aws

관리자 안내서

Amazon Connect 결정

Amazon Connect 결정: 관리자 안내서

Table of Contents

Amazon Connect 결정이란 무엇입니까?

Amazon Connect Decisions는 AI 팀원과 협력하는 공급망 계획 및 인텔리전스 솔루션으로, 팀과 협력하여 수요 신호를 합의된 예측으로 조정하고, 제약 인식 공급 계획을 생성하고, 운영을 적극적으로 모니터링하여 문제를 예방하고, 문제를 해결하고, 지속적인 개선을 위한 근본 원인을 식별합니다.

AI 팀원은 운영 절차 및 규칙에 따라 작동하고, 기존 시스템과 통합하고, 실무자의 결정을 통해 학습하는 등 작업 방식에 적응합니다. Amazon 공급망 전문 지식을 활용하여 첫날부터 효과적인 계획과 권장 사항을 제공합니다.

조정을 처리하고 작업을 실행하는 AI 에이전트 팀을 이끌면 서비스 수준과 운영 자본 효율성을 높이는 전략적 결정에 집중할 수 있습니다.

이점

비즈니스에 맞게 조정

AI 팀원은 비즈니스, 시스템 및 결정에 적응하여 기존 워크플로 내에서 신속하게 혁신을 제공합니다. 운영 절차 및 비즈니스 규칙에 따라 팀원은 기존 계획 및 ERP 시스템을 사용합니다. 계획자의 결정을 통해 학습하여 우선순위에 부합하고 지식을 체계화하여 시간이 지남에 따라 운영을 개선하고 모든 팀원이 더 효과적입니다.

다가오는 상황에 미리 대비합니다.

24/7 조정 작업을 처리하는 AI 에이전트 팀을 리드하여 수요 신호를 조화시키고, 제약 조건 인식 계획을 생성하고, 승인된 작업을 실행합니다. 또한 팀원은 수천 개의 SKUs에 걸쳐 공급업체 중단 또는 인벤토리 정렬 오류를 계단화하는 등 수동 분석에 보이지 않는 패턴을 감지하고 문제가 되기 전에 중요한 사항을 표시합니다. 플래너는 사후 대응 소방에서 사전 예방 계획으로 전환하여 비즈니스 성과를 높이는 전략적 결정을 통해 보다 효과적인 운영을 실행하고 서비스 수준을 개선합니다.

첫날부터 신뢰 구축

AI 팀원은 30년 이상 400M 개 이상의 Amazon SKUs를 감독하고 전문 공급망 도구를 갖춘 과학의 지원을 받습니다. 팀은 세계에서 가장 복잡한 공급망 네트워크 중 하나가 제공하는 도메인 전문 지식을 활용하여 신뢰할 수 있고 확인할 수 있는 명확하고 설명 가능한 근거와 함께 실행 가능한 인사이트와 권장 사항을 out-of-the-box 제공합니다.

기능

적응형 인텔리전스

AI 팀원은 패턴을 관찰하고, 중요한 것을 감지하고, 조치를 권장하고, 승인된 결정을 실행하는 등 지속적인 루프를 통해 모든 계획과 결정을 통해 학습합니다. 이렇게 하면 지식이 제도화됩니다. 플래너가 떠나면 전문 지식이 유지됩니다. 새 구성원은 첫날부터 생산적이므로 수동 재훈련 없이 결과를 개선할 수 있습니다.

수요 인텔리전스

AI 팀원은 Amazon 데이터에 대해 훈련된 18개 이상의 예측 도구 및 파운데이션 모델을 동적으로 오케스트레이션하여 SKU 수준에서 자율적으로 최적화합니다. 기록이 제한적이더라도 첫날부터 정확한 예측을 생성합니다. 정확도를 지속적으로 모니터링하면서 합의 계획을 통해 통계 예측, 고객 약정 및 부서 간 입력을 통합합니다.

공급 인텔리전스

AI 팀원은 미래 예측형 공급 계획(미리 보기)을 생성하고 예외를 영향별로 순위가 매겨진 전략적 결정으로 지능적으로 클러스터링합니다. 네트워크에서 제약 인식 계획을 위한 최적화 모델을 실행합니다. 연중무휴로 작업을 모니터링하고, 중요한 사항을 파악한 다음 기존 시스템에서 승인된 결정을 직접 실행하여 주기를 몇 주에서 몇 시간으로 줄입니다.

에이전트 온보딩

AI 기반 온보딩 에이전트는 자연어 대화를 통해 설정을 안내합니다. JDBC 또는 Amazon S3를 통해 조각화된 데이터를 연결하고, Connect 결정을 준비하고, 예측에 영향을 미치기 전에 문제에 자동으로 플래그를 지정합니다. 실시간 미리 보기를 사용하여 비즈니스 규칙 및 정책을 일반 언어로 구성하여 몇 달이 아닌 몇 주 만에 운영할 수 있습니다.

시작하기

이 섹션에서는 Amazon Connect Decisions 인스턴스를 생성하고, 사용자 권한 역할을 부여하고, Amazon Connect Decisions 웹 애플리케이션에 로그인하는 방법을 배울 수 있습니다.

Amazon Connect 결정을 사용하기 위한 사전 조건

Amazon Connect Decisions 인스턴스를 생성하기 전에 다음 단계를 완료해야 합니다.

- AWS 계정이 있습니다. AWS 계정을 생성하려면 AWS 계정 설정을 참조하세요.
- IAM Identity Center가 활성화되어 있는지 확인합니다. IAM Identity Center를 활성화하려면 IAM Identity Center 활성화를 참조하세요.
- Amazon Connect Decisions 인스턴스를 생성하려는 리전과 동일한 리전에서 IAM Identity Center 인스턴스를 활성화해야 합니다. Amazon Connect Decisions는 미국 동부(버지니아 북부) 및 유럽(아일랜드) 리전에서만 지원됩니다.
- Amazon Connect Decisions 인스턴스가 기존 IAM Identity Center 리전과 동일한 리전에 있지 않은 경우 추가 지원을 위해 문의하세요.
- Amazon Connect 결정 관리자로 할당할 IAM Identity Center 인스턴스에 사용자가 한 명 이상 있어야 합니다. Active Directory를 IAM Identity Center에 연결할 수 있습니다. 자세한 내용은 Microsoft AD 디렉터리에 연결을 참조하세요.
- Amazon Connect Decisions에 액세스해야 하는 사용자를 IAM Identity Center에 추가합니다.
- 인스턴스를 생성하려면 AWS Key Management Service(AWS KMS)가 필요합니다. Amazon Connect Decisions는이 AWS KMS 키를 사용하여 Amazon Connect Decisions로 들어오는 모든 데이터를 암호화합니다. AWS KMS 키에 대한 자세한 내용은 키 생성을 참조하세요.
- 작업 기능을 활성화하려는 경우 관련 데이터를 유지 관리하는 데 사용하는 시스템에 대한 연결을 구성하고 Amazon Connect Decisions가 사용할 자격 증명을 제공해야 합니다. 추가 지원이 필요한 경우 문의하세요.

Amazon Connect 결정에서 지원하는 브라우저

Amazon Connect 결정을 사용하기 전에 다음 표를 사용하여 브라우저가 지원되는지 확인합니다.

브라우저	지원되는 버전
Google Chrome	최신 3개 버전
Mozilla Firefox ESR	버전은 Firefox 수명 종료일까지 지원됩니다. 자세한 내용은 Firefox ESR release calendar를 참조하세요.
Mozilla Firefox	최신 3개 버전
Microsoft Edge 및 Edge Chromium	버전 84 이상
Safari	macOS의 Safari 10 이상

Amazon Connect 결정에서 지원하는 언어

Amazon Connect Decisions는 다음 언어를 지원합니다.

- 영어(미국)

AWS 계정 설정

이 섹션을 사용하여 AWS 계정을 생성하고 IAM 사용자를 생성합니다. AWS 계정 생성 모범 사례에 대한 자세한 내용은 모범 사례 AWS 환경 설정을 참조하세요.

AWS 계정 가입

AWS 계정이 없는 경우 다음 단계를 완료하여 계정을 생성합니다.

AWS 계정에 가입하려면

1. https://portal.aws.amazon.com/billing/signup을 엽니다.
2. 온라인 지시 사항을 따르세요.

   등록 절차 중 전화 또는 텍스트 메시지를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

AWS 계정에 가입하면 AWS 계정 루트 사용자가 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스할 수 있는 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

AWS 는 가입 프로세스가 완료된 후 확인 이메일을 보냅니다. 언제든지 https://aws.amazon.com/으로 이동하고 내 계정을 선택하여 현재 계정 활동을 확인하고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

AWS 계정에 가입한 후 AWS 계정 루트 사용자를 보호하고, AWS IAM Identity Center를 활성화하고, 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 생성합니다.

AWS 계정 루트 사용자 보안

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 AWS Management Console에 계정 소유자로 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 사용 설명서의 Signing in as the root user을 참조하세요.
2. 루트 사용자의 다중 인증(MFA)을 활성화합니다.

   지침은 IAM 사용 설명서의 AWS 계정 루트 사용자(콘솔)에 대한 가상 MFA 디바이스 활성화를 참조하세요.

관리자 액세스 권한이 있는 사용자 생성

1. IAM Identity Center를 활성화합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 IAM Identity Center 활성화를 참조하세요. AWS
2. IAM Identity Center에서 사용자에게 관리 액세스 권한을 부여합니다.

   IAM Identity Center 디렉터리를 ID 소스로 사용하는 방법에 대한 자습서는 IAM Identity Center 사용 설명서의 기본 IAM Identity Center 디렉터리를 사용하여 사용자 액세스 구성을 참조하세요. AWS

관리 액세스 권한이 있는 사용자로 로그인

- IAM IDentity Center 사용자로 로그인하려면 IAM Identity Center 사용자를 생성할 때 이메일 주소로 전송된 로그인 URL을 사용합니다.

  IAM Identity Center 사용자를 사용하여 로그인하는 데 도움이 필요하면 로그인 AWS 사용 설명서의 AWS 액세스 포털에 로그인을 참조하세요.

추가 사용자에게 액세스 권한 할당

1. IAM Identity Center에서 최소 권한 적용 모범 사례를 따르는 권한 세트를 생성합니다.

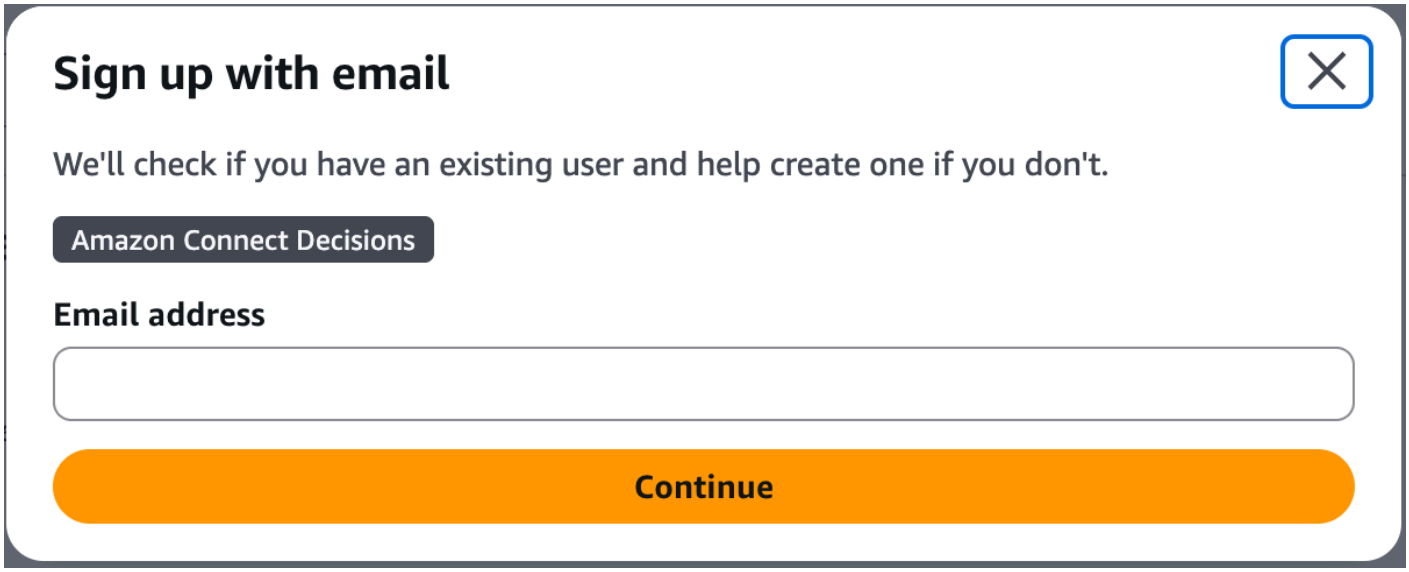
   지침은 AWS IAM Identity Center 사용 설명서의 권한 세트 생성을 참조하세요.
2. 사용자를 그룹에 할당하고, 그룹에 Single Sign-On 액세스 권한을 할당합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 그룹 추가를 참조하세요.

AWS Identity Center 통합 구성

인스턴스를 생성하고 Amazon Connect Decisions 서비스를 사용하려면 기존 IAM Identity Center 사용자 프로필을 연결하거나 새 프로필을 생성해야 합니다.

1. Amazon Connect 결정 콘솔을 엽니다. 기본 AWS 관리 콘솔에서 "Amazon Connect 결정"을 검색할 수도 있습니다.
2. 필요한 경우 콘솔 상단에 있는 리전 선택을 선택하여 AWS 리전을 변경합니다. 드롭다운 목록에서 리전을 선택합니다.
3. Amazon Connect 결정 인스턴스 생성을 선택합니다. 알림이 나타납니다.



4. 이메일 주소를 입력하고 계속을 선택합니다. IdC는 이메일이 기존 사용자와 일치하는지 확인합니다.
5. 다음 중 하나를 수행하세요.
   - IdC가 이메일 주소와 일치하는 경우 - ID 소스 연결을 선택하고 팀을 온보딩합니다.

     > **Note**
     >
     > 조직에 Amazon Connect Decisions에 사용하려는 설정된 IdC 인스턴스가 있는 경우 사용할 수 있습니다.

   - IdC가 기존 사용자와 일치하는 항목을 찾지 못하면 새 사용자 생성 알림이 나타납니다. 다음 단계를 진행합니다.
6. 알림에서 다음을 입력한 후 계속을 선택합니다.
   - 이메일 주소
   - 이름
   - 성

   IdC는 사용자를 자동으로 생성하고 Amazon Connect 결정 관리자로 추가합니다.
7. 다음 중 하나를 수행하세요.
   - 표준 구성을 사용하여 인스턴스를 생성하려면 생성을 선택합니다. 표준 구성 사용을 참조하세요.
   - 사용자 지정 구성을 사용하여 인스턴스를 생성하려면 - 고급 설정에서 편집을 선택합니다. 고급 구성 사용을 참조하세요.

IAM Identity Center와 함께 사용하는 경우 Amazon Connect Decisions는 IAM Identity Center 디렉터리에서 'username' 및 'email' 필드를 검색합니다. 이러한 속성은 Amazon Connect Decisions 인스턴스에 기본적으로 저장되지 않으며 항상 런타임에 검색됩니다. Amazon Connect Decisions는 기본적으로 AWS 소유 KMS 키를 사용하여 유휴 시 이러한 자격 증명 속성을 암호화합니다. Amazon Connect 결정에서는 고객 관리형 KMS 키가 지원되지 않습니다. AWS IAM Identity Center 인스턴스에서 사용자를 삭제하면 Amazon Connect Decisions는 해당 사용자도 인스턴스에서 삭제합니다.

Amazon Connect Decisions 인스턴스 관리

Amazon Connect Decisions에서 인스턴스를 생성하면 공급망 관리 및 분석을 위한 전용 환경이 설정됩니다. 인스턴스를 설정하려면 기본 세부 정보를 구성하고, 설정을 설정하고, 초기 사용자 액세스 권한을 정의합니다.

AWS Management Console 관리자만 인스턴스를 생성할 수 있습니다. Amazon Connect Decisions 인스턴스를 생성하는 AWS Management Console 관리자는 자격 증명 기반 정책 예제에 나열된 모든 권한을 가지고 있어야 합니다. 이 관리자는 IAM 사용자를 Amazon Connect 결정 관리자로 초대하여 Amazon Connect 결정을 관리해야 합니다.

다음 페이지에서는 인스턴스를 생성하고 삭제하는 프로세스를 자세히 설명합니다.

인스턴스 생성

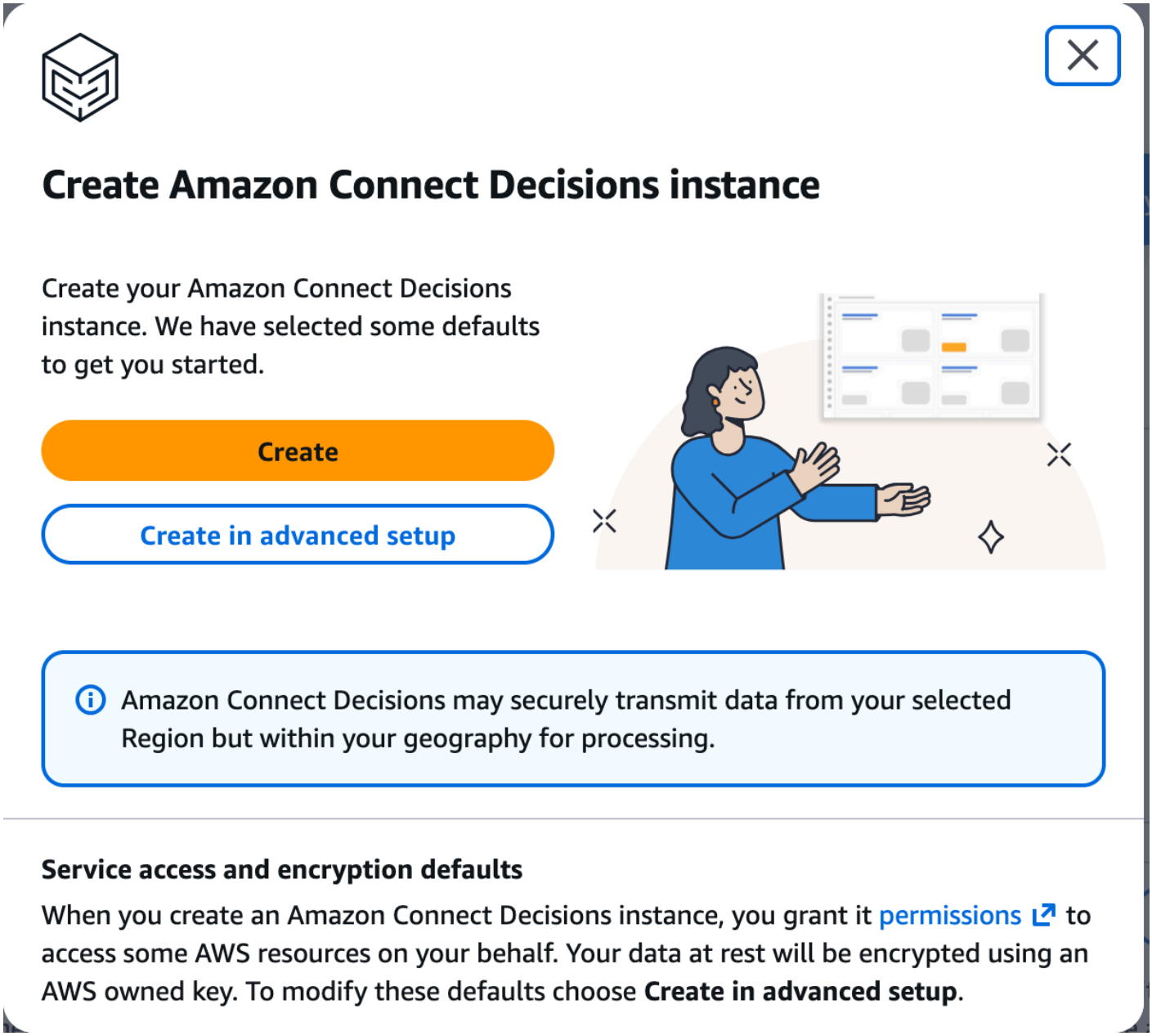
표준 구성 또는 고급 구성이라는 두 가지 방법 중 하나를 사용하여 인스턴스를 생성합니다. 표준 구성은 사전 설정 파라미터를 사용하여 인스턴스를 빠르게 생성하는 자동화된 프로세스를 사용합니다. 고급 구성을 사용하면 자체 파라미터를 설정하여 인스턴스를 사용자 지정할 수 있습니다.

표준 구성 사용

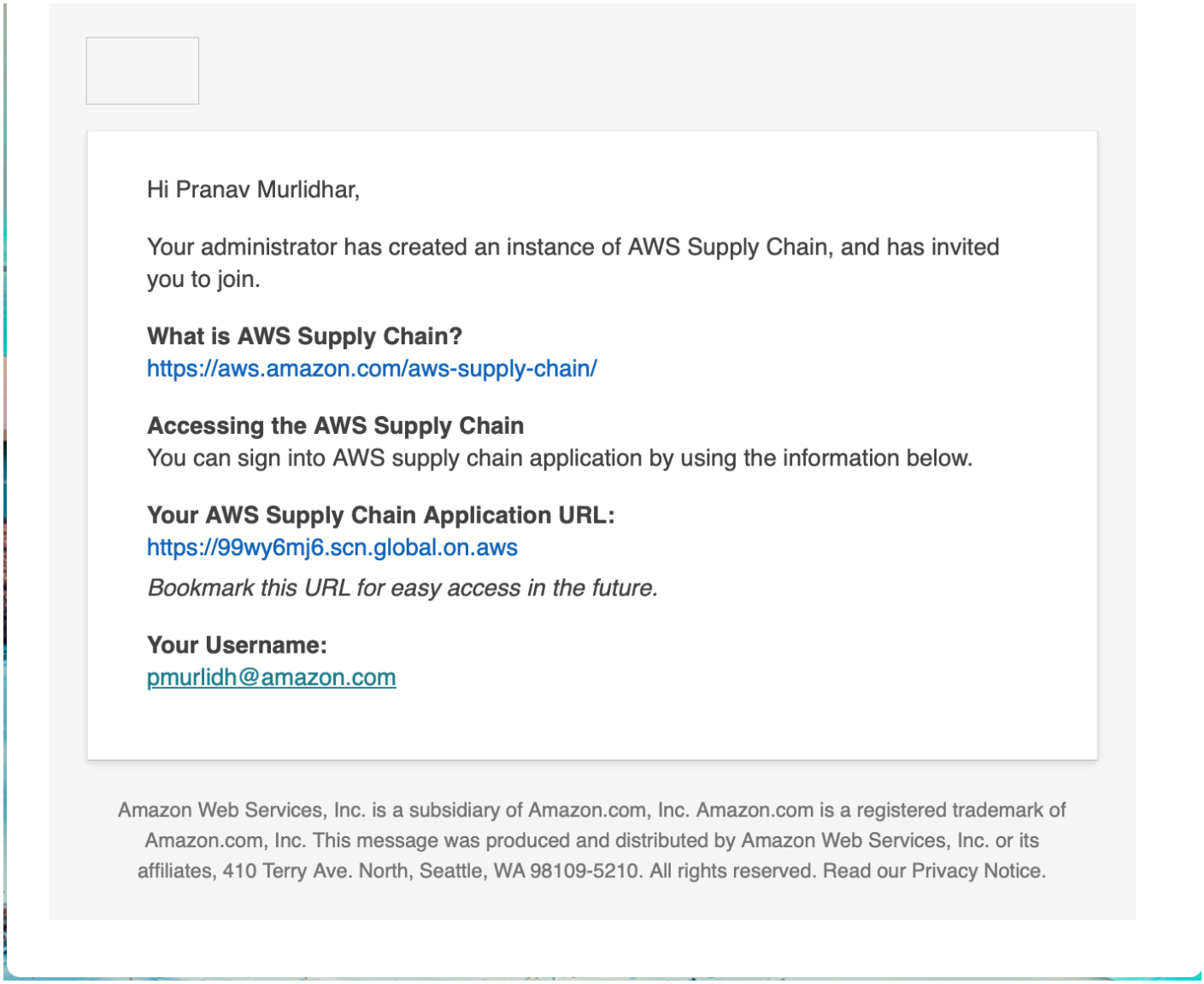
표준 구성은 기본 보안 및 암호화 설정을 사용하여 Amazon Connect Decisions 인스턴스를 생성합니다. 인스턴스는 AWS 지리적 리전에서 작동합니다. 리전에 대한 자세한 내용은 IAM 사용 설명서의 리전 및 엔드포인트와 일반 참조의 리전 엔드포인트를 참조하세요. AWS

사전 설정 파라미터의 표준 구성을 사용하여 Amazon Connect Decisions 인스턴스를 생성하려면 다음 단계를 따르세요.

1. 생성을 선택합니다.



2. 이메일에서 다음을 확인합니다.
   - IdC 팀의 이메일입니다.
   - 자격 증명 관리 팀의 이메일입니다.

