



管理员指南

Amazon Connect 的决定



Amazon Connect 的决定: 管理员指南

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

Amazon Connect 的决策是什么	1
优势	1
功能	1
入门	3
使用 Amazon Connect 决策的先决条件	3
Amazon Connect 决策支持的浏览器	3
Amazon Connect 决策支持的语言	4
设置 AWS 账户	4
注册获取 AWS 账户	4
创建具有管理访问权限的用户	5
配置 AWS Identity 中心集成	6
管理你的 Amazon Connections 实例	7
创建您的实例	7
选择应用程序管理员	11
访问您的实例	13
访问控制	15
访问控制在 Amazon Connect 决策中的运作方式	15
你将在本节中找到什么	15
角色和权限概述	16
管理用户权限角色	20
添加用户	20
更新用户权限	20
删除用户	21
设置属性级访问权限	21
用户分配	22
数据载入	23
1. 术语表	23
2. 用途	23
3. 数据载入有什么用?	23
过程	23
连接您的数据	24
先决条件	24
创建您的第一个源代码流	24
上传您的源数据	24

Source-to-CDM 目标映射	25
Column/Data 映射	26
查看并接受映射	26
监控您的流程	27
最佳实践	28
使用 JDBC 连接到您的数据库	28
什么是 JDBC 连接以及何时应该使用它？	28
先决条件	29
创建 Customer-Managed KMS 密钥	29
配置	31
将您的数据库连接到 CodeDeploy	33
最佳实践	36
了解规范数据模型 (CDM)	37
什么是清洁发展机制？	37
清洁发展机制为何重要	37
数据实体类别	38
支持的数据实体	38
功能所需的实体	39
清洁发展机制与数据载入有何关系	42
数据验证和质量检查	43
概述	43
数据验证的工作原理	43
访问数据验证错误	44
查看验证错误	44
查看错误详情	45
解决数据验证错误	45
最佳实践	46
系统配置	47
你将在本节中找到什么	47
用户配置文件设置	47
访问个人资料设置	47
个人资料信息	48
通知首选项	48
分配的作用域	49
访问控制过滤器切换	49
更改您的实例的访问控制开关：	50

配置与 ERP 的连接	50
在 Secrets Manager 中配置凭证	50
配置 KMS 密钥的权限	51
更新你的密钥的 Secrets Manager 资源政策	52
配置 Amazon Connections 连接	53
配置操作设置	53
安全性	55
数据保护	55
由 Amazon Connect 决策处理的数据	56
数据加密	56
Cross-region 处理	57
Amazon Connect 决策的 IAM	57
使用身份进行身份验证	58
使用策略管理访问	59
IAM 如何处理 Amazon Connect 决策	60
Identity-based 策略示例	62
IAM 故障排除	67
Third-party 子处理器	68
支持的区域：	68
支持的区域：	68
问题排查	70
你将在本节中找到什么	70
常见的安装问题	70
引用完整性错误：“product_id 值与产品数据集中的任何 ID 都不匹配”	70
基础产品中缺少订单历史记录中的商品	70
上传主产品时出现 CSV 解析错误	71
上传后数据未显示	71
数据刷新后 PIV 未更新	71
异常计数似乎太高或太低	71
例外情况未显示财务影响	72
.....	lxxiii

Amazon Connect 的决策是什么

Amazon Connections 是一款供应链规划和情报解决方案，由 AI 团队成员与您的团队合作，将需求信号协调成共识预测，生成具有约束感知能力的供应计划，并主动监控您的运营以预防问题、解决问题并确定持续改进的根本原因。

AI 队友会适应你的工作方式：由你的操作程序和规则驱动，与你的现有系统集成，并从你的从业者的决策中学习。它利用亚马逊供应链专业知识，从第一天起就提供有效的计划和建议。

你领导着一支由人工智能代理组成的团队，负责协调和执行行动，从而腾出时间专注于提高服务水平和营运资金效率的战略决策。

优势

适应您的业务

AI 团队成员可以适应您的业务、系统和决策，在现有工作流程中快速实现转型。在您的操作程序和业务规则的推动下，团队成员使用您现有的计划和 ERP 系统。他们从规划者的决策中学习，与你的优先事项保持一致，将知识制度化，这样你的运营就会随着时间的推移而变得更好，每个团队成员都更加有效。

在即将发生的事情中保持领先地位

领导一支由 AI 代理组成的团队来处理协调工作 24/7 ——协调需求信号、生成约束感知计划和执行批准的行动。队友还可以检测到手动分析看不见的模式，例如成千上万个 SKU 的级联供应商中断或库存失调，并在问题变成问题之前将其浮出水面。规划人员从被动消防转向主动规划，通过推动业务成果的战略决策提高运营效率并提高服务水平。

从第一天起就建立信任

人工智能队友得到了 30 多年来不断完善的科学支持，他们监督了 4 亿多个 Amazon SKU，并配备了专门的供应链工具。您的团队将受益于世界上最复杂的供应链网络之一磨练的领域专业知识，提供开箱即用的可操作见解和建议，并提供您可以信任和验证的清晰、可解释的理由。

功能

自适应智能

AI 队友通过一个连续的循环从每个计划和决策中学习：观察模式、检测重要因素、推荐行动以及执行批准的决策。这使知识制度化——当规划人员离开时，专业知识就会保留；新成员从第一天起就提高了工作效率，无需人工再培训即可改善结果。

需求情报

AI 团队成员动态编排 18 多种预测工具和基于亚马逊数据训练的基础模型，并在 SKU 级别自主优化。即使历史记录有限，也能从第一天起就生成准确的预测。通过共识计划协调统计预测、客户承诺和跨职能投入，同时持续监控准确性。

供应情报

AI 队友生成前瞻性供应计划（预览版），并智能地将异常聚类到按影响排序的战略决策中。运行优化模型，在整个网络中进行约束感知规划。监控运营 24/7，揭示重要内容，然后直接在现有系统中执行经批准的决策，从而将周期从数周缩短到数小时。

代理人入职

AI-powered 入职代理通过自然语言对话指导您完成设置。通过 JDBC 或 Amazon S3 连接碎片数据，为 Connect 决策做好准备，并在问题影响预测之前自动标记问题。通过实时预览以通俗易懂的语言配置业务规则和策略，在几周而不是几个月内即可投入运行。

入门

在本节中，您可以学习创建 Amazon Connections 实例、授予用户权限角色以及登录 Amazon Connections 网络应用程序。

使用 Amazon Connect 决策的先决条件

在创建 Amazon Connections 实例之前，请务必完成以下步骤：

- 您有一个 AWS 账户。要创建 AWS 账户，请参阅[设置 AWS 账户](#)。
- 确保已启用 IAM 身份中心。要启用 IAM 身份中心，请参阅[启用 IAM 身份中心](#)。
- 必须在您要创建 Amazon Connections 实例的同一区域激活 IAM 身份中心实例。仅美国东部（弗吉尼亚北部）和欧洲（爱尔兰）地区支持 Amazon Connect 决策。
- 如果 Amazon Connect Decisions 实例与您现有的 IAM 身份中心区域不在同一个区域，[请联系我们](#)寻求进一步帮助。
- 您必须在 IAM 身份中心实例中至少有一个用户才能分配为 Amazon Connect 决策管理员。您可以将您的活动目录连接到 IAM 身份中心。有关更多信息，请参阅[Connect 到 Microsoft AD 目录](#)。
- 将需要访问 Amazon Connect 决策的其他用户添加到 IAM 身份中心。
- 您需要 AWS 密钥管理服务 (AWS KMS) 来创建实例。Amazon Connections 使用此 AWS KMS 密钥来加密亚马逊连接决策中包含的所有数据。有关 AWS KMS 密钥的信息，请参阅[创建密钥](#)。
- 如果您打算启用操作功能，则需要配置与用于维护相关数据的系统的连接，并提供凭证以供 Amazon Connect Decisions 使用。如需进一步帮助，请[联系我们](#)。

Amazon Connect 决策支持的浏览器

在使用 Amazon Connect 决策之前，请使用下表验证您的浏览器是否受支持。

浏览器	受支持的版本
Google Chrome	最新的三个版本。
Mozilla Firefox ESR	这些版本在 Firefox 的 生命周期终止日期 之前一直受支持。有关详细信息，请参阅 Firefox ESR 发布日历 。

浏览器	受支持的版本
Mozilla Firefox	最新的三个版本。
Microsoft Edge 和 Edge Chromium	84 及更高版本。
Safari	适用于 macOS 的 Safari 10 或更高版本。

Amazon Connect 决策支持的语言

Amazon Connections 支持以下语言：

- 英语 (美国)

设置 AWS 账户

使用此部分创建 AWS 账户并创建 IAM 用户。有关创建 AWS 账户的最佳实践的信息，请参阅[建立最佳实践 AWS 环境](#)。

注册获取 AWS 账户

如果您没有 AWS 帐户，请完成以下步骤来创建一个帐户。

报名参加 AWS 账户

1. 打开 <https://portal.aws.amazon.com/billing/signup>。
2. 按照屏幕上的说明操作。

在注册时，将接到电话或收到短信，要求使用电话键盘输入一个验证码。

当你注册一个 AWS 账户时，会创建一个 AWS 账户 root 用户。根用户有权访问该账户中的所有 AWS 服务和资源。作为最佳安全实践，请为用户分配管理访问权限，并且只使用根用户来执行[需要根用户访问权限的任务](#)。

AWS 注册过程完成后会向您发送一封确认电子邮件。在任何时候，您都可以通过转至 <https://aws.amazon.com/> 并选择 My Account (我的账户) 来查看当前的账户活动并管理您的账户。

创建具有管理访问权限的用户

注册账户后，请保护您的 AWS 账户根用户，启用 AWS IAM Identity Center，并创建一个管理用户，这样您就可以不会使用根用户执行日常任务。

保护你的 AWS 账户根用户

1. 通过选择根用户并输入您的 AWS 账户电子邮件地址，以账户所有者身份登录 [AWS 管理控制台](#)。在下一页上，输入您的密码。

要获取使用根用户登录方面的帮助，请参阅《AWS Sign-In 用户指南》中的 [Signing in as the root user](#)。

2. 为您的根用户启用多重身份验证 (MFA)。

有关说明，请参阅 [IAM 用户指南中的为您的 AWS 账户根用户 \(控制台\) 启用虚拟 MFA 设备](#)。

创建具有管理访问权限的用户

1. 启用 IAM Identity Center。

有关说明，请参阅 [AWS IAM 身份中心用户指南中的启用 AWS IAM 身份中心](#)。

2. 在 IAM Identity Center 中，为用户授予管理访问权限。

有关使用 IAM 身份中心目录作为身份源的教程，请参阅 IAM Identity Center 用户指南中的 [使用默认 AWS IAM 身份中心目录配置用户访问权限](#)。

以具有管理访问权限的用户身份登录

- 要使用您的 IAM Identity Center 用户身份登录，请使用您在创建 IAM Identity Center 用户时发送到您的电子邮件地址的登录 URL。

有关使用 IAM Identity Center 用户 [登录的帮助](#)，请参阅 [AWS Sign-In 用户指南中的登录 AWS 访问门户](#)。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个权限集，该权限集遵循应用最低权限的最佳做法。

