aws

管理指南

AWS AppFabric

AWS AppFabric: 管理指南

Table of Contents

什么是 AWS AppFabric？

AWS AppFabric 快速连接组织中的软件即服务 (SaaS) 应用程序，因此 IT 和安全团队可以使用标准架构轻松管理和保护应用程序，员工可以使用生成式 AI 更快地完成日常任务。

主题

产品

探索两个方面 AWS AppFabric：专 AppFabric 为简化管理和安全性而设计的安全性，以及 AppFabric 通过生成式 AI 功能增强的生产力（预览版）。有关更多信息，请参阅以下主题：

- 什么是 AWS AppFabric 为了安全？
- 什么才是 AWS AppFabric 为了提高工作效率？

优势

您可以使用 AppFabric 执行以下操作：

- 在几分钟内连接您的应用程序，并降低运营成本。
- 提高 SaaS 应用程序数据的可见性，以提升您的安全状况。
- 通过生成式人工智能自动简化跨应用程序的任务。

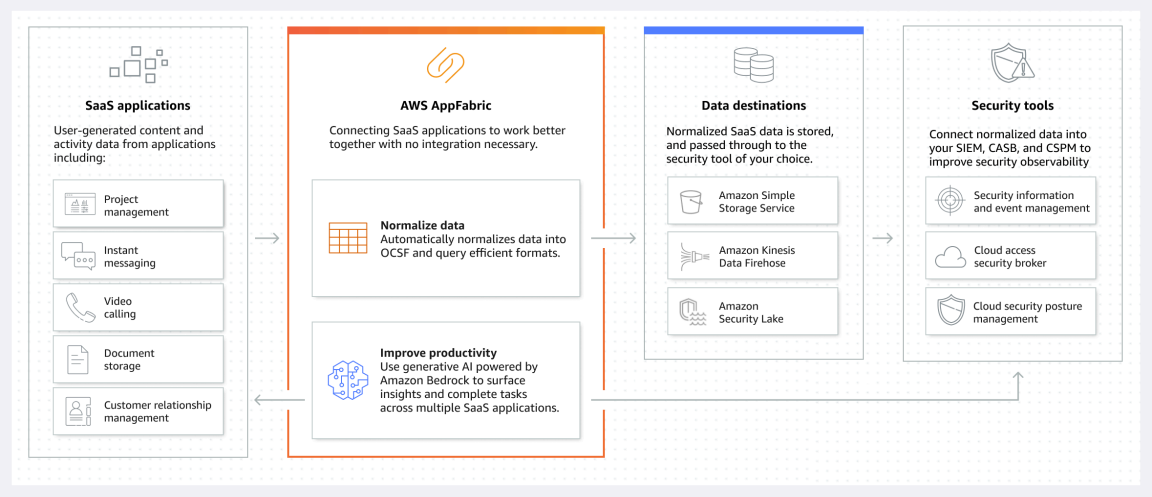
使用案例

你可以用 AppFabric 来：

- 快速连接您的 SaaS 应用程序
  - AppFabric 为了安全，本机将顶级 SaaS 生产力和安全应用程序相互连接，从而提供完全托管的 SaaS 互操作性解决方案。
- 提升您的安保状况
  - 应用程序数据会自动标准化，使管理员能够设置通用策略，标准化安全警报，并轻松管理多个应用程序的用户访问权限。
- 重塑生产力
  - 借助通用的生成式 AI 助手， AppFabric 提高工作效率可以让员工快速获得答案，自动执行任务管理，并在 SaaS 生产力应用程序中生成见解。

如何 AppFabric 运作

AppFabric 无需编码即可快速连接多个 SaaS 应用程序，从而提高工作效率和安全性。下图显示了的好处 AppFabric。



> **Note**
>
> AppFabric for productive 目前已作为预览版推出，在美国东部（弗吉尼亚北部）推出 AWS 区域。有关的更多信息 AWS 区域，请参阅中的AWS AppFabric 终端节点和配额AWS 一般参考。

定价

有关 AppFabric 定价的详细信息和示例，请参阅AWS AppFabric 定价。

可用性

要查看当前支持的 AWS 区域和终端节点 AppFabric，请参阅AWS 一般参考中的AWS AppFabric 终端节点和配额。

什么是 AWS AppFabric 为了安全？

AWS AppFabric 为了安全起见，可以快速连接组织中的软件即服务 (SaaS) 应用程序，因此 IT 和安全团队可以使用标准架构轻松管理和保护应用程序。

主题

优势

AppFabric 为了安全起见，您可以使用来执行以下操作：

- 在几分钟内连接您的应用程序，并降低运营成本。
- 提高 SaaS 应用程序数据的可见性，以提升您的安全状况。

使用案例

AppFabric 为了安全起见，您可以使用来：

- 快速连接您的 SaaS 应用程序
  - AppFabric 为了安全，本机将顶级 SaaS 生产力和安全应用程序相互连接，从而提供完全托管的 SaaS 互操作性解决方案。
- 提升您的安保状况

- 应用程序数据会自动标准化，使管理员能够设置通用策略，标准化安全警报，并轻松管理多个应用程序的用户访问权限。

AppFabric 出于安全考虑，请访问

AppFabric 安全版在美国东部（弗吉尼亚北部）、欧洲（爱尔兰）和亚太地区（东京）提供 AWS 区域。有关的更多信息 AWS 区域，请参阅中的AWS AppFabric 终端节点和配额AWS 一般参考。

