito di accesso ai dati viene applicato alle visualizzazioni.

Instance-level le impostazioni consentono agli amministratori di configurare il comportamento del filtro di controllo degli accessi in tutta l'organizzazione, stabilire connessioni all'ERP e ad altri sistemi esterni e definire in che modo il sistema gestisce le azioni consigliate.

Insieme, queste impostazioni offrono alla tua organizzazione la flessibilità necessaria per adattare Amazon Connect Decisions al tuo contesto operativo specifico, mantenendo al contempo la coerenza all'interno del team.

Impostazioni del profilo utente

Gli utenti possono accedere alle impostazioni del proprio profilo selezionando il proprio nome nell'angolo in alto a destra dell'applicazione e scegliendo Profilo dal menu a discesa. La pagina Profilo consente agli utenti di gestire le informazioni dell'account, le preferenze di notifica e le impostazioni di accesso ai dati.

Accesso alle impostazioni del profilo

Per accedere alle impostazioni del tuo profilo:

1. Seleziona il tuo nome nell'angolo in alto a destra della pagina
2. Scegli Profilo dal menu a discesa
3. La pagina del profilo mostra le informazioni e le impostazioni del tuo account

Informazioni sul profilo

La pagina del profilo mostra i seguenti dettagli dell'account:

Utente: il tuo nome utente

Ruolo: ruolo assegnato (amministratore, responsabile o pianificatore)

Fuso orario: seleziona il fuso orario preferito dal menu a discesa. Questa impostazione determina la modalità di visualizzazione di date e orari in Amazon Connect Decisions.

E-mail: il tuo indirizzo e-mail associato al tuo account Amazon Connect Decisions

Creato: la data e l'ora di creazione dell'account

Aggiornato: la data e l'ora dell'ultima modifica del profilo

Seleziona Salva nell'angolo in alto a destra per salvare eventuali modifiche alle informazioni del tuo profilo.

Preferenze di notifica

La scheda Preferenze di notifica consente di configurare la modalità di ricezione delle notifiche per vari eventi di sistema. È possibile scegliere di ricevere notifiche nell'applicazione, via e-mail o in entrambi.

Piani

Generazione riuscita del piano: scegli in che modo desideri ricevere una notifica quando la generazione del piano viene completata con successo. Le opzioni includono notifiche in-app e notifiche e-mail.

Errore nella generazione del piano: scegli in che modo desideri ricevere una notifica quando la generazione del piano fallisce. Le opzioni includono notifiche in-app e notifiche e-mail.

Configurazioni Insights

Configurazioni di Insights riuscite: scegli come ricevere una notifica quando la configurazione di Insights viene completata correttamente. Le opzioni includono le notifiche in-app.

Configurazioni di Insights non riuscite: scegli come ricevere una notifica quando la configurazione di Insights fallisce. Le opzioni includono notifiche in-app.

Inserimento di dati

Inserimento dati non riuscito: scegli in che modo desideri ricevere una notifica in caso di errore di inserimento dei dati. Le opzioni includono notifiche in-app e notifiche e-mail.

Impostazioni di amministrazione

Gli amministratori possono configurare impostazioni di notifica a livello di sistema che si applicano a tutti gli utenti.

Conservazione delle notifiche: imposta il numero di giorni dopo i quali le notifiche vengono rimosse automaticamente dal sistema. Immettere un valore numerico per specificare il periodo di conservazione.

Seleziona Salva per applicare le tue preferenze di notifica.

Ambito assegnato

La scheda Ambito assegnato mostra le autorizzazioni di accesso ai dati e consente di configurare il modo in cui le visualizzazioni dei dati vengono filtrate in base all'ambito assegnato.

Accesso ai dati

Questa sezione mostra il tuo attuale livello di accesso ai dati. Se hai accesso a tutti i siti e i prodotti, vedrai il messaggio «Hai accesso a tutti i siti e i prodotti».

Filtro di visualizzazione predefinito

Filtra le visualizzazioni in base all'ambito assegnato: se abilitate, le visualizzazioni dei dati filtrano automaticamente per mostrare solo gli articoli all'interno dei prodotti e dei siti assegnati. Attiva o disattiva questa impostazione in base alle tue preferenze.