有关说明，请参阅 [AWS IAM Identity Center 用户指南中的创建权限集](#)。

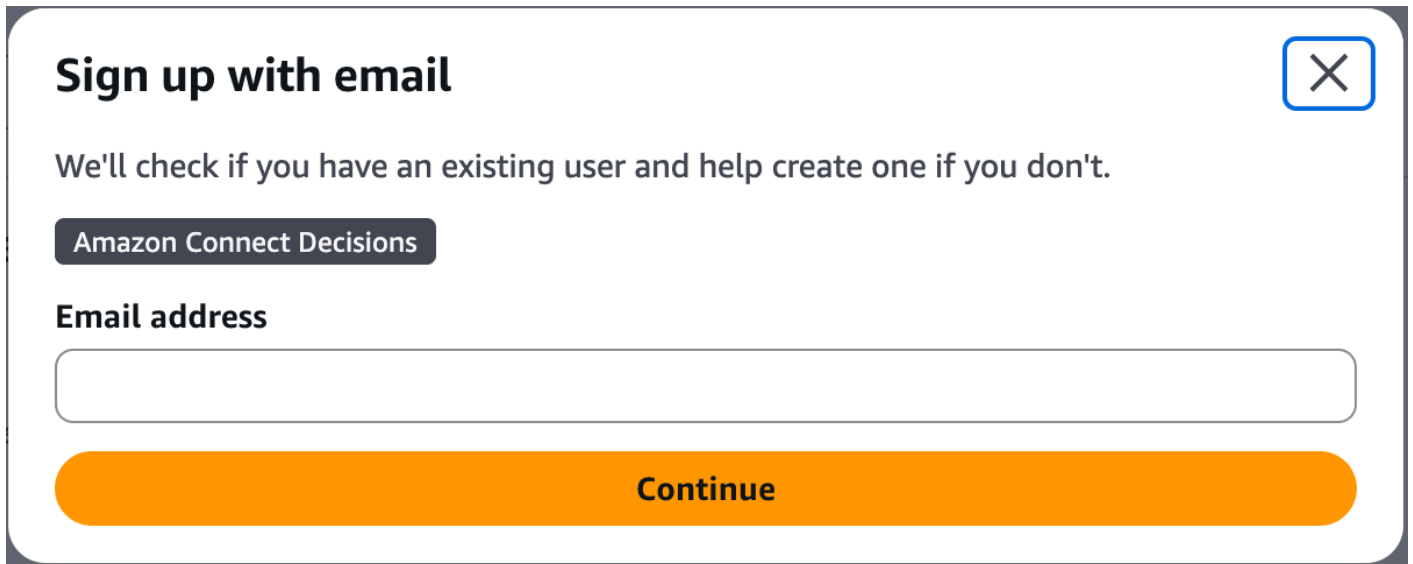
2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

有关说明，请参阅 AWS IAM 身份中心用户指南中的[添加群组](#)。

配置 AWS Identity 中心集成

要创建实例并使用 Amazon Connect Decisions 服务，您需要关联现有的 IAM Identity Center 用户资料或创建新的用户资料。

1. 打开 [Amazon Connections 控制台](#)。您也可以从主 AWS 管理控制台中搜索“Amazon Connect 决策”。
2. 如有必要，可通过选择控制台顶部的选择区域来更改 AWS 区域。从下拉列表中选择您所在的地区。
3. 选择创建 Amazon Connections 实例。将出现一条通知。



4. 输入您的电子邮件地址，然后选择“继续”。IdC 将验证电子邮件是否与现有用户匹配。
5. 请执行以下操作之一：
 - 如果 IdC 将电子邮件地址与用户匹配，请选择 Connect 您的身份来源并加入您的团队。

Note

如果您的组织已建立一个 IdC 实例，您想将其用于 Amazon Connect 决策，则可以使用该实例。

- 如果 IdC 找不到与现有用户的匹配项，则会出现“创建新用户”通知。继续执行下一步骤。

6. 在通知中，输入以下内容，然后选择继续：

- 电子邮件地址
- 名
- 姓

IdC 会自动创建用户并将其添加为 Amazon Connect 决策管理员。

7. 请执行以下操作之一：

- 要使用标准配置创建实例，请选择创建。请参见[使用标准配置](#)。
- 要使用自定义配置创建实例，请在高级设置中选择编辑。请参见[使用高级配置](#)。

与 IAM 身份中心配合使用时，Amazon Connect Decisions 会从 IAM 身份中心目录中检索“用户名”和“电子邮件”字段。这些属性都不是本地存储在您的 Amazon Connect Decisions 实例中，并且始终在运行时进行检索。默认情况下，Amazon Connections 使用 AWS 自有的 KMS 密钥对这些静态身份属性进行加密。Amazon Connect 决策不支持客户托管的 KMS 密钥。如果您删除 AWS IAM 身份中心实例中的用户，Amazon Connect Decisions 也会将该用户从您的实例中删除。

管理你的 Amazon Connections 实例

在中创建实例可 AWS Supply Chain 建立用于供应链管理和分析的专用环境。要设置实例，您需要配置基本详细信息、建立设置并定义初始用户访问权限。

只有 AWS 管理控制台管理员才能创建实例。创建 AWS Supply Chain 实例的 AWS 管理控制台管理员应拥有[Identity-based 策略示例](#)中列出的所有权限。该管理员应邀请 IAM 用户作为 AWS Supply Chain 管理员进行管理 AWS Supply Chain。

以下页面详细描述了创建和删除实例的过程。

创建您的实例

您可以使用以下两种方法之一创建实例：标准配置或高级配置。标准配置使用自动流程，使用预设参数快速创建实例。高级配置允许您通过设置自己的参数来自定义您的实例。

使用标准配置

标准配置使用默认的安全和加密设置创建您的 Amazon Connections 实例。实例在 AWS 地理区域运行。有关区域的更多信息，请参阅 IAM 用户指南中的[区域和终端节点](#)以及 AWS 一般参考中的[区域终端节点](#)。

要使用预设参数的标准配置创建 Amazon Connect Decisions 实例，请按照以下步骤操作。

1. 选择创建。



Create Amazon Connect Decisions instance

Create your Amazon Connect Decisions instance. We have selected some defaults to get you started.

Create

Create in advanced setup



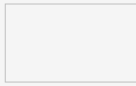
i Amazon Connect Decisions may securely transmit data from your selected Region but within your geography for processing.

Service access and encryption defaults

When you create an Amazon Connect Decisions instance, you grant it [permissions](#) to access some AWS resources on your behalf. Your data at rest will be encrypted using an AWS owned key. To modify these defaults choose **Create in advanced setup**.

2. 请查看您的电子邮件以了解以下内容：

- 来自 iDc 团队的电子邮件。
- 来自身份管理团队的电子邮件。



Hi Pranav Murlidhar,

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

What is AWS Supply Chain?

<https://aws.amazon.com/aws-supply-chain/>

Accessing the AWS Supply Chain

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

Your AWS Supply Chain Application URL:

<https://99wy6mj6.scn.global.on.aws>

Bookmark this URL for easy access in the future.

Your Username:

pmurlidh@amazon.com

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

3. 收到邀请电子邮件后，登录 Amazon Connections。请参阅[登录 Amazon Connections 网络应用程序](#)。

使用高级配置

高级配置允许您通过设置自己的参数来自定义您的实例。要使用预设参数的高级配置创建 Amazon Connect Decisions 实例，请按照以下步骤操作。

1. 在高级设置中选择“创建”。
2. 将会出现“实例属性”页面。

Specify instance details

Instance properties info

AWS Region

US East (N. Virginia) us-east-1

The AWS instance will be created in the region displayed above. To change the AWS region, cancel the create instance setup, select the new region from the Select a Region drop-down on the top-right panel, and restart creating the instance.

Enter an instance name

1 to 62 characters including spaces, underscores, and dashes.

Enter a description - optional

256 characters max.

Instance tags - optional info

A tag is a label that you assign to an AWS resource (such as an instance). Each tag consists of a key and an optional value. You can use tags to identify your instance, for example development, testing, or production.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 tags.

Amazon Connect Decisions may securely transmit data from your selected Region but within your geography for processing.

[Cancel](#) [Create instance](#)

3. 在实例属性页面上输入以下内容：

- 名称-输入实例名称。
- 描述 — 输入对您的 Amazon Connect Decisions 实例（例如，生产实例、测试实例等）的描述。
- 实例标签-您可以向您的实例添加可用于识别的标签。例如，您可以添加一个标签来定义要创建的实例的类型（例如，生产、测试、UAT 等）。

4. 选择创建实例。

删除实例

要删除实例，请按照以下步骤操作。

Note

当您删除实例时，Amazon S3 桶中的信息不会自动删除。

1. 打开 Amazon Connections 控制台，网址为 <https://console.aws.amazon.com/scn/home>。
2. 在 Amazon Connections 控制台控制台上，从下拉列表中选择要删除的实例。

Amazon Connect Decisions

i Amazon Connect Decisions may securely transmit data from your selected Region but within your geography for processing.

Select instance

99wy6mj6

Create instance

Instance details [Info](#)

Delete

Edit

Instance Name

99wy6mj6

Created on: 4/12/2026

Status

Active

Sub-domain

99wy6mj6.scn.global.on.aws

Description

-

AWS KMS Key

AWS owned KMS key

Instance ID

64caf25d-2ece-48f6-8456-37eccee606a6

3. 选择删除。
4. 在“删除 Amazon Connections 实例”页面的“确认”下，键入确认delete要删除该实例。
5. 选择删除。实例删除开始，删除实例后，您将看到一条确认消息。

选择应用程序管理员

作为 AWS 控制台管理员，您可以选择 Amazon Connections 应用程序管理员来管理 Amazon Connections 网络应用程序的访问权限。Amazon Connections 应用程序管理员可以在 Amazon Connections 网络应用程序中添加或删除用户权限角色。

创建实例并连接身份源后，请按照以下步骤选择 Amazon Connections 应用程序管理员。

1. 打开 Amazon Connections 控制台控制台控制面板。
2. 前往“选择应用程序管理员”，然后选择一个用户成为 Amazon Connections 应用程序管理员。搜索结果仅显示符合搜索条件的用户。

Amazon Connect Decisions

Amazon Connect Decisions may securely transmit data from your selected Region but within your geography for processing.

Select instance: 99wy6mj6 Create instance

Instance details [Info](#) Delete Edit

Instance Name 99wy6mj6 <small>Created on: 4/12/2026</small>	Status Active	Sub-domain 99wy6mj6.scn.global.on.aws L
Description -	AWS KMS Key AWS owned KMS key	Instance ID 64caf25d-2ece-48f6-8456-37eccee606a6

User access management [Info](#) Disconnect Identity Center Manage users [L](#)

Amazon Connect Decisions connects to AWS IAM Identity Center, where you can create and manage user identities or easily connect to a variety of third party identity sources. We'll check to see if your organization has a current identity source setup, or give the option to create a new one in IAM Identity Center

Status
Identity source connected

Application admin [Info](#) Add application admins Remove Manage in Amazon Connect Decisions [L](#)

Additional application admins can be managed within the Amazon Connect Decisions application.

Search:

User name	Email
<input type="checkbox"/> pmurlidh@amazon.com	pmurlidh@amazon.com

Instance tags [Info](#) Manage tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value
aws:scn:created-for-instance	64caf25d-2ece-48f6-8456-37eccee606a6

3. (可选) 选择“前往 IAM 身份中心”以添加更多用户。有关添加用户的更多信息，请参阅 AWS IAM Identity Center 用户指南中的[管理您的身份源](#)；有关用户权限角色的更多信息，请参阅[用户权限角色](#)。

Note

在 Amazon Connect 决策控制台中，您一次只能添加一个用户。您不能在 Amazon Connect 决策中将群组添加为应用程序管理员。

4. 选择“发送邀请”。将向 Web 应用程序管理员发送一封电子邮件。Web 应用程序管理员收到邀请电子邮件后，就可以选择应用程序 URL 并登录 Amazon Connections。



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 Connections 网络应用程序中，您将看到该用户列在应用程序管理员下。

访问您的实例

使用控制台是管理服务资源和配置的最简单方法。该控制台提供了一个直观的基于 Web 的界面，您可以在其中查看、创建、修改和监控您的资源。

要访问 Amazon Connect Decisions 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您 AWS 账户中的 Amazon Connections 资源的详细信息。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

作为 Amazon Connections 管理员，您应该已经收到一封电子邮件邀请，使用 Amazon Connections 网络应用程序。

1. 您可以选择电子邮件中的链接，也可以在 Amazon Connect Decisions 控制台控制台控制面板下 Sub-domain 选择网址。
2. 出现 Amazon Connections 网络应用程序登录页面。
3. 输入 AWS IAM 身份中心用户证书，然后选择登录。
4. 您添加的每位用户都会收到一封电子邮件，其中包含指向 Amazon Connect Decisions 的链接，或者您可以选择复制链接并将链接发送给用户。

成功登录后，您将进入您的个性化主页。要更好地了解您的主页，请参阅用户指南中的了解您的主页。

访问控制

Amazon Connections 提供企业级访问管理，让您可以精确控制谁可以访问哪些数据以及在您的实例中执行哪些操作。这样可以确保您的用户只能看到与其职责相关的信息，同时保持组织所需的安全性和合规性标准。

