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 安全性和合规性文档，例如 AWS ISO 认证、支付卡行业 (PCI) 报告和服务组织控制 (SOC) 报告。您可以将安全性和合规性文档（也称为审核项目）提交给您的审计人员或监管人员，以证明您所使用的 AWS 基础设施和服务的安全性和合规性。您还可以使用这些文档作为准则，来评估您自己的云架构以及您公司的内部控制有效性。

此外，AWS Artifact 提供按需下载安全性与合规性文件，例如 ISO 认证以及在 AWS Marketplace 销售其产品的独立软件供应商 (ISV) 的服务组织控制 (SOC) 报告。有关更多信息，请参阅AWS Marketplace供应商见解。

AWS 客户负责制定或获取文档来证明自己公司的安全性和合规性。有关更多信息，请参阅责任共担模式。

您还可以使用 AWS Artifact 查看、接受 AWS 协议并跟踪其状态，如商业伙伴增订合约 (BAA)。受《美国健康保险可携与责任法》(HIPAA) 约束的公司通常需要签署 BAA，以确保受保护的健康信息 (PHI) 得到了相应保护。利用 AWS Artifact，您可以接受 AWS 协议并指定可以合法处理受限信息的 AWS 账户。您可以代表多个账户接受协议。要接受多个账户的协议，请使用 AWS Organizations 创建组织。

有关更多信息，请参阅AWS Artifact。

定价

AWS 会向您免费提供 AWS Artifact 文档和协议。

入门 AWS Artifact

AWS Artifact 为 AWS 安全和合规性报告提供了中心资源。中提供的项目 AWS Artifact 包括服务组织控制 (SOC) 报告、支付卡行业 (PCI) 报告以及认证机构颁发的用于验证 AWS 安全控制措施实施和运营有效性的认证。此外，还 AWS Artifact 提供按需访问安全与合规性文件，例如 ISO 认证以及销售其产品的独立软件供应商 (ISV) 的服务组织控制 (SOC) 报告。 AWS Marketplace有关更多信息，请参阅AWS Marketplace 供应商见解。

AWS Artifact 使您能够接受和管理法律协议，例如商业伙伴附录 (BAA)。如果您使用 AWS Organizations，则可以代表组织内的所有账户接受协议。接受之后，所有现有和后续成员账户将由协议自动涵盖。

任务

- 第 1 步：注册 AWS
- 第 2 步：下载报告
- 第 3 步：管理协议
- 第 4 步：管理通知

第 1 步：注册 AWS

如果您没有 AWS 账户，请完成以下步骤来创建一个。

报名参加 AWS 账户

1. 打开 https://portal.aws.amazon.com/billing/signup。
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。

   当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务 和资源。作为安全最佳实践，应为用户分配管理访问权限，并仅使用 root 用户来执行需要 root 用户访问权限的任务。

第 2 步：下载报告

您可以使用 Adobe Acrobat Reader 下载报告。不支持其他 PDF 阅读器。有关更多信息，请参阅 下载报告 。

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。
3. 在 “报告” 页面上，使用 “AWS 报告” 选项卡访问 AWS 报告，然后导航到 “第三方报告” 选项卡以访问销售其产品的独立软件供应商 (ISV) 的报告。 AWS Marketplace
4. （可选）在搜索字段中输入关键字以查找报告。
5. 选择一个报告，然后选择 下载报告。
6. （可选）在第三方报告选项卡上，您可以通过单击报告标题访问独立软件供应商报告的详细信息页面，以了解有关该报告的更多信息。
7. 可能会要求您接受适用于您正在下载的特定报告的条款和条件。我们建议您仔细阅读。完成后，选择我已阅读并同意条款，然后选择接受条款并下载报告。
8. 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 文档中作为附件嵌入其他信息，因此请务必查看 PDF 文件中的附件以获取支持文档。请在此处查看有关如何查看附件的说明。