Quando questo filtro è abilitato, vedrai solo eccezioni, piani e altri dati pertinenti all'ambito assegnato. Se disabilitato, è possibile visualizzare dati al di fuori dell'ambito assegnato a seconda delle autorizzazioni del ruolo.

Seleziona Salva per applicare le preferenze di filtro.

Attiva/disattiva il filtro di controllo degli accessi

Come indicato in precedenza, tutti gli utenti possono visualizzare tutte le eccezioni, indipendentemente dal fatto che abbiano configurato i prodotti e i siti appropriati (le azioni di modifica richiedono comunque un accesso appropriato). Sebbene ciò faciliti la condivisione delle conoscenze,

gli utenti che si concentrano solo su prodotti e siti specifici possono essere sopraffatti dalle eccezioni o dai consigli relativi ad altri prodotti e siti. Per aiutare gli utenti a concentrarsi sulle eccezioni e sui consigli che li interessano, possono utilizzare l'interruttore di visualizzazione degli accessi nel modo seguente:

- Innanzitutto, un utente con il ruolo «Amministratore» deve abilitare la funzionalità su quell'istanza. Vai alla pagina Impostazioni dell'istanza dalla barra di navigazione a sinistra
- Per impostazione predefinita, vedranno un interruttore che imposta il filtro di visualizzazione di accesso predefinito per l'intera istanza. L'amministratore può decidere di avere un'impostazione unificata per tutti gli utenti dell'istanza o consentire agli utenti di decidere le proprie preferenze
- Se sceglie l'impostazione di attivazione della visualizzazione ad accesso unificato, l' "amministratore» può anche decidere se l'interruttore deve essere abilitato o disabilitato per tutti gli utenti
- Se scelgono di consentire a ciascun utente di selezionare le proprie preferenze, ogni utente avrà la possibilità di attivare autonomamente il filtro di visualizzazione degli accessi. Ogni utente può accedere alla pagina Preferenze utente dal menu a discesa Utente nell'angolo in alto a destra dello schermo

Cambia l'interruttore di controllo degli accessi per la tua istanza:

1. Scegli il cassetto Impostazioni sul lato sinistro
2. Seleziona Applicazione
3. Aggiorna l'interruttore e fai clic su Salva impostazioni

Se l'impostazione è abilitata, il sistema filtrerà automaticamente le pagine di elenco delle eccezioni e dei consigli per mostrare solo quelle che sono state generate per un prodotto O un sito che corrisponde alla configurazione del controllo di accesso

Per gli utenti che hanno abilitato l'opzione «Concedi l'accesso completo a tutti i prodotti e i siti», l'interruttore della visualizzazione di accesso mostrerà comunque tutte le eccezioni e i consigli. Se un utente ha l'interruttore disabilitato ma non ha alcun prodotto o sito configurato, il sistema lo interpreta come se non avesse accesso a nessun prodotto o sito e quindi l'utente non vedrà nulla

Il filtro di visualizzazione degli accessi è considerato un tipo diverso di filtro e pertanto non verrà visualizzato nei chip di filtro nella pagina delle eccezioni e dei consigli. Gli utenti possono comunque applicare altri filtri nello stesso modo di prima, inclusi filtri per altri prodotti e siti

Gli utenti possono comunque accedere alle eccezioni e ai consigli per altri prodotti O siti se disattivano l'opzione di visualizzazione di accesso o dispongono del collegamento ipertestuale diretto ad essi

Configurazione delle connessioni al tuo ERP

Per consentire ad Amazon Connect Decisions di eseguire operazioni per tuo conto nel tuo sistema Enterprise Resource Planning (ERP), devi configurare una connessione che specifichi i parametri di connessione necessari e le credenziali che Amazon Connect Decisions deve utilizzare durante l'operazione.

