aws

管理员指南

AWS Supply Chain

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Supply Chain: 管理员指南

Copyright © 2025 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

什么是 AWS Supply Chain？ 1
支持的浏览器 1
支持的语言 1
..... 1
设置 AWS 账号 3
注册获取 AWS 账户 3
创建具有管理访问权限的用户 3
使用的先决条件 AWS Supply Chain 5
入门 AWS Supply Chain 6
步骤 1：分配 IAM 身份中心用户个人资料 6
第 2 步：创建实例 7
使用标准配置 8
使用高级配置 10
步骤 3：选择 AWS Supply Chain 应用程序所有者 15
登录 AWS Supply Chain Web 应用程序 17
使用 AWS Supply Chain 19
使用 AWS Supply Chain 控制台 19
更新您的个人资料 23
更新您的账户资料 23
更新组织资料 24
管理用户权限角色 24
添加用户 25
更新用户权限 25
删除用户 26
创建自定义用户权限角色 26
删除实例 27
安全性 29
数据保护 29
AWS Supply Chain处理的数据 30
选择退出偏好 30
静态加密 31
传输中加密 31
密钥管理 31
互联网络流量隐私 31

如何在中 AWS Supply Chain 使用补助金 AWS KMS 32
AWS PrivateLink 35
注意事项 36
创建接口端点 36
创建端点策略 36
IAM 37
受众 37
使用身份进行身份验证 38
使用策略管理访问 40
如何 AWS Supply Chain 与 IAM 配合使用 42
基于身份的策略示例 47
故障排除 48
AWS 托管策略 49
AWSSupplyChainFederationAdminAccess 50
策略更新 51
合规性验证 52
恢复能力 53
记录和监控 AWS 供应链 53
AWS Supply Chain 中的数据事件 CloudTrail 54
AWS Supply Chain 中的管理事件 CloudTrail 55
网络应用程序 APIs 55
使用管理事件 EventBridge 61
AWS Supply Chain 事件 62
发送 AWS Supply Chain 事件 62
事件详细信息参考 63
限额 65
常见问题 (FAQs) 67
管理支持 68
文档历史记录 69
..... lxxi

什么是 AWS Supply Chain？

AWS Supply Chain 是一款基于云的供应链管理应用程序，它统一数据并提供基于机器学习的预测方法，以改善需求预测和库存可见性、可行的见解、内置的情境协作、需求计划、供应计划、n 级供应商可见性和可持续性信息管理。 AWS Supply Chain 可以连接到您现有的企业资源规划 (ERP) 和供应链管理系统，并使用机器学习和生成式人工智能将不同的数据转换并集成到供应链数据湖 (SCDL) 中。AWS Supply Chain 可以改善供应链风险管理，无需进行平台重组、支付前期许可费或长期承诺。

主题

- 支持的浏览器 AWS Supply Chain
- 支持的语言 AWS Supply Chain

支持的浏览器 AWS Supply Chain

在使用 Su AWS pply Chain 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	版本在 Firefox end-of-life发布之前一直受支持。有关详细信息，请参阅 Firefox ESR 发布日历。
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。

支持的语言 AWS Supply Chain

AWS Supply Chain 支持以下语言：

- 英语（美国）
- 英语（英国）
- 德语

- 西班牙语
- 法语
- 意大利语
- 葡萄牙语
- 中文（简体）
- 中文（繁体）
- 日语
- 韩语

设置 AWS 账号

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。

主题

- 注册获取 AWS 账户
- 创建具有管理访问权限的用户

注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

报名参加 AWS 账户

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

   注册过程的一部分涉及接听电话或短信，并在电话键盘上输入验证码。

   当您注册时 AWS 账户，就会创建AWS 账户根用户一个。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。您可以随时前往 https://aws.amazon.com/并选择“我的账户”，查看您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

注册后，请保护您的安全 AWS 账户 AWS 账户根用户 AWS IAM Identity Center，启用并创建管理用户，这样您就不会使用 root 用户执行日常任务。

保护你的 AWS 账户根用户

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。AWS Management Console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 登录 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 I A M 用户指南中的为 AWS 账户 根用户启用虚拟 MFA 设备（控制台）。

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 Identity Center 用户指南》中的 Enabling AWS IAM Identity Center。

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

   有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《用户指南》 IAM Identity Center 目录中的使用默认设置配置AWS IAM Identity Center 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网址。

  有关使用 IAM Identity Center 用户登录的帮助，请参阅AWS 登录 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 Create a permission set。

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 Identity Center 用户指南》中的 Add groups。

使用的先决条件 AWS Supply Chain

在创建 AWS Supply Chain 实例之前，请确保完成以下步骤：

- 你有一个 AWS 账户. 要创建 AWS 账户，请参阅设置 AWS 账号。
- 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。
- 您拥有必要的管理权限。有关权限的更多信息，请参阅高级配置。
- 必须在您要创建实例的同一区域激活 IAM 身份中心 AWS Supply Chain 实例。 AWS Supply Chain 仅支持美国东部（弗吉尼亚北部）、美国西部（俄勒冈）、欧洲（法兰克福）、亚太地区（悉尼）和欧洲（爱尔兰）区域。

  如果 AWS Supply Chain 实例与 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 Identity Center 实例中至少有一个用户才能分配为 AWS Supply Chain 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。
- 添加需要访问 IAM 身份中心的所有其他用户。 AWS Supply Chain
- 你需要 AWS Key Management Service (AWS KMS) 来创建实例。 AWS Supply Chain 使用它 AWS KMS key 来加密所有传入的数据 AWS Supply Chain。有关 AWS KMS 密钥的信息，请参阅创建密钥。

入门 AWS Supply Chain

在本节中，您可以学习创建 AWS Supply Chain 实例、授予用户权限角色、登录 AWS Supply Chain Web 应用程序以及创建自定义用户权限角色。最多 AWS 账户 可以有 10 个处于活动或初始化状态的 AWS Supply Chain 实例。

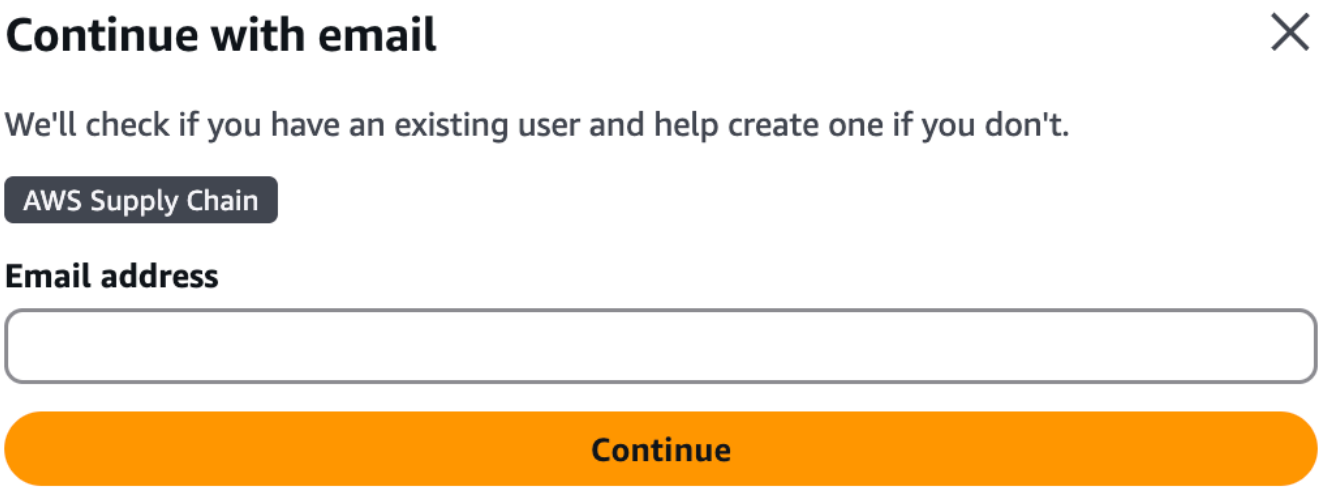
主题

- 步骤 1：分配 IAM 身份中心用户个人资料
- 第 2 步：创建实例
- 步骤 3：选择 AWS Supply Chain 应用程序所有者
- 登录 AWS Supply Chain Web 应用程序

步骤 1：分配 IAM 身份中心用户个人资料

要创建实例并使用该 AWS Supply Chain 服务，您需要连接现有的 IAM Identity Center 用户配置文件或创建新的用户配置文件。

1. 打开 AWS Supply Chain 管理控制台。您也可以从主菜单中搜索AWS Supply Chain“” AWS Management Console。
2. 如有必要，可通过选择控制台顶部的选择区域来更改区域。AWS 从下拉列表中选择您所在的地区。
3. 选择创建 AWS Supply Chain 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 C onnect 您的身份来源并加入您的团队。

     > **Note**
     >
     > 如果您的组织拥有想要使用的已建立 IdC 实例，则可以使用此选项。 AWS Supply Chain

   - 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 AWS Supply Chain 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。请参阅the section called “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。请参阅the section called “使用高级配置”。

第 2 步：创建实例

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。

> **Note**
>
> 只有 AWS Management Console 管理员才能创建实例。创建 AWS Supply Chain 实例的 AWS Management Console 管理员应拥有下面列出的所有权限使用 AWS Supply Chain。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。