在每个区域， AppFabric 为了安全起见，您可以通过以下任何一种方式进行访问：

AWS 管理控制台

AWS 管理控制台 是一个基于浏览器的界面，可用于创建和管理 AWS 资源。 AppFabric 控制台提供对您的 AppFabric 资源的访问权限。您可以使用 AppFabric控制台来创建和管理所有 AppFabric 资源。

AppFabric API

要 AppFabric 以编程方式访问，请使用 AppFabric API，然后直接向服务发出 HTTPS 请求。有关更多信息，请参阅 AWS AppFabric API 参考。

AWS Command Line Interface (AWS CLI)

借助 AWS CLI，您可以在系统的命令行中发出命令与之交互 AppFabric和其他命令 AWS 服务。如果您想构建执行任务的脚本，命令行工具也很实用。有关安装和使用的信息 AWS CLI，请参阅版本 2 的 AWS Command Line Interface 用户指南。有关 AWS CLI 命令的信息 AppFabric，请参阅《AWS CLI 参考》的AppFabric 部分。

相关服务

AppFabric 为了安全起见，您可以将以下内容 AWS 服务 与一起使用：

Amazon Data Firehose

Amazon Data Firehose 是一项提取、转换和加载 (ETL) 服务，可可靠地捕获、转换流数据并将其传输到数据湖、数据存储和分析服务。使用时 AppFabric，您可以选择将开放网络安全架构框架 (OCSF) 标准化或原始审计日志以 JSON 格式输出到 Firehose 流作为目的地。有关更多信息，请参阅在 Firehose 中创建输出位置。

Amazon Security Lake

Amazon Security Lake 会自动将来自 AWS 环境、SaaS 提供商、本地和云源的安全数据集中到存储在您账户中的专用数据湖中。您可以将 AppFabric 审核日志数据与安全湖集成，方法是选择 Amazon Data Firehose 作为目标，然后将 Firehose 配置为在安全湖中以正确的格式和路径传输数据。有关更多信息，请参阅 Amazon Security Lake 用户指南中的从自定义来源收集数据。

Amazon Simple Storage Service

Amazon Simple Storage Service（Amazon S3）是一种对象存储服务，提供行业领先的可扩展性、数据可用性、安全性和性能。使用时 AppFabric，您可以选择将 OCSF 标准化（JSON 或Apache Parquet）或原始（JSON）审计日志输出到新的或现有的 Amazon S3 存储桶作为目标。有关更多信息，请参阅在 Amazon S3 中创建输出位置。

Amazon 快速

Quick 通过超大规模的统一商业智能 (BI) 为数据驱动型组织提供支持。借助 Quick，所有用户都可以通过现代交互式仪表板、分页报告、嵌入式分析和自然语言查询，从同一个真实来源满足不同的分析需求。您可以在 Quick 中分析 AppFabric 审计日志数据，方法是选择存储 AppFabric 日志的 Amazon S3 存储桶作为来源。有关更多信息，请参阅快速用户指南中的使用 Amazon S3 文件创建数据集。您也可以将 Amazon S3 中的 AppFabric 数据导入到亚马逊 Athena，然后在 Quick 中选择 Amazon Athena 作为数据源。有关更多信息，请参阅快速用户指南中的使用 Amazon Athena 数据创建数据集。

AWS Key Management Service

使用 AWS Key Management Service (AWS KMS)，您可以跨应用程序创建、管理和控制加密密钥，以及 AWS 服务。在中创建应用程序包时 AppFabric，需要设置加密密钥来安全地保护您的授权应用程序数据。此密钥对您在 AppFabric 服务中的数据进行加密。 AppFabric 可以使用代表您 AWS 拥有的密钥 创建和管理的 AppFabric 密钥，也可以使用您在中创建和管理的客户托管密钥 AWS KMS。有关更多信息，请参阅创建 AWS KMS 密钥。

开放网络安全架构框架 AWS AppFabric

开放网络安全架构框架 (OCSF) 是由 AWS 网络安全行业的领先合作伙伴共同开发的开源项目。OCSF 为常见安全事件提供了标准架构，定义了版本控制标准以促进架构的演变，还包括安全日志生成者和使用者的自治流程。OCSF 的公共源代码托管在。GitHub

中基于 OCSF 的架构 AppFabric

基于安全性 OCSF 1.1 的架构专 AWS AppFabric 为满足您对其软件即服务 (SaaS) 产品组合的标准化、一致、省力可观察性的需求而量身定制。 AppFabric 确定每个字段和事件的正确映射。 AppFabric 与 OCSF 开源社区合作，引入了新的 OCSF 事件类别、事件类别、活动和对象，以便 OCSF 适用于

SaaS 应用程序事件。 AppFabric 自动规范从 SaaS 应用程序接收的审计事件，并将这些数据传输到您的中的亚马逊简单存储服务 (Amazon S3) 或 Amazon Data Firehose 服务。 AWS 账户对于 Amazon S3 目标，您可以在两个标准化选项（OCSF 或 Raw）和两个数据格式选项（JSON 或 Parquet）之间进行选择。传送到 Firehose 时，您还可以在两个标准化选项（OCSF 或 Raw）之间进行选择，但数据格式仅限于 JSON。