只有已加入 V AWS Marketplace endor Insights 的 AWS 客户才能访问第三方报告。要了解更多信息，请参阅AWS Marketplace 供应商见解。

第 3 步：管理协议

在签订协议之前，您必须下载并同意 AWS Artifact 保密协议 (NDA) 的条款。每份协议都是机密的，不能与公司以外的其他人共享。

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. 选择账户协议来管理您的账户协议，或者选择组织协议来代表您的组织管理协议。
4. 展开协议的章节。

5. 选择 下载并查看。
6. 通读 条款和条件。完成后，选择 接受并下载。
7. 查看协议，然后选中复选框以表示您同意。
8. 选择接受以接受协议。

有关更多信息，请参阅 管理协议 。

第 4 步：管理通知

您可以订阅通知，了解新报告和协议的可用性或现有报告和协议的更新。AWS Artifact 使用 AWS 用户通知服务发送通知。通知将发送到用户在设置通知配置期间提供的电子邮件地址。

创建配置

1. 在 AWS 用户通知服务中打开通知中心页面
2. 选择您想要用于存储 AWS 用户通知服务资源的区域。默认情况下，您的用户通知数据将存储在美国东部（弗吉尼亚州北部），并复制到您选择的其他区域。有关更多详细信息，请参阅通知中心文档。
3. 单击创建配置。
4. 要接收协议通知，请单击 AWS 协议更新的复选框。
5. 要接收报告通知，请单击 AWS 报告更新的复选框。要仅接收特定类别和系列下报告的通知，请单击报告子集复选框，然后单击您感兴趣的类别和系列对应的复选框。
6. 为您的配置输入名称。
7. 输入应向其发送通知的逗号分隔电子邮件列表。
8. （可选）要为通知配置分配标签，请通过展开“标签”部分来输入键值对。注意：标签是您可以分配给 AWS 资源的标记，每个标签由一个密钥和一个您可以定义的可选值组成。标签帮助您管理、搜索和筛选资源。
9. 单击 Submit (提交)。
10. 验证电子邮件将发送到提供的电子邮件地址，电子邮件收件人需要在发送给他们的验证电子邮件中单击验证电子邮件链接。请注意，只有经过验证的电子邮件地址才会开始接收通知。

有关更多信息，请参阅 管理通知。

在 AWS Artifact 中下载报告

您可以从 AWS Artifact 控制台下载报告。当您从 AWS Artifact 下载报告时，会专门为您生成报告，每个报告具有唯一的水印。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，请使用安全的共享服务，如 Amazon 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。

目录

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AWS Artifact 中的身份和访问管理。

当您注册 AWS Artifact 时，您的账户将自动获得下载一些报告的权限。如果您在访问 AWS Artifact 时遇到问题，请按照AWS Artifact服务授权参考页面上的指引进行操作。

下载报告

1. 打开 AWS Artifact 控制台，地址：https://console.aws.amazon.com/artifact/。
2. 在AWS Artifact主页上，选择查看报告。
3. 在报告页面上，使用AWS报告选项卡访问 AWS 报告，然后导航到 第三方报告选项卡以访问在 AWS Marketplace 销售其产品的独立软件供应商 (ISV) 的报告。
4. （可选）在搜索字段中输入关键字以查找报告。
5. 选择一个报告，然后选择 下载报告。
6. （可选）在第三方报告选项卡上，您可以通过单击报告标题访问独立软件供应商报告的详细信息页面，以了解有关该报告的更多信息。
7. 可能会要求您接受适用于您正在下载的特定报告的条款和条件。我们建议您仔细阅读。完成后，选择我已阅读并同意条款，然后选择接受条款并下载报告。
8. 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 文档中作为附件嵌入其他信息，因此请务必查看 PDF 文件中的附件以获取支持文档。请在此处查看有关如何查看附件的说明。

