aws

管理员指南

AWS Supply Chain

AWS Supply Chain: 管理员指南

Table of Contents

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，可与企业资源规划 (ERP) 和供应链管理系统等现有解决方案配合使用。使用 AWS Supply Chain，您可以将现有系统ERP或供应链系统中的库存、供应和需求相关数据连接并提取到一个统一的系统中 AWS Supply Chain 数据模型。

支持的浏览器 AWS Supply Chain

在你使用之前 AWS 供应链，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。
火狐浏览器 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
- French
- 意大利语
- 葡萄牙语
- 中文（简体）

- 中文（繁体）
- 日语
- 韩语
- 印度尼西亚语

设置一个 AWS account

使用此部分创建 AWS 帐户并创建IAM用户。有关创建最佳实践的信息 AWS 账户，请参阅建立最佳实践 AWS 环境。

主题

注册获取 AWS 账户

如果你没有 AWS 账户，请完成以下步骤来创建一个。

要注册 AWS 账户

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

   在注册时，将接到一通电话，要求使用电话键盘输入一个验证码。

   当你注册时 AWS 账户，一个 AWS 账户根用户已创建。root 用户可以访问所有内容 AWS 服务 以及账户中的资源。作为安全最佳实践，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

在你注册之后 AWS 账户，保护你的 AWS 账户根用户，启用 AWS IAM Identity Center，然后创建一个管理用户，这样你就不会使用 root 用户来执行日常任务。

保护你的 AWS 账户根用户

1. 登录 。AWS Management Console以账户所有者的身份选择 Root 用户并输入你的 AWS 账户 电子邮件地址。在下一页上，输入您的密码。

有关使用 root 用户登录的帮助，请参阅中以 root 用户身份登录 AWS 登录 用户指南。

2. 为您的 root 用户开启多重身份验证 (MFA)。

   有关说明，请参阅为您的MFA设备启用虚拟设备 AWS 账户 用户指南中的 root IAM 用户（控制台）。

创建具有管理访问权限的用户

1. 启用IAM身份中心。

   有关说明，请参阅启用 AWS IAM Identity Center中的 AWS IAM Identity Center 用户指南。

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

   有关使用教程 IAM Identity Center 目录 作为您的身份来源，请参阅使用默认设置配置用户访问权限 IAM Identity Center 目录中的 AWS IAM Identity Center 用户指南。

以具有管理访问权限的用户身份登录

- 要使用您的 Ident IAM ity Center 用户登录URL，请使用您在创建 Ident IAM ity Center 用户时发送到您的电子邮件地址的登录信息。

  有关使用IAM身份中心用户登录的帮助，请参阅登录 AWS 访问中的门户 AWS 登录 用户指南。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个遵循应用最低权限权限的最佳实践的权限集。

   有关说明，请参阅中的创建权限集 AWS IAM Identity Center 用户指南。

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，请参阅中的添加群组 AWS IAM Identity Center 用户指南。

关闭一个 AWS account

有关如何关闭的信息 AWS 账户，请参阅关闭账户。

使用的先决条件 AWS Supply Chain

在你创建之前 AWS Supply Chain 实例，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 设置一个 AWS account。
- 确保IAM身份中心已启用。要启用IAM身份中心，请参阅启用IAM身份中心。
- IAM身份中心实例必须在您要创建的同一区域激活 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）和欧洲（爱尔兰）区域。
- 您必须在 Ident IAM ity 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。
- 添加其他需要访问权限的用户 AWS Supply Chain 到IAM身份中心。
- 你需要 AWS Key Management Service (AWS KMS) 来创建实例。 AWS Supply Chain 用这个 AWS KMS key 对传入的所有数据进行加密 AWS Supply Chain。 有关信息 AWS KMS 密钥，请参阅创建密钥。

开始使用 AWS Supply Chain

在本节中，你可以学习如何创建 AWS Supply Chain 实例，授予用户权限角色，登录到 AWS Supply Chain Web 应用程序，并创建自定义用户权限角色。网络 ACL 和安全组都允许 (因此可到达您的实例) 的发起 ping 的 AWS 账户 最多可以有 10 个 AWS Supply Chain 处于活动状态或正在初始化状态的实例。

主题

使用 AWS Supply Chain Console

> **Note**
>
> 如果您的 AWS 账户是的成员账户 AWS 组织并包含服务控制策略 (SCP)，请确保组织SCP向成员账户授予以下权限。如果组织的SCP政策中未包含以下权限， 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以下内容的详细信息 AWS Supply Chain 你中的资源 AWS 账户。 如果您创建的基于身份的策略比所需的最低权限更严格，则控制台将无法按预期运行，适用于使用该策略的实体（用户或角色）。

您无需为仅拨打控制台的用户设置最低控制台权限 AWS CLI 或者 AWS API。相反，只允许访问与他们尝试执行的API操作相匹配的操作。

为确保用户和角色仍然可以使用 AWS Supply Chain 控制台，还要附上 AWS Supply Chain `ConsoleAccess` 或 `ReadOnly` AWS 针对实体的托管策略。有关更多信息，请参阅《用户指南》中的向IAM用户添加权限。

控制台管理员需要以下权限才能创建和更新 AWS Supply Chain 成功执行实例。

```
{
 "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:DescribeOrganization",
     "organizations:EnableAWSServiceAccess"
    ],
    "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:StartPeregrine",
    "sso:DescribeRegisteredRegions",
    "sso:ListDirectoryAssociations",
    "sso:GetPeregrineStatus",
    "sso:GetSSOStatus",
    "sso:ListProfiles",
    "sso:GetProfile",
    "sso:AssociateProfile",
    "sso:AssociateDirectory",
    "sso:RegisterRegion",
    "sso:StartSSO",
    "sso:CreateManagedApplicationInstance",
    "sso:DeleteManagedApplicationInstance",
    "sso:GetManagedApplicationInstance",
    "sso-directory:SearchUsers"
   ],
   "Resource": "*",
   "Effect": "Allow"
  }
 ]
}
```

key_arn 指定您要使用的密钥 AWS Supply Chain 实例。为了获得最佳实践，并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 (“*”)。

创建实例

> **Note**
>
> 只有 AWS Management Console 管理员可以创建实例。这些区域有： AWS Management Console 创建的管理员 AWS Supply Chain 实例应具有下面列出的所有权限使用 AWS Supply Chain Console。该管理员应邀请IAM用户作为 AWS Supply Chain 要管理的管理员 AWS Supply Chain.

