aws

用户指南

AWS Artifact

AWS Artifact: 用户指南

Table of Contents

什么是 AWS Artifact？

AWS Artifact 提供按需下载 AWS 安全与合规性文档。例如，关于遵守国际标准化组织 (ISO) 标准和支付卡行业 (PCI) 安全标准的报告，以及系统和组织控制 (SOC) 报告。 AWS Artifact 还提供认证机构的认证下载，用于验证 AWS 安全控制措施的实施和运作有效性。

借 AWS Artifact助，您还可以为在其上销售产品的独立软件供应商 (ISVs) 下载安全与合规性文档 AWS Marketplace。有关更多信息，请参阅AWS Marketplace 供应商见解。

此外，您还可以使用 AWS Artifact 来查看、接受和跟踪您与 AWS 您的组织 AWS 账户 中的多人签订的协议的状态。 AWS 账户 有关中协议的更多信息 AWS Artifact，请参阅管理中的协议 AWS Artifact。

为了证明您使用的 AWS 基础设施和服务的安全性和合规性，您可以将 AWS Artifact 文件作为审计对象提交给审计师或监管机构。您还可以使用这些审计工件作为指导来评估自己的云架构并评估公司内部控制的有效性。有关审计对象的更多信息，请参阅AWS Artifact FAQs。

> **Note**
>
> AWS 客户有责任编写或获取证明其公司的安全性和合规性的文档。有关更多信息，请参阅责任共担模式。

定价

AWS 免费为您提供 AWS Artifact 文件和协议。

入门 AWS Artifact

要开始使用 AWS Artifact，请在 AWS Artifact 控制台中试用其主要功能。在控制台中，您可以下载 AWS 安全与合规报告，下载并接受法律协议，以及订阅有关 AWS Artifact 文档的通知。

先决条件

要使用的功能 AWS Artifact，您必须具有 AWS 账户。有关设置说明，请参阅《AWS 安装用户指南》AWS 账户中的设置新。

功能

有关使用功能的说明 AWS Artifact，请参阅以下主题：

- 下载报告
- 管理协议
- 配置通知

正在下载报告 AWS Artifact

您可以从 AWS Artifact 控制台下载报告。当您从中下载报告时 AWS Artifact，该报告是专门为您生成的，并且每份报告都有一个唯一的水印。因此，您应该仅与信任的人员共享报告。不要将报告作为电子邮件附件发送，也不要联机共享。要共享报告，请使用诸如 Amazon 之类的安全共享服务 WorkDocs。有些报告要求您先接受条款和条件，然后才能下载这些报告。

内容

下载报告

要下载报告，您必须具有所需的权限。有关更多信息，请参阅 中的身份和访问管理 AWS Artifact。

当您注册时 AWS Artifact，您的账户会自动获得下载某些报告的权限。如果您在访问时遇到问题 AWS Artifact，请按照AWS Artifact 服务授权参考页面上的指导进行操作。

下载报告

1. 打开 AWS Artifact 控制台，网址为https://console.aws.amazon.com/artifact/。
2. 在 AWS Artifact 主页上，选择查看报告。

   在 “报告” 页面的 “AWS 报告” 选项卡上，您可以访问 AWS 报告（例如，SOC1/2/3 PCI、C5 等）。在 “第三方报告” 选项卡上，您可以访问销售其产品的独立软件供应商 (ISVs) 的报告 AWS Marketplace。
3. （可选）要查找报告，请在搜索字段中输入关键字。您还可以根据各个列（包括报告标题、类别、系列和描述）对报告执行有针对性的搜索。例如，要查找云计算合规性控制目录 (C5) 报告，可以使用 “标题”、“包含” 运算符 (:) 和术语 “C5” () 搜索标题列。`Title : C5`
4. （可选）有关报告的更多信息，请选择报告的标题以打开其详细信息页面。
5. 选择一个报告，然后选择 下载报告。
6. 系统可能会提示您接受正在下载的特定报告的条款和条件（接受下载报告的条款）。我们建议您仔细阅读条款和条件。阅读完毕后，选择 “我已阅读并同意条款”，然后选择 “接受条款并下载报告”。

7. 通过PDF查看器打开下载的文件。查看验收条款和条件，然后向下滚动以查找审计报告。报告可能会在PDF文档中以附件形式嵌入其他信息，因此请务必检查PDF文件中的附件以获取支持文档。有关如何查看附件的说明，请参阅查看PDF文档中的附件。

查看PDF文档中的附件

我们建议使用以下目前支持查看PDF附件的应用程序：

Adobe Acrobat

从 Adobe 网站下载最新版本的 Adobe Acrobat Reader，网址为。https://get.adobe.com/reader/

有关如何在 Acrobat Reader 中查看PDF附件的说明，请参阅 Adobe Supp ort 网站PDFs上的链接和附件。

Firefox 浏览器

1. 从 Mozilla 网站下载最新的 Firefox 网络浏览器，网址为 https://www.mozilla。 org/en-US/firefox/new/。
2. 在 Firefox 的内置PDF查看器中打开PDF文件。有关说明，请参阅在 Firefox 中查看PDF文件或在 Mozilla Support 网站上选择其他查看器。
3. 要在 Firefox 的内置PDF查看器中查看PDF附件，请选择 “切换边栏”、“显示附件”。

保护您的文档

AWS Artifact 文件是机密的，应始终保持安全。 AWS Artifact 为其文档使用 AWS 分担责任模型。这意味着 AWS 它负责确保文档在 AWS 云端时的安全，但您有责任在下载文档后确保它们的安全。 AWS Artifact 可能需要您先接受条款和条件，然后才能下载文档。每个下载的文档都有一个可追踪的唯一水印。

仅允许您在公司内部、与您的监管机构和审计人员共享标记为机密的文档。不允许您与您的客户或在您的网站上共享这些文档。我们强烈建议您使用安全的文档共享服务（例如 Amazon WorkDocs）与他人共享文档。请勿通过电子邮件发送文档，也不要将其上传到不安全的网站。

问题排查

如果您无法下载文档或收到错误消息，请参阅中的疑难解答 AWS Artifact FAQ。

管理中的协议 AWS Artifact

您可以使用 AWS Artifact 来查看和管理您 AWS 账户 或组织的协议。例如，受《健康保险流通与问责法》(HIPAA) 约束的公司通常需要与之签订商业伙伴附录 (BAA) 协议， AWS 以确保受保护的健康信息 (PHI) 得到适当的保护。在 AWS Artifact 控制台中，您可以查看和接受此类协议，也可以指定 AWS 账户 可以合法处理的协议PHI。