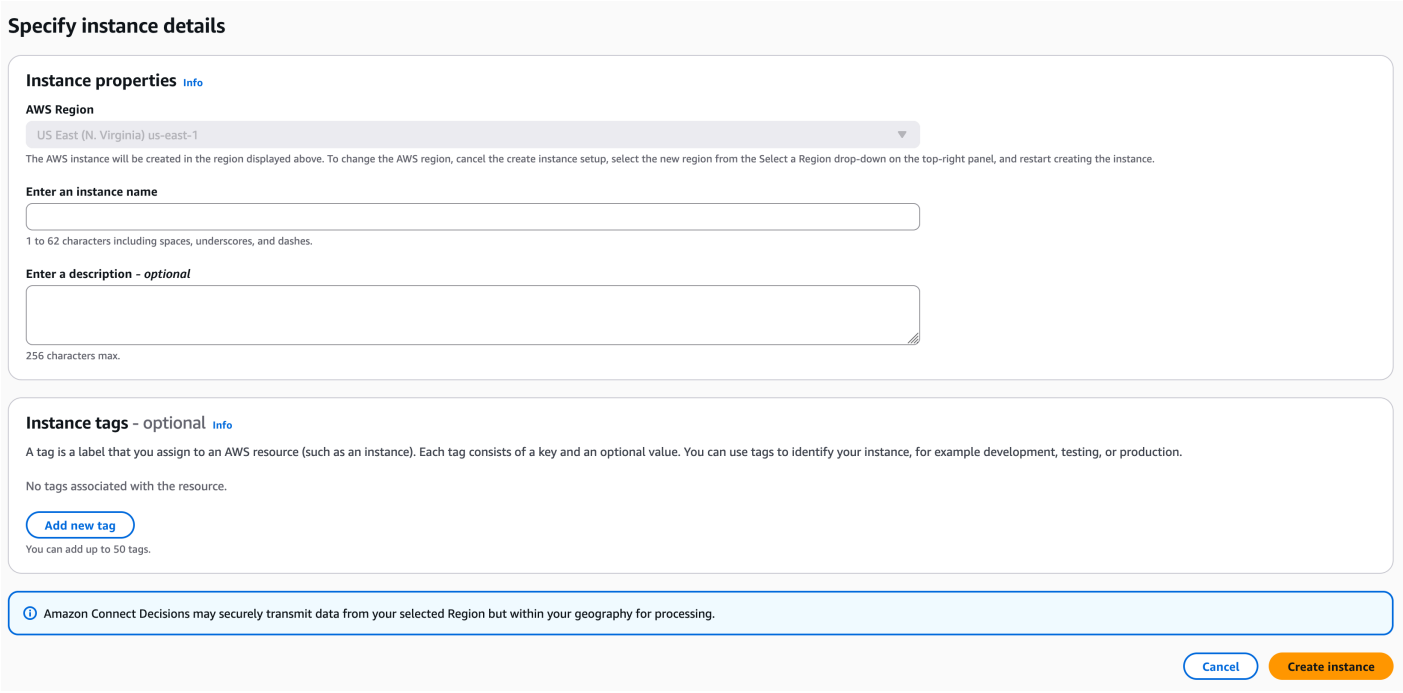


3. 초대 이메일을 받으면 Amazon Connect Decisions에 로그인합니다. Amazon Connect Decisions 웹 애플리케이션에 로그온을 참조하세요.

고급 구성 사용

고급 구성을 사용하면 자체 파라미터를 설정하여 인스턴스를 사용자 지정할 수 있습니다. 사전 설정 파라미터의 고급 구성을 사용하여 Amazon Connect Decisions 인스턴스를 생성하려면 다음 단계를 따르세요.

1. 고급 설정에서 생성을 선택합니다.
2. 인스턴스 속성 페이지가 나타납니다.



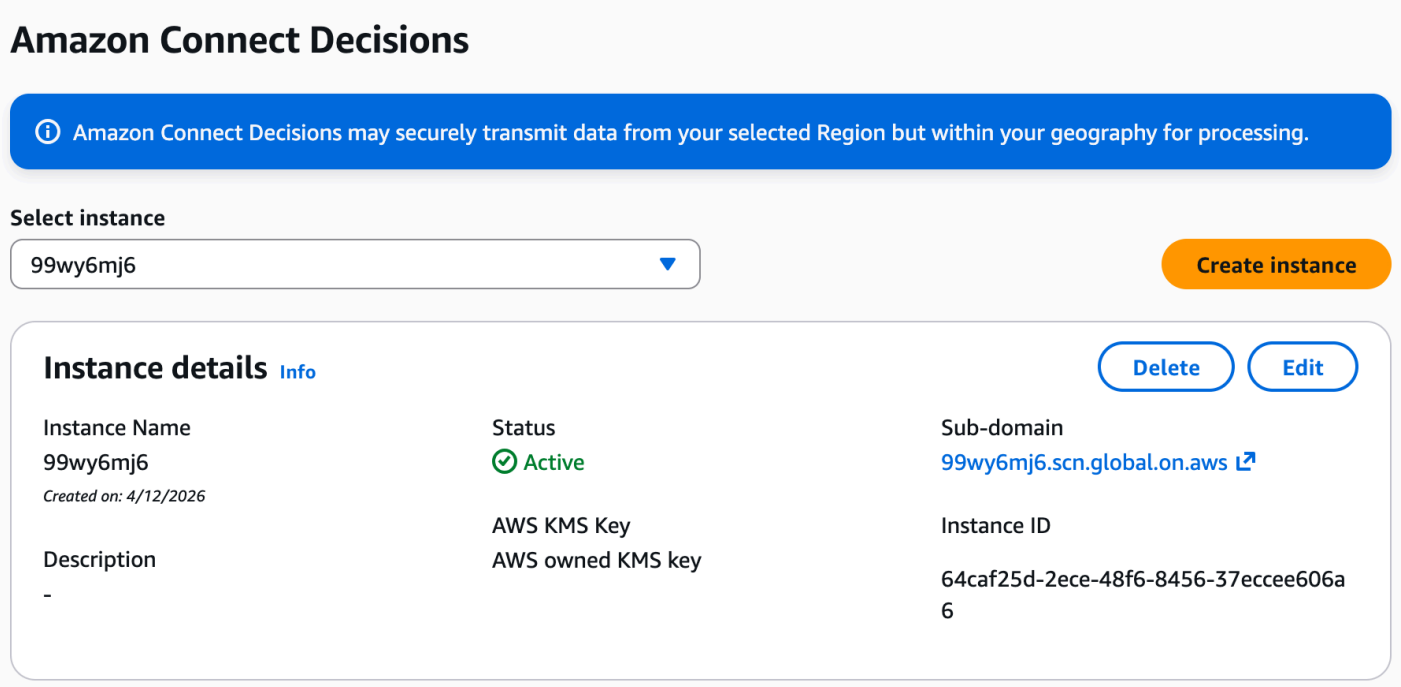
3. 인스턴스 속성 페이지에 다음을 입력합니다.
   - 이름 - 인스턴스 이름을 입력합니다.
   - 설명 - Amazon Connect Decisions 인스턴스(예: 프로덕션 인스턴스, 테스트 인스턴스 등)에 대한 설명을 입력합니다.
   - 인스턴스 태그 - 식별에 사용할 수 있는 태그를 인스턴스에 추가할 수 있습니다. 예를 들어 태그를 추가하여 생성 중인 인스턴스 유형(예: 프로덕션, 테스트, UAT 등)을 정의할 수 있습니다.
4. 인스턴스 생성을 선택합니다.

인스턴스 삭제

인스턴스를 삭제하려면 다음 단계를 따릅니다.

> **Note**
>
> 인스턴스를 삭제할 때 Amazon S3 버킷의 정보는 자동으로 삭제되지 않습니다.

1. https://console.aws.amazon.com/scn/home Amazon Connect Decisions 콘솔을 엽니다.
2. Amazon Connect Decisions 콘솔 대시보드의 드롭다운에서 삭제할 인스턴스를 선택합니다.



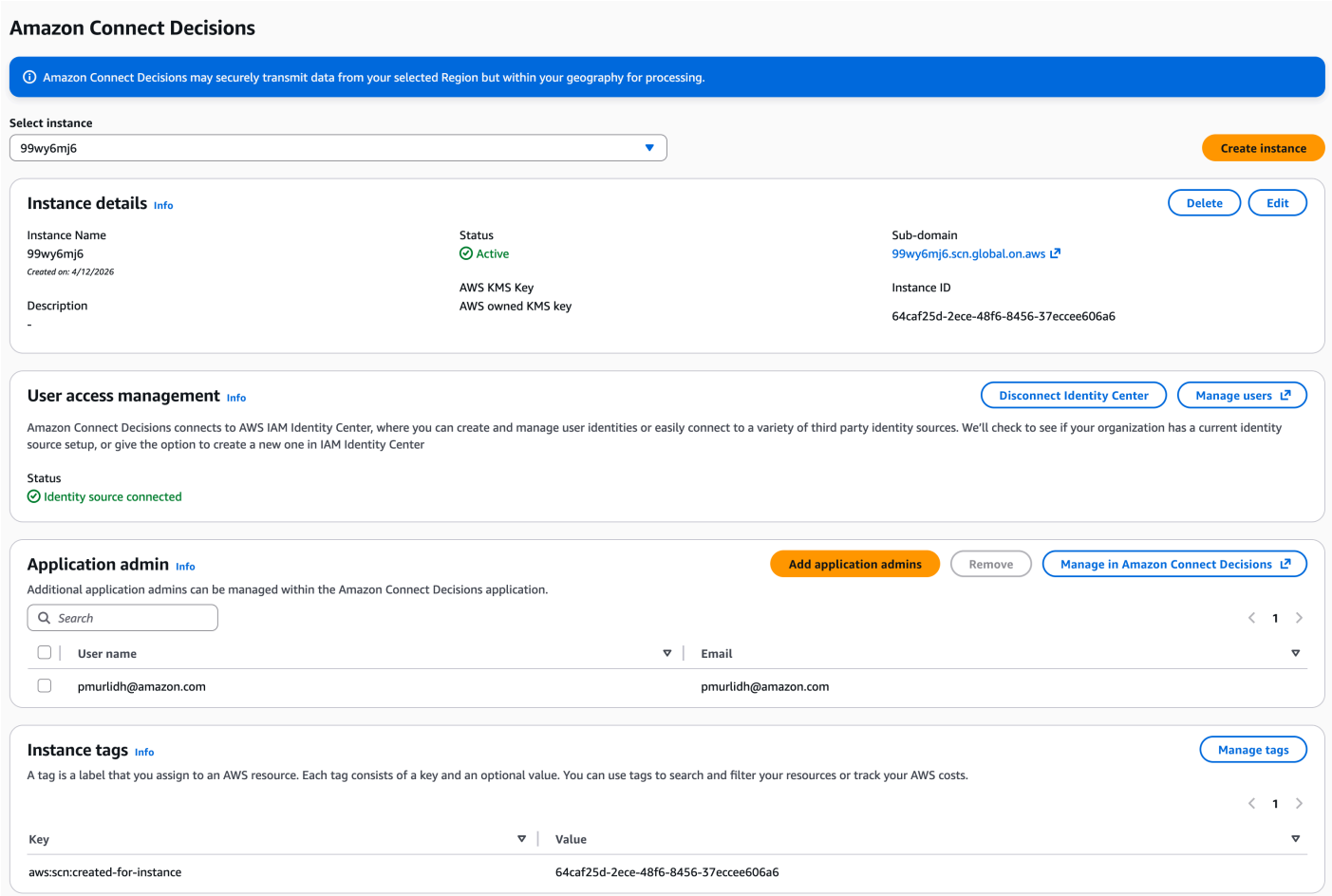
3. 삭제를 선택합니다.
4. Amazon Connect 결정 인스턴스 삭제 페이지의 확인에 `delete`를 입력하여 인스턴스를 삭제할지 확인합니다.
5. 삭제를 선택합니다. 인스턴스 삭제가 시작되고 인스턴스가 삭제되면 확인 메시지가 표시됩니다.

애플리케이션 관리자 선택

AWS 콘솔 관리자는 Amazon Connect Decisions 애플리케이션 관리자를 선택하여 Amazon Connect Decisions 웹 애플리케이션 액세스를 관리합니다. Amazon Connect Decisions 애플리케이션 관리자는 Amazon Connect Decisions 웹 애플리케이션에 사용자 권한 역할을 추가하거나 제거할 수 있습니다.

인스턴스가 생성되고 자격 증명 소스가 연결되면 다음 단계에 따라 Amazon Connect Decisions 애플리케이션 관리자를 선택합니다.

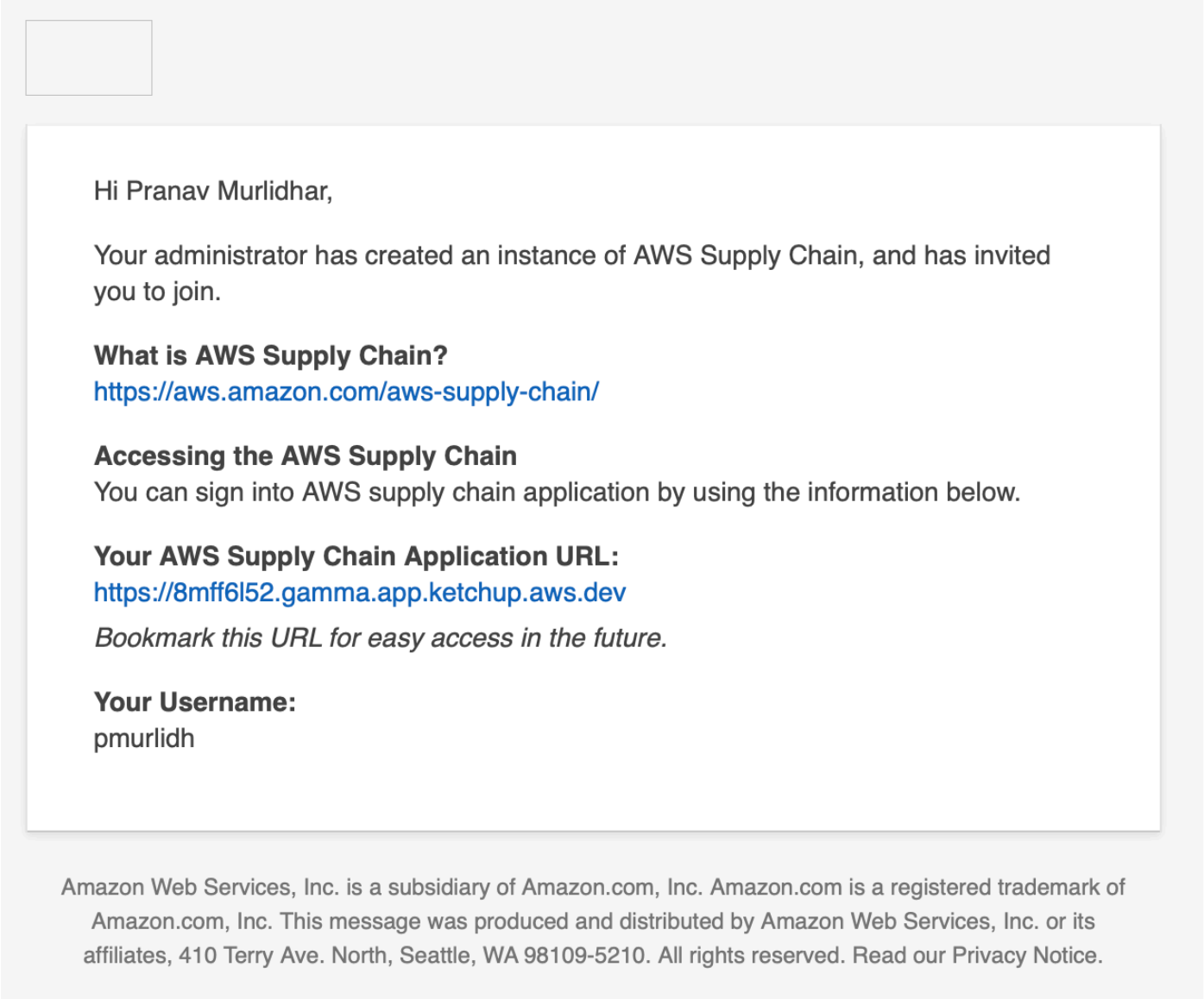
1. Amazon Connect Decisions 콘솔 대시보드를 엽니다.
2. 애플리케이션 관리자 선택으로 이동하여 Amazon Connect Decisions 애플리케이션 관리자가 될 사용자를 선택합니다. 검색 결과에는 검색 기준과 일치하는 사용자만 표시됩니다.



3. (선택 사항) IAM Identity Center로 이동을 선택하여 사용자를 더 추가합니다. 사용자 추가에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 ID 소스 관리를 참조하고 사용자 권한 역할에 대한 자세한 내용은 사용자 권한 역할을 참조하세요.

> **Note**
>
> Amazon Connect 결정 콘솔에서는 한 번에 한 명의 사용자만 추가할 수 있습니다. Amazon Connect 결정에서는 그룹을 애플리케이션 관리자로 추가할 수 없습니다.

4. 초대 전송을 선택합니다. 웹 애플리케이션 관리자에게 이메일이 전송됩니다. 웹 애플리케이션 관리자가 초대 이메일을 받으면 애플리케이션 URL을 선택하고 Amazon Connect 결정에 로그인할 수 있습니다.



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.

Amazon Connect 결정 웹 앱에서 애플리케이션 관리자 아래에 사용자가 나열됩니다.

인스턴스 액세스

콘솔을 사용하면 서비스 리소스와 구성을 가장 쉽게 관리할 수 있습니다. 콘솔은 리소스를 보고, 생성하고, 수정하고, 모니터링할 수 있는 직관적인 웹 기반 인터페이스를 제공합니다.

Amazon Connect 결정 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한은 AWS 계정의 Amazon Connect Decisions 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다. 최소 필수 권한보다 더 제한적인 ID 기반 정책을 생성하는 경우, 콘솔이 해당 정책에 연결된 엔티티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

또는 AWS API만 호출하는 사용자에게는 최소 콘솔 권한을 허용할 필요가 없습니다. 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

Amazon Connect 결정 관리자는 Amazon Connect 결정 웹 애플리케이션에 대한 이메일 초대를 받았어야 합니다.

1. 이메일 또는 Amazon Connect Decisions 콘솔 대시보드의 하위 도메인에서 웹 URL을 선택할 수 있습니다.
2. Amazon Connect Decisions 웹 애플리케이션 로그인 페이지가 나타납니다.
3. AWS IAM Identity Center 사용자 자격 증명을 입력하고 로그인을 선택합니다.
4. 추가한 각 사용자는 Amazon Connect 결정으로 연결되는 링크가 포함된 이메일 메시지를 수신하거나 링크 복사를 선택하고 사용자에게 링크를 보낼 수 있습니다.

성공적으로 로그인하면 개인화된 홈 페이지로 이동합니다. 홈 페이지를 더 잘 이해하려면 사용 설명서의 홈 페이지 이해를 참조하세요.

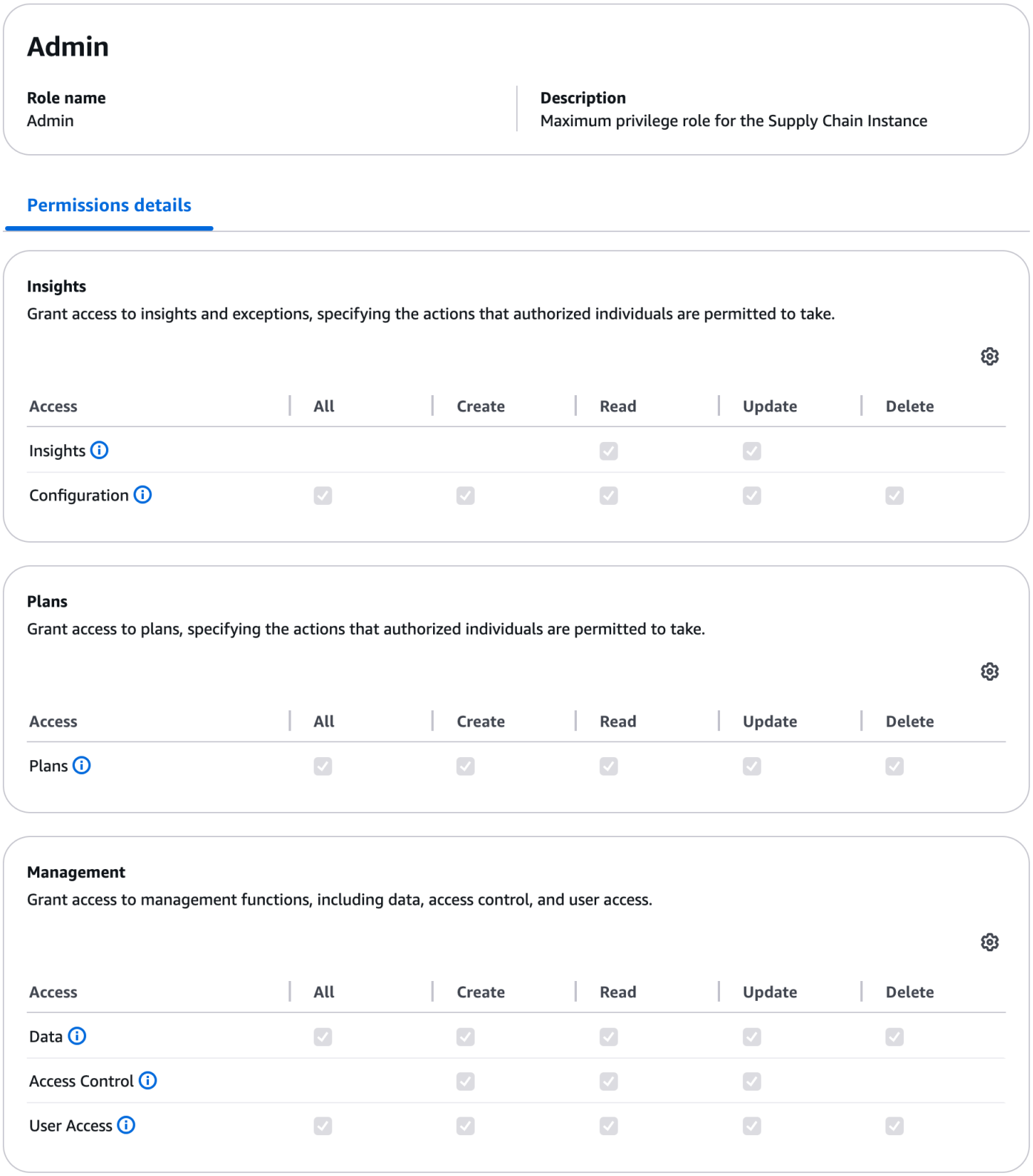
액세스 통제

Amazon Connect Decisions는 인스턴스 내에서 누가 어떤 데이터에 액세스하고 어떤 작업을 수행할 수 있는지 정확하게 제어할 수 있는 엔터프라이즈급 액세스 관리를 제공합니다. 이렇게 하면 사용자가 조직에 필요한 보안 및 규정 준수 표준을 유지하면서 자신의 책임과 관련된 정보만 볼 수 있습니다.

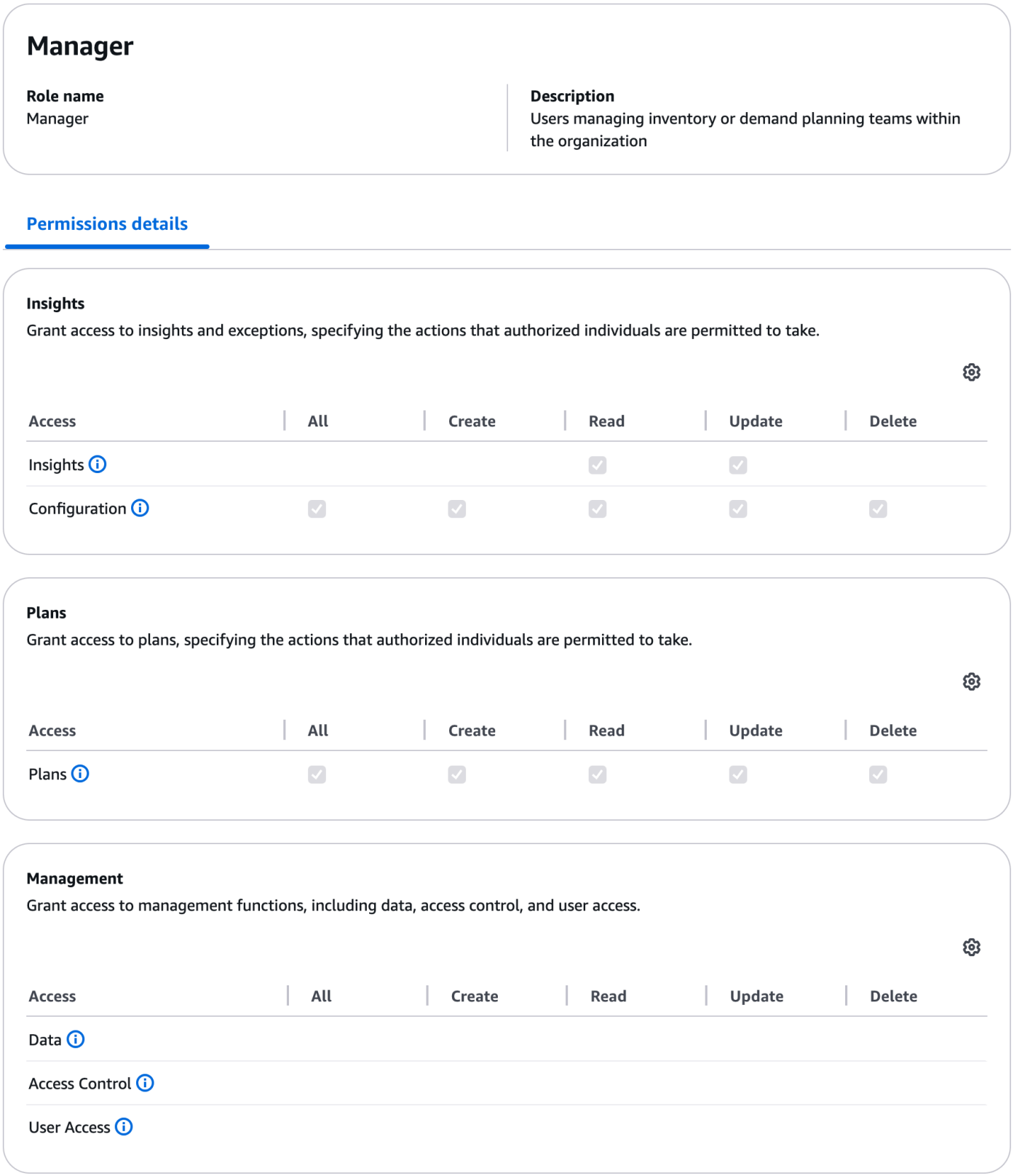
역할 및 권한 개요

Amazon Connect 결정 관리자는 기본 사용자 권한 역할을 사용하거나 사용자 지정 권한 역할을 생성할 수 있습니다. Amazon Connect Decisions에는 다음과 같은 기본 사용자 권한 역할이 있습니다.

