aws

管理員指南

Amazon Connect 決策

Amazon Connect 決策: 管理員指南

Table of Contents

什麼是 Amazon Connect 決策

Amazon Connect Decisions 是一種供應鏈規劃和智慧解決方案，與 AI 團隊成員一起合作，將需求訊號協調為共識預測、產生限制感知供應計劃，並主動監控您的操作，以防止問題、解決問題，並識別持續改進的根本原因。

AI 團隊成員會根據您的工作方式進行調整：由您的操作程序和規則驅動、與現有系統整合，並從從從業人員的決策中學習。它利用 Amazon 供應鏈專業知識，從第一天開始提供有效的計劃和建議。

您領導 AI 代理器團隊，負責處理協調和執行動作，讓您專注於推動服務水準和營運資金效率的策略決策。

優勢

適應您的業務

AI 團隊成員會適應您的業務、系統和決策，快速在現有的工作流程中實現轉型。在營運程序和業務規則的驅動下，團隊成員會使用您現有的規劃和 ERP 系統。他們從規劃者的決策中學習，與您的優先事項保持一致並整理知識，讓您的營運隨著時間變得更好，而且每個團隊成員都更有效率。

保持領先

領導 AI 代理器團隊全年無休地處理協調工作 - 協調需求訊號、產生限制感知計劃，以及執行已核准的動作。團隊成員也會偵測手動分析看不到的模式，例如在數千個 SKUs 之間串聯供應商中斷或庫存不一致，並在問題發生之前浮現重要的事物。規劃人員從被動消防轉向主動規劃，透過推動業務成果的策略決策執行更有效的操作並改善服務水準。

從第一天開始建立信任

AI 團隊成員受到 30 多年來監督超過 400M個 Amazon SKUs 的科學技術支援，並配備專門的供應鏈工具。您的團隊受益於全球最複雜的供應鏈網路之一所提供的領域專業知識，提供可行的洞見和out-of-the-box，並具有明確、可解釋的可信任和驗證理由。

功能

自適應智慧

AI 團隊成員透過持續迴圈從每個計畫和決策中學習：觀察模式、偵測重要事項、建議動作，以及執行核准的決策。這會讓知識機構化 - 當規劃人員離開時，專業知識會保留；新成員從第一天開始就有生產力，改善成果，無需手動重新訓練。

需求智慧

AI 團隊成員可動態協調使用 Amazon 資料訓練的 18+ 個預測工具和基礎模型，並在 SKU 層級自動最佳化。從第一天產生準確的預測，即使歷史記錄有限。透過共識規劃協調統計預測、客戶承諾和跨職能輸入，同時持續監控準確性。

供應智慧

AI 團隊成員會產生具前瞻性的供應計畫（預覽），並以智慧方式將例外狀況叢集成按影響排名的策略決策。在整個網路中執行限制感知規劃的最佳化模型。全年無休監控操作，找出重要事項，然後直接在現有系統中執行核准的決策，將週期從數週縮短為數小時。

客服人員加入

採用 AI 技術的入門客服人員會透過自然語言對話引導您完成設定。透過 JDBC 或 Amazon S3 連接分段資料，為 Connect Decisions 做好準備，並在問題影響預測之前自動標記問題。使用即時預覽以純語言設定業務規則和政策 - 在數週內開始運作，而不是數月。

開始使用

在本節中，您可以了解如何建立 Amazon Connect Decisions 執行個體、授予使用者許可角色，以及登入 Amazon Connect Decisions Web 應用程式。

使用 Amazon Connect Decisions 的先決條件

建立 Amazon Connect Decisions 執行個體之前，請確定您已完成下列步驟：

- 您有 AWS 帳戶。若要建立 AWS 帳戶，請參閱設定 AWS 帳戶。
- 確定已啟用 IAM Identity Center。若要啟用 IAM Identity Center，請參閱啟用 IAM Identity Center。
- IAM Identity Center 執行個體必須在您要建立 Amazon Connect Decisions 執行個體的相同區域中啟用。Amazon Connect Decisions 僅支援美國東部（維吉尼亞北部）和歐洲（愛爾蘭）區域。
- 如果 Amazon Connect Decisions 執行個體與您現有的 IAM Identity Center 區域不在同一個區域中，請聯絡我們以取得進一步協助。
- 您必須在 IAM Identity Center 執行個體中至少有一個使用者，才能指派 做為 Amazon Connect Decisions 管理員。您可以將作用中目錄連線至 IAM Identity Center。如需詳細資訊，請參閱連線至 Microsoft AD 目錄。
- 將需要存取 Amazon Connect Decisions 的任何其他使用者新增至 IAM Identity Center。
- 您需要 AWS Key Management Service (AWS KMS) 才能建立執行個體。Amazon Connect Decisions 使用此 AWS KMS 金鑰來加密 Amazon Connect Decisions 中的所有資料。如需 AWS KMS 金鑰的資訊，請參閱建立金鑰。
- 如果您想要啟用 動作功能，則需要設定您用來維護相關資料之系統的連線，並提供登入資料供 Amazon Connect Decisions 使用。如需進一步協助，請聯絡我們。

Amazon Connect Decisions 支援的瀏覽器

使用 Amazon Connect Decisions 之前，請使用下表驗證您的瀏覽器是否受支援。

瀏覽器	支援的版本
Google Chrome	最近三個版本。
Mozilla Firefox ESR	版本在 Firefox 的生命週期結束日期之前都會受到支援。有關詳細資訊，請參見 Firefox ESR 發布行事曆。

瀏覽器	支援的版本
Mozilla Firefox	最近三個版本。
Microsoft Edge 和 Edge Chromium	84 版及更新版本。
Safari	macOS 上的 Safari 10 或更新版本。

Amazon Connect Decisions 支援的語言

Amazon Connect Decisions 支援下列語言：

- 英文 (美國)

設定 AWS 帳戶

使用本節來建立 AWS 帳戶和建立 IAM 使用者。如需建立 AWS 帳戶的最佳實務資訊，請參閱建立您的最佳實務 AWS 環境。

註冊 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立一個帳戶。

註冊 AWS 帳戶

1. 開啟 https://portal.aws.amazon.com/billing/signup。
2. 請遵循線上指示進行。

   部分註冊程序需接收來電或簡訊，並在電話鍵盤輸入驗證碼。

   當您註冊 AWS 帳戶時，會建立 AWS 帳戶根使用者。根使用者有權存取該帳戶中的所有 AWS 服務和資源。作為安全最佳實務，請將管理存取權指派給使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

AWS 會在註冊程序完成後傳送確認電子郵件給您。您可以隨時登錄 https://aws.amazon.com/ 並選擇我的帳戶，以檢視您目前的帳戶活動並管理帳戶。

建立具有管理存取權的使用者

註冊 AWS 帳戶後，請保護 AWS 帳戶根使用者、啟用 AWS IAM Identity Center，並建立管理使用者，讓您不會將根使用者用於日常任務。

保護 AWS 您的帳戶根使用者

1. 選擇根使用者並輸入您的帳戶 AWS 電子郵件地址，以帳戶擁有者身分登入 AWS 管理主控台。在下一頁中，輸入您的密碼。

   如需使用根使用者登入的說明，請參閱 登入使用者指南中的以根使用者身分AWS 登入。
2. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

   如需說明，請參閱《IAM 使用者指南》中的為 AWS 您的帳戶根使用者 （ 主控台 ） 啟用虛擬 MFA 裝置。

建立具有管理存取權的使用者

1. 啟用 IAM Identity Center。

   如需說明，請參閱《IAM Identity Center AWS 使用者指南》中的啟用 AWS IAM Identity Center。
2. 在 IAM Identity Center 中，將管理存取權授予使用者。

   如需使用 IAM Identity Center 目錄做為身分來源的教學課程，請參閱《IAM Identity Center 使用者指南》中的使用預設 IAM Identity Center 目錄設定使用者存取權。 AWS

以具有管理存取權的使用者身分登入

- 若要使用您的 IAM Identity Center 使用者簽署，請使用建立 IAM Identity Center 使用者時傳送至您電子郵件地址的簽署 URL。

  如需使用 IAM Identity Center 使用者登入的說明，請參閱 登入使用者指南中的登入 AWS 存取入口網站。 AWS

指派存取權給其他使用者

1. 在 IAM Identity Center 中，建立一個許可集來遵循套用最低權限的最佳實務。

   如需說明，請參閱《AWS IAM Identity Center 使用者指南》中的建立許可集。

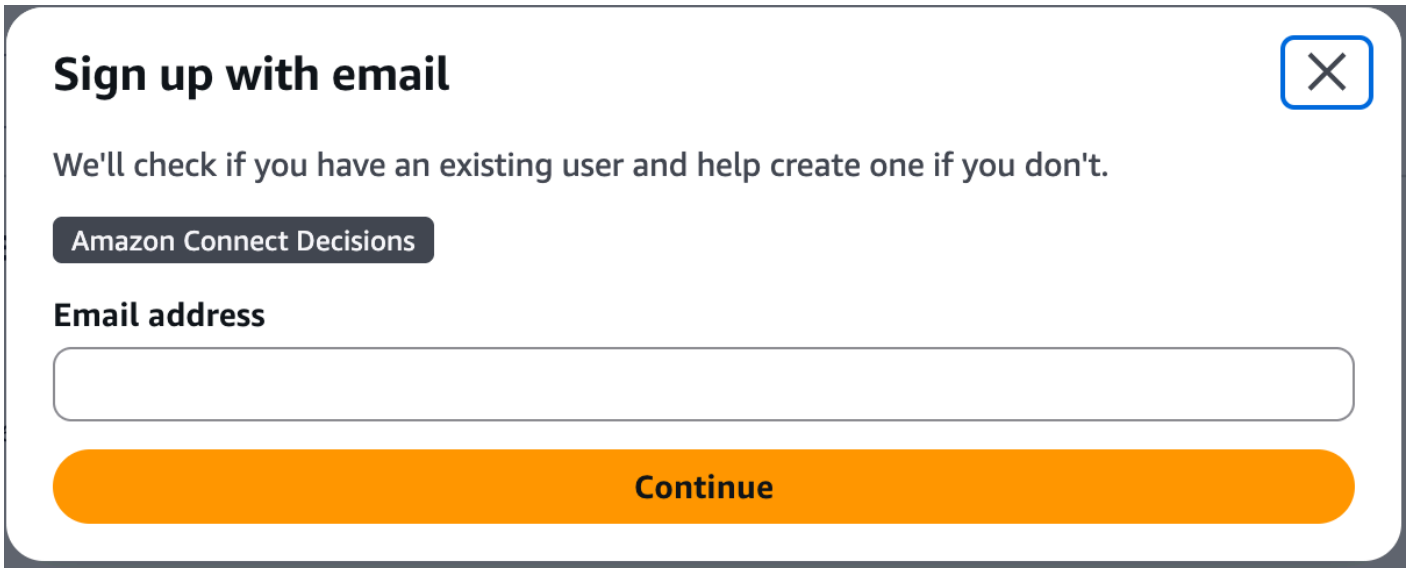
2. 將使用者指派至群組，然後對該群組指派單一登入存取權。

   如需說明，請參閱《AWS IAM Identity Center 使用者指南》中的新增群組。

設定 AWS Identity Center 整合

若要建立執行個體並使用 Amazon Connect Decisions 服務，您需要連接現有的 IAM Identity Center 使用者設定檔或建立新的設定檔。

1. 開啟 Amazon Connect Decisions 主控台。您也可以從主要 AWS 管理主控台搜尋「Amazon Connect Decisions」。
2. 如有必要，請選取主控台頂端的選取區域來變更 AWS 區域。 從下拉式清單中選擇您的區域。
3. 選取建立 Amazon Connect Decisions 執行個體。隨即顯示通知。



4. 輸入您的電子郵件地址，然後選取繼續。IdC 將驗證電子郵件是否符合現有的使用者。
5. 執行以下任意一項：
   - 如果 IdC 將電子郵件地址與使用者相符 – 選取連接您的身分來源並加入您的團隊。

     > **Note**
     >
     > 如果您的組織具有已建立的 IdC 執行個體，而您想要將其用於 Amazon Connect Decisions，則可以使用此執行個體。

   - 如果 IdC 找不到與現有使用者的相符項目 – 會顯示建立新使用者通知。繼續下一個步驟。
6. 在通知中，輸入以下內容，然後選取繼續：

- 電子郵件地址
- 名字
- 姓氏

IdC 會自動建立使用者，並將其新增為 Amazon Connect Decisions 管理員。

7. 執行以下任意一項：
   - 若要使用標準組態建立執行個體 – 選取建立。請參閱使用標準組態。
   - 若要使用自訂組態建立執行個體 – 在進階設定中選取編輯。請參閱使用進階組態。

與 IAM Identity Center 搭配使用時，Amazon Connect Decisions 會從 IAM Identity Center 目錄擷取「使用者名稱」和「電子郵件」欄位。這些屬性都不會原生儲存在 Amazon Connect Decisions 執行個體中，且一律會在執行時間擷取。根據預設，Amazon Connect Decisions 會使用 AWS 擁有的 KMS 金鑰來加密這些靜態身分屬性。Amazon Connect Decisions 不支援客戶受管 KMS 金鑰。如果您在 IAM Identity Center AWS 執行個體中刪除使用者，Amazon Connect Decisions 也會從執行個體中刪除該使用者。

管理您的 Amazon Connect Decisions 執行個體

在 Amazon Connect Decisions 中建立執行個體會建立專用環境，以進行供應鏈管理和分析。若要設定執行個體，您可以設定基本詳細資訊、建立設定，以及定義初始使用者存取許可。

只有 AWS 管理主控台管理員可以建立執行個體。建立 Amazon Connect Decisions 執行個體的 AWS 管理主控台管理員應擁有身分型政策範例下列出的所有許可。此管理員應邀請 IAM 使用者做為 Amazon Connect Decisions 管理員來管理 Amazon Connect Decisions。

以下頁面會詳細說明建立和刪除執行個體的程序。

建立您的執行個體

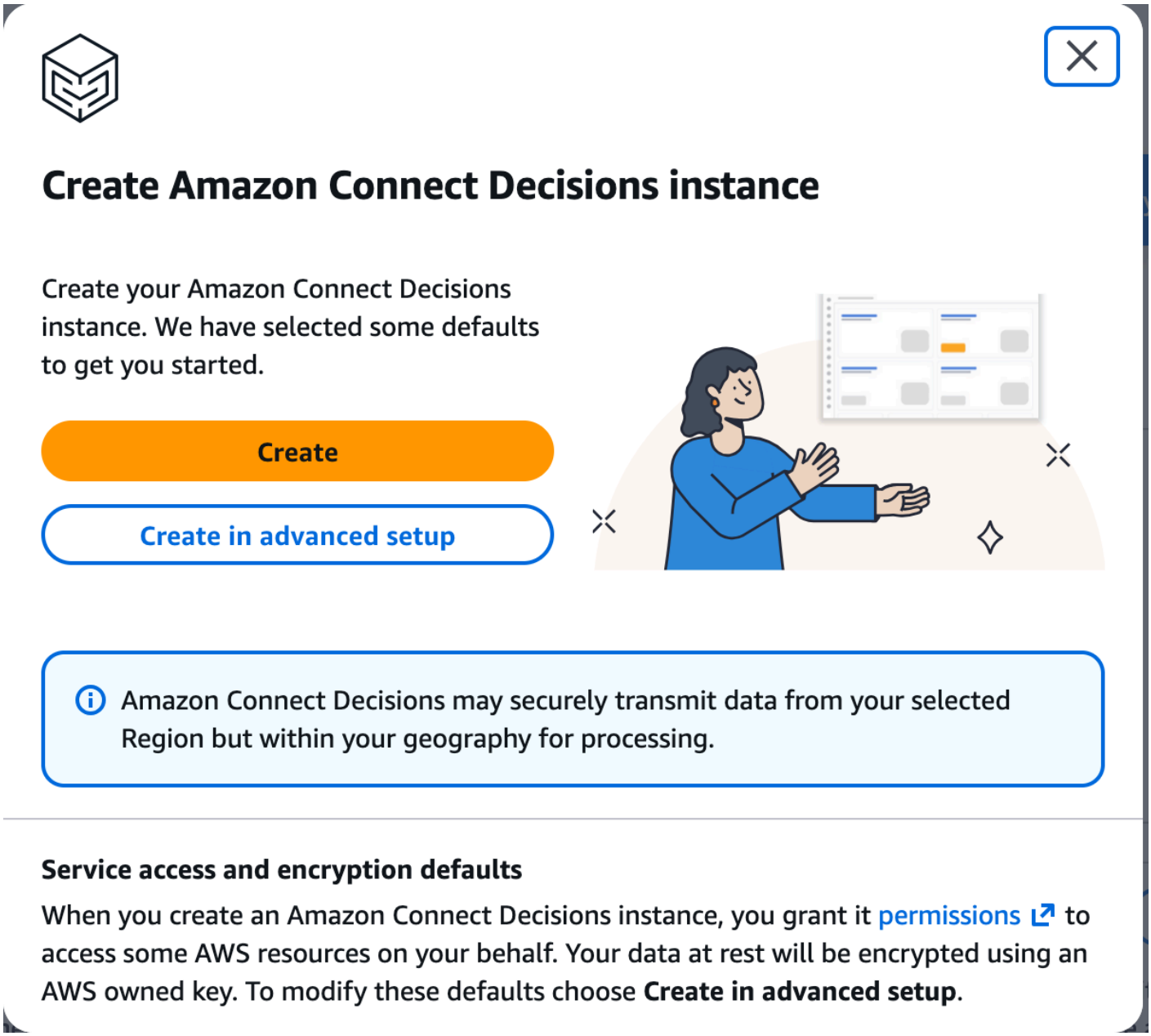
您可以使用兩種方法之一建立執行個體：標準組態或進階組態。標準組態使用自動化程序，可使用預設參數快速建立執行個體。進階組態可讓您透過設定自己的參數來自訂執行個體。

使用標準組態

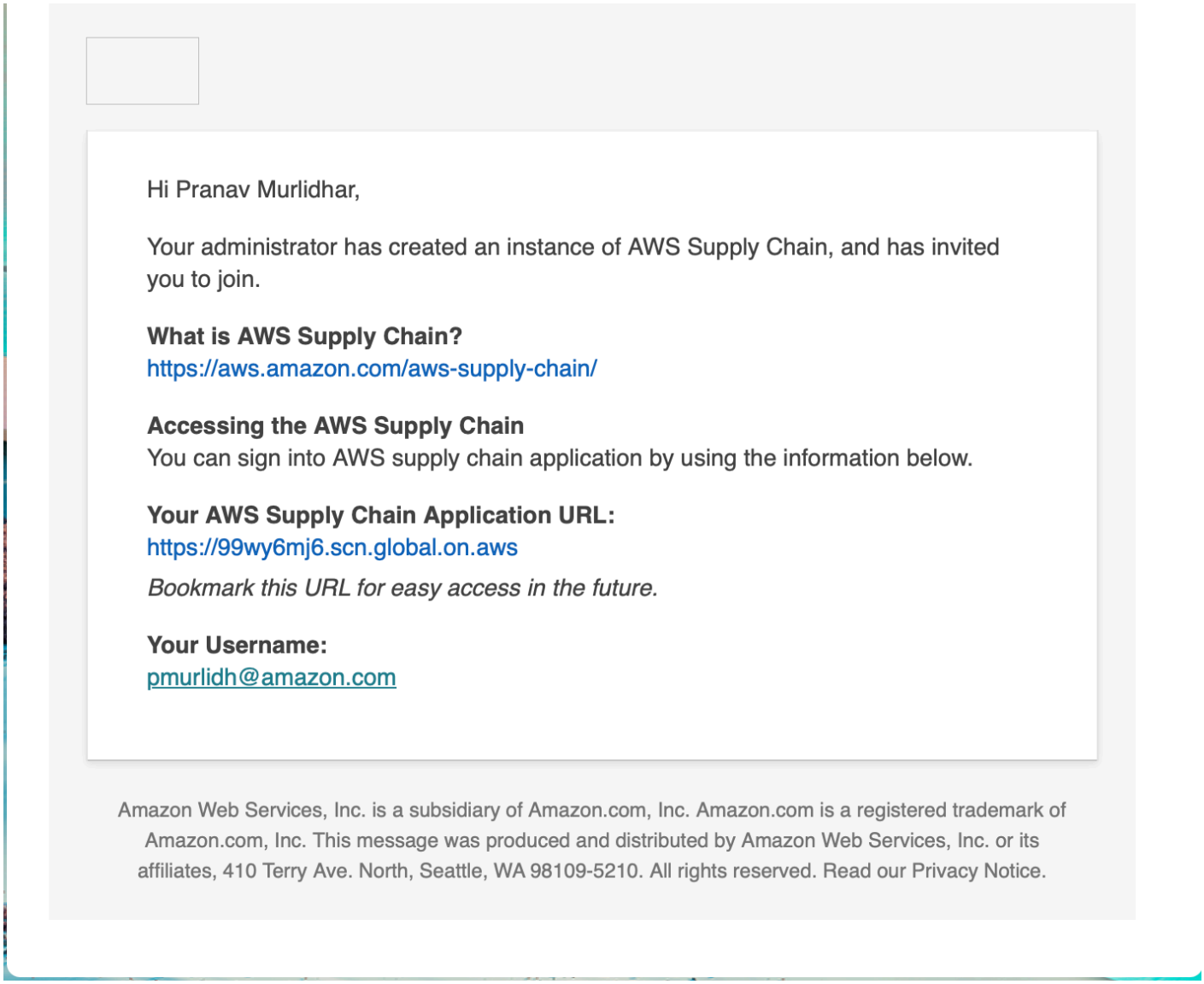
標準組態會使用預設的安全性和加密設定來建立 Amazon Connect Decisions 執行個體。執行個體在 AWS 地理區域中運作。如需區域的詳細資訊，請參閱《IAM 使用者指南》中的區域和端點，以及《AWS 一般參考》中的區域端點。