如果您使用 AWS Organizations，则可以代表组织 AWS 账户 中的所有人接受协议 AWS，例如BAA与。协议自动涵盖所有现有和后续的成员账户，并且可以合法处理PHI。

您还可以使用 AWS Artifact 来确认您 AWS 账户 或组织已接受协议，并查看已接受协议的条款以了解您的义务。如果您的账户或组织不再需要使用已接受的协议，则可以使用终 AWS Artifact 止协议。如果您终止了协议，但后来意识到自己需要它，则可以再次激活该协议。

内容

为你 AWS 账户 接受协议 AWS Artifact

您可以使用 AWS Artifact 控制台来查看和接受与 AWS 您的协议 AWS 账户。

> **Important**
>
> 在接受协议之前，我们建议您咨询法务、隐私和合规性团队。

所需的权限

如果您是账户管理员，则可以向IAM用户和联合用户授予访问和管理您的一项或多项协议的权限。默认情况下，仅具有管理权限的用户能够接受协议。要接受协议IAM，联合用户必须具有所需的权限。

有关更多信息，请参阅 中的身份和访问管理 AWS Artifact。

接受与的协议 AWS

1. 打开 AWS Artifact 控制台，网址为https://console.aws.amazon.com/artifact/。
2. 在 AWS Artifact 导航窗格上，选择协议。
3. 选择 Account agreements (账户协议) 选项卡。
4. 打开 AWS Artifact 控制台，网址为https://console.aws.amazon.com/artifact/。
5. 在导航窗格中，选择 “协议”。
6. 在 “协议” 页面上，执行以下任一操作：
   - 要仅接受您的账户的协议，请选择账户协议选项卡。
   - 要代表您的组织接受协议，请选择组织协议选项卡。
7. 选择协议，然后选择 “下载协议”。

   将出现 “接受NDA下载报告” 对话框。
8. 在下载所选协议之前，必须先接受 AWS Artifact 保密协议的条款 (AWS Artifact NDA)。

   a. 在 “接受NDA下载报告” 对话框中，查看 AWS Artifact NDA。
   b. （可选）要打印副本 AWS Artifact NDA（或将其另存为PDF），请选择 “打印” NDA。
   c. 选择 “我已阅读并同意” 的所有条款NDA。
   d. 要接受 AWS Artifact NDA并下载您选择PDF的协议，请选择接受NDA并下载。
9. 在PDF查看器中，查看您下载PDF的协议。
10. 在 AWS Artifact 控制台中，选择协议，选择接受协议。
11. 在 “接受协议” 对话框中，执行以下操作：

    a. 查看协议。
    b. 选择我同意所有这些条款和条件。
    c. 选择接受协议。
12. 选择 接受 以接受您账户的协议。

为您 AWS 账户 终止协议 AWS Artifact

如果您使用 AWS Artifact 控制台接受单曲协议 AWS 账户，则可以使用控制台终止该协议。否则，请参阅中的离线协议 AWS Artifact。

所需的权限

要终止协议IAM，联合用户必须具有所需的权限。

有关更多信息，请参阅 中的身份和访问管理 AWS Artifact。

终止您的在线协议 AWS

1. 打开 AWS Artifact 控制台，网址为https://console.aws.amazon.com/artifact/。
2. 在 AWS Artifact 导航窗格上，选择协议。
3. 选择 Account agreements (账户协议) 选项卡。
4. 选择协议并选择 终止协议。
5. 选中所有复选框以表示您同意终止协议。
6. 选择 Terminate (终止)。当系统提示您确认时，选择终止。

接受贵组织的协议 AWS Artifact

如果您是组织管理账户的所有者，则可以代表 AWS Organizations 组织 AWS 账户 中的所有人接受与 AWS 之达成的协议。

> **Important**
>
> 在接受协议之前，我们建议您咨询法务、隐私和合规性团队。

AWS Organizations 有两个可用的功能集：整合账单功能和所有功能。要 AWS Artifact 用于您的组织，您所属的组织必须启用所有功能。如果仅针对整合账单配置了您的组织，请参阅AWS Organizations 用户指南中启用组织中的所有功能。

要接受或终止组织协议，您必须使用正确的 AWS Artifact 权限登录管理账户。拥有`organizations:DescribeOrganization`权限的成员账户的用户可以查看代表他们接受的组织协议。

有关更多信息，请参阅《AWS Organizations 用户指南》 AWS Organizations中的使用管理组织中的账户。

所需的权限

要接受协议，管理账户的所有者必须具有所需的权限。

有关更多信息，请参阅 中的身份和访问管理 AWS Artifact。

接受组织的协议

1. 打开 AWS Artifact 控制台，网址为https://console.aws.amazon.com/artifact/。
2. 在 AWS Artifact 控制面板上，选择协议。
3. 选择 Organization agreements (组织协议) 选项卡。
4. 打开 AWS Artifact 控制台，网址为https://console.aws.amazon.com/artifact/。
5. 在导航窗格中，选择 “协议”。
6. 在 “协议” 页面上，执行以下任一操作：
   - 要仅接受您的账户的协议，请选择账户协议选项卡。
   - 要代表您的组织接受协议，请选择组织协议选项卡。
7. 选择协议，然后选择 “下载协议”。

   将出现 “接受NDA下载报告” 对话框。
8. 在下载所选协议之前，必须先接受 AWS Artifact 保密协议的条款 (AWS Artifact NDA)。

   a. 在 “接受NDA下载报告” 对话框中，查看 AWS Artifact NDA。
   b. （可选）要打印副本 AWS Artifact NDA（或将其另存为PDF），请选择 “打印” NDA。
   c. 选择 “我已阅读并同意” 的所有条款NDA。
   d. 要接受 AWS Artifact NDA并下载您选择PDF的协议，请选择接受NDA并下载。
9. 在PDF查看器中，查看您下载PDF的协议。
10. 在 AWS Artifact 控制台中，选择协议，选择接受协议。
11. 在 “接受协议” 对话框中，执行以下操作：

    a. 查看协议。
    b. 选择我同意所有这些条款和条件。
    c. 选择接受协议。
12. 选择 “接受” 以接受组织中所有现有和 future 账户的协议。

终止贵组织的协议 AWS Artifact

如果您使用 AWS Artifact 控制台代表组织中的所有成员账户接受协议 AWS Organizations，则可以使用控制台终止该协议。否则，请参阅中的离线协议 AWS Artifact。