查看 PDF 文档中的附件

建议使用以下目前支持查看 PDF 附件的应用程序：

Adobe Acrobat 查看器

1. 从此处下载最新版本的 Adobe Acrobat。
2. 在 Adobe Acrobat 查看器中打开文件。
3. 要打开附件面板，请单击 PDF 文档左侧的回形针图标或选择查看 > 显示/隐藏 > 导航窗格 > 附件。
4. 在“附件”面板中，双击附件以查看文档。

Firefox 浏览器

1. 从此处下载 Firefox 浏览器
2. 使用“文件”菜单中的“打开文件”选项，在 Firefox 浏览器中打开 PDF 文件。
3. 要打开附件，请单击屏幕左上角的切换侧栏图标。

保护您的文档

AWS Artifact 文档是机密文档，应始终予以保护。AWS Artifact 为其文档使用 AWS 责任共担模式。这表示，AWS 负责在 AWS 云中保证文档的安全性，而您在下载这些文档后负责确保其安全性。AWS Artifact 可能要求您先接受条款和条件，然后您才能下载文档。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文档共享服务 (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。

故障排除

如果您无法下载文档或收到错误消息，请参阅 AWS Artifact 常见问题解答中的故障排除。

管理 AWS Artifact 中协议

AWS Artifact 协议使您能够使用 AWS Management Console 为您的账户或组织审核、接受和管理协议。例如，受《美国健康保险可携与责任法》(HIPAA) 约束的公司通常需要签署商业伙伴增订合约 (BAA) 协议，以确保受保护的健康信息 (PHI) 得到了相应保护。您可以使用 AWS Artifact 接受协议（如与 AWS 签署的 BAA），并指定可以合法处理 PHI 的 AWS 账户。如果使用 AWS Organizations，则可以代表您组织中的所有账户接受协议，如 AWS BAA。所有现有和后续成员账户将由协议自动涵盖，并且可以合法处理 PHI。

您还可以使用 AWS Artifact 确认您的 AWS 账户或组织已接受协议，并审查所接受的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所接受的协议，则可以使用 AWS Artifact 来终止该协议。如果您终止协议，但以后意识到需要它，您可以再次激活。

目录

管理 AWS Artifact 中单个账户的协议

您可以仅接受您账户的协议，即使您的账户是 AWS Organizations 的组织中的成员账户。有关 AWS Organizations 的更多信息，请参阅《AWS Organizations 用户指南》。

接受与 AWS 的协议

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，则可以为 IAM 用户和联合用户授权角色权限，以访问并管理您的一个或多个协议。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 和联合用户必须具有以下权限：

```
artifact:DownloadAgreement
artifact:AcceptAgreement
```

有关更多信息，请参阅Identity and Access Management。

接受与 AWS 的协议

1. 打开 AWS Artifact 控制台，地址：https://console.aws.amazon.com/artifact/。
2. 在 AWS Artifact 导航窗格中，选择 Agreements (协议)。
3. 选择 Account agreements (账户协议) 选项卡。
4. 展开协议的章节。
5. 选择 下载并查看。
6. 通读 条款和条件。完成后，选择 接受并下载。
7. 查看协议，然后选中复选框以表示您同意。
8. 选择 接受 以接受您账户的协议。

终止与 AWS 的协议

如果您已使用 AWS Artifact 控制台接受协议，则可使用此控制台终止该协议。否则，请参阅离线协议。

所需的权限

要终止协议，IAM 和联合用户必须具有以下权限：

```
artifact:TerminateAgreement
```

有关更多信息，请参阅Identity and Access Management。

终止您与 AWS 的在线协议

1. 打开 AWS Artifact 控制台，地址：https://console.aws.amazon.com/artifact/。
2. 在 AWS Artifact 导航窗格中，选择 Agreements (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。

管理 AWS Artifact 中多个账户的协议

如果您是 AWS Organizations 组织的管理账户的所有者，则可以代表您组织中的所有账户接受协议。您必须使用正确的 AWS Artifact 权限登录管理账户才能接受或终止组织协议。具有 `organizations:DescribeOrganization` 权限的成员账户的用户可以查看代表其接受的组织协议。