若要使用預設參數的標準組態建立 Amazon Connect Decisions 執行個體，請遵循下列步驟。

1. 選取建立。



2. 檢查您的電子郵件是否有下列項目：
   - 來自 IdC 團隊的電子郵件。
   - Identity Management 團隊的電子郵件。

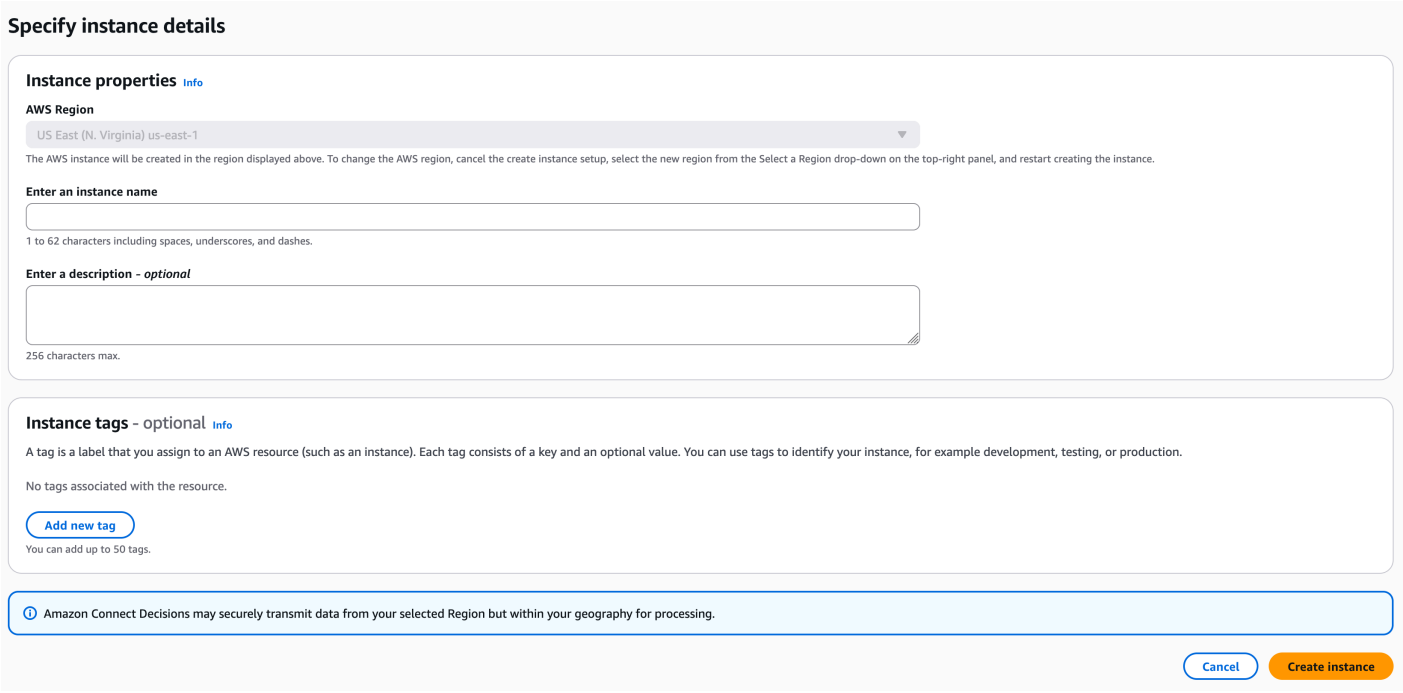


3. 收到邀請電子郵件後，請登入 Amazon Connect Decisions。請參閱登入 Amazon Connect Decisions Web 應用程式。

使用進階組態

進階組態可讓您透過設定自己的參數來自訂執行個體。若要使用預設參數的進階組態建立 Amazon Connect Decisions 執行個體，請遵循下列步驟。

1. 在進階設定中選取建立。
2. 執行個體屬性頁面隨即出現。



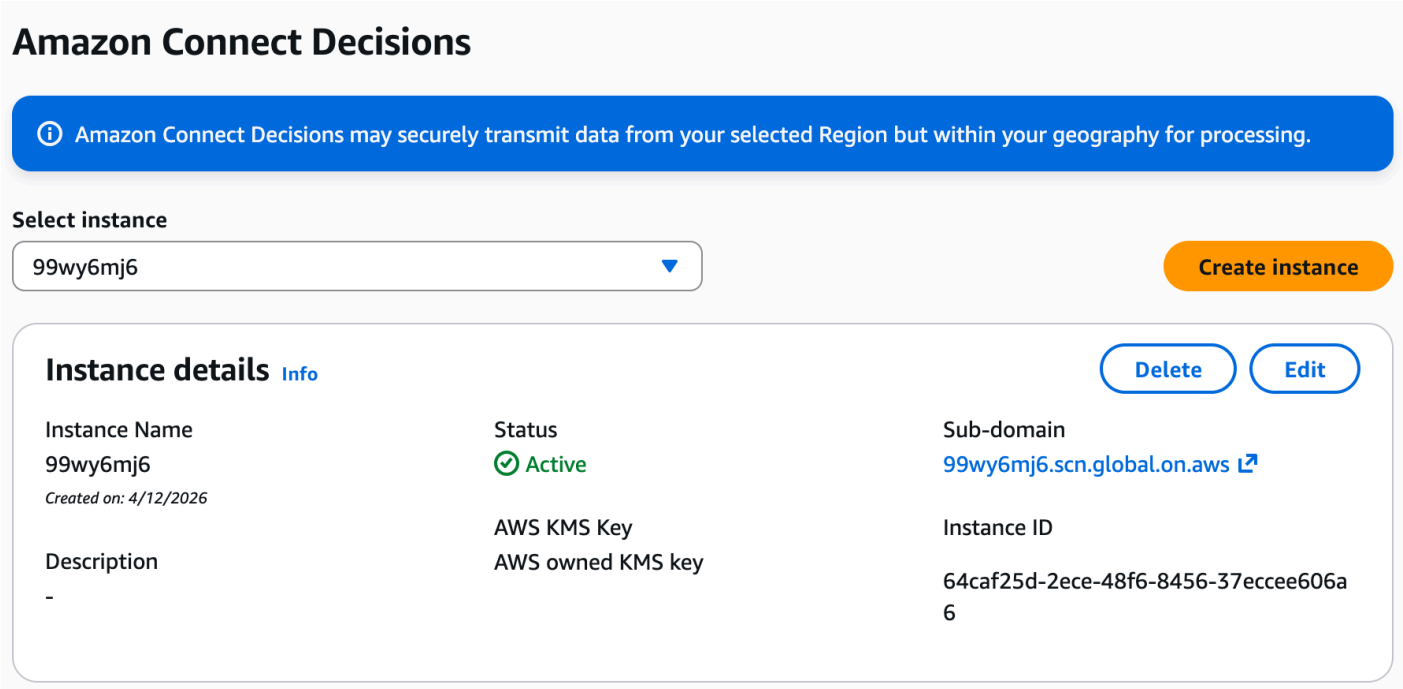
3. 在執行個體屬性頁面上輸入下列項目：
   - 名稱 – 輸入執行個體名稱。
   - 描述 – 輸入 Amazon Connect Decisions 執行個體的描述（例如生產執行個體、測試執行個體等）。
   - 執行個體標籤 – 您可以將標籤新增至執行個體，以用於識別。例如，您可以新增標籤來定義您要建立的執行個體類型（例如生產、測試、UTA 等）。
4. 選取建立執行個體。

刪除執行個體

若要刪除執行個體，請遵循下列步驟。

> **Note**
>
> 當您刪除執行個體時，不會自動刪除 Amazon S3 儲存貯體中的資訊。

1. 在 https：//https://console.aws.amazon.com/scn/home 開啟 Amazon Connect Decisions 主控台。
2. 在 Amazon Connect Decisions 主控台儀表板的下拉式清單中，選取您要刪除的執行個體。



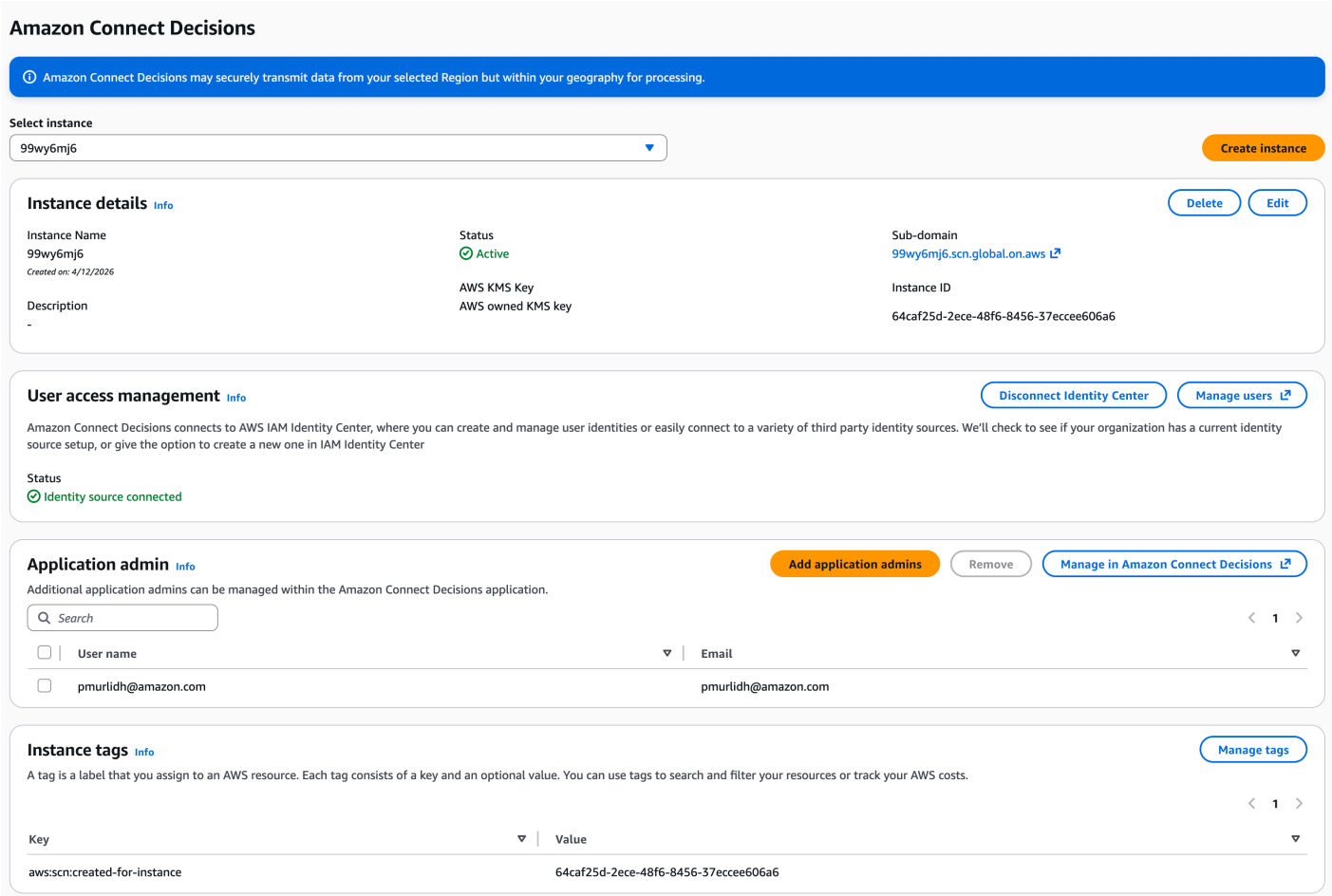
3. 選擇 刪除。
4. 在刪除 Amazon Connect 決策執行個體頁面的確認下，輸入 `delete`以確認您想要刪除執行個體。
5. 選擇 刪除。執行個體刪除開始，一旦刪除執行個體，您將會看到確認訊息。

選擇應用程式管理員

身為 AWS 主控台管理員，您可以選擇 Amazon Connect Decisions 應用程式管理員來管理 Amazon Connect Decisions Web 應用程式存取。Amazon Connect Decisions 應用程式管理員可以將使用者許可角色新增至或移除 Amazon Connect Decisions Web 應用程式。

建立執行個體並連接身分來源後，請依照下列步驟選擇 Amazon Connect Decisions 應用程式管理員。

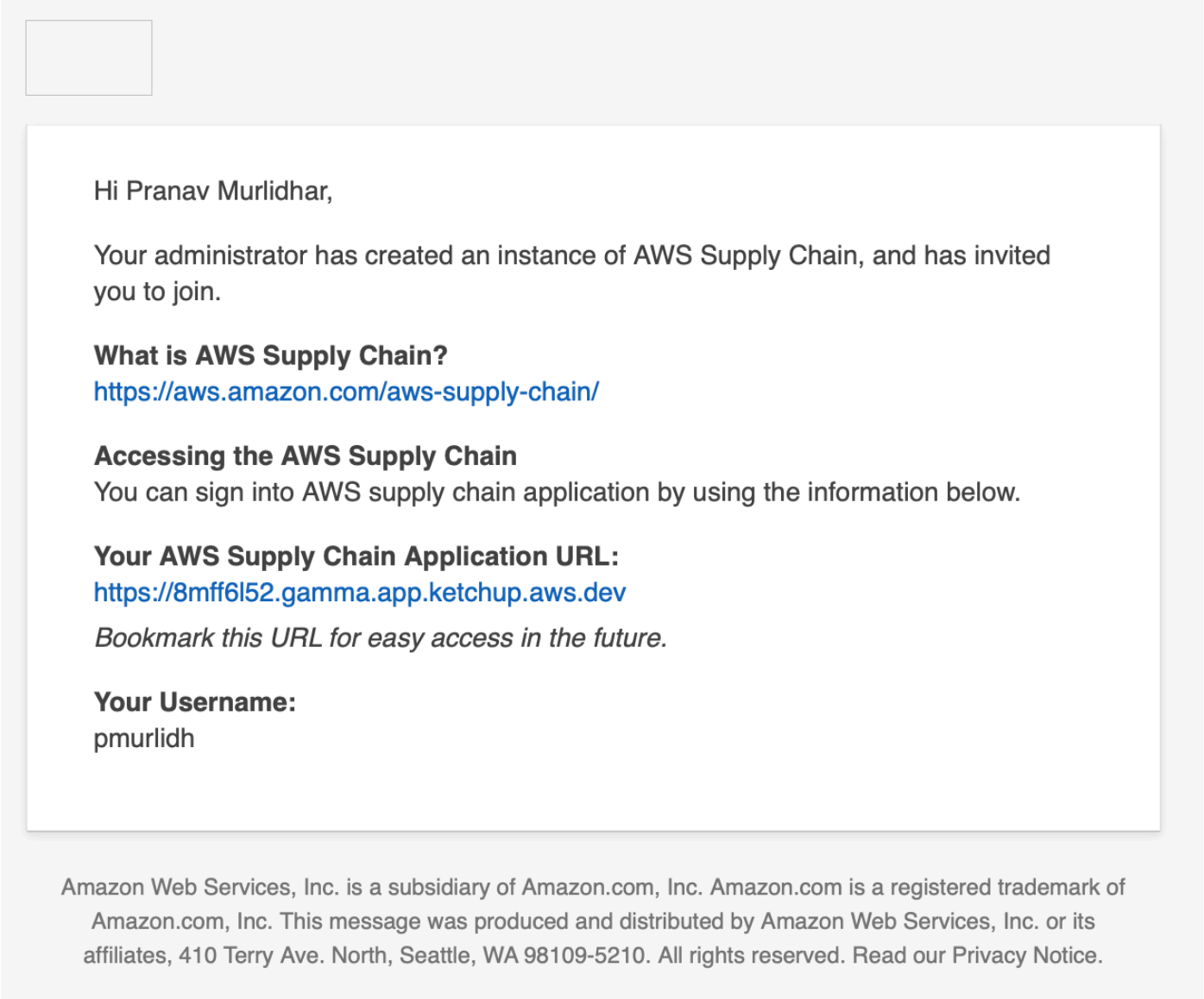
1. 開啟 Amazon Connect Decisions 主控台儀表板。
2. 前往選取應用程式管理員，然後選取要成為 Amazon Connect Decisions 應用程式管理員的使用者。搜尋結果只會顯示符合搜尋條件的使用者。



3. （選用）選擇前往 IAM Identity Center 以新增更多使用者。如需新增使用者的詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的管理您的身分來源，如需使用者許可角色的詳細資訊，請參閱使用者許可角色。

> **Note**
>
> 您一次只能從 Amazon Connect 決策主控台新增一個使用者。您無法在 Amazon Connect Decisions 中將群組新增為應用程式管理員。

4. 選擇傳送邀請。一封電子郵件會傳送給 Web 應用程式管理員。一旦 Web 應用程式管理員收到邀請電子郵件，他們將能夠選取應用程式 URL 並登入 Amazon Connect Decisions。



Hi Pranav Murlidhar,

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

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

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

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

Your Username:
pmurlidh

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

在 Amazon Connect Decisions Webapp 中，您會看到應用程式管理員下列出的使用者。

存取您的執行個體

使用 主控台是管理服務資源和組態的最簡單方式。主控台提供直覺式的 Web 型界面，您可以在其中檢視、建立、修改和監控您的 資源。

若要存取 Amazon Connect Decisions 主控台，您必須擁有一組最低許可。這些許可必須允許您列出和檢視 AWS 帳戶中 Amazon Connect Decisions 資源的詳細資訊。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

對於僅呼叫 或 AWS API 的使用者，您不需要允許最低主控台許可。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

身為 Amazon Connect Decisions 管理員，您應該已收到 Amazon Connect Decisions Web 應用程式的電子郵件邀請。

1. 您可以在電子郵件或 Amazon Connect Decisions 主控台儀表板中選擇連結，在子網域下選擇 Web URL。
2. Amazon Connect Decisions Web 應用程式登入頁面隨即出現。
3. 輸入 AWS IAM Identity Center 使用者憑證，然後選擇登入。
4. 您新增的每個使用者都會收到電子郵件訊息，其中包含前往 Amazon Connect Decisions 的連結，或者您可以選擇複製連結並將連結傳送給使用者。

成功登入後，您將登陸個人化首頁。請參閱《 使用者指南》中的了解您的首頁，以進一步了解您的首頁。

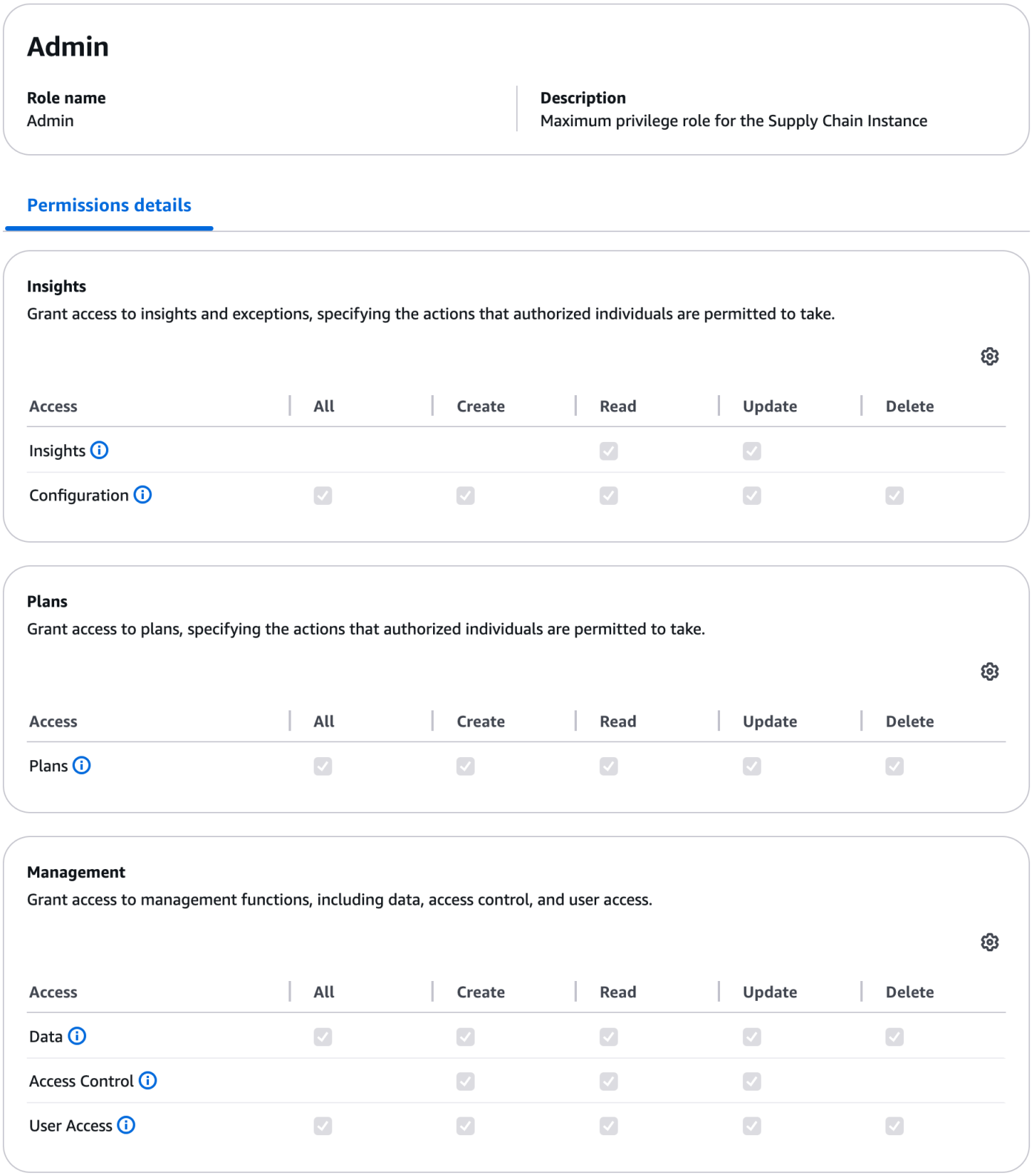
存取控制

Amazon Connect Decisions 提供企業級存取管理，可讓您精確控制誰可以存取哪些資料，以及在執行個體中執行哪些動作。這可確保您的使用者只看到與其責任相關的資訊，同時維護組織所需的安全和合規標準。