访问控制在 Amazon Connect 决策中的运作方式

Amazon Connections 结合了两种互补的访问管理方法：

Role-Based 访问控制 (RBAC) 根据用户的工作职能定义了他们可以做什么。Amazon Connections 包括三个预先配置的角色（管理员、经理和规划师），每个角色都有特定的功能权限。这些角色决定了用户可以访问哪些页面以及他们可以执行哪些操作。

Attribute-Based 访问控制 (ABAC) 通过根据业务环境限制访问，增加了额外的精确度。使用产品和网站属性，您可以确保规划人员只能看到他们管理的特定产品和地点的详细信息，而经理则可以查看其团队的职责范围。

这些功能共同允许您配置反映组织结构的访问权限，无论您是按地理位置、产品类别、地点还是按属性组合进行组织。

你将在本节中找到什么

以下页面将引导您完成：

- **角色和权限概述**：了解管理员、经理和规划师角色，以及 RBAC 和 ABAC 如何在 Amazon Connect 决策中协同工作
- **管理用户权限角色**：将用户添加到您的 Amazon Connections 实例并分配决定其访问级别的角色
- **设置 Attribute-Level 访问权限**：配置数据访问权限以根据产品和站点属性限定每个用户可以查看和修改的数据
- **用户分配**：通过为用户分配特定的计划职责，在整个团队中分配工作

在您配置访问控制时，Amazon Connect Decisions 可确保用户仅获得执行工作所需的权限，遵循最低权限访问原则，同时保持足够简单，供供应链专业人员独立管理。

角色和权限概述

作为 Amazon Connect 决策管理员，您可以使用默认的用户权限角色或创建自定义权限角色。Amazon Connections 具有以下默认用户权限角色：

- 管理员 — 创建、查看和管理所有数据和用户权限的权限。

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 i			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Configuration i	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Plans

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



Access	All	Create	Read	Update	Delete
Plans i	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Management

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



Access	All	Create	Read	Update	Delete
Data i	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Access Control i		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
User Access i	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- 经理-创建、查看和管理以下内容的权限。

Manager

Role name

Manager

Description

Users managing inventory or demand planning teams within the organization

Permissions details

Insights

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



Access	All	Create	Read	Update	Delete
Insights i			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Configuration i	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Plans

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



Access	All	Create	Read	Update	Delete
Plans i	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Management

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



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

- 规划器-创建、查看和管理以下内容的权限。

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 i			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
----------------------------	--	--	-------------------------------------	-------------------------------------	--

Configuration i		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
---------------------------------	--	-------------------------------------	-------------------------------------	-------------------------------------	--

Plans

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



Access	All	Create	Read	Update	Delete
--------	-----	--------	------	--------	--------

Plans i		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
-------------------------	--	-------------------------------------	-------------------------------------	-------------------------------------	--

Management

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



Access	All	Create	Read	Update	Delete
--------	-----	--------	------	--------	--------

Data i					
------------------------	--	--	--	--	--

Access Control i					
----------------------------------	--	--	--	--	--

User Access i					
-------------------------------	--	--	--	--	--

Note

作为 Amazon Connect 决策管理员，在添加用户之前，请注意以下几点：

- 每个默认用户权限角色都定义了一组权限。您可以将用户添加到默认用户权限角色或创建自定义权限角色。
- 一个用户只能分配一个用户权限角色。
- 您无法编辑或删除默认用户权限角色。
- 编辑您创建的自定义权限角色时，该自定义权限角色下所有用户的权限都会更新。
- 当您删除您创建的自定义权限角色时，该自定义权限角色下的所有用户都将失去对 Amazon Connections 的访问权限。
- Amazon Connect 决策不支持添加群组。

管理用户权限角色

添加用户

作为 Amazon Connections 管理员，您可以添加用户以访问 Amazon Connections 网络应用程序。必须先将用户添加到 IAM 身份中心 (IdC)，然后才能将其添加到 Amazon Connections 中。有关向 IdC 添加用户的更多信息，请参阅[分配用户访问权限](#)。

将用户添加到 IdC 后，请按照以下步骤添加用户。

1. 选择“设置”左侧抽屉
2. 选择“用户”。选择“分配用户”
3. 搜索以识别用户。您可以使用“显示姓名”、“电子邮件”、“名字”、“姓氏”、“用户名”进行搜索
4. 选择要添加的用户。
5. 为他们分配一个角色。查看角色和权限概览，详细了解 Amazon Connections 中的用户角色。
6. 选择分配。确认您的选择准确无误。

更新用户权限

要更新当前 Amazon Connect Decisions 用户的用户权限角色，请按照以下步骤操作。

1. 选择“设置”左侧抽屉

2. 选择“用户”。选择“分配用户”
3. 在用户列表中，选择用户以打开用户详细信息页面。
4. 使用角色下拉列表更新用户的角色权限。
5. 单击“更改角色”按钮，确认您要更改角色

删除用户

作为 Amazon Connections 管理员，您可以从 Amazon Connections 网络应用程序中删除用户。请按照以下步骤删除删除用户。

1. 选择“设置”左侧抽屉
2. 选择“用户”。选择“分配用户”
3. 在用户列表中，选择用户以打开用户详细信息页面。
4. 选择删除
5. 单击“删除”按钮，确认要删除该用户

设置属性级访问权限

Attribute-Based 访问控制 (ABAC) 通过根据业务环境限制访问，增加了额外的精确度。使用产品和网站属性，您可以确保规划人员只能看到他们管理的特定产品和地点的详细信息，而经理则可以查看其团队的职责范围。

任何具有“管理员”角色的用户都可以按产品和站点为其他用户配置访问权限：

1. 从左侧导航栏导航到“用户”页面。
2. 从该实例的用户列表中，选择需要配置的用户。
3. 默认情况下，在“数据访问权限”部分，用户将启用“授予对所有产品和网站的完全访问权限”。开启此开关后，它将提供对所有产品和网站的访问权限（在此发布之前的工作原理）。
4. 关闭“授予对所有产品和网站的完全访问权限”，产品和站点配置部分将变为可见。首次访问时不会分配任何产品或站点。
5. 根据需要配置的内容，单击产品或站点的 Add/Remove 按钮。使用搜索来查找和选择该用户所需的物品。
6. 可以为多个用户分配相同的产品或站点。一个用户最多可以拥有 1,000 个产品-站点组合。
7. 可以使用相同的界面删除以前配置的产品或站点。

8. 在向导的最后一页中查看并确认添加和删除的完整列表，以完成访问配置。

配置产品和站点访问权限后，将根据以下分配限制该用户的访问权限：

- 所有用户都可以查看任何例外或推荐页面，无论该页面是针对其访问控制中包含的产品还是网站生成的。
- 要执行变异操作（例如取消异常或将状态从“进行中”更改为“完成”），用户必须在访问控制中配置相应的产品或站点。
- 配置了访问控制的用户也可以使用“用户分配”和“访问视图切换”。

用户分配

用户分配是一项功能，可以更轻松地在多个用户之间平衡见解。使用用户分配，客户可以向用户分配特定的见解，以更好地反映这些任务在现实生活中是如何共享的。其工作原理如下：

- 每当创建异常时，系统都会根据为其访问控制配置了相同产品或站点的所有用户检查为其创建例外的产品和站点
- 如果系统找到匹配的用户，则会使用该用户名更新该异常的“分配给”字段。如果多个用户拥有与例外情况相匹配的产品或网站，则会将其随机分配给其中一个用户
- 每个例外只能分配一个用户，但如果需要，可以将异常重新分配给另一个用户。只能将其重新分配给具有产品或网站访问权限的用户
- Auto-assignment 因为见解是在首次创建异常时发生的。先前创建的见解不会自动重新分配。此外，如果删除用户或更新其访问控制，则用户分配不会自动更新
- 在见解列表页面中，用户可以按分配给维度进行筛选，以轻松识别分配给他们的所有见解。他们还可以使用相同的过滤器来查看未分配的见解。用户分配目前仅适用于见解

数据载入

1. 术语表

- 数据代理 — 帮助自动执行数据集成任务的 AI-powered 助手
- 源流 — 将数据从源系统导入的流程
- 数据集-源数据的结构化表示形式
- S3 存储桶 — 包含您的源数据文件的 Amazon S3 存储位置
- 目标 (转换) 流程 — 将源数据格式转换为 AWS 规范数据模型 (CDM) 格式的过程
- CDM — 规范数据模型，使用的标准化数据结构
- 数据映射-将源数据中的字段与 CDM 结构进行匹配的过程

2. 用途

本指南提供了有关如何将供应链数据导入使用数据代理的分步说明，该 AI-powered 助手可帮助自动执行数据载入任务和解决问题。

3. 数据载入有什么用？

数据载入是将您现有的供应链数据整合到中的过程。为了将您的数据用于规划和预测，它必须采用规范数据模型 (CDM) 的标准化数据结构中的结构化格式。Data onboarding 通过将您的字段映射到 CDM 实体、转换数据类型和格式以及验证数据质量，将您的源数据转换为这种格式。这样可以确保根据您的源数据生成准确的预测和建议。

过程

数据载入分为五个阶段：

1. 准备：从您的系统中收集源数据（请参阅[the section called “先决条件”](#)）
2. 上传：将您的供应链数据上传为 CSV 文件
3. 映射：将源数据集与清洁发展机制目标数据集以及源字段与清洁发展机制实体进行匹配（例如，将您的“商品编号”字段映射到清洁发展机制的“product_id”）
4. 验证：运行质量检查并解决所有数据问题

在整个过程中，的 Data Agent 充当您的 AI-powered 助手数据载入助手。它将保留在屏幕的左侧，您可以使用自然语言与之交互，以帮助自动执行数据加载任务，包括：

- 发现架构：自动扫描您上传的数据以识别结构和关系
- 生成源到目标映射：分析您的源数据并建议哪些 CDM 目标表与您的数据最匹配
- 创建 SQL 转换查询：自动生成 SQL 以将源字段映射到 CDM 目标字段
- 提供映射原理：解释为什么根据重叠数据建议特定的映射
- 问题疑难解答：确定映射或数据加载失败的原因，并推荐具体的修复方法
- 回答问题：解释概念，澄清映射，并在整个过程中提供指导

连接您的数据

先决条件

在开始数据加载之前，请确保您已经：

- Amazon Connect 决策实例
 - 您的实例应该已经使用关联的 S3 存储桶创建
- 数据准备就绪
 - 与您的客户成功部门合作，根据您的计划如何使用 Amazon Connections 决策来确定您需要哪些数据。基本数据要求包括：
 - Sales/Order 历史记录：12 个月以上的交易记录
 - 产品详情：包含规格的完整产品目录
 - Site/Location 信息：仓库、配送中心、零售地点
 - 当前库存量：每个地点的 On-hand 库存
 - 所有源数据均采用 CSV 格式并带有 UTF-8 编码

创建您的第一个源代码流

要开始载入数据，请导航至 Amazon Connections 中的“数据管理”选项卡。在这里，您可以看到所有现有的源流。如果您尚未设置，请选择“创建新源”开始。

上传您的源数据

根据您的用例所需的 CDM 表，上传包含源数据的 CSV 文件。您可以选择处理数据更新的方式：

- 附加：向现有数据添加新数据
- 替换：用新数据替换现有数据

当您上传文件时，Amazon Connect Decisions 会自动在 S3 中为该数据创建文件夹结构，包括：

- 以所选源系统命名的父文件夹
- 以所选源表名命名的子文件夹
- 子文件夹下的所有文件都保存在同一个源表中
- 此文件结构还用于创建 Amazon S3 文件夹路径

Source-to-CDM 目标映射

文件上传后，Amazon Connections 将开始分析您的数据，并将其自动映射到一个或多个 Amazon Connections 的 CDM 目标表。

会发生什么

- 此步骤可能需要 10-15 分钟，具体取决于上传的数据量
- 数据代理在后台工作，为您的源数据识别最佳 CDM 目标数据集。
- 离开此页面将导致自动映射失败。在等待期间，请保持 Amazon Connect 决策和数据管理选项卡处于打开状态，以确保自动映射完成。