如果您的账户不是组织的一部分，则可以按照AWS Organizations用户指南中创建和管理组织中的说明操作来创建或加入组织。

AWS Organizations 有两个可用的功能集：整合账单功能和所有功能。要为您的组织使用 AWS Artifact，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。

如果从组织中删除成员账户，则该成员账户将不再由组织协议所涵盖。管理账户管理员应在从组织中删除成员账户之前将此信息传达给成员账户，以便成员账户可以在必要时添加新协议。有效的组织协议列表可在 AWS Artifact 组织协议中进行查看。

有关更多信息，请参阅AWS Organizations用户指南中管理组织中 Amazon Web Services 账户。

接受您组织的协议

您可以在 AWS Organizations 中代表您组织中的所有成员账户接受协议。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

要接受协议，管理账户的所有者必须具有以下权限：

```
artifact:DownloadAgreement
artifact:AcceptAgreement
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateServiceLinkedRole
```

有关更多信息，请参阅Identity and Access Management。

接受组织的协议

1. 打开 AWS Artifact 控制台，地址：https://console.aws.amazon.com/artifact/。
2. 在 AWS Artifact 控制面板上，选择 Agreements (协议)。
3. 选择 Organization agreements (组织协议) 选项卡。
4. 展开协议的章节。
5. 选择 下载并查看。
6. 通读 条款和条件。完成后，选择 接受并下载。
7. 查看协议，然后选中复选框以表示您同意。
8. 选择 Accept (接受) 以接受您组织中所有现有账户和将来账户的协议。

终止组织协议

如果已使用 AWS Artifact 控制台来代表组织中的所有成员账户接受协议，则可以使用此控制台终止该协议。否则，请参阅离线协议。

所需的权限

要终止协议，管理账户的所有者必须具有以下权限：

```
artifact:DownloadAgreement
artifact:TerminateAgreement
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateServiceLinkedRole
```

有关更多信息，请参阅Identity and Access Management。

终止您与 Amazon Web Services 的在线组织协议

1. 打开 AWS Artifact 控制台，地址：https://console.aws.amazon.com/artifact/。
2. 在 AWS Artifact 控制面板上，选择 Agreements (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。

管理 AWS Artifact 中现有的离线协议

如果您已拥有离线协议，AWS Artifact 将显示您离线接受的协议。例如，控制台可能显示带 活动 状态的 Offline Business Associate Addendum (BAA) (离线商业伙伴增订合约(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您组织中的所有账户。要将离线接受的协议应用于您的组织及组织中的所有账户，您必须具有以下权限：

```
organizations:DescribeOrganization
organizations:EnableAWSServiceAccess
organizations:ListAWSServiceAccessForOrganization
iam:ListRoles
iam:CreateServiceLinkedRole
```

如果您的账户是组织中的成员账户，则您必须具有以下权限才能查看您的离线组织协议：

```
organizations:DescribeOrganization
```

有关更多信息，请参阅Identity and Access Management。

管理 AWS Artifact 中的通知

AWS Artifact 通知允许您设置电子邮件通知。在通知设置页面上，您可以订阅通知并管理其他通知设置，如下所述。AWS Artifact 使用 AWS 用户通知服务发送通知。要使用 AWS Artifact 通知，您必须拥有 AWS Artifact 和 AWS 用户通知服务所需的权限。有关更多信息，请参阅Identity and Access Management。

目录

设置您的通知

在开始接收通知之前，您需要指定存储用户通知数据的区域。请按照以下步骤设置通知中心。

设置通知中心

1. 在 AWS 用户通知服务中打开通知中心页面。
2. 选择您想要存储 AWS 用户通知服务资源的区域。默认情况下，您的用户通知数据将存储在美国东部（弗吉尼亚州北部），并将复制到您选择的其他区域。有关更多详细信息，请参阅通知中心文档。
3. 单击 Submit (提交)。