角色和許可概觀

身為 Amazon Connect Decisions 管理員，您可以使用預設使用者許可角色或建立自訂許可角色。Amazon Connect Decisions 具有下列預設使用者許可角色：

- 管理員 – 建立、檢視和管理所有資料和使用者許可的存取權。



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	✓	✓	✓	✓	✓

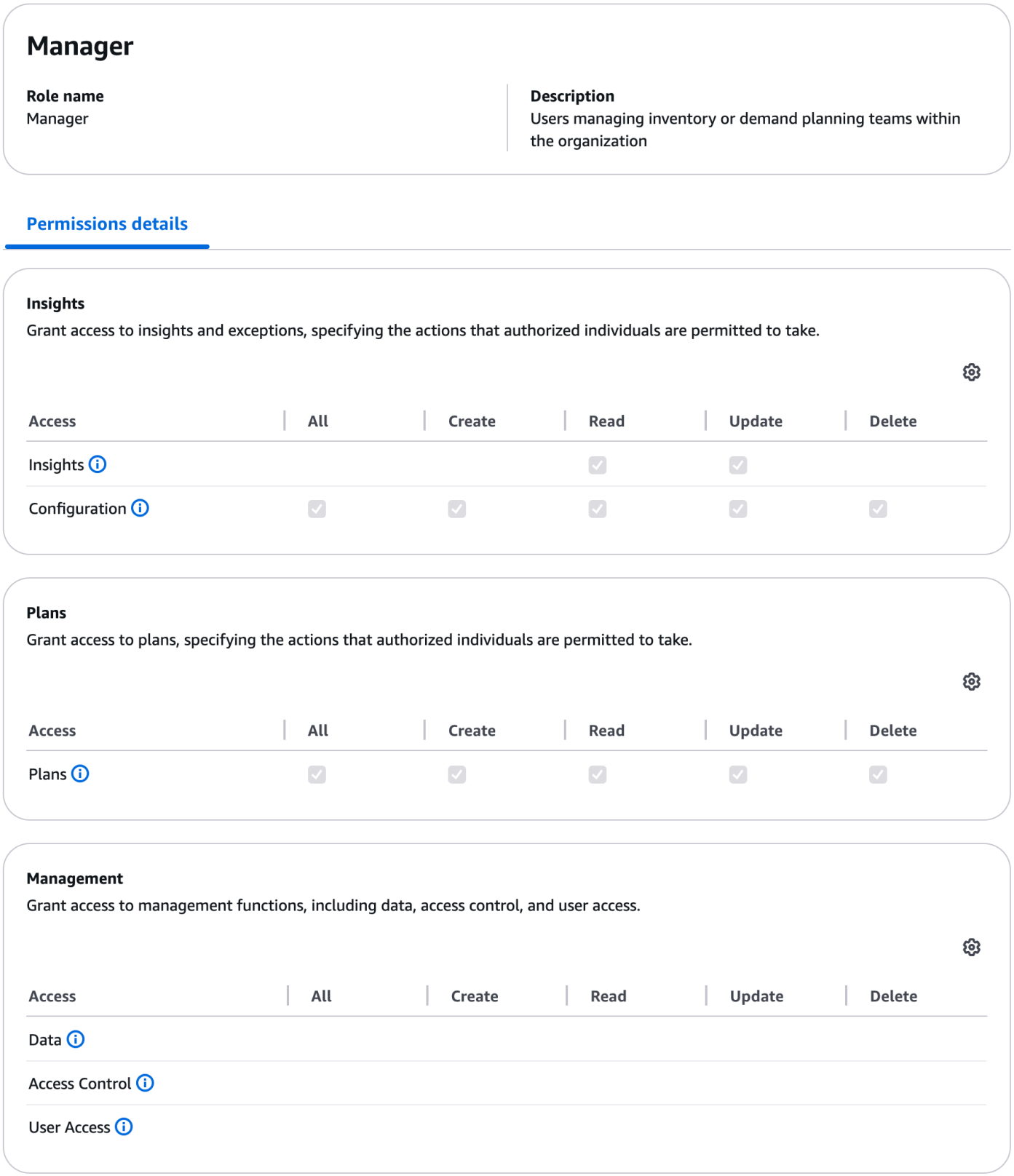
Plans
Grant access to plans, specifying the actions that authorized individuals are permitted to take.

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 – 建立、檢視和管理下列項目的存取權。



- 規劃人員 – 建立、檢視和管理下列項目的存取權。

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**
>
> 身為 Amazon Connect Decisions 管理員，在新增使用者之前，請注意下列事項：
>
> - 每個預設使用者許可角色都以一組許可定義。您可以將使用者新增至預設使用者許可角色，或建立自訂許可角色。
> - 一個使用者只能指派給一個使用者許可角色。
> - 您無法編輯或刪除預設使用者許可角色。
> - 編輯您建立的自訂許可角色時，會更新自訂許可角色下所有使用者的許可。
> - 當您刪除您建立的自訂許可角色時，自訂許可角色下的所有使用者都將無法存取 Amazon Connect Decisions。
> - Amazon Connect Decisions 不支援新增群組。

管理使用者許可角色

新增使用者

身為 Amazon Connect Decisions 管理員，您可以新增使用者來存取 Amazon Connect Decisions Web 應用程式。使用者必須先新增至 IAM Identity Center (IdC)，然後才能新增至 Amazon Connect Decisions。如需將使用者新增至 IdC 的詳細資訊，請參閱指派使用者存取權。

將使用者新增至 IdC 後，請依照下列步驟新增使用者。

1. 選擇設定左側抽屜
2. 選取使用者。選取指派使用者
3. 搜尋以識別使用者。您可以使用顯示名稱、電子郵件、名字、姓氏、使用者名稱進行搜尋
4. 選取您要新增的使用者。
5. 指派角色給他們。檢視角色和許可概觀，以進一步了解 Amazon Connect Decisions 中的使用者角色。
6. 選取指派。確認您的選擇正確無誤。

更新使用者許可

若要更新目前 Amazon Connect Decisions 使用者的使用者許可角色，請遵循下列步驟。

1. 選擇設定左側抽屜
2. 選取使用者。選取指派使用者
3. 在使用者清單中，選取使用者以開啟使用者詳細資訊頁面。
4. 使用角色下拉式清單來更新使用者的角色許可。
5. 按一下變更角色按鈕，確認您想要變更角色

刪除使用者

身為 Amazon Connect Decisions 管理員，您可以從 Amazon Connect Decisions Web 應用程式刪除使用者。請依照下列步驟刪除使用者。

1. 選擇設定左側抽屜
2. 選取使用者。選取指派使用者
3. 在使用者清單中，選取使用者以開啟使用者詳細資訊頁面。
4. 選取刪除
5. 按一下刪除按鈕，確認您想要刪除使用者

設定屬性層級存取

屬性型存取控制 (ABAC) 會根據業務內容限制存取，增加一層額外的精確度。使用產品和網站屬性，您可以確保規劃人員只能查看他們管理的特定產品和位置的詳細資訊，同時經理可以保持團隊責任領域的可見性。

任何具有 'Admin' 角色的使用者都可以根據產品和網站為其他使用者設定存取權：

1. 從左側導覽列導覽至使用者頁面。
2. 從該執行個體中的使用者清單中，選取需要組態的使用者。
3. 根據預設，在資料存取區段中，使用者將啟用「授予所有產品和網站的完整存取權」。當此切換開啟時，它可以存取所有產品和網站（啟動之前的運作方式）。
4. 關閉「授予所有產品和網站的完整存取權」，產品和網站組態區段就會顯示。第一次存取時，不會指派任何產品或網站。
5. 根據您需要設定的內容，按一下產品或網站的新增/移除按鈕。使用搜尋來尋找並選取該使用者所需的項目。
6. 多個使用者可以將相同的產品或網站指派給他們。使用者最多可以有 1，000 個產品網站組合。

7. 您可以使用相同的界面移除先前設定的產品或網站。
8. 檢閱並確認精靈最終頁面中新增和移除的完整清單，以完成存取組態。

設定產品和網站存取權後，將根據這些指派限制該使用者的存取權：

- 所有使用者都可以檢視任何例外狀況或建議頁面，無論其是否針對存取控制中包含的產品或網站產生。
- 若要執行變動動作（例如關閉例外狀況或將狀態從進行中變更為完成），使用者必須在其存取控制中設定適當的產品 OR 網站。
- 具有已設定存取控制的使用者也可以使用使用者指派和存取檢視切換。

使用者指派

使用者指派是一項功能，可讓您更輕鬆地平衡多個使用者之間的洞見。使用使用者指派，客戶可以將特定洞見指派給使用者，以更好地反映這些任務在現實世界中如何共用。其運作方式如下：

- 每當建立例外狀況時，系統會針對為其存取控制設定相同產品 OR 網站的所有使用者，檢查為其建立例外狀況的產品和網站
- 如果系統找到符合的使用者，則該例外狀況的 Assigned To 欄位會以使用者名稱更新。如果多個使用者的產品或網站符合例外狀況，則會將其隨機指派給其中一個使用者
- 每個例外狀況只能指派一個使用者，但可以視需要將例外狀況重新指派給另一個使用者。它只能重新指派給具有產品或網站存取權的使用者
- 首次建立例外狀況時，會自動指派洞見。先前建立的洞見不會自動重新指派。此外，如果刪除使用者或更新其存取控制，則不會自動更新使用者指派
- 在洞見清單頁面中，使用者可以依指派至維度進行篩選，以輕鬆識別指派給他們的所有洞見。他們也可以使用此相同的篩選條件來檢視未指派的洞見。使用者指派目前僅適用於洞察

資料加入

連接您的資料

先決條件

開始資料加入之前，請確定您已：

- Amazon Connect Decisions 執行個體
  - 您的執行個體應該已使用相關聯的 S3 儲存貯體建立
- 資料已準備
  - 與您的 Amazon Customer Success 對手合作，根據您計劃使用 Amazon Connect 決策的方式，判斷您需要哪些資料。基本資料需求包括：
    - 銷售/訂單歷史記錄：12 個月以上的交易記錄
    - 產品詳細資訊：使用規格完成產品目錄
    - 站台/位置資訊：倉儲、配送中心、零售據點
    - 目前庫存持有：每個位置的現有庫存
  - 使用 UTF-8 編碼的 CSV 格式的所有來源資料

第一次登入：加入問卷

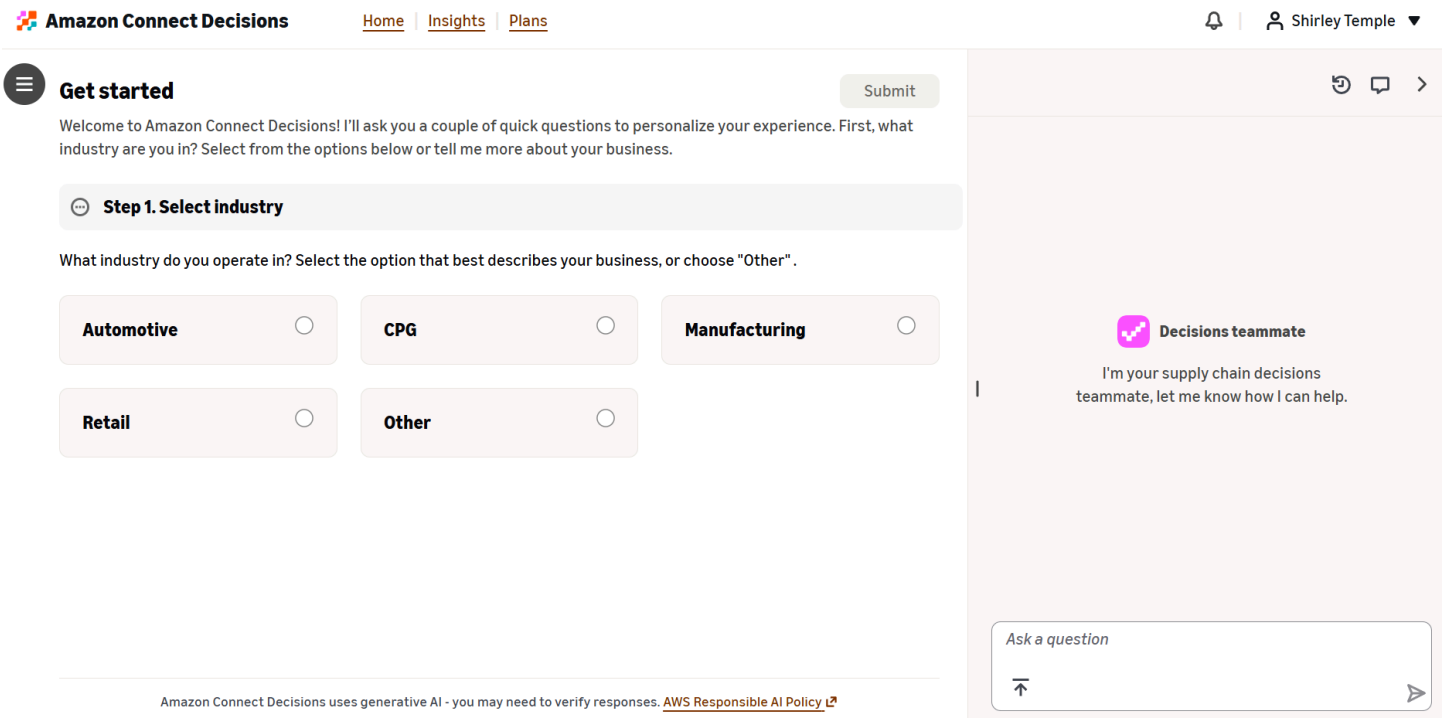
當您第一次登入 Amazon Connect Decisions 時，系統會顯示引導式入職問卷。此個人化精靈可協助決策團隊成員將與您的業務最相關的功能情境化。問卷會收集有關您的產業、主要業務挑戰和偏好規劃方法的資訊。您的回應將有助於根據您的選擇最佳化加入步驟，讓系統簡化後續的設定工作流程，並為您的業務呈現最相關的組態路徑。您必須先完成所有步驟，才能存取完整的應用程式。Decisions Teammate 可透過右側邊欄在整個入職過程中即時回答問題。

> **Note**
>
> 這是僅限第一次登入時的一次性選擇。您的回應提供額外的內容，以最佳化後續的加入步驟，並協助客服人員了解您的業務環境。無論您的選擇為何，所有功能都仍然可以完全存取。

步驟 1：選取產業

您看到的內容：歡迎訊息和一組選項按鈕，提示您選擇最能描述您業務的產業。

1. 選取最能代表您業務的選項按鈕。
2. 如果沒有套用任何預先定義的選項，請選取其他。



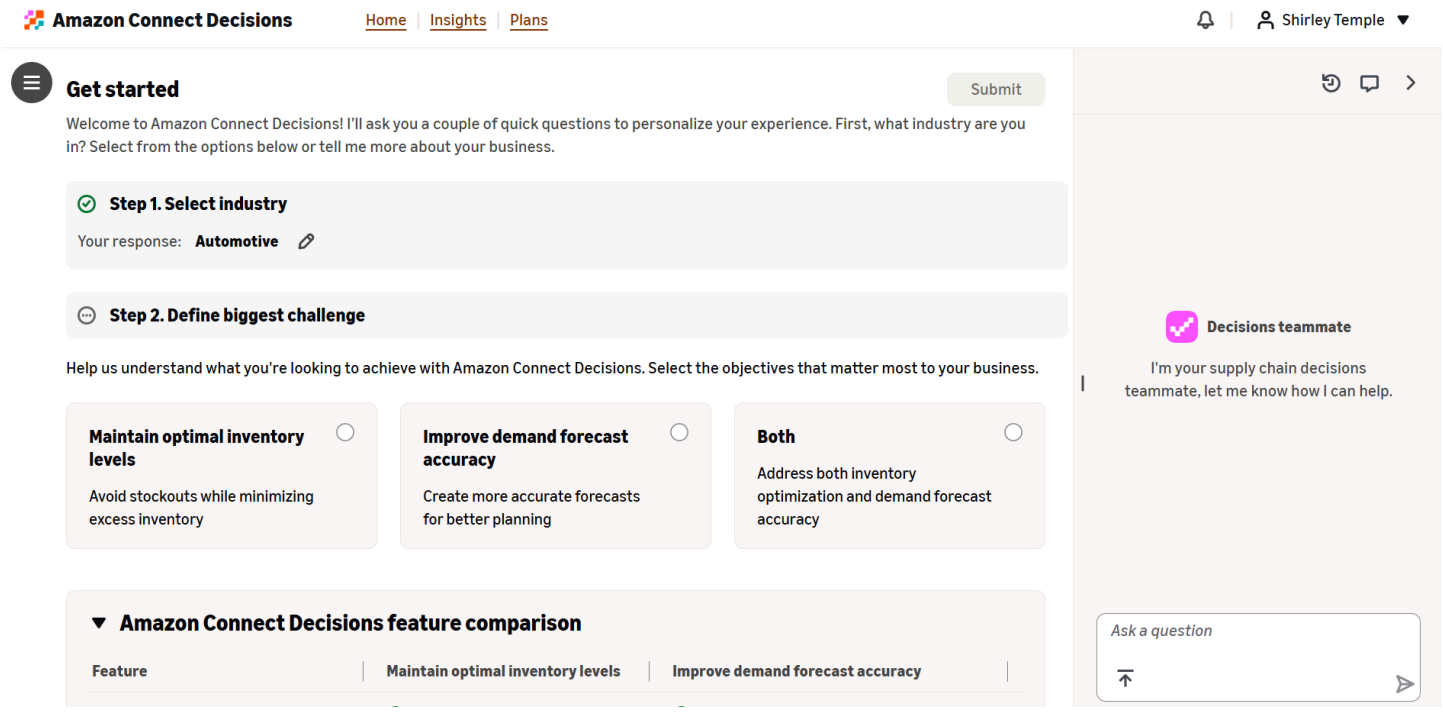
步驟 2：定義您的最大挑戰

您看到的內容：您的步驟 1 回應會以編輯選項顯示。在其下方，您需要從三個選項中識別您的主要業務挑戰。系統會顯示功能比較表，協助您了解與每個選擇相關聯的功能。

1. 檢閱選項。如需可用的選項及其意義，請參閱下表。
2. 選取代表您最緊迫挑戰的選項按鈕。
3. 或者，檢閱選項下方的功能比較表，以了解每個選擇中包含的內容。

業務挑戰選項

選項	說明	已啟用的主要功能
維持最佳庫存層級	如果您的主要挑戰是避免庫存不足，同時將過多庫存降至最低，請選擇此選項。	庫存最佳化；預防缺貨；減少過多庫存；供應規劃；廠商前置時間追蹤
改善需求預測準確性	如果您的主要挑戰正在建立更準確的預測，以更好地規劃決策，請選擇此選項。	基準預測；共識規劃；預測準確度追蹤
兩者	如果您需要同時處理庫存最佳化和需求預測準確性，請選擇此選項。	已啟用所有特定供需功能



步驟 3：選擇您的庫存規劃方法

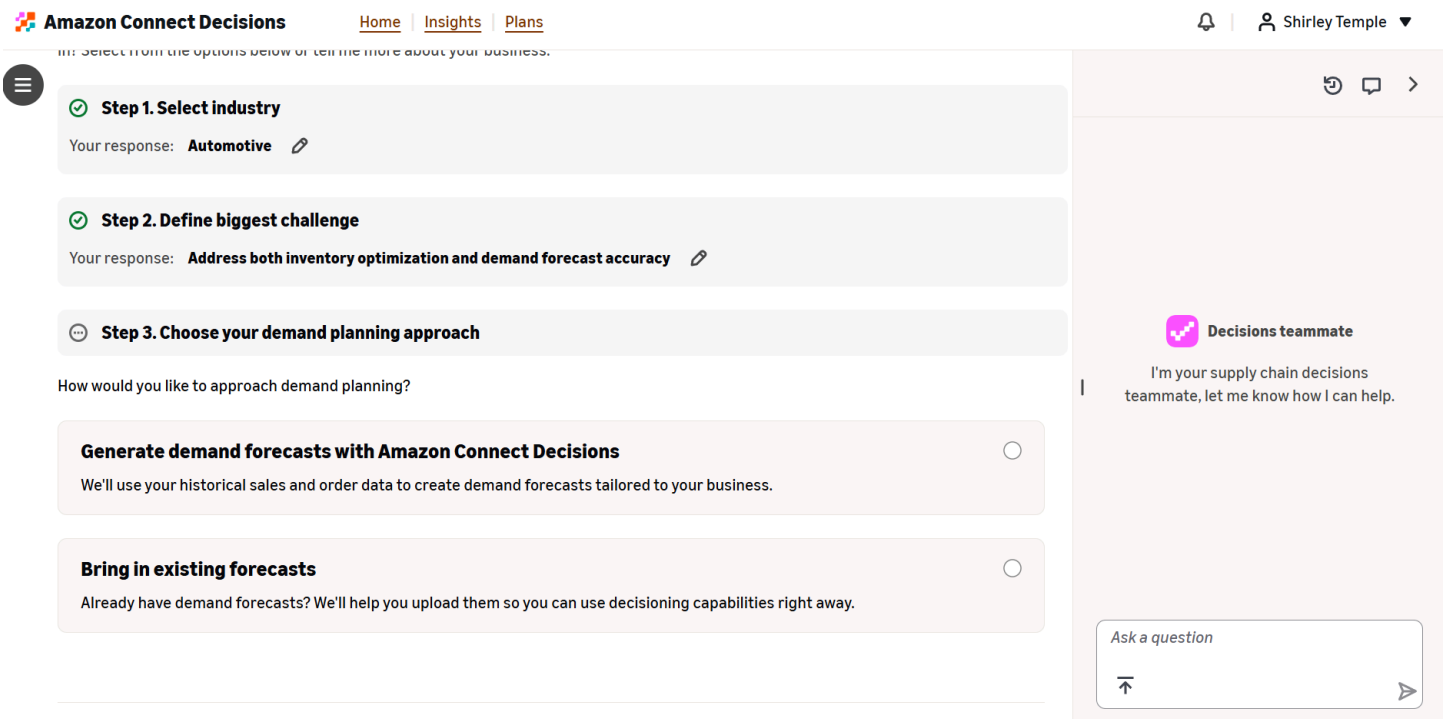
您看到的內容：步驟 1 和 2 會顯示為已完成（以綠色核取記號表示），並顯示您的回應且可編輯。步驟 3 詢問您希望如何處理庫存規劃，並反白兩個選項。