完成后，数据代理会根据重叠的数据提供源到目标映射的基本原理，您可以查看这些基本原理，并就任何映射结果向代理提问。

要查看和编辑源映射，您可以：

- 使用自然语言直接与数据代理交互以更新源-目标映射。
- 选择“操作”选项，然后选择“编辑来源”。

编辑映射

从这里，你可以：

- 如果需要，可以手动更新源映射和目标映射

- 使用屏幕右侧的数据代理提问以确认映射
- 参考[用户指南](#)以了解有关特定数据集的更多信息

Column/Data 映射

源到目标映射完成后，Amazon Connect Decisions 将自动创建从您的源数据集到 CDM 目标的 SQL 转换查询。完成任何映射后，您将收到来自数据代理的通知，详细说明映射的结果：

在这里，您应该通过从“操作”菜单中选择“查看 SQL”来查看为映射生成的 SQL。

查看映射 (SQL)，您将看到：

- 您已添加的源数据集列
- 目标 CDM 表列供参考
- 连接它们的转换 SQL
- 数据代理提供的映射理由

编辑映射

您可以通过两个选项来编辑任何映射：

- 使用 Data Agent：使用自然语言提问、管理和更新映射
- 直接编辑 SQL：如果您熟悉 SQL，则可以直接修改查询

测试您的更改

编辑映射查询时，请继续使用“测试查询”功能对其进行测试，这将为您的预览提供可滚动的预览，了解如何将您的数据转换为目标 CDM 的示例。使用它来确保您的转换正常运行，并验证从源到目标 CDM 的所有适当更新。

对映射输出感到满意后，选择“保存查询”以保存该源-目标对的转换查询。

查看并接受映射

查看每个源数据集的其余映射。对于问题或疑难解答帮助，Data Agent 会一直显示在屏幕的右侧。

对所有映射都感到满意后，请接受它们以完成数据载入。

处理失败的映射

如果有任何映射失败，则可以选择“重新启动映射”以重新启动所有映射，或者通过“重试 SQL 生成”从“操作”菜单中手动重试单个映射。数据代理还可以使用自然语言重试映射，如果错误持续存在，它将继续帮助您识别和解决问题。

监控您的流程

“目标”选项卡

接受映射后，您将被导航到数据管理中的目标选项卡，您可以：

- 查看目标流程
- 管理和编辑映射 (“管理流程”)
- 删除过时的流程
- 查看这些流程的执行状态

选择“管理流程”将带您回到数据映射体验，在此体验中，您可以继续使用数据代理来随着时间的推移完善映射。

“来源”选项卡

返回到“来源”选项卡，您可以找到：

- 已创建的源数据集
- 与其关联的 S3 存储桶
- 以下选项：
 - 通过另一个文件上传来追加更多源数据
 - 管理流程
 - 删除流程
 - 查看执行情况

选择“管理流程”将带您回到数据映射体验，在此体验中，您可以继续使用数据代理来随着时间的推移完善映射。

您还可以根据需要访问“创建新源”，以重新启动任何新数据源的数据加载流程。

最佳实践

数据准备

- 按照“先决条件”部分中的步骤操作
- 对所有 CSV 文件使用 UTF-8 编码
- 确保文件名是唯一的
- 上传前验证数据质量

使用数据代理

- 请具体说明您的要求
- 当你不明白它的任何决定时，可以要求解释
- 在接受之前测试所有 SQL 更改
- 使用预览功能验证变换

持续维护

- 保持源数据更新
- 定期监控流程执行情况
- 收到通知后立即解决数据错误
- 为您的团队记录自定义转换

使用 JDBC 连接到您的数据库

本指南将引导您 CodeDeploy 使用 Java 数据库连接 (JDBC) 将数据库连接到。您将为数据库凭据设置安全加密，并建立安全连接以直接从现有数据库读取数据。

什么是 JDBC 连接以及何时应该使用它？

JDBC 连接允许直接 CodeDeploy 连接到现有数据库以读取数据，而不必要求您导出和上传 CSV 文件或设置自己的提取、转换和加载 (ETL) 管道。

在以下情况下使用 JDBC 连接：

- 您的数据已存储在 AWS Glue兼容的关系数据库中。有关兼容的数据库和版本，请参阅[本指南](#)。
- 您希望无需手动导出文件即可进行实时或近实时的数据访问
- 您的数据量很大，并且经常更新
- 您更愿意将数据保存在当前位置而不是复制

如果您使用的是较小的数据集或更喜欢基于文件的上传，那么标准的 CSV 上传过程可能会更简单地满足您的需求。有关此过程的更多详细信息，请参阅《数据加载用户指南》。

先决条件

在开始之前，请确保您满足以下条件：

- 有权创建 AWS KMS 密钥和 SageMaker AI 资源的 AWS 账户
- 您的 AWS 账户 ID 和 CodeDeploy 将要运营的地区
- 数据库连接详细信息：主机名、端口、数据库名称和凭据
- 对您的数据库进行管理访问以验证连接
- 您的数据库已配置为接受来自 AWS 服务的连接

创建 Customer-Managed KMS 密钥

在将数据库连接到之前 CodeDeploy，您需要为数据库凭据设置加密。(AWS KMS) 提供了此安全层，可确保您的数据库密码永远不会以纯文本形式存储。

创建您的 KMS 密钥

1. 导航到 AWS KMS 控制台
 - a. AWS 管理控制台 在浏览器中打开
 - b. 在顶部的搜索栏中，键入“KMS”，然后从结果中选择“密钥管理服务”
 - c. 这将打开 AWS KMS 控制面板，您可以在其中管理加密密钥
2. 启动密钥创建
 - a. 在 AWS KMS 仪表板上，找到并单击右上角的创建密钥按钮
 - b. 这将启动密钥创建向导，该向导将指导您完成设置过程
3. 配置密钥类型和用法
 - a. 在“配置密钥”页面上，选择 Symmetric 作为密钥类型（这是默认且推荐的选项）

- b. 保持“密钥用法”下的“加密和解密”处于选中状态
4. 设置密钥识别详细信息
 - a. 在“别名”字段中，输入密钥的描述性名称，例如 `aws-supply-chain-database-key`
 - b. 在“描述”字段中，添加诸如“CodeDeploy 数据库凭据的加密密钥”之类的上下文
 - c. (可选) 添加标签以帮助组织和跟踪您的 AWS 资源 (例如，密钥：“Project”，值：“CodeDeploy”)
 5. 定义密钥管理权限
 - a. 选择应该能够管理此密钥 (创建、删除、修改策略) 的 IAM 用户或角色
 - b. 至少要包括你自己的管理员角色，以确保你以后可以在需要时修改密钥
 - c. 这些管理员可以管理密钥，但不会自动获得使用密钥的权限 `encryption/decryption`
 - d. 在“密钥删除”部分，允许密钥管理员删除此密钥 (这是默认且推荐的选项)
 6. 定义密钥使用权限
 - a. 在此页面上，您将看到用于选择可以使用密钥的 IAM 用户和角色的选项
 - b. 跳过此处选择特定用户的步骤，您将在下一步中配置服务权限
 7. 为 CodeDeploy 服务配置密钥策略
 - a. 你会看到一个带有默认 JSON 的策略编辑器
 - b. 在 AWS KMS 密钥策略编辑器中，将以下语句附加到现有的“Statement”数组中
 - c. 此策略授予您的账户完全控制权，并允许 CodeDeploy 的服务 (SageMaker AI 和 AWS Glue) 解密您的数据库凭证

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

8. 审查并最终确定

- a. 在摘要页面上查看所有配置设置
- b. 验证您的别名、描述和政策是否正确
- c. 单击“完成”创建密钥
- d. 创建完成后，您将返回到 AWS KMS 控制面板，您的新密钥将出现在列表中

会发生什么

立即创建密钥。创建后，您将在 AWS KMS 控制台中看到您的新密钥列出，其状态为“已启用”。密钥现已准备就绪，可以在 SageMaker AI 中加密您的数据库凭证。

配置

既然您有了密 AWS KMS 钥，就要在中创建一个密钥来安全地存储您的数据库凭证，然后配置 CodeDeploy 允许访问这些凭证的资源策略。

创建你的秘密

1. 导航到
 - a. 在 AWS 管理控制台 搜索栏中，键入“Secrets Manager”
 - b. 从结果中选择“Secrets Manager”以打开服务控制面板
2. 开始创建新密钥
 - a. 点击“存储新秘密”按钮
 - b. 在“选择密钥类型”页面上，选择“其他类型的密钥”（这使您可以灵活地构建凭据）
3. 输入您的数据库凭证

在键值对部分，将您的数据库连接详细信息添加为字符串：

```
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. 选择您的加密密钥
 - a. 在“加密密钥”下，选择“选择密 AWS KMS 钥”
 - b. 从下拉列表中，选择您在上一步中创建的 AWS KMS 密钥（例如，aws-supply-chain-database-key）

c. 这样可以确保您的凭证使用客户管理的密钥进行加密

5. 说出你的秘密

a. 为您的密钥输入一个描述性名称，例如 `aws-supply-chain-production-database`

b. (可选) 添加诸如 “ CodeDeploy 生产环境的数据库凭证 ” 之类的描述

c. 如果组织需要，可以添加标签 (例如，密钥：“环境”，值：“生产”)

6. 添加资源权限

a. 单击 “编辑权限”。在策略编辑器中，粘贴以下策略。此策略允许 CodeDeploy 的服务读取您的密钥。

```
{
  "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. 保存策略

a. 单击 “保存” 以应用资源策略

b. 该策略现已激活，CodeDeploy 允许检索您的数据库凭证

8. 配置轮换 (可选)

a. 在此设置中，您可以通过选择 “禁用自动旋转” 来跳过自动旋转

b. 如果您的安全策略需要，您可以稍后启用轮换

9. 审核和创建

a. 查看您的所有秘密信息

b. 单击 “存储” 创建密钥

c. 您将返回到 SageMaker AI 控制面板

10. 保存你的秘密 ARN

a. 在密钥列表中找到你新创建的密钥

b. 单击密钥名称打开其详细信息页面

c. 在顶部，你会看到秘密 ARN

- d. 复制并保存此 ARN。ARN 格式如下所示：`arn:aws:secretsmanager:us-east-1:123456789012:secret:aws-supply-chain-production-database-AbCdEf`

11 编辑资源权限

- a. 单击“编辑权限”
- b. 粘贴复制的密钥 ARN 并<COPY-THE-SECRET-ARN-HERE-AFTER-CREATING>替换为复制的 ARN
- c. 单击“保存”以附加策略

会发生什么

现在，您的密钥已安全存储并使用您的 AWS KMS 密钥进行加密。CodeDeploy 的服务有权在建立数据库连接时检索凭证，但凭证处于静态加密状态。

将您的数据库连接到 CodeDeploy

配置好密 AWS KMS 钥和密钥后，即可在中建立 JDBC 连接。CodeDeploy

配置您的 JDBC 连接

1. 导航到 CodeDeploy > 数据管理
 - a. 登录您的 CodeDeploy 实例
 - b. 从主导航栏中选择“数据管理”
 - c. 在选项卡导航中，导航到“连接”
 - d. 选择“新建连接”以创建新连接



2. 输入您的连接详情

- 连接名称（必填）：输入此连接的唯一标识符（例如，“生产数据库”）
- 描述（可选）：添加有关此连接的目的和用法的详细信息，以帮助您的团队了解它访问了哪些数据

- **JDBC 网址 (必填)** : 按以下格式输入完整的 JDBC 连接字符串 : `jdbc:<database-type>://<hostname>:<port>/<database>` (例如,) `jdbc:postgresql://db.example.com:5432/mydb`
- **架构名称 (可选)** : 根据需要指定数据库架构 (例如, “public”、“dbo”、“myschema”)。留空以使用数据库的默认架构
- **机密 ARN (必填)** : 粘贴您在上一步中保存的秘密 ARN。这 CodeDeploy 允许从 SageMaker AI 安全地检索您的数据库凭证。
- **强制执行 SSL 连接** : 选中此复选框 (推荐) 以要求对数据库连接进行 SSL/TLS 加密
- **VPC 终端节点服务名称 (必填)** : 输入用于私有连接的 VPC 终端节点服务名称 (格式 : `com.amazonaws.vpce.<region>.vpce-svc-xxxxxxxxxx`)

JDBC Connection

Configure your JDBC data source connection. All fields marked as required must be filled to establish a connection.