如果从组织中删除成员帐户，则该成员帐户将不再受组织协议的保护。在从组织中删除成员账户之前，管理账户管理员应将此信息传达给成员账户，以便他们可以在必要时签订新的协议。您可以在 AWS Artifact 控制台的 “协议” 页面的 “组织协议” 下查看有效的组织协议列表。

有关更多信息 AWS Organizations，请参阅《AWS Organizations 用户指南》中的使用管理组织 AWS Organizations中的账户。

所需的权限

要终止协议，管理账户的所有者必须具有所需的权限。

有关更多信息，请参阅 中的身份和访问管理 AWS Artifact。

终止您的在线组织协议 AWS

1. 打开 AWS Artifact 控制台，网址为https://console.aws.amazon.com/artifact/。
2. 在 AWS Artifact 控制面板上，选择协议。
3. 选择 Organization agreements (组织协议) 选项卡。
4. 选择协议并选择 终止协议。
5. 选中所有复选框以表示您同意终止协议。
6. 选择 Terminate (终止)。当系统提示您确认时，选择终止。

中的离线协议 AWS Artifact

如果您已有脱机协议，则 AWS Artifact 会显示您脱机接受的协议。例如，控制台可能会显示处于活动状态的离线业务伙伴附录 (BAA)。该活动状态表示已接受协议。要终止离线协议，请参阅协议中包含的终止指南和说明。

如果您的账户是 AWS Organizations 组织中的管理账户，则可以使用 AWS Artifact 将离线协议的条款应用于组织中的所有账户。要将离线接受的协议应用于您的组织和组织中的所有账户，您必须拥有所需的权限。

如果您的账户是组织中的成员账户，则必须具有查看离线组织协议的权限。

有关更多信息，请参阅 中的身份和访问管理 AWS Artifact。

在中配置电子邮件通知 AWS Artifact

您可以使用 AWS Artifact 控制台为中的协议和报告更新配置电子邮件通知 AWS Artifact。 AWS Artifact 使用发送这些电子邮件通知 AWS 用户通知服务。要接收 AWS Artifact 电子邮件通知，必须先在 用户通知服务 控制台中选择 AWS 用户通知服务 通知中心。然后，在 AWS Artifact 控制台中，您可以为通知设置创建配置，在其中指定您的通知收件人以及他们将收到哪些通知。

要配置 AWS Artifact 电子邮件通知，您必须拥有 AWS Artifact 和所需的权限 AWS 用户通知服务。有关更多信息，请参阅 中的身份和访问管理 AWS Artifact。

内容

先决条件：在中选择通知中心 用户通知服务

在接收 AWS Artifact 电子邮件通知之前，必须先打开 用户通知服务 控制台，然后在要存储 用户通知服务 数据的 AWS 区域 位置选择通知中心。需要选择通知中心 AWS 用户通知服务，通知中心 AWS Artifact 用于发送通知。

选择通知中心

1. 打开 AWS 用户通知服务 控制台的通知中心页面。
2. 在您要存储 AWS 用户通知服务 资源的 AWS 区域 位置中选择通知中心。默认情况下，您的 用户通知服务 数据存储在美国东部（弗吉尼亚北部）区域。 用户通知服务 会将您的通知数据复制到您选择的其他区域。有关更多信息，请参阅《AWS 用户通知服务 用户指南》中的通知中心文档。
3. 选择 保存并继续。

为 AWS Artifact 通知设置创建配置

选择 用户通知服务 通知中心后，可以在 AWS Artifact 控制台中为通知设置创建配置。在您创建的配置中，您可以指定要接收 AWS Artifact 通知的收件人电子邮件地址。您还可以指定这些收件人应接收有关哪些更新的通知，例如 AWS Artifact 协议更新和所有（或一部分） AWS Artifact 报告的更新。

创建配置

1. 打开 AWS Artifact 控制台的通知设置页面。
2. 选择创建配置。
3. 在创建配置页面上，执行以下操作：
   - 要接收协议通知，请在协议下选择 AWS 协议更新。
   - 要接收报告通知，请在报告下选择 AWS 报告更新。
     a. 要接收所有报告的通知，请选择所有报告。
     b. 要仅接收特定类别和系列下的报告的通知，请选择报告子集。然后，选择您感兴趣的类别和系列。
   - 在配置名称下，输入配置的名称。
   - 在 “电子邮件” 下的 “收件人” 中，输入要接收 AWS Artifact 通知电子邮件的电子邮件地址列表，以逗号分隔。
   - （可选）要向通知配置添加标签，请展开标签，选择添加新标签，然后以键值对的形式输入标签。有关为 用户通知服务 资源添加标签的更多信息，请参阅AWS 用户通知服务 用户指南中的为AWS 用户通知服务 资源添加标签。
   - 选择创建配置。

     用户通知服务 向您提供的每个收件人电子邮件地址发送一封验证电子邮件。要验证电子邮件地址，收件人必须在验证电子邮件中选择 “验证电子邮件”。只有经过验证的电子邮件地址才会收到 AWS Artifact 通知。

编辑 AWS Artifact 通知设置的配置

为 AWS Artifact 通知设置创建配置后，您可以随时编辑配置以更改通知设置。例如，要添加或删除收件人，请更改他们收到的通知类型，以及添加或删除标签。

编辑配置

1. 打开 AWS Artifact 控制台的通知设置页面。
2. 选择要编辑的配置。
3. 选择编辑。
4. 编辑任何配置选项和字段。完成后，选择保存更改。

如果您已将新的电子邮件地址添加为通知收件人，则 AWS 用户通知服务 会向这些电子邮件地址发送一封验证电子邮件。要验证电子邮件地址，收件人必须在验证电子邮件中选择 “验证电子邮件”。只有经过验证的电子邮件地址才会收到 AWS Artifact 通知。

删除 AWS Artifact 通知设置的配置

如果您不再需要为 AWS Artifact 通知设置创建的配置，则可以在 AWS Artifact 控制台中删除该配置。

删除配置

1. 打开 AWS Artifact 控制台的通知设置页面。
2. 选择要删除的配置。
3. 选择删除。
4. 在 “删除配置” 对话框中，选择 “删除”。

中的身份和访问管理 AWS Artifact

注册时 AWS，您需要提供与您的 AWS 帐户关联的电子邮件地址和密码。这些是您的根证书，可让您完全访问您的所有 AWS 资源，包括的资源 AWS Artifact。但是，我们强烈建议不要使用根账户进行日常访问。我们还建议您不要与他人共享账户凭证，因为这样会让他们获得您账户的完全访问权。