要创建 AWS Supply Chain 实例，请按照以下步骤操作。

> **Note**
>
> 您最多可以在一个中创建 10 个实例 AWS 账户。 这 10 个实例包括活动实例和正在初始化实例。如果你已经激活了 Ident IAM ity Center（的继任者） AWS 单点登录），您必须创建自己的 AWS Supply Chain 同一个实例 AWS 区域 你在那里激活了IAM身份中心。 AWS Supply Chain 不支持跨区域的IAM身份中心呼叫。

1. 打开 AWS Supply Chain 控制台位于https://console.aws.amazon.com/scn/home。
2. 如有必要，请更改 AWS 区域。 在控制台窗口顶部的栏中，打开选择区域列表并选择一个区域。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。另请参阅《中的区域和终端节点》Amazon Web Services 一般参考.

   > **Note**
   >
   > 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。
   > AWS Supply Chain.

3. 在 AWS Supply Chain 控制面板，选择创建实例。
4. 在实例属性页面上，输入以下信息：
   - AWS 区域 -选择您已激活 “IAM身份中心” 的区域。要更改区域，请从右上角的下拉菜单中选择选择区域。创建实例后不能更改区域。
   - 名称 — 输入实例名称。
   - （可选）描述 — 输入实例的描述。
5. 在 下AWS KMS密钥，输入您的KMS密钥并使用以下内容更新您的KMS密钥策略：

> **Note**
>
> 作为应用程序管理员，当您将用户添加到 AWS Supply Chain 例如，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，请参阅用户权限角色。

> **Note**
>
> Replace（替换） *YourAccountNumber*, *Region*, *YourInstanceID*，以及 *YourKmsKeyArn* 和你的 AWS 账户, AWS 区域， AWS Supply Chain 实例 ID，以及 AWS KMS 钥匙。

```
{
"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"
                }

            }
        }
    ]
}
```

如果您没有KMS密钥，请选择 “创建” 以转到 AWS KMS 控制台，您可以在其中创建此密钥。使用之前的KMS密钥策略。有关如何创建KMS密钥的详细信息，请参阅中的创建密钥 AWS Key Management Service 开发者指南。

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

6. （可选）在实例标签下，选择添加新标签为您的实例分配标签。您可以使用这些标签标识实例。有关创建标签的信息，请参阅创建标签。
7. 选择创建实例。

   大约需要 2 到 3 分钟 AWS Supply Chain 待创建的实例。创建实例后，“状态” 字段位于 AWS Supply Chain 仪表板显示为 “活动”。
8. 一旦你的 AWS Supply Chain 实例已创建，请更新您的KMS策略以允许 AWS Supply Chain 访问你的 AWS KMS 钥匙。

> **Note**
>
> Replace（替换）*YourInstanceID* 和你的 AWS Supply Chain 实例 ID。您可以在上找到您的实例 ID AWS Supply Chain 控制台仪表板。

```
 {
    "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": "YourKmsKeyArn"
},
{
    "Sid": "Enable ASC to backfill KMS permissions",
    "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":"YourKmsKeyArn"
}
```

选择一个 AWS Supply Chain 应用程序所有者

作为 AWS 控制台管理员，你正在选择一个 AWS Supply Chain 应用程序所有者来管理 AWS Supply Chain Web 应用程序访问权限。这些区域有： AWS Supply Chain 应用程序所有者可以向中添加或删除用户权限角色 AWS Supply Chain 网络应用程序。

创建实例并连接身份源后，请按照以下步骤选择一个 AWS Supply Chain 应用程序所有者。

1. 在 AWS Supply Chain 控制台仪表板的 “应用程序所有者” 下，选择 “分配应用程序所有者”。
2. 在选择应用程序所有者下，选择将充当应用程序所有者的用户 AWS Supply Chain 应用程序所有者。您只能搜索用户名，并且仅显示符合搜索条件的用户。

   要添加更多用户，请选择前往IAM身份中心。有关添加用户的更多信息，请参阅在 Ident IAMity Center 中管理身份；有关用户权限角色的更多信息，请参阅用户权限角色。

   > **Note**
   >
   > 您一次只能从中添加一个用户 AWS Supply Chain 控制台。您无法在中添加群组作为应用程序所有者 AWS Supply Chain.

3. 选择发送邀请。

   在 AWS Supply Chain 控制台控制台，您将看到该用户列在 “应用程序所有者” 下。
4. 在中选择 “管理” AWS Supply Chain在中添加和删除用户 AWS Supply Chain 网络应用程序。

分配要访问的IAM群组 AWS Supply Chain

作为应用程序所有者或 AWS Supply Chain 管理员，您只能将身为 Identity C IAM enter 群组成员的用户添加到 AWS Supply Chain.

1. 在 AWS Supply Chain 控制台仪表板的 “群组” 下，选择 “分配群组”。

   此时将出现组页面。
2. 在群组名称下，选择拥有可以访问的用户的群组 AWS Supply Chain 然后选择 “分配”。

   您将在群组下方看到您添加的群组 AWS Supply Chain 仪表板。

3. 您可以选择 “管理群组” 在 Ident IAM ity Center 中添加新群组。在 Ident IAM ity Center 中添加群组后，该群组将列在 “群组名称” 下 AWS Supply Chain.

登录到 AWS 供应链 Web 应用程序

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

1. 你可以选择电子邮件中的链接，也可以在 AWS Supply Chain 控制台仪表板的 “子域” 下，选择 Web URL。

   这些区域有：AWS Supply Chain出现 Web 应用程序登录页面。
2. 输入 AWS IAM身份中心用户凭据，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 “开启你的队友” AWS Supply Chain页面上，选择您想要访问的用户 AWS Supply Chain 网络应用程序。选择邀请用户。有关信息 AWS Supply Chain 用户权限角色，请参阅用户权限角色。
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 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 仪表板。

更新你的个人资料

您可以随时通过以下网址更新您的账户和组织资料 AWS Supply Chain 网络应用程序。

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 应用程序控制面板，从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 应用程序控制面板，从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。

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

作为 AWS Supply Chain 管理员，您可以添加用户来访问 AWS Supply Chain 网络应用程序。请按照以下步骤添加用户。

1. 在 AWS Supply Chain 控制面板，从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. 选择添加新用户。

   此时将出现添加用户页面。
4. 在添加用户下拉菜单中，选择用户，然后在选择角色下，选择该用户的角色。
5. 选择添加。

更新用户权限

更新当前的用户权限角色 AWS Supply Chain 用户，请按照以下步骤操作。

1. 在 AWS Supply Chain 控制面板，从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， AWS Supply Chain 仪表板是自定义的。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，您可以从中删除用户 AWS Supply Chain 网络应用程序。请按照以下步骤删除删除用户。