Connection details

Connection name
e.g. production-database, staging-analytics

Description
Provide details about the purpose and usage of this connection

JDBC URL
e.g. jdbc:postgresql://db.example.com:5432/mydb

Schema name
e.g. public, dbo, myschema

Authentication details

Secret ARN
AWS Secrets Manager ARN containing database credentials

Security configuration

Require SSL/TLS encryption for database connections (recommended)

Enforce SSL connection

Network configuration

VPC endpoint service name
VPC endpoint service name for private connectivity

3. Connect 连接到您的数据库

- a. 单击“Connect”以测试并建立连接。CodeDeploy 将验证它是否可以使用提供的凭据成功连接到您的数据库。此步骤最多可能需要 2 分钟。
- b. 如果连接成功, 您将自动导航到表格选择
- c. 如果连接失败, 请查看您的连接详细信息以确保所有字段都准确无误 :
 - 验证您的密钥 ARN 是否正确

- 确认您的数据库凭证准确无误
 - 检查您的 JDBC 网址格式是否正确
 - 确保您的数据库已配置为接受来自 AWS 服务的连接
 - 验证您的 AWS KMS 密钥和 SageMaker AI 策略配置是否正确
- d. 您还可以使用聊天体验通过提问“为什么我的数据库连接失败？”之类的问题来帮助解决连接问题或“帮我调试我的 JDBC 连接”
4. 选择要收录的表
- a. 连接后，您将看到“选择表”屏幕，其中显示了数据库中所有可用的表
 - b. 选中要收录的每张表旁边的复选框
5. 配置表格刷新计划
- a. 对于每个选定的表格，单击“操作”列中的三点菜单，然后选择“计划刷新”
 - b. 在“配置负载详细信息”对话框中，设置：
 - 节奏：刷新频率（每小时、每天、每周或自定义）
 - 开始时间：开始刷新的时间（以 UTC 和您的时区偏移量显示）
 - 刷新类型：选择完成刷新（替换所有数据）或增量更新（向现有数据添加新数据；需要选择记录时间戳列）
 - c. 根据需要对每张桌子重复此操作
 - d. 配置完所有表后，单击“开始映射”

Configure load details

Schedule
Configure when and how your data will be refreshed.

Cadence **Start hour**
How often the data should be refreshed. The hour when the refresh should start (your timezone: -08:00).

Daily 00:00 UTC

Refresh type
Choose how data should be updated during each refresh.

Complete refresh
Replace all existing data with fresh data from the source.

Incremental update
Update existing records and add new ones based on a key column.

Cancel Save

6. 继续进行数据映射

- a. 从现在开始，体验与数据加载流程相同
- b. 按照《数据载入用户指南》的“数据映射”部分完成设置

会发生什么

建立连接并选择表后，CodeDeploy 就可以从数据库中读取数据。连接保持活跃和安全，凭证通过 SageMaker AI 进行加密和管理。

最佳实践

安全和访问管理

- 安全地存储凭据：始终用于存储数据库凭据，切勿在连接字符串或配置文件中对凭据进行硬编码
- 启用 SSL/TLS 加密：保持“强制 SSL 连接”选项处于启用状态，以确保传输过程中对数据进行加密
- 定期审查 AWS KMS 和 SageMaker AI 政策：确保只有经过授权的服务和账户才能访问您的加密密钥和机密
- 使用最低权限访问权限：仅向数据库用户授 CodeDeploy 予用于连接的最低必要权限

连接配置

- 使用描述性连接名称：选择清晰、有意义的名称来表示环境和目的（例如，“production-inventory-db”而不是“db1”）
- 记录您的连接：使用描述字段记下连接访问了哪些数据、谁拥有这些数据以及任何特殊注意事项
- 在继续操作之前测试连接：在选择表格和配置刷新计划之前，请务必验证您的连接是否正常
- 验证 JDBC 网址格式：Double-check 您的 JDBC 网址语法与您的数据库类型相匹配以避免连接错误

数据刷新策略

- 选择适当的刷新频率：根据源数据更改频率和业务需求选择刷新频率
- 在低活动期间安排刷新：在数据库负载较低时配置刷新时间，以最大限度地减少对性能的影响
- 尽可能使用增量更新：对于频繁更改的大型数据集，增量更新比完全刷新更有效
- 选择有意义的时间戳列：使用增量更新时，请选择能够准确反映记录创建或修改时间的列

使用聊天进行故障排除

- 具体说明您的请求：在寻求帮助以解决连接或映射问题时，请提供清晰的背景信息
- 询问解释：如果您不理解建议或生成的 SQL 查询，请要求澄清
- 在接受之前测试所有 SQL 更改：使用预览功能验证转换是否按预期使用实际数据
- 利用聊天进行故障排除：当连接失败或刷新遇到错误时，请询问诸如“为什么我的连接失败？”之类的诊断问题 或“帮我理解这个刷新错误”

持续维护

- 定期监控刷新执行情况：检查数据管理中的“目标”和“来源”选项卡，确保刷新成功完成
- 及时解决错误：CodeDeploy 提醒您刷新失败时，请快速调查和解决问题以避免数据缺口
- 安全地更新凭据：当数据库密码更改时，在中进行更新，CodeDeploy 将自动使用新的凭据
- 记录自定义配置：记下任何特殊的刷新计划、转换逻辑或连接要求以供团队参考
- 定期查看表选择：随着数据需求的变化，重新审视您正在采集哪些表，以及刷新计划是否仍然符合业务需求

了解规范数据模型 (CDM)

规范数据模型 (CDM) 是使用的标准化数据结构。在载入供应链数据时，必须将其转换为 CDM 格式，以便可以对其进行处理，以获得规划、预测和运营见解。

本主题解释了什么是清洁发展机制，它为何重要，以及有哪些数据实体可用。

什么是清洁发展机制？

清洁发展机制定义了一组常见的数据实体和字段，这些实体和字段代表供应链概念，例如产品、地点、订单、装运和库存。无论您的源数据的格式或结构如何，CDM 都提供了一个统一的架构，该架构适用于其所有功能。

在数据加载期间，您的源数据将映射到 CDM 目标表。数据代理可以自动建议源字段和 CDM 字段之间的映射，并生成 SQL 转换查询以转换数据。

清洁发展机制为何重要

- 一致性 — 所有功能都在相同的数据结构上运行，确保需求计划、库存优化和交货时间洞察方面的行为一致。

- 互操作性 — 来自不同源系统 (ERP、WMS、TMS) 的数据被标准化为单一模型，从而实现跨系统分析。
- 简化了入门流程 — 数据代理在生成自动映射时使用 CDM 作为目标架构，从而减少了手动工作。
- 数据质量 — 根据清洁发展机制定义进行验证检查，以便在数据用于生产之前发现问题。

数据实体类别

CDM数据实体分为两类：

- Non-transactional 数据-不经常变化的参考数据或主数据，例如产品、站点、贸易伙伴和地理位置。
- 交易数据 — 经常变化的运营数据，例如预测、库存水平、订单和出货量。

支持的数据实体

下表列出了CDM支持的所有数据实体。

支持的 CDM数据实体

数据实体	数据类型	必需
公司	Non-transactional 数据	是
产品	Non-transactional 数据	是
贸易伙伴	Non-transactional 数据	是
供应商产品	Non-transactional 数据	是
地理位置	Non-transactional 数据	是
产品层次结构	Non-transactional 数据	是
运输车道	Non-transactional 数据	是
供应商交货时间	Non-transactional 数据	是
Site	Non-transactional 数据	是
供应商假期	Non-transactional 数据	是

数据实体	数据类型	必需
预测	交易性数据	是
库存	交易性数据	是
入库订单 (PO/STO)	交易性数据	是
出库订单行	交易性数据	是
货件	交易性数据	是
库存政策	交易性数据	是
入库订单行 (PO/STO)	交易性数据	是
出库货件	交易性数据	是
入库订单行计划	交易性数据	是

功能所需的实体

并非中的每个功能都需要所有 CDM 实体。以下各节描述了哪些实体是必需的、可选的或不适用于每项功能。

库存可见性

用于库存可见性的清洁发展机制实体

数据实体	数据类型	必需
公司	Non-transactional	可选
产品	Non-transactional	是
贸易伙伴	Non-transactional	可选
供应商产品	Non-transactional	不适用
地理位置	Non-transactional	可选

数据实体	数据类型	必需
产品层次结构	Non-transactional	可选
运输车道	Non-transactional	可选
供应商交货时间	Non-transactional	不适用
Site	Non-transactional	是
供应商假期	Non-transactional	不适用
预测	事务性	可选
库存	事务性	是
入库订单 (PO/STO)	事务性	可选
出库订单行	事务性	可选
Shipment	事务性	可选
库存政策	事务性	是
入库订单行	事务性	可选
出库货件	事务性	可选
入库订单行计划	事务性	可选

备货时间洞察

CDM实体以获取交货时间见解

数据实体	数据类型	必需
公司	Non-transactional	可选
产品	Non-transactional	是
贸易伙伴	Non-transactional	是

数据实体	数据类型	必需
供应商产品	Non-transactional	是
地理位置	Non-transactional	可选
产品层次结构	Non-transactional	可选
运输车道	Non-transactional	是
供应商交货时间	Non-transactional	是
Site	Non-transactional	是
供应商假期	Non-transactional	可选
预测	事务性	不适用
库存	事务性	不适用
入库订单 (PO/STO)	事务性	是
出库订单行	事务性	不适用
Shipment	事务性	是
库存政策	事务性	不适用
入库订单行	事务性	是
出库货件	事务性	不适用
入库订单行计划	事务性	是

需求规划

用于需求规划的清洁发展机制实体

数据实体	数据类型	必需
公司	Non-transactional	可选

数据实体	数据类型	必需
产品	Non-transactional	是
贸易伙伴	Non-transactional	不适用
供应商产品	Non-transactional	不适用
地理位置	Non-transactional	可选
产品层次结构	Non-transactional	可选
运输车道	Non-transactional	不适用
供应商交货时间	Non-transactional	不适用
Site	Non-transactional	是
供应商假期	Non-transactional	不适用
预测	事务性	不适用
库存	事务性	不适用
入库订单 (PO/STO)	事务性	不适用
出库订单行	事务性	是
Shipment	事务性	不适用
库存政策	事务性	不适用
入库订单行	事务性	不适用
出库货件	事务性	不适用
入库订单行计划	事务性	不适用

清洁发展机制与数据载入有何关系

当您把数据加载到中时，该过程遵循以下步骤：

1. 上传-您将源数据作为 CSV 文件上传到 Amazon S3。
2. 地图 — 数据代理会分析您的源数据集，并建议哪些 CDM 目标表与您的数据最匹配。
3. 转换-SQL 转换查询将您的源数据格式转换为 CDM 格式。
4. 验证 — 对转换后的数据进行质量检查，以验证其是否符合 CDM 要求。
5. 激活-一旦验证，数据就会流入功能并可用于这些功能。

有关加载数据的分步说明，请参阅数据加载主题。

数据验证和质量检查

概述

在 Amazon Connect 决策功能执行之前，数据验证可确保您的数据符合质量要求。系统会根据您配置的计划、指标和规则验证数据，以识别可能阻碍或降低性能的问题。

数据验证的工作原理

验证触发器

数据验证将在以下时间自动运行：

- Insights 配置更改：当您创建或修改指标、规则或其他配置时
- 计划创建：创建临时计划时或每次计划运行时
- 数据刷新：每次数据刷新后，您的目标数据流
- 能力执行：在 AI 队友操作之前或操作期间（例如，导致异常的根源或确定建议时）

验证类型

Amazon Connections 执行两种类型的验证：

Data Presence Validation 会根据您配置的资源（指标、规则、计划）验证是否加载了所需的数据集和字段。

数据质量验证根据您的设置配置验证所提供的数据是否符合质量要求，包括：

- 设置标准验证：确认产品和网站符合您的规则标准（例如产品类别、地点位置）

- 层次结构验证：如果您在设置中使用层次结构，则可以识别缺失的层次结构关系
- 范围验证：确认已识别产品和地点的所有必要数据都存在
- 质量评估：评估数据质量和可用性以满足运营需求

渐进式验证

Amazon Connections 为产品和网站提供有效数据的功能，而不是屏蔽整个数据集的功能。当验证问题影响到特定产品或站点时，系统会继续使用有效数据处理产品和站点，识别存在数据问题的产品或站点，并提醒您注意需要注意的特定项目。这使您可以开始使用功能，同时解决剩余的数据问题。