订阅通知

1. 打开 AWS Artifact 通知设置页面。
2. 单击订阅 Artifact 通知开关，订阅 AWS Artifact 的通知。

取消订阅通知

1. 打开 AWS Artifact 通知设置页面。
2. 单击订阅 Artifact 通知 开关，取消订阅 AWS Artitfact 的通知。

创建配置

1. 打开 AWS Artifact 通知设置页面。
2. 单击 创建配置。
3. 要接收协议通知，请选中 AWS 协议更新旁边的复选框。
4. 要接收报告通知，请选中AWS 报告更新旁边的复选框。
5. 要接收所有报告的通知，请选中所有报告旁边的复选框。
6. 要仅接收特定类别和系列下的报告的通知，单击报告子集复选框。然后，单击您感兴趣的类别和系列对应的复选框。
7. 为您的配置输入名称。
8. 输入应向其发送通知的电子邮件的逗号分隔列表。
9. （可选）要为通知配置分配标签，请通过展开“标签”部分来输入键值对。注意：标签是您可以分配给 AWS 资源的标记，每个标签由一个密钥和一个您可以定义的可选值组成。标签帮助您管理、搜索和筛选资源。
10. 单击 创建配置。
11. 验证电子邮件将发送到提供的电子邮件地址，电子邮件收件人需要在发送给他们的验证电子邮件中单击验证电子邮件链接。请注意，只有经过验证的电子邮件地址才会开始接收通知。

编辑配置

1. 打开 AWS Artifact 通知设置页面。
2. 单击您要编辑的配置行。
3. 单击页面右上方的编辑按钮。
4. 您可以编辑任何字段。对更改感到满意后，按保存更改。
5. 如果您添加了新的电子邮件地址，则系统将向每个电子邮件地址发送一封验证电子邮件。在验证电子邮件中单击验证电子邮件链接。

删除配置

1. 打开 AWS Artifact 通知设置页面。
2. 单击要删除的配置行。
3. 单击 Delete（删除）。
4. 阅读警告消息后，单击删除。

为配置分配标签

标签是分配给 Amazon Web Services 资源的一种标记。每个标签都包含您定义的一个键和一个可选值。标签帮助您管理、搜索和筛选资源。创建或编辑配置时，您可以选择设置标签。要阅读更多信息，请参阅为资源添加标签

故障排除

如果您在使用 AWS Artifact 通知时收到错误消息，请参阅 AWS Artifact 常见问题中的故障排除。

AWS Artifact 中的身份和访问管理

注册 AWS 时，您需要提供与您的 AWS 账户关联的电子邮件地址和密码。这些是您的根凭证，它们提供对您所有 AWS 资源的完全访问权限，包括 AWS Artifact 的资源。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。

不要使用根凭证登录您的 AWS 账户，也不要与他人共享您的凭证。对于您自己以及可能需要在 AWS Artifact 中访问文档或协议的任何人，您应该创建一个称为 IAM 用户 的专用用户身份。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。

如果您已管理 AWS 外部的用户身份，则可以使用 IAM 身份提供程序，而不必创建 IAM 用户。有关更多信息，请参阅 IAM 用户指南中的身份提供者和联合身份验证。

内容

设置用户 AWS Artifact 访问权限

完成以下步骤，根据其所需的访问权限级别向用户授予 AWS Artifact 权限。

任务

步骤 1：创建 IAM policy

作为 IAM 管理员，您可以创建策略来授予 AWS Artifact 操作和资源的权限。

创建 IAM policy

使用以下过程创建 IAM policy，您可以使用该策略向您的 IAM 用户和组授予权限。

1. 打开 IAM 控制台：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 示例 IAM policies 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 组并附加策略

作为 IAM 管理员，您可以创建组并将创建的策略附加到组。您可以随时将 IAM 用户添加到组。

创建 IAM 组并附加策略

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 用户并将其添加到组

作为 IAM 管理员，您可以随时将用户添加到组。这会向用户授予该组的权限。

创建一个 IAM 用户并将该用户添加到组

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. 请选择下一步：审核。如果您已准备好，请选择 创建用户。