1. 在 AWS Supply Chain 控制面板，从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，从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。

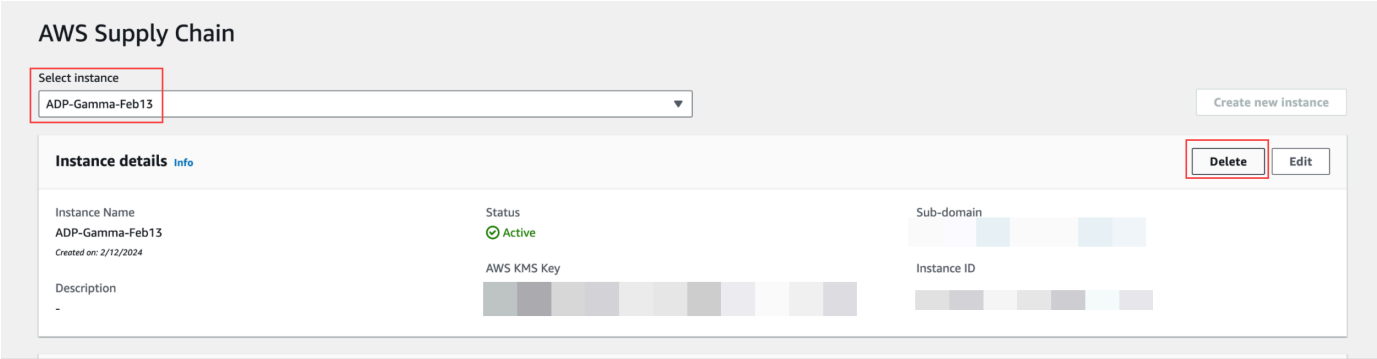
6. 在产品访问权限下，搜索产品（在搜索栏中键入），然后选择产品。
7. 选择保存。

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



3. 选择删除。
4. 关于删除 AWS Supply Chain 在 “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。

中的安全性 AWS Supply Chain

云安全位于 AWS 是最高优先级。作为 AWS 客户，您将受益于数据中心和网络架构 AWS 旨在满足大多数对安全敏感的组织的要求。

安全是您和您的共同责任 AWS。 责任共担模型将其描述为云的安全和云端的安全：

- 云安全 — AWS 负责保护运行的基础架构 AWS 服务 在 AWS Cloud. AWS 还为您提供可以安全使用的服务。作为安全措施的一部分，第三方审计师会定期测试和验证我们安全的有效性 AWS 合规计划。了解适用于以下方面的合规计划 AWS Supply Chain，请参阅 AWS 按合规计划划分的范围内的服务 。
- 云端安全 — AWS 服务 你使用的决定了你的责任。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。

本文档可帮助您了解在使用分担责任模型时如何应用分担责任模型 AWS Supply Chain。 以下主题向您展示了如何配置 AWS Supply Chain 以实现您的安全与合规目标。你还会学习如何使用其他 AWS 服务 帮助你监控和保护你的 AWS Supply Chain 资源的费用。

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对于 AWS Supply Chain
- 适用于 AWS Supply Chain 的 AWS 托管式策略
- AWS Supply Chain 的合规性验证
- AWS Supply Chain 中的故障恢复能力
- 日志记录和监控 AWS Supply Chain
- 管理 AWS Supply Chain 使用的事件 Amazon EventBridge

中的数据保护 AWS Supply Chain

这些区域有： AWS 分担责任模型适用于以下领域的数据保护 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设施 AWS Cloud。 您有责任保持对托管在此基础架构上的内容的控制。您还负责以下各项的安全配置和管理任务 AWS 服务 你用的。有关数据隐私的更多信息，

请参阅数据隐私FAQ。 有关欧洲数据保护的信息，请参阅 AWS 责任共担模型和GDPR博客文章 AWS 安全博客。

出于数据保护的目的，我们建议您进行保护 AWS 账户 凭据并使用设置个人用户 AWS IAM Identity Center 或者 AWS Identity and Access Management (IAM)。这样，每个用户只获得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)。
- 使用SSL/TLS与之通信 AWS 资源的费用。我们需要 TLS 1.2，建议使用 TLS 1.3。
- 使用API进行设置和用户活动记录 AWS CloudTrail。 有关使用 CloudTrail 轨迹捕获的信息 AWS 活动，请参阅使用中的 CloudTrail 轨迹 AWS CloudTrail 用户指南。
- 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。
- 如果您在访问时需要 FIPS 140-3 经过验证的加密模块 AWS 通过命令行界面或API，使用FIPS端点。有关可用FIPS端点的更多信息，请参阅联邦信息处理标准 (FIPS) 140-3。

我们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）。这包括你何时使用 AWS Supply Chain 或其他 AWS 服务 使用控制台，API， AWS CLI，或 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URL向外部服务器提供，我们强烈建议您不要在中包含凭据信息，URL以验证您对该服务器的请求。

数据由 AWS Supply Chain

限制特定用户的授权用户可以访问的数据 AWS 供应链实例，数据保存在其中 AWS 供应链由您隔离 AWS 账户 ID 和你的 AWS 供应链实例 ID。

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

我们可能会使用和存储由以下人员处理的您的内容 AWS Supply Chain，如AWS服务条款中所述。如果你想退出 AWS Supply Chain 要使用或存储您的内容，您可以在 Organizations 中创建退出政策。AWS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

分类为的联系人数据PII，或表示客户内容由以下用户存储的数据 AWS Supply Chain，使用有时间限制且特定于磁盘的密钥进行静态加密（也就是说，在将其放置、存储或保存到磁盘之前）AWS Supply Chain 实例。

Amazon S3 服务器端加密用于加密所有控制台和 Web 应用程序数据 AWS Key Management Service 每个客户账户独有的数据密钥。有关信息 AWS KMS keys，参见什么是 AWS Key Management Service？ 在 AWS Key Management Service 开发人员指南。

> **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进行加密 data-at-rest -。CMK

传输中加密

与之交换的数据 AWS 供应链在用户的网络浏览器和用户之间的传输中受到保护 AWS 供应链使用行业标准TLS加密。

密钥管理

AWS Supply Chain 部分支持 KMS-CMK。

有关更新AWSKMS密钥的信息，请参阅 AWS Supply Chain，请参阅 创建实例。

互联网络流量隐私

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

虚拟私有云 (VPC) 终端节点 AWS Supply Chain 是中的一个逻辑实体VPC，它只允许连接到 AWS Supply Chain。 将请求VPC路由到 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。