先决条件和使用建议 AWS AppFabric

如果您是新 AWS 客户，请先完成本页列出的设置先决条件，然后再开始使用 AWS AppFabric 以提高安全性。对于这些设置过程，您可以使用 AWS Identity and Access Management （IAM）服务。有关 IAM 的完整信息，请参阅《IAM 用户指南》。

主题

注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

报名参加 AWS 账户

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

   在注册时，将接到电话或收到短信，要求使用电话键盘输入一个验证码。

   当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务 和资源。作为最佳安全实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

AWS 注册过程完成后会向您发送一封确认电子邮件。您可以随时前往 https://aws.amazon.com/并选择“我的账户”，查看您当前的账户活动并管理您的账户。

创建具有管理访问权限的用户

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

保护你的 AWS 账户根用户

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。AWS 管理控制台在下一页上，输入您的密码。

   要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的 Signing in as the root user。
2. 为您的根用户启用多重身份验证（MFA）。

   有关说明，请参阅 I A M 用户指南中的为 AWS 账户 根用户启用虚拟 MFA 设备（控制台）。

创建具有管理访问权限的用户

1. 启用 IAM Identity Center。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的启用 AWS IAM Identity Center。
2. 在 IAM Identity Center 中，为用户授予管理访问权限。

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

以具有管理访问权限的用户身份登录

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

  有关使用 IAM Identity Center 用户登录的帮助，请参阅AWS 登录 用户指南中的登录 AWS 访问门户。

将访问权限分配给其他用户

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

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 Create a permission set。

2. 将用户分配到一个组，然后为该组分配单点登录访问权限。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 Add groups。

（必需）完成应用程序先决条件

AppFabric 为了确保从应用程序接收用户信息和审核日志的安全性，许多应用程序都要求您具有特定的角色和计划类型。为了安全起见，请确保您已查看要授权的每个应用程序 AppFabric 的先决条件，并且您有正确的计划和角色。有关特定于应用程序的先决条件的更多信息，请参阅支持的应用程序，或选择以下应用程序特定主题之一。

- 配置1Password为 AppFabric
- 配置Asana为 AppFabric
- 配置Azure Monitor为 AppFabric
- 配置Atlassian Confluence为 AppFabric
- 配置Atlassian Jira suite为 AppFabric
- 配置Box为 AppFabric
- 配置Cisco Duo为 AppFabric
- 配置Dropbox为 AppFabric
- 配置Genesys Cloud为 AppFabric
- 配置GitHub为 AppFabric
- 配置Google Analytics为 AppFabric
- 配置Google Workspace为 AppFabric
- 配置HubSpot为 AppFabric
- 配置IBM Security® Verify为 AppFabric
- 配置JumpCloud为 AppFabric
- 将 Microsoft 365 配置为 AppFabric
- 配置Miro为 AppFabric
- 配置Okta为 AppFabric
- 配置OneLogin by One Identity为 AppFabric
- 配置PagerDuty为 AppFabric
- 配置Ping Identity为 AppFabric
- 配置Salesforce为 AppFabric

- 配置ServiceNow为 AppFabric
- 配置Singularity Cloud为 AppFabric
- 配置Slack为 AppFabric
- 配置Smartsheet为 AppFabric
- 配置Terraform Cloud为 AppFabric
- 配置Webex by Cisco为 AppFabric
- 配置Zendesk为 AppFabric
- 配置Zoom为 AppFabric

（可选）创建输出位置

AppFabric 为了安全起见，支持将亚马逊简单存储服务 (Amazon S3) Service 和 Amazon Data Firehose 作为审核日志摄取目标。

Amazon S3

在创建接收目标时，您可以使用 AppFabric 控制台创建新的 Amazon S3 存储桶。您还可以使用 Amazon S3 服务创建存储桶。如果您选择使用 Amazon S3 服务创建存储桶，则必须在创建 AppFabric 提取目标之前创建存储桶，然后在创建接收目标时选择存储桶。只要现有的 Amazon S3 存储桶满足现有存储桶的以下要求 AWS 账户，您就可以选择使用其中的现有 Amazon S3 存储桶：

- AppFabric 为了安全起见，要求您的 Amazon S3 存储桶与您的 Amazon S3 资源 AWS 区域 相同。
- 您可以使用以下方法之一对存储桶进行加密：
  - 具有 Amazon S3 托管密钥的服务器端加密（SSE-S3）
  - 使用 AWS Key Management Service (AWS KMS) 密钥进行服务器端加密 (SSE-KMS)，使用默认值 AWS 托管式密钥 ()。`aws/s3`

Amazon Data Firehose

您可以选择使用 Amazon Data Firehose 作为安全数据的接收目的地。 AppFabric 要使用 Firehose，您可以在创建摄取 AWS 账户 之前或在中创建摄取目标时在中创建 Firehose 传送流。 AppFabric您可以使用 AWS 管理控制台、 AWS CLI、或创建 Firehose 传送流。 AWS APIs SDKs有关流配置说明，请参阅以下主题：