与其使用根凭证登录您的 AWS 账户或与他人共享您的证书，不如为自己和可能需要访问文档或协议的任何人创建一个名为IAM用户的特殊用户身份 AWS Artifact。利用这种方法，您可以为每个用户提供单独的登录信息，并且您可以向每个用户只授予他们使用特定文档时所需的权限。您也可以通过向 IAM 组授予权限并将 IAM 用户添加到组来向多个 IAM 用户授予相同权限。

如果您已经在外部管理用户身份 AWS，则可以使用IAM身份提供商而不是创建IAM用户。有关更多信息，请参阅《IAM用户指南》中的身份提供商和联合。

内容

向用户授予访问权限 AWS Artifact

完成以下步骤， AWS Artifact 根据用户所需的访问权限级别向他们授予权限。

任务

步骤 1：创建 IAM 策略

作为IAM管理员，您可以创建授予 AWS Artifact 操作和资源权限的策略。

创建 IAM策略

使用以下过程创建可用于向IAM用户和组授予权限的IAM策略。

1. 打开IAM控制台，网址为https://console.aws.amazon.com/iam/。
2. 在导航窗格中，选择策略。
3. 选择创建策略。
4. 选择JSON选项卡。
5. 输入策略文档。您可以创建自己的策略，也可以使用 的IAM策略示例 AWS Artifact 中的策略之一。
6. 请选择Review Policy（查看策略）。策略验证程序将报告任何语法错误。
7. 在查看策略页面上，输入一个唯一的名称，该名称可帮助您记住策略的用途。您还可以提供描述。
8. 选择创建策略。

步骤 2：创建IAM群组并附加策略

作为IAM管理员，您可以创建一个群组并将您创建的策略附加到该群组。您可以随时向群组中添加IAM用户。

创建IAM群组并附加您的策略

1. 在导航窗格中，选择组，然后选择创建新组。
2. 对于 组名称，为您的组键入一个名称，然后选择 下一步。
3. 在搜索框中，键入创建的策略的名称。选中策略的复选框，然后选择 下一步。
4. 审核组名称和策略。如果您已准备好，请选择 创建组。

步骤 3：创建IAM用户并将其添加到群组

作为IAM管理员，您可以随时向群组中添加用户。这会向用户授予该组的权限。

创建IAM用户并将该用户添加到群组

1. 在导航窗格中，选择用户，然后选择添加用户。
2. 对于用户名，输入一个或多个用户的姓名。

3. 选中 AWS Management Console access（管理控制台访问）旁边的复选框。配置自动生成的密码或自定义密码。您可以选择性地选择用户必须在下次登录时创建新密码，以便在用户首次登录时要求重置密码。
4. 选择下一步: 权限。
5. 选择 将用户添加到组，然后选择您创建的组。
6. 选择 Next: Tags（下一步: 标签）。您可以选择性地为用户添加标签。
7. 选择 下一步: 审核。如果您已准备好，请选择 创建用户。

将报告迁移到细粒度权限 AWS Artifact

现在，您可以对使用精细权限。 AWS Artifact通过这些细粒度的权限，您可以精细控制提供对诸如接受条款和下载报告等功能的访问权限。

要通过细粒度权限访问报告，您可以使用托AWSArtifactReportsReadOnlyAccess管策略或根据以下建议更新权限。如果您之前选择不使用细粒度权限，则应使用报告控制台中提供的 “选择加入Artif AWS actic 报告的细粒度权限” 链接来选择加入。

如果更新到新权限时出现问题，您可以选择通过控制台中的 “选择退出 Arti AWS fact 报告的精细权限” 链接使用旧权限访问报告。

将报告迁移到新权限

迁移非资源特定权限

将包含旧权限的现有策略替换为包含细粒度权限的策略。

遗留政策：

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "artifact:Get"
        ],
        "Resource": [
            "arn:aws:artifact:::report-package/*"
        ]
```

```
    }]
}
```

具有细粒度权限的新策略：

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "artifact:ListReports",
            "artifact:GetReportMetadata",
            "artifact:GetReport",
            "artifact:GetTermForReport"
        ],
        "Resource": "*"
    }]
}
```

迁移资源特定权限

将包含旧权限的现有策略替换为包含细粒度权限的策略。报告资源通配符权限已被条件键取代。

遗留政策：

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "artifact:Get"
        ],
        "Resource": [
            "arn:aws:artifact:::report-package/Certifications and Attestations/SOC/*",
            "arn:aws:artifact:::report-package/Certifications and Attestations/PCI/*",
            "arn:aws:artifact:::report-package/Certifications and Attestations/ISO/*"
        ]
    }]
}
```

具有精细权限和条件密钥的新策略：

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "artifact:ListReports"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "artifact:GetReportMetadata",
                "artifact:GetReport",
                "artifact:GetTermForReport"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "artifact:ReportSeries": [
                        "SOC",
                        "PCI",
                        "ISO"
                    ],
                    "artifact:ReportCategory": [
                        "Certifications and Attestations"
                    ]
                }
            }
        }
    ]
}
```

迁移到 Artifact 协议的精细权限 AWS

AWSArtifact 现在允许客户对协议使用细粒度的权限。通过这些细粒度的权限，客户可以精细控制访问功能，例如查看和接受保密协议，以及接受和终止协议。

要通过细粒度权限访问协议，您可以使用AWSArtifactAgreementsReadOnlyAccess或AWSArtifactAgreementsFullAccess托管策略或根据以下建议更新您的权限。如果您之前选择不使用细粒度权限，则应使用协议控制台中提供的 “选择加入Artif AWS act协议的细粒度权限” 链接来选择加入。

如果更新到新权限时出现问题，您可以选择通过控制台中的 “选择退出 Artif AWS act 协议的细粒度权限” 链接访问具有旧权限的协议。

迁移到新权限

旧版IAM操作 “DownloadAgreement” 已被用于下载未接受协议的 GetAgreement “” 操作和用于下载已接受协议的 “GetCustomerAgreement” 操作所取代。此外，还引入了更精细的操作来控制查看和接受保密协议的访问权限（ ）NDAs。要利用这些精细操作并保持查看和执行协议的能力，用户必须将包含旧权限的现有策略替换为包含细粒度权限的策略。

将权限迁移到账户级别的下载协议

旧策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:DownloadAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    }
  ]
}
```

具有精细权限的新策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementsActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
```

```
      "Resource": "*"
    },
    {
      "Sid": "GetAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:GetAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptNdaForAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    }
  ]
}
```