操作方法 AWS Supply Chain 将补助金用于 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 使用创建多个补助 AWS KMS CreateInstance操作期间传递的密钥。 AWS Supply Chain 通过向发送CreateGrant请求来代表您创建授权 AWS KMS。 补助金 AWS KMS 是用来给 AWS Supply Chain 访问 AWS KMS 输入客户账户。

> **Note**
>
> AWS Supply Chain 使用它自己的授权机制。将用户添加到 AWS Supply Chain，您不能使用拒绝列出同一个用户 AWS KMS 政策。

AWS Supply Chain 将补助金用于以下用途：

- 将GenerateDataKey请求发送至 AWS KMS 对存储在您的实例中的数据进行加密。
- 将解密请求发送至 AWS KMS 以便读取与实例关联的加密数据。
- 添加DescribeKeyCreateGrant、和RetireGrant权限，以便在将数据发送给其他人时确保数据安全 AWS 像 Amazon Forecast 这样的服务。

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。如果你这样做， AWS Supply Chain 将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 AWS CloudTrail `EncryptGenerateDataKey`、和的事件`Decrypt`用于监视调用的KMS 操作 AWS Supply Chain 要访问由您的客户托管密钥加密的数据，请执行以下操作：

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。

为接口端点创建端点策略

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
- 可以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对于 AWS Supply Chain

AWS Identity and Access Management (IAM) 是一个 AWS 服务 可帮助管理员安全地控制对以下内容的访问权限 AWS 资源的费用。IAM管理员控制谁可以进行身份验证（登录）和授权（拥有权限）才能使用 AWS Supply Chain 资源的费用。IAM是一个 AWS 服务 无需支付额外费用即可使用。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- 操作方法 AWS Supply Chain 与 IAM
- 基于身份的策略示例 AWS Supply Chain
- 故障排除 AWS Supply Chain 身份和访问权限

受众

你怎么用 AWS Identity and Access Management (IAM) 会有所不同，具体取决于你所做的工作 AWS Supply Chain.

服务用户-如果您使用 AWS Supply Chain 服务来完成您的工作，然后您的管理员会为您提供所需的凭证和权限。当你用得越多 AWS Supply Chain 功能才能完成工作，您可能需要其他权限。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。如果您无法访问中的功能 AWS Supply Chain，请参阅故障排除 AWS Supply Chain 身份和访问权限。

服务管理员-如果你负责 AWS Supply Chain 您公司的资源，您可能拥有完全访问权限 AWS Supply Chain。 你的工作是确定哪个 AWS Supply Chain 您的服务用户应访问的功能和资源。然后，您必须向IAM管理员提交更改服务用户权限的请求。查看此页面上的信息以了解的基本概念IAM。要详细了解贵公司可以如何IAM与 AWS Supply Chain，请参阅 操作方法 AWS Supply Chain 与 IAM。

IAM管理员-如果您是IAM管理员，则可能需要详细了解如何编写策略来管理访问权限 AWS Supply Chain。 查看示例 AWS Supply Chain 您可以在中使用的基于身份的策略IAM，请参阅。基于身份的策略示例 AWS Supply Chain

使用身份进行身份验证

身份验证是您登录的方式 AWS 使用您的身份凭证。您必须经过身份验证（登录到 AWS) 作为 AWS 账户根用户、以IAM用户身份或通过担任IAM角色来完成。

你可以登录 AWS 使用通过身份源提供的凭证作为联合身份。 AWS IAM Identity Center（IAM身份中心）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，您的管理员之前使用IAM角色设置了联合身份。当你访问时 AWS 通过使用联合，您就是在间接担任角色。

根据您的用户类型，您可以登录 AWS Management Console 或者 AWS 访问门户。有关登录的更多信息 AWS，请参阅如何登录您的 AWS 账户中的 AWS 登录 用户指南。

如果你访问 AWS 以编程方式， AWS 提供了一个软件开发套件 (SDK) 和一个命令行界面 (CLI)，用于使用您的凭证对您的请求进行加密签名。如果你不使用 AWS 工具，你必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅签名 AWS APIIAM用户指南中的请求。

无论使用何种身份验证方法，您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) 来提高帐户的安全性。要了解更多信息，请参阅中的多重身份验证 AWS IAM Identity Center《用户指南》和《使用多因素身份验证》(MFA) AWS（在 IAM 用户指南中）。

AWS 账户 根用户

当你创建 AWS 账户，您从一个登录身份开始，该身份可以完全访问所有人 AWS 服务 以及账户中的资源。这个身份叫做 AWS 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问。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。有关需要您以 root 用户身份登录的任务的完整列表，请参阅《用户指南》中的 “需要根用户凭据的IAM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进行访问 AWS 服务 通过使用临时证书。

联合身份是企业用户目录中的用户、Web 身份提供商、 AWS Directory Service、身份中心目录或任何访问的用户 AWS 服务 通过使用通过身份源提供的凭证。当联合身份访问时 AWS 账户，他们扮演角色，角色提供临时证书。

要进行集中访问管理，我们建议您使用 AWS IAM Identity Center。 您可以在 Ident IAM ity 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，以便在您的所有用户和群组中使用 AWS 账户 和应用程序。有关IAM身份中心的信息，请参阅什么是IAM身份中心？ 在 AWS IAM Identity Center 用户指南。

IAM 用户和组

IAM用户是你内心的身份 AWS 账户 对个人或应用程序具有特定权限。在可能的情况下，我们建议使用临时证书，而不是创建拥有密码和访问密钥等长期凭证的IAM用户。但是，如果您有需要IAM用户长期凭证的特定用例，我们建议您轮换访问密钥。有关更多信息，请参阅《IAM用户指南》中的定期轮换需要长期凭证的用例的访问密钥。

IAM群组是指定IAM用户集合的身份。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并授予该群组管理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》中的何时创建IAM用户（而不是角色）。

IAM角色

IAM角色是你内在的身份 AWS 账户 具有特定权限的。它与IAM用户类似，但与特定人员无关。你可以暂时扮IAM演一个角色 AWS Management Console 通过切换角色。你可以通过调用来扮演角色 AWS CLI 或者 AWS API操作或使用自定义URL。有关使用角色的方法的更多信息，请参阅《IAM用户指南》中的使用IAM角色。

IAM具有临时证书的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》中的为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需