- AWS 管理控制台 说明 — 在《亚马逊数据 Firehose 开发者指南》中创建亚马逊数据 Firehose 传送流

- AWS CLI 指令 — create-delivery-stream在《AWS CLI 命令参考》中
- AWS APIs 和 SDKs 说明 — CreateDeliveryStream在 Amazon Data Firehos e API 参考中

出于安全考虑，使用 Amazon Data Fireh AppFabric ose 作为输出目标时的要求如下：

- AppFabric 对于安全资源，您必须使用与您 AWS 区域 相同的方法创建直播。
- 必须选择直接 PUT 作为来源。
- 将AmazonKinesisFirehoseFullAccess AWS 托管策略附加到您的用户，或者为您的用户附加以下权限：

```
{
    "Sid": "TagFirehoseDeliveryStream",
    "Effect": "Allow",
    "Action": ["firehose:TagDeliveryStream"],
    "Condition": {
        "ForAllValues:StringEquals": {"aws:TagKeys": "AWSAppFabricManaged"}
    },
    "Resource": "arn:aws:firehose:*:*:deliverystream/*"
}
```

Firehose 支持与各种第三方安全工具集成，例如Splunk和。Logz.io有关如何正确配置 Amazon Kinesis 以使其向这些工具输出数据的信息，请参阅《亚马逊数据 Firehose 开发者指南》中的目标设置。

（可选）创建 AWS KMS 密钥

在创建安全应用程序捆绑包的过程中，您将选择或设置加密密钥，以安全地保护您的数据免受所有授权应用程序的侵害。 AppFabric 此密钥将用于在 AppFabric 服务中加密您的数据。

AppFabric 为了安全起见，默认情况下会加密数据。 AppFabric 为了安全起见，可以使用代表您 AWS 拥有的密钥 创建和管理的 AppFabric 密钥，也可以使用您在 AWS Key Management Service (AWS KMS) 中创建和管理的客户托管密钥。 AWS 拥有的密钥 是 a AWS 服务 拥有并管理的 AWS KMS 密钥集合，用于多个密钥 AWS 账户。客户管理的密 AWS KMS 钥 AWS 账户 是您创建、拥有和管理的密钥。有关客户托管密钥 AWS 拥有的密钥 的更多信息，请参阅《AWS Key Management Service 开发人员指南》中的客户 AWS 密钥和密钥。

为了安全起见，如果您想使用客户管理的密钥来加密数据（例如授权令牌），则可以使用创建一个AWS KMS。 AppFabric 有关授予客户托管密钥访问权限的权限策略的更多信息 AWS KMS，请参阅本指南的密钥策略部分。

为了安全起见， AWS AppFabric 请开始使用

AWS AppFabric 为了安全起见，您必须先创建一个应用程序包，然后授权应用程序并将其连接到您的应用程序包。将应用程序授权连接到应用程序后，您可以使用 AppFabric 安全功能，例如审核日志提取和用户访问权限。

本节介绍如何开始 AppFabric 在中使用 AWS 管理控制台。

主题

先决条件

在开始之前，必须先创建一个 AWS 账户 和一个管理用户。有关更多信息，请参阅注册获取 AWS 账户和创建具有管理访问权限的用户。

第 1 步：创建应用程序捆绑包

App bundle 会存储您的所有内容 AppFabric ，用于安全应用程序授权和摄取。要创建应用程序捆绑包，请设置加密密钥以安全保护您的授权应用程序数据。

1. 打开 AppFabric 控制台，网址为https://console.aws.amazon.com/appfabric/。
2. 在页面右上角的选择区域选择器中，选择一个。 AWS 区域 AppFabric 仅在美国东部（弗吉尼亚北部）、欧洲（爱尔兰）和亚太地区（东京）地区提供。
3. 选择开始使用。
4. 在开始使用页面上，进入步骤 1。创建应用程序捆绑包，选择创建应用程序捆绑包。
5. 在加密部分中，设置加密密钥以安全保护您的数据免受所有授权应用程序的访问。此密钥用于在安全服务中 AppFabric加密您的数据。

AppFabric 为了安全起见，默认情况下会加密数据。 AppFabric 可以使用代表您 AWS 拥有的密钥创建和管理的密钥，也可以使用您 AppFabric 在 AWS Key Management Service (AWS KMS) 中创建和管理的客户托管密钥。

6. 对于 AWS KMS 密钥，选择使用 AWS 拥有的密钥 或客户托管密钥。

   如果您选择使用客户托管密钥，请输入您要使用的现有密钥的 Amazon 资源名称（ARN）或密钥 ID，或者选择创建 AWS KMS 密钥。

   选择 AWS 拥有的密钥 或客户托管密钥时，请考虑以下几点：

   - AWS 拥有的密钥是 AWS Key Management Service (AWS KMS) 密钥的集合，这些密钥由一个人 AWS 服务 拥有并管理，用于多个密钥 AWS 账户。尽管 AWS 拥有的密钥 不在您的账户中 AWS 账户，但 AWS 服务 可以使用 AWS 拥有的密钥 来保护您账户中的资源。 AWS 拥有的密钥 不要计入您账户的 AWS KMS 配额。您不必创建或维护该密钥或其密钥策略。的轮换因服务 AWS 拥有的密钥 而异。有关 for 轮换的信息 AppFabric， AWS 拥有的密钥 请参阅静态加密。
   - 客户托管密钥是您 AWS 账户 自己创建、拥有和管理的 KMS 密钥。您可以完全控制这些 AWS KMS 按键。您可以建立和维护他们的密钥策略、 AWS Identity and Access Management (IAM) 策略和授权。您可以启用和禁用它们、轮换其加密材料、添加标签、创建引用 AWS KMS 密钥的别名以及安排删除 AWS KMS 密钥。客户管理的密钥显示在的客户管理的密钥页面上 AWS 管理控制台 AWS KMS。