- Administrator - 모든 데이터와 사용자 권한을 생성, 확인, 관리할 수 있는 액세스 권한입니다.



- 관리자 - 다음을 생성, 확인 및 관리할 수 있는 액세스 권한입니다.



- 플래너 - 다음을 생성, 확인 및 관리할 수 있는 액세스 권한입니다.

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**
>
> Amazon Connect 결정 관리자는 사용자를 추가하기 전에 다음 사항에 유의하세요.
>
> - 각 기본 사용자 권한 역할은 권한 집합으로 정의됩니다. 기본 사용자 권한 역할에 사용자를 추가하거나 사용자 정의 권한 역할을 생성할 수 있습니다.
> - 한 사용자에게 하나의 사용자 권한 역할만 할당할 수 있습니다.
> - 기본 사용자 권한 역할은 편집하거나 삭제할 수 없습니다.
> - 생성한 사용자 지정 권한 역할을 편집하면 해당 사용자 지정 권한 역할에 속한 모든 사용자의 권한이 업데이트됩니다.
> - 생성한 사용자 지정 권한 역할을 삭제하면 사용자 지정 권한 역할의 모든 사용자가 Amazon Connect Decisions에 액세스할 수 없게 됩니다.
> - Amazon Connect 결정에서는 그룹 추가가 지원되지 않습니다.

사용자 권한 역할 관리

사용자 추가

Amazon Connect 결정 관리자는 사용자를 추가하여 Amazon Connect 결정 웹 애플리케이션에 액세스할 수 있습니다. 먼저 사용자를 IAM Identity Center(IdC)에 추가한 다음 Amazon Connect Decisions에 추가할 수 있습니다. IdC에 사용자를 추가하는 방법에 대한 자세한 내용은 사용자 액세스 할당을 참조하세요.

사용자가 IdC에 추가되면 다음 단계에 따라 사용자를 추가합니다.

1. 설정 왼쪽 사이드 드로어를 선택합니다.
2. 사용자를 선택합니다. 사용자 할당 선택
3. 를 검색하여 사용자를 식별합니다. 표시 이름, 이메일, 이름, 성, 사용자 이름을 사용하여 검색할 수 있습니다.
4. 추가할 사용자를 선택합니다.
5. 역할을 할당합니다. Amazon Connect 결정의 사용자 역할에 대해 자세히 알아보려면 역할 및 권한 개요를 참조하세요.
6. 할당을 선택합니다. 선택 항목이 정확한지 확인합니다.

사용자 권한 업데이트

현재 Amazon Connect Decisions 사용자의 사용자 권한 역할을 업데이트하려면 다음 단계를 따르세요.

1. 설정 왼쪽 사이드 드로어를 선택합니다.
2. 사용자를 선택합니다. 사용자 할당 선택
3. 사용자 목록에서 사용자를 선택하여 사용자 세부 정보 페이지를 엽니다.
4. 역할 드롭다운을 사용하여 사용자의 역할 권한을 업데이트합니다.
5. 역할 변경 버튼을 클릭하여 역할을 변경할지 확인합니다.

사용자 삭제

Amazon Connect 결정 관리자는 Amazon Connect 결정 웹 애플리케이션에서 사용자를 삭제할 수 있습니다. 다음 단계에 따라 사용자를 삭제합니다.

1. 설정 왼쪽 사이드 드로어를 선택합니다.
2. 사용자를 선택합니다. 사용자 할당 선택
3. 사용자 목록에서 사용자를 선택하여 사용자 세부 정보 페이지를 엽니다.
4. 삭제를 선택합니다.
5. 삭제 버튼을 클릭하여 사용자를 삭제할지 확인합니다.

속성 수준 액세스 설정

속성 기반 액세스 제어(ABAC)는 비즈니스 컨텍스트에 따라 액세스를 제한하여 정밀도 계층을 추가합니다. 제품 및 사이트 속성을 사용하면 플래너가 관리하는 특정 제품 및 위치에 대한 세부 정보만 보고 관리자는 팀의 책임 영역에 대한 가시성을 유지할 수 있습니다.

'관리자' 역할을 가진 모든 사용자는 다른 사용자를 위해 제품 및 사이트별로 액세스를 구성할 수 있습니다.

1. 왼쪽 탐색 모음에서 사용자 페이지로 이동합니다.
2. 해당 인스턴스의 사용자 목록에서 구성이 필요한 사용자를 선택합니다.
3. 기본적으로 데이터 액세스 섹션에서 사용자는 "모든 제품 및 사이트에 대한 전체 액세스 권한 부여"를 활성화할 수 있습니다. 이 토글이 켜져 있으면 모든 제품 및 사이트(이 출시 전 작동 방식)에 액세스할 수 있습니다.

4. "모든 제품 및 사이트에 대한 전체 액세스 권한 부여"를 끄면 제품 및 사이트 구성 섹션이 표시됩니다. 처음 액세스할 때 제품 또는 사이트가 할당되지 않습니다.
5. 구성해야 하는 항목에 따라 제품 또는 사이트에 대한 추가/제거 버튼을 클릭합니다. 검색을 사용하여 해당 사용자에게 필요한 항목을 찾고 선택합니다.
6. 여러 사용자가 동일한 제품 또는 사이트를 할당받을 수 있습니다. 사용자는 최대 1,000개의 제품 사이트 조합을 가질 수 있습니다.
7. 이전에 구성된 제품 또는 사이트는 동일한 인터페이스를 사용하여 제거할 수 있습니다.
8. 마법사의 마지막 페이지에서 추가 및 제거의 전체 목록을 검토하고 확인하여 액세스 구성을 완료합니다.

제품 및 사이트 액세스가 구성되면 다음 할당에 따라 해당 사용자의 액세스가 제한됩니다.

- 모든 사용자는 액세스 제어에 포함된 제품 또는 사이트에 대해 생성되었는지 여부에 관계없이 모든 예외 또는 권장 사항 페이지를 볼 수 있습니다.
- 변경 작업(예: 예외 무시 또는 진행 중에서 완료로 상태 변경)을 수행하려면 액세스 제어에 적절한 제품 또는 사이트가 구성되어 있어야 합니다.
- 액세스 제어가 구성된 사용자는 사용자 할당 및 액세스 보기 토글을 사용할 수도 있습니다.

사용자 할당

사용자 할당은 여러 사용자 간에 인사이트의 균형을 보다 쉽게 맞출 수 있는 기능입니다. 고객은 사용자 할당을 사용하여 사용자에게 특정 인사이트를 할당하여 이러한 작업이 실제로 공유되는 방식을 더 잘 반영할 수 있습니다. 작동 방식은 다음과 같습니다.

- 예외가 생성될 때마다 시스템은 액세스 제어를 위해 구성된 동일한 제품 또는 사이트가 있는 모든 사용자에 대해 예외가 생성되는 제품 및 사이트를 확인합니다.
- 시스템에서 일치하는 사용자를 찾으면 해당 예외에 대한 할당 대상 필드가 사용자 이름으로 업데이트됩니다. 둘 이상의 사용자에게 예외와 일치하는 제품 또는 사이트가 있는 경우 둘 중 하나에 무작위로 할당됩니다.
- 각 예외에는 한 명의 사용자만 할당할 수 있지만 필요한 경우 다른 사용자에게 예외를 다시 할당할 수 있습니다. 제품 또는 사이트 액세스 권한이 있는 사용자에게만 재할당할 수 있습니다.
- 인사이트에 대한 자동 할당은 예외가 처음 생성될 때 발생합니다. 이전에 생성된 인사이트는 자동으로 재할당되지 않습니다. 또한 사용자가 삭제되거나 액세스 제어가 업데이트된 경우 사용자 할당이 자동으로 업데이트되지 않습니다.

- 인사이트 목록 페이지에서 사용자는 할당된 대상 차원을 기준으로 필터링하여 자신에게 할당된 모든 인사이트를 쉽게 식별할 수 있습니다. 또한이 동일한 필터를 사용하여 할당되지 않은 인사이트를 볼 수 있습니다. 사용자 할당은 현재 인사이트에만 사용할 수 있습니다.

데이터 온보딩

데이터 연결

사전 조건

데이터 온보딩을 시작하기 전에 다음을 갖추어야 합니다.

- Amazon Connect 결정 인스턴스
  - 인스턴스가 연결된 S3 버킷으로 이미 생성되어 있어야 합니다.
- 준비된 데이터
  - Amazon Customer Success와 협력하여 Amazon Connect Decisions를 어떻게 사용할 계획인지에 따라 필요한 데이터를 결정합니다. 기본 데이터 요구 사항은 다음과 같습니다.
    - 판매/주문 기록: 12개월 이상의 트랜잭션 레코드
    - 제품 세부 정보: 사양이 포함된 전체 제품 카탈로그
    - 사이트/위치 정보: 창고, 배포 센터, 소매 위치
    - 현재 인벤토리 보유: 각 위치의 보유 인벤토리
  - UTF-8 인코딩을 사용하는 CSV 형식의 모든 소스 데이터

최초 로그인: 온보딩 설문

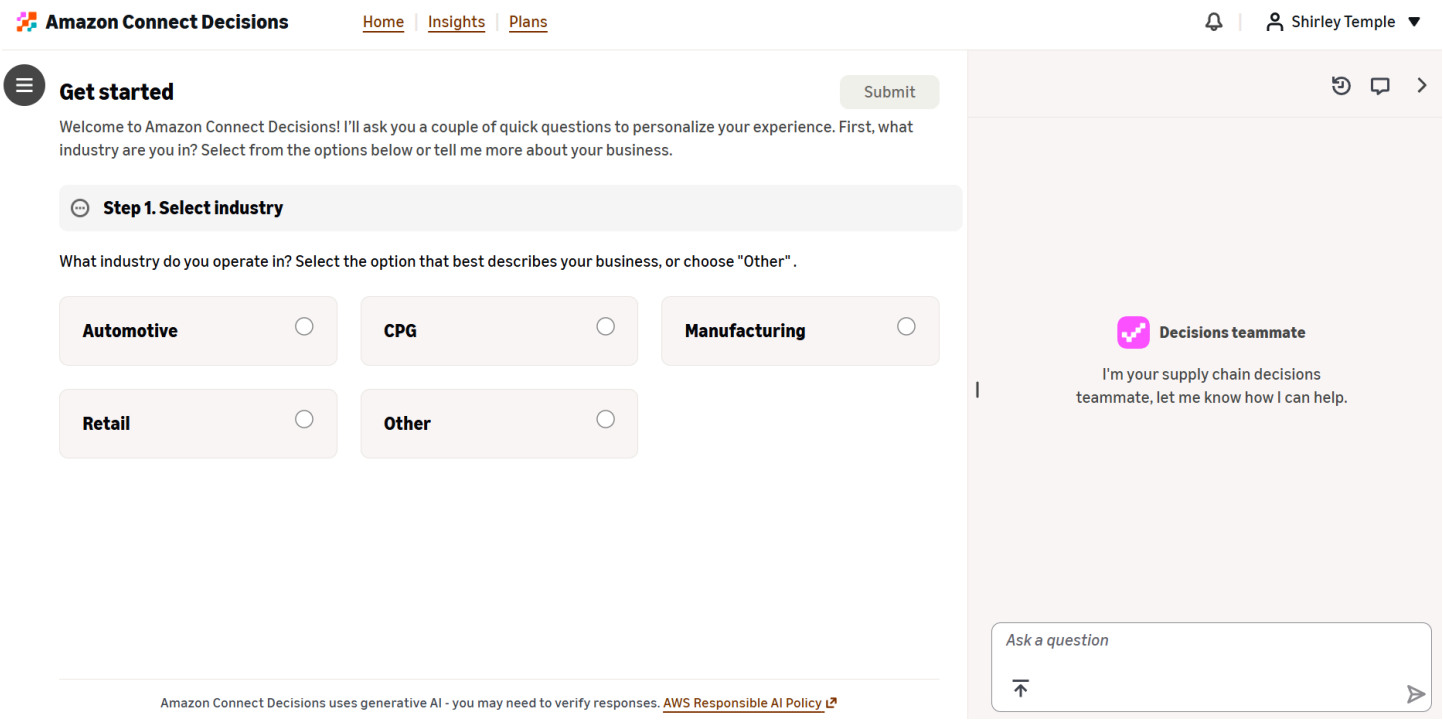
Amazon Connect Decisions에 처음 로그인하면 시스템에서 안내 온보딩 설문이 표시됩니다. 이 개인화 마법사는 의사 결정 팀원이 비즈니스와 가장 관련성이 높은 기능을 컨텍스트화하는 데 도움이 됩니다. 이 설문은 업계, 주요 비즈니스 과제 및 선호하는 계획 접근 방식에 대한 정보를 수집합니다. 응답은 선택에 따라 온보딩 단계를 최적화하는 데 도움이 되므로 시스템이 후속 설정 워크플로를 간소화하고 비즈니스에 가장 관련성이 높은 구성 경로를 표시할 수 있습니다. 전체 애플리케이션에 액세스하기 전에 모든 단계를 완료해야 합니다. Decisions Teammate는 오른쪽 사이드바를 통해 온보딩 프로세스 전반에 걸쳐 실시간으로 질문에 답변할 수 있습니다.

> **Note**
>
> 이는 처음 로그인할 때만 일회성 선택입니다. 응답은 후속 온보딩 단계를 최적화하고 에이전트가 비즈니스 환경을 이해하는 데 도움이 되는 추가 컨텍스트를 제공합니다. 모든 기능은 선택에 관계없이 완전히 액세스할 수 있습니다.

1단계: 산업 선택

표시되는 내용: 비즈니스를 가장 잘 설명하는 산업을 선택하라는 환영 메시지와 라디오 버튼 세트입니다.

1. 비즈니스를 가장 잘 나타내는 라디오 버튼을 선택합니다.
2. 사전 정의된 옵션이 적용되지 않는 경우 기타를 선택합니다.



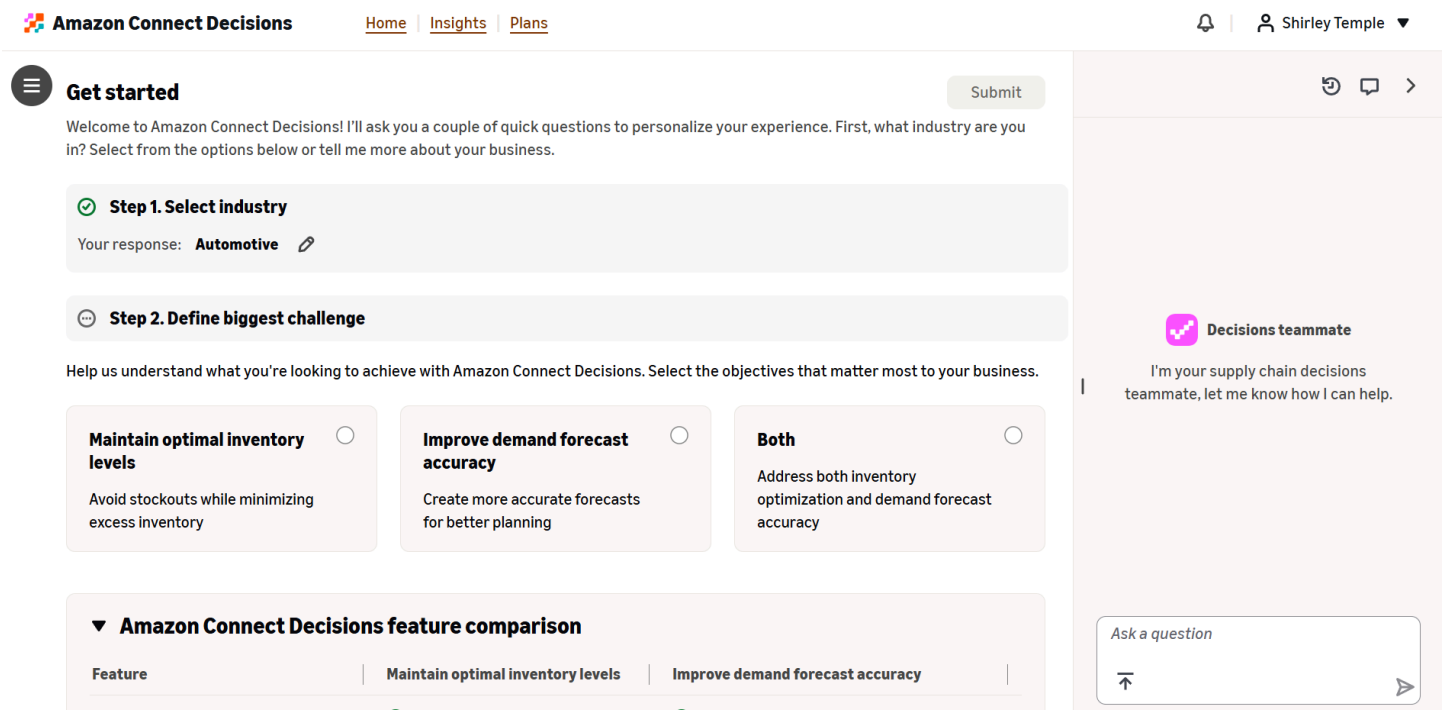
2단계: 가장 큰 문제 정의

표시되는 내용: 1단계 응답이 편집 옵션과 함께 표시됩니다. 그 아래에는 세 가지 옵션에서 주요 비즈니스 문제를 식별하라는 메시지가 표시됩니다. 각 선택과 연결된 기능을 이해하는 데 도움이 되는 기능 비교 표가 표시됩니다.

1. 옵션을 검토합니다. 사용 가능한 옵션과 그 의미는 다음 표를 참조하세요.
2. 가장 시급한 문제를 나타내는 라디오 버튼을 선택합니다.
3. 선택 사항으로 옵션 아래의 기능 비교 표를 검토하여 각 선택 항목에 포함된 내용을 이해합니다.

비즈니스 챌린지 옵션

옵션	설명	주요 기능 활성화
최적의 인벤토리 수준 유지	기본 챌린지가 초과 인벤토리를 최소화하면서 재고 부족을 피하는 경우이 옵션을 선택합니다.	인벤토리 최적화, 재고 부족 방지, 과도한 인벤토리 감소, 공급 계획, 공급업체 리드 타임 추적
수요 예측 정확도 개선	더 나은 계획 결정을 위해 더 정확한 예측을 생성하는 것이 주요 과제인 경우이 옵션을 선택합니다.	기준 예측, 합의 계획, 예측 정확도 추적
둘 다	인벤토리 최적화와 수요 예측 정확도를 동시에 해결해야 하는 경우이 옵션을 선택합니다.	모든 공급별 및 수요별 기능이 활성화됨



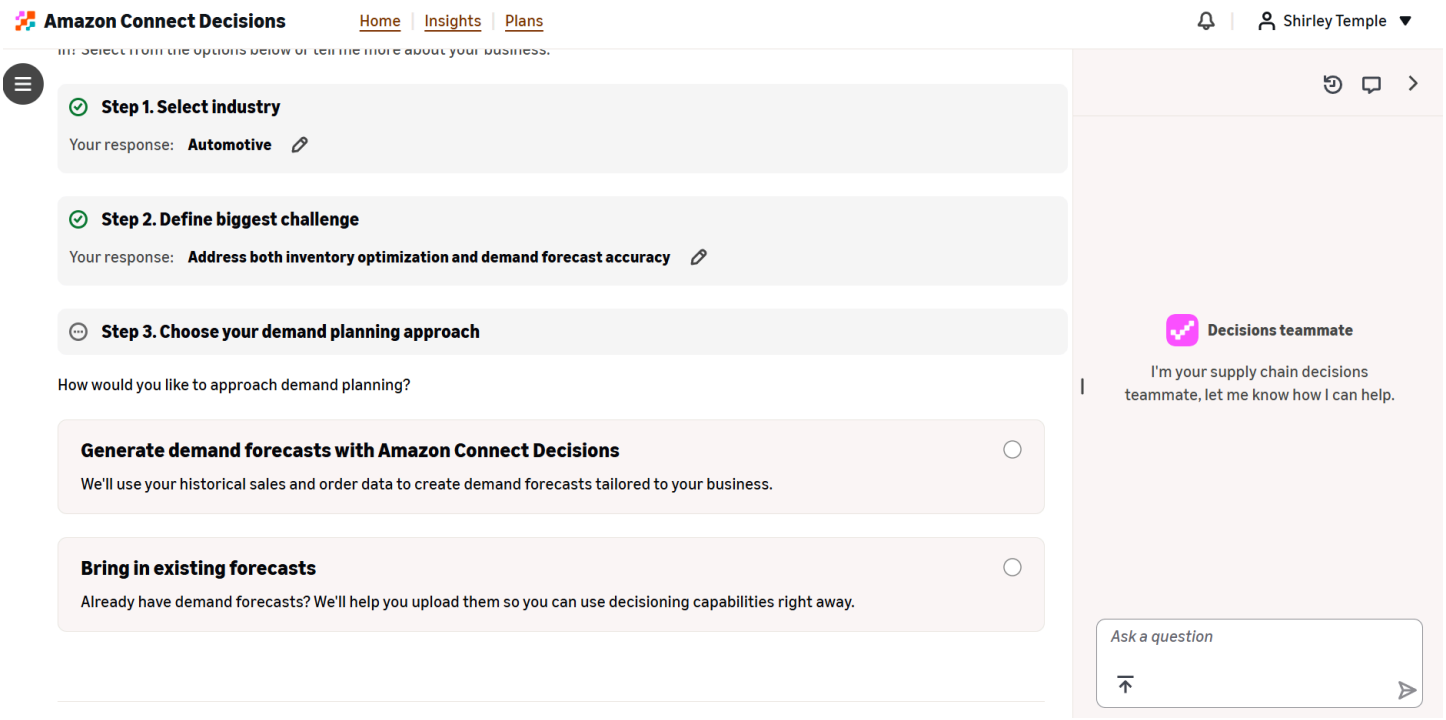
3단계: 인벤토리 계획 접근 방식 선택

표시되는 내용: 1단계와 2단계가 완료됨(녹색 확인 표시)으로 표시되고 응답이 표시되고 편집할 수 있습니다. 3단계에서는 두 가지 옵션이 강조 표시된 상태에서 인벤토리 계획에 접근하는 방법을 묻습니다.

1. 두 가지 인벤토리 계획 옵션을 검토합니다. 사용 가능한 옵션과 그 의미는 다음 표를 참조하세요.
2. 현재 상태와 일치하는 접근 방식의 라디오 버튼을 선택합니다.

인벤토리 계획 접근 방식 옵션

옵션	설명	최적의 용도
Amazon Connect Decisions를 사용하여 인벤토리 계획 생성	시스템은 과거 판매 및 인벤토리 데이터를 사용하여 비즈니스에 맞는 계획을 생성합니다.	기존 계획 솔루션이 없거나 기록 데이터에서 AI 생성 계획을 활용하려는 조직입니다.
기존 인벤토리 예측 또는 계획 가져오기	결정 기능을 즉시 사용할 수 있도록 기존 인벤토리 계획 또는 프로젝션을 업로드합니다. 시스템은 데이터를 업로드하고 매핑하는 데 도움이 됩니다.	이미 계획 프로세스를 수립했으며 계획 소스를 변경하지 않고 모니터링, 인사이트 생성 및 권장 기능을 활용하려는 조직입니다.



4단계: 수요 계획 접근 방식 선택

표시되는 내용: 1~3단계가 완료된 것으로 표시됩니다. 4단계에서는 수요 계획에 접근하는 방법을 묻습니다.