1. 檢閱兩個庫存規劃選項。如需可用的選項及其意義，請參閱下表。

2. 針對符合您目前狀態的方法，選取選項按鈕。

庫存規劃方法選項

選項	說明	最適合
使用 Amazon Connect Decisions 產生庫存計劃	系統會使用您的歷史銷售和庫存資料，為您的業務建立量身打造的計劃。	沒有現有規劃解決方案或想要利用 AI 從歷史資料產生的計劃的組織。
導入現有的庫存預測或計劃	上傳現有的庫存計劃或預測，以便您立即使用決策功能。系統會協助您上傳和映射資料。	組織已建立規劃程序，並希望利用監控、產生洞見和建議功能，而無需變更其計畫來源。



步驟 4：選擇您的需求規劃方法

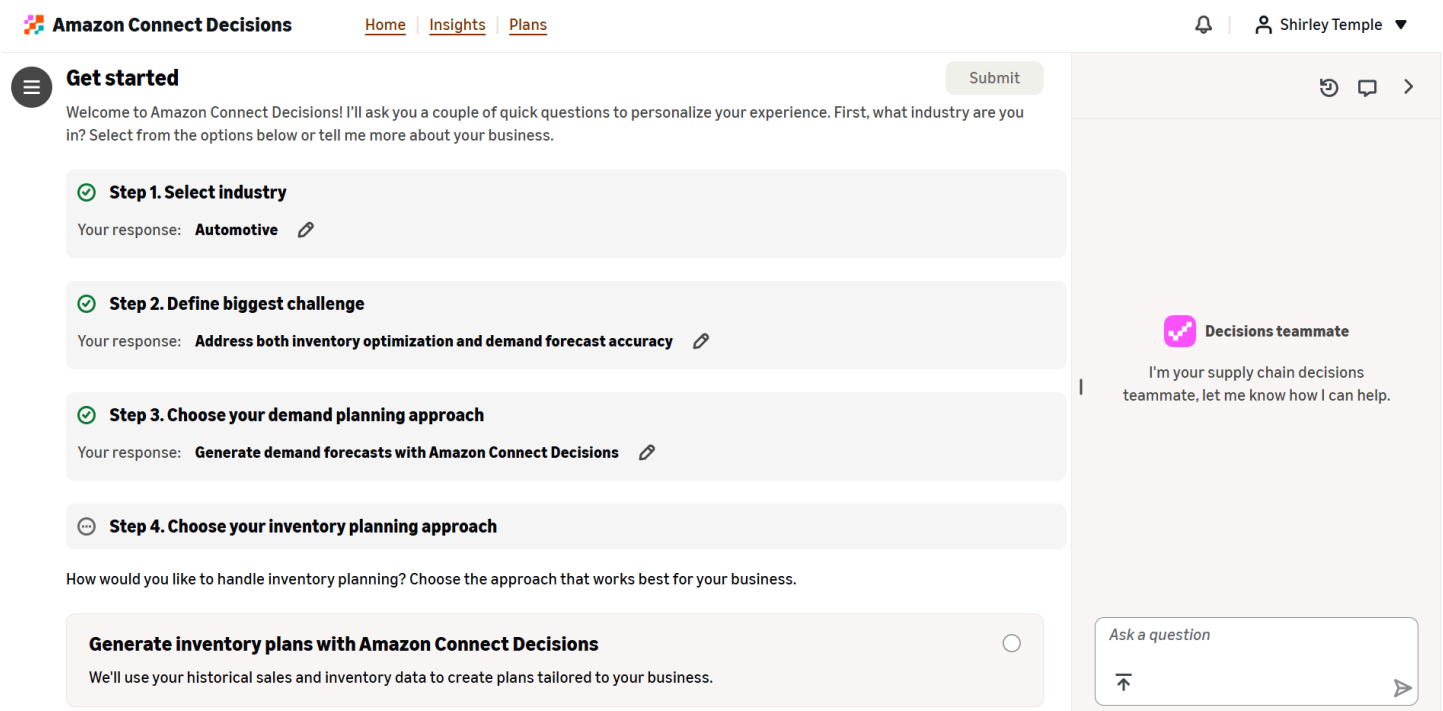
您看到的內容：步驟 1 到 3 會顯示為已完成。步驟 4 詢問您想要如何處理需求規劃。

1. 檢閱兩個需求規劃選項。如需可用選項及其意義，請參閱下表。
2. 針對符合您目前狀態的方法，選取選項按鈕。
3. 按一下提交以完成入職問卷。

請記住：此入職問卷是一次性內容輸入，有助於根據您的選擇最佳化入職步驟。它不會更改代理程式行為或限制對任何功能的存取。Amazon Connect Decisions 的所有功能仍可供您完整使用。

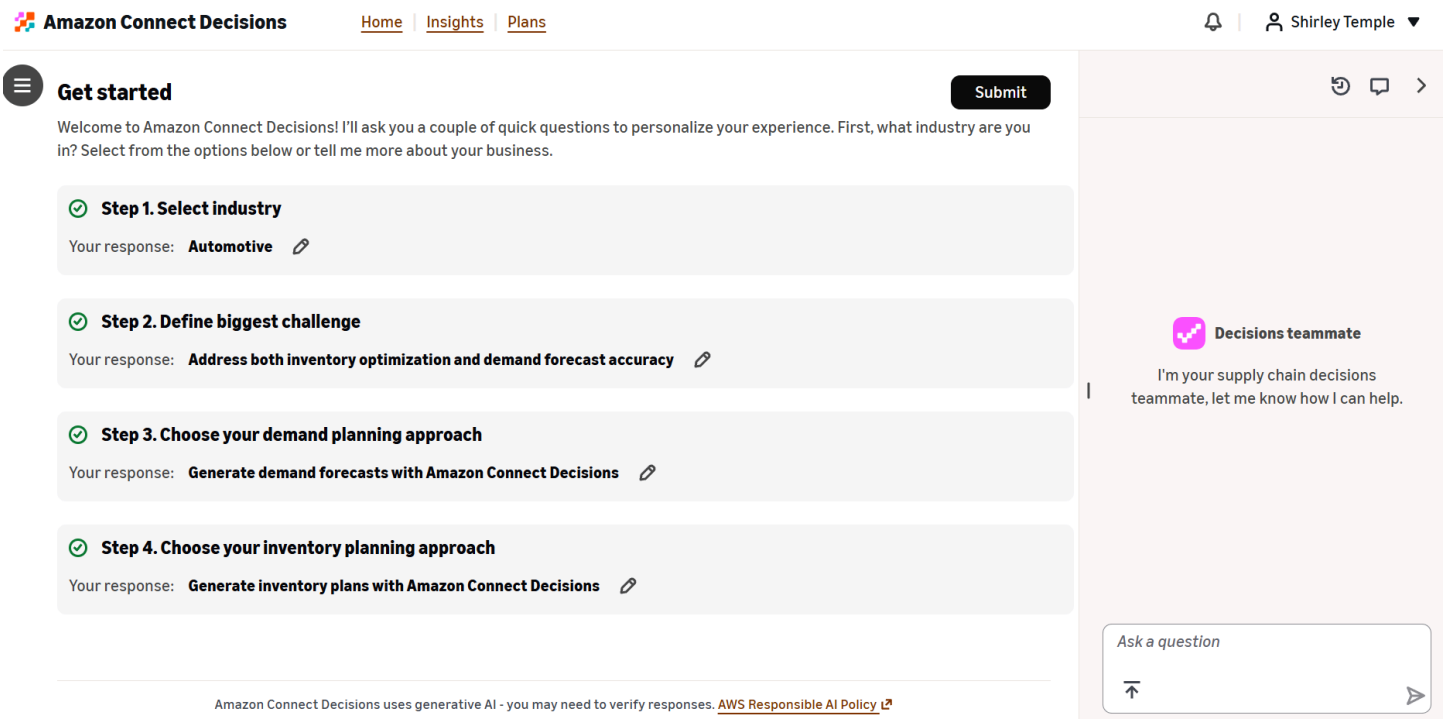
需求規劃方法選項

選項	說明	最適合
使用 Amazon Connect Decisions 產生需求預測	系統會使用您的歷史銷售和訂單資料來建立針對您的業務量身打造的需求預測。Amazon Connect Decisions 協調超過 18 種預測工具，以產生準確的基準預測。	沒有現有預測解決方案或想要將其目前方法取代為 AI 產生的預測的組織。
導入現有的預測	上傳現有的需求預測，讓您可以立即使用決策功能。系統會協助您映射和匯入預測資料。	已經建立預測程序並希望利用監控、洞見產生和建議功能的組織，無需變更預測來源。

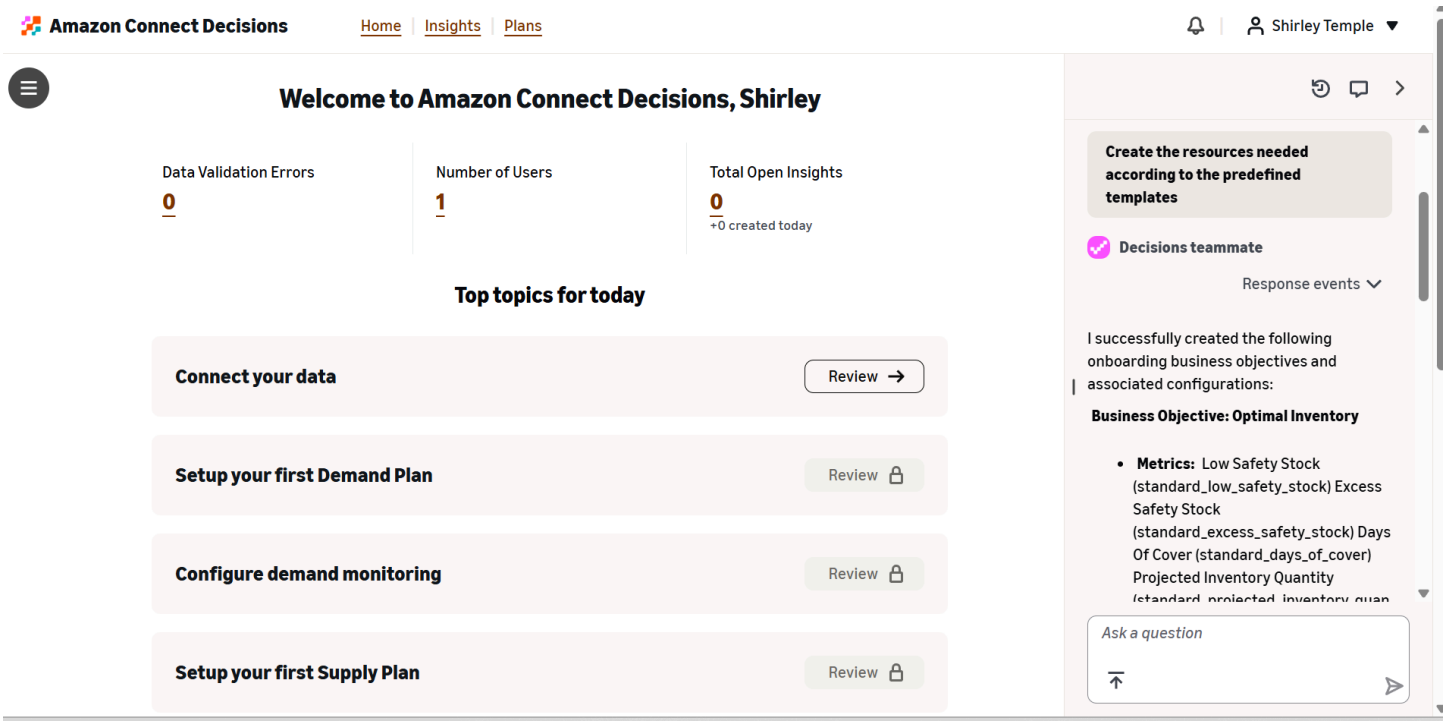


完成問卷後

完成這四個步驟後，請按一下提交：

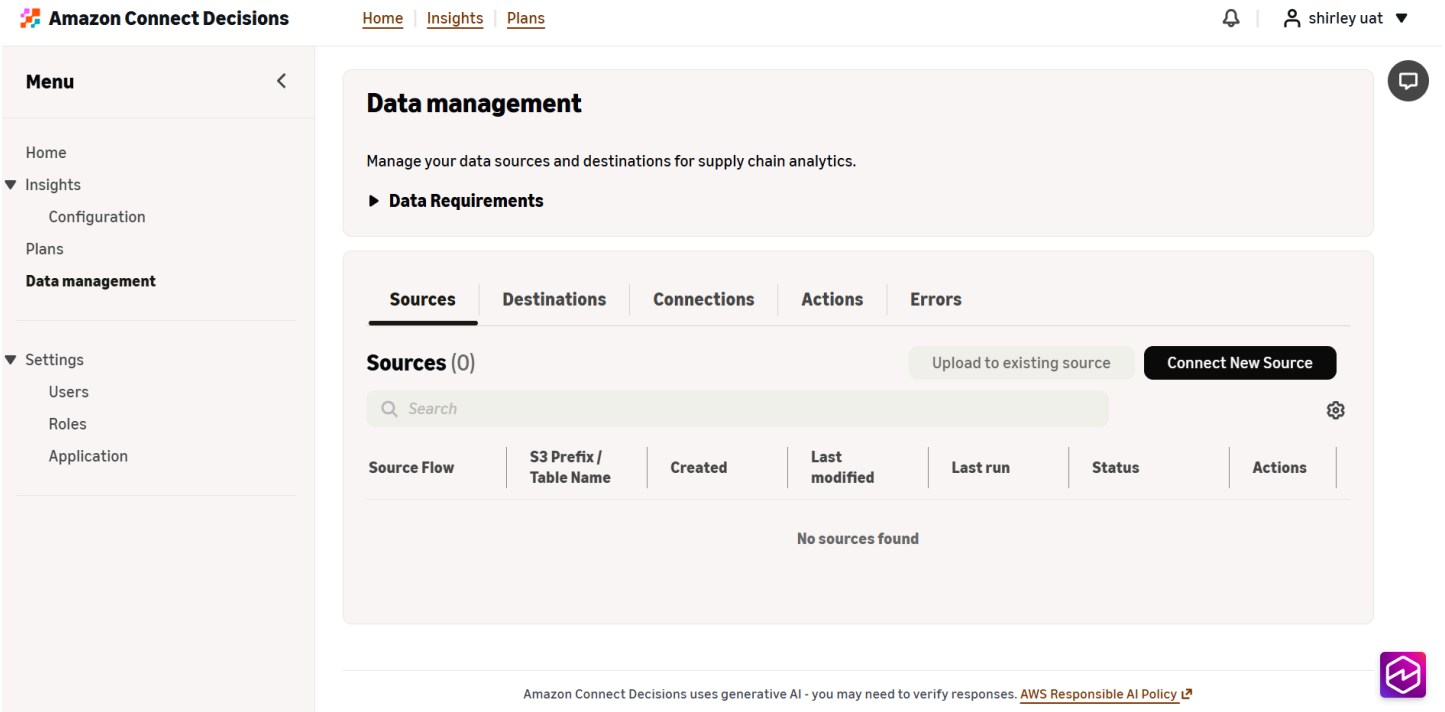


- 系統會將您重新導向至首頁，其中包含儀表板和主題卡，旨在引導您完成剩餘的加入步驟。
- 系統會根據您的選擇，在應用程式中自動建立指標和規則。這些會以草稿狀態建立，且不會立即處於作用中狀態。
- 您可以檢閱自動建立的指標和規則，然後在它們符合您的需求時啟用它們，或根據您的特定業務需求建立自己的指標和規則。



建立您的第一個來源流程

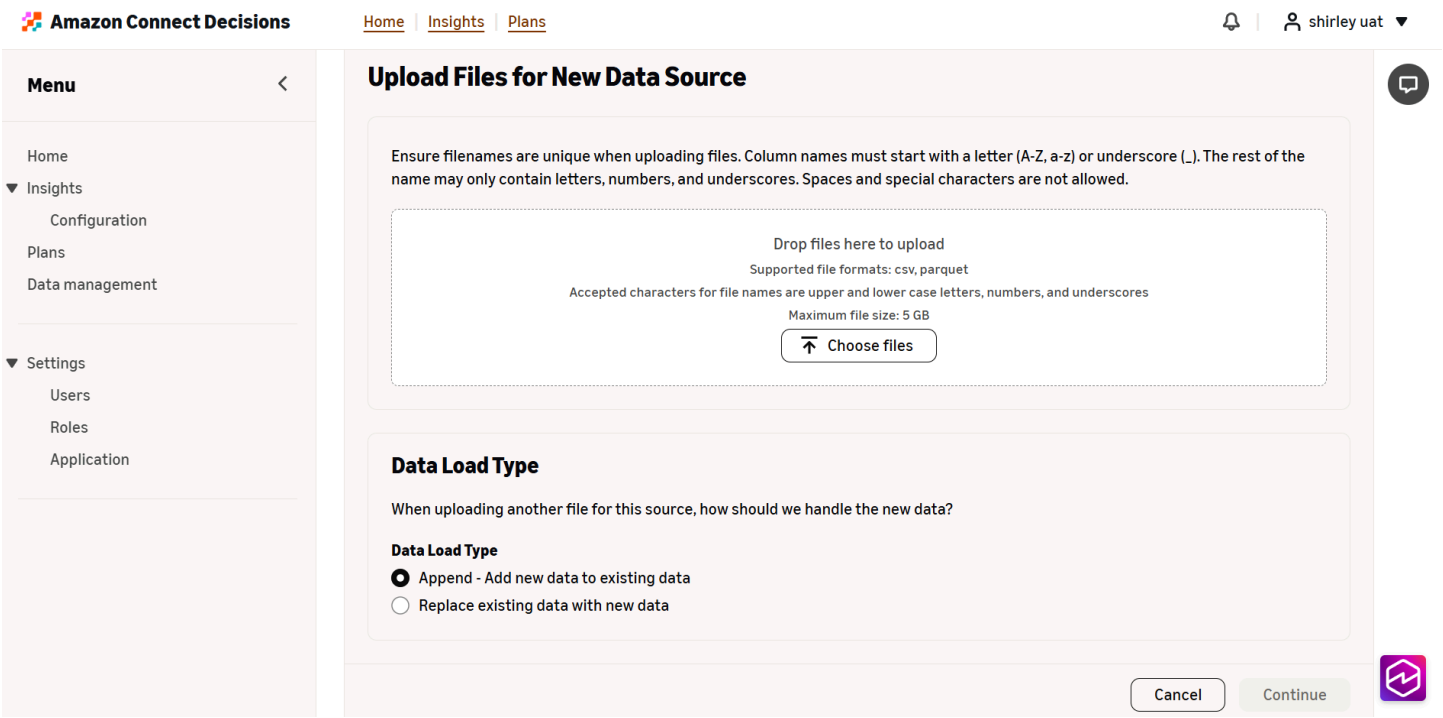
若要開始加入您的資料，請按一下檢閱以連接您的資料主題卡，或導覽至 Amazon Connect Decisions 中「Hamburger 選單」中的資料管理索引標籤。您可以在這裡查看所有現有的來源流程。如果您尚未設定，請按一下「連接新來源」開始。



上傳您的來源資料

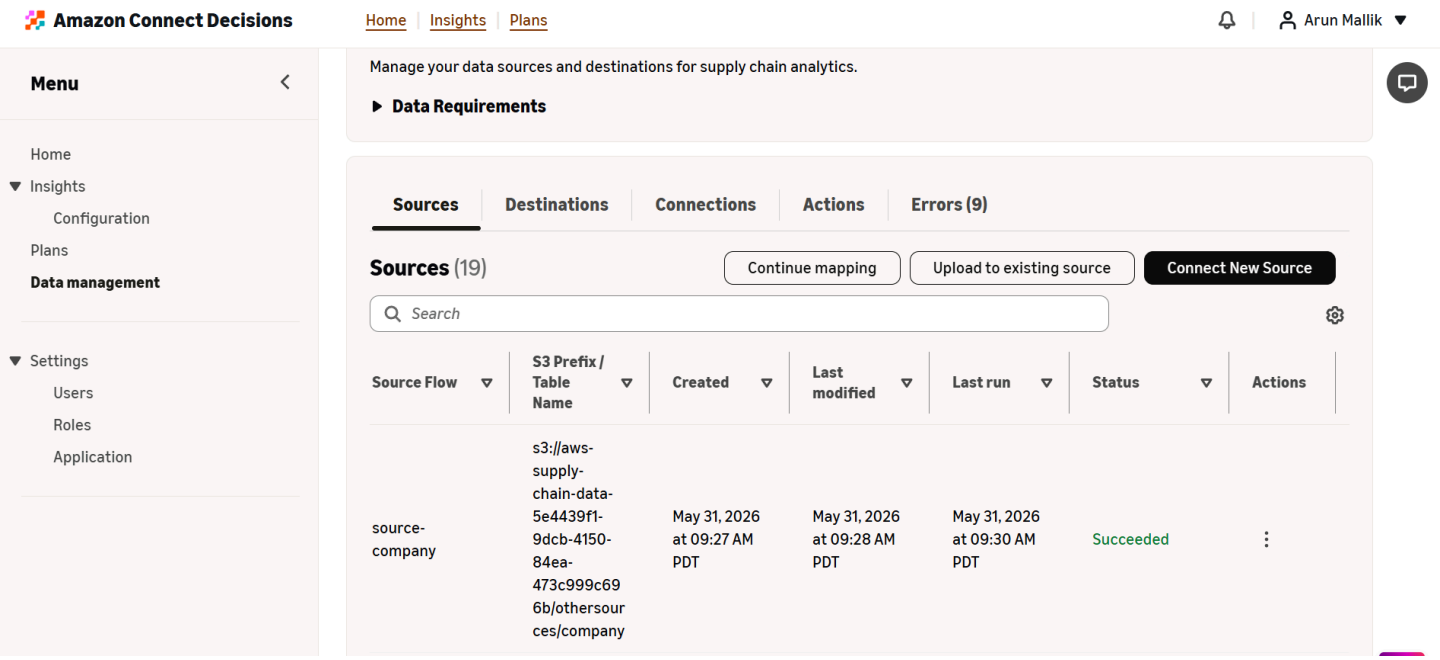
根據使用案例所需的 CDM 資料表，上傳包含來源資料的 CSV 檔案。您可以選擇如何處理資料更新：