将非资源特定权限迁移到账户级别的下载、接受和终止协议

旧策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    }
  ]
}
```

具有精细权限的新策略：

```
{
 "Version": "2012-10-17",
 "Statement": [
   {
        "Sid": "ListAgreementActions",
        "Effect": "Allow",
        "Action": [
            "artifact:ListAgreements",
            "artifact:ListCustomerAgreements"
        ],
        "Resource": "*"
      },
      {
        "Sid": "AWSAgreementActions",
        "Effect": "Allow",
        "Action": [
          "artifact:GetAgreement",
          "artifact:AcceptNdaForAgreement",
          "artifact:GetNdaForAgreement",
          "artifact:AcceptAgreement"
        ],
        "Resource": "arn:aws:artifact:::agreement/*"
      },
      {
        "Sid": "CustomerAgreementActions",
        "Effect": "Allow",
        "Action": [
            "artifact:GetCustomerAgreement",
            "artifact:TerminateAgreement"
        ],
        "Resource": "arn:aws:artifact::*:customer-agreement/*"
      }
    ]
}
```

将非资源特定权限迁移到组织级别的下载、接受和终止协议

旧策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iam:ListRoles",
      "Resource": "arn:aws:iam:::role/*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam:::role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

具有精细权限的新策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
```

```
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
```

```
      "Sid": "GetRoleToCheckForRoleExistence",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

迁移特定资源的权限，以便在账户级别下载、接受和终止协议

旧策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement"
      ],
      "Resource": [
        "arn:aws:artifact:::agreement/AWS Business Associate Addendum"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:TerminateAgreement"
      ],
```

```
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*"
      ]
    }
  ]
}
```

具有精细权限的新策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/agreement-9c1kBcYznTkcpRIm"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

迁移特定资源的权限，以便在组织层面下载、接受和终止协议

旧策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
        "arn:aws:artifact:::agreement/AWS Organizations Business Associate Addendum"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "iam:ListRoles",
      "Resource": "arn:aws:iam:::role/*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam:::role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

具有精细权限的新策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/agreement-y03aUwMAEorHtqjv"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
```

```
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "GetRoleToCheckForRoleExistence",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

协议的传统资源到细粒度的资源映射

协议已更新ARN，以获得更精细的权限。以前提及旧协议资源的任何内容都应替换为新ARN协议。以下是传统资源与细粒度资源之间的协议ARN对应关系。

协议名称	旧版权限ARN的 Artifact	ARN用于细粒度权限的 Artifact
AWS商业伙伴附录	arn: aws: artifact::: 协议/ 商业伙伴附录 AWS	arn: aws: artifact::: 协议/协议-9c1 T kBcYzn kcpRIm
AWS新西兰应通报的数据泄露附录	arn: aws: artifact::: agrement/ 新西兰应通报的数据泄露附录 AWS	arn: aws: artifact::: 协议/协议-3 YRq9rGUIu72r7Gt

协议名称	旧版权限ARN的 Artifact	ARN用于细粒度权限的 Artifact
AWS澳大利亚应通报的数据泄露附录	arn: aws: artifact::: agrement/ 澳大利亚应通报数据泄露附 AWS录	arn: aws: artifact::: 协议/协议-8 9 sbLSDe bitmAXNr
AWSSEC第17a-4条增编	arn: aws: artifact::: 协议/ 规则 17a-4 附录 AWS SEC	arn: aws: artifact::: 协议/协议- bexgr7sjv XAW4Gxu
AWSSEC第18a-6条规则增编	arn: aws: artifact::: 协议/ 规则 18a-6 附录 AWS SEC	arn: aws: artifact::: 协议/协议- HZTdNwJuqOKLReXC
AWSOrganizations B	arn: aws: artifact::: Agrement/ Organizations AWS	arn: aws: artifact::: 协议/协议- y03 aUw MAEorHtqjv
AWSOrganizations 澳大利亚应通报数据泄露	arn: aws: artifact::: agrement/ Organizations 澳大利亚应通报数据泄露 AWS	arn: aws: arnactifact::: 协议/协议-y pDMFXTe PE7kEg4b
AWSOrganizations 新西兰应通报的数据泄露附录	arn: aws: artifact::: agrement/ Organizations 新西兰应通报数据泄露AWS附录	arn: aws: artifact::: 协议/协议-3 V52 uojEjr vOnvrh

的IAM策略示例 AWS Artifact

您可以创建向IAM用户授予权限的权限策略。您可以授予用户访问 AWS Artifact 报告的权限，以及代表单个账户或组织接受和下载协议的能力。

以下示例策略显示了您可以根据IAM用户所需的访问权限级别向他们分配的权限。

- 使用细粒度权限管理 AWS 报告的策略示例
- 管理第三方报告的策略示例
- 管理协议的策略示例
- 要集成的策略示例 AWS Organizations
- 管理管理账户协议的策略示例
- 管理组织协议的策略示例
- 管理通知的策略示例

Example 通过细粒度权限管理 AWS 报告的策略示例

> **Tip**
>
> 您应该考虑使用AWSArtifactReportsReadOnlyAccess托管策略，而不是定义自己的策略。

以下策略授予通过细粒度权限下载所有 AWS 报告的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

以下策略通过细粒度权限授予仅下载 AWS SOCPCI、和ISO报告的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
```

```
          "artifact:ReportSeries": [
            "SOC",
            "PCI",
            "ISO"
          ],
          "artifact:ReportCategory": [
            "Certifications And Attestations"
          ]
        }
      }
    }
  ]
}
```

Example 管理第三方报告的策略示例

> **Tip**
>
> 您应该考虑使用AWSArtifactReportsReadOnlyAccess托管策略，而不是定义自己的策略。

第三方报告由IAM资源`report`表示。

以下政策授予所有第三方报告功能的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports",
        "artifact:GetReportMetadata",
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

以下政策授予下载第三方报告的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetTermForReport"
      ],
      "Resource": "*"
    }
  ]
}
```

以下策略授予列出第三方报告的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReport"
      ],
      "Resource": "*"
    }
  ]
}
```

以下政策授予查看所有版本的第三方报告详细信息的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReportMetadata"
      ],
      "Resource": [
        "arn:aws:artifact:us-east-1::report/report-jRVRFP8HxUN5zpPh:*"
      ]
```

```
    }
  ]
}
```