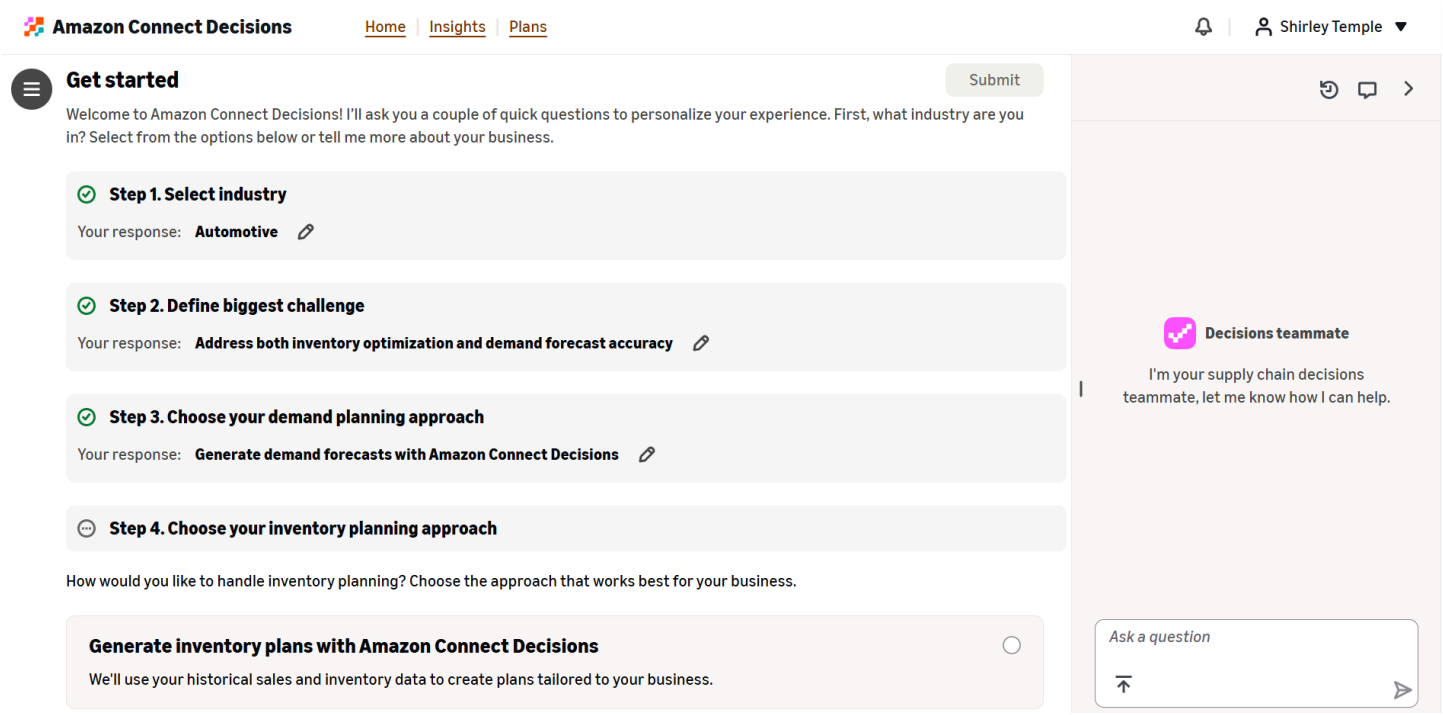
1. 두 가지 수요 계획 옵션을 검토합니다. 사용 가능한 옵션과 그 의미는 다음 표를 참조하세요.
2. 현재 상태와 일치하는 접근 방식의 라디오 버튼을 선택합니다.
3. 제출을 클릭하여 온보딩 설문지를 완료합니다.

참고:이 온보딩 설문지는 선택 사항에 따라 온보딩 단계를 최적화하는 데 도움이 되는 일회성 컨텍스트 입력입니다. 에이전트 동작을 변경하거나 기능에 대한 액세스를 제한하지 않습니다. Amazon Connect Decisions의 모든 기능은 계속 사용할 수 있습니다.

수요 계획 접근 방식 옵션

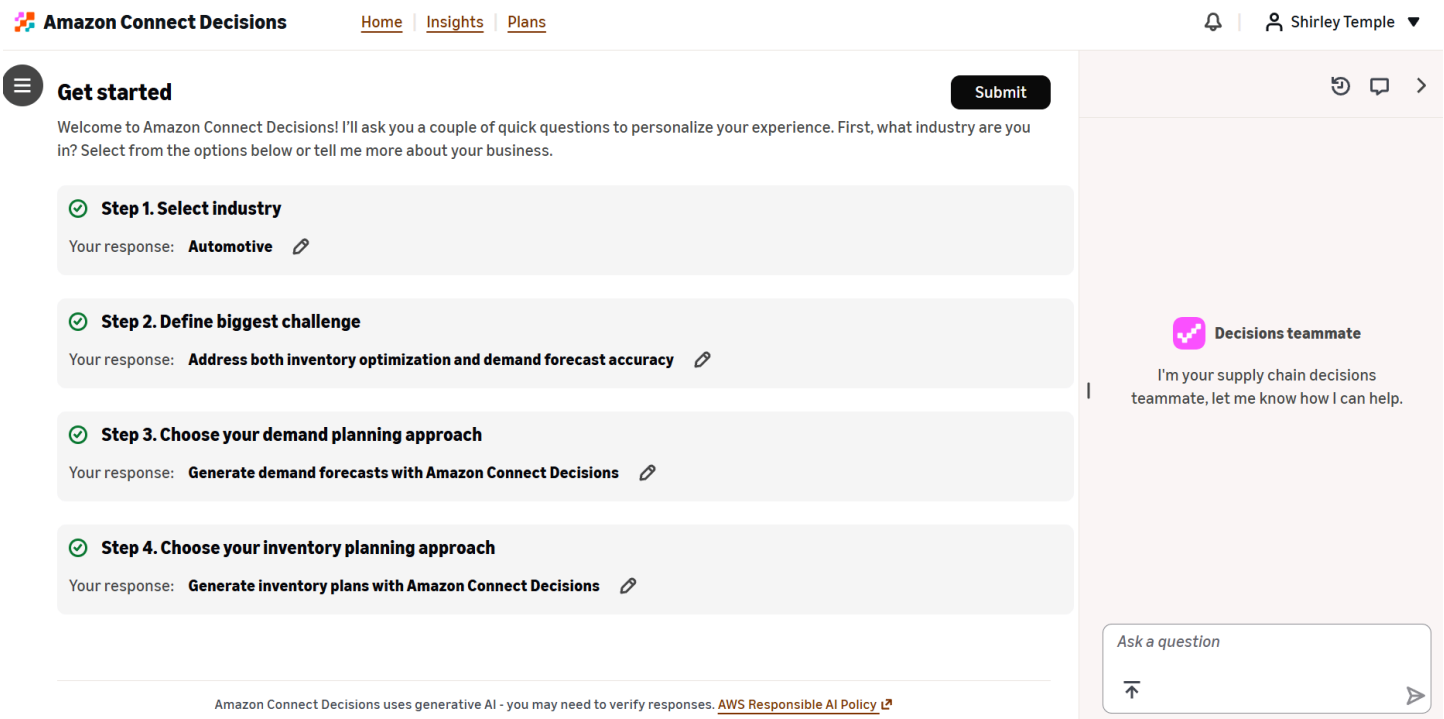
옵션	설명	최적의 용도
Amazon Connect 결정으로 수요 예측 생성	시스템은 과거 판매 및 주문 데이터를 사용하여 비즈니스에 맞는 수요 예측을 생성합니다. Amazon Connect Decisions는	기존 예측 솔루션이 없거나 현재 접근 방식을 AI 생성 예측으로 바꾸려는 조직.

옵션	설명	최적의 용도
	18개 이상의 예측 도구를 오케스트레이션하여 정확한 기준 예측을 생성합니다.	
기존 예측 가져오기	결정 기능을 즉시 사용할 수 있도록 기존 수요 예측을 업로드합니다. 시스템은 예측 데이터를 매핑하고 가져오는 데 도움이 됩니다.	이미 예측 프로세스를 수립했으며 예측 소스를 변경하지 않고 모니터링, 인사이트 생성 및 권장 기능을 활용하려는 조직입니다.

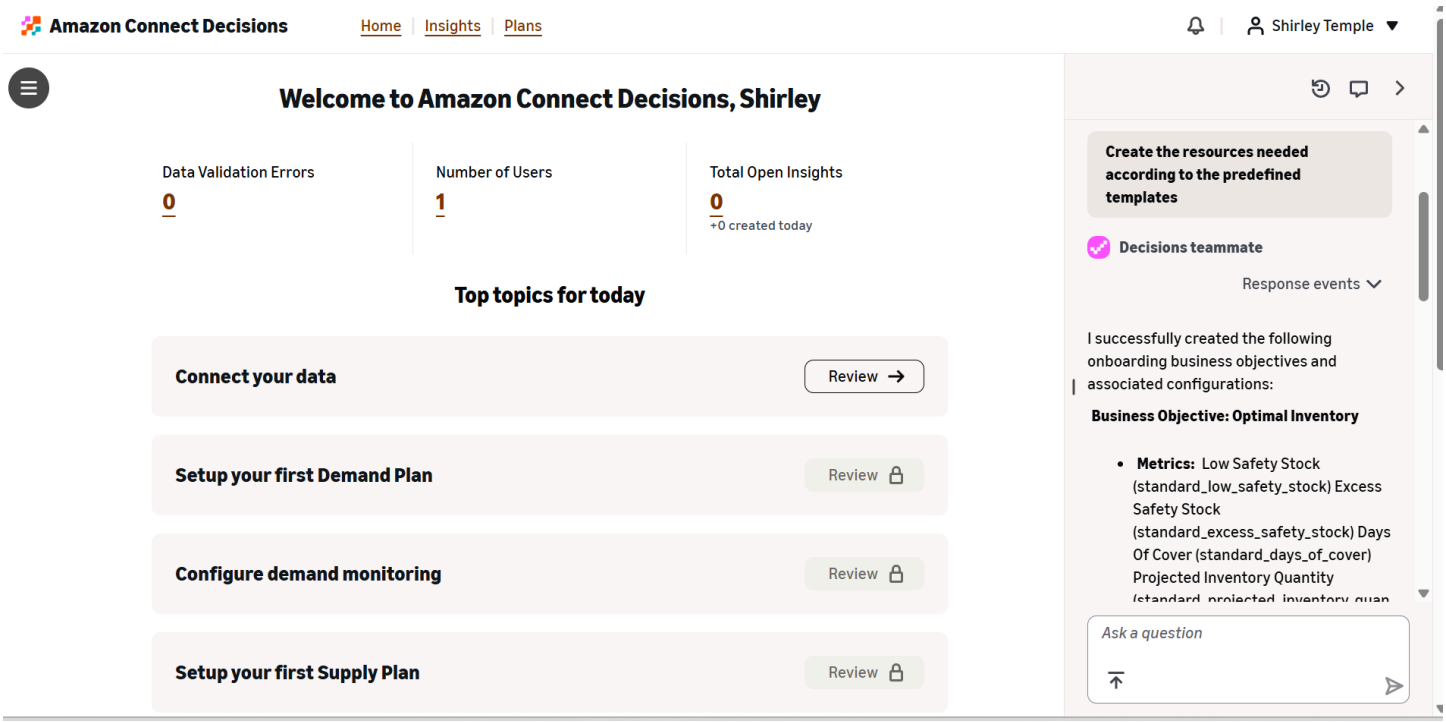


설문 조사 완료 후

네 단계를 모두 완료한 후 제출을 클릭합니다.

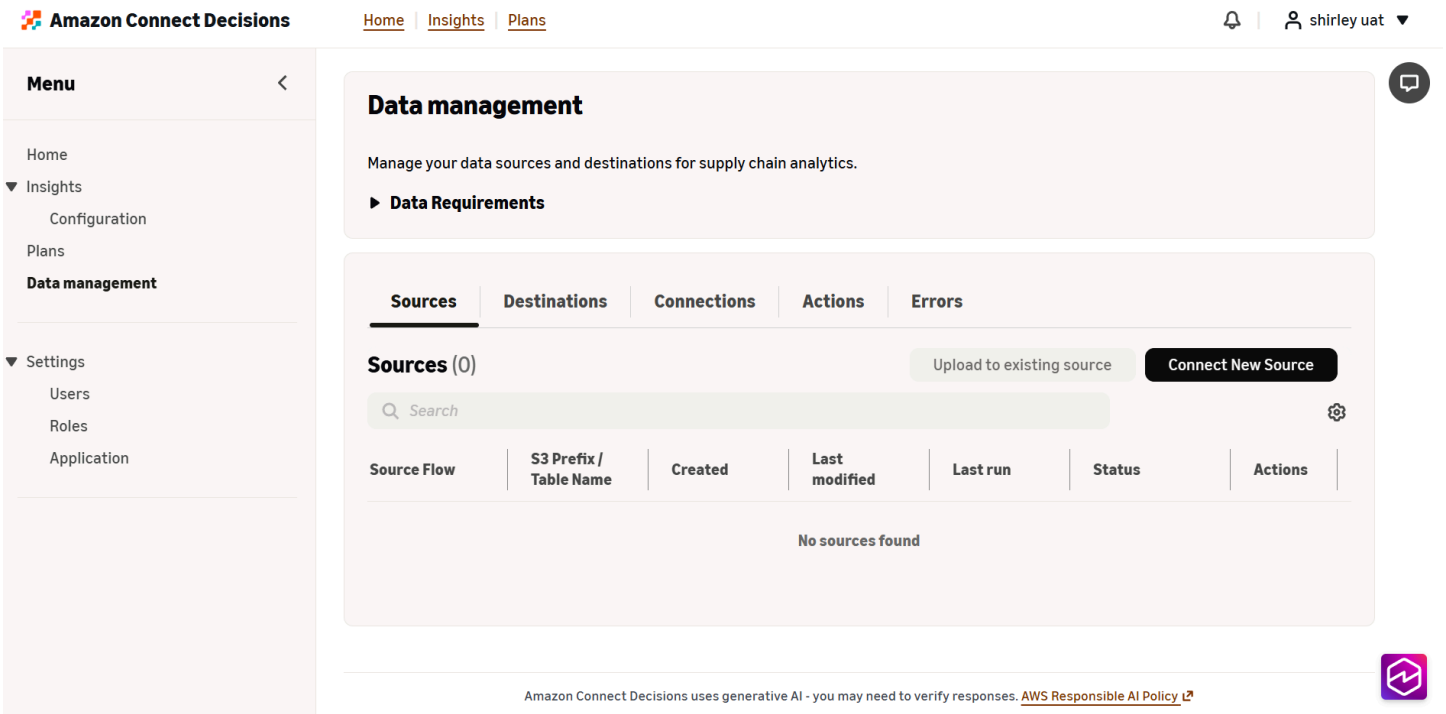


- 나머지 온보딩 단계를 안내하도록 설계된 대시보드 및 주제 카드가 있는 홈 페이지로 리디렉션됩니다.
- 시스템은 선택한 항목에 따라 애플리케이션 내에 지표와 규칙을 자동으로 생성합니다. 이는 초안 상태로 생성되며 즉시 활성화되지 않습니다.
- 자동으로 생성된 지표 및 규칙을 검토한 다음 필요에 따라 활성화하거나 특정 비즈니스 요구 사항에 맞는 고유한 지표 및 규칙을 생성할 수 있습니다.



첫 번째 소스 흐름 생성

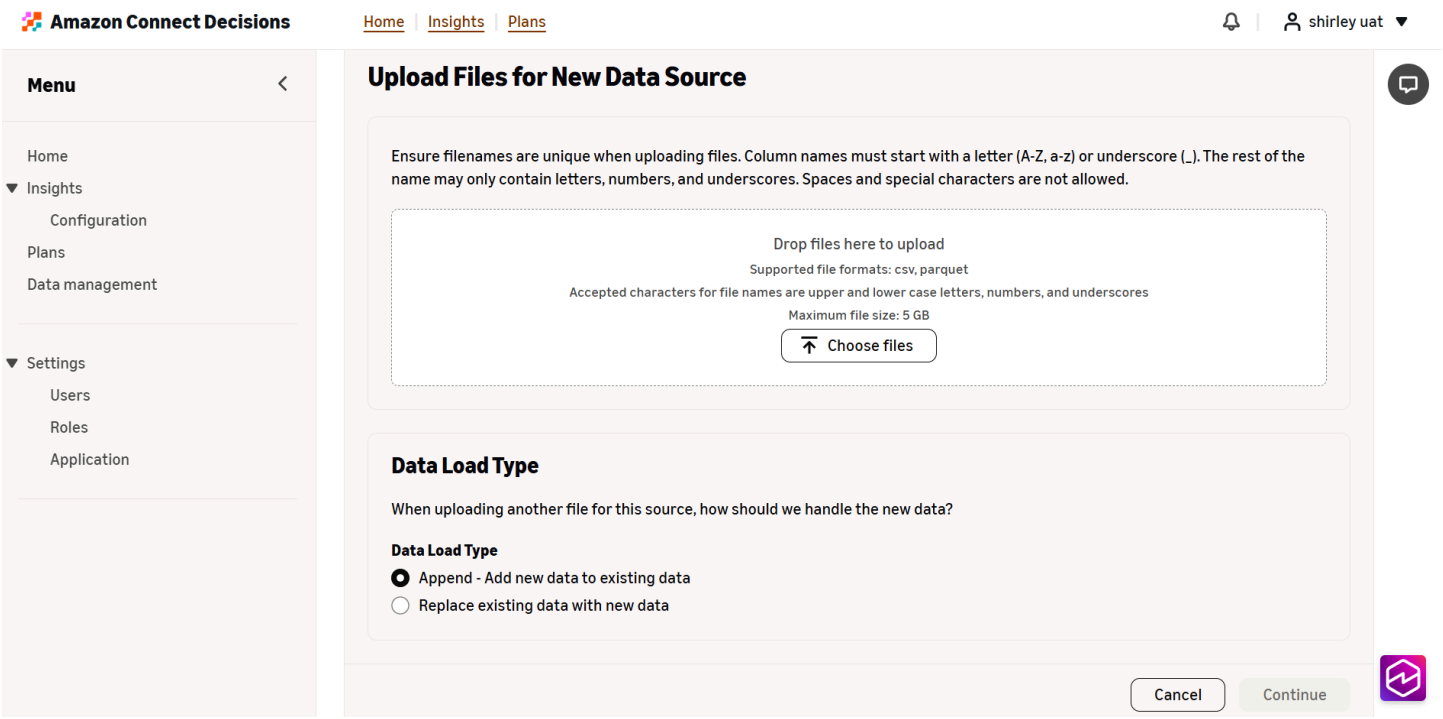
데이터 온보딩을 시작하려면 데이터 주제 카드 연결 검토를 클릭하거나 Amazon Connect 결정의 '햄버거 메뉴'에서 데이터 관리 탭으로 이동합니다. 여기에서 기존 소스 흐름을 모두 볼 수 있습니다. 아직 설정하지 않은 경우 "새 소스 연결"을 클릭하여 시작합니다.



소스 데이터 업로드

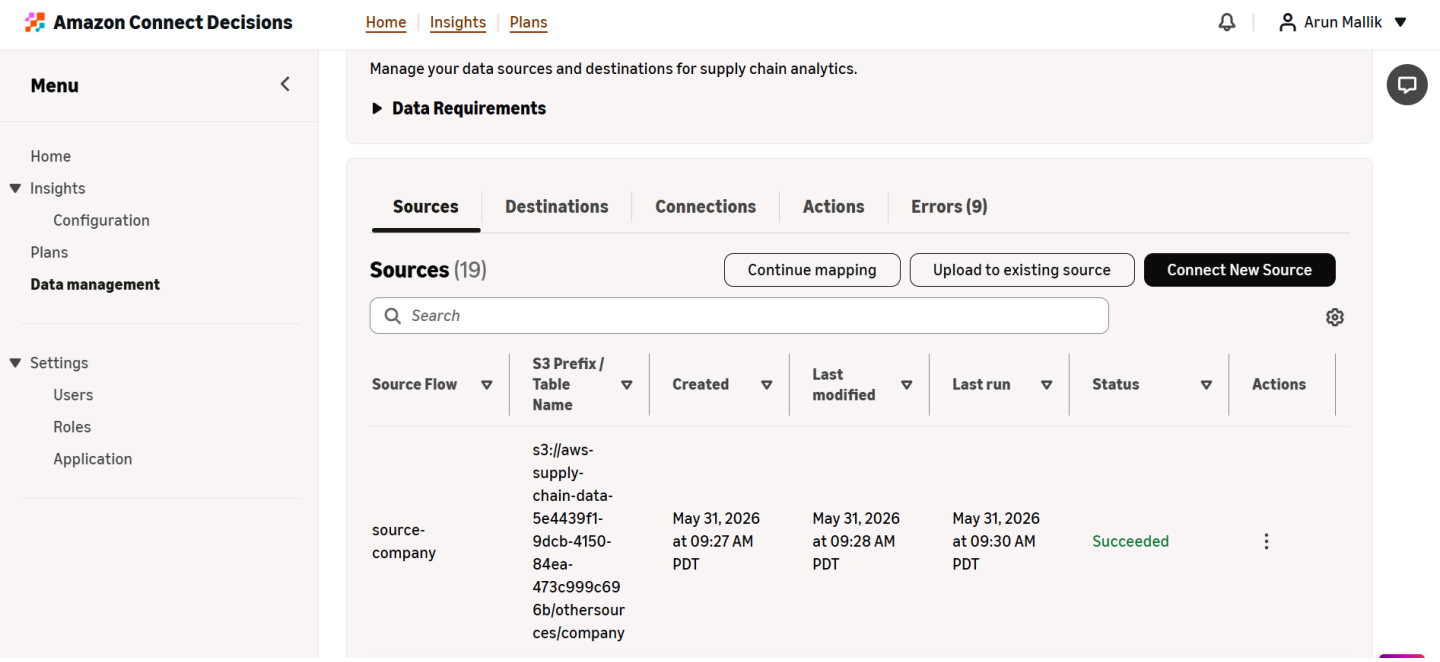
사용 사례에 필요한 CDM 테이블을 기반으로 소스 데이터가 포함된 CSV 파일을 업로드합니다. 데이터 업데이트를 처리하는 방법을 선택할 수 있습니다.

- 추가: 기존 데이터에 새 데이터 추가
- 바꾸기: 기존 데이터를 새 데이터로 바꾸기



파일을 업로드하면 Amazon Connect Decisions는 다음을 포함하여 해당 데이터에 대한 폴더 구조를 S3에 자동으로 생성합니다.

- 선택한 소스 시스템의 이름을 따서 명명된 상위 폴더
- 선택한 소스 테이블 이름의 이름을 따서 명명된 하위 폴더
- 하위 폴더 아래의 모든 파일은 동일한 소스 테이블에 저장됩니다.
- 이 파일 구조는 Amazon S3 폴더 경로를 생성하는 데에도 사용됩니다.