- 附加：將新資料新增至現有資料
- 取代：將現有資料取代為新資料



當您上傳檔案時，Amazon Connect Decisions 會自動在 S3 中為該資料建立資料夾結構，包括：

- 以您選取的來源系統命名的父資料夾
- 以您選取的來源資料表名稱命名的子資料夾
- 子資料夾下的所有檔案都會儲存到相同的來源資料表
- 此檔案結構也用於建立 Amazon S3 資料夾路徑

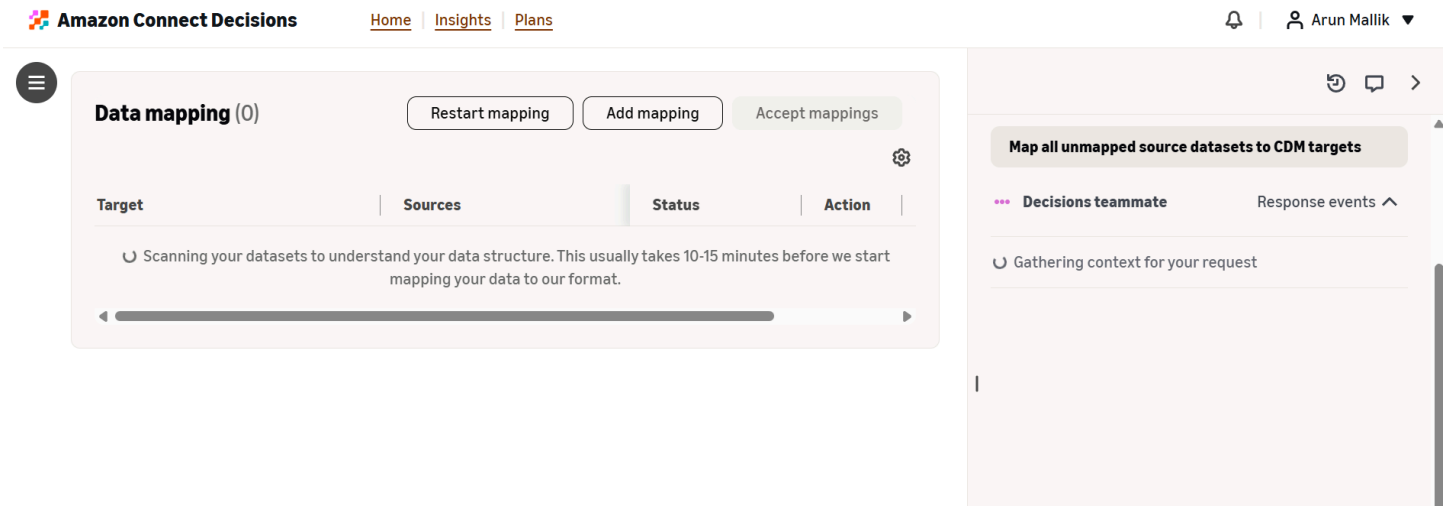


Source-to-CDM 目的地映射

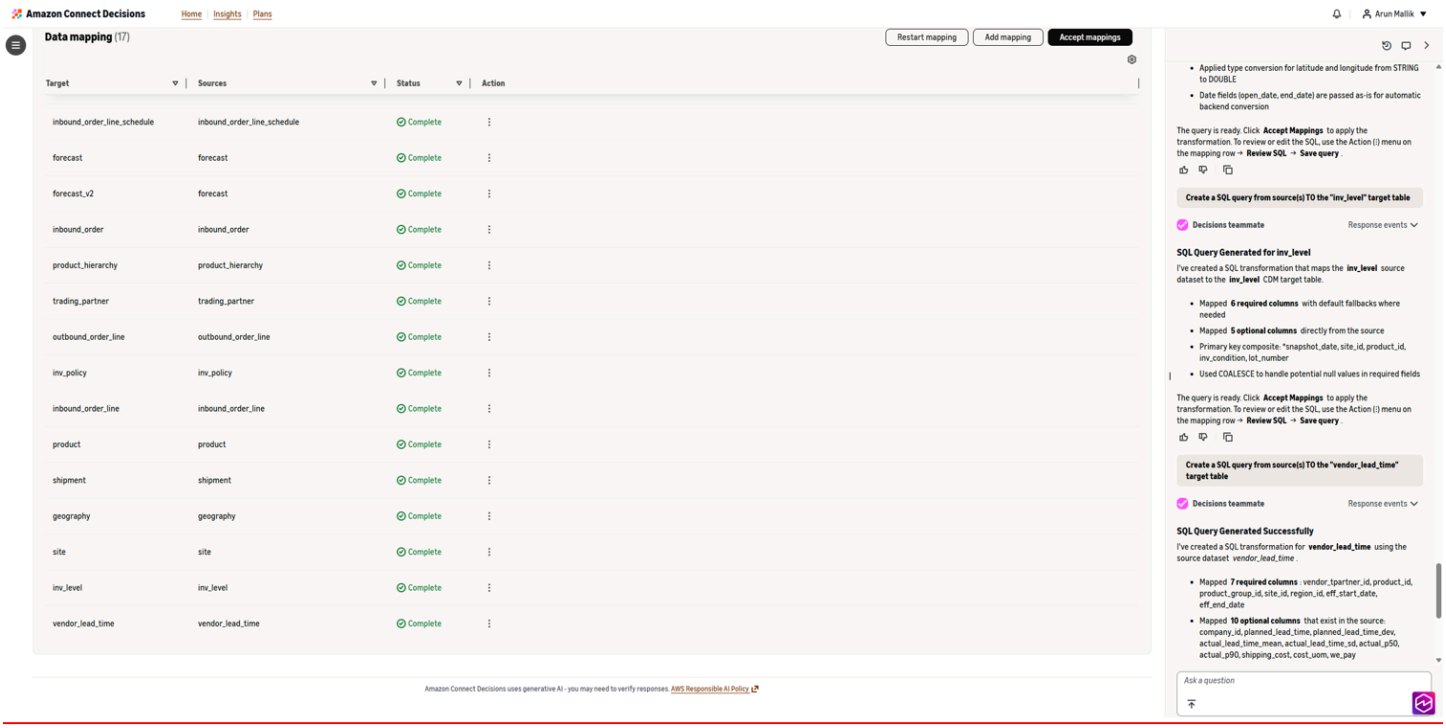
上傳檔案後，Amazon Connect Decisions 會開始分析您的資料，並自動將其映射至一或多個 Amazon Connect Decisions 的 CDM 目的地資料表。

預期事項

- 此步驟可能需要 10-15 分鐘，取決於上傳的資料量
- Data Agent 會在背景運作，以識別來源資料的最佳 CDM 目的地資料集。
- 離開此頁面會導致自動映射失敗。等待時，請保持開啟 Amazon Connect Decisions and Data Management 索引標籤，以確保自動映射完成。

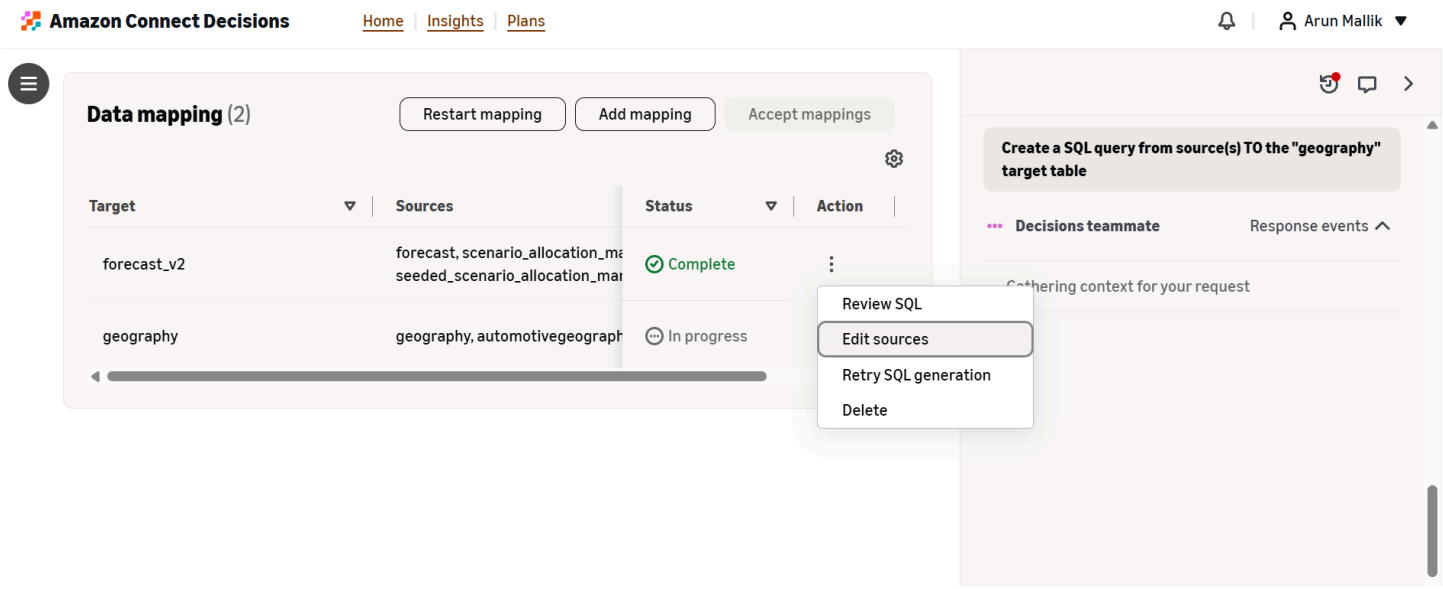


完成後，資料代理程式會根據重疊的資料提供source-to-destination映射的原理，您可以檢閱這些資料，並針對任何映射結果向代理程式提出問題。



若要檢閱和編輯來源映射，您可以：

- 使用自然語言直接與 Data Agent 互動，以更新來源目的地映射。
- 按一下動作，然後選取「編輯來源」。



編輯映射

從這裡，您可以：

- 視需要手動更新來源和目的地映射
- 使用畫面右側的資料代理程式提出問題，以確認映射
- 參考使用者指南以進一步了解特定資料集

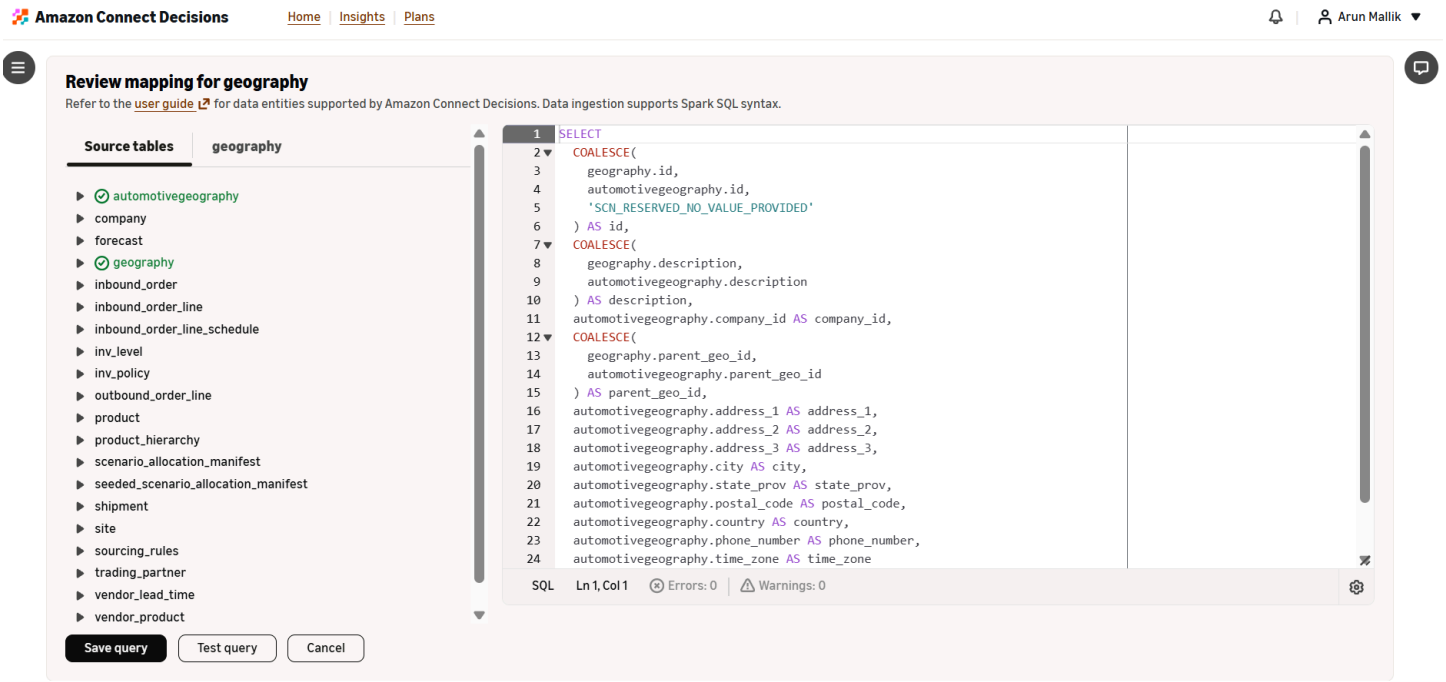
資料欄/資料映射

source-to-destination映射完成後，Amazon Connect Decisions 會自動從您的來源資料集建立 SQL 轉換查詢至 CDM 目的地。任何映射完成後，您會收到來自 Data Agent 的通知，詳細說明映射的結果。

從這裡，您應該從動作功能表中選取「檢閱 SQL」來檢閱為映射產生的 SQL。

檢閱映射 (SQL)，您會看到：

- 您已新增的來源資料集資料欄
- 供參考的目的地 CDM 資料表欄
- 連接它們的轉換 SQL
- Data Agent 提供的映射原理



編輯映射

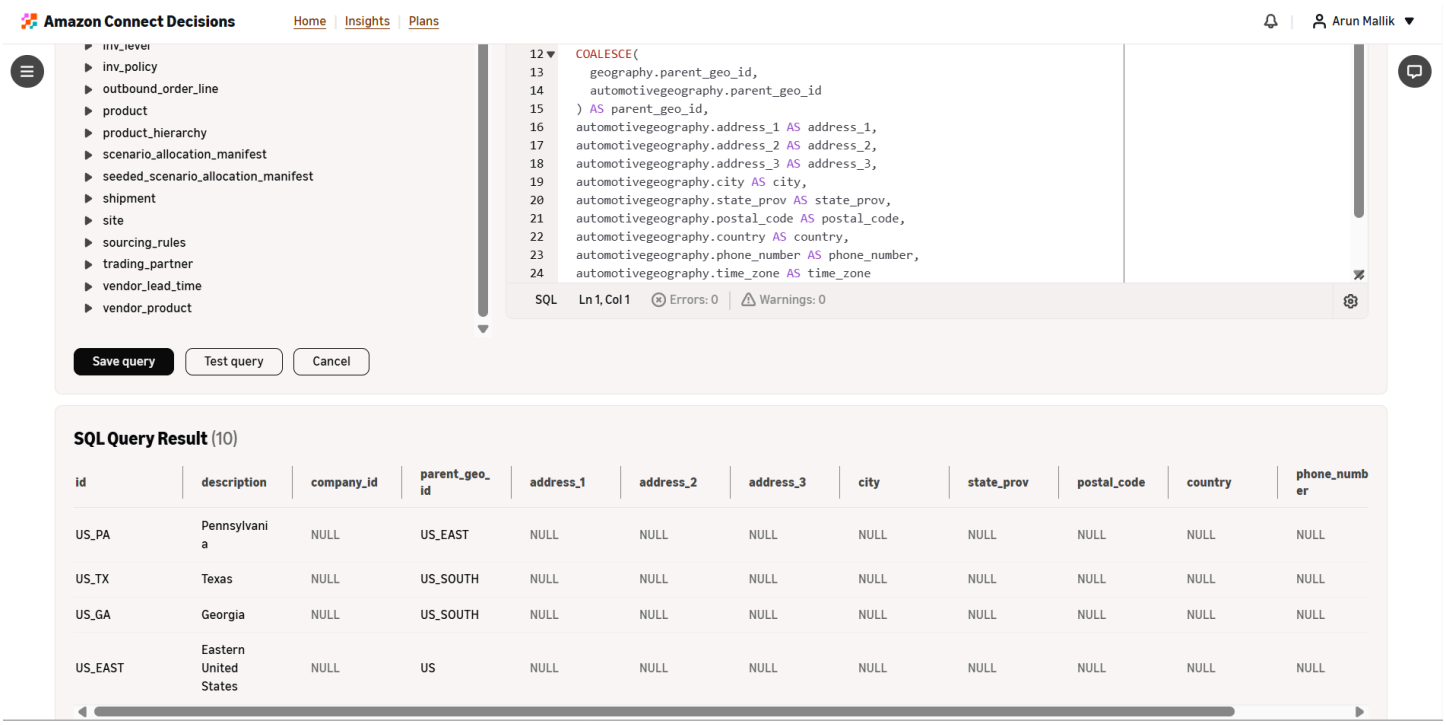
您有兩個選項可編輯任何映射：

- 使用 Data Agent：使用自然語言提出問題、管理和更新映射
- 直接編輯 SQL：如果您熟悉 SQL，可以直接修改查詢

測試您的變更

當您編輯映射查詢時，請繼續使用「測試查詢」功能進行測試，這將為您提供如何將資料轉換為目的地 CDM 的範例的可捲動預覽。使用此選項可確保您的轉換正確執行，並驗證source-to-destination CDM 的任何適當更新。