访问数据验证错误

您可以通过三个入口点查看数据验证错误：

1. 主页上的“数据验证错误”指标
2. 主页上的数据验证错误主题卡
3. 左侧导航栏中的“数据管理” > “错误”选项卡

查看验证错误

“错误”页面显示所有未解决和已解决的验证错误。您可以按以下任一列进行搜索和筛选：

- ID：验证错误的唯一标识符
- 状态
 - 打开：错误尚未解决
 - 已@@ 解决：错误已得到修复和验证
- 说明：数据质量问题的解释
- 问题类型
 - 缺少必填数据：未提供触发操作的必填数据（例如，供应计划中没有 outbound_order_line 来源表）
 - 无效的数据值：数据存在但包含不正确的值（例如，负产品成本）
 - 缺少关系：缺少必需的层次结构或参考关系（例如，缺少产品层次结构）
 - 数据不足：没有足够的数据来执行所需的操作（例如，需求计划需要 12 个月的历史订单数据，但只有 3 个月的历史订单数据）

- 权能：受影响的能力或资源
 - 供应计划
 - 需求计划
 - Insight (包括例外情况、建议和供应或需求的 RCA)
- 目的地：受影响的目的地流
- 优先级
 - 严重：至少有一个技能被完全屏蔽且无法执行
 - 高：至少一项功能被部分屏蔽 (某些产品或网站无法处理)
 - 中：至少有一项能力的精度降低 (将运行，但结果会降低)
- 创建时间：显示首次检测到错误的的时间的时间戳

查看错误详情

选择任意错误以查看详细信息。详细信息屏幕显示上述信息以及“上次发生时间”时间戳、相关资源和链接 (代表受问题影响的能力的指标、规则或计划) ，以及多达 100 行受影响数据的预览，显示数据验证错误的表现方式。

可用操作

在错误详细信息屏幕上，您可以：

- 疑难解答：启动 AI 队友以自然语言协助解决问题，并获得详细的补救指导
- 解决错误：如果您已修复潜在问题，请手动将错误标记为已解决
- 下载：下载完整的受影响数据集以进行详细分析和更正

解决数据验证错误

分辨率工作流程

1. 查看错误描述和优先级以了解其影响
2. 查看受影响的数据预览，查看哪些特定记录受到影响
3. 按照提供的具体补救建议进行操作
4. 选择适当的操作：
 - 对于配置问题：与您的经理和规划人员合作调整指标、规则或计划配置

- 解决映射问题：更正上传的源数据或更新数据转换和映射
- 对于缺失或无效的数据：上传更正后的数据

5. 解决基本问题后，手动将错误标记为已解决

与 AI 队友合作

使用“疑难解答”选项提问“我应该先关注哪些错误？”之类的问题 或“哪些错误阻碍了我的需求计划？”，获取有关问题及其影响的详细说明，获取有关解决方法的分步指导，并了解错误如何影响您的特定配置。AI 队友可以作为指导，在 Amazon Connect 决策和您的源数据系统中解决问题。

最佳实践

- 按严重性划分优先级：首先关注严重错误，因为它们会完全阻碍功能的执行。然后解决部分阻碍处理的高优先级错误，以及降低准确性的中优先级问题。
- 仔细查看建议：每个错误都包含根据您的配置针对问题量身定制的具体、可操作的指导。
- 使用渐进式验证对您有利：在使用功能之前，不要等着解决所有错误。在您努力为其他产品和网站解决问题的同时，系统支持有效产品和网站的功能。
- 数据刷新后进行监控：在每次数据更新后检查是否有新的验证错误，以便在问题影响生产工作流程之前尽早发现问题。
- 策略性地下载受影响的数据：当您需要分析预览之外的所有受影响记录，或者需要向数据团队提供完整的数据集时，请使用下载选项。
- 使用 AI 队友解决复杂问题：“疑难解答”选项提供适合您的特定情况和配置的情境帮助。
- 验证解决方法：修复数据问题后，手动将错误标记为已解决以确认修复成功并将其从“打开”列表中删除。

系统配置

Amazon Connect 决策中的设置是按范围和受众组织的。有些设置是个性化的，允许每位用户量身定制自己的体验。其他配置是由管理员管理的实例级配置，这些配置会影响所有用户的系统行为方式或系统与更广泛的技术环境的连接方式。

User-level 设置允许个人管理其帐户信息、通知首选项以及如何将数据访问范围应用于其视图。

Instance-level 设置允许管理员在整个组织中配置访问控制筛选器行为，建立与 ERP 和其他外部系统的连接，以及定义系统如何处理建议的操作。

这些设置共同使您的组织能够灵活地调整 Amazon Connect 决策以适应您的特定运营环境，同时保持整个团队的一致性。

你将在本节中找到什么

以下页面将指导您完成在 Amazon Connect 决策中配置设置：

- **用户配置文件设置**：从您的个人资料页面管理您的账户信息、通知首选项和数据访问范围
- **Access Control Filter Toggle**：配置系统如何根据实例级别和个人用户级别的用户访问权限筛选见解和建议
- **配置与您的 ERP 的连接**：将 Amazon Connect 决策与您的 ERP 和其他外部系统联系起来，以实现数据交换并支持建议的操作
- **配置操作设置**：定义系统如何处理和执行建议的操作，包括控制操作行为的参数和约束

用户配置文件设置

用户可以通过在应用程序的右上角选择自己的姓名并从下拉菜单中选择“个人资料”来访问其个人资料设置。个人资料页面允许用户管理其账户信息、通知首选项和数据访问设置。

访问个人资料设置

要访问您的个人资料设置，请执行以下操作：

1. 在页面的右上角选择你的名字
2. 从下拉菜单中选择“个人资料”
3. 个人资料页面显示您的账户信息和设置

个人资料信息

个人资料页面显示以下账户详细信息：

用户：您的用户名

角色：分配给您的角色（管理员、经理或规划师）

时区：从下拉菜单中选择您的首选时区。此设置决定了在 Amazon Connect 决策中如何显示日期和时间。

电子邮件：与您的 Amazon Connections 账户关联的电子邮件地址

已创建：您的账户的创建日期和时间

更新：上次修改您的个人资料的日期和时间

选择右上角的“保存”以保存对您的个人资料信息所做的任何更改。

通知首选项

“通知首选项”选项卡允许您配置接收各种系统事件通知的方式。您可以选择在应用程序中接收通知，也可以选择通过电子邮件或两者兼而有之。

计划

计划生成成功：选择计划生成成功完成后您希望以何种方式收到通知。选项包括应用程序内通知和电子邮件通知。

计划生成失败：选择计划生成失败时您希望以何种方式收到通知。选项包括应用程序内通知和电子邮件通知。

见解配置

Insights 配置成功：选择在见解配置成功完成时您希望以何种方式收到通知。选项包括应用程序内通知。

Insights 配置失败：选择在见解配置失败时您希望以何种方式收到通知。选项包括应用程序内通知。

数据摄取

数据提取失败：选择数据摄取失败时您希望如何收到通知。选项包括应用程序内通知和电子邮件通知。

管理员设置

管理员可以配置适用于所有用户的系统范围的通知设置。

通知保留：设置自动从系统中删除通知的天数。输入一个数值来指定保留期。

选择“保存”以应用您的通知首选项。

分配的作用域

Assigned Scope 选项卡显示您的数据访问权限，并允许您配置如何根据分配的范围筛选数据视图。

数据访问

此部分显示您当前的数据访问级别。如果您有权访问所有网站和产品，则会看到消息“您可以访问所有网站和产品”。

默认视图筛选器

按我分配的范围筛选视图：启用后，数据视图会自动筛选，仅显示您分配的产品和网站中的商品。根据您的喜好开启或关闭此设置。

启用此筛选条件后，您只能看到与分配的范围相关的例外、计划和其他数据。禁用后，您可能会看到分配范围之外的数据，具体取决于您的角色权限。

选择“保存”以应用您的筛选器首选项。

访问控制过滤器切换

如前所述，所有用户都可以查看所有例外情况，无论他们是否配置了适当的产品和站点（变异操作仍需要适当的访问权限）。虽然这样可以更轻松地共享知识，但只关注特定产品和网站的用户可能会被其他产品和网站的例外情况或推荐所淹没。为了帮助用户专注于对他们重要的例外情况和建议，他们可以使用访问视图切换开关，如下所示：

- 首先，具有“管理员”角色的用户必须在该实例上启用该功能。从左侧导航栏导航到“实例设置”页面
- 默认情况下，他们将看到一个开关，用于设置整个实例的默认访问视图过滤器。“管理员”可以决定为实例中的所有用户设置一个统一的设置，也可以让用户决定自己的偏好
- 如果他们选择统一访问视图切换设置，“管理员”还可以决定是应为所有用户启用还是禁用该切换

- 如果他们选择让每个用户选择自己的首选项，则每个用户都可以选择为自己切换访问视图过滤器。每个用户都可以从屏幕右上角的“用户”下拉列表中导航到“用户首选项”页面

更改您的实例的访问控制开关：

1. 选择“设置”左侧抽屉
2. 选择应用程序
3. 更新切换开关并点击保存设置

如果启用该设置，系统将自动筛选例外和推荐列表页面，仅显示为与访问控制配置匹配的产品或网站生成的例外和推荐

对于启用了“授予对所有产品和网站的完全访问权限”的用户，访问视图切换开关仍将显示所有例外情况和建议。如果用户禁用了该切换，但未配置任何产品或站点，则系统会将其解释为无法访问任何产品和网站，因此用户将看不到任何内容

访问视图筛选器被视为另一种类型的过滤器，因此不会显示在例外和推荐页面的筛选器芯片中。用户仍然可以像以前一样应用其他过滤器，包括其他产品和网站过滤器

如果用户关闭了访问视图开关，或者他们有指向这些产品的直接超链接，他们仍然可以访问其他产品或网站的例外情况和推荐

配置与 ERP 的连接

要让 Amazon Connect Decisions 在您的企业资源规划 (ERP) 系统中代表您执行操作，您必须配置一个连接，指定必要的连接参数以及 Amazon Connections 在操作期间应使用的凭证。

支持的 ERP 系统：

- SAP S/4HANA

在 Secrets Manager 中配置凭证

1. 使用你的账号，使用 [Secrets Manager 创建 Secrets Manager 密钥](#)
 - 在 Secrets Manager 中输入凭证时，将下方 (<username>和<password>) 的占位符值替换为 Amazon Connections 应使用的实际用户名和密码
 - 如果使用控制台，Other type of secret 请选择 Secret Type

- 如果通过控制台中的Key/value pairs选项卡输入详细信息，请输入 2 对：
 - 密钥:username; 值:<username>
 - 密钥:password; 值:<password>
- 如果使用Plaintext选项卡在控制台中输入密钥，请输入包含两对的 JSON 对象：

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

2. 使用 KMS 密 AWS 钥加密您的密钥，记下密钥的 ID，因为您在后续步骤中将需要它
3. 创建密钥后，请记住其 Amazon 资源名称 (ARN)，因为在后续步骤中您将需要它
 - 例如：arn:aws:secretsmanager:<Region>:<AccountId>:secret:<SecretName>-<SixRandomCharacters>