以下政策授予查看特定版本的第三方报告详细信息的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReportMetadata"
      ],
      "Resource": [
        "arn:aws:artifact:us-east-1::report/report-jRVRFP8HxUN5zpPh:1"
      ]
    }
  ]
}
```

> **Tip**
>
> 您应该考虑使用AWSArtifactAgreementsReadOnlyAccess或AWSArtifactAgreementsFullAccess 托管策略，而不是定义自己的策略。

Example 管理协议的策略示例

以下策略授予下载所有协议的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": [
```

```
        "*"
      ]
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

以下政策授予接受所有协议的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
```

```
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    }
  ]
}
```

以下政策授予终止所有协议的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

以下策略授予查看和执行账户级别协议的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
```

```
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    }
  ]
}
```

Example 要集成的策略示例 AWS Organizations

以下策略授予创建 AWS Artifact 用于集成的IAM角色的权限 AWS Organizations。您组织的管理账户必须具有这些权限才能开始使用组织协议。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
```

```
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

以下策略授予授予使用权限 AWS Artifact 的权限 AWS Organizations。您组织的管理账户必须具有这些权限才能开始使用组织协议。

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization"
      ],
      "Resource": "*"
   }
 ]
}
```

Example 管理管理账户协议的策略示例

以下策略授予管理管理账户协议的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
```

```
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
```

```
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Example 管理组织协议的策略示例

以下策略授予管理组织协议的权限。具有所需权限的另一位用户必须设置组织协议。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
```

```
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

以下策略授予查看组织协议的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
```

```
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    }
  ]
}
```

Example 管理通知的策略示例

以下策略授予使用 AWS Artifact 通知的完全权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",
        "notifications:AssociateChannel",
        "notifications:CreateEventRule",
        "notifications:CreateNotificationConfiguration",
        "notifications:DeleteEventRule",
        "notifications:DeleteNotificationConfiguration",
        "notifications:DisassociateChannel",
        "notifications:GetEventRule",
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
        "notifications:ListTagsForResource",
        "notifications:TagResource",
```

```
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration",
        "notifications-contacts:CreateEmailContact",
        "notifications-contacts:DeleteEmailContact",
        "notifications-contacts:GetEmailContact",
        "notifications-contacts:ListEmailContacts",
        "notifications-contacts:SendActivationCode"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

以下策略授予列出所有配置的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListNotificationConfigurations",
        "notifications:ListNotificationHubs",
        "notifications-contacts:GetEmailContact"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

以下策略授予创建配置的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",
        "notifications-contacts:CreateEmailContact",
        "notifications-contacts:SendActivationCode",
        "notifications:AssociateChannel",
        "notifications:CreateEventRule",
        "notifications:CreateNotificationConfiguration",
        "notifications:ListEventRules",
        "notifications:ListNotificationHubs",
        "notifications:TagResource",
        "notifications-contacts:ListEmailContacts"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

以下策略授予编辑配置的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetAccountSettings",
        "artifact:PutAccountSettings",
        "notifications:AssociateChannel",
        "notifications:DisassociateChannel",
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListTagsForResource",
        "notifications:TagResource",
        "notifications:UntagResource",
        "notifications:UpdateEventRule",
        "notifications:UpdateNotificationConfiguration",
        "notifications-contacts:GetEmailContact",
```

```
        "notifications-contacts:ListEmailContacts"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

以下策略授予删除配置的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:DeleteNotificationConfiguration",
        "notifications:ListEventRules"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

以下策略授予查看配置详细信息的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:GetNotificationConfiguration",
        "notifications:ListChannels",
        "notifications:ListEventRules",
        "notifications:ListTagsForResource",
        "notifications-contacts:GetEmailContact"
      ],
      "Resource": [
        "*"
```

```
      ]
    }
  ]
}
```

以下策略授予注册或取消注册通知中心的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "notifications:DeregisterNotificationHub",
        "notifications:RegisterNotificationHub"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

将 AWS 托管策略用于 AWS Artifact

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托管式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 当新服务启动或现有服务 AWS 服务 有新API操作可用时，最有可能更新 AWS 托管策略。

有关更多信息，请参阅 IAM IAM 用户指南中的 AWS 托管式策略。

AWS 托管策略： AWSArtifactReportsReadOnlyAccess

您可以将 AWSArtifactReportsReadOnlyAccess 策略附加到 IAM 身份。

此策略授予允许列出、查看和下载报告的*read-only*权限。

权限详细信息

该策略包含以下权限。

- artifact— 允许委托人从 AWS Artifact中列出、查看和下载报告。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:Get",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS 托管策略： AWSArtifactAgreementsReadOnlyAccess

您可以将 AWSArtifactAgreementsReadOnlyAccess 策略附加到 IAM 身份。

此政策授*read-only*予列出 Arti AWS fact 服务协议和下载已接受协议的权限。它还包括列出和描述组织详细信息的权限。此外，该策略还允许检查所需的服务相关角色是否存在。

权限详细信息

该策略包含以下权限。

- artifact— 允许委托人列出所有协议并查看其中的已接受协议。 AWS Artifact
- IAM— 允许委托人使用 GetRole检查服务关联角色是否存在。
- organization— 允许委托人描述组织并列出组织的服务访问权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementsActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GetCustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "AWSOrganizationActions",
      "Effect": "Allow",
      "Action": [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GetRole",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    }
```

```
  ]
}
```

AWS 托管策略： AWSArtifactAgreementsFullAccess

您可以将 AWSArtifactAgreementsFullAccess 策略附加到 IAM 身份。

此政策授予列出、下载、接受和终止 Artifact AWS 协议的*full*权限。它还包括在组织服务中列出和启用AWS服务访问权限的权限，以及描述组织详细信息的权限。此外，该策略还允许检查所需的服务相关角色是否存在，如果不存在，则创建一个。

权限详细信息

该策略包含以下权限。

- artifact— 允许委托人列出、下载、接受和终止来自 AWS Artifact的协议。
- IAM— 允许委托人使用 GetRole创建服务关联角色并检查服务关联角色是否存在。
- organization— 允许委托人描述组织并列出/启用组织的服务访问权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:ListAgreements",
        "artifact:ListCustomerAgreements"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AWSAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetAgreement",
        "artifact:AcceptNdaForAgreement",
        "artifact:GetNdaForAgreement",
        "artifact:AcceptAgreement"
      ],
```

```
      "Resource": "arn:aws:artifact:::agreement/*"
    },
    {
      "Sid": "CustomerAgreementActions",
      "Effect": "Allow",
      "Action": [
        "artifact:GetCustomerAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": "arn:aws:artifact::*:customer-agreement/*"
    },
    {
      "Sid": "CreateServiceLinkedRoleForOrganizationsIntegration",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": [
            "artifact.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "GetRoleToCheckForRoleExistence",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    },
    {
      "Sid": "EnableServiceTrust",
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
```