迁移到精细权限

AWS Artifact 现在允许客户使用精细权限。通过这些精细权限，客户将可以精细地控制对各种功能的访问权限，例如接受条款和下载报告等。

要通过精细权限访问报告，客户应使用 AWSArtifactReportsReadOnlyAccess 托管式策略或根据以下建议更新权限。然后，客户应使用控制台中提供的试用新 AWS 报告页面链接选择加入。

如果更新到新权限时出现问题，用户可以使用控制台中提供的旧报告页面链接，从使用旧权限访问报告。

迁移到新权限

迁移非资源特定权限

用户需要将包含旧权限的现有策略替换为包含精细权限的策略

旧策略：

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

具有精细权限的新策略：

```
{
  "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

用户需要将其包含旧权限的现有策略替换为包含精细权限的策略。报告资源通配符权限已被条件键取代。

旧策略：

```
{
  "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/*"
      ]
    }
  ]
}
```

包含精细权限和条件键的新策略。

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

示例 IAM policies

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。

以下策略示例显示您可以根据 IAM 用户所需的访问级别为其分配的权限。

- 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": "*"
    }
  ]
}
```

以下策略授予通过细粒度权限仅下载 AWS SOC、PCI 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"
      ]
    }
  ]
}
```

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。IAM 用户必须拥有此权限才能接受协议。

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

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:DownloadAgreement"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

以下策略授予接受协议的权限。

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

以下策略授予终止协议的权限。

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

```
      ]
    }
  ]
}
```

以下策略授予管理单一账户协议的权限。

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

Example 要集成的策略示例 AWS Organizations

以下策略授予创建用于与集成的 IAM 角色的权限 AWS Organizations。 AWS Artifact 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": "iam:ListRoles",
      "Resource": "arn:aws:iam::*:role/*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
```

```
      "Resource": "arn:aws:iam::*:role/aws-service-role/artifact.amazonaws.com/
AWSServiceRoleForArtifact"
    }
  ]
}
```

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": [
    {
      "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": "*"
    }
  ]
}
```

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": [
    {
      "Effect": "Allow",
      "Action": [
        "artifact:AcceptAgreement",
        "artifact:DownloadAgreement",
        "artifact:TerminateAgreement"
      ],
      "Resource": [
        "arn:aws:artifact::*:customer-agreement/*",
```

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

```
}
```

适用于 AWS Artifact 的 AWS 托管式策略

AWS 托管策略是由 AWS 创建和管理的独立策略。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：AWSArtifactReportsReadOnlyAccess

您可以将 `AWSArtifactReportsReadOnlyAccess` 策略附加到 IAM 身份。

此策略将授予 *`read-only`* 权限，允许列出、查看和下载报告。

权限详细信息

该策略包含以下权限。

- `artifact` – 允许主体列出、查看和下载 AWS Artifact 中的报告。

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

```
      "Effect": "Allow",
      "Action": [
        "artifact:Get",
        "artifact:GetReport",
        "artifact:GetReportMetadata",
        "artifact:GetTermForReport",
        "artifact:ListReports"
      ],
      "Resource": "*"
    }
  ]
}
```

Artifact 对 AWS 托管式策略的更新

查看从该服务开始跟踪这些更改以来，有关适用于 Artifact 的 AWS 托管式策略更新的详细信息。要自动接受有关此页面更改的提示，请订阅有关 Artifact 文档历史记录页面上的 RSS 信息源。

更改	说明	日期
Artifact 已开始跟踪更改	Artifact 已开始跟踪其 AWS 托管式策略的更改，并推出了 AWSArtifactReports ReadOnlyAccess。	2023-12-15

为 AWS Artifact 使用服务相关角色

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独特类型的 IAM 角色，它与 AWS Artifact 直接相关。服务相关角色由 AWS Artifact 预定义，并包含该服务代表您调用其他 AWS 服务所需的一切权限。