要配置权限集。为了控制您的身份在进行身份验证后可以访问的内容，Ident IAM ity Center 会将权限集关联到中的IAM角色。有关权限集的信息，请参阅中的权限集 AWS IAM Identity Center 用户指南。

- 临时IAM用户权限-IAM 用户或角色可以代入一个IAM角色，为特定任务临时获得不同的权限。
- 跨账户访问-您可以使用IAM角色允许其他账户中的某人（受信任的委托人）访问您账户中的资源。角色是授予跨账户访问权限的主要方式。但是，有些 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）。要了解角色和基于资源的跨账户访问策略之间的区别，请参阅IAM用户指南IAM中的跨账户资源访问权限。
- 跨服务访问 — 一些 AWS 服务 使用其他功能 AWS 服务。 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，你被视为校长。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使用委托人的权限调用 AWS 服务，再加上请求的 AWS 服务 向下游服务发出请求。FAS只有当服务收到需要与其他服务进行交互的请求时，才会发出请求 AWS 服务 或需要完成的资源。在这种情况下，您必须具有执行这两个操作的权限。有关提出FAS请求时的政策详情，请参阅转发访问会话。
  - 服务角色-服务IAM角色是服务代替您执行操作的角色。IAM管理员可以在内部创建、修改和删除服务角色IAM。有关更多信息，请参阅创建角色以向某人委派权限 AWS 服务（在 IAM 用户指南中）。
  - 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。 该服务可以代替您执行操作。服务相关角色显示在您的 AWS 账户 并归该服务所有。IAM管理员可以查看但不能编辑服务相关角色的权限。
- 在 Amazon 上运行的应用程序 EC2 — 您可以使用IAM角色管理在EC2实例上运行的应用程序的临时证书 AWS CLI 或者 AWS API请求。这比在EC2实例中存储访问密钥更可取。要分配 AWS 在EC2实例上扮演角色并使其可供其所有应用程序使用，则可以创建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 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用IAM角色还是使用IAM用户，请参阅《用户指南》中的何时创建IAM角色（而不是IAM用户）。

使用策略管理访问

您可以控制访问权限 AWS 通过创建策略并将其附加到 AWS 身份或资源。策略是中的一个对象 AWS 当与身份或资源关联时，它定义了他们的权限。 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。大多数策略都存储在 AWS 作为JSON文件。有关JSON策略文档结构和内容的更多信息，请参阅《IAM用户指南》中的JSON策略概述。

管理员可以使用 AWS JSON用于指定谁有权访问什么的策略。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。要授予用户对其所需资源执行操作的权限，IAM管理员可以创建IAM策略。然后，管理员可以将IAM策略添加到角色中，用户可以代入这些角色。

IAM无论您使用何种方法执行操作，策略都会定义该操作的权限。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中获取角色信息 AWS Management Console，AWS CLI，或者 AWS API.

基于身份的策略

基于身份的策略是可以附加到身份（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用户指南中的创建IAM策略。

基于身份的策略可以进一步归类为内联策略或托管策略。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，您可以将其附加到您的多个用户、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或内联策略之间进行选择，请参阅《IAM用户指南》中的在托管策略和内联策略之间进行选择。

基于资源的策略

基于资源的JSON策略是您附加到资源的策略文档。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。你不能用 AWS 基于资源的策略IAM中的托管策略。

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。

亚马逊 S3， AWS WAF，Amazon VPC 就是支持的服务示例ACLs。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-权限边界是一项高级功能，您可以在其中设置基于身份的策略可以向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 是指定组织或组织单位 (OU) 的最大权限的JSON策略 AWS Organizations. AWS Organizations 是一项用于对多个进行分组和集中管理的服务 AWS 账户 你的企业拥有的。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限制了成员账户中实体的权限，包括每个 AWS 账户根用户。 有关 Organization SCPs s 和的更多信息，请参阅中的服务控制策略 AWS Organizations 用户指南。
- 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。要了解如何做 AWS 决定在涉及多种策略类型时是否允许请求，请参阅IAM用户指南中的策略评估逻辑。

操作方法 AWS Supply Chain 与 IAM

在使用管理IAM访问权限之前 AWS Supply Chain，了解哪些IAM功能可以与之配合使用 AWS Supply Chain.

IAM你可以使用的功能 AWS Supply Chain

IAM功能	AWS Supply Chain 支持
基于身份的策略	是
基于资源的策略	否

IAM功能	AWS Supply Chain 支持
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

要从更高层次的角度了解如何 AWS Supply Chain 和其他 AWS 服务适用于大多数IAM功能，请参阅 AWS 《IAM用户指南》IAM中与之配合使用的服务。

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用户指南中的创建IAM策略。

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。要了解可以在JSON策略中使用的所有元素，请参阅IAM用户指南中的IAMJSON策略元素参考。

基于身份的策略示例 AWS Supply Chain

查看以下示例 AWS Supply Chain 基于身份的策略，请参阅。基于身份的策略示例 AWS Supply Chain

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JSON策略是您附加到资源的策略文档。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.

要启用跨账户访问权限，您可以将整个账户或另一个账户中的IAM实体指定为基于资源的策略中的委托人。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状态时 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》IAM中的跨账户资源访问权限。

的政策行动 AWS Supply Chain

支持策略操作：是

管理员可以使用 AWS JSON用于指定谁有权访问什么的策略。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`Action`元素描述了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同名 AWS API操作。也有一些例外，例如没有匹配API操作的仅限权限的操作。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。

中的政策行动 AWS Supply Chain 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"
         ]
```

查看以下示例 AWS Supply Chain 基于身份的策略，请参阅。基于身份的策略示例 AWS Supply Chain

的政策资源 AWS Supply Chain

支持策略资源：是

管理员可以使用 AWS JSON用于指定谁有权访问什么的策略。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。

ResourceJSON策略元素指定要应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。最佳做法是，使用资源的 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": "*"
```

查看以下示例 AWS Supply Chain 基于身份的策略，请参阅。基于身份的策略示例 AWS Supply Chain

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用于指定谁有权访问什么的策略。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。

如果您在一条语句中指定多个Condition元素，或者在单个Condition元素中指定多个键， AWS 使用逻辑AND运算对其进行评估。如果您为单个条件键指定多个值， AWS 使用逻辑OR运算评估条件。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，只有在资源上标有IAM用户的用户名时，您才能向IAM用户授予访问该资源的权限。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。要查看全部 AWS 全局条件键，请参见 AWS 《IAM 用户指南》中的全局条件上下文密钥。