您可以使用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。

主题

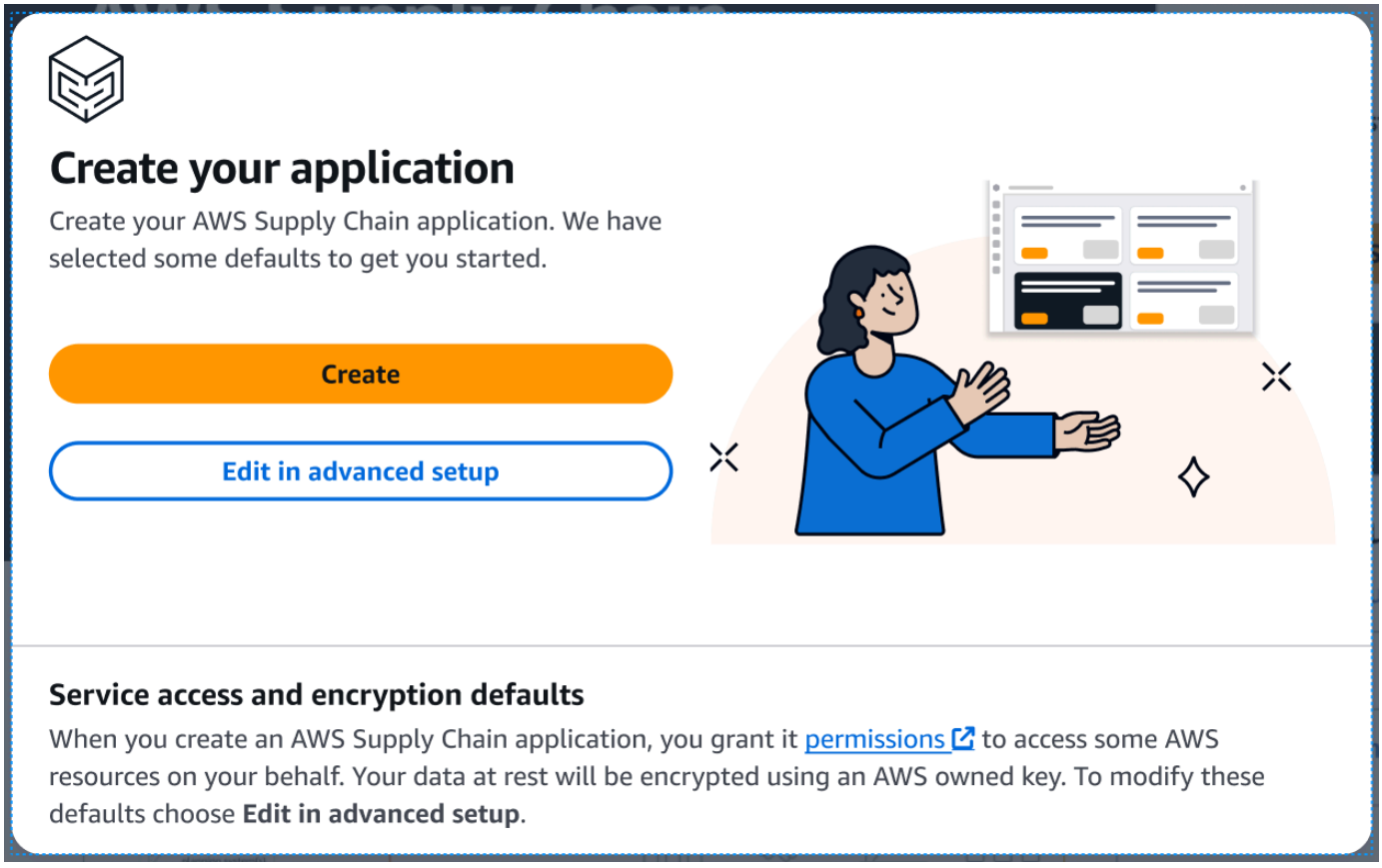
- 使用标准配置
- 使用高级配置

使用标准配置

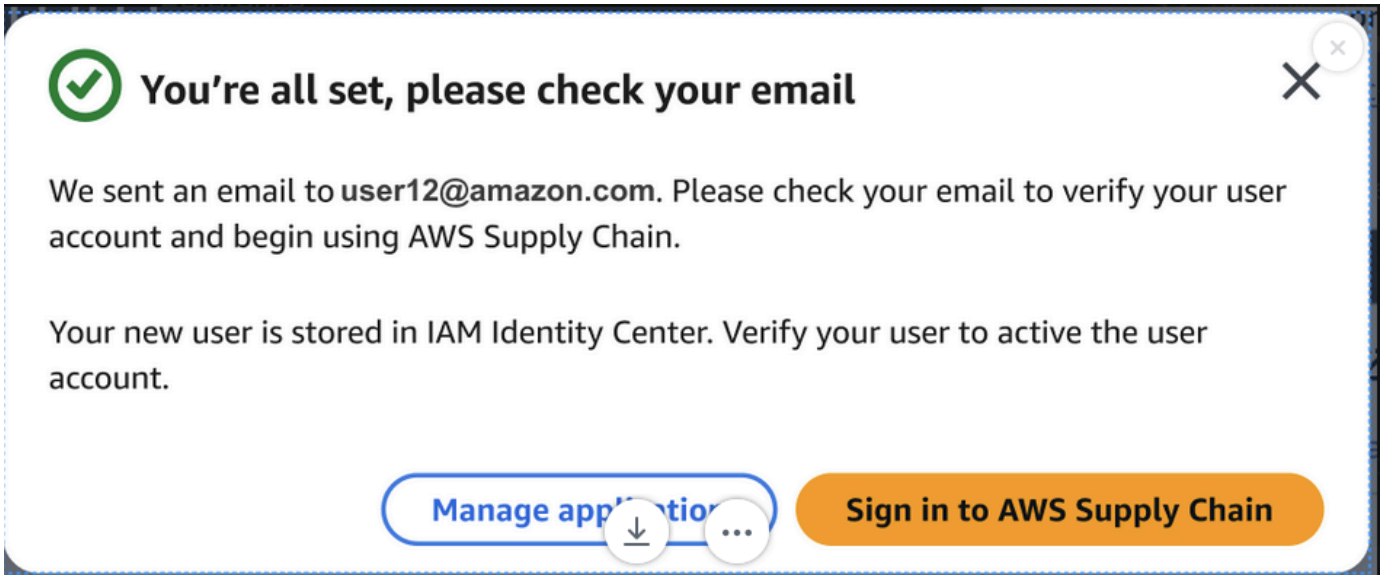
标准配置使用默认的安全和加密设置创建您的 AWS Supply Chain 实例。实例在 AWS 地理区域运行。有关区域的更多信息，请参阅 IAM 用户指南中的区域和终端节点以及中的区域终端节点AWS 一般参考。

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

1. 选择创建。

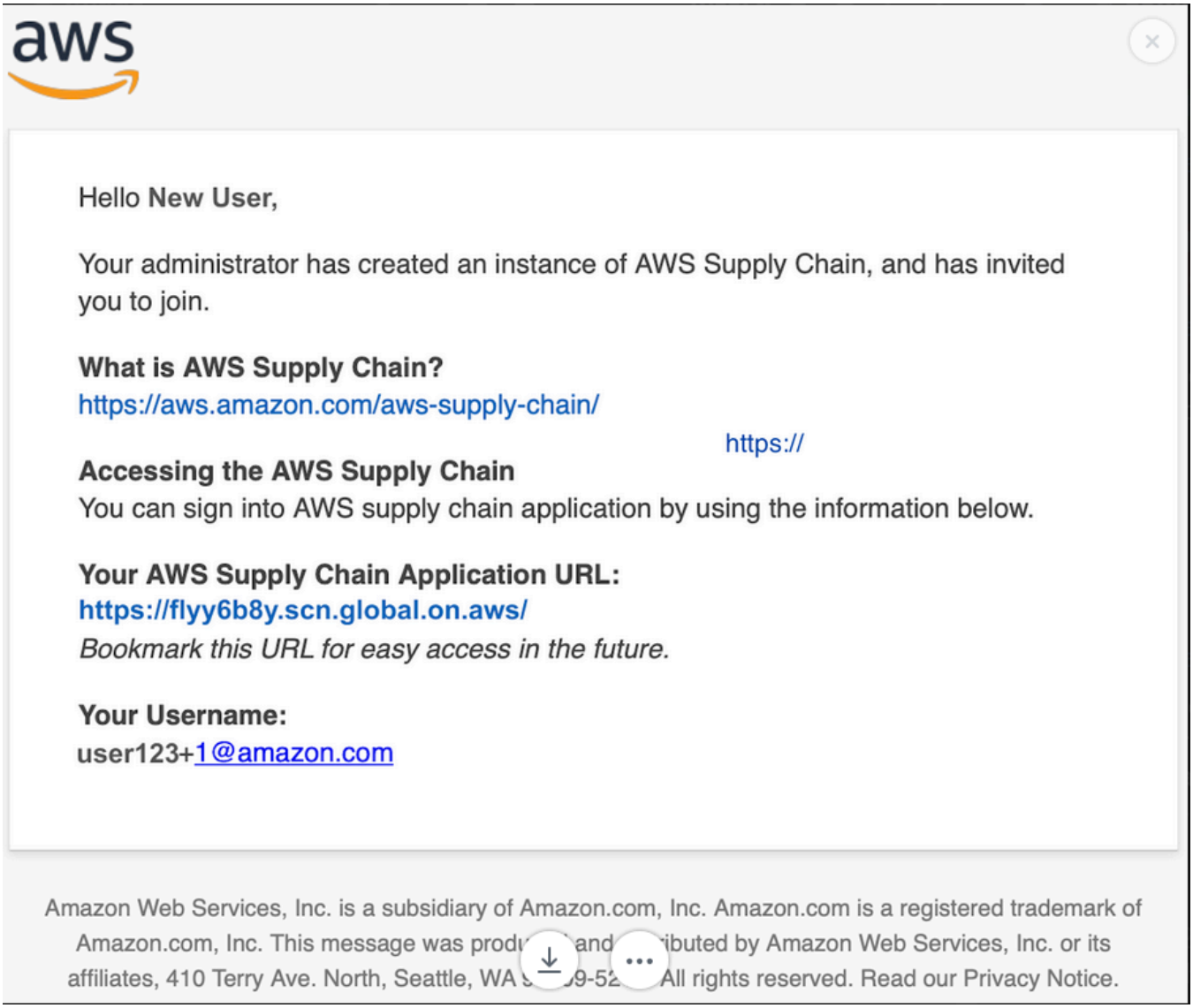


将出现确认信息。



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。

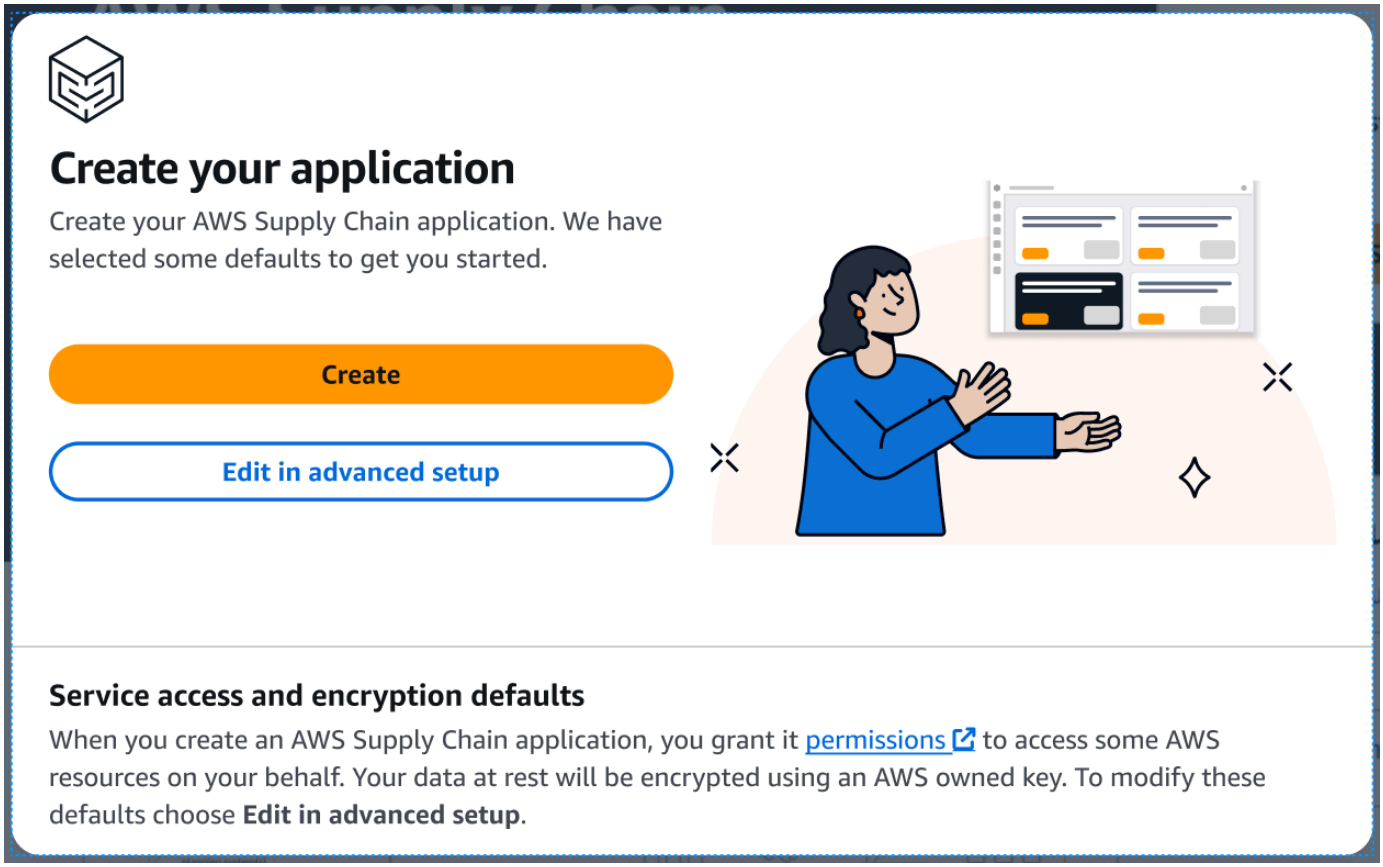


3. 收到邀请电子邮件后，请登录 AWS Supply Chain。见the section called “登录 AWS Supply Chain Web 应用程序”。