Sistemi ERP supportati:

- SAP S/4HANA

Configurazione delle credenziali in Secrets Manager

1. Usando il tuo account, usa Secrets Manager per creare un segreto di Secrets Manager
   - Quando inserisci le credenziali in Secrets Manager, sostituisci i valori segnaposto riportati di seguito (`<username>`e`<password>`) con il nome utente e la password effettivi che Amazon Connect Decisions dovrebbe usare
   - Se usi la console, scegli `Other type of secret` `Secret Type`
   - Se inserisci i dettagli tramite la `Key/value pairs` scheda della console, inserisci 2 coppie:
     - Chiave:`username`; Valore: <*username*>
     - Chiave:`password`; Valore: <*password*>
   - Se usi la `Plaintext` scheda per inserire il segreto nella console, inserisci un oggetto JSON con le due coppie:

     ```
     {
       "Username": "<username>",
       "Password": "<password>"
     }
     ```
2. Crittografa il tuo segreto con una chiave AWS KMS, prendi nota dell'ID della chiave, poiché ti servirà nei passaggi successivi
3. Una volta creato il tuo segreto, prendi nota del relativo Amazon Resource Name (ARN), poiché ti servirà nei passaggi successivi

- ad esempio: `arn:aws:secretsmanager:<Region>:<AccountId>:secret:<SecretName>-<SixRandomCharacters>`

Configura le autorizzazioni sulla chiave KMS

Devi fornire le autorizzazioni necessarie affinché Amazon Connect Decisions possa accedervi e utilizzarlo.

1. Aggiorna la tua policy KMS per consentire ad Amazon Connect Decisions di accedere alla tua chiave tramite il ruolo dell'istanza
   - Nota: sostituisci <YourAccountNumber> e <YourInstanceID> con il tuo AWS account e l'ID dell'istanza 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. Aggiorna la policy in linea per il tuo ruolo di istanza per concedere l'autorizzazione sulla chiave
   - Nota: sostituisci <YourAccountNumber> e <YourSecretArn> <YourInstanceID> inserisci l'ARN segreto, l' AWS account e l'ID dell'istanza della catena AWS di fornitura.

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

Aggiorna la politica delle risorse di Secrets Manager per il tuo Secret

1. Aggiorna la politica delle risorse di Secrets Manager per il tuo Secret
   - Nota: sostituisci <YourSecretArn> con l'ARN del tuo segreto

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

Configurazione della connessione Amazon Connect Decisions

1. Nella tua istanza di Amazon Connect Decisions, vai alla pagina Gestione dei dati
2. Seleziona la `Connections` scheda
3. Fare clic sul pulsante `Create Connection`.
4. Nella `Create Connector` pagina, fai clic sul `Select` pulsante nella riga corrispondente al tipo di `SAP S/4HANA` connettore
5. Nella `Configure SAP S/4HANA API Connector` pagina inserisci le informazioni necessarie:
   - `Connection Name`: nome di connessione univoco
   - `API Endpoint URL`: l'URL dell'endpoint dell'API OData dell'istanza SAP (S/4HANA ad esempio:) `https://<hostname>:<port>`
   - `Client Number`: il numero del client SAP a 3 cifre (ad esempio:) `100`
   - `Secret ARN`: l'Amazon Resource Name (ARN) del segreto in Secrets Manager in cui sono archiviate le credenziali che devono essere utilizzate da Amazon Connect Decisions
6. Fai clic sul pulsante `Create Connector`

Configurazione delle impostazioni delle azioni

Amazon Connect Decisions ti consente di controllare i tipi di azioni da offrire per eseguire operazioni per tuo conto nel tuo sistema Enterprise Resource Planning (ERP). Per impostazione predefinita, tutti i tipi di azione sono disabilitati e devi abilitare questa funzionalità per ogni tipo di azione desiderato.

> **Note**
>
> L'abilitazione del supporto per un determinato tipo di azione controlla se l'opzione di Amazon Connect Decisions che esegue l'azione per tuo conto verrà presentata in tutto il sistema (ad esempio: quando si esamina un Insight con una raccomandazione del tipo specificato). Amazon Connect Decisions non eseguirà queste azioni (anche quando il supporto è abilitato) finché non accetti la raccomandazione specifica.