查看以下示例 AWS Supply Chain 基于身份的策略，请参阅。基于身份的策略示例 AWS Supply Chain

将临时证书与 AWS Supply Chain

支持临时凭证：是

一段时间 AWS 服务 使用临时证书登录时不起作用。欲了解更多信息，包括哪个 AWS 服务 使用临时证书，请参阅 AWS 服务 可以IAM在《IAM用户指南》中使用。

如果您登录，则使用的是临时证书 AWS Management Console 使用除用户名和密码之外的任何方法。例如，当你访问时 AWS 使用贵公司的单点登录 (SSO) 链接，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》中的切换到角色（控制台）。

您可以使用手动创建临时证书 AWS CLI 或者 AWS API。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，请参阅中的临时安全证书IAM。

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，你被视为校长。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使用委托人的权限调用 AWS 服务，再加上请求的 AWS 服务 向下游服务发出请求。FAS只有当服务收到需要与其他服务进行交互的请求时，才会发出请求 AWS 服务 或需要完成的资源。在这种情况下，您必须具有执行这两个操作的权限。有关提出FAS请求时的政策详情，请参阅转发访问会话。

的服务角色 AWS Supply Chain

支持服务角色：是

服务IAM角色是服务代替您执行操作的角色。IAM管理员可以在内部创建、修改和删除服务角色IAM。有关更多信息，请参阅创建角色以向某人委派权限 AWS 服务（在 IAM 用户指南中）。

> **Warning**
>
> 更改服务角色的权限可能会中断 AWS Supply Chain 功能。仅在以下情况下编辑服务角色 AWS Supply Chain 提供了执行此操作的指导。

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服务角色 AWS 服务。 该服务可以代替您执行操作。服务相关角色显示在您的 AWS 账户 并归该服务所有。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 AWS 服务 那可以用IAM。在表中查找服务相关角色列中包含 Yes 的表。选择是链接以查看该服务的服务相关角色文档。

基于身份的策略示例 AWS Supply Chain

默认情况下，用户和角色无权创建或修改 AWS Supply Chain 资源的费用。他们也无法使用AWS管理控制台、AWS命令行界面 (AWSCLI) 或AWSAPI。要授予用户对其所需资源执行操作的权限，IAM管理员可以创建IAM策略。然后，管理员可以将IAM策略添加到角色中，用户可以代入这些角色。

要了解如何使用这些示例策略文档创建IAM基于身份的JSON策略，请参阅IAM用户指南中的创建IAM策略。

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创建、访问或删除 AWS Supply Chain 您账户中的资源。这些操作可能会使您付出代价 AWS 账户。 创建或编辑基于身份的策略时，请遵循以下准则和建议：

- 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 AWS 为许多常见用例授予权限的托管策略。它们在你的 AWS 账户。 我们建议您通过定义来进一步减少权限 AWS 特定于您的用例的客户托管政策。有关更多信息，请参阅 AWS 托管策略或 AWS 《IAM用户指南》 中工作职能的托管策略。
- 应用最低权限权限-使用IAM策略设置权限时，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。有关使用应用权限IAM的更多信息，请参阅IAM用户指南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-您可以在策略中添加条件以限制对操作和资源的访问权限。例如，您可以编写一个策略条件来指定所有请求都必须使用发送SSL。如果通过特定条件使用服务操作，则也可以使用条件来授予对服务操作的访问权限 AWS 服务之外的压缩算法（ 例如 AWS CloudFormation。 有关更多信息，请参阅《IAM用户指南》中的IAMJSON策略元素：条件。
- 使用 A IAM ccess Analyzer 验证您的IAM策略以确保权限的安全性和功能性 — A IAM ccess Analyzer 会验证新的和现有的策略，以便策略符合IAM策略语言 (JSON) 和IAM最佳实践。IAMAccess Analyzer 提供了 100 多项策略检查和可行的建议，可帮助您制定安全和实用的策略。有关更多信息，请参阅《IAM用户指南》中的 IAMAccess Analyzer 策略验证。

- 需要多因素身份验证 (MFA)-如果您的场景需要IAM用户或 root 用户 AWS 账户，请打开MFA以提高安全性。要要求MFA何时调用API操作，请在策略中添加MFA条件。有关更多信息，请参阅《IAM用户指南》中的配置MFA受保护的API访问权限。