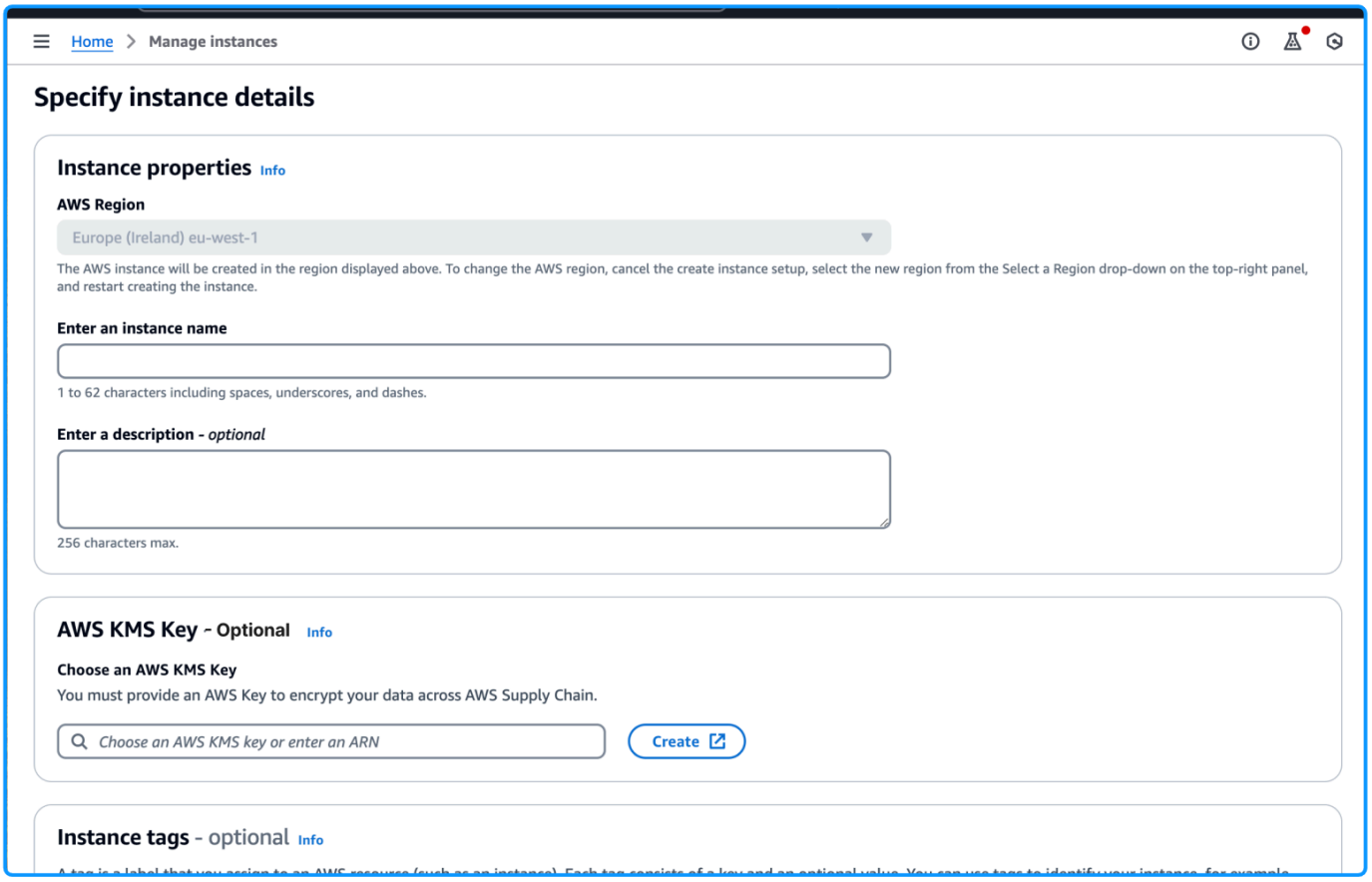
使用高级配置

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 AWS Supply Chain 实例，请按照以下步骤操作。

1. 在高级设置中选择 “编辑”。


Create your application
Create your AWS Supply Chain application. We have selected some defaults to get you started.
Create
Edit in advanced setup
Service access and encryption defaults
When you create an AWS Supply Chain application, 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 Edit in advanced setup.

将会出现 “实例属性” 页面。



2. 在实例属性页面上输入以下内容：

   - 名称-输入实例名称。
   - 描述-输入您的 AWS Supply Chain 实例的描述（例如，生产实例、测试实例等）。
   - AWS KMS 密钥（可选）— 您可以选择使用默认 AWS KMS 密钥（推荐）或提供自己的 AWS KMS 密钥。请参阅the section called “使用自定义 AWS KMS 密钥”了解更多信息。
   - 实例标签-您可以向您的实例添加可用于识别的标签。例如，您可以添加标签来定义要创建的实例的类型（例如，生产、测试、UAT 等）。

   > **Note**
   >
   > 如果您计划使用 S/4 Hana 数据连接，请确保您提供的 AWS KMS 密钥的`aws-supply-chain-access`标签的`true`关联值为。

3. 选择创建实例。

4. （可选）创建 AWS Supply Chain 实例后，如果您选择在 AWS KMS 密钥下使用自己的密AWS KMS 钥，请更新您的 KMS 策略 AWS Supply Chain 以允许访问您的 AWS KMS 密钥。

> **Note**
>
> 将*YourAccountNumber*和*YourInstanceID*替换为您的 AWS 账户 和 AWS Supply Chain 实例 ID。

```
 {

    "Sid": "Allow AWS Supply Chain to access the AWS KMS Key",
    "Effect": "Allow",
    "Principal":  {
        "AWS": "arn:aws:iam::YourAccountNumber:role/service-role/scn-instance-
role-YourInstanceID"
    },
    "Action":  [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": "*"
}
```

使用自定义 AWS KMS 密钥

创建实例时，您可以使用自己的 AWS KMS 密钥。如果您想管理自己的密钥，但又不想使用现有密钥，则可以创建一个新密钥。

> **Note**
>
> 对于 AWS Supply Chain 实例，建议使用 AWS 自有密钥是默认设置。

使用现有 AWS KMS 密钥

1. 选择“自定义加密设置”。
2. 前往“选择密 AWS KMS 钥”。

3. 在提供的字段中输入您的密钥。
4. 选择更新。

创建密 AWS KMS 钥

1. 选择创建。
2. 按照创建 KMS 密钥中的步骤操作。
3. 使用以下权限更新新密钥。

   - 定义密钥管理权限：保持未选中状态
   - 定义密钥使用权限：保持未选中状态
   - 更新密钥策略：编辑密钥策略并替换为：

```
{

    "Version": "2012-10-17",
    "Statement":  [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal":  {
                "AWS": "arn:aws:iam::YourAccountNumber:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow access through SecretManager for all principals in the
 account that are authorized to use SecretManager",
            "Effect": "Allow",
            "Principal":  {
                "AWS": "*"
            },
            "Action":  [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:CreateGrant",
                "kms:DescribeKey",
```

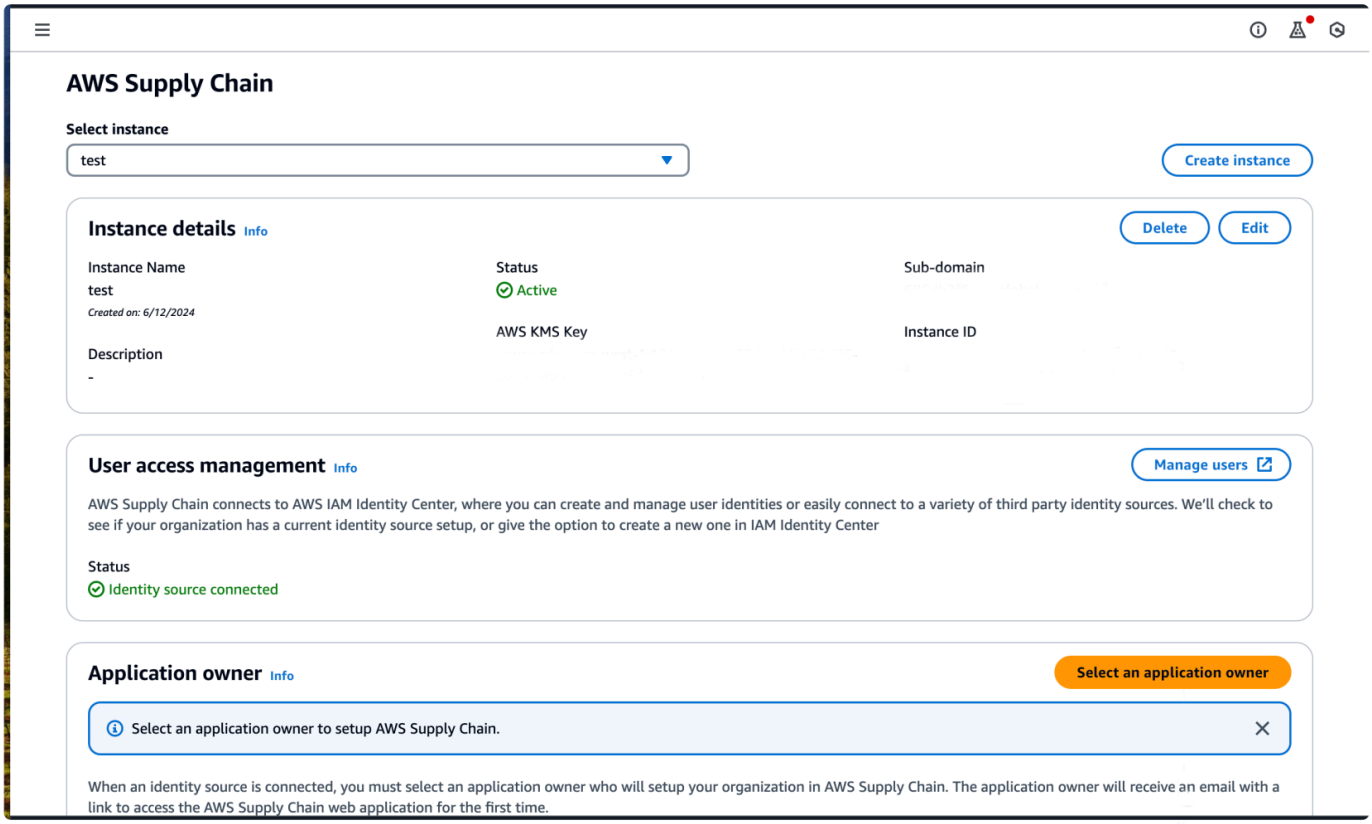
```
                "kms:GenerateDataKeyWithoutPlaintext",
                "kms:ReEncryptFrom",
                "kms:ReEncryptTo"
            ],
            "Resource": "*",
            "Condition":  {
                "StringEquals":  {
                    "kms:ViaService": "secretsmanager.Region.amazonaws.com",
                    "kms:CallerAccount": "YourAccountNumber"
                }
            }
        },
        {
            "Sid": "Allow AWS Supply Chain to access the AWS KMS Key",
            "Effect": "Allow",
            "Principal":  {
                "Service": "scn.Region.amazonaws.com"
            },
            "Action":  [
                "kms:Encrypt",
                "kms:GenerateDataKeyWithoutPlaintext",
                "kms:ReEncryptFrom",
                "kms:ReEncryptTo",
                "kms:Decrypt",
                "kms:GenerateDataKey",
                "kms:DescribeKey",
                "kms:CreateGrant",
                "kms:RetireGrant"
            ],
            "Resource":"*"
        }
    ]
}
```

步骤 3：选择 AWS Supply Chain 应用程序所有者

作为 AWS 控制台管理员，您可以选择 AWS Supply Chain 应用程序所有者来管理 AWS Supply Chain Web 应用程序的访问权限。 AWS Supply Chain 应用程序所有者可以向 AWS Supply Chain Web 应用程序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 AWS Supply Chain 应用程序所有者。

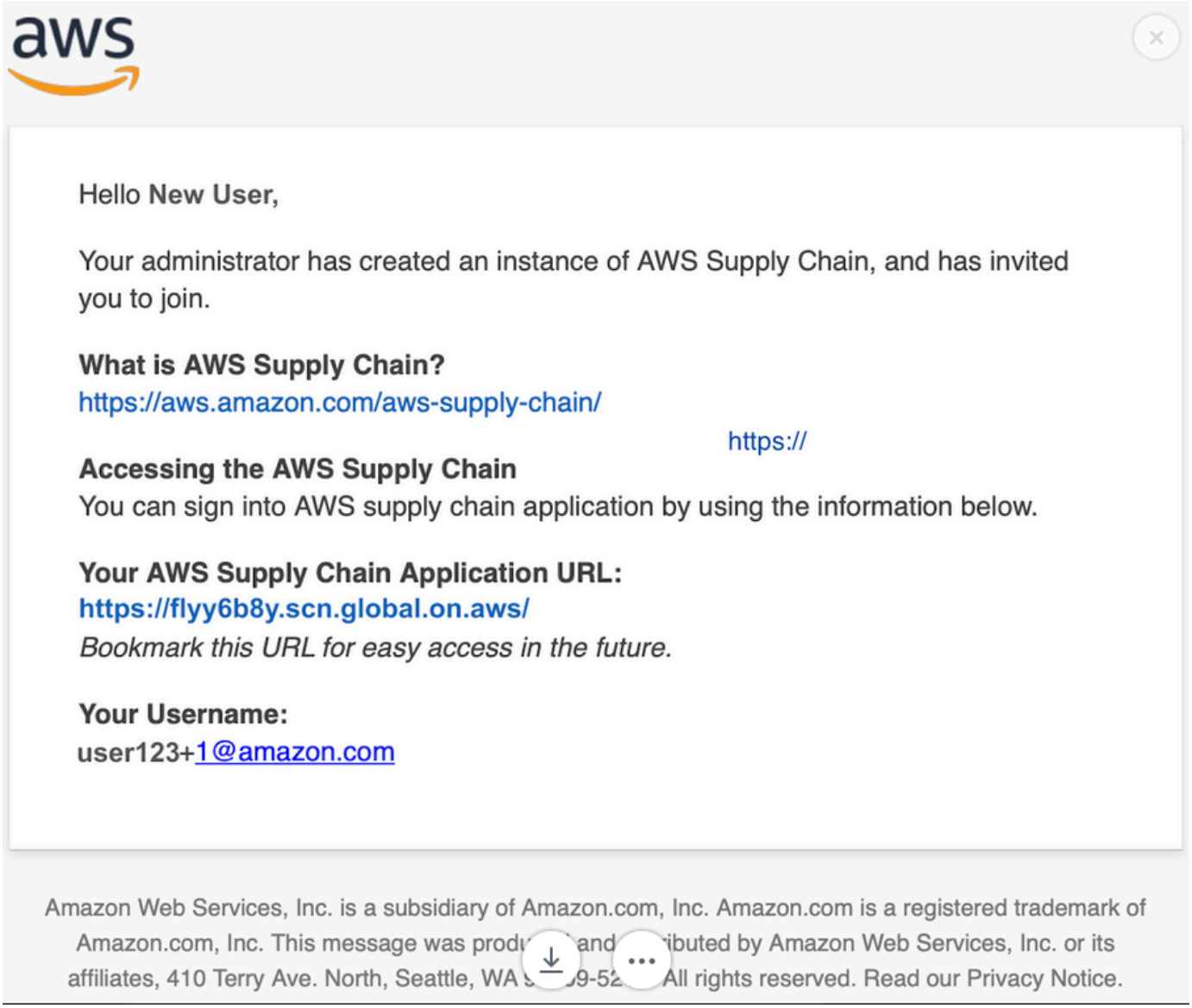
1. 打开 AWS Supply Chain 控制台仪表板。
2. 转至选择应用程序所有者，然后选择一个用户作为 AWS Supply Chain 应用程序所有者。搜索结果仅显示符合搜索条件的用户。