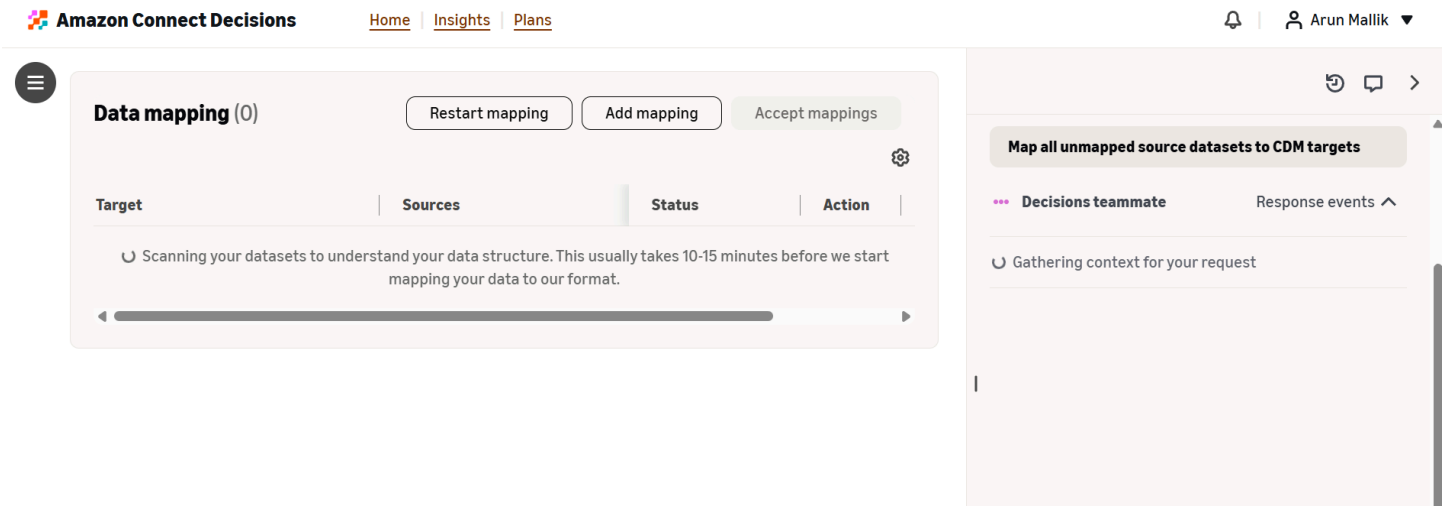


Source-to-CDM 대상 매핑

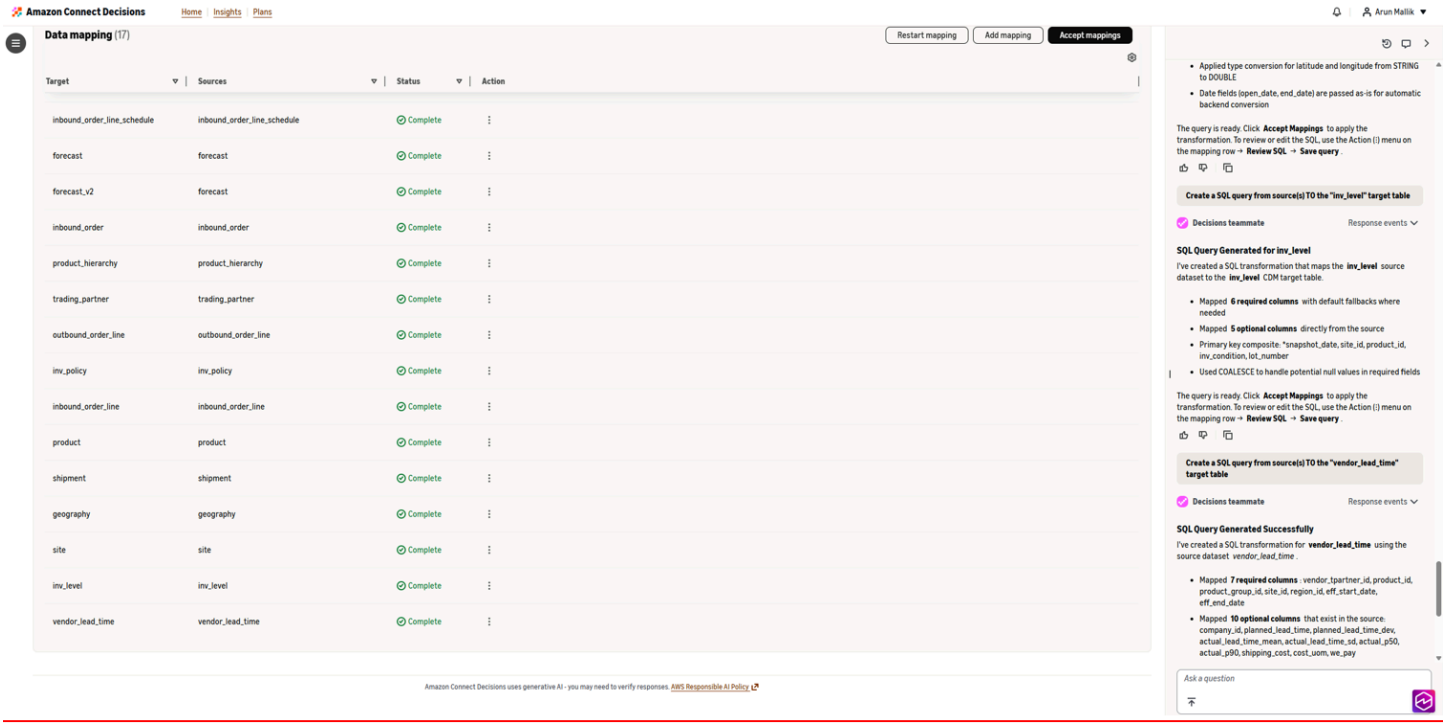
파일이 업로드되면 Amazon Connect Decisions는 데이터 분석을 시작하고 이를 하나 이상의 Amazon Connect Decisions CDM 대상 테이블에 자동으로 매핑합니다.

기대할 수 있는 사항

- 이 단계는 업로드된 데이터의 양에 따라 10~15분이 걸릴 수 있습니다.
- Data Agent는 백그라운드에서 작동하여 소스 데이터에 가장 적합한 CDM 대상 데이터 세트를 식별합니다.
- 이 페이지에서 벗어나면 자동 매핑이 실패합니다. 기다리는 동안 Amazon Connect 결정 및 데이터 관리 탭을 열어 두어 자동 매핑이 완료되도록 하세요.

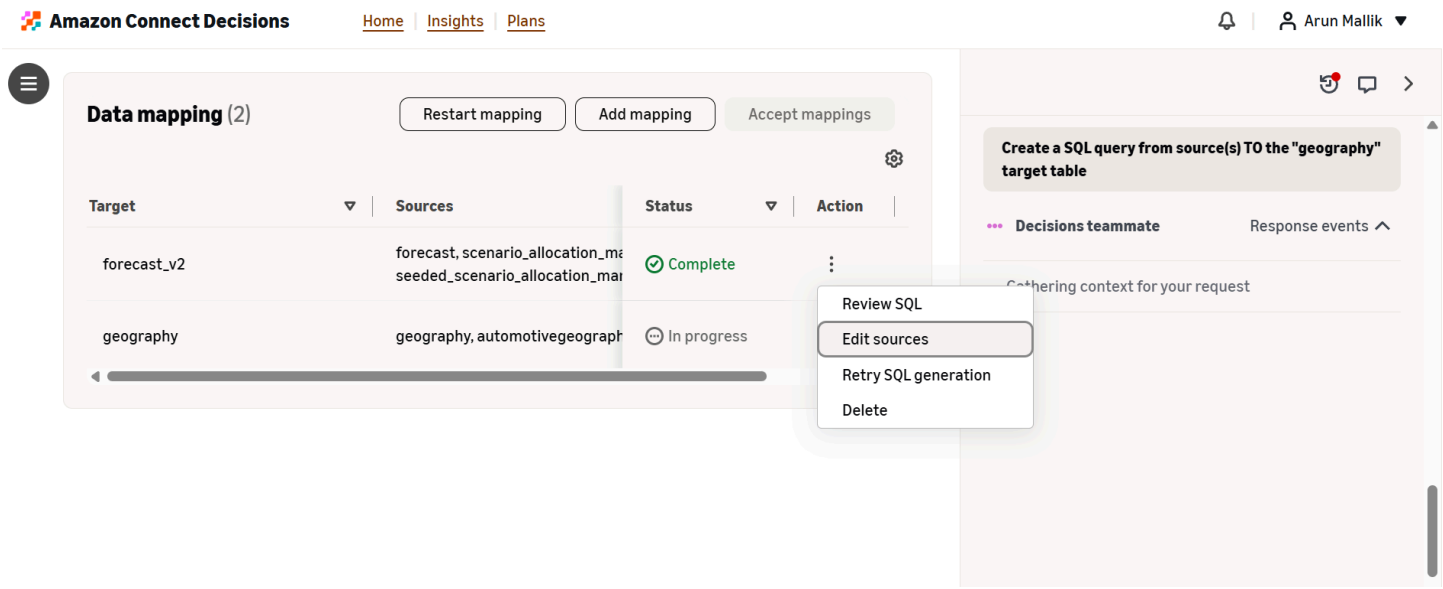


완료되면 Data Agent는 중첩 데이터를 기반으로 source-to-destination 매핑에 대한 근거를 제공하며, 이를 검토하고 매핑 결과에 대해 에이전트에게 질문할 수 있습니다.



소스 매핑을 검토하고 편집하려면 다음을 수행할 수 있습니다.

- 자연어를 사용하여 데이터 에이전트와 직접 상호 작용하여 소스 대상 매핑을 업데이트합니다.
- 작업을 클릭하고 "소스 편집"을 선택합니다.



매핑 편집

여기에서 다음을 수행할 수 있습니다.

- 필요한 경우 소스 및 대상 매핑을 수동으로 업데이트합니다.
- 화면 오른쪽에 있는 Data Agent를 사용하여 매핑을 확인하는 질문을 합니다.
- 특정 데이터 세트에 대해 자세히 알아보려면 사용 설명서를 참조하세요.

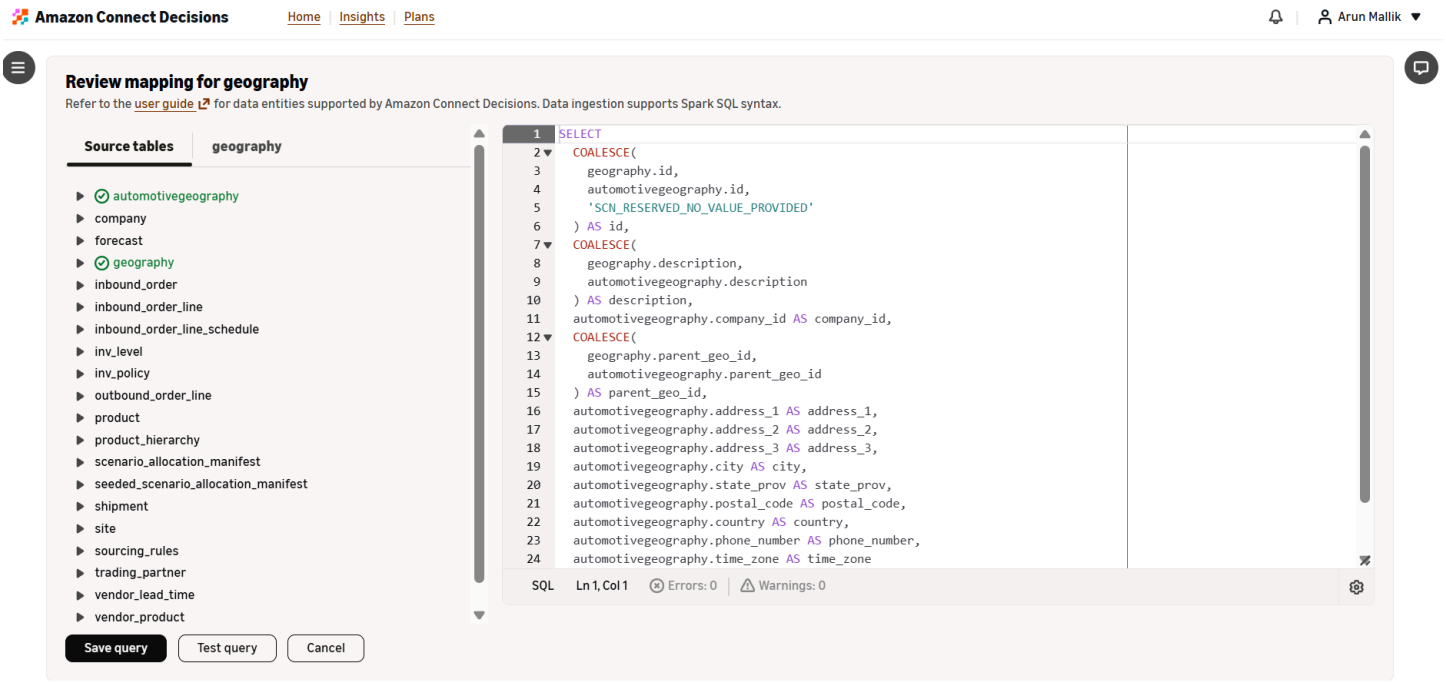
열/데이터 매핑

source-to-destination 매핑이 완료되면 Amazon Connect Decisions는 소스 데이터 세트에서 CDM 대상으로 SQL 변환 쿼리를 자동으로 생성합니다. 매핑이 완료되면 Data Agent로부터 매핑 결과를 자세히 설명하는 알림을 받게 됩니다.

여기에서 작업 메뉴에서 "SQL 검토"를 선택하여 매핑에 대해 생성된 SQL을 검토해야 합니다.

매핑(SQL)을 검토하면 다음이 표시됩니다.

- 추가한 소스 데이터 세트 열
- 참조용 대상 CDM 테이블 열
- 이를 연결하는 변환 SQL
- Data Agent에서 제공하는 매핑의 근거



매핑 편집

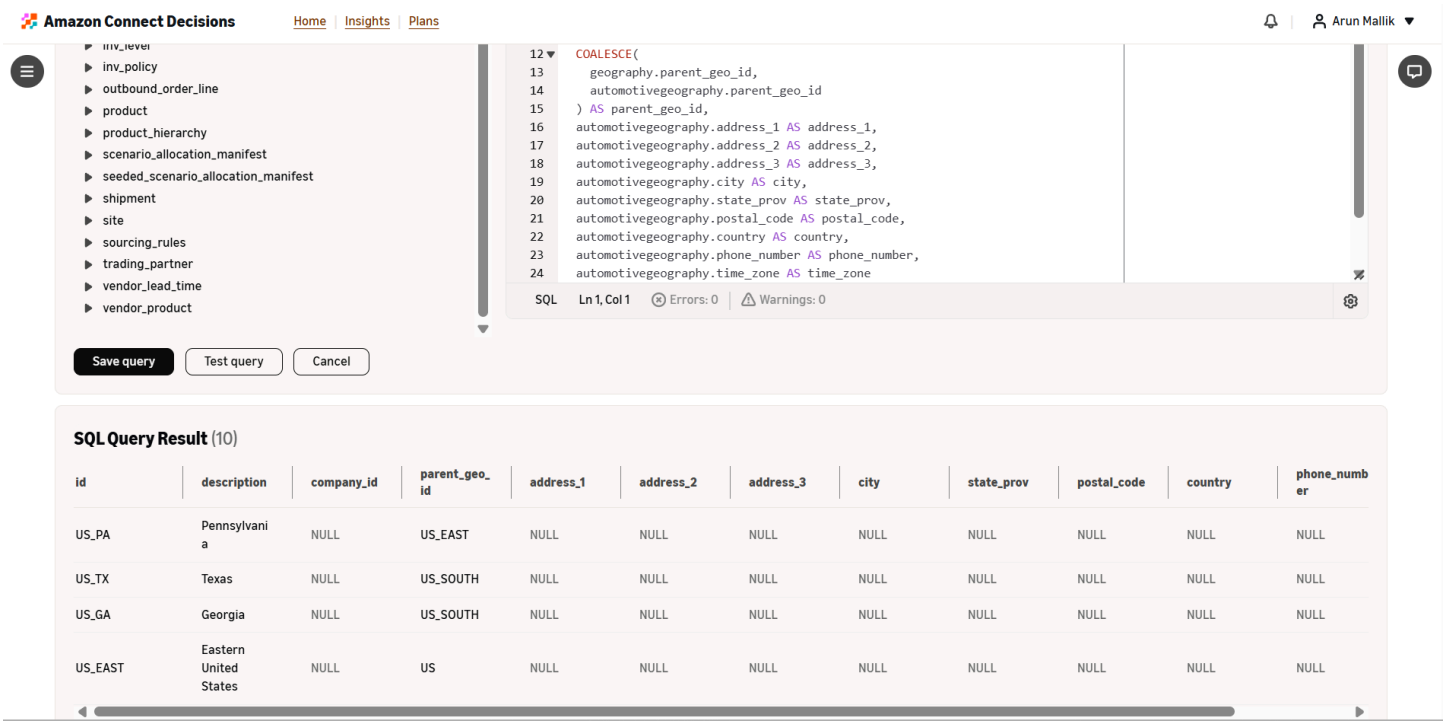
매핑을 편집하는 두 가지 옵션이 있습니다.

- Data Agent 작업: 자연어를 사용하여 매핑 질문, 관리 및 업데이트
- SQL Directly 편집: SQL에 익숙한 경우 쿼리를 직접 수정할 수 있습니다.

변경 사항 테스트

매핑 쿼리를 편집할 때 "테스트 쿼리" 기능을 사용하여 계속 테스트합니다. 그러면 데이터가 대상 CDM으로 변환되는 방식에 대한 샘플을 스크롤하여 미리 볼 수 있습니다. 이를 사용하여 변환이 제대로 실행되도록 하고 source-to-destination CDM에서 적절한 업데이트를 검증합니다.

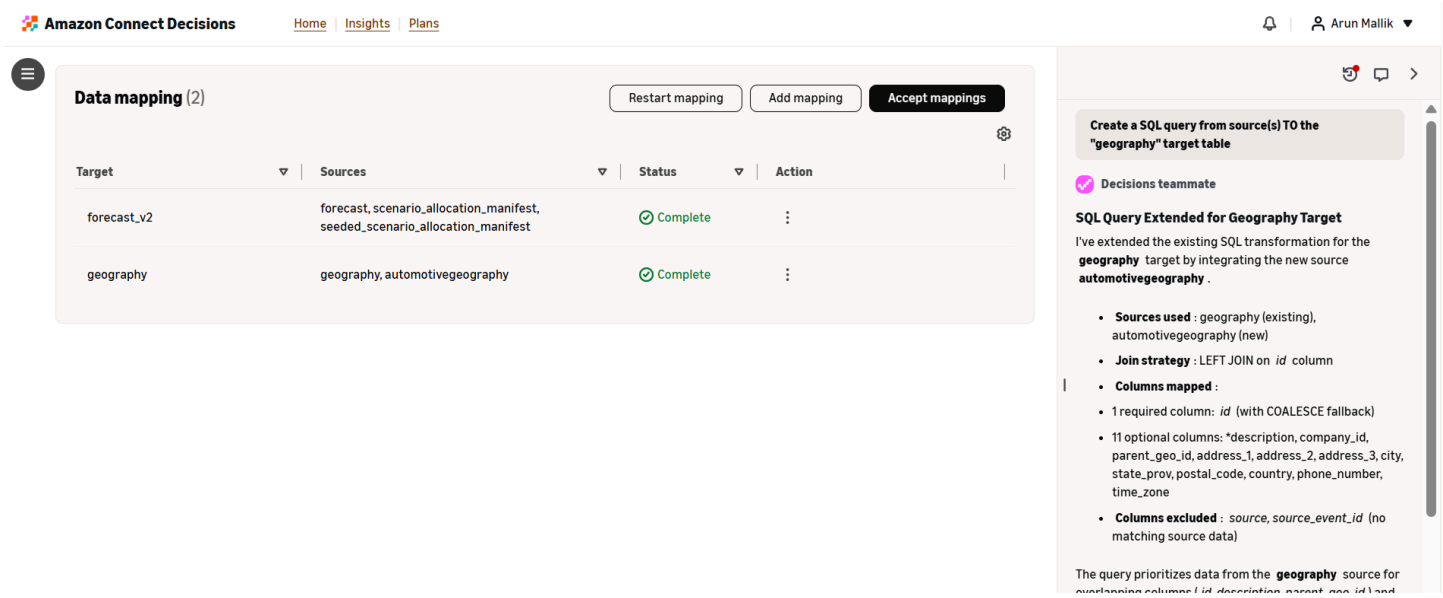
매핑 출력에 만족하면 "쿼리 저장"을 선택하여 해당 소스 대상 페어에 대한 변환 쿼리를 저장합니다.



매핑 검토 및 수락

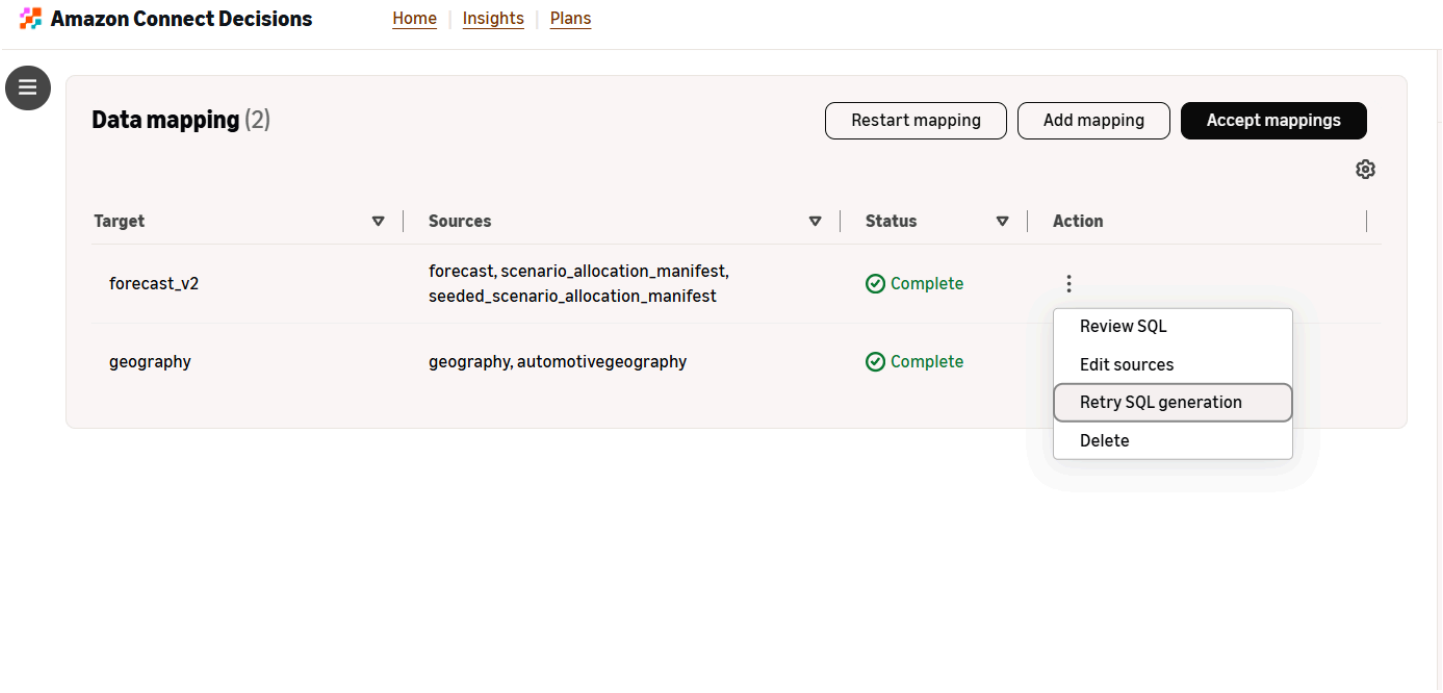
각 소스 데이터 세트에 대해 나머지 매핑을 검토합니다. Data Agent는 질문이나 문제 해결 도움말을 위해 화면 오른쪽에 지속적인 상태를 유지합니다.

모든 매핑에 만족하면 매핑 수락을 클릭하여 데이터 온보딩을 완료하도록 수락합니다.



실패한 매핑 처리

매핑에 실패한 경우 "매핑 다시 시작"을 선택하여 모든 매핑을 다시 시작하거나 "SQL 생성 재시도"를 통해 작업 메뉴에서 단일 매핑을 수동으로 재시도할 수 있습니다. 또한 Data Agent는 자연어를 사용하여 매핑을 재시도할 수 있으며 오류가 계속 지속될 경우 문제를 식별하고 해결하는 데 계속 도움이 됩니다.