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

AWS ArtifactAWS 托管策略的更新

查看 AWS Artifact 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 Artifact 文档历史记录” 页面上的订阅RSS源。

更改	描述	日期
AWS Artifact 开始跟踪更改	AWS Artifact 开始跟踪其 AWS 托管策略的变更并已推出 AWSArtifactReports ReadOnlyAccess。	2023-12-15
引入了AWS协议管理策略	引入 AWSArtifactAgreements ReadOnlyAccess 并 AWSArtifactAgreementsFullAccess 管理策略。	2024-11-21

将服务相关角色用于 AWS Artifact

AWS Artifact 使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种与之直接关联的独特IAM角色类型。 AWS Artifact服务相关角色由服务预定义 AWS Artifact ，包括该服务代表您调用其他 AWS 服务所需的所有权限。

服务相关角色使设置变得 AWS Artifact 更加容易，因为您不必手动添加必要的权限。 AWS Artifact 定义其服务相关角色的权限，除非另有定义，否则 AWS Artifact 只能担任其角色。定义的权限包括信任策略和权限策略，并且该权限策略不能附加到任何其他IAM实体。

只有在首先删除服务相关角色的相关资源后，才能删除该角色。这样可以保护您的 AWS Artifact 资源，因为您不会无意中删除访问资源的权限。

有关支持服务相关角色的其他服务的信息，请参阅与服务关联角色配合使用的AWS 服务，IAM并在服务相关角色列中查找带有 “是” 的服务。选择是和链接，查看该服务的服务相关角色文档。

的服务相关角色权限 AWS Artifact

AWS Artifact 使用名为的服务相关角色 AWSServiceRoleForArtifact— AWS Artifact 允许通过 AWS Organizations收集有关组织的信息。

AWSServiceRoleForArtifact 服务相关角色信任以下服务来代入该角色：

- `artifact.amazonaws.com`

名为的角色权限策略 AWSArtifactServiceRolePolicy AWS Artifact 允许对`organizations`资源完成以下操作。

- `DescribeOrganization`
- `DescribeAccount`
- `ListAccounts`
- `ListAWSServiceAccessForOrganization`

为创建服务相关角色 AWS Artifact

您无需手动创建服务相关角色。当您进入组织管理账户中的组织协议选项卡并选择中的入门链接时 AWS Management Console，将为您 AWS Artifact 创建服务相关角色。

如果您删除该服务相关角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。当你进入组织管理账户中的组织协议选项卡并选择入门链接时， AWS Artifact 会再次为你创建服务相关角色。

编辑的服务相关角色 AWS Artifact

AWS Artifact 不允许您编辑 AWSServiceRoleForArtifact 服务相关角色。创建服务相关角色后，将无法更改角色名称，因为可能有多个实体引用该角色。但是，您可以使用编辑角色的描述IAM。有关更多信息，请参阅《IAM用户指南》中的编辑服务相关角色。

删除的服务相关角色 AWS Artifact

如果您不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样您就没有未被主动监控或维护的未使用实体。但是，您必须先清除服务相关角色的资源，然后才能手动删除它。

> **Note**
>
> 如果您尝试删除资源时 AWS Artifact 服务正在使用该角色，则删除可能会失败。如果发生这种情况，请等待几分钟后重试。

删除使用的 AWS Artifact 资源 AWSServiceRoleForArtifact

1. 访问控制台中的 “组织协议” 表格 AWS Artifact
2. 终止任何有效的组织协议

使用手动删除服务相关角色 IAM

使用IAM控制台 AWS CLI、或删除 AWSServiceRoleForArtifact 服务相关角色。 AWS API有关更多信息，请参阅IAM用户指南中的删除服务相关角色。

AWS Artifact 服务相关角色支持的区域

AWS Artifact 不支持在提供服务的每个区域中使用服务相关角色。您可以在以下区域使用该 AWSServiceRoleForArtifact 角色。

区域名称	区域标识	Support in AWS Artifact
美国东部（弗吉尼亚州北部）	us-east-1	是
美国东部（俄亥俄州）	us-east-2	否
美国西部（加利福尼亚北部）	us-west-1	否
美国西部（俄勒冈州）	us-west-2	是
非洲（开普敦）	af-south-1	否
亚太地区（香港）	ap-east-1	否
亚太地区（雅加达）	ap-southeast-3	否
亚太地区（孟买）	ap-south-1	否
Asia Pacific (Osaka)	ap-northeast-3	否

区域名称	区域标识	Support in AWS Artifact
Asia Pacific (Seoul)	ap-northeast-2	否
亚太地区（新加坡）	ap-southeast-1	否
亚太地区（悉尼）	ap-southeast-2	否
亚太地区（东京)	ap-northeast-1	否
加拿大（中部）	ca-central-1	否
欧洲地区（法兰克福）	eu-central-1	否
欧洲地区（爱尔兰）	eu-west-1	否
欧洲地区（伦敦）	eu-west-2	否
欧洲地区（米兰）	eu-south-1	否
欧洲地区（巴黎）	eu-west-3	否
欧洲地区（斯德哥尔摩）	eu-north-1	否
中东（巴林）	me-south-1	否
中东 (UAE)	me-central-1	否
South America（São Paulo）	sa-east-1	否
AWS GovCloud （美国东部）	us-gov-east-1	否
AWS GovCloud （美国西部）	us-gov-west-1	否

使用IAM条件键生成 AWS Artifact 报告

您可以使用IAM条件键根据特定的报告类别和系列提供对 AWS Artifact报告的精细访问权限。

以下示例策略显示了您可以根据特定的报告类别和系列向IAM用户分配的权限。

Example 管理 AWS 报告读取权限的策略示例

AWS Artifact 报告用IAM资源表示。`report`

以下政策授予阅读该`Certifications and Attestations`类别下所有 AWS Artifact 报告的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "artifact:ReportCategory": "Certifications and Attestations"
        }
      }
    }
  ]
}
```

以下政策允许您授予阅读该SOC系列下所有 AWS Artifact 报告的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "artifact:ListReports"
            ],
```

```
            "Resource": "*"
        },{
            "Effect": "Allow",
            "Action": [
                "artifact:GetReport",
                "artifact:GetReportMetadata",
                "artifact:GetTermForReport"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "artifact:ReportSeries": "SOC",
                    "artifact:ReportCategory": "Certifications and Attestations"
                }
            }
        }
    ]
}
```