Tipi di azioni supportati:

- Crea ordine di acquisto
- Aggiorna ordine di acquisto

- Annulla ordine di acquisto

Configura il supporto delle azioni per ogni tipo di azione:

1. Nella tua istanza di Amazon Connect Decisions, vai alla pagina Gestione dei dati
2. Seleziona la `Actions` scheda
3. Trova il tipo di azione che desideri configurare nell'elenco
4. Per abilitare il supporto per il tipo di azione:
   - Seleziona una delle connessioni elencate nel menu a discesa per quel tipo di azione
   - Nota: il menu a discesa mostrerà solo le connessioni disponibili che sono state configurate di un tipo che supporta la `Actions` funzionalità (ad esempio:) `SAP S/4HANA`
5. Per disabilitare il supporto per il tipo di azione:
   - Seleziona `No connection` nel menu a discesa quel tipo di azione
6. Fai clic `Save` per salvare le modifiche

Sicurezza

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi in Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. Third-party i revisori testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei programmi di conformità AWS. Per ulteriori informazioni sui programmi di conformità che si applicano alle decisioni di Amazon Connect, consulta AWS Services in Scope by Compliance Program.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della propria azienda e le leggi e normative vigenti.

Questa documentazione aiuta a comprendere come applicare il modello di responsabilità condivisa quando si utilizza Amazon Connect. I seguenti argomenti mostrano come configurare Amazon Connect Decisions per raggiungere i tuoi obiettivi di sicurezza e conformità.

Protezione dei dati

Il modello di responsabilità AWS condivisa si applica alla protezione dei dati in Amazon Connect Decisions. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutto il AWS cloud. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile delle attività di configurazione e gestione della sicurezza per i AWS servizi che utilizza. Per ulteriori informazioni sulla privacy dei dati, consulta Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post sul blog AWS Shared Responsibility Model e GDPR sull'AWS Security Blog.

Ai fini della protezione dei dati, ti consigliamo di proteggere le credenziali AWS dell'account e di configurare i singoli utenti con AWS Identity and Access Management (IAM). In questo modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere il proprio lavoro. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l’autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. È consigliabile TLS 1.2 o versioni successive.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno AWS dei servizi.
- Utilizza servizi di sicurezza gestiti avanzati come Amazon Macie, che aiuta a scoprire e proteggere i dati sensibili archiviati in Amazon Simple Storage Service.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Amazon Connect Decisions o altri AWS servizi utilizzando la console di AWS gestione, l'API, AWS Command Line Interface (AWS CLI) o AWS gli SDK. Tutti i dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i registri di fatturazione o diagnostica.

Crittografia dei dati

Questo argomento fornisce informazioni specifiche su Amazon Connect Decisions sulla crittografia in transito e sulla crittografia a riposo.

Crittografia dei dati in transito

Tutte le comunicazioni tra i clienti e Amazon Connect Decisions e tra Amazon Connect Decisions e le sue dipendenze downstream sono protette tramite connessioni TLS 1.2 o versioni successive.

Crittografia dei dati a riposo

Amazon Connect Decisions archivia i dati inattivi utilizzando DynamoDB e Amazon Simple Storage Service (Amazon S3). Per impostazione predefinita, i dati inattivi vengono crittografati utilizzando soluzioni di AWS crittografia. Amazon Connect Decisions crittografa i tuoi dati utilizzando chiavi AWS di crittografia di proprietà di AWS Key Management Service (AWS KMS). Non devi intraprendere alcuna azione per proteggere le chiavi AWS gestite che crittografano i tuoi dati. Per ulteriori informazioni, consulta le chiavi di proprietà di AWS nella AWS KMS Developer Guide.

Se modifichi la chiave KMS utilizzata per crittografare i dati sulla tua istanza Amazon Connect Decisions nella AWS console, devi creare una nuova istanza per iniziare a utilizzare la nuova chiave per crittografare i tuoi dati. Tutti i dati crittografati con la chiave precedente non verranno conservati e solo i dati verranno crittografati con la chiave aggiornata. Se desideri mantenere i dati utilizzati con un metodo di crittografia precedente, puoi tornare alla chiave che utilizzavi durante quelle conversazioni.

Le tue conversazioni con Amazon Connect Decisions sulla webapp e nelle applicazioni di chat sono crittografate solo con AWS-owned chiavi.