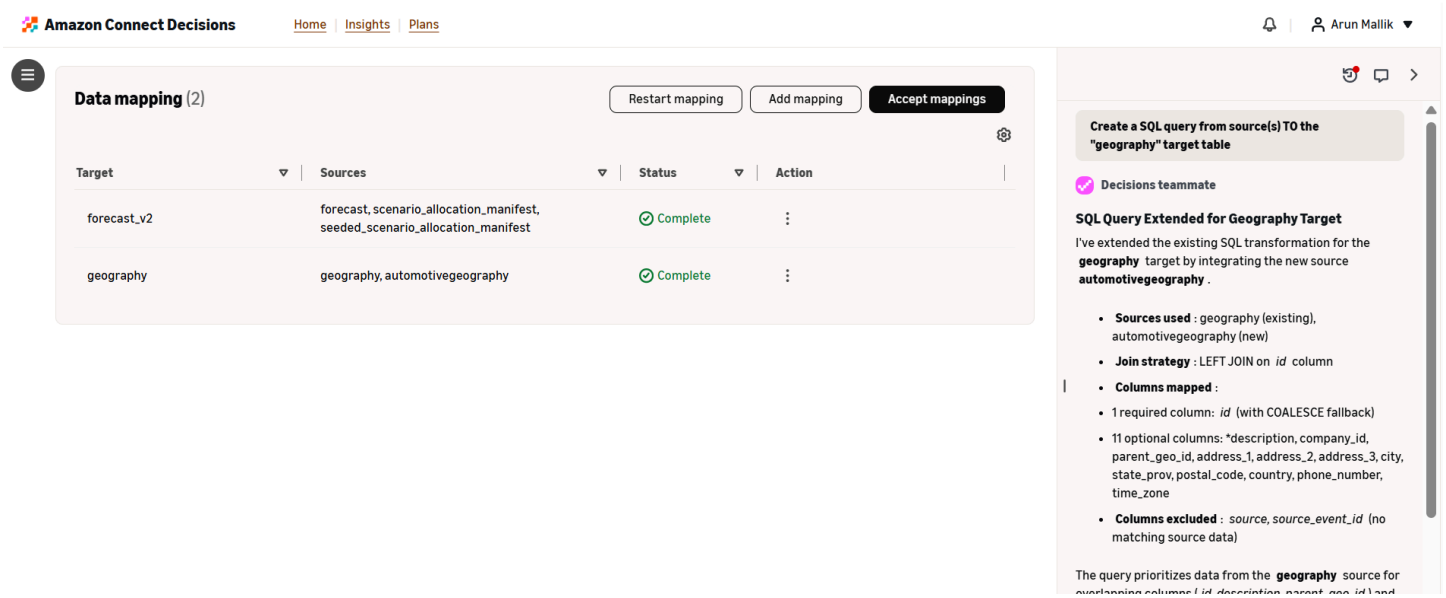
一旦您對映射輸出感到滿意，請選取「儲存查詢」以儲存該來源目的地對的轉換查詢。



檢閱並接受映射

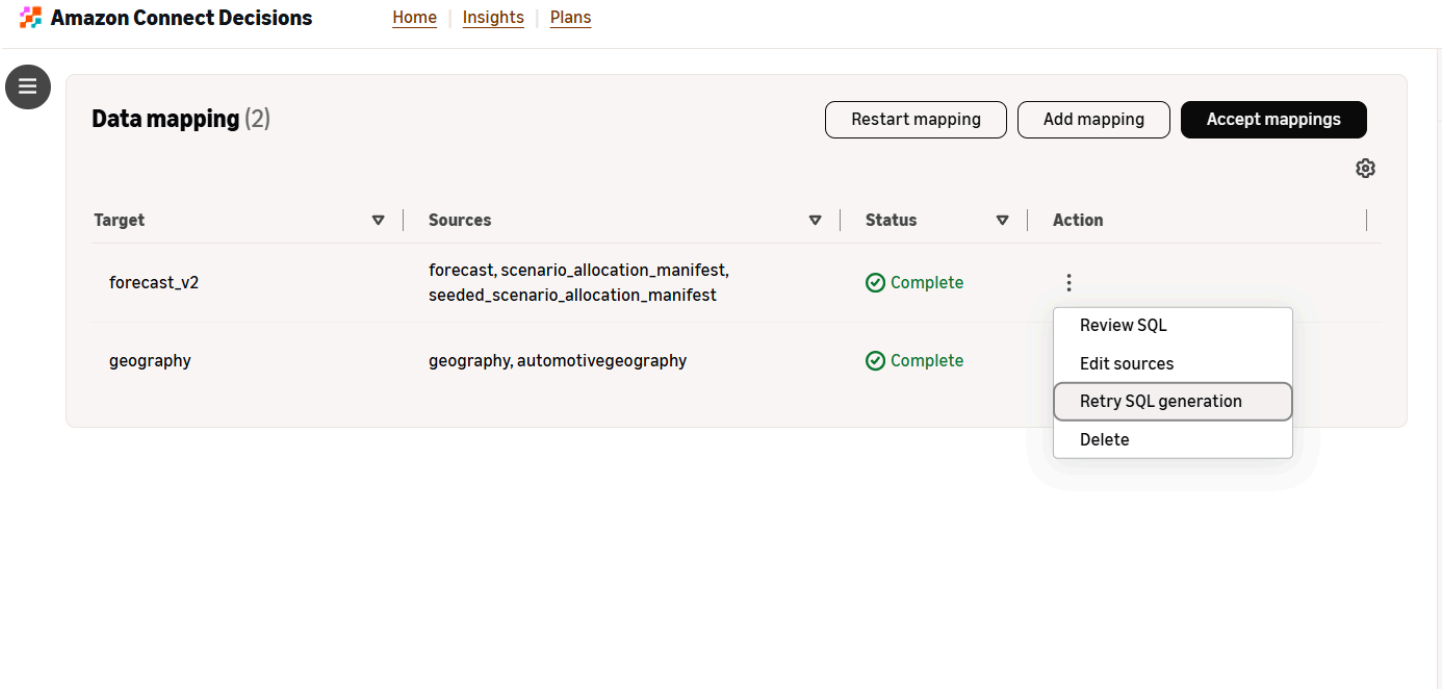
檢閱每個來源資料集的其餘映射。Data Agent 會維持在畫面右側，以取得問題或故障診斷協助。

一旦您滿意所有映射，請按一下接受映射，接受它們以完成資料加入。



處理失敗的映射

如果任何映射失敗，您可以選擇「重新啟動映射」以重新啟動所有映射，或透過「重試 SQL 產生」從動作功能表手動重試單一映射。Data Agent 也可以使用自然語言重試映射，如果錯誤持續存在，則將繼續協助您識別和解決問題。

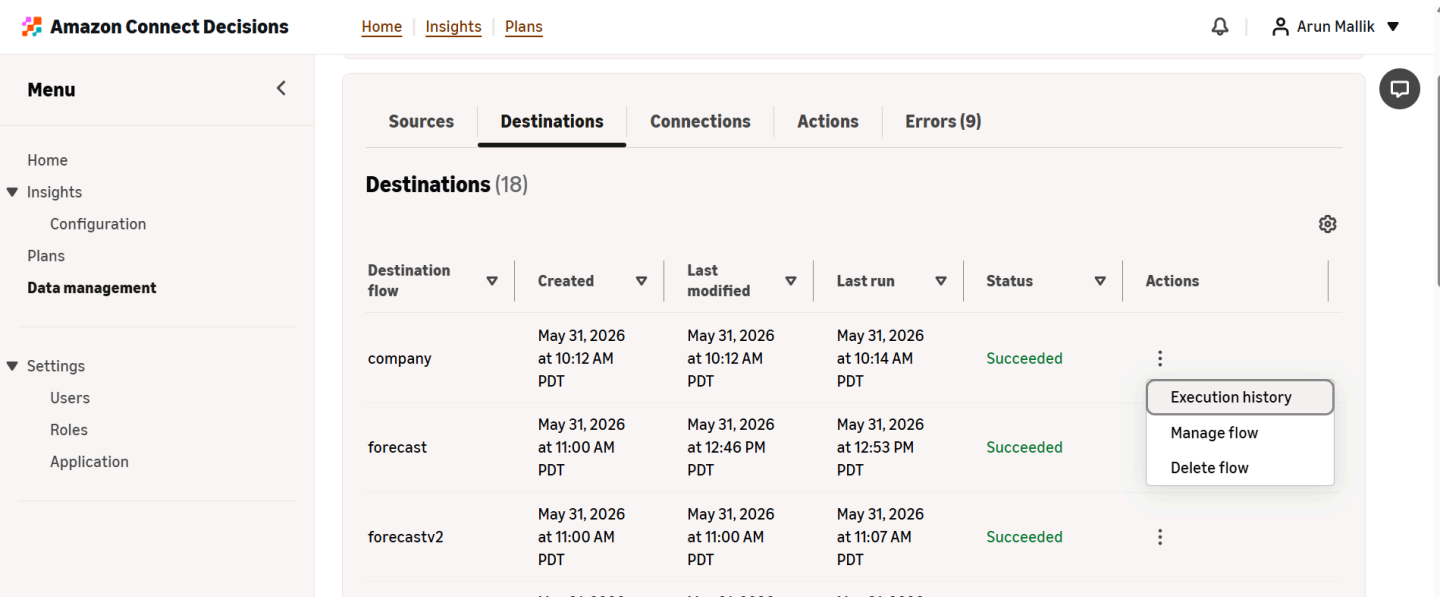


監控您的流程

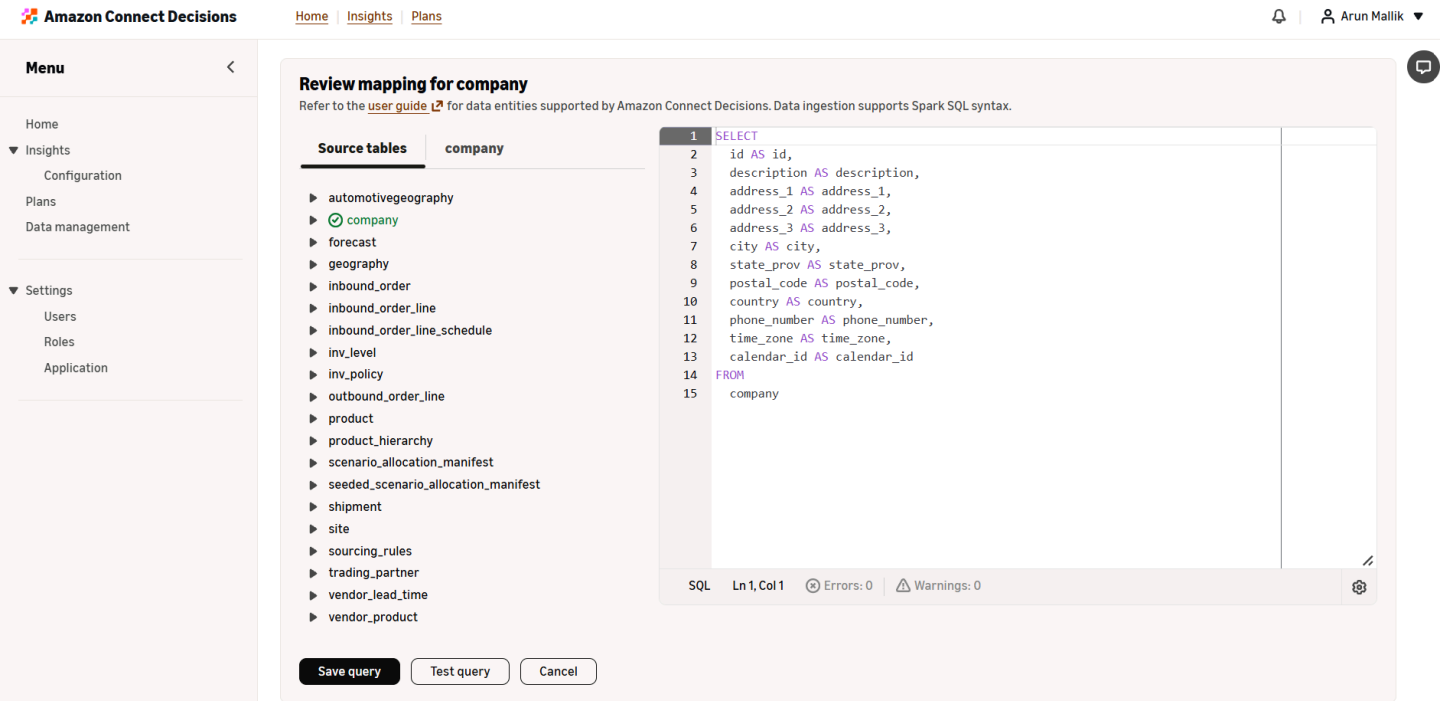
目的地標籤

接受映射後，您將會導覽至資料管理中的目的地索引標籤，您可以在其中：

- 檢閱目的地流程
- 管理和編輯映射 ("Manage Flow")
- 刪除淘汰的流程
- 檢閱這些流程的執行狀態



選取「管理流程」將帶您回到資料映射體驗，您可以在其中繼續與資料代理程式合作，以隨著時間精簡映射。



來源索引標籤

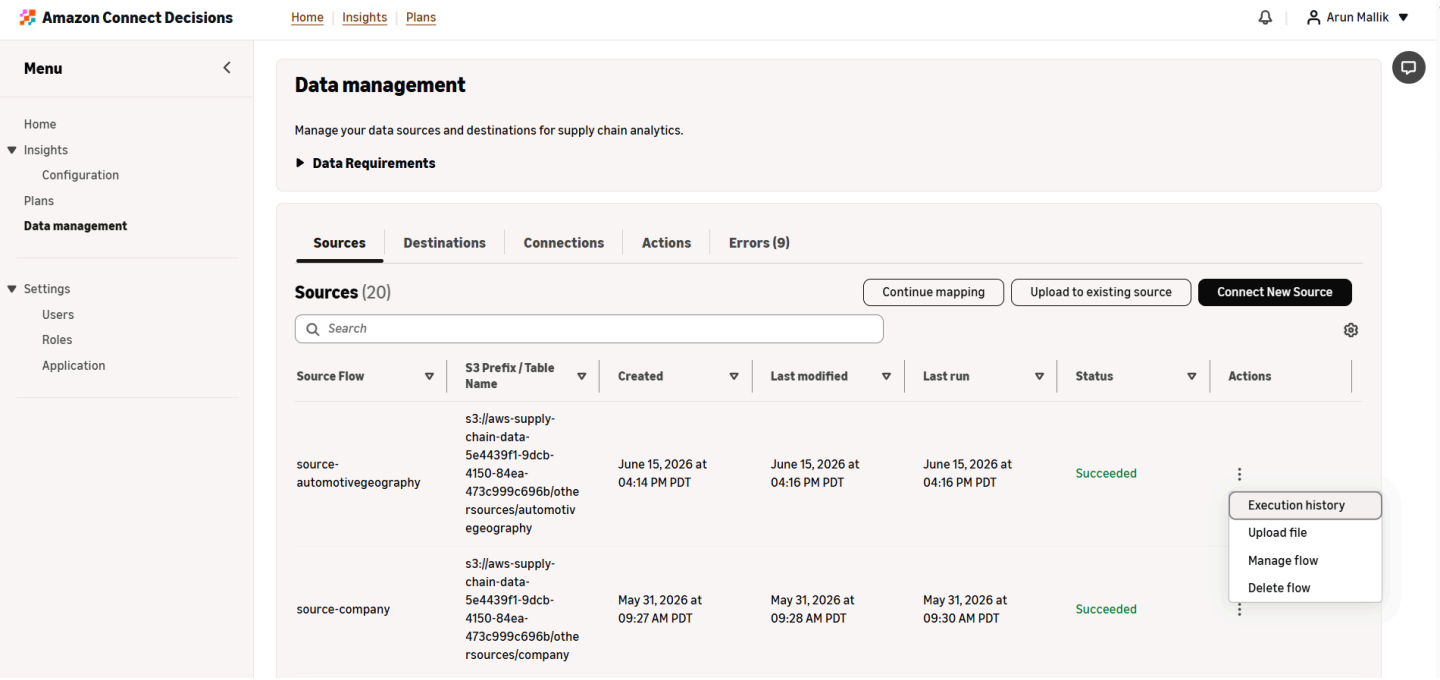
導覽回您可以找到的來源索引標籤：

- 已建立的來源資料集
- 其相關聯的 S3 儲存貯體

- 選項：
  - 透過另一個檔案上傳附加更多來源資料
  - 管理流程
  - 刪除流程
  - 檢閱執行

選取「管理流程」將帶您回到資料映射體驗，您可以在其中繼續與資料代理程式合作，以隨著時間精簡映射。

您也可以視需要存取建立新來源，以重新啟動任何新資料來源的資料加入程序。



最佳實務

資料準備

- 遵循先決條件區段中的步驟
- 對所有 CSV 檔案使用 UTF-8 編碼
- 確保檔案名稱是唯一的
- 上傳前驗證資料品質

使用資料代理程式

- 在您的請求中具體說明
- 當您不了解其任何決策時，請尋求說明
- 在接受之前測試所有 SQL 變更
- 使用預覽功能來驗證轉換

持續維護

- 讓您的來源資料保持最新狀態
- 定期監控流程執行
- 收到通知時立即解決資料錯誤
- 為您的團隊記錄自訂轉換

使用 JDBC 連線至您的資料庫

本指南會逐步引導您使用 Java Database Connectivity (JDBC) 將資料庫連線至 Amazon Connect Decisions。您將為資料庫登入資料設定安全加密，並建立 Amazon Connect Decisions 可用來存取資料的連線。

什麼是 JDBC 連線以及何時應使用它？

JDBC 連線可讓 Amazon Connect Decisions 連線至現有的資料庫以讀取資料，而不是要求您匯出和上傳 CSV 檔案，或設定自己的擷取、轉換、載入 (ETL) 管道至 S3。此方法的理想時機如下：

- 您的資料已存放在與 AWS Glue 相容的關聯式資料庫中。如需相容的資料庫和版本，請參閱本指南。
- 您想要即時或near-real-time的資料存取，無需手動匯出檔案
- 您的資料磁碟區很大且經常更新
- 您偏好將資料保留在目前的位置，而不是將其複製
- 如果您使用的是較小的資料集，或偏好以檔案為基礎的上傳，標準 CSV 上傳程序可能更符合您的需求。如需此程序的詳細資訊，請參閱資料加入使用者指南。

先決條件

開始前，請確保您具備以下條件：

- 具有建立 KMS 金鑰和 Secrets Manager 資源許可的 AWS 帳戶
- 您的 AWS 帳戶 ID 和 Amazon Connect Decisions 將運作的區域
- 資料庫連線詳細資訊：主機名稱、連接埠、資料庫名稱和登入資料
- 對資料庫的管理存取權，以驗證連線能力
- 您的資料庫設定為接受來自 AWS 服務的連線

建立客戶受管 KMS 金鑰

將資料庫連線至 Amazon Connect Decisions 之前，您需要設定資料庫登入資料的加密。AWS Key Management Service (KMS) 提供此安全層，確保您的連線詳細資訊仍受到保護。

建立您的 KMS 金鑰

1. 導覽至 AWS KMS 主控台
   - 在瀏覽器中開啟 AWS 管理主控台
   - 在頂端的搜尋列中，輸入 "KMS"，然後從結果中選取 "Key Management Service"
   - 這會開啟 KMS 儀表板，您將在其中管理加密金鑰
2. 啟動金鑰建立
   - 在 KMS 儀表板上，找到並按一下右上角的建立金鑰按鈕
   - 這會啟動金鑰建立精靈，引導您完成設定程序
3. 設定金鑰類型和用量
   - 在「設定金鑰」頁面上，選取對稱做為金鑰類型 （這是預設和建議的選項）
   - 在金鑰用量下保持選取「加密和解密」
4. 設定金鑰識別詳細資訊
   - 在「Alias」欄位中，輸入金鑰的描述性名稱，例如 `aws-supply-chain-database-key`
   - 在「描述」欄位中，新增內容，例如「Amazon Connect Decisions 資料庫登入資料的加密金鑰」
   - 或者，新增標籤以協助組織和追蹤您的 AWS 資源 （例如，金鑰：「專案」、值：「Amazon Connect 決策」）
5. 定義金鑰管理許可

- 選取應該能夠管理此金鑰的 IAM 使用者或角色（建立、刪除、修改政策）
- 至少包含您自己的管理員角色，以確保您可以視需要稍後修改金鑰
- 這些管理員可以管理金鑰，但不會自動擁有將其用於加密/解密的許可
- 在「金鑰刪除」區段中，允許金鑰管理員刪除此金鑰。（這是預設和建議的選項）

6. 定義金鑰使用許可
   - 在此頁面上，您將看到選擇可使用金鑰之 IAM 使用者和角色的選項
   - 略過在此處選取特定使用者，您將在下一個步驟中設定服務許可
7. 設定 Amazon Connect Decisions 服務的金鑰政策
   - 您將看到具有預設 JSON 的政策編輯器
   - 在 KMS 金鑰政策編輯器中，將下列陳述式附加至您現有的「陳述式」陣列
   - 此政策授予您的帳戶完全控制權，並允許 Amazon Connect Decisions 的服務 (Secrets Manager 和 Glue) 解密您的資料庫憑證

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

8. 檢閱並完成
   - 在摘要頁面上檢閱所有組態設定
   - 確認您的別名、描述和政策正確無誤
   - 按一下完成以建立金鑰
   - 建立後，您將返回 KMS 儀表板，您的新金鑰將出現在清單中

預期事項

金鑰建立是立即的。建立後，您會在 KMS 主控台中看到列出狀態為 "Enabled" 的新金鑰。金鑰現在已準備好在 Secrets Manager 中加密您的資料庫憑證。

設定 AWS Secrets Manager

現在您已擁有 KMS 金鑰，您將在 AWS Secrets Manager 中建立秘密，以安全地存放資料庫憑證，然後設定允許 Amazon Connect Decisions 存取此秘密的資源政策。

建立您的秘密

1. 導覽至 AWS Secrets Manager
   - 在 AWS 管理主控台搜尋列中，輸入「Secrets Manager」
   - 從結果中選取「Secrets Manager」以開啟服務儀表板
2. 開始建立新的秘密
   - 按一下儲存新的秘密按鈕
   - 在「選擇秘密類型」頁面上，選取其他類型的秘密 （這可讓您靈活地建構登入資料）
3. 輸入您的資料庫登入資料
   - 在鍵/值對區段中，將資料庫連線詳細資訊新增為字串：

```
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. 選取您的加密金鑰
   - 在「加密金鑰」下，選取選擇 AWS KMS 金鑰
   - 從下拉式清單中選取您在步驟 1 中建立的 KMS 金鑰 （例如 `aws-supply-chain-database-key`）
   - 這可確保您的登入資料使用客戶受管金鑰加密
5. 為您的秘密命名
   - 輸入秘密的描述性名稱，例如 `aws-supply-chain-production-database`
   - 或者，新增描述，例如「Amazon Connect Decisions 生產環境的資料庫登入資料」
   - 視需要為組織新增標籤 （例如金鑰：「環境」、值：「生產」）

6. 新增資源許可

- 按一下「編輯許可」。在政策編輯器中，貼上下列政策。此政策允許 Amazon Connect Decisions 的服務讀取您的秘密

```
{
  "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. 儲存政策

- 按一下儲存以套用資源政策
- 此政策現在處於作用中狀態，並允許 Amazon Connect Decisions 擷取您的資料庫登入資料

8. 設定輪換 （選用）

- 針對此設定，您可以選取停用自動輪換來略過自動輪換
- 如果您的安全政策需要輪換，您可以稍後啟用輪換

9. Review and create (檢閱和建立)

- 檢閱您的所有秘密詳細資訊
- 按一下儲存以建立秘密
- 您將返回 Secrets Manager 儀表板

10.儲存您的秘密 ARN

- 在秘密清單中尋找新建立的秘密
- 按一下秘密名稱以開啟其詳細資訊頁面
- 在頂端，您會看到秘密 ARN
- 複製並儲存此 ARN
- ARN 格式如下所示： `arn:aws:secretsmanager:us-east-1:123456789012:secret:aws-supply-chain-production-database-AbCdEf`

11.編輯資源許可

- 按一下「編輯許可」

- 貼上複製的秘密 ARN，並將 取代<COPY-THE-SECRET-ARN-HERE-AFTER-CREATING>為您複製的 ARN
- 按一下儲存以連接政策

預期事項

您的秘密現在已使用 KMS 金鑰安全地儲存和加密。Amazon Connect Decisions 的服務具有在建立資料庫連線時擷取憑證的許可，但憑證會保持靜態和傳輸中加密。