     要明确地标识客户托管密钥，请使用 `DescribeKey` 操作。对于客户托管密钥，`DescribeKey` 响应的 `KeyManager` 字段的值为 `CUSTOMER`。您可以在加密操作中使用您的客户托管密钥，也可以在 AWS CloudTrail 日志中审核使用情况。对于许多与 AWS 服务 之集成的密钥 AWS KMS，您可以指定客户托管的密钥来保护为您存储和管理的数据。客户管理的密钥需要支付月费，超出 AWS 免费套餐的使用量则需要付费。客户托管的密钥计入您账户的 AWS KMS 配额。

   有关客户托管密钥 AWS 拥有的密钥 的更多信息，请参阅《AWS Key Management Service 开发人员指南》中的客户 AWS 密钥和密钥。

   > **Note**
   >
   > 创建应用程序包时， AppFabric 为了安全起见，还会在您的 AWS 账户 名为服务相关角色 (SLR) 中创建一个特殊的 IAM 角色。 AppFabric它允许该服务向 Amazon 发送指标 CloudWatch。添加审核日志目标后，SLR 允许安全服务访问您的 AWS 资源（Amazon

S3 存储桶、Amazon Data Firehose 传输流）。 AppFabric 有关更多信息，请参阅 将服务相关角色用于 AppFabric。

7. （可选）对于标签，您可以选择将标签添加到应用程序捆绑包。标签是键/值对，用于将元数据分配到您创建的资源。有关更多信息，请参阅《标签编辑器用户指南》中的为 AWS 资源AWS添加标签。
8. 要创建您的应用程序捆绑包，请选择创建应用程序捆绑包。

第 2 步：授权应用程序

成功创建应用程序包后， AppFabric 为了安全起见，您现在可以授权与每个应用程序进行连接和交互。已授权的应用程序会进行加密并存储在您的应用程序捆绑包中。要为每个应用程序捆绑包设置多个应用程序授权，请根据需要为每个应用程序重复应用程序授权步骤。

在开始授权应用程序之前，请在 AppFabric 为了安全起见，中支持的应用程序 中查看并验证每个应用程序的先决条件，例如所需的计划类型。

1. 在开始使用页面上，进入步骤 2。授权应用程序，选择创建应用程序授权。
2. 在 “应用程序授权” 部分，从 “应用程序” 下拉列表中选择要授予安全连接权限的应用程序。AppFabric AppFabric 为了安全起见，显示的应用程序是当前支持的应用程序。
3. 选择应用程序时，将显示必填的信息字段。这些字段包括租户 ID 和租户名称，还可能包括客户端 ID、客户端密钥或个人访问令牌。这些字段的输入值因应用程序而异。有关如何查找这些值的特定于应用程序的详细说明，请参阅 AppFabric 为了安全起见，中支持的应用程序。
4. （可选）对于标签，您可以选择将标签添加到应用程序授权中。标签是键/值对，用于将元数据分配到您创建的资源。有关更多信息，请参阅《标签编辑器用户指南》中的为 AWS 资源AWS添加标签。
5. 选择创建应用程序授权。
6. 如果出现弹出窗口（取决于正在连接的应用程序），请选择 “允许” 以授权与您的应用程序 AppFabric 进行安全连接。

   如果您的应用程序授权成功，您将在开始使用页面上看到一条应用程序授权已连接的成功消息。
7. 您可以随时在导航窗格中每个应用程序状态下的应用程序授权页面上查看应用程序授权状态。“已连接” 状态表示您的应用程序已 AppFabric 获得授权，以确保连接到应用程序的安全性，并且已完成。
8. 下表显示了可能的应用程序授权状态，包括您可以采取哪些故障排除步骤来修复相关错误。

状态名称	状态描述	故障排除步骤
待处理	状态为 “待定” 表示应用程序的应用程序授权已创建，但 AppFabric 出于安全考虑，尚未连接到该应用程序。	当您看到此状态时，请从应用程序授权页面的操作下拉列表中选择连接以启动连接。如果此错误仍然存在，请检查是否已禁用浏览器的弹出窗口拦截器。如果出现任何错误消息，例如带有 400 Bad Request 的弹出窗口，请检查所有信息（例如租户 ID、客户端 ID 和客户机密钥）是否输入正确。也可能未正确创建应用程序的应用程序授权。有关更多信息，请参阅支持的应用程序。
连接验证失败	连接验证失败的状态意味着 AppFabric 出于安全考虑，无法验证应用程序授权与应用程序的连接。	检查是否正确输入了用于应用程序授权的所有信息，例如租户 ID、客户端 ID 和客户端密钥。
令牌自动轮换失败	令牌自动轮换失败状态表示在成功连接应用程序授权后 OAuth 刷新令牌失败。	如果此错误仍然存在，请检查应用程序的身份验证应用。有关更多信息，请参阅支持的应用程序。