Cross-region elaborazione

Amazon Connect Decisions è basato su Amazon Bedrock e utilizza l'inferenza interregionale (CRIS) per distribuire il traffico tra diverse AWS regioni e migliorare le prestazioni e l'affidabilità dell'inferenza del modello di linguaggio di grandi dimensioni (LLM). Con l'inferenza tra regioni, ottieni:

- Maggiore throughput e resilienza durante i periodi di forte domanda
- Prestazioni migliorate
- Accesso alle funzionalità e alle caratteristiche di Amazon Connect Decisions lanciate di recente che si basano sui più potenti LLM ospitati su Amazon Bedrock

Cross-region l'inferenza funziona in modo diverso in base alla AWS regione in cui viene creata l'istanza Amazon Connect Decisions.

Per tutte le istanze create nella regione geografica degli Stati Uniti, Amazon Connect Decisions utilizzerà Global CRIS. Ciò significa che le richieste di inferenza verranno indirizzate alle AWS regioni commerciali supportate in tutto il mondo, ottimizzando le risorse disponibili e consentendo una maggiore produttività del modello. Consulta la guida per l'utente di Amazon Bedrock per ulteriori informazioni su Global CRIS.

Per tutte le istanze create nella regione geografica dell'UE, Amazon Connect Decisions utilizzerà Geographic CRIS. Ciò significa che le richieste di inferenza vengono conservate all'interno delle AWS regioni che fanno parte della geografia in cui risiedono originariamente i dati. Consulta la guida per l'utente di Amazon Bedrock per ulteriori informazioni su Geographic CRIS.

Ad esempio, una richiesta effettuata da un'istanza Amazon Connect Decisions creata nella regione Stati Uniti orientali (Virginia settentrionale) (us-east-1) può essere instradata verso AWS qualsiasi regione a livello globale come Asia Pacifico (Sydney) (ap-southeast-2). Tuttavia, una richiesta effettuata da un'istanza di Amazon Connect Decisions creata nella regione Europa (Irlanda) (eu-

west-1) viene indirizzata AWS a una regione dell'UE come Europa (Francoforte) (eu-central-1). Per ulteriori informazioni, consulta Regioni supportate per Amazon Connect Decisions.

Sebbene l'inferenza tra regioni non modifichi il luogo in cui vengono archiviati i dati, le richieste e i risultati di output potrebbero spostarsi al di fuori della regione in cui si trovano originariamente i dati. Tutti i dati vengono crittografati durante la trasmissione attraverso la rete sicura di Amazon. L'utilizzo dell'inferenza tra regioni non prevede costi aggiuntivi. Per informazioni su dove vengono archiviati i dati quando usi Amazon Connect Decisions, consulta la sezione Protezione dei dati in Amazon Connect Decisions.

IAM per decisioni su Amazon Connect

AWS Identity and Access Management (IAM) è un servizio AWS che permette agli amministratori di controllare in modo sicuro l'accesso alle risorse AWS. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse Amazon Connect Decisions. IAM è un servizio AWS che è possibile utilizzato senza alcun costo aggiuntivo.

Come funziona IAM con Amazon Connect Decisions?

Prima di utilizzare IAM per gestire l'accesso ad Amazon Connect Decisions, scopri quali funzionalità IAM sono disponibili per l'uso con Amazon Connect Decisions. Per avere una visione di alto livello di come Amazon Connect Decisions e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta i servizi AWS che funzionano con IAM nella IAM User Guide.

Identity-based politiche per Amazon Connect Decisions

Supporta le policy basate sull'identità: sì

Identity-based le policy sono documenti relativi alle policy di autorizzazione JSON che puoi allegare a un'identità, ad esempio un utente IAM, un gruppo di utenti o un ruolo. Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente di IAM.

Con le policy basate sull'identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente IAM.

Resource-based politiche all'interno di Amazon Connect Decisions

Supporta le policy basate su risorse: no

Resource-based le politiche sono documenti di policy JSON che alleghi a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy di bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. In una policy basata sulle risorse è obbligatorio specificare un'entità principale. I principali possono includere account, utenti, ruoli, utenti federati o servizi. AWS

Per consentire l'accesso multi-account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata sulle risorse. Per ulteriori informazioni, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Azioni politiche per Amazon Connect Decisions

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso in una policy. Includere le operazioni in una policy per concedere le autorizzazioni di eseguire l'operazione associata.