將您的資料庫連線至 Amazon Connect 決策

設定 KMS 金鑰和秘密後，您就可以在 Amazon Connect Decisions 中建立 JDBC 連線。

設定您的 JDBC 連線

1. 導覽至 Amazon Connect 決策 > 資料管理
   - 登入您的 Amazon Connect Decisions 執行個體
   - 從主要導覽中，選取「資料管理」
   - 在索引標籤導覽中，導覽至「連線」
   - 選取「新連線」以建立新的連線
2. 輸入您的連線詳細資訊
   - 連線名稱（必要）：輸入此連線的唯一識別符（例如 "production-database")
   - 描述（選用）：新增此連線的目的和使用詳細資訊，以協助您的團隊了解其存取的資料
   - JDBC URL（必要）：以下列格式輸入您的完整 JDBC 連線字串： `jdbc:<database-type>://<hostname>:<port>/<database>`（例如 `jdbc:postgresql://db.example.com:5432/mydb`)
   - 結構描述名稱（選用）：視需要指定資料庫結構描述（例如 "public"、"dbo"、"myschema")。保留空白以使用資料庫的預設結構描述
   - 秘密 ARN（必要）：貼上您從步驟 2 儲存的秘密 ARN。這可讓 Amazon Connect Decisions 從 Secrets Manager 安全地擷取您的資料庫登入資料。
   - 強制執行 SSL 連線：保持選取此核取方塊（建議），以要求資料庫連線使用 SSL/TLS 加密
   - VPC 端點服務名稱（必要）：透過 AWS PrivateLink 輸入私有連線的 VPC 端點服務名稱（格式：`com.amazonaws.vpce.<region>.vpce-svc-xxxxxxxxx`)
3. 連線至您的資料庫

- 按一下「連線」來測試和建立連線。Amazon Connect Decisions 將驗證是否可以使用提供的登入資料成功連線至您的資料庫。此步驟最多可能需要 2 分鐘，因此請勿在連線期間離開此畫面。
- 如果連線成功，您會自動導覽至資料表選擇
- 如果連線失敗：
  - 檢閱您的連線詳細資訊，以確保所有欄位皆正確無誤：
    - 驗證您的秘密 ARN 是否正確
    - 確認您的資料庫登入資料正確無誤
    - 檢查您的 JDBC URL 格式是否正確
    - 確保您的資料庫已設定為接受來自 AWS 服務的連線
    - 確認您的 KMS 金鑰和 Secrets Manager 政策已正確設定
  - 您也可以透過詢問「為什麼我的資料庫連線失敗？」等問題，使用聊天體驗來協助疑難排解連線問題。或「協助我偵錯我的 JDBC 連線」

4. 選取要擷取的資料表
   - 連線後，您會看到選取資料表畫面，顯示資料庫中所有可用的資料表
   - 選取您要擷取之每個資料表旁的核取方塊
5. 設定資料表重新整理排程
   - 針對每個選取的資料表，按一下動作欄中的三點功能表，然後選取「排程重新整理」
   - 在設定載入詳細資訊對話方塊中，設定：
     - Cadence：重新整理的頻率（每小時、每日、每週或自訂）
     - 開始時間：重新整理開始的時間（以 UTC 顯示，並顯示時區位移）
     - 重新整理類型：選擇完成重新整理（取代所有資料）或增量更新（將新資料新增至現有資料；需要選取記錄時間戳記欄）
     - 視需要為每個資料表重複
   - 設定所有資料表時按一下開始映射
6. 繼續資料映射
   - 從現在開始，體驗與我們的資料加入流程相同
   - 遵循資料加入使用者指南中的資料映射區段來完成設定

預期事項

建立連線並選取資料表後，Amazon Connect Decisions 可以從資料庫讀取資料。連線會保持作用中且安全，並透過 AWS Secrets Manager 加密和管理登入資料。您不需要手動更新 Amazon Connect Decisions 中的登入資料，您在 Secrets Manager 中所做的任何變更都會自動反映。

最佳實務

安全與存取管理

- 安全地存放登入資料：一律使用 AWS Secrets Manager 來存放資料庫登入資料，絕不要在連線字串或組態檔案中硬式編碼登入資料
- 啟用 SSL/TLS 加密：保持啟用「強制 SSL 連線」選項，以確保資料傳輸中加密資料
- 定期檢閱 KMS 和 Secrets Manager 政策：確保只有授權的服務和帳戶可以存取您的加密金鑰和秘密
- 使用最低權限存取：僅將最低必要許可授予 Amazon Connect Decisions 將用於連線的資料庫使用者

連線組態

- 使用描述性連線名稱：選擇明確、有意義的名稱來表示環境和用途（例如，「production-inventory-db」而不是「db1」）
- 記錄您的連線：使用描述欄位記下連線存取哪些資料、誰擁有它，以及任何特殊考量
- 在繼續之前測試連線：選取資料表和設定重新整理排程之前，請務必驗證連線是否正常運作
- 驗證 JDBC URL 格式：再次檢查您的 JDBC URL 語法是否符合您的資料庫類型，以避免連線錯誤

資料重新整理策略

- 選擇適當的重新整理節奏：根據來源資料變更的頻率和業務需求，選取重新整理頻率
- 低活動期間排程重新整理：設定資料庫負載較低的重新整理時間，將效能影響降至最低
- 盡可能使用增量更新：對於經常變更的大型資料集，增量更新比完全重新整理更有效率
- 選取有意義的時間戳記資料欄：使用增量更新時，請選擇準確反映記錄建立或修改時間的資料欄

使用聊天進行疑難排解

- 在您的請求中具體說明：在請求協助疑難排解連線或映射問題時提供清晰的內容
- 要求說明：如果您不了解建議或產生的 SQL 查詢，請要求釐清

- 在接受之前測試所有 SQL 變更：使用預覽功能來驗證轉換是否與實際資料如預期般運作
- 利用聊天進行故障診斷：當連線失敗或重新整理遇到錯誤時，詢問診斷問題，例如「為什麼我的連線失敗？」 或「協助我了解此重新整理錯誤」

持續維護

- 定期監控重新整理執行：檢查資料管理中的目的地和來源索引標籤，以確保重新整理成功完成
- 迅速解決錯誤：當 Amazon Connect Decisions 提醒您重新整理失敗時，請快速調查並解決問題，以避免資料漏洞
- 安全地更新登入資料：資料庫密碼變更時，在 AWS Secrets Manager 中更新登入資料，Amazon Connect Decisions 會自動使用新的登入資料
- 文件自訂組態：記下任何特殊重新整理排程、轉換邏輯或連線需求，以供您的團隊參考
- 定期檢閱資料表選擇：隨著資料需求的變化，請重新檢視您正在擷取的資料表，以及重新整理排程是否仍符合業務需求

了解正式資料模型 (CDM)

正式資料模型 (CDM) 是 所使用的標準化資料結構。當您加入供應鏈資料時，它必須轉換為 CDM 格式，以便 可以處理它以進行規劃、預測和操作洞察。

本主題說明什麼是 CDM、它的重要性，以及可用的資料實體。

什麼是 CDM？

CDM 定義一組常見的資料實體和欄位，代表供應鏈概念，例如產品、站點、訂單、貨物和庫存。無論您來源資料的格式或結構為何，CDM 都會提供單一、一致的結構描述，可用於其所有功能。

在資料加入期間，您的來源資料會映射至 CDM 目的地資料表。Data Agent 可以自動建議來源欄位和 CDM 欄位之間的映射，並產生 SQL 轉換查詢以轉換您的資料。

為什麼 CDM 很重要

- 一致性： 中的所有功能都以相同的資料結構運作，確保需求規劃、庫存最佳化和前置時間洞察之間的行為一致。
- 互通性 — 來自不同來源系統 (ERP、WMS、TMS) 的資料會標準化為單一模型，以啟用跨系統分析。
- 簡化加入 — 資料代理程式在產生自動映射時使用 CDM 作為目標結構描述，從而減少手動工作。

- 資料品質：針對 CDM 定義執行驗證檢查，以便在生產環境中使用資料之前發現問題。

資料實體類別

CDM 資料實體分為兩個類別：

- 非交易資料 — 不常變更的參考或主資料，例如產品、網站、交易合作夥伴和地理位置。
- 交易資料 — 經常變更的操作資料，例如預測、庫存水準、訂單和運送。

支援的資料實體

下表列出 CDM 中支援的所有資料實體。

支援的 CDM 資料實體

資料實體	資料類型	必要
公司	非交易資料	是
產品	非交易資料	是
交易合作夥伴	非交易資料	是
供應商產品	非交易資料	是
地理位置	非交易資料	是
產品階層	非交易資料	是
運輸通道	非交易資料	是
供應商前置時間	非交易資料	是
Site	非交易資料	是
供應商假日	非交易資料	是
預測	交易資料	是
Inventory	交易資料	是

資料實體	資料類型	必要
傳入順序 (PO/STO)	交易資料	是
傳出訂單行	交易資料	是
運送	交易資料	是
庫存政策	交易資料	是
傳入順序列 (PO/STO)	交易資料	是
傳出裝運	交易資料	是
傳入順序行排程	交易資料	是

功能所需的實體

並非 中的每個功能都需要所有 CDM 實體。下列各節說明哪些實體需要、選用或不適用於每個功能。

庫存可見性

清查可見性的 CDM 實體

資料實體	資料類型	必要
公司	非交易	選用
產品	非交易	是
交易合作夥伴	非交易	選用
供應商產品	非交易	不適用
地理位置	非交易	選用
產品階層	非交易	選用
運輸通道	非交易	選用
供應商前置時間	非交易	不適用

資料實體	資料類型	必要
Site	非交易	是
供應商假日	非交易	不適用
預測	交易	選用
Inventory	交易	是
傳入順序 (PO/STO)	交易	選用
傳出訂單行	交易	選用
運送	交易	選用
庫存政策	交易	是
傳入順序行	交易	選用
傳出裝運	交易	選用
傳入順序行排程	交易	選用

前置時間洞察

用於前置時間洞察的 CDM 實體

資料實體	資料類型	必要
公司	非交易	選用
產品	非交易	是
交易合作夥伴	非交易	是
供應商產品	非交易	是
地理位置	非交易	選用
產品階層	非交易	選用

資料實體	資料類型	必要
運輸通道	非交易	是
供應商前置時間	非交易	是
Site	非交易	是
供應商假日	非交易	選用
預測	交易	不適用
Inventory	交易	不適用
傳入順序 (PO/STO)	交易	是
傳出訂單行	交易	不適用
運送	交易	是
庫存政策	交易	不適用
傳入順序行	交易	是
傳出裝運	交易	不適用
傳入順序行排程	交易	是

需求規劃

用於需求規劃的 CDM 實體

資料實體	資料類型	必要
公司	非交易	選用
產品	非交易	是
交易合作夥伴	非交易	不適用
供應商產品	非交易	不適用

資料實體	資料類型	必要
地理位置	非交易	選用
產品階層	非交易	選用
運輸通道	非交易	不適用
供應商前置時間	非交易	不適用
Site	非交易	是
供應商假日	非交易	不適用
預測	交易	不適用
Inventory	交易	不適用
傳入順序 (PO/STO)	交易	不適用
傳出訂單行	交易	是
運送	交易	不適用
庫存政策	交易	不適用
傳入順序行	交易	不適用
傳出裝運	交易	不適用
傳入順序行排程	交易	不適用

CDM 與資料加入的關係

當您將資料加入 時，程序會遵循下列步驟：

1. 上傳 — 您可以將來源資料以 CSV 檔案形式上傳至 Amazon S3。
2. 映射 — Data Agent 會分析來源資料集，並建議最符合您資料的 CDM 目的地資料表。
3. 轉換 — SQL 轉換查詢會將來源資料格式轉換為 CDM 格式。
4. 驗證 — 品質檢查會根據轉換的資料執行，以驗證是否符合 CDM 要求。

5. 啟用 — 驗證後，資料會流入 並可供 功能使用。

如需資料加入step-by-step說明，請參閱資料加入主題。

資料驗證和品質檢查

概觀

資料驗證可確保您的資料在執行 Amazon Connect Decisions 功能之前符合品質要求。系統會根據您設定的計劃、指標和規則驗證資料，以識別可能封鎖或降低效能的問題。

資料驗證的運作方式

驗證觸發條件

資料驗證會在下列時間自動執行：

- Insights 組態變更：當您建立或修改指標、規則或其他組態時
- 計劃建立：當您建立臨機操作計劃或在每次排程計劃執行時
- 資料重新整理：每次資料重新整理至目的地流程之後
- 能力執行：在 AI 團隊成員操作之前或期間（例如，當根造成例外狀況或決定建議時）

驗證類型

Amazon Connect Decisions 會執行兩種類型的驗證：

資料存在驗證會根據您設定的資源（指標、規則、計劃），驗證是否已載入必要的資料集和欄位。

資料品質驗證會根據您的設定組態，驗證提供的資料是否符合品質要求，包括：

- 設定條件驗證：確認產品和網站符合您的規則條件（例如產品類別、網站位置）
- 階層驗證：如果您在設定中使用階層，則識別缺少的階層關係
- 範圍驗證：確認已識別產品和網站存在所有必要的資料
- 品質評估：針對操作需求評估資料品質和可用性

漸進式驗證

Amazon Connect Decisions 為具有有效資料的產品和網站啟用 功能，而不是封鎖整個資料集的功能。當驗證問題影響特定產品或網站時，系統會繼續處理具有有效資料的產品和網站、識別具有資料問題的產品或網站，並提醒您需要注意的特定項目。這可讓您開始使用 功能，同時解決剩餘的資料問題。

存取資料驗證錯誤

您可以透過三個進入點檢視資料驗證錯誤：

1. 首頁上的「資料驗證錯誤」指標
2. 首頁上的資料驗證錯誤主題卡
3. 左側導覽 >「錯誤」索引標籤中的「資料管理」

檢閱驗證錯誤

錯誤頁面會顯示所有開啟和已解決的驗證錯誤。您可以依下列任一欄進行搜尋和篩選：

- ID：驗證錯誤的唯一識別符
- 狀態
  - 開啟：錯誤尚未解決
  - 已解決：已修正並驗證錯誤
- 描述：說明資料品質問題
- 問題類型
  - 缺少必要資料：未提供觸發 操作的強制性資料（例如，沒有用於 Supply Plan 的 outbound_order_line 來源資料表）
  - 無效的資料值：資料存在，但包含不正確的值（例如負產品成本）
  - 缺少關係：缺少必要的階層或參考關係（例如缺少產品階層）
  - 資料不足：沒有足夠的資料可供執行所需的操作（例如，需求計劃需要 12 個月的歷史訂單資料，但只有 3 個月）
- 功能：受影響的功能或資源
  - 供應計畫
  - 需求計劃
  - Insight（包括例外狀況、建議和 RCA for Supply or Demand)

- 目的地：受影響的目的地流程
- 優先順序
  - 關鍵：至少一個功能已完全封鎖，無法執行
  - 高：至少有一個功能被部分封鎖（無法處理某些產品或網站）
  - 中：至少一個功能的準確性降低（將執行但結果降低）
- 建立時間：時間戳記顯示第一次偵測到錯誤的時間

檢視錯誤詳細資訊

選取任何錯誤以檢視詳細資訊。詳細資訊畫面會顯示上述資訊，以及上次發生的時間戳記、相關資源和連結（代表受問題影響功能的指標、規則或計劃），以及最多 100 個受影響資料的預覽，其中顯示資料驗證錯誤如何呈現。

可用的動作

從錯誤詳細資訊畫面，您可以：

- 故障診斷：啟動 AI 團隊成員以協助以自然語言對問題進行故障診斷，並接收詳細的修補指導
- 解決錯誤：如果您已修正基礎問題，請手動將錯誤標記為已解決
- 下載：下載完整的受影響資料集以進行詳細分析和更正

解決資料驗證錯誤

解決工作流程

1. 檢閱錯誤描述和優先順序，以了解影響
2. 檢查受影響的資料預覽，以查看哪些特定記錄受到影響
3. 遵循針對修復提供的特定建議
4. 選擇適當的動作：
   - 對於組態問題：與經理和規劃人員合作來調整指標、規則或計劃組態
   - 對於映射問題：正確上傳的來源資料或更新資料轉換和映射
   - 對於遺失或無效的資料：上傳更正的資料
5. 解決基礎問題後，手動將錯誤標記為已解決

使用 AI 團隊成員

使用疑難排解選項來提出問題，例如「我應該先專注於哪些錯誤？」 或「哪些錯誤阻礙了我的需求計劃？」、收到問題及其影響的詳細說明、取得解決方法的step-by-step指引，以及了解錯誤如何影響您的特定組態。AI 團隊成員可以做為解決 Amazon Connect Decisions 和來源資料系統中問題的指南。

最佳實務

- 依嚴重性排定優先順序：先專注於關鍵錯誤，因為它們會完全封鎖執行功能。然後解決部分封鎖處理的高優先順序錯誤，接著是降低準確度的中等優先順序問題。
- 仔細檢閱建議：每個錯誤都包含根據您的組態針對問題量身打造的特定、可行的指導。
- 對您的優勢使用漸進式驗證：使用 功能之前，請不要等待解決每個錯誤。當您為其他人解決問題時，系統會啟用有效產品和網站的功能。
- 資料重新整理後進行監控：在每次資料更新後檢查是否有新的驗證錯誤，在問題影響生產工作流程之前及早發現問題。
- 以策略方式下載受影響的資料：當您需要分析預覽以外的所有受影響記錄，或需要將完整的資料集提供給資料團隊時，請使用下載選項。
- 針對複雜問題使用 AI 團隊成員：疑難排解選項提供情境協助，以適應您的特定情況和組態。
- 驗證解決方案：修正資料問題後，手動將錯誤標記為已解決，以確認您的修正成功，並從開啟清單中移除。

系統組態

Amazon Connect Decisions 中的設定會依範圍和對象進行組織。有些設定是個人設定，可讓每個使用者量身打造自己的體驗。其他則是由管理員管理的執行個體層級組態，會影響系統對所有使用者的行為，或如何連線到更廣泛的技術環境。

使用者層級設定可讓個人管理其帳戶資訊、通知偏好設定，以及其資料存取範圍如何套用至其檢視。

執行個體層級設定可讓管理員設定整個組織的存取控制篩選條件行為、建立與 ERP 和其他外部系統的連線，以及定義系統如何處理建議的動作。

這些設定可讓您的組織靈活地根據特定操作內容調整 Amazon Connect Decisions，同時保持整個團隊的一致性。

使用者設定檔設定

使用者可以透過選取應用程式右上角的名稱，然後從下拉式選單中選擇設定檔來存取其設定檔設定。設定檔頁面可讓使用者管理其帳戶資訊、通知偏好設定和資料存取設定。

存取設定檔設定

若要存取您的設定檔設定：

1. 在頁面右上角選取您的名稱
2. 從下拉式選單中選擇設定檔
3. 設定檔頁面會顯示您的帳戶資訊和設定

設定檔資訊

設定檔頁面會顯示下列帳戶詳細資訊：

使用者：您的使用者名稱

角色：您指派的角色（管理員、經理或規劃人員）

時區：從下拉式選單中選取您偏好的時區。此設定會決定日期和時間在 Amazon Connect Decisions 中的顯示方式。

電子郵件：與您的 Amazon Connect Decisions 帳戶相關聯的電子郵件地址

已建立：您帳戶建立的日期和時間

更新：您的設定檔上次修改的日期和時間

選取右上角的儲存，以儲存設定檔資訊的任何變更。

通知偏好設定

通知偏好設定索引標籤可讓您設定如何接收各種系統事件的通知。您可以選擇在應用程式中透過電子郵件或兩者接收通知。

計劃

計劃產生成功：選擇您希望在計劃產生成功完成時收到通知的方式。選項包括應用程式內通知和電子郵件通知。

計劃產生失敗：選擇您希望在計劃產生失敗時收到通知的方式。選項包括應用程式內通知和電子郵件通知。

Insights 組態

Insights 組態成功：選擇當 Insights 組態成功完成時，您希望收到通知的方式。選項包括應用程式內通知。

Insights 組態失敗：選擇您希望在 Insights 組態失敗時收到通知的方式。選項包括應用程式內通知。

資料擷取

資料擷取失敗：選擇您希望在資料擷取失敗時收到通知的方式。選項包括應用程式內通知和電子郵件通知。

管理員設定

管理員可以設定適用於所有使用者的全系統通知設定。

通知保留：設定系統自動移除通知的天數。輸入數值以指定保留期間。

選取儲存以套用您的通知偏好設定。

指派的範圍

指派範圍索引標籤會顯示您的資料存取許可，並可讓您根據指派的範圍來設定資料檢視的篩選方式。

資料存取

本節顯示您目前的資料存取層級。如果您可以存取所有網站和產品，您會看到「您可以存取所有網站和產品」訊息。

預設檢視篩選條件

依我的指派範圍篩選檢視：啟用時，資料檢視會自動篩選，以僅顯示指派產品和網站中的項目。根據您的偏好開啟或關閉此設定。

啟用此篩選條件時，您只會看到例外狀況、計劃，以及與指派範圍相關的其他資料。停用時，視您的角色許可而定，您可能會看到超出指派範圍的資料。

選取儲存以套用您的篩選條件偏好設定。

存取控制篩選條件切換

如前所述，所有使用者都可以檢視所有例外狀況，無論他們是否已設定適當的產品和網站 （變動動作仍需要適當的存取權）。雖然這可讓您更輕鬆地分享知識，但僅專注於特定產品和網站的使用者可能會因為其他產品和網站的例外狀況或建議而感到不堪負荷。為了協助使用者專注於對其重要的例外狀況和建議，他們可以使用存取檢視切換，如下所示：

- 首先，具有 'Admin' 角色的使用者必須在該執行個體上啟用 功能。從左側導覽列導覽至執行個體設定頁面
- 根據預設，他們將看到一個切換，該切換會設定整個執行個體的預設存取檢視篩選條件。'Admin' 可以決定為執行個體中的所有使用者有一個統一設定，或讓使用者決定其偏好設定
- 如果他們選擇統一存取檢視切換設定，'Admin' 也可以決定是否應為所有使用者啟用或停用切換
- 如果他們選擇讓每個使用者選取自己的偏好設定，則每個使用者都可以自行切換存取檢視篩選條件。每個使用者可以從畫面右上角的使用者下拉式清單導覽至使用者偏好設定頁面