配置 KMS 密钥的权限

您需要为 Amazon Connect 决策提供访问和使用它所需的权限。

1. 更新您的 KMS 策略以允许 Amazon Connect 决策通过实例角色访问您的密钥
 - 注意：<YourInstanceID>用您的 AWS 账户<YourAccountNumber>和 Amazon Connections 实例编号替换和。

```
{
  "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. 更新您的实例角色的内联策略以授予对密钥的权限

- 注意：<YourInstanceID>用您的秘密 ARN <YourSecretArn>、AWS 账户<YourAccountNumber>和 AWS 供应链实例 ID 替换和。

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

更新你的密钥的 Secrets Manager 资源政策

1. 更新你的密钥的 Secrets Manager 资源政策

- 注意：<YourSecretArn>替换为你的密钥的 ARN

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

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

配置 Amazon Connections 连接

1. 在您的 Amazon Connect 决策实例中，导航至数据管理页面
2. 选择Connections选项卡
3. 单击 Create Connection 按钮
4. 在Create Connector页面中，单击SAP S/4HANA连接器类型行上的Select按钮
5. 在Configure SAP S/4HANA API Connector页面中输入必要的信息：
 - Connection Name: 唯一的连接名称
 - API Endpoint URL: 你的 SAP S/4HANA 实例的 OData API 端点网址 (例如:https://<hostname>:<port>)
 - Client Number: 3 位数的 SAP 客户机号码 (例如:100)
 - Secret ARN : Secrets Manager 中密钥的亚马逊资源名称 (ARN)，用于存储 Amazon Connections 决策使用的凭证
6. 单击Create Connector按钮

配置操作设置

Amazon Connections 允许您控制应提供哪些操作类型，以便在您的企业资源规划 (ERP) 系统中代表您执行操作。默认情况下，所有操作类型都处于禁用状态，您必须为每种所需的操作类型启用此功能。

Note

启用对给定操作类型的支持可控制是否在整个系统中显示 Amazon Connect Decisions 代表您执行操作的选项 (例如：在查看包含给定类型建议的见解时)。在您接受具体建议之前，Amazon Connections 不会执行这些操作 (即使启用了支持)。

支持的操作类型：

- 创建采购订单
- 更新采购订单
- 取消采购订单

为每种操作类型配置动作支持：

1. 在您的 Amazon Connect 决策实例中，导航至数据管理页面
2. 选择Actions选项卡
3. 在列表中找到您要配置的操作类型
4. 要启用对操作类型的支持，请执行以下操作：
 - 为该操作类型选择下拉菜单中列出的连接之一
 - 注意：下拉列表将仅显示已配置为支持该Actions功能的类型的可用连接（例如:SAP S/4HANA）
5. 要禁用对操作类型的支持，请执行以下操作：
 - No connection在下拉菜单中选择该操作类型
6. 点击Save保存您的更改

安全性

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。[责任共担模式](#)将其描述为云的 安全性和云中 的安全性：

- 云安全 — AWS 负责保护在云中运行 AWS 服务的基础架构 AWS Cloud。AWS 还为您提供可以安全使用的服务。Third-party 作为 [AWS 合规计划](#) 的一部分，审计师定期测试和验证我们安全的有效性。要了解适用于 Amazon Connect 决策的合规计划，请参阅[按合规计划划分的范围内的 AWS 服务](#)。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您的公司的要求以及适用的法律法规。

该文档将帮助您了解如何在使用 Amazon Connect 时应用责任共担模式。以下主题向您展示如何配置 Amazon Connect 决策以实现您的安全和合规目标。

数据保护

[责任 AWS 共担模型](#)适用于 Amazon Connect 决策中的数据保护。如本模型所述 AWS，负责保护运行所有 AWS 云的全球基础架构。您负责维护对托管在此基础结构上的内容的控制。您还负责所用 AWS 服务的安全配置和管理任务。有关数据隐私的更多信息，请参阅[数据隐私常见问题](#)。有关欧洲数据保护的信息，请参阅 [AWS 安全博客上的 AWS 责任共担模型和 GDPR](#) 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户凭证并使用 AWS Identity and Access Management (IAM) 设置个人用户。这仅向每个用户授予履行其工作职责所需的权限。我们还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证 (MFA)。
- 用于 SSL/TLS 与 AWS 资源通信。建议使用 TLS 1.2 或更高版本。
- 使用设置 API 和用户活动日志 AWS CloudTrail。
- 使用 AWS 加密解决方案以及 AWS 服务中的所有默认安全控制。
- 使用高级托管安全服务，例如 Amazon Macie，它有助于发现和保护存储在亚马逊简单存储服务中的敏感数据。

- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅 [《美国联邦信息处理标准 \(FIPS\) 第 140-2 版》](#)。

强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入[标签](#)或自由格式文本字段（如名称字段）。这包括您使用 AWS 管理控制台、API、AWS Command Line Interface (AWS CLI) 或 AWS 软件开发工具包使用 Amazon Connect 决策或其他 AWS 服务时。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。

由 Amazon Connect 决策处理的数据

为了限制特定 Amazon Connections 实例的授权用户可以访问的数据，Amazon Connections 中保存的数据按您的 AWS 账户 ID 和 Amazon Connections 实例 ID 进行隔离。

Amazon Connect Decisions 处理各种供应链数据，例如用户信息、从数据连接器中提取的信息以及库存详情。

数据加密

本主题提供特定于 Amazon Connect 决策的信息，这些信息涉及传输中的加密和静态加密。

传输中加密

客户与 Amazon Connections 之间以及 Amazon Connections 与其下游依赖关系之间的所有通信均使用 TLS 1.2 或更高版本的连接进行保护。

静态加密

Amazon Connections 使用 DynamoDB 和亚马逊简单存储服务 (Amazon S3) 存储静态数据。默认情况下，静态数据使用 AWS 加密解决方案进行加密。Amazon Connections 使用来自 AWS Key Management Service (AWS KMS) 的 AWS 自有加密密钥对您的数据进行加密。您无需采取任何措施来保护加密数据的 AWS 托管密钥。有关更多信息，请参阅《AWS KMS 开发人员指南》中的 [AWS 拥有的密钥](#)。

如果您在 AWS 控制台中更改用于加密 Amazon Connect Decisions 实例上数据的 KMS 密钥，则必须创建一个新实例才能开始使用新密钥加密您的数据。任何使用先前密钥加密的数据都不会保留，只会使用更新的密钥对数据进行加密。如果要保留以前加密方法的数据，则可以恢复到对话期间使用的密钥。

您在网络应用程序和聊天应用程序中与 Amazon Connections 的对话仅使用 AWS-owned 密钥进行加密。

Cross-region 处理

Amazon Connections 由 Amazon Bedrock 提供支持，它使用跨区域推理 (CRI) 在不同 AWS 区域之间分配流量，以增强大型语言模型 (LLM) 的推理性能和可靠性。通过跨区域推理，您可以：

- 在高需求时期提高吞吐量和弹性
- 提高性能
- 访问新推出的 Amazon Connections 功能和功能，这些功能和功能依赖于 Amazon Bedrock 上托管的最强大的 LLM

Cross-region 根据创建 Amazon Connections 实例的 AWS 区域，推理的工作原理会有所不同。

对于在美国地理区域创建的所有实例，Amazon Connect Decisions 都将使用全球 CRI。这意味着推理请求将被路由到全球支持的商业 AWS 区域，从而优化可用资源并实现更高的模型吞吐量。要[了解有关全球 CRI 的更多信息](#)，请参阅 [Amazon Bedrock 用户指南](#)。

对于在欧盟地理区域创建的所有实例，Amazon Connect 决策将使用地理 CRI。这意味着推理请求保存在数据最初所在的地理 AWS 区域内。要[了解有关地理 CRIS 的更多信息](#)，请参阅 [Amazon Bedrock 用户指南](#)。

例如，在美国东部（弗吉尼亚北部）（us-east-1）地区创建的 Amazon Connect Decisions 实例发出的请求可以路由到全球 AWS 任何区域，例如亚太地区（悉尼）（ap-southeast-2）。但是，对于从在欧洲（爱尔兰）（eu-west-1）地区创建的 Amazon Connections 实例发出的请求，将路由到欧盟境内的区域，例如欧洲（法 AWS 兰克福）（eu-central-1）。有关更多信息，请参阅 [Amazon Connect 决策支持的区域](#)。

尽管跨区域推理不会改变数据的存储位置，但您的请求和输出结果可能会移出数据最初所在的区域。所有数据在通过 Amazon 的安全网络传输时都已加密。使用跨区域推理不会产生额外成本。有关使用 Amazon Connect 决策时数据存储位置的信息，请参阅 [Amazon Connect 决策中的数据保护](#)。

Amazon Connect 决策的 IAM

Amazon Identity and Access Management (IAM) 是一个亚马逊云科技服务，可以帮助管理员安全地控制对亚马逊云科技资源的访问。IAM 管理员控制谁可以接受身份验证（登录）和授权（有权限）使用 Amazon Connections 资源。IAM 是一项 AWS 服务，您无需支付额外费用即可使用。

使用身份进行身份验证

身份验证是您使用身份凭证登录亚马逊云科技的方法。您必须作为 AWS 账户根用户、IAM 用户或通过担任 IAM 角色进行身份验证。

您可以使用来自 AWS IAM 身份中心 (IAM Identity Center) 等身份源的证书、单点登录身份验证或 Google/Facebook 凭证，以联合身份登录。有关登录的更多信息，请参阅 [AWS Sign-In 用户指南中的如何登录您的 AWS 账户](#)。

对于编程访问，AWS 提供了用于对请求进行加密签名的软件开发工具包和 CLI。有关更多信息，请参阅 IAM 用户指南中针对 [API 请求的 AWS 签名版本 4](#)。

亚马逊云科技账户根用户

创建 AWS 账户时，首先要有一个名为 AWS 账户根用户的登录身份，该用户可以完全访问所有 AWS 服务和资源。我们强烈建议不要使用根用户进行日常任务。有关需要根用户凭证的任务，请参阅《IAM 用户指南》中的 [需要根用户凭证的任务](#)。

联合身份

作为最佳实践，要求人类用户使用与身份提供商的联合身份验证才能使用临时证书访问 AWS 服务。

联合身份是指您的企业目录、Web 身份提供商或 Directory Service 中使用来自身份源的证书访问 AWS 服务的用户。联合身份代入可提供临时凭证的角色。

对于集中访问管理，我们建议使用 AWS IAM 身份中心。有关更多信息，请参阅 [什么是 IAM 身份中心？](#) 在 AWS IAM 身份中心用户指南中。

IAM 用户和群组

[IAM 用户](#)是对某个人员或应用程序具有特定权限的一个身份。建议使用临时凭证，而非具有长期凭证的 IAM 用户。有关更多信息，请参阅 IAM 用户指南中的 [要求人类用户使用与身份提供商的联合身份验证使用临时证书访问 AWS](#)。

[IAM 组](#)指定一组 IAM 用户，便于更轻松地对大量用户进行权限管理。有关更多信息，请参阅《IAM 用户指南》中的 [IAM 用户使用案例](#)。

IAM 角色

[IAM 角色](#)是具有特定权限的身份，可提供临时凭证。您可以通过[从用户切换到 IAM 角色 \(控制台\)](#)或调用 AWS CLI 或 AWS API 操作来代入角色。有关更多信息，请参阅《IAM 用户指南》中的[担任角色的方法](#)。

IAM 角色对于联合用户访问、临时 IAM 用户权限、跨账户访问、跨服务访问以及在 Amazon EC2 上运行的应用程序非常有用。有关更多信息，请参阅《IAM 用户指南》中的 [IAM 中的跨账户资源访问](#)。

使用策略管理访问

您可以通过创建策略并将其附加到 AWS 身份或资源来控制 AWS 中的访问权限。策略定义了与身份或资源关联时的权限。当委托人提出请求时，AWS 会评估这些政策。大多数策略在亚马逊云科技中存储为 JSON 文档。有关 JSON 策略文档的更多信息，请参阅《IAM 用户指南》中的 [JSON 策略概述](#)。

管理员使用策略，通过定义哪个主体可以在什么条件下对哪些资源执行哪些操作来指定谁有权访问什么。

默认情况下，用户和角色没有权限。IAM 管理员创建 IAM 策略并将其添加到角色中，然后用户可以担任这些角色。IAM 策略定义权限，与执行操作所用的方法无关。

Identity-based 政策

Identity-based 策略是您附加到身份（用户、组或角色）的 JSON 权限策略文档。这些策略控制身份可以执行什么操作、对哪些资源执行以及在什么条件下执行。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的 [使用客户管理型策略定义自定义 IAM 权限](#)。

Identity-based 策略可以是内联策略（直接嵌入到单个身份中）或托管策略（附加到多个身份的独立策略）。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的 [在托管策略与内联策略之间进行选择](#)。

Resource-based 政策

Resource-based 策略是您附加到资源的 JSON 策略文档。示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。您必须在基于资源的策略中 [指定主体](#)。

Resource-based 策略是位于该服务中的内联策略。您不能在基于资源的策略中使用来自 IAM 的 AWS 托管策略。

其他策略类型

AWS 支持其他策略类型，这些策略类型可以设置更常见的策略类型授予的最大权限：

- 权限边界-设置基于身份的策略可以向 IAM 实体授予的最大权限。有关更多信息，请参阅《IAM 用户指南》中的 [IAM 实体的权限边界](#)。

- 服务控制策略 (SCP)-在 AWS Organizations 中指定组织或组织单位的最大权限。有关更多信息，请参阅 AWS Organizations 用户指南中的[服务控制策略](#)。
- 资源控制策略 (RCP)-设置账户中资源的最大可用权限。有关更多信息，请参阅 AWS Organizations 用户指南中的[资源控制策略 \(RCP\)](#)。
- 会话策略-为角色或联合用户创建临时会话时作为参数传递的高级策略。有关更多信息，请参阅《IAM 用户指南》中的[会话策略](#)。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解涉及多种策略类型时 AWS 如何确定是否允许请求，请参阅 IAM 用户指南中的[策略评估逻辑](#)。

IAM 如何处理 Amazon Connect 决策

在使用 IAM 管理对 Amazon Connections 的访问权限之前，请先了解哪些可用于 Amazon Connections 的 IAM 功能。要全面了解 Amazon Connect 决策和其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中与 IAM 配合使用的[AWS 服务](#)。

Identity-based Amazon Connect 决策政策

支持基于身份的策略：是

Identity-based 策略是您可以附加到身份（例如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的[使用客户管理型策略定义自定义 IAM 权限](#)。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的[IAM JSON 策略元素引用](#)。

Resource-based Amazon Connect 决策中的政策

支持基于资源的策略：否

Resource-based 策略是您附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中[指定主体](#)。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户访问，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。有关更多信息，请参阅《IAM 用户指南》中的 [IAM 中的跨账户资源访问](#)。

针对 Amazon Connect 决策的政策行动

支持策略操作：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 Action 元素描述可用于在策略中允许或拒绝访问的操作。在策略中包含操作以授予执行关联操作的权限。

Amazon Connect 决策中的策略操作在操作前使用以下前缀：