9. 要授权其他应用程序，请根据需要重复步骤 1 到 8。

第 3 步：设置审核日志提取

在应用程序捆绑包中创建了至少一个应用程序授权后，您现在可以设置审核日志提取了。审核日志提取使用来自授权应用程序的审核日志，并将其标准化为开放网络安全架构框架 (OCSF)。然后，它们将被运送至其中一个或多个目标 AWS。也可以选择将 Raw - JSON 文件传输至目标。

1. 在开始使用页面上，进入步骤 3。设置审核日志提取部分，选择提取快速设置。

> **Note**
>
> 要加快设置速度，请进入提取快速设置页面（仅可从开始使用页面访问），一次性为多个提取目标相同的应用程序授权创建提取。例如，相同的亚马逊 S3 存储桶或 Amazon Data Firehose 数据流。
>
> 您也可以从提取页面创建提取，该页面可从导航窗格访问。在提取页面上，每次您可以设置一次目标不同的提取。在提取页面上，您还可以为提取创建标签。以下为提取快速设置页面的说明。

2. 对于选择应用程序授权，选择要创建审核日志提取的应用程序授权。为了安全起见，“应用程序授权” 下拉列表中显示的租户名称是您之前为其创建应用程序授权的应用程序的 AppFabric 租户名称。
3. 在添加目标中，选择所选应用程序的审核日志提取目标。目标选项包括亚马逊 S3-现有存储桶、亚马逊 S3-新存储桶或亚马逊 Data Firehose。如果您选择了多个租户名称，则您选择的目标将应用于每次应用程序授权提取。
4. 选择目标时，会出现其他必填字段。

   a. 如果您选择 Amazon S3 - 新存储桶作为目标，则必须输入要创建的 S3 存储桶的名称。有关如何创建 Amazon S3 存储桶的更多说明，请参阅创建输出目标。

   b. 如果您选择 Amazon S3 - 现有存储桶作为目标，请选择要使用的 Amazon S3 存储桶的名称。

   c. 如果您选择 Amazon Data Firehose 作为目的地，请从 Firehose 传输流名称下拉列表中选择传输流的名称。有关如何创建 Amazon Data Firehose 传输流的更多说明，请参阅创建输出目标并注意安全 AppFabric 所需的权限策略。

5. 对于架构和格式，对于亚马逊 S3 存储桶，您可以选择将审核日志存储为 Ra w-JSON、OCSF-JSON、OCSF（Parquet适用于亚马逊 S 3 存储桶）或 Raw-JSON 或 OCSF -JSON（适用于 Firehos e）。

   原始数据格式提供将审核日志数据从数据字符串转换为 JSON 的功能。为了安全起见，OCSF 数据格式将您的审核日志数据标准化 AppFabric 为开放式网络安全架构框架 (OCSF) 架构。有关如何 AppFabric 使用 OCSF 的更多信息，请参阅开放网络安全架构框架 AWS AppFabric。每次只能选择一种模式和格式数据类型进行数据提取。如果要添加其他架构和格式数据类型，则可以通过重复提取创建过程来设置其他提取目标。

6. （可选）如果要为提取添加标签，请从导航窗格转到提取页面。要转到提取详细信息页面，请选择租户名称。对于标签，您可以选择在提取中添加标签。标签是键/值对，用于将元数据分配到您创建的资源。有关更多信息，请参阅《标签编辑器用户指南》中的为 AWS 资源AWS添加标签。
7. 选择设置提取。

   成功设置提取后，您将在开始使用页面看到一条提取已创建的成功消息。
8. 您也可以随时在导览窗格的提取页面上查看您的提取状态和提取目标的状态。在此页面上，您可以看到在创建应用程序授权时创建的租户名称、目标和提取状态。提取状态为已启用，表示您的提取已启用。如果您在此页面上选择应用程序授权的租户名称，则可以看到该应用程序授权的详细信息页面，包括目标详细信息和状态。提取目标的状态为活动，表示目标已正确设置且处于活动状态。如果应用程序授权的状态为已连接，且提取目标状态为活动，表示应处理并提交审核日志。如果应用程序授权状态或提取目标状态为失败状态，表示即使启用了提取状态，也不会处理或传送审核日志。要修复应用程序授权失败，请参阅步骤 2。授权应用程序。
9. 下表显示了可能出现的提取和提取目标状态，以及您可以采取以修复任何错误状态的故障排除步骤。

状态或状态名称	说明	故障排除步骤
Disabled (已禁用)	提取已禁用状态表示您的提取已禁用。	您可以通过在提取页面的操作下拉列表中选择启用来启用提取。
已失败	提取目标的失败状态表示提取目标不接受审核日志。例如，出现这种状态可能是由于存储位置已满。	要修复这些问题，请访问亚马逊 S3 或 Firehose 控制台。

第 4 步：使用用户访问工具

使用安全用户访问工具，安全和 IT 管理员团队可以使用员工的公司电子邮件地址进行简单搜索，从而快速查看谁有权访问特定应用程序。 AppFabric 这种方法有助于减少在诸如用户取消配置的任务上花费的时间，这些任务可能需要手动检查或审核用户对 SaaS 应用程序的访问。如果找到了用户， AppFabric 出于安全考虑，将在应用程序中提供该用户的姓名以及应用程序内用户状态（例如，Active）（如果应用程序提供）。 AppFabric 为了安全起见，搜索应用程序包中的所有授权应用程序，以返回用户有权访问的应用程序列表。