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**
>
> 您一次只能从 AWS Supply Chain 控制台添加一个用户。您无法在 AWS Supply Chain中添加组作为应用程序所有者。

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，便可以选择应用程序 URL 并登录 AWS Supply Chain。



在 AWS Supply Chain 控制台控制面板上，您将看到该用户列在 “应用程序所有者” 下。

在 AWS Supply Chain 中选择 “管理”，在 AWS Supply Chain Web 应用程序中添加和删除用户

登录 AWS Supply Chain Web 应用程序

作为 AWS Supply Chain 管理员，您应该已经收到一封电子邮件邀请，进入 AWS Supply Chain Web 应用程序。

1. 您可以在电子邮件中选择链接，也可以在 AWS Supply Chain 控制台控制面板的子域下，选择 Web URL。

此时将出现 AWS Supply Chain Web 应用程序登录页面。

2. 输入 AWS IAM 身份中心用户证书，然后选择登录。

> **Note**
>
> 只有在您首次登录时，系统才会要求您填写账户和组织的资料。

3. 在完成您的资料页面上，输入您的职位名称和时区。选择下一步。
4. 在让我们添加您的组织信息页面上，输入组织名称并选择总部位置。您可以选择添加公司徽标。选择下一步。
5. 在在 AWS Supply Chain上设置队友页面上，选择您希望其访问 AWS Supply Chain Web 应用程序的用户。选择邀请用户。有关 AWS Supply Chain 用户权限角色的信息，请参阅管理用户权限角色。
6. 如果您想稍后添加用户，可以选择暂时跳过。

   此时将出现引导完成页面。
7. 您添加的每位用户都会收到一封电子邮件，其中包含指向的链接 AWS Supply Chain，或者您可以选择复制链接并将链接发送给用户。
8. 选择继续进入主页以查看 AWS Supply Chain 控制面板。

使用 AWS Supply Chain

AWS Supply Chain 是一款基于云的应用程序，可帮助您了解供应链网络，快速做出明智的决策，并提高供应链弹性。使用 AWS Supply Chain，您可以连接不同的数据源，使用机器学习生成见解，并与内部团队和外部合作伙伴协作。本节将引导您了解一些 AWS Supply Chain 基本功能。

主题

- 使用 AWS Supply Chain 控制台
- 更新您的个人资料
- 管理用户权限角色
- 删除实例

使用 AWS Supply Chain 控制台

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。本节介绍如何访问和导航控制台以执行常见的管理任务。

> **Note**
>
> 如果您的 AWS 账户是某个 AWS 组织的成员账户并且包含服务控制策略 (SCP)，请确保该组织的 SCP 向该成员账户授予以下权限。如果组织的 SCP 策略中未包含以下权限，则 AWS Supply Chain 实例创建将失败。

要访问 AWS Supply Chain 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的 AWS Supply Chain 资源的详细信息 AWS 账户。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 AWS CLI 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。

控制台管理员需要以下权限才能成功创建和更新 AWS Supply Chain 实例。

```
{
 "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": [
     "chime:CreateAppInstance",
     "chime:DeleteAppInstance",
     "chime:PutAppInstanceRetentionSettings",
     "chime:TagResource"
    ],
    "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:CreateGrant",
     "kms:RetireGrant",
     "kms:DescribeKey"
    ],
    "Resource": key_arn,
    "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"
  }
 ]
}
```

*key_arn*指定您要用于 AWS Supply Chain 实例的密钥。有关最佳实践以及仅限访问您想要使用的密钥 AWS Supply Chain，请参阅在 IAM 策略声明中指定 KMS 密钥。要表示所有 KMS 密钥，请单独使用通配符 (“*”)。

更新您的个人资料

您可以随时在 AWS Supply Chain Web 应用程序上更新您的账户和组织资料。

更新您的账户资料

要更新您的账户资料，请按照以下步骤操作。

1. 在 AWS Supply Chain Web 应用程序仪表板的左侧导航窗格中，选择设置图标。
2. 选择账户资料。

   此时将出现账户资料页面。
3. 更新账户信息，然后选择保存。

更新组织资料

要更新组织资料，请按照以下步骤操作。

1. 在 AWS Supply Chain Web 应用程序仪表板的左侧导航窗格中，选择设置图标。
2. 选择组织，然后选择组织资料。

   此时将出现组织资料页面。
3. 更新组织徽标或总部位置，然后选择保存。

管理用户权限角色

作为 AWS Supply Chain 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。 AWS Supply Chain 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。
- 数据分析师 — 创建、查看和管理所有数据连接的权限。
- 库存管理者 — 创建、查看和管理洞察的权限。
- 需求计划员-创建、查看和管理预测、改写和发布需求计划的权限。
- 合作伙伴数据管理员 — 管理和查看合作伙伴、管理和查看数据请求以及查看可持续性数据的权限。
- 供应规划员 — 管理和查看供应计划的权限。

> **Note**
>
> 作为 AWS Supply Chain 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。
> - 删除您创建的自定义权限角色后，该自定义权限角色下的所有用户都将失去访问权限 AWS Supply Chain。
> - 中不支持添加群组 AWS Supply Chain。

主题

- 添加用户
- 更新用户权限
- 删除用户
- 创建自定义用户权限角色

添加用户

作为 AWS Supply Chain 管理员，您可以添加用户以访问 AWS Supply Chain Web 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 AWS Supply Chain。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. 在 AWS Supply Chain 控制面板上选择 “设置” 图标。
2. 选择 “用户和权限”。
3. 选择 “用户”、“用户”。此时将出现管理用户页面。
4. 选择 “添加新用户”。此时将出现添加用户页面。
5. 从 “添加用户” 下拉菜单中选择用户。
6. 从 “选择角色” 下拉菜单中为用户选择角色。
7. 选择添加。

更新用户权限

要更新当前 AWS Supply Chain 用户的用户权限角色，请执行以下步骤。

1. 在 AWS Supply Chain 控制面板的左侧导航窗格中，选择设置图标。
2. 选择权限，然后选择用户。

   此时将出现管理用户页面。
3. 在 “管理用户” 页面上，选择要更新其用户权限角色的用户或组，然后从 “权限角色” 下拉菜单中选择一个权限角色。

> **Note**
>
> 根据您分配的角色权限，可以自定义 AWS Supply Chain 控制面板。有关更多信息，请参阅 创建自定义用户权限角色。

4. 选择保存。

删除用户

作为 AWS Supply Chain 管理员，您可以从 AWS Supply Chain Web 应用程序中删除用户。请按照以下步骤删除删除用户。

1. 在 AWS Supply Chain 控制面板的左侧导航窗格中，选择设置图标。
2. 选择权限，然后选择用户。

   此时将出现管理用户页面。
3. 在管理用户页面上，选择要删除的用户，然后选择删除图标。

创建自定义用户权限角色

除了默认的用户权限角色外，您还可以创建自定义用户权限角色以包含多个权限角色并添加特定的位置和产品。按照以下步骤创建新的权限角色。

1. 在 AWS Supply Chain 控制面板的左侧导航窗格中，选择设置图标。选择属性，然后选择权限角色。

   此时将出现权限角色页面。
2. 选择创建新角色。
3. 在管理权限角色页面的角色名称下，输入名称。
4. 移动滑块以选择用户权限角色。

   - 管理 — 为用户分配管理权限可以添加、编辑和管理信息。
   - 查看 — 为用户分配查看权限只能查看当前信息。

5.

> **Note**
>
> 如果您的实例已连接到数据来源，则只能在位置访问权限和产品访问权限下选择产品和位置。例如，您可以创建一个自定义管理员用户，专门管理西雅图位置的鳄梨，或者创建一个洞察用户，专门管理西雅图位置的鳄梨洞察。

在位置访问权限下，搜索区域（在搜索栏中键入），然后选择区域。

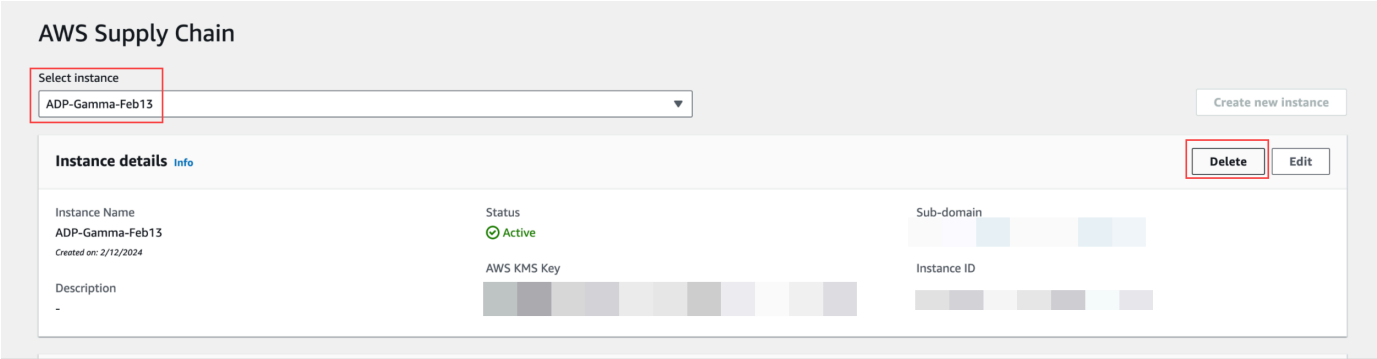
6. 在产品访问权限下，搜索产品（在搜索栏中键入），然后选择产品。
7. 选择保存。

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 AWS Supply Chain 控制台，网址为https://console.aws.amazon.com/scn/home。
2. 在 AWS Supply Chain 控制台控制面板的下拉列表中，选择要删除的实例。



3. 选择删除。
4. 在“删除 AWS Supply Chain 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。

> **Note**
>
> 删除实例后，与 Amazon Q 相关的信息将自动删除。 AWS Supply Chain

安全性 AWS Supply Chain

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 AWS 构建的数据中心和网络架构。

安全性是您和 AWS的共同责任。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 AWS 服务 中运行的基础架构 AWS 云。 AWS 还为您提供可以安全使用的服务。作为 AWS 合规性计划的一部分，第三方审核人员将定期测试和验证安全性的有效性。要了解适用的合规计划 AWS Supply Chain，请参阅按合规计划划分的范围内的AWSAWS 服务按合规计划。
- 云中的安全性 — 您 AWS 服务 使用的安全性决定了您的责任。您还需要对其它因素负责，包括您的数据的敏感性、您的要求以及适用的法律法规。

此文档将帮助您了解如何在使用 AWS Supply Chain时应用责任共担模式。以下主题向您展示如何进行配置 AWS Supply Chain 以满足您的安全和合规性目标。您还将学习如何使用其他方法 AWS 服务 来帮助您监控和保护您的 AWS Supply Chain 资源。