Le azioni politiche in Amazon Connect Decisions utilizzano il seguente prefisso prima dell'azione:

```
scn
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

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

Risorse politiche per Amazon Connect Decisions

Supporta le risorse relative alle policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

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

Chiavi delle condizioni delle politiche per Amazon Connect Decisions

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. È possibile compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta. Per visualizzare tutte le chiavi di condizione AWS globale, consulta le chiavi di contesto delle condizioni globali di AWS nella IAM User Guide.

Utilizzo di credenziali temporanee con Amazon Connect Decisions

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono un accesso a breve termine alle AWS risorse e vengono create automaticamente quando utilizzi la federazione o cambi ruolo. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza temporanee nei servizi IAM e AWS che funzionano con IAM nella IAM User Guide.

Sessioni di accesso inoltrato per Amazon Connect Decisions

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Le sessioni di accesso inoltrato (FAS) utilizzano le autorizzazioni del principale che chiama un AWS servizio, combinate con il servizio richiedente per effettuare richieste ai AWS servizi downstream. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

Ruoli di servizio per Amazon Connect Decisions

Supporta i ruoli di servizio: sì

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta Creare un ruolo per delegare le autorizzazioni a un AWS servizio nella Guida per l'utente IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità di Amazon Connect Decisions. Modifica i ruoli di servizio solo quando Amazon Connect Decisions fornisce indicazioni in tal senso.

Identity-based esempi di policy

Per impostazione predefinita, gli utenti e i ruoli non sono autorizzati a creare o modificare risorse Amazon Connect Decisions. Inoltre, non possono eseguire attività utilizzando la console di AWS gestione, l'interfaccia a riga di AWS comando (AWS CLI) o AWS l'API. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per scoprire come creare una policy basata sull'identità IAM utilizzando questi esempi di documenti di policy JSON, consulta Creating IAM policies nella IAM User Guide.

Politica IAM di gestione delle istanze

Di seguito è riportata la policy IAM necessaria per creare, aggiornare o eliminare le istanze tramite la console o l'API pubblica (sono escluse tutte le operazioni Webapp).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "scn:*",
            "Resource": "*",
            "Effect": "Allow"
        },
```

```
        {
            "Action": [
                "s3:GetObject",
                "s3:PutObject",
                "s3:ListBucket",
                "s3:CreateBucket",
                "s3:PutBucketVersioning",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutEncryptionConfiguration",
                "s3:PutBucketPolicy",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketPublicAccessBlock",
                "s3:DeleteObject",
                "s3:ListAllMyBuckets",
                "s3:PutBucketOwnershipControls",
                "s3:PutBucketNotification",
                "s3:PutAccountPublicAccessBlock",
                "s3:PutBucketLogging",
                "s3:PutBucketTagging"
            ],
            "Resource": "arn:aws:s3:::aws-supply-chain-*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "cloudtrail:CreateTrail",
                "cloudtrail:PutEventSelectors",
                "cloudtrail:GetEventSelectors",
                "cloudtrail:StartLogging"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "events:DescribeRule",
                "events:PutRule",
                "events:PutTargets"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
```

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

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

Best practice per le policy

Identity-based le politiche determinano se qualcuno può creare, accedere o eliminare le risorse Amazon Connect Decisions nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l'account AWS . Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy gestite di AWS che concedono autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo account AWS . Consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente di AWS specifiche per i propri casi d'uso. Per ulteriori informazioni, consulta AWS managed policies o AWS managed policies for job functions nella IAM User Guide.
- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite un AWS servizio specifico, ad esempio CloudFormation. Per maggiori informazioni, consultare la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente di IAM.
- Richiesta dell'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o utenti root nel tuo account AWS , attiva MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungere le condizioni MFA alle policy. Per

maggiori informazioni, consultare Protezione dell'accesso API con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Risoluzione dei problemi di IAM

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Amazon Connect Decisions e IAM.