有关中最佳做法的更多信息IAM，请参阅《IAM用户指南》IAM中的安全最佳实践。

故障排除 AWS Supply Chain 身份和访问权限

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

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进入 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 如果您无权执行某项操作，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虚构*`my-example-widget`*资源的详细信息但没有虚构权限时，就会出现以下示例错误。`scn:`*`GetWidget`*

```
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

如果您收到一条错误消息，说您无权执行`iam:PassRole`操作，则必须更新您的策略以允许您将角色传递给 AWS Supply Chain.

一段时间 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尝试使用控制台在中执行操作时，会出现以下示例错误 AWS Supply Chain。 但是，该操作要求服务拥有由服务角色授予的权限。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 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，可以担任角色。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，请参阅操作方法 AWS Supply Chain 与 IAM。
- 要了解如何提供对您的资源的访问权限 AWS 账户 您拥有的，请参阅向其他IAM用户提供访问权限 AWS 账户 您在《IAM用户指南》中拥有的内容。
- 了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅提供访问权限 AWS 账户 《IAM用户指南》中由第三方所有。
- 要了解如何通过联合身份验证提供访问权限，请参阅《用户指南》中的向经过外部身份验证的用户提供访问权限（联合身份验证）。IAM
- 要了解使用角色和基于资源的策略进行跨账户访问的区别，请参阅IAM用户指南IAM中的跨账户资源访问权限。

适用于 AWS Supply Chain 的 AWS 托管式策略

AWS 托管式策略是由 AWS 创建和管理的独立策略。AWS 托管式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 托管式策略可能不会为您的特定使用场景授予最低权限，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 托管式策略中定义的权限。如果 AWS 更新在 AWS 托管式策略中定义的权限，则更新会影响该策略所附加到的所有主体身份（用户、组和角色）。当新的 AWS 服务启动或新的 API 操作可用于现有服务时，AWS 最有可能更新 AWS 托管式策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

AWS 托管式策略：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 用户和组的管理权限，并附加到 AWS Supply Chain 代表您创建的角色。不应将 AWSSupplyChainFederationAdminAccess 策略附加到任何其他 IAM 实体。

尽管此策略通过 scn:* 权限提供对 AWS Supply Chain 的所有访问权限，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，并且没有管理员 API 的权限。

权限详细信息

此策略包含以下权限：

- `Chime` — 提供在 Amazon Chime 应用程序实例下创建或删除用户的权限；提供管理渠道、渠道成员和版主的权限；提供向渠道发送消息的权限。Chime 操作的作用域为标记有“SCNInstanceId”的应用程序实例。
- `AWS IAM Identity Center (AWS SSO)` — 提供关联和取消关联用户资料以及列出与 IAM Identity Center 应用程序实例关联的资料所需的权限。
- `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。提供对具有资源库 arn:aws:s3:::aws-supply-chain-data-* 的存储桶的 GetBucketLocation、GetBucketPolicy、PutObject、GetObject 和 ListBucket 访问。
- `SecretsManager` — 提供创建机密和更新机密策略的权限。

- KMS — 为 Amazon AppFlow 服务提供列出密钥和密钥别名的权限。提供为标记有键值 aws-suply-chain-access : true 的 KMS 密钥的 DescribeKey、CreateGrant 和 ListGrants 权限；提供创建机密和更新机密策略的权限。

  权限（kms:ListKeys、kms:ListAliases、kms:GenerateDataKey 和 kms:Decrypt）不限于 Amazon AppFlow，这些权限可以授予账户中的任何 AWS KMS 密钥。

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

对 AWS 托管式策略的 AWS Supply Chain 更新

下表显示了对 AWS 托管式策略的 AWS Supply Chain 更新的详细信息（从该服务开始跟踪这些更改开始）。有关此页面更改的自动提示，请订阅 AWS Supply Chain 文档历史记录页面上的 RSS 源。

更改	描述	日期
AWSSupplyChainFederationAdminAccess — 更新了策略	AWS Supply Chain 更新了托管式策略，允许联合用户在 IAM Identity Center 中执行 ListProfileAssociations 操作。	2023 年 11 月 1 日
AWSSupplyChainFederationAdminAccess — 更新了策略	AWS Supply Chain 更新了托管式策略，允许联合用户在具有资源库 arn:aws:s3:::aws-supply- chain-data-* 的专用 S3 桶上执行 PutObject 和 GetObject 操作。	2023 年 9 月 21 日
AWSSupplyChainFederationAdminAccess — 新增了策略	AWS Supply Chain 增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

更改	描述	日期
AWS Supply Chain 开启了跟踪更改	AWS Supply Chain 为其 AWS 托管式策略开启了跟踪更改。	2023 年 3 月 1 日

AWS Supply Chain 的合规性验证

作为多个 AWS Supply Chain 合规性计划的一部分，第三方审核员将评估 AWS 的安全性和合规性。其中包括 SOC、PCI、FedRAMP、HIPAA 及其他。

有关特定合规性计划范围内的 AWS 服务 列表，请参阅合规性计划范围内的 AWS 服务。有关常规信息，请参阅 AWS 合规性计划。

您可以使用 AWS Artifact 下载第三方审计报告。有关更多信息，请参阅在 AWS Artifact 中下载报告。

您使用 AWS Supply Chain 的合规性责任取决于您数据的敏感度、您公司的合规性目标以及适用的法律法规。AWS 提供以下资源来帮助满足合规性：

- 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。
- 设计符合 HIPAA 安全性和合规性要求的架构白皮书 — 此白皮书介绍公司如何使用 AWS 创建符合 HIPAA 标准的应用程序。
- AWS 合规性资源 — 此业务手册和指南集合可能适用于您的行业和地点。
- 《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 — 此 AWS 服务 提供了 AWS 中安全状态的全面视图，可帮助您检查是否符合安全行业标准和最佳实践规范。

AWS Supply Chain 中的故障恢复能力

AWS 全球基础设施围绕 AWS 区域 和可用区构建。AWS 区域 提供多个物理分离和隔离的可用区。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故障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设施相比，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 全球基础设施之外，AWS Supply Chain 还提供了多种功能，以帮助支持您的数据弹性和备份需求。

日志记录和监控 AWS Supply Chain

日志记录和监控是维护可靠性、可用性和性能的重要组成部分 AWS 供应链和你的另一个 AWS 解决方案。 AWS 提供了 AWS CloudTrail 值得关注的监控工具 AWS 供应链，在出现问题时进行报告，并在适当时自动采取行动。

> **Note**
>
> APIs仅从中调用 AWS Supply Chain 控制台被捕捉到 AWS CloudTrail.

AWS CloudTrail捕获由您或代表您API拨打的电话和相关事件 AWS 账户 并将日志文件传输到您指定的 Amazon S3 存储桶。您可以识别哪些用户和账户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。你可以查看 AWS scn.amazonaws.com 下的供应链活动。有关更多信息，请参阅 。AWS CloudTrail 用户指南。

> **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，当您将用户添加到 AWS Supply Chain 例如，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，请参阅用户权限角色。

AWS Supply Chain 中的数据事件 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。

您可以记录以下的数据事件 AWS Supply Chain 使用 CloudTrail 控制台进行资源类型， AWS CLI，或 CloudTrail API操作。

- 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. 选择数据事件以记录数据事件。
  2. 从数据事件类型列表中，选择要为其记录数据事件的资源类型。
  3. 选择要使用的日志选择器模板。您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，或者创建自定义日志选择器模板来筛选`readOnly`、`eventName`、和`resources.ARN`字段。
- 要使用记录数据事件 AWS CLI，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。您可以添加条件来筛选`readOnly`、`eventName`、和`resources.ARN`字段的值。
  - 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，请参阅使用记录跟踪的数据事件 AWS CLI.
  - 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命令来更新现有的事件数据存储。有关更多信息，请参阅使用记录事件数据存储的数据事件 AWS CLI.

*您可以将高级事件选择器配置为在`eventName`、和`resources.ARN`字段上进行筛选`readOnly`，以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的资源执行的管理操作的信息 AWS account。这些也称为控制层面操作。默认情况下， CloudTrail 记录管理事件。

AWSSupply 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列出的名字是 AWS Supply Chain 代表联合用户的应用程序。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。 对这些内容的访问权限由APIs以下人员控制 AWS Supply Chain 基于联合用户角色权限的应用程序。你不应该试图控制对这些内容的访问APIs以防止干扰 AWS Supply Chain 应用程序。

用户角色

APIs以下内容用于管理用户、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
```