主题

- 中的数据保护 AWS Supply Chain
- AWS Supply Chain 使用接口端点进行访问 (AWS PrivateLink)
- IAM 适用于 AWS Supply Chain
- AWS 的托管策略 AWS Supply Chain
- 合规性验证 AWS Supply Chain
- 韧性在 AWS Supply Chain
- 日志和监控 AWS Supply Chain
- 使用管理 AWS Supply Chain 事件 Amazon EventBridge

中的数据保护 AWS Supply Chain

分 AWS 担责任模型适用于中的数据保护 AWS Supply Chain。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS 云。您负责维护对托管在此基础结构上的内容的控制。您还负责您所使用的 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 Security Blog 上的 AWS Shared Responsibility Model and 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 IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。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）。
- 使用 SSL/TLS 与资源通信。 AWS 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。有关使用 CloudTrail 跟踪捕获 AWS 活动的信息，请参阅《AWS CloudTrail 用户指南》中的使用跟 CloudTrail 踪。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 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 Amazon S3 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 140-3 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 140-3 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）。这包括您使用控制台、API AWS Supply Chain 或以其他 AWS 服务 方式使用控制台 AWS CLI、API 或时 AWS SDKs。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。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

AWS Supply Chain处理的数据

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

AWS Supply Chain 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。

选择退出偏好

如 AWS服务条款所述 AWS Supply Chain，我们可能会使用和存储由处理的您的内容。如果您想选择退出 AWS Supply Chain 使用或存储您的内容，可以在 AWS Organizations 中创建选择退出政策。有关创建选择退出策略的更多信息，请参阅 AI 服务选择退出策略语法和示例。

静态加密

归类为 PII 的联系人数据或代表客户内容的数据（包括 Amazon Q 中 AWS Supply Chain 使用的内容）将使用有时间限制且特定于实例的密钥进行静态加密（即在将其放入、存储或保存到磁盘之前）。AWS Supply Chain AWS Supply Chain

Amazon S3 服务器端加密用于使用每个客户账户独有的 AWS Key Management Service 数据密钥对所有控制台和 Web 应用程序数据进行加密。有关的信息 AWS KMS keys，请参阅什么是 AWS Key Management Service？ 在《AWS Key Management Service 开发人员指南》中。

> **Note**
>
> AWS Supply Chain 功能供应计划和 N 层可见性不支持使用提供的 KMS-C data-at-rest MK 进行加密。

传输中加密

包括在 Amazon Q 中与 AWS 供应链 AWS Supply Chain 交换的内容在内的数据在用户的网络浏览器和 AWS 供应链之间传输时均使用行业标准 TLS 加密进行保护。

密钥管理

AWS Supply Chain 部分支持 KMS-CMK。

有关更新 AWS KMS 密钥的信息 AWS Supply Chain，请参阅第 2 步：创建实例。

互联网络流量隐私

> **Note**
>
> AWS Supply Chain 不支持 PrivateLink。

的虚拟私有云 (VPC) 终端节点 AWS Supply Chain 是 VPC 内的逻辑实体，仅允许连接 AWS Supply Chain。VPC 将请求路由到 VPC AWS Supply Chain 并将响应路由回 VPC。有关更多信息，请参阅《VPC 用户指南》中的 VPC 终端节点。

如何在中 AWS Supply Chain 使用补助金 AWS KMS

AWS Supply Chain 需要获得授权才能使用您的客户托管密钥。

AWS Supply Chain 使用CreateInstance操作期间传递的 AWS KMS 密钥创建多个授权。 AWS Supply Chain 通过向发送CreateGrant请求来代表您创建授权 AWS KMS。中的授权 AWS KMS 用于授予对客户账户中 AWS KMS 密钥的 AWS Supply Chain 访问权限。

> **Note**
>
> AWS Supply Chain 使用它自己的授权机制。将用户添加到后 AWS Supply Chain，您就无法使用该 AWS KMS 策略拒绝列出同一个用户。

AWS Supply Chain 将补助金用于以下用途：

- 向发送GenerateDataKey请求 AWS KMS 以加密存储在您的实例中的数据。
- 向发送 Decrypt 请求 AWS KMS 以读取与实例关联的加密数据。
- 添加DescribeKeyCreateGrant、和RetireGrant权限，以便在将数据发送到 Amazon Forecast 等其他 AWS 服务时确保您的数据安全。

您可以随时撤销授予访问权限，或删除服务对客户托管密钥的访问权限。如果这样做，将 AWS Supply Chain 无法访问由客户托管密钥加密的任何数据，这会影响依赖该数据的操作。

监控您的加密情况 AWS Supply Chain

以下示例是EncryptGenerateDataKey、和Decrypt监控 KMS 操作 AWS CloudTrail 的事件，这些操作由调用 AWS Supply Chain 以访问由您的客户托管密钥加密的数据：

Encrypt

```
          {
"eventVersion": "1.08",
"userIdentity": {
    "type": "AWSService",
    "invokedBy": "scn.amazonaws.com"
},
"eventTime": "2024-03-06T22:39:32Z",
```

```
    "eventSource": "kms.amazonaws.com",
    "eventName": "Encrypt",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "172.12.34.56"
    "userAgent": "Example/Desktop/1.0 (V1; OS)",
    "requestParameters": {
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
    },
    "responseElements": null,
    "requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "readOnly": true,
    "resources": [
        {
            "accountId": account ID,
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "112233445566",
    "sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
    "eventCategory": "Management"
}
```

GenerateDataKey

```
            {
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "scn.amazonaws.com"
    },
     "eventTime": "2024-03-06T22:39:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-east-1",
```

```
    "sourceIPAddress": "172.12.34.56"
    "userAgent": "Example/Desktop/1.0 (V1; OS)",
    "requestParameters": {
        "encryptionContext": {
            "aws:s3:arn": "arn:aws:s3:::test/rawEvent/bf6666c1-111-48aaca-b6b0-
dsadsadsa3432423/noFlowName/scn.data.inboundorder/20240306_223934_536"
        },
        "keyId": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample",
        "keySpec": "AES_222"
    },
    "responseElements": null,
    "requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "readOnly": true,
    "resources": [
        {
            "accountId": account ID,
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "112233445566",
    "sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
    "eventCategory": "Management"
}
```

Decrypt

```
            {
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "scn.amazonaws.com"
    },
     "eventTime": "2024-03-06T22:39:32Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
```

```
    "awsRegion": "us-east-1",
    "sourceIPAddress": "172.12.34.56"
    "userAgent": "Example/Desktop/1.0 (V1; OS)",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample",
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "eventID": "12a345n4-78a4-8888-0000-a000-6q000yy666rr",
    "readOnly": true,
    "resources": [
        {
            "accountId": account ID,
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
east-1:123456789:key/1234abcd-11ab-22bc-33ef-123456sample"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "112233445566",
    "sharedEventID": "fdf9ee0f-e43f-4e43-beac-df69067edb8b",
    "eventCategory": "Management"
}
```


AWS Supply Chain 使用接口端点进行访问 (AWS PrivateLink)

您可以使用 AWS PrivateLink 在您的 VPC 和之间创建私有连接 AWS Supply Chain。您可以像在 VPC 中 AWS Supply Chain 一样进行访问，无需使用互联网网关、NAT 设备、VPN 连接或 AWS Direct Connect 连接。VPC 中的实例不需要公有 IP 地址即可访问 AWS Supply Chain。

您可以通过创建由 AWS PrivateLink提供支持的接口端点来建立此私有连接。我们将在您为接口端点启用的每个子网中创建一个端点网络接口。这些是请求者托管的网络接口，用作发往 AWS Supply Chain 的流量的入口点。

有关更多信息，请参阅AWS PrivateLink 指南 AWS PrivateLink中的AWS 服务 直通访问。

的注意事项 AWS Supply Chain

在为设置接口终端节点之前 AWS Supply Chain，请查看AWS PrivateLink 指南中的注意事项。

AWS Supply Chain 支持通过接口端点调用其所有 API 操作。

为创建接口终端节点 AWS Supply Chain

您可以创建用于 AWS Supply Chain 使用 Amazon VPC 控制台或 AWS Command Line Interface (AWS CLI) 的接口终端节点。有关更多信息，请参阅《AWS PrivateLink 指南》中的创建接口端点。

AWS Supply Chain 使用以下服务名称创建接口终端节点：

```
com.amazonaws.region.scn
```

如果为接口端点启用私有 DNS，则可使用其默认区域 DNS 名称向 AWS Supply Chain 发出 API 请求。例如，*scn*.*region*.amazonaws.com。

为 VPC 端点创建端点策略

端点策略是一种 IAM 资源，您可以将其附加到接口端点。默认终端节点策略允许 AWS Supply Chain 通过接口终端节点进行完全访问。要控制允许 AWS Supply Chain 从您的 VPC 访问权限，请将自定义终端节点策略附加到接口终端节点。

端点策略指定以下信息：

- 可以执行操作的委托人（AWS 账户、IAM 用户和 IAM 角色）
- 可执行的操作
- 可对其执行操作的资源

有关更多信息，请参阅《AWS PrivateLink 指南》中的使用端点策略控制对服务的访问权限。

示例：用于 AWS Supply Chain 操作的 VPC 终端节点策略

以下是自定义端点策略的一个示例。将此策略附加到接口端点时，其会向所有资源上的所有主体授予对列出的 AWS Supply Chain 操作的访问权限。

```
{
```

```
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [

            "scn:action-1",
            "scn:action-2",
            "scn:action-3"

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

IAM 适用于 AWS Supply Chain

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以进行身份验证（登录）和授权（拥有权限）使用 AWS Supply Chain 资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- 如何 AWS Supply Chain 与 IAM 配合使用
- 适用于 AWS Supply Chain的基于身份的策略示例
- 对 AWS Supply Chain 身份和访问进行故障排除

受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您所做的工作 AWS Supply Chain。

服务用户-如果您使用 AWS Supply Chain 服务完成工作，则管理员会为您提供所需的凭证和权限。当你使用更多 AWS Supply Chain 功能来完成工作时，你可能需要额外的权限。了解如何管理访问权限

有助于您向管理员请求适合的权限。如果您无法访问 AWS Supply Chain中的特征，请参阅 对 AWS Supply Chain 身份和访问进行故障排除。

服务管理员-如果您负责公司的 AWS Supply Chain 资源，则可能拥有完全访问权限 AWS Supply Chain。您的工作是确定您的服务用户应访问哪些 AWS Supply Chain 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要详细了解您的公司如何将 IAM 与配合使用 AWS Supply Chain，请参阅如何 AWS Supply Chain 与 IAM 配合使用。

IAM 管理员：如果您是 IAM 管理员，您可能希望了解如何编写策略以管理对 AWS Supply Chain的访问权限的详细信息。要查看您可以在 IAM 中使用的 AWS Supply Chain 基于身份的策略示例，请参阅。适用于 AWS Supply Chain的基于身份的策略示例

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （IAM Identity Center）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅《IAM 用户指南》中的用于签署 API 请求的AWS 签名版本 4。

无论使用何种身份验证方法，您都可能需要提供其他安全信息。例如， AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《AWS IAM Identity Center 用户指南》中的多重身份验证和《IAM 用户指南》中的 IAM 中的AWS 多重身份验证。

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建帐户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，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（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C enter 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。 AWS Directory Service当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和群组，也可以连接并同步到您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户 和应用程序中使用。有关 IAM Identity Center 的信息，请参阅 AWS IAM Identity Center 用户指南中的什么是 IAM Identity Center？。

IAM 用户和群组

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的用例，应在需要时更新访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可以拥有一个名为的群组，IAMAdmins并向该群组授予管理 IAM 资源的权限。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《IAM 用户指南》中的 IAM 用户的使用案例。

IAM 角色

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。要在中临时担任 IAM 角色 AWS Management Console，您可以从用户切换到 IAM 角色（控制台）。您可以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的代入角色的方法。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问：要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关用于联合身份验证的角色的信息，请参阅《IAM 用户指南》中的针对第三方身份提供商创建角色（联合身份验证）。如果您使用

IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。

- 临时 IAM 用户权限：IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取：您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅 IAM 用户指南中的 IAM 中的跨账户资源访问。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在服务中拨打电话时，该服务通常会在 Amazon 中运行应用程序 EC2 或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两项操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。
  - 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 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》中的创建向 AWS 服务委派权限的角色。
  - 服务相关角色-服务相关角色是一种与服务相关联的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。
- 在 A@@ mazon 上运行的应用程序 EC2 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这比在 EC2 实例中存储访问密钥更可取。要为 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建一个附加到该实例的实例配置文件。实例配置文件包含该角色，并允许在 EC2 实例上运行的程序获得临时证书。有关更多信息，请参阅 IAM 用户指南中的使用 IAM 角色向在 A mazon EC2 实例上运行的应用程序授予权限。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的结构和内容的更多信息，请参阅 IAM 用户指南中的 JSON 策略概览。

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。

默认情况下，用户和角色没有权限。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。

IAM 策略定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或 AWS API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（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》中的使用客户托管策略定义自定义 IAM 权限。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。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。

基于资源的策略

基于资源的策略是附加到资源的 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。

基于资源的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 IAM 中的 AWS 托管策略。

访问控制列表 (ACLs)

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。 ACLs 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3 和 Amazon VPC 就是支持的服务示例 ACLs。 AWS WAF要了解更多信息 ACLs，请参阅《亚马逊简单存储服务开发者指南》中的访问控制列表 (ACL) 概述。

其他策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界：权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅IAM 用户指南中的 IAM 实体的权限边界。
- 服务控制策略 (SCPs) — SCPs 是 JSON 策略，用于指定中组织或组织单位 (OU) 的最大权限 AWS Organizations。 AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果您启用组织中的所有功能，则可以将服务控制策略 (SCPs) 应用于您的任何或所有帐户。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organization SCPs s 和的更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略。
- 资源控制策略 (RCPs) — RCPs 是 JSON 策略，您可以使用它来设置账户中资源的最大可用权限，而无需更新附加到您拥有的每个资源的 IAM 策略。RCP 限制成员账户中资源的权限，并可能影响身份（包括身份）的有效权限 AWS 账户根用户，无论这些身份是否属于您的组织。有关 Organizations 的更多信息 RCPs，包括 AWS 服务 该支持的列表 RCPs，请参阅《AWS Organizations 用户指南》中的资源控制策略 (RCPs)。
- 会话策略：会话策略是当您以编程方式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。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。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。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

如何 AWS Supply Chain 与 IAM 配合使用

在使用 IAM 管理访问权限之前 AWS Supply Chain，请先了解有哪些 IAM 功能可供使用 AWS Supply Chain。

您可以搭配使用的 IAM 功能 AWS Supply Chain

IAM 特征	AWS Supply Chain 支持
基于身份的策略	是

IAM 特征	AWS Supply Chain 支持
基于资源的策略	否
策略操作	是
策略资源	是
策略条件键	是
临时凭证	是
转发访问会话（FAS）	是
服务角色	是
服务相关角色	否

要全面了解 AWS Supply Chain 以及其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中的与 IAM 配合使用的AWS 服务。

基于身份的策略 AWS Supply Chain

支持基于身份的策略：是

基于身份的策略是可附加到身份（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。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。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。

基于身份的策略示例 AWS Supply Chain

要查看 AWS Supply Chain 基于身份的策略的示例，请参阅。适用于 AWS Supply Chain的基于身份的策略示例

内部基于资源的政策 AWS Supply Chain

支持基于资源的策略：否

基于资源的策略是附加到资源的 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。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时 AWS 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。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。

的政策行动 AWS Supply Chain

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。策略操作通常与关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

正在执行的策略操作在操作前 AWS Supply Chain 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"
         ]
```