借助服务相关角色，您无需手动添加所需的权限，因此可以更轻松地设置 AWS Artifact。AWS Artifact 定义其服务相关角色的权限，除非另外定义，否则只有 AWS Artifact 可以担任其角色。定义的权限包括信任策略和权限策略，而且权限策略不能附加到任何其它 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。这将保护您的 AWS Artifact 资源，因为您不会无意中移除对资源的访问权限。

有关支持服务相关角色的其他服务的信息，请参阅与 IAM 配合使用的 AWS 服务，并查找服务相关角色列中显示为是的服务。选择是，可转到查看该服务的服务相关角色文档的链接。

AWS Artifact 的服务相关角色权限

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

AWSServiceRoleForArtifact 服务相关角色信任以下服务担任该角色：

- `artifact.amazonaws.com`

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

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

为 AWS Artifact 创建服务相关角色

您无需手动创建服务相关角色。当您访问组织管理账户中的“组织协议”选项卡并选择 AWS Management Console 中“入门”链接时，AWS Artifact 会为您创建服务相关角色。

如果您删除此服务相关角色，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。当您访问组织管理账户中的“组织协议”选项卡并选择“入门”链接时，AWS Artifact 会再次为您创建服务相关角色。

编辑 AWS Artifact 的服务相关角色

AWS Artifact 不允许您编辑 AWSServiceRoleForArtifact 服务相关角色。创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。但是可以使用 IAM 编辑角色描述。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 AWS Artifact 的服务相关角色

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**
>
> 如果在您试图删除资源时 AWS Artifact 服务正在使用该角色，则删除操作可能会失败。如果发生这种情况，请等待几分钟后重试。

删除 AWSServiceRoleForArtifact 使用的 AWS Artifact 资源

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

要使用 IAM 手动删除服务相关角色

使用 IAM 控制台、AWS CLI 或 AWS API 删除 AWSServiceRoleForArtifact 服务相关角色。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 服务相关角色的受支持区域

AWS Artifact 并非在提供该服务的每个区域中都支持使用服务相关角色。您可以在以下区域中使用 AWSServiceRoleForArtifact 角色。

区域名称	区域标识	AWS Artifact 中的支持
美国东部（弗吉尼亚州北部）	us-east-1	可以
美国东部（俄亥俄州）	us-east-2	不可以
美国西部（北加利福尼亚）	us-west-1	不可以
美国西部（俄勒冈州）	us-west-2	可以
非洲（开普敦）	af-south-1	不可以
亚太地区（香港）	ap-east-1	不可以
亚太地区（雅加达）	ap-southeast-3	不可以
亚太地区（孟买）	ap-south-1	不可以
亚太地区（大阪）	ap-northeast-3	不可以

区域名称	区域标识	AWS Artifact 中的支持
亚太地区（首尔）	ap-northeast-2	不可以
亚太地区（新加坡）	ap-southeast-1	不可以
亚太地区（悉尼）	ap-southeast-2	不可以
亚太地区（东京)	ap-northeast-1	不可以
加拿大（中部）	ca-central-1	不可以
欧洲地区（法兰克福）	eu-central-1	不可以
欧洲地区（爱尔兰）	eu-west-1	不可以
欧洲地区（伦敦）	eu-west-2	不可以
欧洲地区（米兰）	eu-south-1	不可以
欧洲地区（巴黎）	eu-west-3	不可以
欧洲地区（斯德哥尔摩）	eu-north-1	不可以
中东（巴林）	me-south-1	不可以
中东（阿联酋）	me-central-1	不可以
南美洲（圣保罗）	sa-east-1	不可以
AWS GovCloud（美国东部）	us-gov-east-1	不可以
AWS GovCloud（美国西部）	us-gov-west-1	不可以

使用 IAM 条件键

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

以下示例策略演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 报告读取访问权限的策略示例

AWS Artifact 报告由 IAM 资源 `report` 表示。

以下策略将授予读取 `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"
        }
      }
    }
  ]
}
```

以下策略让您可以授予读取 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"
                }
            }
        }
    ]
}
```