洞察

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以下内容用于 AWS Supply Chain 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以下内容用于 AWS Supply Chain 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
```

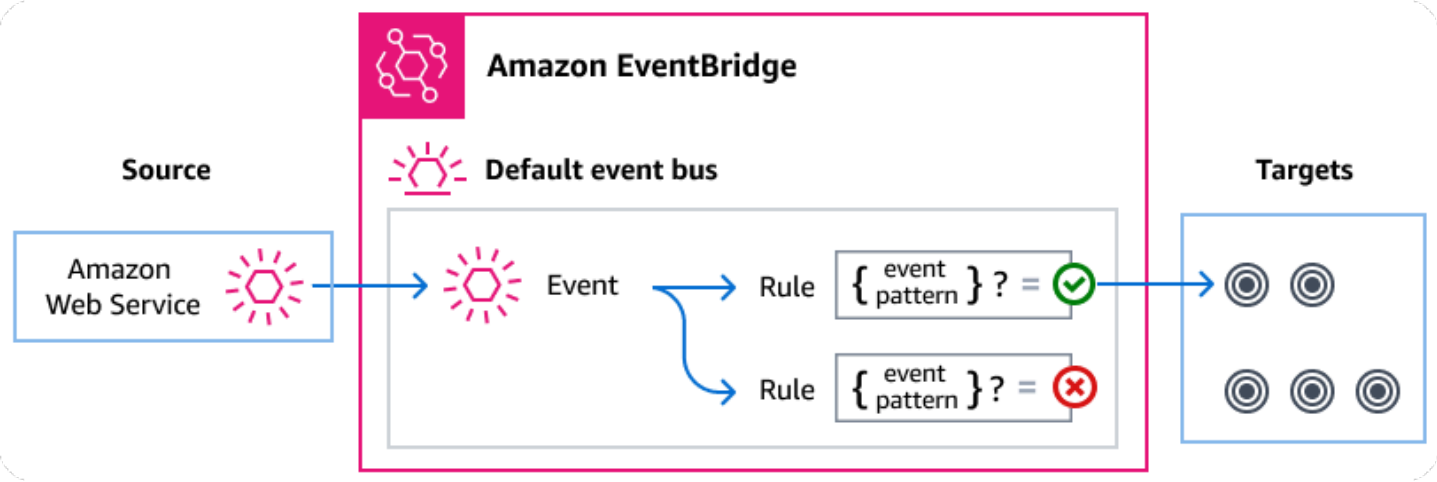
管理 AWS Supply Chain 使用的事件 Amazon EventBridge

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

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：

和许多人一样 AWS 服务， 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事件中自动配置 AWS 账户。）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 events
- 交付 AWS Supply Chain 使用的事件 EventBridge 规则
- AWS Supply Chain 事件详情参考

AWS Supply Chain events

AWS Supply Chain 将以下事件发送到默认值 EventBridge 自动执行事件总线。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。活动可能无法按顺序交付。

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

活动详情类型	描述
AWS供应链数据集成状态变更	显示每个已收录到的文件的状态 AWS Supply Chain.

交付 AWS Supply Chain 使用的事件 EventBridge 规则

要有 EventBridge 默认事件总线发送 AWS Supply Chain 事件到目标，则必须创建规则。每条规则都包含一个事件模式， EventBridge 与事件总线上收到的每个事件进行匹配。如果事件数据与指定的事件模式相匹配， EventBridge 将该事件传递给规则的目标。

有关创建事件总线规则的全面说明，请参阅中创建对事件做出反应的规则 EventBridge 用户指南。

创建匹配的事件模式 AWS Supply Chain events

每个事件模式都是一个包含以下内容的JSON对象：

- 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`事件相匹配 AWS Supply Chain:

```
{
```

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

有关编写事件模式的更多信息，请参阅中的事件模式 EventBridge 用户指南。

AWS Supply Chain 事件详情参考

所有活动来自 AWS 服务有一组通用的字段，其中包含有关事件的元数据，例如 AWS 服务，即事件的来源、事件的生成时间、事件发生的账户和地区等。有关这些常规字段的定义，请参阅中的事件结构参考 Amazon EventBridge 用户指南。

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。下面的参考文献定义了各种详细信息字段 AWS Supply Chain 事件。

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

- 所有事件的`source`字段 AWS Supply Chain 设置为`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。

有关构造使规则匹配的事件模式的信息 AWS Supply Chain 事件，请参阅中的事件模式 Amazon EventBridge 用户指南。

有关活动及其方式的更多信息 EventBridge 处理它们，请参阅 Amazon EventBridge中的事件 Amazon EventBridge 用户指南。

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，每个限额是区域特定的。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
账户中每个实例的见解关注列表 AWS	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

常见问题 (FAQs)

以下信息可以帮助您解决在启用 Ident IAM ity 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？	IAMIdentity Center 是IAM其中的一项功能，用于管理身份源的同步。IAM身份中心是的身份来源 AWS Supply Chain 实例。您需要配置 Ident IAM ity Center 才能设置 AWS 控制台和 AWS Supply Chain 网络应用程序。有关 Ident IAM ity Center 的更多信息，请参阅启用 AWS IAM身份中心位于 AWS IAM Identity Center 用户指南。
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，您可以启用IAM身份中心访问权限 AWS 账户。例如，如果您的IAM身份中心未在同一版本中启用 AWS 账户作为 AWS Supply Chain 实例账户。有关创建组织 Ident IAM ity Center 实例的好处的更多信息，请参阅中的 Ident IAMity Center 的组织实例 AWS IAM Identity Center 用户指南。
为什么需要委派管理员权限 AWS Supply Chain?	无需委派管理员即可使用 AWS Supply Chain 但这是最佳实践 AWS 组织设置以限制对组织管理帐户的访问权限并管理 Ident IAM ity Center。有关更多信息，请参阅 “委托管理员转子” AWS 组织。 。 创建组织实例时，请确保将用于创建组织实例的账户 AWS Supply Chain 实例与 Ident IAM ity Center 账户属于同一个组织。确保已启用创建实例所需的权限，然后您就可以创建一个 AWS Supply Chain 实例与IAM身份中心账户位于同一区域。有关创建所需权限的信息 AWS Supply Chain 实例，请参阅开始使用 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：

- 如果你有 AWS Support 帐户，前往 Supp ort Center 并提交工单。
- 打开 AWS Management Console然后选择 AWS 供应链、Su pport、C reate case。

提供以下信息会有帮助：

- 您的 AWS 供应链实例 ID/ ARN。
- 您的 AWS 区域。
- 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
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-chain-data-* 访问 PutObject 和 GetObject 操作专用的 Amazon S3 存储桶。	2023 年 9 月 21 日
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	2023 年 9 月 7 日

	AWS Supply Chain ations 上使用或存储您的内容。	
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。