要查看 AWS Supply Chain 基于身份的策略的示例，请参阅。适用于 AWS Supply Chain的基于身份的策略示例

的政策资源 AWS Supply Chain

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。语句必须包含 Resource 或 NotResource 元素。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符（*）指示语句应用于所有资源。

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

要查看 AWS Supply Chain 基于身份的策略的示例，请参阅。适用于 AWS Supply Chain的基于身份的策略示例

的策略条件密钥 AWS Supply Chain

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。

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。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。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM 策略元素：变量和标签。

AWS 支持全局条件密钥和特定于服务的条件密钥。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

要查看 AWS Supply Chain 基于身份的策略的示例，请参阅。适用于 AWS Supply Chain的基于身份的策略示例

将临时凭证与 AWS Supply Chain

支持临时凭证：是

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关更多信息，包括哪些 AWS 服务 适用于临时证书，请参阅 IAM 用户指南中的AWS 服务 与 IA M 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的从用户切换到 IAM 角色（控制台）。

您可以使用 AWS CLI 或 AWS API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 AWS。 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 中的临时安全凭证。

转发访问会话 AWS Supply Chain

支持转发访问会话（FAS）：是

当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两项操作的权限。有关发出 FAS 请求时的策略详细信息，请参阅转发访问会话。

AWS Supply Chain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》中的创建向 AWS 服务委派权限的角色。

> **Warning**
>
> 更改服务角色的权限可能会中断 AWS Supply Chain 功能。只有在 AWS Supply Chain 提供操作指导时才编辑服务角色。

的服务相关角色 AWS Supply Chain

支持服务相关角色：否

服务相关角色是一种与服务相关联的 AWS 服务服务角色。服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

有关创建或管理服务相关角色的详细信息，请参阅使用 IAM 的AWS 服务 服务。在表中查找服务相关角色列中包含 Yes 额表。选择是链接以查看该服务的服务相关角色文档。

适用于 AWS Supply Chain的基于身份的策略示例

默认情况下，用户和角色无权创建或修改 AWS Supply Chain 资源。它们还无法使用 AWS 管理控制台、AWS 命令行界面（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。

主题

- 策略最佳实践

策略最佳实践

基于身份的策略决定了某人是否可以在您的账户中创建、访问或删除 AWS Supply Chain 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 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管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 托管式策略或工作职能的AWS 托管式策略。
- 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 服务的（例如）使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 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 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。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 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。

对 AWS Supply Chain 身份和访问进行故障排除

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

主题

- 我无权在以下位置执行操作 AWS Supply Chain
- 我无权执行 iam：PassRole
- 我想允许我以外的人 AWS 账户 访问我的 AWS Supply Chain 资源

我无权在以下位置执行操作 AWS Supply Chain

如果 AWS Management Console 告诉您，您无权执行某个操作，则必须联系您的管理员寻求帮助。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

如果您收到一个错误，表明您无权执行 `iam:PassRole` 操作，则必须更新策略以允许您将角色传递给 AWS Supply Chain。

有些 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 marymajor 的 IAM 用户尝试使用控制台在 AWS Supply Chain中执行操作时，会发生以下示例错误。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 AWS 账户 访问我的 AWS Supply Chain 资源

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 (ACLs) 的服务，您可以使用这些策略向人们授予访问您的资源的权限。

要了解更多信息，请参阅以下内容：

- 要了解是否 AWS Supply Chain 支持这些功能，请参阅如何 AWS Supply Chain 与 IAM 配合使用。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 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。

AWS 的托管策略 AWS Supply Chain

AWS 托管策略是由创建和管理的独立策略 AWS。 AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住，AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于您的使用场景的客户管理型策略来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务 的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管策略。

AWS 托管策略：AWSSupplyChainFederationAdminAccess

AWSSupplyChainFederationAdminAccess 为 AWS Supply Chain 联合用户提供对 AWS Supply Chain 应用程序的访问权限，包括在 AWS Supply Chain 应用程序中执行操作所需的权限。该策略提供对 IAM Identity Center 用户和群组的管理权限，并附加到由 AWS Supply Chain 为您创建的角色。您不应将该 AWSSupplyChainFederationAdminAccess 策略附加到任何其他 IAM 实体。

尽管此策略 AWS Supply Chain 通过 scn: * 权限提供所有访问权限，但该 AWS Supply Chain 角色决定了您的权限。该 AWS Supply Chain 角色仅包含所需的权限，没有管理员权限 APIs。

权限详细信息

该策略包含以下权限：

- Chime— 提供在 Amazon Chime 下创建或删除用户的权限 AppInstance；提供管理频道、频道成员和版主的权限；提供向频道发送消息的权限。Chime 操作的范围仅限于标有 “SCNInstanceID” 的应用程序实例。
- AWS IAM Identity Center (AWS SSO)— 提供在 IAM Identity Center 中关联和取消关联用户配置文件、列出配置文件关联、列出应用程序分配、描述应用程序、描述实例以及获取应用程序分配配置所需的权限。
- AppFlow — 提供创建、更新和删除连接配置文件的权限；提供创建、更新、删除、启动和停止流的权限；提供对标记和取消标记流以及描述流记录的权限。
- Amazon S3 — 提供列出所有存储桶的权限。使用资源 arn arn: aws: s3:::-* 提供 GetBucketLocation GetObject、、和 ListBucket 访问存储桶的权限。 GetBucketPolicy PutObject aws-supply-chain-data

- SecretsManager — 提供创建机密和更新机密策略的权限。
- KMS— 为 Amazon AppFlow 服务提供对列表密钥和密钥别名的访问权限。为 DescribeKey标有 key-value 的 KMS 密钥提供 CreateGrant 和 ListGrants 权限 aws-suply-chain-access：true；提供创建密钥和更新密钥策略的访问权限。

  权限（kms: ListKeys、kms: ListAliases、kms: GenerateDataKey、kms: 和 kms: decrypt）不限于亚马逊 AppFlow ，这些权限可以授予您账户中的任何 AWS KMS 密钥。

要查看此策略的权限，请参阅AWSSupplyChainFederationAdminAccess中的 AWS Management Console。

AWS Supply ChainAWS 托管策略的更新

下表列出了 AWS Supply Chain 自该服务开始跟踪这些更改以来 AWS 托管策略更新的详细信息。要获得有关此页面变更的自动提醒，请订阅 “ AWS Supply Chain 文档历史记录” 页面上的 RSS feed。

更改	描述	日期
AWSSupplyChainFederationAdminAccess - 更新的策略	AWS Supply Chain 更新了托管策略，允许联合用户访问 ListApplicationAssignments、 DescribeApplication DescribeInstance、和 IAM Identity Center 中的 GetApplicationAssignmentConfiguration 操作。	2024 年 12 月 10 日
AWSSupplyChainFederationAdminAccess - 更新的策略	AWS Supply Chain 更新了托管策略，允许联合用户访问 IAM 身份中心中的 ListProfileAssociations 操作。	2023 年 11 月 1 日
AWSSupplyChainFederationAdminAccess - 更新的策略	AWS Supply Chain 更新了托管策略，允许联合用户使用资源 arn: aws: s3::: aws-supply-	2023 年 9 月 21 日

更改	描述	日期
	chain-data-* 访问 PutObject 和 GetObject 操作专用 S3 存储桶。	
AWSSupplyChainFederationAdminAccess：新策略	AWS Supply Chain 添加了允许联合用户访问 AWS Supply Chain 应用程序的新策略。这包括在 AWS Supply Chain 应用程序中执行操作所需的权限。	2023 年 3 月 1 日
AWS Supply Chain 开始跟踪更改	AWS Supply Chain 开始跟踪其 AWS 托管策略的更改。	2023 年 3 月 1 日

合规性验证 AWS Supply Chain

AWS Supply Chain 作为多个合规计划的一部分，第三方审计师对安全性和 AWS 合规性进行评估。其中包括 SOC、PCI、FedRAMP、HIPAA 及其他。

有关 AWS 服务 属于特定合规计划范围的列表，请参阅按合规计划划分的范围内的AWS 服务按合规计划。有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS Supply Chain 时的合规责任取决于数据的敏感性、贵公司的合规目标以及适用的法律和法规。 AWS 提供了以下资源来帮助实现合规性：

- 安全性与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了部署以安全性和合规性为重点的基准 AWS 环境的步骤。
- HIPAA 安全与合规架构白皮书 — 本白皮书描述了公司如何使用来 AWS 创建符合 HIPAA 标准的应用程序。
- AWS 合规资源AWS — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- 《AWS Config 开发人员指南》中的使用规则评估资源 — 此指南评测您的资源配置对内部实践、行业指南和法规的遵循情况。

- AWS Security Hub— 这 AWS 服务 可以全面了解您的安全状态， AWS 以帮助您检查是否符合安全行业标准和最佳实践。

韧性在 AWS Supply Chain

AWS 全球基础设施是围绕 AWS 区域 可用区构建的。 AWS 区域 提供多个物理隔离、隔离的可用区。通过低延迟、高吞吐量和高度冗余的网络进行连接。利用可用区，您可以设计和操作在可用区之间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础结构相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域 和可用区的更多信息，请参阅AWS 全球基础设施。

除了 AWS 全球基础架构外，还 AWS Supply Chain 提供多项功能来帮助支持您的数据弹性和备份需求。

日志和监控 AWS Supply Chain

日志和监控是维护 AWS 供应链和其他 AWS 解决方案的可靠性、可用性和性能的重要组成部分。AWS 提供了 AWS CloudTrail 监控工具，用于监视 AWS 供应链，在出现问题时报告并在适当时自动采取行动。