1. 在开始使用页面上，进入步骤 4。使用用户访问工具，选择查找用户。
2. 在电子邮箱地址字段中，键入用户的电子邮箱地址，然后选择搜索。
3. 在搜索结果部分，您可以看到用户有权访问的所有授权应用程序的列表。要在应用程序中显示用户的姓名及其状态（如有），请选择搜索结果。
4. 搜索结果栏中出现找到用户的消息，表示用户已列出可以访问的应用程序。下表显示了可能出现的搜索结果、错误以及为解决这些错误可以采取的措施。

搜索结果	说明
找不到用户	未找到使用该电子邮箱地址的用户。
未找到授权令牌。为应用程序连接应用程序授权。	检查是否正确输入了用于应用程序授权的所有信息，例如租户 ID、客户端 ID 和客户端密钥。
授权令牌已撤销。为应用程序连接应用程序授权。	检查是否正确输入了用于应用程序授权的所有信息，例如租户 ID、客户端 ID 和客户端密钥。
我们无法轮换授权令牌。为应用程序连接应用程序授权。	成功连接应用程序授权后， OAuth 刷新令牌失败。如果此错误仍然存在，请检查应用程序的身份验证应用。有关更多信息，请参阅支持的应用程序。
未找到所需权限。为应用程序连接应用程序授权。	检查是否正确输入了用于应用程序授权的所有信息，例如租户 ID、客户端 ID 和客户端密钥。
应用程序授权无效。	检查是否正确输入了用于应用程序授权的所有信息，例如租户 ID、客户端 ID 和客户端密钥。
由于权限不足，我们无法调用应用程序 API。	检查是否正确输入了用于应用程序授权的所有信息，例如租户 ID、客户端 ID 和客户端密钥。
超出应用程序请求限制。	这是从应用程序收到的错误消息。您可以稍后尝试搜索电子邮箱地址。

搜索结果	说明
应用程序遇到了内部服务器错误	这是从应用程序收到的错误消息。您可以稍后尝试搜索电子邮箱地址。
应用程序遇到了网关错误	这是从应用程序收到的错误消息。您可以稍后尝试搜索电子邮箱地址。
应用程序尚未准备好处理请求	这是从应用程序收到的错误消息。您可以稍后尝试搜索电子邮箱地址。
应用程序遇到了请求错误。	这是我们从应用程序收到的错误消息。您可以稍后再次尝试搜索电子邮件。
应用程序遇到了服务不可用错误。	这是我们从应用程序收到的错误消息。您可以稍后再次尝试搜索电子邮件。

步骤 5：Connect AppFabric 以获取安全工具和其他目标中的安全数据

来自的标准化（或原始）应用程序数据与任何支持从 AppFabric Amazon S3 提取数据并与 Firehose 集成的工具兼容，包括、、Barracuda XDR、、、DynatraceLogz.ioNetskopeNetWitnessRapid7Splunk、和等安全工具或您的专有安全解决方案。要从中获取标准化（或原始）应用程序数据 AppFabric，请按照前面的步骤 1 到 3 进行操作。有关如何设置特定安全工具和服务的更多详细信息，请参阅兼容的安全工具和服务。

AppFabric 为了安全起见，中支持的应用程序

AWS AppFabric 为了安全起见，支持与以下应用程序集成。选择应用程序的名称，了解有关如何设置安全性 AppFabric 以连接到该应用程序的更多信息。

主题

- 配置1Password为 AppFabric
- 配置Asana为 AppFabric
- 配置Azure Monitor为 AppFabric
- 配置Atlassian Confluence为 AppFabric
- 配置Atlassian Jira suite为 AppFabric

配置1Password为 AppFabric

1Password是一款密码管理器，可帮助您为所有在线帐户创建、存储和使用强密码。它还可以通过加密来保护您的数据，提醒您出现漏洞，并允许您共享密码。

AWS AppFabric 出于安全考虑，您可以使用来审核来自的日志和用户数据1Password，将数据标准化为开放网络安全架构框架 (OCSF) 格式，并将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

AppFabric 支持 1Password

AppFabric 支持接收来自的用户信息和审核日志1Password。

先决条件

AppFabric 要使用将审核日志从支持的目标传输1Password到支持的目的地，您必须满足以下要求：

- 您必须拥有有效的付费1Password商业版或企业版订阅计划。有关更多信息，请参阅1Password网站上的1Password企业版。
- 您的1Password账户中必须具有管理员角色或团队所有者。有关更多信息，请参阅1Password支持网站中的群组。

速率限制注意事项

1Password AuditLog 事件 API 将请求限制为每分钟 600 个，每小时最多 30,000 个。超过这些限制会返回错误。有关更多信息，请参阅 “1Password事件 1Password API 参考” 中的 API 速率限制。

数据延迟注意事项

审计事件发送到目标位置的时间可能会延迟多达 30 分钟。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。不过，这可以在账户级别进行自定义。如需帮助，请联系 支持。