Non sono autorizzato a eseguire un'azione in Amazon Connect Decisions

Se la console di AWS gestione non è autorizzata a eseguire un'azione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è la persona da cui si sono ricevuti il nome utente e la password.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa `my-example-widget` fittizia ma non dispone di autorizzazioni `scn:GetWidget` fittizie.

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

In questo caso, Mateo chiede al suo amministratore di aggiornare le policy per poter accedere alla risorsa `my-example-widget` mediante l'operazione `scn:GetWidget`.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo ad Amazon Connect Decisions.

Alcuni AWS servizi consentono di trasferire un ruolo esistente a quel servizio anziché creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Amazon Connect Decisions. Tuttavia, l'azione richiede

che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per trasmettere il ruolo al servizio.

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

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire l'accesso a persone esterne al mio AWS account per accedere alle mie risorse Amazon Connect Decisions

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo degli accessi (ACL), utilizzare tali policy per concedere alle persone l'accesso alle proprie risorse.

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se Amazon Connect Decisions supporta queste funzionalità, consulta Come Amazon Connect Decisions funziona con IAM.
- Per scoprire come fornire l'accesso alle tue risorse su tutti AWS gli account di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro AWS account di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse ad AWS account di terze parti, consulta Fornire l'accesso agli AWS account di proprietà di terze parti nella IAM User Guide.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente di IAM.

Third-party sottoprocessori

Amazon Connect Decisions utilizza Boomi, un'API di terze parti, per consentire l'esecuzione di azioni per tuo conto in sistemi esterni. Quando utilizzi una funzionalità di Amazon Connect Decisions che si

collega ai tuoi sistemi di terze parti, ci autorizzi a utilizzare Boomi come middleware di integrazione per trasmettere ed elaborare i tuoi dati crittografati; i tuoi dati non vengono archiviati separatamente all'interno di Boomi.

Per saperne di più su Boomi e su come funziona, consulta la documentazione pubblica di Boomi.

Regioni supportate

Questa pagina descrive le AWS regioni in cui puoi usare Amazon Connect Decisions. Per ulteriori informazioni sulle AWS regioni, consulta Specificare AWS le regioni che il tuo account può utilizzare nella Guida di riferimento alla gestione degli AWS account.

I tuoi dati potrebbero essere elaborati in una regione diversa da quella in cui utilizzi Amazon Connect Decisions. Per informazioni sull'elaborazione tra regioni in Amazon Connect Decisions, consulta Cross-region elaborazione. Per informazioni su dove vengono archiviati i dati durante l'elaborazione, consulta Protezione dei dati.

Regioni supportate

Amazon Connect Decisions è disponibile nella Console di AWS gestione, nella AWS Console Mobile Application, nel AWS sito Web e nel sito Web di AWS documentazione nelle seguenti AWS regioni. Queste Regioni sono abilitate per impostazione predefinita, e quindi non è necessario abilitarle prima dell'uso. Per ulteriori informazioni, consulta Regions that are enabled by default.

Utilizzi Amazon Connect Decisions nelle seguenti regioni.

AWS Nome della regione	Nome in codice	Geografia (Stati Uniti, UE, ecc.)
Stati Uniti orientali (Virginia settentrionale)	us-east-1	US
Europa (Irlanda)	eu-west-1	UE

Risoluzione dei problemi

In caso di problemi durante la configurazione o l'uso quotidiano di Amazon Connect Decisions, questa sezione fornisce indicazioni per aiutarti a diagnosticare e risolvere i problemi più comuni. Inizia identificando la categoria che meglio corrisponde al problema riscontrato, quindi segui i passaggi per la risoluzione dei problemi nella pagina pertinente. Se non sei sicuro della categoria adatta, inizia con i problemi di configurazione comuni, che copre la più ampia gamma di problemi di configurazione iniziale.

Problemi di configurazione comuni

Errori di integrità referenziale: «i valori product_id non corrispondono a nessun id nel set di dati del prodotto»

La causa più comune sono gli spazi bianchi finali nei campi ID. I sistemi di origine che esportano da database a larghezza fissa spesso riempiono i campi di stringa con spazi. Il master del prodotto può avere ID puliti («MAT604") mentre il file della riga d'ordine ha ID riempiti («MAT604 «). Il sistema esegue una rigorosa corrispondenza delle stringhe, quindi queste non si uniranno.