> **Note**
>
> APIs 仅从 AWS Supply Chain 控制台调用的会被捕获 AWS CloudTrail。

AWS CloudTrail 捕获由您的 AWS 账户 或代表该账户发出的 API 调用和相关事件，并将日志文件传输到您指定的 Amazon S3 桶。您可以标识哪些用户和账户调用了 AWS、发出调用的源 IP 地址以及调用的发生时间。你可以在 scn. amazonaws.com 下查看 AWS 供应链事件。有关更多信息，请参阅 用户指南。AWS CloudTrail

> **Note**
>
> 请注意以下几点 AWS Supply Chain：
>
> - 当您邀请无权访问的用户时 AWS Supply Chain，这些用户不会在从 Web 应用程序收到的通知中收到信息。受邀用户会收到一封电子邮件通知，其中包含指向 Web 应用程序的链接。只有拥有所需的用户权限，他们才能登录并查看通知中的内容。

- 无论是否拥有特定洞察的用户权限，所有用户都可以查看洞察聊天消息。
- 作为应用程序管理员，当你向 AWS Supply Chain 实例添加用户时，他们可以访问 AWS KMS key。您可以管理添加或删除用户的用户权限。有关用户权限的更多信息，请参阅管理用户权限角色。

AWS Supply Chain 中的数据事件 CloudTrail

> **Note**
>
> 下面 APIs 列出AWS Supply Chain 网络应用程序 APIs的 Web 应用程序列在中的数据事件中 CloudTrail。

数据事件可提供对资源或在资源中所执行资源操作（例如，读取或写入 Amazon S3 对象）的相关信息。这些也称为数据层面操作。数据事件通常是高容量活动。默认情况下， CloudTrail 不记录数据事件。 CloudTrail 事件历史记录不记录数据事件。

记录数据事件将收取额外费用。有关 CloudTrail 定价的更多信息，请参阅AWS CloudTrail 定价。

您可以使用 CloudTrail 控制台或 CloudTrail API 操作记录 AWS Supply Chain 资源类型的数据事件。AWS CLI

- 要使用 CloudTrail 控制台记录数据事件，请创建跟踪或事件数据存储以记录数据事件，或者更新现有的跟踪或事件数据存储以记录数据事件。
  1. 选择数据事件来记录数据事件。
  2. 在数据事件类型列表中，选择要对其记录数据事件的资源类型。
  3. 选择要使用的记录选择器模板。可以记录资源类型的所有数据事件、记录所有 `readOnly` 事件、记录所有 `writeOnly` 事件，或者创建自定义记录选择器模板来根据 `readOnly`、`eventName` 和 `resources.ARN` 字段进行筛选。
- 要使用记录数据事件 AWS CLI，请将`--advanced-event-selectors`参数配置为将`eventCategory`字段设置为等于`Data`并将`resources.type`字段设置为资源类型值。可以添加条件来根据 `readOnly`、`eventName` 和 `resources.ARN` 字段的值进行筛选。
  - 要配置记录数据事件的跟踪，请运行 put-event-selectors 命令。有关更多信息，请参阅使用 AWS CLI记录跟踪的数据事件。

- 要配置事件数据存储以记录数据事件，请运行 create-event-data-store命令创建新的事件数据存储以记录数据事件，或者运行 update-event-data-store命令更新现有的事件数据存储。有关更多信息，请参阅使用 AWS CLI记录事件数据存储的数据事件。

*可以将高级事件选择器配置为根据 `eventName`、`readOnly` 和 `resources.ARN` 字段进行筛选，从而仅记录那些对您很重要的事件。有关这些字段的更多信息，请参阅 AdvancedFieldSelector.

AWS Supply Chain 中的管理事件 CloudTrail

管理事件提供有关对您 AWS 账户中的资源执行的管理操作的信息。这些也称为控制面板操作。默认情况下， CloudTrail 记录管理事件。

AWS Supply Chain 将所有控制平面操作记录 CloudTrail 为管理事件。

AWS Supply Chain 网络应用程序 APIs

本节中 APIs 列出的由 AWS Supply Chain 应用程序代表联合用户调用。 APIs 这些内容在 CloudTrail 日志中不可见，也未在《服务授权参考》文档中捕获，请参阅AWS Supply Chain。对 APIs 这些内容的访问由基于联合用户角色权限的 AWS Supply Chain 应用程序控制。你不应该为了防止干扰应用程序而试图控制 APIs 对这些内容的 AWS Supply Chain 访问。

用户角色

APIs 以下内容用于管理中的用户、用户角色、用户通知和聊天消息 AWS Supply Chain。

```
scn:AddMembersToResourceBasedChat
scn:AssignGalaxyRoleToUser
scn:AssociateUser
scn:BatchGetUsers
scn:BatchMarkNotificationAsDelivered
scn:CreateRole
scn:DeleteRole
scn:DescribeChatForUser
scn:GetAccessDetailConfig
scn:GetChatPreferencesForUser
scn:GetMessagingSessionConnectionDetails
scn:GetNotificationsPreference
scn:GetOrCreateChimeUser
scn:GetOrCreateResourceBasedChat
```

```
scn:GetOrCreateUserBasedChat
scn:GetOrganizationInfo
scn:GetResourceBasedChatArn
scn:GetUserDetails
scn:ListChatMembers
scn:ListChatMessages
scn:ListChatModerators
scn:ListChats
scn:ListRoles
scn:ListUserNotifications
scn:ListUsersWithRole
scn:MarkNotificationAsDelivered
scn:MarkNotificationAsRead
scn:RemoveMemberFromResourceBasedChat
scn:RemoveUser
scn:SearchChimeUsers
scn:SearchUsers
scn:SendChatMessage
scn:SetNotificationsPreference
scn:UpdateChatPreferencesForUser
scn:UpdateChatReadMarker
scn:UpdateOrganizationInfo
scn:UpdateRole
scn:UpdateUser
```

数据湖

APIs 以下内容用于在数据湖中创建和管理数据流和连接。

```
scn:CreateConnection
scn:CreateDataflow
scn:CreateDeleteDataByPartitionJob
scn:CreateExtractFlows
scn:CreatePresignedUrl
scn:CreateSampleParsingJob
scn:CreateSapODataConnection
scn:CreateUpdateDatasetSchemaJob
scn:DeleteConnection
scn:DeleteDataflow
```

```
scn:DeleteExtractFlows
scn:DeleteSapODataConnection
scn:describeDatasetGroup
scn:DescribeDataset
scn:DescribeJob
scn:GetConnection
scn:GetCreateExtractFlowsStatus
scn:GetDataflow
scn:ListConnections
scn:ListCustomerFiles
scn:ListDataflows
scn:ListDataflowStats
scn:ListDatasets
scn:UpdateConnection
scn:UpdateDataflow
scn:UpdateExtractFlow
```

见解

Insights 应用程序使用 APIs 以下内容来管理筛选条件、关注列表和查看库存变化。

```
scn:AddModeratorToResourceBasedChat
scn:ComputePostRebalancedQuantities
scn:ComputePostRebalancedQuantitiesV1
scn:CreateInsightFilter
scn:CreateInsightSubscription
scn:DeleteInsightFilter
scn:DeleteInsightSubscription
scn:GetInsightLineItem
scn:GetInsightSubscription
scn:GetInstanceAttribute
scn:GetInstanceRequiredDatasetAvailabilityStatus
scn:GetKpiData
scn:GetModelEndpointStatus
scn:GetPIVForProduct
scn:GetPIVForSite
scn:GetPIVForSiteAndProduct
scn:GetPIVForSitesAndProducts
scn:GetProducts
```

```
scn:GetProductSummaryAggregates
scn:GetSites
scn:GetSiteSummaryAggregates
scn:IsUserAuthorizedForInsightLineItem
scn:ListCustomAttributeValues
scn:ListGeographiesAsGalaxyAdmin
scn:ListInsightFilters
scn:ListInsightLineItems
scn:ListInsightSubscriptions
scn:ListInventoryQuantityAggregates
scn:ListInventoryRisksBySiteAndProduct
scn:ListInventorySummariesBySite
scn:ListPIVProductsBySite
scn:ListProductHierarchiesAsGalaxyAdmin
scn:ListProducts
scn:ListProductsAsGalaxyAdmin
scn:ListSites
scn:ListUsers
scn:PotentiallyComputeThenListRebalancingOptionsForInsightLineItem
scn:RegisterInstanceAttribute
scn:UpdateInsightFilter
scn:UpdateInsightLineItemStatus
scn:UpdateInsightSubscription
scn:UpdateRebalancingOptionStatus
scn:UpdateRebalancingOptionStatusV1
```

需求规划功能

APIs 以下内容 AWS Supply Chain 用于创建和管理预测、需求计划或工作簿。

```
scn:AssociateDatasetWithWorkbook
scn:CreateBaselineForecast
scn:CreateDemandPlan
scn:CreateDemandPlanningCycle
scn:CreateDemandPlanningDatasetExportJob
scn:CreateDerivedForecast
scn:CreateWorkbook
scn:DeleteDemandForecastConfig
scn:DeleteDemandPlanningCycle
```

```
scn:DeleteDerivedForecast
scn:DeleteWorkbook
scn:DescribeBaselineForecast
scn:DescribeDemandPlanningCycleAccuracyJob
scn:DescribeDerivedForecast
scn:DescribePlanningCycle
scn:DescribeWorkbook
scn:DisassociatePlanningCycle
scn:GetDemandForecastConfig
scn:GetDemandPlan
scn:GetDemandPlanningCycle
scn:GetDemandPlanningCycleAccuracy
scn:GetDemandPlanningDatasetJob
scn:ListDemandPlans
scn:ListDerivedForecasts
scn:ListForecastingJobs
scn:ListPlanningCycles
scn:ListWorkbooks
scn:PublishDemandPlan
scn:PutDemandForecastConfig
scn:StartDemandPlanningCycleAccuracyJob
scn:StartForecastingJob
scn:UpdateDemandPlan
scn:UpdateDemandPlanningCycleMetadata
scn:UpdateWorkbook
```

供应计划

APIs 以下内容 AWS Supply Chain 用于创建和管理供应计划。

```
scn:CreateReplenishmentPipeline
scn:GetReplenishmentPipeline
scn:UpdateReplenishmentPipeline
scn:ListReplenishmentPipelinesByInstance
scn:GetInstanceReplenishmentConfig
scn:CreateBacktest
scn:CreateReplenishmentReviewInstanceConfig
scn:GetReplenishmentReviewInstanceConfig
scn:ListReplenishmentVendors
```

```
scn:GetExceptionsSupplyInsightsStatistics
scn:GetPorSupplyInsightsStatistics
scn:GetPlanToPOConversionAnalytics
scn:GetPurchasePlanStatistics
scn:ListPlanExceptions
scn:ListPurchaseOrderRequestLines
scn:UpdatePurchaseOrderRequestLines
scn:ListBomPurchasePlans
scn:ListBomProductionPlans
scn:ListBomTransferPlans
scn:ListBomInsights
scn:ListBomProcesses
scn:ExportBomPlans
scn:GetBomPlanSummary
scn:GetDashboardAnalytics
scn:GetPurchaseOrderRequestExplanation
scn:ListBomSupplyPlan
scn:GetBomPlanRecordDetails
scn:GetBomPlanSummaryAnalytics
scn:ListBomPurchaseOrders
scn:ListBomTransferOrders
scn:ListBomProductionOrders
scn:ExportAllExplodedBoms
scn:ExportBillOfMaterials
scn:ExportInventoryPolicy
scn:ExportProductionProcess
scn:ExportSourcingRule
scn:ExportTransportationLane
scn:ExportVendorLeadTime
scn:ImportBillOfMaterials
scn:ImportInventoryPolicy
scn:ImportProductionProcess
scn:ImportSourcingRule
scn:ImportTransportationLane
scn:ImportVendorLeadTime
```

亚马逊 Q in AWS Supply Chain

APIs 以下内容在 Amazon Q 中使用 AWS Supply Chain。

```
scn:GetQMessage
scn:ListQMessages
scn:PutQMessageFeedback
scn:SendQMessage
scn:GetQEnablementStatus
scn:UpdateQEnablementStatus
```