以下政策允许您授予阅读除该Certifications and Attestations类别下 AWS Artifact 报告之外的所有报告的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:ListReports"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport"
      ],
      "Resource": "*",
      "Condition": {
```

```
        "StringEquals": {
          "artifact:ReportSeries": "SOC",
          "artifact:ReportCategory": "Certifications and Attestations"
        }
      }
    }
  ]
}
```

使用记录 AWS Artifact API通话 AWS CloudTrail

AWS Artifact 与 AWS CloudTrail一项服务集成，该服务提供用户、角色或 AWS 服务在中执行的操作的记录 AWS Artifact。 CloudTrail 将API呼叫捕获 AWS Artifact 为事件。捕获的调用包括来自 AWS Artifact 控制台的调用和对 AWS Artifact API操作的代码调用。如果您创建了跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括的事件 AWS Artifact。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的 “事件历史记录” 中查看最新的事件。使用收集的信息 CloudTrail，您可以确定向哪个请求发出 AWS Artifact、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

要了解更多信息 CloudTrail，请参阅《AWS CloudTrail 用户指南》。

AWS Artifact 信息在 CloudTrail

CloudTrail 在您创建账户 AWS 账户 时已在您的账户上启用。当活动发生在中时 AWS Artifact，该活动会与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在中查看、搜索和下载最近发生的事件 AWS 账户。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录您的 AWS 账户事件（包括的事件） AWS Artifact，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。预设情况下，在控制台中创建跟踪记录时，此跟踪记录应用于所有 AWS 区域。跟踪记录 AWS 分区中所有区域的事件，并将日志文件传送到您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅下列内容：

- 创建跟踪记录概述
- CloudTrail 支持的服务和集成
- 为以下各项配置亚马逊SNS通知 CloudTrail
- 接收来自多个地区的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail 日志文件

AWS Artifact 支持将以下操作作为事件记录在 CloudTrail 日志文件中：

- ListReports
- GetAccountSettings
- GetReportMetadata
- GetReport
- GetTermForReport

- PutAccountSettings
- AcceptAgreement
- AcceptNdaForAgreement
- GetAgreement
- GetCustomerAgreement
- GetNdaForAgreement
- ListAgreements
- ListCustomerAgreements
- TerminateAgreement

每个事件或日记账条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用 root 还是 AWS Identity and Access Management (IAM) 用户凭据发出。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

有关更多信息，请参阅CloudTrail userIdentity元素。

了解 AWS Artifact 日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。 CloudTrail 日志文件不是公共API调用的有序堆栈跟踪，因此它们不会按任何特定的顺序出现。

以下示例显示了演示该 GetReportMetadata 操作的 CloudTrail 日志条目。

```
{
  "Records": [
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::999999999999:user/myUserName",
        "accountId": "999999999999",
```

```
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
      },
      "eventTime": "2015-03-18T19:03:36Z",
      "eventSource": "artifact.amazonaws.com",
      "eventName": "GetReportMetadata",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "Python-httplib2/0.8 (gzip)",
      "errorCode": "AccessDenied",
      "errorMessage": "User: arn:aws:iam::999999999999:user/myUserName is not
 authorized to perform: artifact:GetReportMetadata on resource: arn:aws:artifact:us-
east-1::report/report-f1DIWBmGa2Lhsadg",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "7aebcd0f-cda1-11e4-aaa2-e356da31e4ff",
      "eventID": "e92a3e85-8ecd-4d23-8074-843aabfe89bf",
      "eventType": "AwsApiCall",
      "recipientAccountId": "999999999999"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::999999999999:user/myUserName",
        "accountId": "999999999999",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
      },
      "eventTime": "2015-03-18T19:04:42Z",
      "eventSource": "artifact.amazonaws.com",
      "eventName": "GetReportMetadata",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "Python-httplib2/0.8 (gzip)",
      "requestParameters": {
        "reportId": "report-f1DIWBmGa2Lhsadg"
      },
      "responseElements": null,
      "requestID": "a2198ecc-cda1-11e4-aaa2-e356da31e4ff",
      "eventID": "20b84ce5-730f-482e-b2b2-e8fcc87ceb22",
      "eventType": "AwsApiCall",
      "recipientAccountId": "999999999999"
```

```
    }
  ]
}
```

的文档历史记录 AWS Artifact

下表提供了《 AWS Artifact 用户指南》的 AWS Artifact 版本历史和相关更改。

变更	说明	日期
用于执行协议的精细权限 AWSArtifactAgreementsFullAccess 和 AWSArtifactAgreementsReadOnlyAccess 托管策略	为 AWS Artifact 协议执行以及启动AWSArtifactAgreementsFullAccess AWSArtifactAgreementsReadOnlyAccess AWS 和管理策略启用了细粒度访问权限。	2024 年 11 月 21 日
精细的报告访问权限和托管策略 AWSArtifactReportReadOnlyAccess	启用了对 AWS Artifact 报告的精细访问权限，启用了报告条件密钥并启动了AWSArtifactReportsReadOnlyAccess托管策略。	2023 年 12 月 15 日
AWS Artifact 服务相关角色	添加了与服务相关的角色文档，并更新了 AWS Artifact 和 AWS Organizations 集成的示例策略。	2023 年 9 月 26 日
通知	发布了管理通知的文档，并对 AWS Artifact API参考、CloudTrail 日志记录文档以及身份和访问管理页面进行了相关更新。	2023 年 8 月 1 日
第三方报告 - 公开发布	添加了API参考文档和 CloudTrail 日志记录文档，并公开了第三方报告。	2023 年 1 月 27 日
第三方报告（预览）	发布了销售其产品的独立软件供应商 (ISVs) 的合规报告 AWS Marketplace。为第三方	2022 年 11 月 30 日

	报告的身份和访问管理页面添加了示例策略。	
安全性	在“身份和访问管理”页面中添加了用于防止混淆副手的部分。	2021 年 12 月 20 日
报告	删除了保密协议，并引入了报告下载条款和条件。	2020 年 12 月 17 日
主页和搜索	在报告和协议页面上添加了服务主页和搜索栏。	2020 年 5 月 15 日
GovCloud 启动	推出 AWS Artifact 于 AWS GovCloud (US) Regions.	2019 年 11 月 7 日
AWS Organizations 协议	添加了管理组织协议的支持。	2018 年 6 月 20 日
协议	增加了对管理 AWS Artifact 协议的支持。	2017 年 6 月 17 日
初始版本	此版本引入了 AWS Artifact。	2016 年 11 月 30 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。