以下策略让您可以授予读取所有 AWS Artifact 报告，但 `Certifications and Attestations` 类别下的报告除外的权限。

```
{
  "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 AWS Artifact 记录 AWS CloudTrail API 调用

AWS Artifact 与 AWS CloudTrail 集成，后者是在 AWS 中记录用户、角色或 AWS Artifact 服务所执行操作的服务。CloudTrail 将 AWS Artifact 的API 调用作为事件捕获。捕获的调用包含来自 AWS Artifact 控制台和代码的 AWS Artifact API 操作调用。如果您创建跟踪，则可以使 CloudTrail 事件持续传送到 Amazon S3 存储桶（包括 AWS Artifact 的事件）。如果您不配置跟踪记录，则仍可在 CloudTrail 控制台中的 Event history（事件历史记录）中查看最新事件。使用 CloudTrail 收集的信息，您可以确定向 AWS Artifact 发出了什么请求、发出请求的 IP 地址、何人发出的请求、请求的发出时间以及其他详细信息。

要了解有关 CloudTrail 的更多信息，请参阅AWS CloudTrail用户指南。

CloudTrail 中的 AWS Artifact 信息

在您创建 AWS 账户 时，将在该账户上启用 CloudTrail。当 AWS Artifact 中发生活动时，该活动将记录在 CloudTrail 事件中，并与其他 AWS 服务事件一同保存在 Event history（事件历史记录）中。您可以在 AWS 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用 CloudTrail 事件历史记录查看事件。

对于AWS 账户中的事件的持续记录（包括 AWS Artifact 的事件），请创建跟踪记录。通过跟踪记录，CloudTrail 可将日志文件传送至 Simple Storage Service（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。此跟踪记录在 AWS 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Simple Storage Service（Amazon S3）桶。此外，您可以配置其他 AWS 服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取行动。有关更多信息，请参阅下列内容：

- 创建跟踪概览
- CloudTrail 支持的服务和集成
- 为 CloudTrail 配置 Amazon SNS 通知
- 从多个区域接收 CloudTrail 日志文件和从多个账户接收 CloudTrail 日志文件

AWS Artifact 支持将以下操作记录为 CloudTrail 日志文件中的事件：

- ListReports
- GetAccountSettings
- GetReportMetadata

- GetReport
- GetTermForReport
- PutAccountSettings

每个事件或日志条目都包含有关生成请求的人员信息。身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证还是 AWS Identity and Access Management（IAM）用户凭证发出的。
- 请求是使用角色还是联合身份用户的临时安全凭证发出的。
- 请求是否由其它 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，可用于将事件作为日志文件传送到您指定的 Amazon S3 桶。CloudTrail 日志文件包含一个或多个日志条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

下面的示例显示了一个 CloudTrail 日志条目，该条目说明了 GetReportMetadata 操作。

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

AWS Artifact 的文档历史记录

下表介绍了 AWS Artifact 的版本。

变更	说明	日期
精细报告访问权限和 AWSArtifactReportReadOnlyAccess 托管式策略	启用了对 Artifact 报告的精细访问权限，启用了报告条件键，并推出了 AWSArtifactReportsReadOnlyAccess 托管式策略。	2023 年 12 月 15 日
AWS Artifact 服务相关角色	添加了服务相关角色文档，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 API 参考指南、CloudTrail 日志记录文档和 AWS Artifact 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、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）	发布了在 AWS Marketplace 销售其产品的独立软件供应商 (ISV) 的合规报告。此外，还向身份和访问管理页面添加了第三方报告的示例策略。	2022 年 11 月 30 日
安全性	在“身份和访问管理”页面中添加了用于防止混淆代理人的章节。	2021 年 12 月 20 日

报告	移除了保密协议，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 上线	已在 GovCloud 地区推出 AWS Artifact。	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。