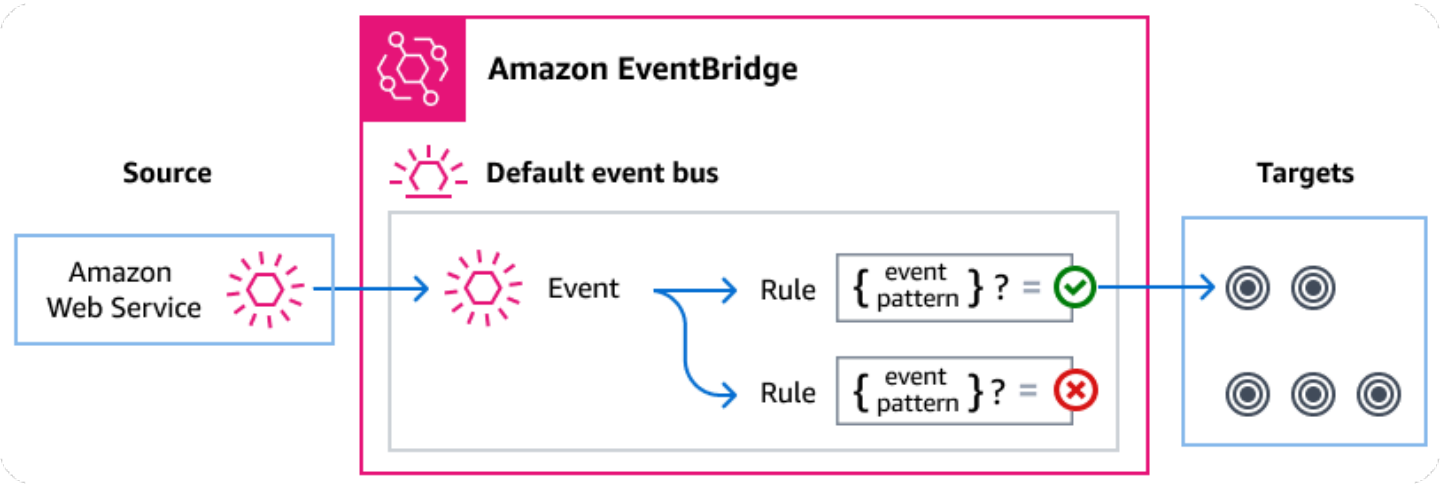
使用管理 AWS Supply Chain 事件 Amazon EventBridge

使用 EventBridge，您可以自动执行其他服务，以响应 Step Functions 标准工作流程的执行状态变化。

Amazon EventBridge 是一项无服务器服务，它使用事件将应用程序组件连接在一起，使您可以更轻松地构建可扩展的事件驱动应用程序。事件驱动型架构是一种构建松耦合软件系统的风格，这些系统通过发出和响应事件 来协同工作。事件代表资源或环境中的变化。

下面将介绍操作方式：

与许多 AWS 服务一样， AWS Supply Chain 生成事件并将其发送到 EventBridge 默认事件总线。（默认事件总线会在每个 AWS 账户中自动配置。）事件总线是接收事件并将其传送到零个或多个目的地或目标的路由器。为事件总线指定的规则会在事件到达时进行评估。每条规则都会检查事件是否与规则的事件模式相匹配。如果事件确实匹配，事件总线会将事件发送到指定的目标。



主题

- AWS Supply Chain 事件
- 使用 EventBridge 规则交付 AWS Supply Chain 事件

- AWS Supply Chain 事件详情参考

AWS Supply Chain 事件

AWS Supply Chain 自动将以下事件发送到默认 EventBridge 事件总线。与规则的事件模式相匹配的事件将按原样传送到指定的目标。事件可能不按顺序传送。

有关更多信息，请参阅《Amazon EventBridge 用户指南》中的 EventBridge 事件。

事件详细信息类型	描述
AWS 供应链数据集成状态变更	显示每个已收录到 AWS Supply Chain的文件的状态。

使用 EventBridge 规则交付 AWS Supply Chain 事件

要让 EventBridge 默认事件总线向目标发送 AWS Supply Chain 事件，必须创建规则。每条规则都包含一个事件模式，该模式与事件总线上接收到的每个事件进行 EventBridge 匹配。如果事件数据与指定的事件模式匹配，则将该事件 EventBridge 传送到规则的目标。

有关创建事件总线规则的全面说明，请参阅《EventBridge 用户指南》中的创建对事件作出反应的规则。

创建与事件匹配 AWS Supply Chain 的事件模式

每个事件模式是一个 JSON 对象，其中包含：

- 标识发送事件的服务的 `source` 属性。对于 AWS Supply Chain 事件，来源是`aws.supplychain`。
- （可选）：包含要匹配的事件类型数组的 `detail-type` 属性。
- （可选）：包含要匹配的其他事件数据的 `detail` 属性。

例如，以下事件模式与来自的所有`AWS Supply Chain Data Integration Status Change`事件匹配 AWS Supply Chain：

```
{
  "source": ["aws.supplychain"],
  "detail-type": ["AWS Supply Chain Data Integration Status Change"]
```

```
}
```

有关写入事件模式的更多信息，请参阅《EventBridge 用户指南》中的事件模式。

AWS Supply Chain 事件详情参考

来自 AWS 服务的所有事件都有一组公共字段，其中包含有关事件的元数据，例如作为事件来源的 AWS 服务、事件的生成时间、事件发生的账户和区域等。有关这些常规字段的定义，请参阅《Amazon EventBridge 用户指南》中的事件结构参考。

此外，每个事件都有一个 `detail` 字段，其中包该特定事件专有的数据。下面的参考定义了各种 AWS Supply Chain 事件的详细信息字段。

使用 EventBridge 来选择和管理 AWS Supply Chain 事件时，记住以下几点很有用：

- 来自的所有事件的`source`字段均设置 AWS Supply Chain 为`aws.supplychain`。
- `detail-type` 字段指定事件类型。

  例如，`AWS Supply Chain Data Integration Status Change`。
- `detail` 字段包含该特定事件专有的数据。

有关如何构造使规则能够匹配 AWS Supply Chain 事件的事件模式的信息，请参阅《Amazon EventBridge 用户指南》中的事件模式。

有关事件及其 EventBridge 处理方式的更多信息，请参阅《Amazon EventBridge 用户指南》中的Amazon EventBridge 事件。

AWS 供应链数据集成状态变更

以下是该`AWS Supply Chain Data Integration Status Change event`事件的示例。

```
{
    "version": "0",
    "id": "instanceID",
    "detail-type": "AWS Supply Chain Data Integration Status Change",
    "source": "aws.supplychain",
    "account": "acccountID",
    "time": "2024-03-30T12:26:13Z",
    "region": "us-east-1",
```

```
    "resources": [],
    "detail": {
        "version": "1.0",
        "instanceId": "instanceID",
        "flowArn": "arn:aws:scn:region:acccountID:instance/instanceID/data-integration-
flows/flowname",
        "flowExecutionId": "flowExecutionId",
        "status": "IN_PROGRESS",
        "startTime": "2024-03-30T12:26:13Z",
        "endTime": "",
        "message": "",
        "sourceType": "S3",
        "sourceInfo": {
            "s3Source": {
                "bucketName": "aws-supply-chain-data-instanceID",
                "key": "flowname"
            }
        }
    }
}
```

endTime仅在状态为失败或成功时可用。

的配额 AWS Supply Chain

您的每个配额 AWS 账户 都有默认配额，以前称为限制 AWS 服务。除非另有说明，否则，每个配额是区域特定的。对于设置为您的账户级别的资源，您可以申请增加配额。有关账户级别配额的更多信息，请参阅下表。

要查看的配额 AWS Supply Chain，请打开 S ervice Quotas 控制台。在导航窗格中，选择 AWS 服务，然后选择 AWS Supply Chain。

要请求提高配额，请参阅《服务配额用户指南》中的请求提高配额。如果配额在服务配额中尚不可用，请使用提高限制表格。

您的 AWS 账户 配额与以下有关 AWS Supply Chain。

资源	默认	可调整
实例的数量 Note 一个 AWS 账户中最多可以创建 10 个实例。	10	否
Amazon S3 桶的数量	100	否
AWS 账户内已激活和待处理的邀请	30	是
AWS 账户内的数据请求	4,000	是
每个关注列表的见解行项目	1000	否
账户中每个实例的 Insight AWS s 关注列表	1000	是
账户内每位用户的 Insight AWS s 关注列表	100	是

资源	默认	可调整
AWS 账户内每个实例的数据集成流	100	否
账户内每个实例的自定义数据集命名空间 AWS	20	是
AWS 账户内每个实例的每个自定义数据集命名空间的数据集	250	是
AWS 账户中每个实例的默认数据集命名空间中的数据集	1000	否

常见问题 (FAQs)

以下信息可以帮助您解决启用 IAM Identity Center 时遇到的常见问题。

问题	回答
为什么需要集成 IAM 身份中心？	IAM 身份中心是 IAM 中的一项功能，用于管理身份源的同步。IAM 身份中心是 AWS Supply Chain 实例的身份来源。您需要配置 IAM 身份中心以设置 AWS 控制台和 AWS Supply Chain Web 应用程序。有关 IAM 身份中心的更多信息，请参阅AWS IAM Identity Center 用户指南中的启用 AWS IAM 身份中心。
为什么要使用 IAM 身份中心组织实例 AWS Supply Chain？	通过创建组织实例，您可以跨 AWS 账户启用 IAM 身份中心访问权限。例如，如果您的 IAM 身份中心未在与 AWS Supply Chain 实例 AWS 账户相同的账户中启用。有关创建组织 IAM Identity Center 实例的好处的更多信息，请参阅AWS IAM Identity Center 用户指南中的 IAM Identity Center 的组织实例。
为什么需要委派管理员权限 AWS Supply Chain？	不需要委派管理员即可使用， AWS Supply Chain 但 AWS 组织设置的最佳做法是限制对组织管理账户的访问权限并管理 IAM Identity Center。有关更多信息，请参阅 Organizations 的委托管理员转子。 AWS 。 创建组织实例时，请确保用于创建 AWS Supply Chain 实例的账户与 IAM Identity Center 账户属于同一个组织。确保已启用创建实例所需的权限，并且您可以在 IAM Identity Center 账户所在的区域创建 AWS Supply Chain 实例。有关创建 AWS Supply Chain 实例所需权限的信息，请参阅入门 AWS Supply Chain。

AWS 支持

如果您是管理员并且需要联系支持人员 AWS Supply Chain，请选择以下选项之一：

- 如果您有 支持 帐户，请前往 Su pport Center 并提交工单。
- 打开 AWS Management Console，并依次选择 AWS Supply Chain、Support 和创建案例。

提供以下信息会有帮助：

- 您的 AWS 供应链实例 ID/ARN。
- 你所在 AWS 的地区。
- 问题的详细说明。

《 AWS Supply Chain 管理员指南》的文档历史记录

下表描述了的文档版本 AWS Supply Chain。

变更	说明	日期
更新了 AWS Supply Chain 配额	更新了与相关的 AWS 账户的配额 AWS Supply Chain。	2024 年 5 月 12 日
更新了 AWS 托管策略	AWS Supply Chain 更新了托管策略，允许联合用户访问 ListApplicationAssignments、 DescribeApplication DescribeInstance、和 IAM Identity Center 中的 GetApplicationAssignmentConfiguration 操作。	2024 年 12 月 10 日
KMS 政策更新	已更新 KMS 策略 AWS Supply Chain 以允许访问您的 AWS KMS 密钥。	2024 年 3 月 18 日
PrivateLink 支持	您可以使用接口终端节点 (AWS PrivateLink) AWS Supply Chain 进行访问。	2024 年 2 月 26 日
添加了组	用户必须是 IAM Identity Center 组的一员才能访问 AWS Supply Chain。	2023 年 11 月 14 日
更新了 AWS 托管策略	AWS Supply Chain 更新了托管策略，允许联合用户访问 IAM 身份中心中的 ListProfileAssociations 操作。	2023 年 11 月 1 日
更新了 AWS 托管策略	AWS Supply Chain 更新了托管策略，允许联合用户使用资源 arn: aws: s3::: aws-supply-	2023 年 9 月 21 日

	chain-data-* 访问 PutObject 和 GetObject 操作专用的 Amazon S3 存储桶。	
更新了有关区域支持的信息	AWS Supply Chain 亚太地区（悉尼）地区现在也支持需求规划。	2023 年 9 月 12 日
使用 AWS 控制台选择加入和退出 AWS Supply Chain	AWS Supply Chain 用户现在可以使用 AWS 控制台选择加入和退出在 AWS Organiz AWS Supply Chain ations 上使用或存储您的内容。	2023 年 9 月 7 日
更新了有关区域支持的信息	AWS Supply Chain 现在亚太地区（悉尼）地区和欧洲（爱尔兰）地区也受支持。	2023 年 7 月 19 日
更新了有关如何联系 AWS Support 和创建实例的信息	AWS Supply Chain 用户现在可以联系 AWS Support 寻求帮助，并更新了有关如何创建实例的内容。	2023 年 4 月 3 日
添加了 AWS 托管策略	AWS Supply Chain 添加了一项新政策，允许联合用户访问 AWS 供应链应用程序，包括在 AWS 供应链应用程序中执行操作所需的权限。	2023 年 3 月 1 日
初始版本	《AWS Supply Chain 管理员指南》的初始版本。	2022 年 11 月 29 日

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。