```
scn
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

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

Amazon Connect 决策的政策资源

支持策略资源：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

Resource JSON 策略元素指定要向其应用操作的一个或多个对象。作为最佳实践，请使用其 [Amazon 资源名称 \(ARN\)](#) 指定资源。对于不支持资源级权限的操作，请使用通配符 (*) 指示语句应用于所有资源。

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

Amazon Connect 决策的政策条件密钥

支持特定于服务的策略条件键：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

Condition 元素根据定义的条件指定语句何时执行。您可以创建使用[条件运算符](#)（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。要查看所有 AWS 全局条件密钥，请参阅 IAM 用户指南中的[AWS 全局条件上下文密钥](#)。

在 Amazon Connect 决策中使用临时证书

支持临时凭证：是

临时证书提供对 AWS 资源的短期访问权限，并且是在您使用联合身份或切换角色时自动创建的。AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 用户指南中的[IAM 和 AWS 服务中与 IAM 配合使用的 AWS 服务中的临时安全证书](#)。

Amazon Connect 决策的转发访问会话

支持转发访问会话 (FAS)：是

转发访问会话 (FAS) 使用调用 AWS 服务的委托人的权限以及请求 AWS 服务的权限，向下游服务发出请求。有关发出 FAS 请求时的策略详情，请参阅[转发访问会话](#)。

Amazon Connect 决策的服务角色

支持服务角色：是

服务角色是由一项服务担任、代表您执行操作的[IAM 角色](#)。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅 IAM 用户指南中的[创建角色以向 AWS 服务委派权限](#)。

Warning

更改服务角色的权限可能会中断 Amazon Connect 决策的功能。只有当 Amazon Connect 决策提供相关指导时，才能编辑服务角色。

Identity-based 策略示例

默认情况下，用户和角色无权创建或修改 Amazon Connections 资源。他们也无法使用 AWS 管理控制台、AWS 命令行界面 (AWS CLI) 或 AWS API 执行任务。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的[创建 IAM policy](#)。

实例管理 IAM 政策

以下是通过控制台或公共 API 创建、更新或删除实例所需的 IAM 政策（不包括所有 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"
}
]
```

策略最佳实践

Identity-based 策略决定是否有人可以在您的账户中创建、访问或删除亚马逊Connect Decisions资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向您的用户和工作负载授予权限，请使用 AWS 托管策略来授予许多常见用例的权限。您可以在 AWS 账户中找到这些策略。我们建议通过定义特定于您的使用案例的 AWS 客户管理型策略来进一步减少权限。有关更多信息，请参阅 [IAM 用户指南中的 AWS 托管策略或 AWS 工作职能托管策略](#)。
- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 [IAM 中的策略和权限](#)。
- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定 AWS 服务（例如）使用的，则也可以使用条件来授予对这些操作的访问权限 CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 [IAM JSON 策略元素：条件](#)。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性：IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言（JSON）和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 [使用 IAM Access Analyzer 验证策略](#)。
- 需要多重身份验证（MFA）– 如果您所处的场景要求您的 AWS 账户中有 IAM 用户或根用户，请启用 MFA 来提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的 [使用 MFA 保护 API 访问](#)。

有关 IAM 中的最佳实践的更多信息，请参阅《IAM 用户指南》中的 [IAM 中的安全最佳实践](#)。

IAM 故障排除

使用以下信息来帮助您诊断和修复在使用 Amazon Connections 和 IAM 时可能遇到的常见问题。

我无权在 Amazon Connect 决策中执行任何操作

如果您无权在 AWS 管理控制台上执行某项操作，则必须联系管理员寻求帮助。管理员是指提供用户名和密码的人员。

当 mateojackson IAM 用户尝试使用控制台查看有关虚构 my-example-widget 资源的详细信息，但不拥有虚构 scn:GetWidget 权限时，会发生以下示例错误。

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

在这种情况下，Mateo 请求他的管理员更新其策略，以允许他使用 scn:GetWidget 操作访问 my-example-widget 资源。

我无权执行 iam : PassRole

如果您收到错误消息，说您无权执行该 iam:PassRole 操作，则必须更新您的策略，以允许您将角色传递给 Amazon Connect Decisions。

某些 AWS 服务允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为的 IAM 用户 marymajor 尝试使用控制台在 Amazon Connect 决策中执行操作时，会出现以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

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

在这种情况下，必须更新 Mary 的策略以允许她执行 iam:PassRole 操作。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人进入 AWS 访问我的 Amazon Connections 资源的账户

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表 (ACL) 的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解 Amazon Connections 是否支持这些功能，请参阅 [Amazon Connections 如何与 IAM 配合使用](#)。
- 要了解如何通过您拥有的 AWS 账户提供对资源的访问权限，请参阅 [IAM 用户指南中的向您拥有的另一个 AWS 账户中的 IAM 用户提供访问权限](#)。
- 要了解如何向第三方 AWS 账户提供对您的资源的访问权限，请参阅 [IAM 用户指南中的向第三方 AWS 账户提供访问权限](#)。
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的 [为经过外部身份验证的用户（身份联合验证）提供访问权限](#)。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 [IAM 中的跨账户资源访问](#)。

Third-party 子处理器

Amazon Connections 使用第三方 API Boomi 来支持在外部系统中代表您执行操作。当您使用连接到您的第三方系统的 Amazon Connect Decisions 功能时，即表示您授权我们使用 Boomi 作为我们的集成中间件来传输和处理您的加密数据；您的数据不会单独存储在 Boomi 中。

要了解有关 Boomi 及其工作原理的更多信息，请参阅 [Boomi 的公共文档](#)。

支持的区域：

本页描述了您可以使用 Amazon Connections 决策的 AWS 区域。有关 AWS 区域的更多信息，请参阅 [《账户管理参考指南》中的指定您的 AWS 账户可以使用的 AWS 区域](#)。

您的数据可能在与您使用 Amazon Connections 的地区不同的地区进行处理。有关 Amazon Connect 决策中有关跨区域处理的信息，请参阅 [Cross-region 处理](#)。有关处理期间数据存储位置的信息，请参阅 [数据保护](#)。

支持的区域：

Amazon Connections 可在以下 AWS 地区的 AWS 管理控制台、AWS 台、Console Mobile Application、AWS 网站、AWS 文档网站上找到。这些区域默认处于启用状态，即使用前无需手动启用。有关更多信息，请参阅 [默认启用的区域](#)。

您在以下区域使用 Amazon Connect 决策。

AWS 地区名称	代号名	地理位置 (美国、欧盟等)
美国东部 (弗吉尼亚州北部)	us-east-1	美国
欧洲地区 (爱尔兰)	eu-west-1	EU

问题排查

当 Amazon Connect 决策的设置或日常使用过程中出现问题时，本节将提供指导以帮助您诊断和解决最常见的问题。首先确定与您遇到的问题最匹配的类别，然后按照相关页面上的疑难解答步骤进行操作。如果您不确定哪个类别适用，请从常见安装问题开始，该问题涵盖了最广泛的初始配置问题。

你将在本节中找到什么

以下页面将指导您解决 Amazon Connect 决策中的常见问题：

- 常见设置问题：对初始实例设置、用户配置和入门配置期间遇到的问题进行故障排除

如果您无法使用本节中的指南解决问题，请与 Support 联系，AWS 提供有关错误消息、问题发生前所采取的步骤以及任何相关配置信息的详细信息。

常见的安装问题

引用完整性错误：“product_id 值与产品数据集中的任何 ID 都不匹配”

最常见的原因是 ID 字段中的尾随空格。从固定宽度的数据库导出的源系统通常用空格填充字符串字段。主产品可能有干净的 ID (“MAT604”)，而订单行文件有填充的 ID (“MAT604”)。系统会进行严格的字符串匹配，因此这些字符串不会加入。

修复：将 TRIM () 添加到数据流 SQL 转换中的所有字符串 ID 字段。将其应用于 product_ID、ship_from_site_id、customer_tpartner_id 和任何其他加入密钥。还要检查文件之间是否存在引用不一致之处。重新导出 CSV 时，请使用 QUOTE_ALL 来防止出现类型推断问题，即看起来像数字的 ID (例如 “111613”) 在一个文件中被视为整数，在另一个文件中被视为字符串。

预防：即使你今天看不到问题，也要始终修剪 SQL 转换中的所有 ID 字段，这是默认做法。在两次导出之间，源数据可能会发生变化。

基础产品中缺少订单历史记录中的商品

您的订单历史记录通常会包含不在当前主产品中的产品 (停产产品、一次性商品、测试 SKU)。如果任何 product_id 没有匹配的产品主记录，则系统将拒绝整个订单文件。

修复：(a) 在基本产品中为缺失的产品创建存根行，其中包含最少的必填字段（ID、描述、base_uom），或者 (b) 筛选订单历史记录以仅包含基本产品中存在的产品。选项 (a) 是首选，因为它保留了可能对谱系和趋势检测有用的需求历史记录。

上传主产品时出现 CSV 解析错误

包含逗号、引号或特殊字符的产品描述可能会中断 CSV 解析。您可能在特定行上看到诸如“预期 17 个字段，已看到 19”之类的错误。

修复：带有正确引号 Re-export 的文件 (QUOTE_ALL)。检查描述字段中是否有嵌入逗号的特定失败行。

上传后数据未显示

- 确认您的文件格式没有更改（扩展名、列标题、编码）。
- 检查文件名和扩展名是否符合预期模式 — 将.csv 重命名为.csv000 或类似名称会中断摄取。
- 上传后，允许最多 30 分钟完成数据摄取。
- 如果列标题在两次加载之间发生变化（例如，由命名的列 month/year），则需要上传之前进行预处理步骤。

数据刷新后 PIV 未更新

- PIV 会在摄取完成大约 15 分钟后触发，运行时间约为 20-30 分钟。
- End-to-end 从数据上传到新的 PIV：大约 1-1.5 小时。
- 如果 PIV 在 24 小时以上未更新，请联系支持人员。

异常计数似乎太高或太低

- 太高：阈值可能过于宽松，或者单个产品+网站可能会在不同的日期生成多个例外。请联系支持人员查看规则配置。
- 太低：阈值可能过于严格，或者某些商品可能缺少所需的数据（例如预测、库存水平）。

Spot-check 您熟悉的几款产品，并将系统显示的内容与您的源系统进行比较。

例外情况未显示财务影响

财务影响要求在产品数据中填写单位成本。如果产品缺少成本或为零，则不会显示任何美元价值。请咨询您的支持团队了解成本数据覆盖范围——跨多个成本字段的瀑布式方法通常可以提供最佳覆盖范围。

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。