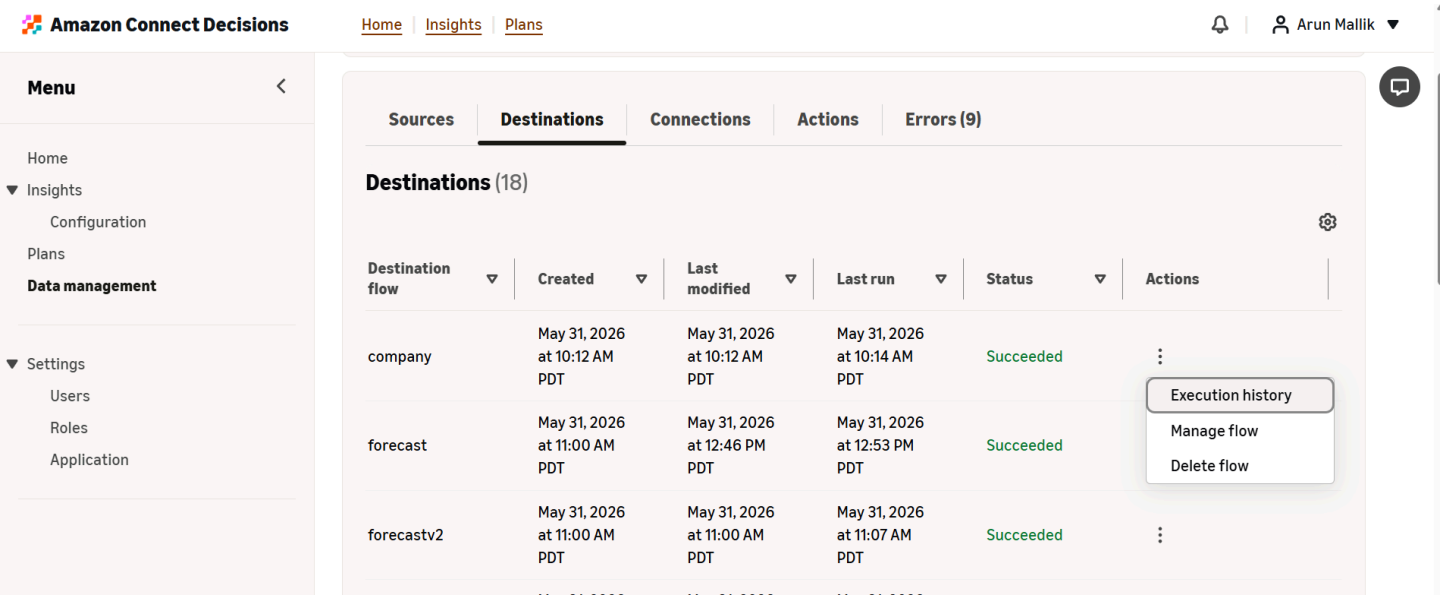


흐름 모니터링

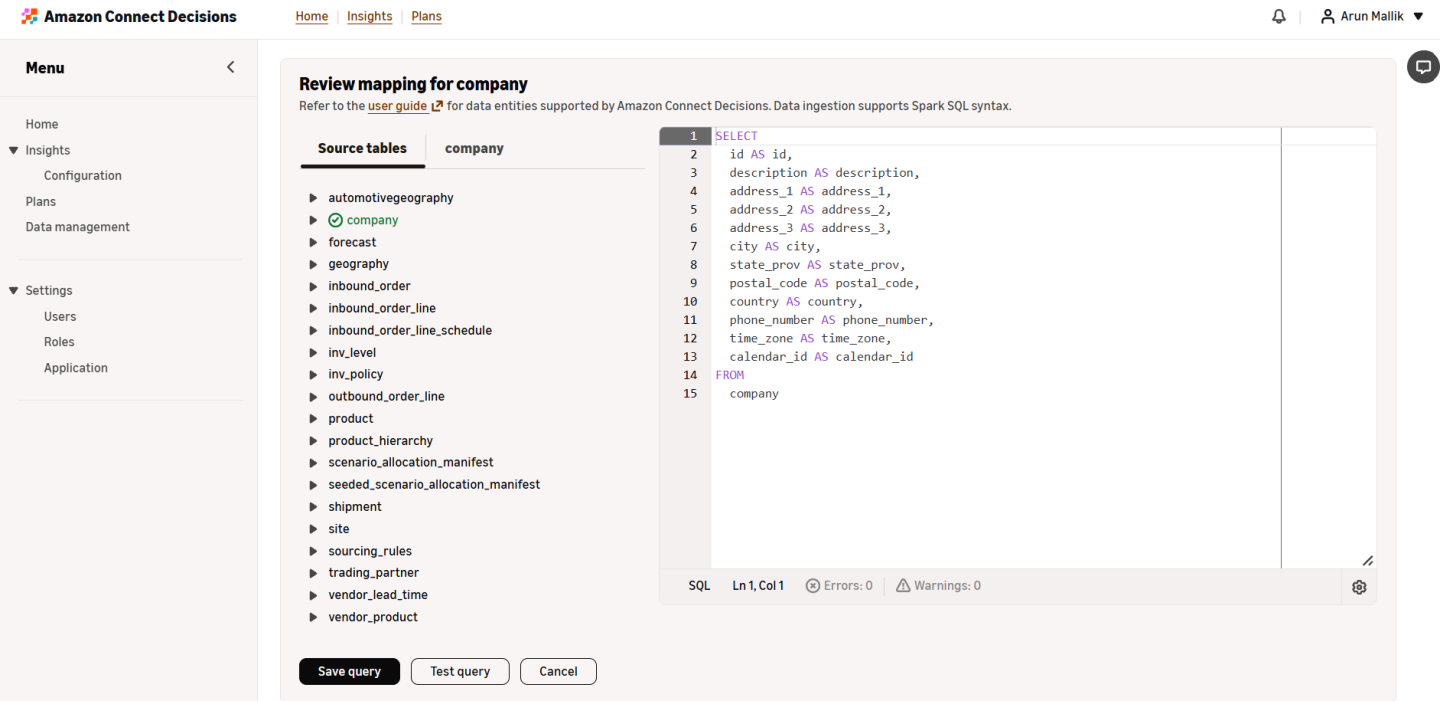
대상 탭

매핑을 수락하면 데이터 관리 내의 대상 탭으로 이동하여 다음을 수행할 수 있습니다.

- 대상 흐름 검토
- 매핑 관리 및 편집("흐름 관리")
- 더 이상 사용되지 않는 흐름 삭제
- 이러한 흐름의 실행 상태 검토



"흐름 관리"를 선택하면 데이터 에이전트와 계속 협력하여 시간이 지남에 따라 매핑을 세분화할 수 있는 데이터 매핑 환경으로 돌아갑니다.



소스 탭

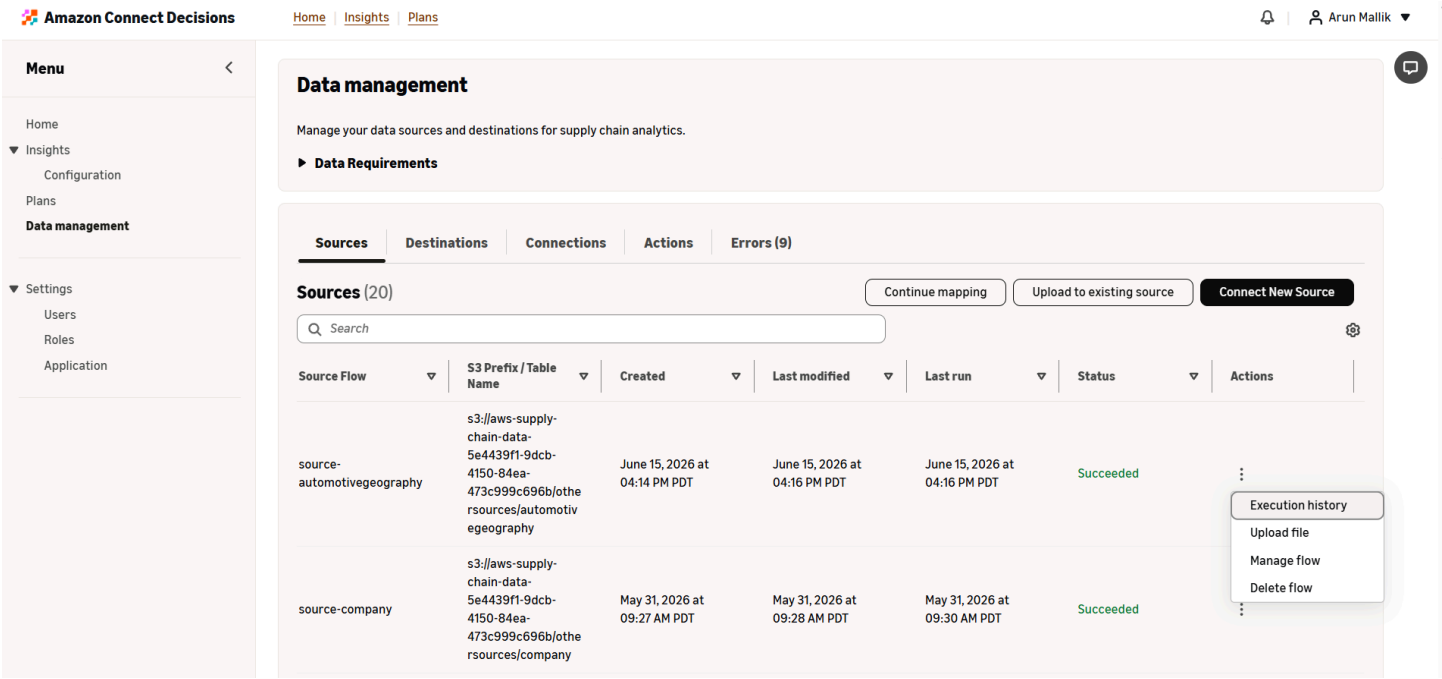
소스 탭으로 돌아가면 다음을 찾을 수 있습니다.

- 생성된 소스 데이터 세트
- 연결된 S3 버킷

- 옵션:
  - 다른 파일 업로드를 통해 더 많은 소스 데이터 추가
  - 흐름 관리
  - 흐름 삭제
  - 실행 검토

"흐름 관리"를 선택하면 데이터 에이전트와 계속 협력하여 시간이 지남에 따라 매핑을 세분화할 수 있는 데이터 매핑 환경으로 돌아갑니다.

또한 필요에 따라 새 소스 생성에 액세스하여 새 데이터 소스에 대한 데이터 온보딩 프로세스를 다시 시작할 수 있습니다.



모범 사례

데이터 준비

- 사전 조건 섹션의 단계를 따릅니다.
- 모든 CSV 파일에 UTF-8 인코딩 사용
- 파일 이름이 고유한지 확인
- 업로드하기 전에 데이터 품질 검증

Data Agent 작업

- 요청에 구체적이어야 합니다.
- 결정을 이해하지 못할 때 설명을 요청합니다.
- 수락하기 전에 모든 SQL 변경 사항 테스트
- 미리 보기 기능을 사용하여 변환 확인

지속적 유지 관리

- 소스 데이터를 최신 상태로 유지
- 흐름 실행을 정기적으로 모니터링
- 알림을 받으면 즉시 데이터 오류 해결
- 팀에 대한 사용자 지정 변환 문서화

JDBC를 사용하여 데이터베이스에 연결

이 가이드에서는 Java Database Connectivity(JDBC)를 사용하여 데이터베이스를 Amazon Connect Decisions에 연결하는 방법을 안내합니다. 데이터베이스 자격 증명에 대한 보안 암호화를 설정하고 Amazon Connect Decisions가 데이터에 액세스하는 데 사용할 수 있는 연결을 설정합니다.

JDBC 연결이란 무엇이며 언제 사용해야 합니까?

JDBC 연결을 사용하면 Amazon Connect Decisions가 CSV 파일을 내보내고 업로드하거나 자체 추출, 변환, 로드(ETL) 파이프라인을 S3로 설정할 필요 없이 기존 데이터베이스에 연결하여 데이터를 읽을 수 있습니다. 이 접근 방식은 다음과 같은 경우에 이상적입니다.

- 데이터가 AWS Glue 호환 관계형 데이터베이스에 이미 저장되어 있습니다. 호환되는 데이터베이스 및 버전은 이 가이드를 참조하세요.
- 수동 파일 내보내기 없이 실시간 또는 near-real-time 데이터 액세스를 원하는 경우
- 데이터 볼륨이 크고 자주 업데이트됨
- 데이터를 복제하는 대신 현재 위치에 보관하는 것이 좋습니다.
- 더 작은 데이터 세트로 작업하거나 파일 기반 업로드를 선호하는 경우 필요에 따라 표준 CSV 업로드 프로세스가 더 간단할 수 있습니다. 이 프로세스에 대한 자세한 내용은 데이터 온보딩 사용 설명서를 참조하세요.

사전 조건

시작하기 전에 다음을 갖추었는지 확인하세요.

- KMS 키 및 Secrets Manager 리소스를 생성할 수 있는 권한이 있는 AWS 계정
- AWS 계정 ID 및 Amazon Connect 결정이 운영될 리전
- 데이터베이스 연결 세부 정보: 호스트 이름, 포트, 데이터베이스 이름 및 자격 증명
- 연결을 확인하기 위한 데이터베이스에 대한 관리 액세스
- AWS 서비스의 연결을 수락하도록 구성된 데이터베이스

고객 관리형 KMS 키 생성

데이터베이스를 Amazon Connect Decisions에 연결하기 전에 데이터베이스 자격 증명에 대한 암호화를 설정해야 합니다. AWS Key Management Service (KMS)는이 보안 계층을 제공하여 연결 세부 정보를 보호합니다.

KMS 키 생성

1. AWS KMS 콘솔로 이동
   - 브라우저에서 AWS Management Console을 엽니다.
   - 상단의 검색 창에 "KMS"를 입력하고 결과에서 "Key Management Service"를 선택합니다.
   - 그러면 암호화 키를 관리할 KMS 대시보드가 열립니다.
2. 키 생성 시작
   - KMS 대시보드에서 오른쪽 상단의 키 생성 버튼을 찾아 클릭합니다.
   - 그러면 설정 프로세스를 안내하는 키 생성 마법사가 시작됩니다.
3. 키 유형 및 사용량 구성
   - "키 구성" 페이지에서 키 유형으로 대칭을 선택합니다(기본 및 권장 옵션).
   - 키 사용에서 "암호화 및 복호화"를 선택한 상태로 유지
4. 키 식별 세부 정보 설정
   - "별칭" 필드에 다음과 같이 키를 설명하는 이름을 입력합니다. `aws-supply-chain-database-key`
   - "설명" 필드에 "Amazon Connect Decisions 데이터베이스 자격 증명의 암호화 키"와 같은 컨텍스트를 추가합니다.

- 선택적으로 AWS 리소스를 구성하고 추적하는 데 도움이 되는 태그를 추가합니다(예: 키: "프로젝트", 값: "Amazon Connect 결정").

5. 키 관리 권한 정의
   - 이 키를 관리할 수 있어야 하는 IAM 사용자 또는 역할 선택(정책 생성, 삭제, 수정)
   - 필요한 경우 나중에 키를 수정할 수 있도록 최소한 자체 관리자 역할을 포함합니다.
   - 이러한 관리자는 키를 관리할 수 있지만 암호화/암호 해독에 사용할 수 있는 권한은 자동으로 없습니다.
   - "키 삭제" 섹션에서 키 관리자가이 키를 삭제하도록 허용합니다(기본 및 권장 옵션).
6. 키 사용 권한 정의
   - 이 페이지에는 키를 사용할 수 있는 IAM 사용자 및 역할을 선택하는 옵션이 표시됩니다.
   - 여기에서 특정 사용자 선택을 건너뛰면 다음 단계에서 서비스 권한을 구성합니다.
7. Amazon Connect Decisions 서비스에 대한 키 정책 구성
   - 기본 JSON이 있는 정책 편집기가 표시됩니다.
   - KMS 키 정책 편집기에서 기존 "Statement" 배열에 다음 문을 추가합니다.
   - 이 정책은 계정에 모든 권한을 부여하고 Amazon Connect Decisions의 서비스(Secrets Manager 및 Glue)가 데이터베이스 자격 증명을 해독하도록 허용합니다.

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

8. 검토 및 완료
   - 요약 페이지에서 모든 구성 설정 검토
   - 별칭, 설명 및 정책이 올바른지 확인
   - 완료를 클릭하여 키를 생성합니다.

- 생성되면 새 키가 목록에 나타나는 KMS 대시보드로 돌아갑니다.

기대할 수 있는 사항

키 생성은 즉시 이루어집니다. 생성되면 KMS 콘솔에 "Enabled" 상태의 새 키가 나열됩니다. 이제 키가 Secrets Manager에서 데이터베이스 자격 증명을 암호화할 준비가 되었습니다.

AWS Secrets Manager 구성

이제 KMS 키가 있으므로 AWS Secrets Manager에서 보안 암호를 생성하여 데이터베이스 자격 증명을 안전하게 저장한 다음 Amazon Connect Decisions가이 보안 암호에 액세스할 수 있도록 허용하는 리소스 정책을 구성합니다.

보안 암호 생성

1. AWS Secrets Manager로 이동
   - AWS Management Console 검색 창에 "Secrets Manager"를 입력합니다.
   - 결과에서 "Secrets Manager"를 선택하여 서비스 대시보드를 엽니다.
2. 새 보안 암호 생성 시작
   - 새 보안 암호 저장 버튼을 클릭합니다.
   - "보안 암호 유형 선택" 페이지에서 다른 유형의 보안 암호를 선택합니다(이렇게 하면 보안 인증 정보를 유연하게 구성할 수 있음).
3. 데이터베이스 자격 증명 입력
   - 키-값 페어 섹션에서 데이터베이스 연결 세부 정보를 문자열로 추가합니다.

```
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. 암호화 키 선택
   - "암호화 키"에서 AWS KMS 키 선택을 선택합니다.
   - 드롭다운에서 1단계에서 생성한 KMS 키(예: `aws-supply-chain-database-key`)를 선택합니다.
   - 이렇게 하면 자격 증명이 고객 관리형 키로 암호화됩니다.

5. 보안 암호 이름 지정
   - 와 같이 암호를 설명하는 이름을 입력합니다. `aws-supply-chain-production-database`
   - 선택적으로 "Amazon Connect Decisions 프로덕션 환경의 데이터베이스 자격 증명"과 같은 설명을 추가합니다.
   - 조직에 필요한 경우 태그를 추가합니다(예: 키: "Environment", 값: "Production").
6. 리소스 권한 추가
   - "권한 편집"을 클릭합니다. 정책 편집기에서 다음 정책을 붙여 넣습니다. 이 정책은 Amazon Connect Decisions의 서비스가 보안 암호를 읽도록 허용합니다.

```
{
  "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. 정책 저장
   - 저장을 클릭하여 리소스 정책을 적용합니다.
   - 이제 정책이 활성화되어 Amazon Connect Decisions가 데이터베이스 자격 증명을 검색할 수 있습니다.
8. 교체 구성(선택 사항)
   - 이 설정의 경우 자동 교체 비활성화를 선택하여 자동 교체를 건너뛸 수 있습니다.
   - 보안 정책에 필요한 경우 나중에 교체를 활성화할 수 있습니다.
9. 검토 및 생성
   - 모든 보안 암호 세부 정보 검토
   - 저장을 클릭하여 보안 암호를 생성합니다.
   - Secrets Manager 대시보드로 돌아갑니다.
10. 보안 암호 ARN 저장
    - 보안 암호 목록에서 새로 생성된 보안 암호를 찾습니다.
    - 보안 암호 이름을 클릭하여 세부 정보 페이지를 엽니다.

- 상단에 보안 암호 ARN이 표시됩니다.
- 이 ARN 복사 및 저장
- ARN 형식은 다음과 같습니다. `arn:aws:secretsmanager:us-east-1:123456789012:secret:aws-supply-chain-production-database-AbCdEf`

11.리소스 권한 편집

- "권한 편집"을 클릭합니다.
- 복사한 보안 암호 ARN을 붙여넣고를 복사한 ARN<COPY-THE-SECRET-ARN-HERE-AFTER-CREATING>으로 바꿉니다.
- 저장을 클릭하여 정책을 연결합니다.

기대할 수 있는 사항

이제 보안 암호가 안전하게 저장되고 KMS 키로 암호화됩니다. Amazon Connect Decisions의 서비스는 데이터베이스 연결을 설정할 때 자격 증명을 검색할 수 있는 권한이 있지만 자격 증명은 저장 및 전송 중에 암호화된 상태로 유지됩니다.

데이터베이스를 Amazon Connect 결정에 연결

KMS 키와 보안 암호가 구성되면 Amazon Connect 결정에서 JDBC 연결을 설정할 준비가 된 것입니다.

JDBC 연결 구성

1. Amazon Connect 결정 > 데이터 관리로 이동
   - Amazon Connect Decisions 인스턴스에 로그인
   - 기본 탐색에서 "데이터 관리"를 선택합니다.
   - 탭 탐색 내에서 "연결"로 이동합니다.
   - "새 연결"을 선택하여 새 연결을 생성합니다.
2. 연결 세부 정보 입력
   - 연결 이름(필수):이 연결의 고유 식별자를 입력합니다(예: "production-database").
   - 설명(선택 사항): 팀이 액세스하는 데이터를 이해하는 데 도움이 되도록이 연결의 용도 및 사용에 대한 세부 정보를 추가합니다.
   - JDBC URL(필수): 전체 JDBC 연결 문자열을 형식으로 입력합니다`jdbc:<database-type>://<hostname>:<port>/<database>`(예: `jdbc:postgresql://db.example.com:5432/mydb`).

- 스키마 이름(선택 사항): 필요한 경우 데이터베이스 스키마를 지정합니다(예: "public", "dbo", "myschema"). 데이터베이스의 기본 스키마를 사용하려면 비워 둡니다.
- 보안 암호 ARN(필수): 2단계에서 저장한 보안 암호 ARN을 붙여넣습니다. 이렇게 하면 Amazon Connect Decisions가 Secrets Manager에서 데이터베이스 자격 증명을 안전하게 검색할 수 있습니다.
- SSL 연결 적용: 데이터베이스 연결에 SSL/TLS 암호화를 요구하려면이 확인란을 선택(권장) 상태로 유지합니다.
- VPC 엔드포인트 서비스 이름(필수): AWS PrivateLink를 통한 프라이빗 연결을 위해 VPC 엔드포인트 서비스 이름을 입력합니다(형식: `com.amazonaws.vpce.<region>.vpce-svc-xxxxxxxxx`).

3. 데이터베이스에 연결
   - "Connect"를 클릭하여 연결을 테스트하고 설정합니다. Amazon Connect Decisions는 제공된 자격 증명을 사용하여 데이터베이스에 성공적으로 연결할 수 있는지 확인합니다. 이 단계는 최대 2분이 걸릴 수 있으므로 연결 중에이 화면을 벗어나지 마십시오.
   - 연결이 성공하면 테이블 선택으로 자동 이동합니다.
   - 연결에 실패하는 경우:
     - 연결 세부 정보를 검토하여 모든 필드가 정확한지 확인합니다.
       - 보안 암호 ARN이 올바른지 확인
       - 데이터베이스 자격 증명이 정확한지 확인
       - JDBC URL 형식이 올바른지 확인
       - AWS 서비스의 연결을 수락하도록 데이터베이스가 구성되어 있는지 확인합니다.
       - KMS 키 및 Secrets Manager 정책이 올바르게 구성되었는지 확인
     - 채팅 경험을 사용하여 "내 데이터베이스 연결이 실패하는 이유는 무엇입니까?"와 같은 질문을 하여 연결 문제를 해결할 수도 있습니다. 또는 "JDBC 연결을 디버깅할 수 있도록 도와주세요"
4. 수집할 테이블 선택
   - 연결되면 데이터베이스에서 사용 가능한 모든 테이블을 보여주는 테이블 선택 화면이 표시됩니다.
   - 수집하려는 각 테이블 옆의 확인란을 선택합니다.
5. 테이블 새로 고침 일정 구성
   - 선택한 각 테이블에 대해 작업 열에서 점 3개 메뉴를 클릭하고 "Schedule refresh"를 선택합니다.
   - 로드 세부 정보 구성 대화 상자에서 다음을 설정합니다.
     - Cadence: 새로 고침 빈도(시간별, 일별, 주별 또는 사용자 지정)

    - 시작 시간: 새로 고침이 시작되는 시간(시간대 오프셋과 함께 UTC로 표시됨)
    - 새로 고침 유형: 새로 고침 완료(모든 데이터 교체) 또는 증분 업데이트(기존에 새 데이터 추가, 타임스탬프 기록 열 선택 필요)를 선택합니다.
    - 필요에 따라 각 테이블에 대해 반복합니다.
  - 모든 테이블이 구성되면 매핑 시작을 클릭합니다.
6. 데이터 매핑 계속
  - 이 시점부터 경험은 데이터 온보딩 흐름과 동일합니다.
  - 데이터 온보딩 사용 설명서의 데이터 매핑 섹션에 따라 설정을 완료합니다.

기대할 수 있는 사항

연결이 설정되고 테이블이 선택되면 Amazon Connect Decisions는 데이터베이스에서 데이터를 읽을 수 있습니다. AWS Secrets Manager를 통해 암호화되고 관리되는 자격 증명을 사용하여 연결이 활성 상태로 안전하게 유지됩니다. Amazon Connect 결정에서 자격 증명을 수동으로 업데이트할 필요가 없습니다. Secrets Manager에서 변경한 내용은 자동으로 반영됩니다.

모범 사례

보안 및 액세스 관리

- 보안 인증 정보 저장: 항상 AWS Secrets Manager를 사용하여 데이터베이스 보안 인증 정보를 저장하고 연결 문자열 또는 구성 파일에 보안 인증 정보를 하드코딩하지 않습니다.
- SSL/TLS 암호화 활성화: 전송 중 데이터가 암호화되도록 'SSL 연결 적용' 옵션을 활성화된 상태로 유지합니다.
- KMS 및 Secrets Manager 정책을 정기적으로 검토: 승인된 서비스 및 계정만 암호화 키 및 보안 암호에 액세스할 수 있는지 확인합니다.
- 최소 권한 액세스 사용: Amazon Connect Decisions가 연결에 사용할 데이터베이스 사용자에게 필요한 최소 권한만 부여합니다.

연결 구성

- 설명 연결 이름 사용: 환경 및 목적을 나타내는 명확하고 의미 있는 이름을 선택합니다(예: "db1"이 아닌 "production-inventory-db").
- 연결 문서화: 설명 필드를 사용하여 연결이 액세스하는 데이터, 연결을 소유한 사람 및 특별한 고려 사항을 기록해 둡니다.

- 계속하기 전에 연결 테스트: 테이블을 선택하고 새로 고침 일정을 구성하기 전에 항상 연결이 작동하는지 확인합니다.
- JDBC URL 형식 검증: 연결 오류를 방지하려면 JDBC URL 구문이 데이터베이스 유형과 일치하는지 다시 확인합니다.

데이터 새로 고침 전략

- 적절한 새로 고침 주기 선택: 소스 데이터가 변경되는 빈도와 비즈니스 요구 사항에 따라 새로 고침 빈도를 선택합니다.
- 활동이 적은 기간 동안 새로 고침 예약: 성능 영향을 최소화하기 위해 데이터베이스의 부하가 낮을 때 새로 고침 시간 구성
- 가능한 경우 증분 업데이트 사용: 자주 변경되는 대규모 데이터 세트의 경우 증분 업데이트가 전체 새로 고침보다 더 효율적입니다.
- 의미 있는 타임스탬프 열 선택: 증분 업데이트를 사용하는 경우 레코드가 생성되거나 수정된 시기를 정확하게 반영하는 열을 선택합니다.