變更執行個體的存取控制切換：

1. 選擇設定左側抽屜
2. 選取應用程式

3. 更新切換並按一下儲存設定

如果啟用設定，系統會自動篩選例外狀況和建議清單頁面，僅顯示針對與存取控制組態相符的產品 OR 網站所產生的頁面

對於已啟用「授予所有產品和網站的完整存取權」的使用者，存取檢視切換仍然會顯示所有例外狀況和建議。如果使用者已停用切換功能，但未設定任何產品或網站，系統會將該系統解釋為無法存取任何產品和網站，因此使用者不會看到任何內容

存取檢視篩選條件被視為不同類型的篩選條件，因此不會在例外狀況和建議頁面的篩選條件晶片中顯示 。使用者仍然可以像以前一樣套用其他篩選條件，包括其他產品和網站篩選條件

如果使用者關閉存取檢視切換開關，或具有直接超連結，使用者仍然可以存取其他產品或網站的例外狀況和建議

設定與 ERP 的連線

若要讓 Amazon Connect Decisions 在企業資源規劃 (ERP) 系統中代表您執行操作，您必須設定連線，指定必要的連線參數，以及 Amazon Connect Decisions 在操作期間應使用的登入資料。

支援的 ERP 系統：

- SAP S/4HANA

在 Secrets Manager 中設定登入資料

1. 使用您的帳戶，使用 Secrets Manager 建立 Secrets Manager 秘密
   - 在 Secrets Manager 中輸入登入資料時，請將以下預留位置值 (<username> 和 <password>) 取代為 Amazon Connect Decisions 應使用的實際使用者名稱和密碼
   - 如果使用 主控台，請`Other type of secret`為 選擇 `Secret Type`
   - 如果透過主控台中的`Key/value pairs`索引標籤輸入詳細資訊，請輸入 2 對：
     - 金鑰：`username`；值： *<username>*
     - 金鑰：`password`；值： *<password>*
   - 如果使用 `Plaintext`標籤在主控台中輸入秘密，請使用兩個配對輸入 JSON 物件：

```
{
  "Username": "<username>",
```

```
  "Password": "<password>"
}
```

2. 使用 AWS KMS 金鑰加密秘密，並記下金鑰的 ID，因為後續步驟中會需要它
3. 建立秘密後，請記下其 Amazon Resource Name (ARN)，因為後續步驟中會需要它
   - 例如： `arn:aws:secretsmanager:<Region>:<AccountId>:secret:<SecretName>-<SixRandomCharacters>`

設定 KMS 金鑰的許可

您需要提供 Amazon Connect Decisions 存取和使用它所需的許可。

1. 更新您的 KMS 政策，以允許 Amazon Connect Decisions 透過執行個體角色存取您的金鑰
   - 注意：將 <YourAccountNumber> 和 取代<YourInstanceID>為 AWS 您的帳戶和 Amazon Connect Decisions 執行個體 ID。

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

2. 更新執行個體角色的內嵌政策，以授予金鑰的許可
   - 注意：將 <YourSecretArn>、 <YourAccountNumber>和 取代<YourInstanceID>為您的秘密 ARN、 AWS 帳戶和 AWS 供應鏈執行個體 ID。

```
{
```

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

更新秘密的 Secrets Manager 資源政策

1. 更新秘密的 Secrets Manager 資源政策
   - 注意：<YourSecretArn>將 取代為您秘密的 ARN

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

設定 Amazon Connect Decisions Connection

1. 在您的 Amazon Connect Decisions 執行個體中，導覽至資料管理頁面
2. 選取Connections標籤
3. 按一下 Create Connection 按鈕
4. 在 Create Connector頁面中，按一下SAP S/4HANA連接器類型的列上的Select按鈕
5. 在Configure SAP S/4HANA API Connector頁面中，輸入必要的資訊：
   - Connection Name：唯一連線名稱
   - API Endpoint URL：SAP S/4HANA 執行個體的 OData API 端點 URL （例如：https://<hostname>:<port>)
   - Client Number：3 位數 SAP 用戶端號碼 （例如：100)
   - Secret ARN：存放 Amazon Connect Decisions 所用登入資料的 Secrets Manager 中秘密的 Amazon Resource Name (ARN)
6. 按一下Create Connector按鈕

設定動作設定

Amazon Connect Decisions 可讓您控制應該針對哪些動作類型，在企業資源規劃 (ERP) 系統中代表您執行操作。根據預設，所有動作類型都會停用，而且您必須為每個所需的動作類型啟用此功能。

> **Note**
>
> 啟用特定動作類型的支援，可控制 Amazon Connect Decisions 代表您執行動作的選項是否會在整個系統中顯示 （例如：使用指定類型的建議檢閱 Insight 時）。在您接受特定建議之前，Amazon Connect Decisions 不會執行這些動作 （即使已啟用支援）。

支援的動作類型：

- 建立採購訂單
- 更新採購訂單
- 取消採購訂單

為每個動作類型設定動作支援：

1. 在您的 Amazon Connect Decisions 執行個體中，導覽至資料管理頁面
2. 選取Actions標籤
3. 在清單中尋找您要設定的動作類型
4. 若要啟用 動作類型的支援：
   - 選取該動作類型的下拉式選單中列出的其中一個連線
   - 注意：下拉式清單只會顯示已設定支援 Actions功能的類型之可用連線 （例如：SAP S/4HANA)
5. 若要停用對 動作類型的支援：
   - 選取該動作類型的下拉式選單No connection中的
6. 按一下Save以儲存您的變更

安全

的雲端安全 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構專為滿足最安全敏感組織的需求而建置。

安全性是 AWS 與您之間的共同責任。共同責任模型 將此描述為雲端的安全和雲端內的安全：

- 雲端的安全性 – AWS 負責保護在 中執行 AWS 服務的基礎設施 AWS 雲端。 AWS 也為您提供可安全使用的服務。在 AWS 合規計劃中，第三方稽核員會定期測試並驗證我們的安全功效。若要了解適用於 Amazon Connect Decisions 的合規計劃，請參閱合規計劃範圍內的 AWS 服務。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件有助於您了解如何在使用 Amazon Connect 時套用共同責任模型。下列主題說明如何設定 Amazon Connect Decisions 以符合您的安全與合規目標。

資料保護

AWS 共同責任模型適用於 Amazon Connect Decisions 中的資料保護。如此模型所述， AWS 負責保護執行所有 AWS 雲端的 全球基礎設施。您負責維護在此基礎設施上託管內容的控制權。您也必須負責您所使用 AWS 服務的安全組態和管理任務。如需有關資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需歐洲資料保護的相關資訊，請參閱 AWS 安全部落格上的 AWS 共同責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您保護 AWS 帳戶登入資料，並使用 AWS Identity and Access Management (IAM) 設定個別使用者。如此一來，每個使用者都只會獲得授予完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源通訊。建議使用 TLS 1.2 或更新版本。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案，以及 服務中的所有 AWS 預設安全控制。
- 使用進階受管安全服務，例如 Amazon Macie，可協助探索和保護存放在 Amazon Simple Storage Service 中的敏感資料。
- 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-2 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 AWS Amazon Connect Decisions 或使用 管理主控台、API、AWS Command Line Interface (AWS CLI) 或 AWS SDKs的其他 AWS 服務時。您輸入用於名稱的標籤或任意格式文字欄位的任何資料都可用於帳單或診斷日誌。

資料加密

本主題提供 Amazon Connect Decisions 有關傳輸中加密和靜態加密的特定資訊。

傳輸中加密

客戶與 Amazon Connect Decisions 之間的所有通訊，以及 Amazon Connect Decisions 與其下游相依性之間的通訊，都會使用 TLS 1.2 或更新版本的連線進行保護。

靜態加密

Amazon Connect Decisions 使用 DynamoDB 和 Amazon Simple Storage Service (Amazon S3) 存放靜態資料。根據預設，靜態資料會使用加密解決方案進行 AWS 加密。Amazon Connect Decisions 會使用來自 AWS Key Management Service () 的 AWS 擁有加密金鑰來加密您的資料AWS KMS。您不需要採取任何動作來保護加密資料的 AWS 受管金鑰。如需詳細資訊，請參閱《 AWS KMS 開發人員指南》中的 AWS 擁有的金鑰。

如果您在 AWS 主控台中變更用來加密 Amazon Connect Decisions 執行個體上資料的 KMS 金鑰，您必須建立新的執行個體，才能開始使用新的金鑰來加密您的資料。任何使用上一個金鑰加密的資料都不會保留，而且只會使用更新後的金鑰加密資料。如果您想要從先前的加密方法維護資料，您可以還原到在這些對話期間使用的金鑰。

您在 Web 應用程式和聊天應用程式中與 Amazon Connect Decisions 的對話只會使用 AWS 擁有的金鑰加密。

跨區域處理

Amazon Connect Decisions 採用 Amazon Bedrock 技術，並使用跨區域推論 (CRIS) 將流量分散到不同 AWS 區域，以增強大型語言模型 (LLM) 推論效能和可靠性。利用跨區域推論可實現以下目標：

- 在高需求期間提高輸送量和彈性
- 提升效能
- 存取新推出的 Amazon Connect Decisions 功能和功能，這些功能依賴於 Amazon Bedrock 上託管的最強大 LLMs

根據建立 Amazon Connect Decisions 執行個體 AWS 所在的區域，跨區域推論的運作方式會有所不同。

對於在美國地理區域建立的所有執行個體，Amazon Connect Decisions 將使用全域 CRIS。這表示推論請求將路由到全球支援的商業 AWS 區域，最佳化可用資源並實現更高的模型輸送量。請參閱 Amazon Bedrock 使用者指南，進一步了解 Global CRIS。

對於在歐盟地理區域建立的所有執行個體，Amazon Connect Decisions 將使用地理 CRIS。這表示推論請求會保留在原始資料所在地理位置的 AWS 區域中。請參閱 Amazon Bedrock 使用者指南，進一步了解地理 CRIS。

例如，從美國東部（維吉尼亞北部）(us-east-1) 區域中建立的 Amazon Connect Decisions 執行個體提出的請求，可以路由到全球任何 AWS 區域，例如亞太區域（雪梨）(ap-southeast-2)。不過，對於從歐洲（愛爾蘭）(eu-west-1) 區域建立的 Amazon Connect Decisions 執行個體提出的請求，會路由到歐洲（法蘭克福）(eu-central-1) 等歐洲 AWS 區域。如需詳細資訊，請參閱 Amazon Connect Decisions 支援的 區域。

雖然跨區域推論不會變更資料存放位置，但您的請求和輸出結果可能會移動到原始資料所在的區域之外。所有資料在 Amazon 的安全網路上傳輸時，都會經過加密。使用跨區域推論無需額外付費。如需有關使用 Amazon Connect Decisions 時資料存放位置的資訊，請參閱 Amazon Connect Decisions 中的資料保護。

適用於 Amazon Connect 決策的 IAM

AWS Identity and Access Management (IAM) 是一種 AWS 服務，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證（登入）和授權（具有許可）來使用 Amazon Connect Decisions 資源。IAM 是一種您可以免費使用的 AWS 服務。

IAM 如何使用 Amazon Connect Decisions

在您使用 IAM 管理 Amazon Connect Decisions 的存取權之前，請先了解哪些 IAM 功能可與 Amazon Connect Decisions 搭配使用。若要全面了解 Amazon Connect Decisions 和其他 AWS 服務如何與大多數 IAM 功能搭配使用，請參閱《IAM 使用者指南》中的可與 IAM 搭配使用的 AWS 服務。

Amazon Connect Decisions 的身分型政策

支援身分型政策：是

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素參考。

Amazon Connect Decisions 中的資源型政策

支援資源型政策：否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。委託人可以包括帳戶、使用者、角色、聯合身分使用者 AWS 或服務。

如需啟用跨帳戶存取權，您可以在其他帳戶內指定所有帳戶或 IAM 實體作為資源型政策的主體。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的快帳戶資源存取。

Amazon Connect Decisions 的政策動作

支援政策動作：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。政策會使用動作來授予執行相關聯動作的許可。

Amazon Connect Decisions 中的政策動作在動作之前使用以下字首：

```
scn
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

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

Amazon Connect Decisions 的政策資源

支援政策資源：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

`Resource` JSON 政策元素可指定要套用動作的物件。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (*) 表示該陳述式適用於所有資源。

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

Amazon Connect Decisions 的政策條件索引鍵

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON 政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

`Condition` 元素會根據定義的條件，指定陳述式的執行時機。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的 AWS 全域條件內容索引鍵。

搭配 Amazon Connect Decisions 使用臨時登入資料

支援臨時憑證：是

臨時登入資料提供 AWS 資源的短期存取權，當您使用聯合或切換角色時，會自動建立。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 的 IAM 和 AWS 服務的臨時安全登入資料。 https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_aws-services-that-work-with-iam.html

轉送 Amazon Connect Decisions 的存取工作階段

支援轉寄存取工作階段 (FAS)：是

轉送存取工作階段 (FAS) 使用呼叫 AWS 服務的委託人許可，結合 請求 AWS 服務向下游服務提出請求。如需提出 FAS 請求時的政策詳細資訊，請參閱轉發存取工作階段。

Amazon Connect Decisions 的服務角色

支援服務角色：是

服務角色是服務擔任的 IAM 角色，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以將許可委派給 AWS 服務。

> **Warning**
>
> 變更服務角色的許可可能會中斷 Amazon Connect Decisions 功能。只有在 Amazon Connect Decisions 提供指引時，才能編輯服務角色。

身分型政策範例

根據預設，使用者和角色沒有建立或修改 Amazon Connect Decisions 資源的許可。他們也無法使用 AWS 管理主控台、 AWS 命令列界面 (AWS CLI) 或 AWS API 來執行任務。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

執行個體管理 IAM 政策

以下是透過主控台或公有 API 建立、更新或刪除執行個體所需的 IAM 政策 （ 不包含所有 Webapp 操作 ）。

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

政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 Amazon Connect Decisions 資源。這些動作可能會讓您的 AWS 帳戶產生成本。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用 AWS 受管政策來授予許多常見使用案例的許可。在您的 AWS 帳戶中提供了這些政策。我們建議您定義特定於使用案例的 AWS 客戶管理政策，以便進一步減少許可。如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策或任務函數的 AWS 受管政策。

- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱《IAM 使用者指南》中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定服務使用服務動作，您也可以使用條件來授予存取 AWS 服務動作的權限，例如 CloudFormation。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM Access Analyzer 驗證政策。
- 需要多重要素驗證 (MFA) – 如果存在需要 AWS 帳戶中 IAM 使用者或根使用者的情況，請開啟 MFA 提供額外的安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的透過 MFA 的安全 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱《IAM 使用者指南》中的 IAM 安全最佳實務。

疑難排解 IAM

使用以下資訊來協助您診斷和修正使用 Amazon Connect Decisions 和 IAM 時可能遇到的常見問題。

我無權在 Amazon Connect Decisions 中執行動作

如果您無權執行 動作的 AWS 管理主控台，則必須聯絡管理員尋求協助。您的管理員是為您提供使用者名稱和密碼的人員。

下列範例錯誤會在`mateojackson` IAM 使用者嘗試使用主控台檢視一個虛構 `my-example-widget` 資源的詳細資訊，但卻無虛構 `scn:GetWidget` 許可時發生。

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

在此情況下，Mateo 會請求管理員更新他的政策，允許他使用 `my-example-widget` 動作存取 `scn:GetWidget` 資源。

我未獲授權執行 iam:PassRole

如果您收到錯誤，告知您無權執行 `iam:PassRole`動作，您的政策必須更新，以允許您將角色傳遞給 Amazon Connect Decisions。

有些 AWS 服務可讓您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為 的 IAM `marymajor` 使用者嘗試使用主控台在 Amazon Connect Decisions 中執行動作時，會發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞給服務的許可。

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

在這種情況下，Mary 的政策必須更新，允許她執行 `iam:PassRole` 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想要允許 AWS 帳戶外的人員存取我的 Amazon Connect Decisions 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要了解 Amazon Connect Decisions 是否支援這些功能，請參閱 Amazon Connect Decisions 如何與 IAM 搭配使用。
- 若要了解如何在您擁有的 AWS 帳戶中提供資源的存取權，請參閱《IAM 使用者指南》中的為您擁有的另一個 AWS 帳戶中的 IAM 使用者提供存取權。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的將存取權提供給第三方擁有 AWS 的帳戶。
- 如需了解如何透過聯合身分提供存取權，請參閱《IAM 使用者指南》中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。

第三方子處理器

Amazon Connect Decisions 使用第三方 API Boomi，以便在外部系統中代表您採取動作。當您使用連線至第三方系統的 Amazon Connect Decisions 功能時，您授權我們使用 Boomi 做為整合中介軟體來傳輸和處理您的加密資料；您的資料不會單獨存放在 Boomi 中。

若要進一步了解 Boomi 及其運作方式，請參閱 Boomi 的公有文件。

支援的區域

此頁面說明您可以使用 Amazon Connect Decisions AWS 的區域。如需 AWS 區域的詳細資訊，請參閱《帳戶管理參考指南》中的指定 AWS 您的帳戶可以使用的區域。 AWS

您的資料可能會在與使用 Amazon Connect Decisions 的區域不同的區域中處理。如需 Amazon Connect Decisions 中跨區域處理的資訊，請參閱跨區域處理。如需處理期間資料儲存位置的相關資訊，請參閱資料保護。

支援的區域

Amazon Connect Decisions 可在下列 AWS 區域的 AWS 管理主控台、 AWS 主控台行動應用程式、 AWS 網站、 AWS 文件網站中取得。這些區域預設為啟用，表示您不需要啟用即可使用。如需詳細資訊，請參閱預設啟用的區域。

您可以在下列區域中使用 Amazon Connect Decisions。

AWS 區域名稱	程式碼名稱	地理區域 （美國、歐洲等）
美國東部 (維吉尼亞北部)	us-east-1	美國
歐洲 (愛爾蘭)	eu-west-1	歐盟

疑難排解

在設定或day-to-day使用 Amazon Connect Decisions 期間發生問題時，本節提供指引，協助您診斷和解決最常見的問題。首先找出最符合您所遇到問題的類別，然後遵循相關頁面上的疑難排解步驟。如果您不確定適用哪個類別，請從常見設定問題開始，該問題涵蓋最廣泛的初始組態問題。

常見的設定問題

參考完整性錯誤：「product_id 值與產品資料集中的任何 ID 不相符」

最常見的原因是 ID 欄位中的結尾空格。從固定寬度資料庫匯出的來源系統通常會以空格填補字串欄位。產品主節點可能有乾淨的 IDs("MAT604")，而訂單列檔案有填充 IDs("MAT604")。系統會執行嚴格的字串比對，因此這些字串不會加入。

修正：將 TRIM() 新增至資料流程 SQL 轉換中的所有字串 ID 欄位。將其套用至 product_id、Ship_from_site_id、Customer_tpartner_id 和任何其他聯結金鑰。同時檢查檔案之間的引號不一致。重新匯出 CSVs時，請使用 QUOTE_ALL 來防止類型推論問題，其中數字外觀 IDs（例如 "111613") 在另一個檔案和字串中被視為整數。

預防：始終 TRIM SQL 轉換中的所有 ID 欄位作為預設實務，即使您今天沒有看到問題。來源資料可能會在匯出之間變更。

產品主伺服器缺少訂單歷史記錄中的產品

您的訂單歷史記錄通常包含不在目前產品主伺服器中的產品（已停產的產品、一次性項目、測試 SKUs)。如果任何 product_id 沒有相符的產品主記錄，系統將拒絕整個訂單檔案。

修正：(a) 為缺少具有最少必要欄位 (id、 description、base_uom) 的產品在產品主節點中建立 Stub 資料列，或 (b) 篩選訂單歷史記錄，只包含產品主節點中存在的產品。選項 (a) 是偏好的，因為它保留了對譜系和趨勢偵測可能有用的需求歷史記錄。

產品主控上傳的 CSV 剖析錯誤

包含逗號、引號或特殊字元的產品描述可能會中斷 CSV 剖析。您可能會在特定資料列上看到「預期 17 個欄位，看到 19」等錯誤。

修正：使用適當的引號 (QUOTE_ALL) 重新匯出檔案。在描述欄位中檢查內嵌逗號的特定失敗資料列。

上傳後未顯示的資料

- 確認您的檔案格式未變更（延伸、資料欄標頭、編碼）。
- 檢查檔案名稱和副檔名是否符合預期的模式 — 將 .csv 重新命名為 .csv000 或類似項目會中斷擷取。
- 上傳後，最多需要 30 分鐘才能完成資料擷取。
- 如果資料欄標頭在載入之間變更（例如，以月/年命名的資料欄），則需要預先處理步驟才能上傳。

資料重新整理後 PIV 未更新

- PIV 會在擷取完成後約 15 分鐘觸發，並執行約 20-30 分鐘。
- 從資料上傳到新 PIV End-to-end：約 1–1.5 小時。
- 如果 PIV 未在超過 24 小時內更新，請聯絡 支援。

例外狀況計數似乎過高或過低

- 太高：閾值可能太鬆，或單一產品 + 網站在不同日期產生多個例外狀況。聯絡 支援以檢閱規則組態。
- 太低：閾值可能太嚴格，或某些產品可能缺少必要的資料（例如預測、庫存層級）。

抽查一些您熟悉的產品，並比較系統顯示的內容與來源系統。

在例外狀況上沒有顯示財務影響

財務影響需要將單位成本填入產品資料中。如果某個產品的成本遺失或為零，則不會顯示美元值。向您的支援團隊確認成本資料涵蓋範圍 — 跨多個成本欄位的瀑布式方法通常提供最佳涵蓋範圍。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。