Correzione: aggiungi TRIM () a tutti i campi ID stringa nelle trasformazioni SQL del flusso di dati. Applicalo a product_id, ship_from_site_id, customer_tpartner_id e qualsiasi altra chiave di join. Controlla anche le incongruenze di citazione tra i file. Quando riesporti i file CSV, usa QUOTE_ALL per evitare problemi di inferenza dei tipi in cui gli ID dall'aspetto numerico (ad esempio, «111613") vengono trattati come numeri interi in un file e stringhe in un altro.

Prevenzione: come procedura predefinita, elimina sempre tutti i campi ID nelle trasformazioni SQL, anche se oggi non riscontri il problema. I dati di origine possono cambiare tra le esportazioni.

Prodotti nella cronologia degli ordini non presenti nella scheda prodotto

La cronologia degli ordini contiene spesso prodotti che non sono presenti nella scheda prodotto corrente (prodotti fuori produzione, articoli monouso, SKU di prova). Il sistema rifiuterà l'intero file dell'ordine se un product_id non ha un record anagrafico del prodotto corrispondente.

Correzione: (a) create righe stub nella scheda tecnica del prodotto per i prodotti mancanti con un numero minimo di campi obbligatori (id, description, base_uom) oppure (b) filtra la cronologia degli ordini per includere solo i prodotti presenti nella scheda prodotto. L'opzione (a) è preferibile perché

conserva la cronologia della domanda che può essere utile per il rilevamento della provenienza e delle tendenze.

Errori di analisi CSV durante il caricamento della scheda tecnica del prodotto

Le descrizioni dei prodotti contenenti virgole, virgolette o caratteri speciali possono interrompere l'analisi del file CSV. Potresti visualizzare errori come «Previsti 17 campi, visto 19" su righe specifiche.

Correzione: Re-export il file con le citazioni corrette (QUOTE_ALL). Controlla le righe mancanti specifiche per le virgole incorporate nei campi della descrizione.

I dati non vengono visualizzati dopo il caricamento

- Verifica che il formato del file non sia cambiato (estensione, intestazioni di colonna, codifica).
- Verifica che i nomi e le estensioni dei file corrispondano allo schema previsto: rinominare .csv in .csv000 o simili interromperà l'ingestione.
- Attendi fino a 30 minuti per completare l'inserimento dei dati dopo il caricamento.
- Se le intestazioni delle colonne cambiano tra i caricamenti (ad esempio, le colonne denominate da month/year), è necessaria una fase di pre-elaborazione prima del caricamento.

PIV non si aggiorna dopo l'aggiornamento dei dati

- Il PIV si attiva circa 15 minuti dopo il completamento dell'ingestione e impiega circa 20-30 minuti per funzionare.
- End-to-end dal caricamento dei dati al nuovo PIV: circa 1—1,5 ore.
- Se il PIV non si aggiorna da più di 24 ore, contatta l'assistenza.

Il numero di eccezioni sembra troppo alto o troppo basso

- Troppo alto: la soglia potrebbe essere troppo bassa oppure un singolo prodotto+sito potrebbe generare più eccezioni per date diverse. Contatta l'assistenza per rivedere la configurazione delle regole.
- Troppo bassa: la soglia potrebbe essere troppo restrittiva o potrebbero mancare i dati richiesti (ad esempio previsioni, livelli di inventario) per alcuni prodotti.

Spot-check alcuni prodotti che conosci bene e confronta ciò che mostra il sistema con quello del tuo sistema di origine.

Nessun impatto finanziario relativo alle eccezioni

L'impatto finanziario richiede che il costo unitario sia inserito nei dati di prodotto. Se il costo è mancante o è pari a zero per un prodotto, non verrà visualizzato alcun valore in dollari. Rivolgiti al tuo team di assistenza sulla copertura dei dati relativi ai costi: un approccio a cascata che abbraccia più campi di costo in genere offre la migliore copertura.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.