문제 해결을 위한 채팅 작업

- 요청에 구체적으로 명시: 연결 또는 매핑 문제 해결에 도움을 요청할 때 명확한 컨텍스트 제공
- 설명 요청: 권장 사항 또는 생성된 SQL 쿼리를 이해하지 못하는 경우 설명을 요청합니다.
- 수락하기 전에 모든 SQL 변경 사항 테스트: 미리 보기 기능을 사용하여 변환이 실제 데이터와 함께 예상대로 작동하는지 확인합니다.
- 채팅을 활용하여 문제 해결: 연결에 실패하거나 새로 고침에 오류가 발생하면 "내 연결이 실패하는 이유는 무엇입니까?"와 같은 진단 질문을 합니다. 또는 "이 새로 고침 오류를 이해하도록 도와주세요"

지속적 유지 관리

- 새로 고침 실행을 정기적으로 모니터링: 데이터 관리의 대상 및 소스 탭을 확인하여 새로 고침이 성공적으로 완료되었는지 확인합니다.
- 오류 즉시 해결: Amazon Connect Decisions에서 오류를 새로 고치라는 알림을 받으면 데이터 격차를 방지하기 위해 문제를 신속하게 조사하고 해결합니다.
- 보안 인증 정보 업데이트: 데이터베이스 암호가 변경되면 AWS Secrets Manager에서 업데이트하면 Amazon Connect Decisions에서 새 보안 인증 정보를 자동으로 사용합니다.

- 사용자 지정 구성 문서화: 팀 참조를 위해 특별 새로 고침 일정, 변환 로직 또는 연결 요구 사항에 대한 메모를 보관합니다.
- 테이블 선택 항목 주기적으로 검토: 데이터 요구 사항이 발전함에 따라 수집 중인 테이블과 새로 고침 일정이 여전히 비즈니스 요구 사항에 맞는지 다시 검토합니다.

표준 데이터 모델(CDM) 이해

표준 데이터 모델(CDM)은에서 사용하는 표준화된 데이터 구조입니다. 공급망 데이터를 온보딩할 때가 계획, 예측 및 운영 인사이트를 위해 처리할 수 있도록 CDM 형식으로 변환해야 합니다.

이 주제에서는 CDM의 정의, CDM이 중요한 이유, 사용 가능한 데이터 엔터티에 대해 설명합니다.

CDM이란 무엇입니까?

CDM은 제품, 사이트, 주문, 배송 및 재고와 같은 공급망 개념을 나타내는 일반적인 데이터 엔터티 및 필드 세트를 정의합니다. 소스 데이터의 형식이나 구조에 관계없이 CDM은 모든 기능에서가 사용하는 일관된 단일 스키마를 제공합니다.

데이터 온보딩 중에 소스 데이터는 CDM 대상 테이블에 매핑됩니다. Data Agent는 소스 필드와 CDM 필드 간의 매핑을 자동으로 제안하고 SQL 변환 쿼리를 생성하여 데이터를 변환할 수 있습니다.

CDM이 중요한 이유

- 일관성 -의 모든 기능은 동일한 데이터 구조에서 작동하여 수요 계획, 인벤토리 최적화 및 리드 타임 인사이트 전반에서 균일한 동작을 보장합니다.
- 상호 운용성 - 서로 다른 소스 시스템(ERP, WMS, TMS)의 데이터가 단일 모델로 정규화되어 시스템 간 분석이 가능합니다.
- 간소화된 온보딩 - 데이터 에이전트는 자동 매핑을 생성할 때 CDM을 대상 스키마로 사용하여 수동 작업을 줄입니다.
- 데이터 품질 - CDM 정의에 대해 검증 검사를 실행하여 프로덕션에서 데이터를 사용하기 전에 문제를 포착합니다.

데이터 엔터티 범주

CDM 데이터 엔터티는 다음 두 가지 범주로 나뉩니다.

- 비거래 데이터 - 제품, 사이트, 거래 파트너 및 지역과 같이 자주 변경되지 않는 참조 또는 마스터 데이터입니다.
- 트랜잭션 데이터 - 예측, 인벤토리 수준, 주문, 배송 등 자주 변경되는 운영 데이터입니다.

지원되는 데이터 엔터티

다음 표에는 CDM에서 지원되는 모든 데이터 엔터티가 나열되어 있습니다.

지원되는 CDM 데이터 엔터티

데이터 엔터티	데이터 유형	필수
Company	비트랜잭션 데이터	예
제품	비트랜잭션 데이터	예
거래 파트너	비트랜잭션 데이터	예
공급업체 제품	비트랜잭션 데이터	예
지역	비트랜잭션 데이터	예
제품 계층 구조	비트랜잭션 데이터	예
운송 경로	비트랜잭션 데이터	예
공급업체 리드 타임	비트랜잭션 데이터	예
사이트	비트랜잭션 데이터	예
공급업체 휴일	비트랜잭션 데이터	예
예측	트랜잭션 데이터	예
인벤토리	트랜잭션 데이터	예
인바운드 주문(PO/STO)	트랜잭션 데이터	예
아웃바운드 주문 라인	트랜잭션 데이터	예
Shipment	트랜잭션 데이터	예

데이터 엔터티	데이터 유형	필수
인벤토리 정책	트랜잭션 데이터	예
인바운드 주문 라인(PO/STO)	트랜잭션 데이터	예
아웃바운드 발송	트랜잭션 데이터	예
인바운드 주문 라인 일정	트랜잭션 데이터	예

기능에 필요한 개체

의 모든 기능에 모든 CDM 엔터티가 필요한 것은 아닙니다. 다음 섹션에서는 각 기능에 필수, 선택 또는 적용되지 않는 엔터티를 설명합니다.

인벤토리 가시성

인벤토리 가시성을 위한 CDM 엔터티

데이터 엔터티	데이터 유형	필수
Company	비트랜잭션	선택 사항
제품	비트랜잭션	예
거래 파트너	비트랜잭션	선택 사항
공급업체 제품	비트랜잭션	해당 사항 없음
Geography	비트랜잭션	선택 사항
제품 계층 구조	비트랜잭션	선택 사항
운송 경로	비트랜잭션	선택 사항
공급업체 리드 타임	비트랜잭션	해당 사항 없음
사이트	비트랜잭션	예
공급업체 휴일	비트랜잭션	해당 사항 없음

데이터 엔터티	데이터 유형	필수
예측	트랜잭션	선택 사항
인벤토리	트랜잭션	예
인바운드 주문(PO/STO)	트랜잭션	선택 사항
아웃바운드 주문 라인	트랜잭션	선택 사항
Shipment	트랜잭션	선택 사항
인벤토리 정책	트랜잭션	예
인바운드 주문 라인	트랜잭션	선택 사항
아웃바운드 발송	트랜잭션	선택 사항
인바운드 주문 라인 일정	트랜잭션	선택 사항

리드 타임 인사이트

리드 타임 인사이트를 위한 CDM 엔터티

데이터 엔터티	데이터 유형	필수
Company	비트랜잭션	선택 사항
제품	비트랜잭션	예
거래 파트너	비트랜잭션	예
공급업체 제품	비트랜잭션	예
Geography	비트랜잭션	선택 사항
제품 계층 구조	비트랜잭션	선택 사항
운송 경로	비트랜잭션	예
공급업체 리드 타임	비트랜잭션	예

데이터 엔터티	데이터 유형	필수
사이트	비트랜잭션	예
공급업체 휴일	비트랜잭션	선택 사항
예측	트랜잭션	해당 사항 없음
인벤토리	트랜잭션	해당 사항 없음
인바운드 주문(PO/STO)	트랜잭션	예
아웃바운드 주문 라인	트랜잭션	해당 사항 없음
Shipment	트랜잭션	예
인벤토리 정책	트랜잭션	해당 사항 없음
인바운드 주문 라인	트랜잭션	예
아웃바운드 발송	트랜잭션	해당 사항 없음
인바운드 주문 라인 일정	트랜잭션	예

수요 계획

수요 계획을 위한 CDM 엔터티

데이터 엔터티	데이터 유형	필수
Company	비트랜잭션	선택 사항
제품	비트랜잭션	예
거래 파트너	비트랜잭션	해당 사항 없음
공급업체 제품	비트랜잭션	해당 사항 없음
Geography	비트랜잭션	선택 사항
제품 계층 구조	비트랜잭션	선택 사항

데이터 엔터티	데이터 유형	필수
운송 경로	비트랜잭션	해당 사항 없음
공급업체 리드 타임	비트랜잭션	해당 사항 없음
사이트	비트랜잭션	예
공급업체 휴일	비트랜잭션	해당 사항 없음
예측	트랜잭션	해당 사항 없음
인벤토리	트랜잭션	해당 사항 없음
인바운드 주문(PO/STO)	트랜잭션	해당 사항 없음
아웃바운드 주문 라인	트랜잭션	예
Shipment	트랜잭션	해당 사항 없음
인벤토리 정책	트랜잭션	해당 사항 없음
인바운드 주문 라인	트랜잭션	해당 사항 없음
아웃바운드 발송	트랜잭션	해당 사항 없음
인바운드 주문 라인 일정	트랜잭션	해당 사항 없음

CDM과 데이터 온보딩의 관계

데이터를에 온보딩할 때 프로세스는 다음 단계를 따릅니다.

1. 업로드 - 소스 데이터를 Amazon S3에 CSV 파일로 업로드합니다.
2. 맵 - Data Agent는 소스 데이터 세트를 분석하고 데이터와 가장 일치하는 CDM 대상 테이블을 제안합니다.
3. 변환 - SQL 변환 쿼리는 소스 데이터 형식을 CDM 형식으로 변환합니다.
4. 검증 - 품질 검사는 변환된 데이터에 대해 실행되어 CDM 요구 사항을 준수하는지 확인합니다.
5. 활성화 - 검증되면 데이터가 로 들어오고 기능에 사용할 수 있게 됩니다.

데이터 온보딩에 대한 step-by-step 지침은 데이터 온보딩 주제를 참조하세요.

데이터 검증 및 품질 검사

개요

데이터 검증은 Amazon Connect Decisions 기능이 실행되기 전에 데이터가 품질 요구 사항을 충족하는지 확인합니다. 시스템은 구성된 계획, 지표 및 규칙을 기반으로 데이터를 검증하여 성능을 차단하거나 저하시킬 수 있는 문제를 식별합니다.

데이터 검증 작동 방식

검증 트리거

데이터 검증은 다음과 같은 시점에 자동으로 실행됩니다.

- Insights 구성 변경: 지표, 규칙 또는 기타 구성을 생성하거나 수정하는 경우
- 계획 생성: 임시 계획을 생성하거나 예약된 각 계획 실행 시
- 데이터 새로 고침: 대상 흐름에 대한 각 데이터 새로 고침 후
- 기능 실행: AI 팀원 운영 전 또는 도중(예: 예외를 근본적으로 유발하거나 권장 사항을 결정하는 경우)

검증 유형

Amazon Connect Decisions는 다음 두 가지 유형의 검증을 수행합니다.

데이터 존재 확인은 구성된 리소스(지표, 규칙, 계획)를 기반으로 필요한 데이터 세트와 필드가 로드되었는지 확인합니다.

데이터 품질 검증은 제공된 데이터가 다음을 포함한 설정 구성에 따라 품질 요구 사항을 충족하는지 확인합니다.

- 설정 기준 검증: 제품 및 사이트가 규칙 기준(예: 제품 범주, 사이트 위치)과 일치하는지 확인합니다.
- 계층 구조 검증: 설정에서 계층 구조를 사용하는 경우 누락된 계층적 관계를 식별합니다.
- 범위 검증: 식별된 제품 및 사이트에 필요한 모든 데이터가 존재하는지 확인합니다.
- 품질 평가: 운영 요구 사항에 대한 데이터 품질 및 사용성을 평가합니다.

점진적 검증

Amazon Connect Decisions를 사용하면 전체 데이터 세트의 기능을 차단하는 대신 유효한 데이터가 있는 제품 및 사이트에 대한 기능을 사용할 수 있습니다. 검증 문제가 특정 제품 또는 사이트에 영향을 미치는 경우 시스템은 유효한 데이터가 있는 제품 및 사이트를 계속 처리하고, 데이터 문제가 있는 제품 또는 사이트를 식별하고, 주의가 필요한 특정 항목을 알려줍니다. 이렇게 하면 나머지 데이터 문제를 해결하면서 기능 사용을 시작할 수 있습니다.

데이터 검증 오류 액세스

다음 세 가지 진입점을 통해 데이터 검증 오류를 볼 수 있습니다.

1. 홈 페이지의 "데이터 검증 오류" 지표
2. 홈 페이지의 데이터 검증 오류 주제 카드
3. 왼쪽 탐색 창의 "데이터 관리" > "오류" 탭

검증 오류 검토

오류 페이지에는 열려 있거나 해결된 모든 검증 오류가 표시됩니다. 다음 열 중 하나를 기준으로 검색하고 필터링할 수 있습니다.

- ID: 검증 오류의 고유 식별자
- 상태
  - 열기: 오류가 해결되지 않음
  - 해결됨: 오류가 수정되고 검증되었습니다.
- 설명: 데이터 품질 문제에 대한 설명
- 문제 유형
  - 필수 데이터 누락: 작업을 트리거하기 위한 필수 데이터가 제공되지 않음(예: 공급 계획에 대한 outbound_order_line 소스 테이블 없음)
  - 잘못된 데이터 값: 데이터가 존재하지만 잘못된 값을 포함합니다(예: 음수 제품 비용).
  - 관계 누락: 필수 계층적 또는 참조 관계가 누락됨(예: 제품 계층 구조 누락)
  - 데이터 부족: 필요한 작업을 수행하는 데 사용할 수 있는 데이터가 충분하지 않음(예: 수요 계획에 12개월의 과거 주문 데이터가 필요하지만 3개월만 있음)
- 기능: 영향을 받는 기능 또는 리소스
  - 공급 계획

  - 수요 계획
  - 인사이트(공급 또는 수요에 대한 예외, 권장 사항 및 RCA 포함)
- 대상: 영향을 받는 대상 흐름
- 우선 순위
  - 심각: 하나 이상의 기능이 완전히 차단되어 실행할 수 없음
  - 높음: 하나 이상의 기능이 부분적으로 차단됨(일부 제품 또는 사이트를 처리할 수 없음)
  - 중간: 하나 이상의 기능이 정확도가 떨어졌습니다(실행되지만 결과가 저하됨).
- 생성 시간: 오류가 처음 감지된 시간을 보여주는 타임스탬프

오류 세부 정보 보기

오류를 선택하면 자세한 정보를 볼 수 있습니다. 세부 정보 화면에는 위의 정보가 마지막 발생 날짜 타임스탬프, 관련 리소스 및 링크(문제의 영향을 받는 기능을 나타내는 지표, 규칙 또는 계획), 데이터 검증 오류가 어떻게 나타나는지 보여주는 최대 100개의 영향을 받는 데이터 행 미리 보기와 함께 표시됩니다.

사용 가능한 작업

오류 세부 정보 화면에서 다음을 수행할 수 있습니다.

- 문제 해결: AI 팀원을 시작하여 자연어로 문제 해결을 지원하고 자세한 문제 해결 지침을 받습니다.
- 오류 해결: 기본 문제를 해결한 경우 오류를 수동으로 해결됨으로 표시합니다.
- 다운로드: 자세한 분석 및 수정을 위해 영향을 받는 전체 데이터 세트를 다운로드합니다.

데이터 검증 오류 해결

해결 워크플로

1. 오류 설명 및 우선 순위를 검토하여 영향을 이해합니다.
2. 영향을 받는 데이터 미리 보기를 확인하여 영향을 받는 특정 레코드를 확인합니다.
3. 문제 해결을 위해 제공된 특정 권장 사항을 따릅니다.
4. 적절한 작업을 선택합니다.
   - 구성 문제의 경우: 관리자 및 플래너와 협력하여 지표, 규칙 또는 계획 구성을 조정합니다.
   - 매핑 문제의 경우: 업로드된 소스 데이터를 수정하거나 데이터 변환 및 매핑을 업데이트합니다.

- 누락되거나 유효하지 않은 데이터의 경우: 수정된 데이터 업로드

5. 기본 문제를 해결한 후 오류를 수동으로 해결됨으로 표시합니다.

AI Teammate 작업

문제 해결 옵션을 사용하여 "먼저 어떤 오류에 집중해야 합니까?"와 같은 질문을 합니다. 또는 "어떤 오류가 수요 계획을 차단하고 있나요?", 문제 및 그 영향에 대한 자세한 설명을 받고, 해결 접근 방식에 대한 step-by-step 지침을 받고, 오류가 특정 구성에 미치는 영향을 이해합니다. AI 팀원은 Amazon Connect 결정 및 소스 데이터 시스템 내에서 문제를 해결하기 위한 가이드 역할을 할 수 있습니다.

모범 사례

- 심각도별 우선순위 지정: 중요한 오류는 기능 실행을 완전히 차단하므로 먼저 중요 오류에 집중합니다. 그런 다음 처리를 부분적으로 차단하는 높은 우선 순위 오류와 정확도를 낮추는 중간 우선 순위 문제를 해결합니다.
- 권장 사항 주의 깊게 검토: 각 오류에는 구성에 따라 문제에 맞게 조정된 구체적이고 실행 가능한 지침이 포함되어 있습니다.
- 이점에 대한 점진적 검증 사용: 기능을 사용하기 전에 모든 오류를 해결할 때까지 기다리지 마세요. 시스템은 다른 사용자의 문제 해결을 위해 작업하는 동안 유효한 제품 및 사이트에 대한 기능을 활성화합니다.
- 데이터 새로 고침 후 모니터링: 각 데이터 업데이트 후 새 검증 오류를 확인하여 프로덕션 워크플로에 영향을 미치기 전에 문제를 조기에 포착합니다.
- 영향을 받는 데이터를 전략적으로 다운로드: 미리 보기 이후 영향을 받는 모든 레코드를 분석해야 하거나 데이터 팀에 전체 데이터 세트를 제공해야 하는 경우 다운로드 옵션을 사용합니다.
- 복잡한 문제에 AI 팀원 사용: 문제 해결 옵션은 특정 상황 및 구성에 맞는 상황별 지원을 제공합니다.
- 해결 방법 확인: 데이터 문제를 해결한 후 오류를 해결된 것으로 수동으로 표시하여 수정이 성공했는지 확인하고 열기 목록에서 제거합니다.

시스템 구성

Amazon Connect 결정의 설정은 범위 및 대상별로 구성됩니다. 일부 설정은 개인 설정이므로 각 사용자가 자신의 경험을 조정할 수 있습니다. 다른 구성은 관리자가 관리하는 인스턴스 수준 구성으로, 모든 사용자의 시스템 작동 방식 또는 광범위한 기술 환경에 연결하는 방식에 영향을 미칩니다.

사용자 수준 설정을 사용하면 개인이 계정 정보, 알림 기본 설정 및 데이터 액세스 범위가 뷰에 적용되는 방식을 관리할 수 있습니다.

인스턴스 수준 설정을 사용하면 관리자가 조직 전체에서 액세스 제어 필터 동작을 구성하고, ERP 및 기타 외부 시스템에 대한 연결을 설정하고, 시스템이 권장 작업을 처리하는 방법을 정의할 수 있습니다.

이러한 설정을 함께 사용하면 조직 전체의 일관성을 유지하면서 특정 운영 컨텍스트에 맞게 Amazon Connect 결정을 유연하게 조정할 수 있습니다.

사용자 프로필 설정

사용자는 애플리케이션의 오른쪽 상단 모서리에서 자신의 이름을 선택하고 드롭다운 메뉴에서 프로필을 선택하여 프로필 설정에 액세스할 수 있습니다. 프로필 페이지에서 사용자는 계정 정보, 알림 기본 설정 및 데이터 액세스 설정을 관리할 수 있습니다.

프로필 설정 액세스

프로필 설정에 액세스하려면:

1. 페이지 오른쪽 상단 모서리에서 이름을 선택합니다.
2. 드롭다운 메뉴에서 프로필을 선택합니다.
3. 프로필 페이지에 계정 정보 및 설정이 표시됩니다.

프로필 정보

프로필 페이지에는 다음 계정 세부 정보가 표시됩니다.

사용자: 사용자 이름

역할: 할당된 역할(관리자, 관리자 또는 플래너)

시간대: 드롭다운 메뉴에서 원하는 시간대를 선택합니다. 이 설정은 Amazon Connect 결정 전체에 날짜와 시간이 표시되는 방법을 결정합니다.

이메일: Amazon Connect Decisions 계정과 연결된 이메일 주소

생성됨: 계정이 생성된 날짜 및 시간

업데이트됨: 프로필이 마지막으로 수정된 날짜 및 시간

오른쪽 상단 모서리에서 저장을 선택하여 프로필 정보에 대한 변경 사항을 저장합니다.

알림 기본 설정

알림 기본 설정 탭을 사용하면 다양한 시스템 이벤트에 대한 알림을 수신하는 방법을 구성할 수 있습니다. 애플리케이션, 이메일 또는 둘 다에서 알림을 수신하도록 선택할 수 있습니다.

계획

계획 생성 성공: 계획 생성이 성공적으로 완료되면 알림을 받을 방법을 선택합니다. 옵션에는 인앱 알림 및 이메일 알림이 포함됩니다.

계획 생성 실패: 계획 생성 실패 시 알림을 받을 방법을 선택합니다. 옵션에는 인앱 알림 및 이메일 알림이 포함됩니다.

Insights 구성

인사이트 구성 성공: 인사이트 구성이 성공적으로 완료되면 알림을 받을 방법을 선택합니다. 옵션에는 인앱 알림이 포함됩니다.

인사이트 구성 실패: 인사이트 구성이 실패할 때 알림을 받을 방법을 선택합니다. 옵션에는 인앱 알림이 포함됩니다.

데이터 수집

데이터 수집 실패: 데이터 수집이 실패할 때 알림을 받을 방법을 선택합니다. 옵션에는 인앱 알림 및 이메일 알림이 포함됩니다.

관리자 설정

관리자는 모든 사용자에게 적용되는 시스템 전체의 알림 설정을 구성할 수 있습니다.

알림 보존: 시스템에서 알림이 자동으로 제거되는 일수를 설정합니다. 숫자 값을 입력하여 보존 기간을 지정합니다.

저장을 선택하여 알림 기본 설정을 적용합니다.

할당된 범위

할당된 범위 탭에는 데이터 액세스 권한이 표시되고 할당된 범위를 기반으로 데이터 뷰를 필터링하는 방법을 구성할 수 있습니다.

데이터 액세스

이 섹션에는 현재 데이터 액세스 수준이 표시됩니다. 모든 사이트 및 제품에 액세스할 수 있는 경우 "모든 사이트 및 제품에 액세스할 수 있습니다."라는 메시지가 표시됩니다.

기본 보기 필터

내 할당된 범위로 보기 필터링: 활성화된 경우 데이터 보기는 할당된 제품 및 사이트 내의 항목만 표시하도록 자동으로 필터링됩니다. 기본 설정에 따라이 설정을 켜거나 끕니다.

이 필터가 활성화되면 할당된 범위와 관련된 예외, 계획 및 기타 데이터만 표시됩니다. 비활성화하면 역할 권한에 따라 할당된 범위를 벗어나는 데이터가 표시될 수 있습니다.

저장을 선택하여 필터 기본 설정을 적용합니다.

액세스 제어 필터 토글

앞서 언급했듯이 모든 사용자는 적절한 제품 및 사이트가 구성되어 있는지 여부에 관계없이 모든 예외를 볼 수 있습니다(변경 작업에는 여전히 적절한 액세스가 필요함). 이렇게 하면 지식을 더 쉽게 공유할 수 있지만 특정 제품 및 사이트에만 집중하는 사용자는 다른 제품 및 사이트에 대한 예외 또는 권장 사항에 압도될 수 있습니다. 사용자가 자신에게 중요한 예외 및 권장 사항에 집중할 수 있도록 다음과 같이 액세스 보기 토글을 사용할 수 있습니다.

- 먼저 '관리자' 역할을 가진 사용자는 해당 인스턴스에서 기능을 활성화해야 합니다. 왼쪽 탐색 모음에서 인스턴스 설정 페이지로 이동합니다.
- 기본적으로 전체 인스턴스에 대한 기본 액세스 보기 필터를 설정하는 토글이 표시됩니다. '관리자'는 인스턴스의 모든 사용자에 대해 하나의 통합 설정을 사용하거나 사용자가 기본 설정을 결정하도록 할 수 있습니다.

- 통합 액세스 보기 토글 설정을 선택하는 경우 '관리자'는 모든 사용자에 대해 토글을 활성화할지 또는 비활성화할지 결정할 수도 있습니다.
- 각 사용자가 자신의 기본 설정을 선택하도록 선택한 경우 각 사용자는 액세스 보기 필터를 전환할 수 있습니다. 각 사용자는 화면 오른쪽 상단의 사용자 드롭다운에서 사용자 기본 설정 페이지로 이동할 수 있습니다.

인스턴스의 액세스 제어 토글을 변경합니다.

1. 설정 왼쪽 사이드 드로어를 선택합니다.
2. 애플리케이션 선택
3. 토글을 업데이트하고 저장 설정을 클릭합니다.

설정이 활성화된 경우 시스템은 액세스 제어 구성과 일치하는 제품 또는 사이트에 대해 생성된 항목만 표시하도록 예외 및 권장 사항 목록 페이지를 자동으로 필터링합니다.

"모든 제품 및 사이트에 대한 전체 액세스 권한 부여"가 활성화된 사용자의 경우 액세스 보기 토글에는 여전히 모든 예외 및 권장 사항이 표시됩니다. 사용자에게 토글이 비활성화되어 있지만 제품 또는 사이트가 구성되어 있지 않은 경우 시스템은 이를 제품 및 사이트에 액세스할 수 없는 것으로 해석하므로 사용자는 아무것도 볼 수 없습니다.

액세스 보기 필터는 다른 유형의 필터로 간주되므로 예외 및 권장 사항 페이지의 필터 칩에가 표시되지 않습니다. 사용자는 여전히 다른 제품 및 사이트 필터를 포함하여 이전과 동일한 방식으로 다른 필터를 적용할 수 있습니다.

사용자는 액세스 보기 토글을 끄거나 직접 하이퍼링크가 있는 경우 다른 제품 또는 사이트에 대한 예외 및 권장 사항에 계속 액세스할 수 있습니다.

ERP에 대한 연결 구성

Amazon Connect Decisions가 Enterprise Resource Planning(ERP) 시스템에서 사용자를 대신하여 작업을 수행하도록 하려면 필요한 연결 파라미터와 Amazon Connect Decisions가 작업 중에 사용해야 하는 자격 증명을 지정하는 연결을 구성해야 합니다.

지원되는 ERP 시스템:

- SAP S/4HANA

Secrets Manager에서 자격 증명 구성

1. 계정을 사용하여 Secrets Manager를 사용하여 Secrets Manager 보안 암호 생성
   - Secrets Manager에 자격 증명을 입력할 때 아래 자리 표시자 값(<username> 및 <password>)을 Amazon Connect Decisions에서 사용해야 하는 실제 사용자 이름과 암호로 바꿉니다.
   - 콘솔을 사용하는 경우에 Other type of secret 대해를 선택합니다. Secret Type
   - 콘솔의 Key/value pairs 탭을 통해 세부 정보를 입력하는 경우 2 페어를 입력합니다.
     - 키: username, 값: <*username*>
     - 키: password, 값: <*password*>
   - Plaintext 탭을 사용하여 콘솔에 보안 암호를 입력하는 경우 두 쌍이 있는 JSON 객체를 입력합니다.

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

2. AWS KMS 키로 보안 암호를 암호화하고 후속 단계에서 필요하므로 키의 ID를 기록해 둡니다.
3. 보안 암호가 생성되면 후속 단계에서 필요하므로 Amazon 리소스 이름(ARN)을 기록해 둡니다.
   - 예: arn:aws:secretsmanager:<Region>:<AccountId>:secret:<SecretName>-<SixRandomCharacters>

KMS 키에 대한 권한 구성

Amazon Connect Decisions가 액세스하고 사용하는 데 필요한 권한을 제공해야 합니다.

1. Amazon Connect Decisions가 인스턴스 역할을 통해 키에 액세스할 수 있도록 KMS 정책을 업데이트합니다.
   - 참고: <YourAccountNumber> 및를 AWS 계정 및 Amazon Connect 결정 인스턴스 ID<YourInstanceID>로 바꿉니다.

```
{
    "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. 키에 대한 권한을 부여하도록 인스턴스 역할에 대한 인라인 정책 업데이트

   - 참고: <YourSecretArn> <YourAccountNumber> 및를 보안 암호 ARN, AWS 계정 및 AWS 공급망 인스턴스 ID<YourInstanceID>로 바꿉니다.

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

보안 암호에 대한 Secrets Manager 리소스 정책 업데이트

1. 보안 암호에 대한 Secrets Manager 리소스 정책 업데이트
   - 참고:를 보안 암호의 ARN<YourSecretArn>으로 바꿉니다.

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

Amazon Connect 결정 연결 구성

1. Amazon Connect 결정 인스턴스에서 데이터 관리 페이지로 이동합니다.
2. Connections 탭을 선택합니다.
3. Create Connection 버튼을 클릭합니다.
4. Create Connector 페이지에서 SAP S/4HANA 커넥터 유형의 행에 있는 Select 버튼을 클릭합니다.
5. Configure SAP S/4HANA API Connector 페이지에 필요한 정보를 입력합니다.
   - Connection Name: 고유한 연결 이름
   - API Endpoint URL: SAP S/4HANA 인스턴스의 OData API 엔드포인트 URL(예: https://<hostname>:<port>)
   - Client Number: 3자리 SAP 클라이언트 번호(예: 100)
   - Secret ARN: Amazon Connect 결정에서 사용할 자격 증명이 저장되는 Secrets Manager의 보안 암호의 Amazon 리소스 이름(ARN)

6. Create Connector 버튼을 클릭합니다.

작업 설정 구성

Amazon Connect Decisions를 사용하면 Enterprise Resource Planning(ERP) 시스템에서 사용자를 대신하여 작업을 수행하기 위해 제공해야 하는 작업 유형을 제어할 수 있습니다. 기본적으로 모든 작업 유형은 비활성화되어 있으므로 원하는 각 작업 유형에 대해이 기능을 활성화해야 합니다.

> **Note**
>
> 지정된 작업 유형에 대한 지원을 활성화하면 사용자를 대신하여 작업을 수행하는 Amazon Connect 결정 옵션이 시스템 전체에서 표시되는지 여부가 제어됩니다(예: 지정된 유형의 권장 사항을 사용하여 Insight를 검토할 때). Amazon Connect Decisions는 사용자가 특정 권장 사항을 수락할 때까지 이러한 작업을 수행하지 않습니다(지원이 활성화된 경우에도).

지원되는 작업 유형:

- 구매 주문 생성
- 구매 주문 업데이트
- 구매 주문 취소

각 작업 유형에 대한 작업 지원을 구성합니다.

1. Amazon Connect 결정 인스턴스에서 데이터 관리 페이지로 이동합니다.
2. Actions 탭을 선택합니다.
3. 목록에서 구성하려는 작업 유형 찾기
4. 작업 유형에 대한 지원을 활성화하려면:
   - 해당 작업 유형에 대한 드롭다운 메뉴에 나열된 연결 중 하나를 선택합니다.
   - 참고: 드롭다운에는 Actions 기능을 지원하는 유형으로 구성된 사용 가능한 연결만 표시됩니다(예: SAP S/4HANA).
5. 작업 유형에 대한 지원을 비활성화하려면:
   - 드롭다운 메뉴에서 해당 작업 유형에 대해 No connection를 선택합니다.
6. 변경 사항을 저장Save하려면 클릭합니다.

보안

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS 와 사용자 간의 공동 책임입니다. 공동 책임 모델은 이를 클라우드의 보안과 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 는에서 AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다 AWS 클라우드. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사원은 정기적으로 AWS 규제 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다. Amazon Connect 결정에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 제공 범위 내 AWS 서비스를 참조하세요.
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 문서는 Amazon Connect를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목표에 맞게 Amazon Connect 결정을 구성하는 방법을 보여줍니다.

데이터 보호

AWS 공동 책임 모델은 Amazon Connect 결정의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든 AWS 클라우드를 실행하는 글로벌 인프라를 보호할 책임이 있습니다. 사용자는 이 인프라에 호스팅되는 콘텐츠에 대한 통제 권한을 유지할 책임이 있습니다. 또한 사용하는 AWS 서비스의 보안 구성 및 관리 작업에 대한 책임이 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 AWS 계정 자격 증명을 보호하고 AWS Identity and Access Management (IAM)를 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이러한 방식에서는 각 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2 이상을 권장합니다.

- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail.
- 서비스 내의 AWS 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용합니다.
- Amazon Simple Storage Service에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용합니다.
- 명령줄 인터페이스 또는 API를 AWS 통해에 액세스할 때 FIPS 140-2 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-2를 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 관리 콘솔, API, AWS Command Line Interface (AWS CLI) 또는 AWS SDKs를 AWS 사용하여 Amazon Connect 결정 또는 기타 AWS 서비스를 사용하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드를 입력하는 모든 데이터는 결제 또는 진단 로그에 사용될 수 있습니다.

데이터 암호화

이 주제에서는 전송 중 암호화 및 저장 중 암호화에 대한 Amazon Connect 결정 관련 정보를 제공합니다.

전송 중 암호화

고객과 Amazon Connect Decisions 간의 모든 통신과 Amazon Connect Decisions와 다운스트림 종속성 간의 모든 통신은 TLS 1.2 이상의 연결을 사용하여 보호됩니다.

저장 시 암호화

Amazon Connect Decisions는 DynamoDB 및 Amazon Simple Storage Service(Amazon S3)를 사용하여 저장 데이터를 저장합니다. 저장 데이터는 기본적으로 암호화 솔루션을 사용하여 AWS 암호화됩니다. Amazon Connect Decisions는 ()의 AWS AWS Key Management Service 소유 암호화 키를 사용하여 데이터를 암호화합니다AWS KMS. 데이터를 암호화하는 AWS 관리형 키를 보호하기 위해 어떤 조치도 취할 필요가 없습니다. 자세한 내용은AWS KMS 개발자 안내서에서 AWS 소유 키 섹션을 참조하세요.

AWS 콘솔에서 Amazon Connect Decisions 인스턴스의 데이터를 암호화하는 데 사용되는 KMS 키를 변경하는 경우 새 인스턴스를 생성하여 새 키를 사용하여 데이터를 암호화해야 합니다. 이전 키로 암호화된 모든 데이터는 유지되지 않으며 업데이트된 키로 데이터만 암호화됩니다. 이전 암호화 방법의 데이터를 유지하려면 해당 대화 중에 사용했던 키로 되돌릴 수 있습니다.

웹앱 및 채팅 애플리케이션에서 Amazon Connect Decisions와의 대화는 AWS 소유 키로만 암호화됩니다.

교차 리전 처리

Amazon Connect Decisions는 Amazon Bedrock으로 구동되며 교차 리전 추론(CRIS)을 사용하여 여러 AWS 리전에 트래픽을 분산하여 대규모 언어 모델(LLM) 추론 성능과 신뢰성을 개선합니다. 교차 리전 추론을 사용하면 다음을 얻을 수 있습니다.

- 수요가 많은 기간에 처리량 및 복원력 향상
- 성능 개선
- Amazon Bedrock에서 호스팅되는 가장 강력한 LLMs에 의존하는 새로 시작된 Amazon Connect Decisions 기능 및 기능에 대한 액세스

교차 리전 추론은 Amazon Connect Decisions 인스턴스가 생성된 AWS 리전에 따라 다르게 작동합니다.

미국 지리적 리전에서 생성된 모든 인스턴스에 대해 Amazon Connect Decisions는 글로벌 CRIS를 사용합니다. 즉, 추론 요청이 전 세계에서 지원되는 상용 AWS 리전으로 라우팅되어 사용 가능한 리소스를 최적화하고 모델 처리량을 높일 수 있습니다. Global CRIS에 대한 자세한 내용은 Amazon Bedrock 사용 설명서를 참조하세요.

EU 지리적 리전에서 생성된 모든 인스턴스에 대해 Amazon Connect Decisions는 지리적 CRIS를 사용합니다. 즉, 추론 요청은 데이터가 원래 상주하는 리전의 일부인 AWS 리전 내에 보관됩니다. 지리적 CRIS에 대한 자세한 내용은 Amazon Bedrock 사용 설명서를 참조하세요.

예를 들어 미국 동부(버지니아 북부)(us-east-1) 리전에서 생성된 Amazon Connect Decisions 인스턴스에서 이루어진 요청은 아시아 태평양(시드니)(ap-southeast-2)과 같은 전 세계 모든 AWS 리전으로 라우팅될 수 있습니다. 그러나 유럽(아일랜드)(eu-west-1) 리전에서 생성된 Amazon Connect Decisions 인스턴스에서 이루어진 요청의 경우 유럽(프랑크푸르트)(eu-central-1)과 같은 EU 내 AWS 리전으로 라우팅됩니다. 자세한 내용은 Amazon Connect 결정에 지원되는 리전을 참조하세요.

교차 리전 추론은 데이터가 저장되는 위치는 변경되지 않지만 요청 및 출력 결과는 데이터가 원래 상주하는 리전 외부로 이동할 수 있습니다. 모든 데이터는 암호화되어 Amazon의 보안 네트워크를 통해 전송됩니다. 교차 리전 추론을 사용하는 데 드는 추가 비용은 없습니다. Amazon Connect 결정 사용 시 데이터가 저장되는 위치에 대한 자세한 내용은 Amazon Connect 결정의 데이터 보호를 참조하세요.

Amazon Connect 결정을 위한 IAM

AWS Identity and Access Management(IAM)는 AWS 리소스에 대한 관리자의 액세스를 안전하게 제어하는 데 도움이 되는 AWS 서비스입니다. IAM 관리자는 Amazon Connect Decisions 리소스를 사용할 수 있는 인증(로그인) 및 권한(권한 있음)을 받을 수 있는 사용자를 제어합니다. IAM은 추가 비용 없이 사용할 수 있는 AWS 서비스입니다.

IAM이 Amazon Connect 결정과 작동하는 방법

IAM을 사용하여 Amazon Connect Decisions에 대한 액세스를 관리하기 전에 Amazon Connect Decisions에서 사용할 수 있는 IAM 기능을 알아봅니다. Amazon Connect 결정 및 기타 AWS 서비스에서 대부분의 IAM 기능을 사용하는 방법을 전체적으로 알아보려면 IAM 사용 설명서의 IAM으로 작업하는 AWS 서비스를 참조하세요.

Amazon Connect 결정에 대한 자격 증명 기반 정책

ID 기반 정책 지원: 예

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. JSON 정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

Amazon Connect 결정 내 리소스 기반 정책

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는 AWS 서비스가 포함될 수 있습니다.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM에서 교차 계정 리소스 액세스를 참조하세요.

Amazon Connect 결정에 대한 정책 작업

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하세요.

Amazon Connect Decisions의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
scn
```

단일 문에서 여러 작업을 지정하려면 쉼표로 구분합니다.

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

Amazon Connect Decisions에 대한 정책 리소스

정책 리소스 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

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

Amazon Connect 결정의 정책 조건 키

서비스별 정책 조건 키 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소는 정의된 기준에 따라 문이 실행되는 시기를 지정합니다. 같음(equals) 또는 미만(less than)과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

Amazon Connect Decisions에서 임시 자격 증명 사용

임시 자격 증명 지원: 예

임시 자격 증명은 AWS 리소스에 대한 단기 액세스를 제공하며 페더레이션 또는 전환 역할을 사용할 때 자동으로 생성됩니다. 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는 것이 AWS 좋습니다. 자세한 내용은 IAM 사용 설명서의 IAM의 임시 보안 자격 증명 및 IAM으로 작업하는 AWS 서비스를 참조하세요.

Amazon Connect Decisions에 대한 전달 액세스 세션

전달 액세스 세션(FAS) 지원: 예

전달 액세스 세션(FAS)은 서비스를 호출하는 AWS 보안 주체의 권한을 요청 AWS 서비스와 결합하여 다운스트림 서비스에 요청합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

Amazon Connect 결정의 서비스 역할

서비스 역할 지원: 예

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스에 권한을 위임할 역할 생성을 참조하세요.

> **Warning**
>
> 서비스 역할에 대한 권한을 변경하면 Amazon Connect 결정 기능이 중단될 수 있습니다. Amazon Connect Decisions가 관련 지침을 제공하는 경우에만 서비스 역할을 편집합니다.

ID 기반 정책 예시

기본적으로 사용자 및 역할에는 Amazon Connect Decisions 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS 관리 콘솔, AWS 명령줄 인터페이스(AWS CLI) 또는 AWS API를 사용하여 작업을 수행할 수 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

이러한 JSON 정책 예시 문서를 사용하여 IAM 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성 단원을 참조하세요.

인스턴스 관리 IAM 정책

다음은 콘솔 또는 퍼블릭 API를 통해 인스턴스를 생성, 업데이트 또는 삭제하는 데 필요한 IAM 정책입니다(모든 웹앱 작업 제외).

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

정책 모범 사례

자격 증명 기반 정책에 따라 계정에서 사용자가 Amazon Connect Decisions 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. 자격 증명 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. AWS 계정에서 사용할 수 있습니다. 사용 사례에 고유한 AWS 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책 또는 직무에 대한 AWS 관리형 정책을 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 IAM의 정책 및 권한을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정

책 조건을 작성할 수 있습니다. 와 같은 특정 서비스를 통해 사용되는 경우 조건을 사용하여 AWS 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 CloudFormation. 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.

- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer에서 정책 검증을 참조하세요.
- 다중 인증(MFA) 필요 – AWS 계정에 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우, 추가 보안을 위해 MFA를 설정합니다. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA를 통한 보안 API 액세스를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

IAM 문제 해결

다음 정보를 사용하여 Amazon Connect 결정 및 IAM 작업 시 발생할 수 있는 일반적인 문제를 진단하고 수정할 수 있습니다.

Amazon Connect 결정에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없는 AWS Management Console의 경우 관리자에게 문의하여 지원을 받아야 합니다. 관리자는 사용자 이름과 암호를 제공한 사람입니다.

다음의 예제 오류는 `mateojackson` IAM 사용자가 콘솔을 사용하여 가상 `my-example-widget` 리소스에 대한 세부 정보를 보려고 하지만 가상 `scn:GetWidget` 권한이 없을 때 발생합니다.

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

이 경우 Mateo는 `my-example-widget` 태스크를 사용하여 `scn:GetWidget` 리소스에 액세스하도록 허용하는 정책을 업데이트하라고 관리자에게 요청합니다.

iam:PassRole을 수행하도록 인증되지 않음

`iam:PassRole` 작업을 수행할 권한이 없다는 오류가 수신되면 Amazon Connect Decisions에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스를 사용하면 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 역할을 서비스에 전달할 권한이 있어야 합니다.

다음 예제 오류는 라는 IAM 사용자가 콘솔을 사용하여 Amazon Connect 결정에서 작업을 수행하려고 `marymajor` 할 때 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 권한이 없습니다.

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

이 경우, Mary가 `iam:PassRole`작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 AWS 계정 외부의 사람이 내 Amazon Connect Decisions 리소스에 액세스하도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우, 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세한 내용은 다음을 참조하세요.

- Amazon Connect 결정에서 이러한 기능을 지원하는지 여부를 알아보려면 Amazon Connect 결정에서 IAM을 사용하는 방법을 참조하세요.
- 소유한 AWS 계정 전체에서 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 소유한 다른 AWS 계정의 IAM 사용자에게 액세스 권한 제공을 참조하세요.
- 타사 AWS 계정에 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 소유 AWS 계정에 대한 액세스 권한 제공을 참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.

타사 하위 프로세서

Amazon Connect Decisions는 타사 API인 Boomi를 사용하여 외부 시스템에서 사용자를 대신하여 작업을 수행할 수 있습니다. 타사 시스템에 연결하는 Amazon Connect Decisions의 기능을 사용하면 Boomi를 통합 미들웨어로 사용하여 암호화된 데이터를 전송하고 처리할 수 있습니다. 데이터는 Boomi 내에 별도로 저장되지 않습니다.

Boomi 및 작동 방식에 대해 자세히 알아보려면 Boomi의 공개 설명서를 참조하세요.

지원되는 리전:

이 페이지에서는 Amazon Connect 결정을 사용할 수 있는 AWS 리전을 설명합니다. AWS 리전에 대한 자세한 내용은 AWS 계정 관리 참조 안내서의 계정에서 사용할 수 있는 AWS 리전 지정을 참조하세요.

Amazon Connect Decisions를 사용하는 리전과 다른 리전에서 데이터가 처리될 수 있습니다. Amazon Connect 결정의 리전 간 처리에 대한 자세한 내용은 리전 간 처리를 참조하세요. 처리 중에 데이터가 저장되는 위치에 대한 자세한 내용은 데이터 보호 섹션을 참조하세요.

지원되는 리전:

Amazon Connect Decisions는 다음 AWS 리전의 AWS Management Console, AWS Console Mobile Application, AWS website, AWS Documentation 웹 사이트에서 사용할 수 있습니다. 이러한 리전은 기본적으로 활성화되어 있으므로 사용하기 전에 활성화할 필요가 없습니다. 자세한 내용은 기본적으로 활성화된 리전 섹션을 참조하세요.

다음 리전에서 Amazon Connect 결정을 사용합니다.

AWS 리전 이름	코드 이름	지역(미국, EU 등)
미국 동부(버지니아 북부)	us-east-1	US
유럽(아일랜드)	eu-west-1	EU

문제 해결

Amazon Connect 결정의 설정 또는 day-to-day 사용 중에 문제가 발생하는 경우이 섹션에서는 가장 일반적인 문제를 진단하고 해결하는 데 도움이 되는 지침을 제공합니다. 먼저 현재 겪고 있는 문제와 가장 일치하는 범주를 식별한 다음 관련 페이지의 문제 해결 단계를 따릅니다. 어떤 범주가 적용되는지 잘 모르는 경우 가장 광범위한 초기 구성 문제를 다루는 일반적인 설정 문제로 시작합니다.

일반적인 설정 문제

참조 무결성 오류: “product_id 값이 제품 데이터 세트의 ID와 일치하지 않습니다.”

가장 일반적인 원인은 ID 필드의 후행 공백입니다. 고정 너비 데이터베이스에서 내보내는 소스 시스템은 문자열 필드를 공백으로 묶는 경우가 많습니다. 제품 마스터에는 클린 IDs("MAT604")가 있고 주문 라인 파일에는 패딩된 IDs("MAT604")가 있을 수 있습니다. 시스템은 엄격한 문자열 일치를 수행하므로 조인되지 않습니다.

수정: 데이터 흐름 SQL 변환의 모든 문자열 ID 필드에 TRIM()을 추가합니다. product_id, ship_from_site_id, customer_tpartner_id 및 기타 조인 키에 적용합니다. 또한 파일 간에 인용 불일치가 있는지 확인합니다. CSVs 다시 내보낼 때 QUOTE_ALL을 사용하여 숫자처럼 보이는 IDs(예: "111613")가 한 파일의 정수와 다른 파일의 문자열로 처리되는 유형 추론 문제를 방지합니다.

방지: 오늘 문제가 표시되지 않더라도 SQL 변환의 모든 ID 필드를 항상 기본 관행으로 잘라냅니다. 소스 데이터는 내보내기 간에 변경될 수 있습니다.

주문 내역의 제품이 제품 마스터에서 누락됨

주문 내역에는 현재 제품 마스터에 없는 제품(중단된 제품, 일회성 항목, 테스트 SKUs)이 포함되는 경우가 많습니다. product_id에 일치하는 제품 마스터 레코드가 없는 경우 시스템은 전체 주문 파일을 거부합니다.

수정 사항: (a) 최소 필수 필드(id, description, base_uom)가 있는 누락된 제품에 대해 제품 마스터에 스텁 행을 생성하거나 (b) 제품 마스터에 있는 제품만 포함하도록 주문 기록을 필터링합니다. 옵션 (a)는 계보 및 추세 감지에 유용할 수 있는 수요 기록을 보존하기 때문에 선호됩니다.

제품 마스터 업로드 시 CSV 구문 분석 오류

쉼표, 따옴표 또는 특수 문자가 포함된 제품 설명은 CSV 구문 분석을 중단시킬 수 있습니다. 특정 행에서 "예상 17개 필드, 19개로 표시됨"과 같은 오류가 표시될 수 있습니다.

수정: 적절한 따옴표(QUOTE_ALL)를 사용하여 파일을 다시 내보냅니다. 설명 필드에 포함된 쉼표가 있는지 실패한 특정 행을 확인합니다.

업로드 후 데이터가 표시되지 않음

- 파일 형식이 변경되지 않았는지 확인합니다(확장명, 열 헤더, 인코딩).
- 파일 이름과 확장명이 예상 패턴과 일치하는지 확인합니다. .csv를 .csv000 이상으로 변경하면 수집이 중단됩니다.
- 업로드 후 데이터 수집이 완료될 때까지 최대 30분이 소요됩니다.
- 로드 간에 열 헤더가 변경되는 경우(예: 월/년으로 이름이 지정된 열) 업로드 전에 사전 처리 단계가 필요합니다.

데이터 새로 고침 후 PIV가 업데이트되지 않음

- PIV는 수집이 완료된 후 약 15분 후에 트리거되며 실행하는 데 약 20~30분이 걸립니다.
- 데이터 업로드에서 새로운 PIV로의 End-to-end: 약 1~1.5시간.
- PIV가 24시간 이상 업데이트되지 않은 경우 지원팀에 문의하십시오.

예외 수가 너무 높거나 너무 낮은 것 같습니다.

- 너무 높음: 임계값이 너무 느슨하거나 단일 제품+사이트에서 여러 날짜에 대해 여러 예외가 발생할 수 있습니다. 지원팀에 문의하여 규칙 구성을 검토하세요.
- 너무 낮음: 임계값이 너무 제한적이거나 일부 제품에 필요한 데이터(예: 예측, 인벤토리 수준)가 누락되었을 수 있습니다.

잘 알고 있는 몇 가지 제품을 스팟 확인하고 시스템에 표시되는 내용과 소스 시스템을 비교합니다.

예외에 대한 재정적 영향 없음

재정적 영향을 받으려면 단위 비용을 제품 데이터에 채워야 합니다. 비용이 누락되거나 제품에 대해 0인 경우 달러 값이 표시되지 않습니다. 비용 데이터 적용 범위에 대해 지원 팀에 문의하세요. 일반적으로 여러 비용 필드의 폭포 접근 방식이 최상의 적용 범위를 제공합니다.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.