正在 AppFabric 连接您的1Password账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric使用进行授权1Password。要查找授权所需的信息 1Password AppFabric，请按以下步骤操作。

创建个人1Password访问令牌

1Password支持公共客户端的个人访问令牌。完成以下步骤以生成个人访问令牌。

1. 登录您的 1Password 账户。
2. 在导航窗格中选择 “集成”。
3. 如果存在现有集成，请选择目录。否则，请继续下一步。
4. 在 “事件报告集成” 下选择 “其他”。
5. 在添加集成页面上，输入您的安全信息和事件管理 (SIEM) 系统名称（例如 S AppFabric ecure）
6. 选择添加集成，然后在设置令牌页面中完成以下步骤。
    a. 提供要在 AppFabric 安全环境中使用的令牌名称。
    b. 我们建议您在 “过期后到期” 下拉列表中选择 “永不”。如果选择了任何其他值，则在过期时间过后1Password撤消令牌。
    c. 在 “要报告的事件” 部分，选择登录尝试次数、项目使用事件和审核事件。
7. 选择发行代币以创建代币。
8. 选择 “保存于” 1Password 并完成以下步骤。
    a. 标题将根据您的系统和令牌名称自动填充。
    b. 在 “选择文件库” 下选择 “私有”。
    c. 选择保存。

有关更多信息，请参阅1Password网站上的 “1Password事件报告入门”。

应用程序授权

租户编号

AppFabric 将请求您的租户 ID。中的租户 ID AppFabric 将是您的1Password登录地址。完成以下步骤以查找您的租户 ID。

1. 登录您的 1Password 账户。
2. 在导航窗格中，选择设置。
3. 页面上列出了您的1Password登录信息。例如，e xample- account.1password.com。

租户名称

输入标识此唯一1Password组织的名称。 AppFabric 使用租户名称来标记应用程序授权和通过应用程序授权创建的任何摄取。

服务账户令牌

您必须拥有来自服务帐号的1Password服务帐号令牌才能进入 AppFabric 1Password应用程序授权。如果您还没有服务账户令牌，请使用以下步骤创建：

AppFabric 将请求服务帐号令牌。中的服务帐号令牌 AppFabric是您创建的个人访问令牌。在 1Password 门户中完成以下步骤以查找个人访问令牌。

1. 选择控制面板。
2. 选择 “人员”。
3. 选择账户所有者姓名。
4. 选择私有。
5. 选择 “查看保管库”。
6. 选择代币名称。

客户授权

AppFabric 使用租户 ID、租户名称和服务帐号令牌在中创建应用程序授权。然后选择 Connect 以激活授权。

配置Asana为 AppFabric

Asana 是一个工作管理平台，可帮助个人、团队和组织协调工作，涵盖日常任务到跨职能战略计划。它提供了清晰的生态系统，每个人都可以在其中沟通、协作和协调。借助 Asana，团队可以将关键业务工具整合到一个地方，这样无论工作在何处出现，都能向前推进。

AWS AppFabric 出于安全考虑，您可以使用来审核来自的日志和用户数据Asana，将数据标准化为开放网络安全架构框架 (OCSF) 格式，并将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

AppFabric 支持 Asana

AppFabric 支持接收来自的用户信息和审核日志Asana。

先决条件

AppFabric 要使用将审核日志从支持的目标传输Asana到支持的目的地，您必须满足以下要求：

- 您必须拥有具有 Asana 的企业账户。有关创建或升级到 Asana 企业账户的更多信息，请参阅 Asana 网站上的 Asana 企业账户。
- 您的 Asana 账户中必须有具有超级管理员角色的用户。有关角色的更多信息，请参阅 Asana 网站上的 Asana 中的管理员和超级管理员角色。

速率限制注意事项

Asana 对 Asana API 施加速率限制。有关 Asana API 速率限制的更多信息，请参阅 Asana 开发人员指南网站上的速率限制。如果 AppFabric 和您的现有Asana应用程序的组合超过限制，则显示在中的审核日志 AppFabric 可能会延迟。

数据延迟注意事项

审计事件发送到目标位置的时间可能会延迟多达 30 分钟。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。不过，这可以在账户级别进行自定义。如需帮助，请联系 支持。

正在 AppFabric 连接您的Asana账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric使用进行授权Asana。要查找授权所需的信息 Asana AppFabric，请按以下步骤操作。

应用程序授权

租户编号

AppFabric 将请求您的租户 ID。中的租户 ID AppFabric 在中称为域 ID Asana。要查找域 ID，请按照 Asana 主屏幕上的以下说明进行操作：

1. 选择您的账户个人资料头像，然后选择管理员控制台。
2. 然后选择设置。
3. 滚动到域设置。
4. 将此部分中的域 ID 输入到 AppFabric 租户 ID 配置中。

租户名称

输入标识此唯一Asana组织的名称。 AppFabric 使用租户名称来标记应用程序授权和通过应用程序授权创建的任何摄取。

服务账户令牌

您必须拥有来自服务帐号的Asana服务帐号令牌才能进入 AppFabric Asana应用程序授权。如果您还没有服务账户令牌，请使用以下步骤创建：

1. 要创建服务账户，请按照 Asana 指南网站上的服务账户中的说明进行操作。
2. 首次查看添加服务账户页面时，请复制并保存添加服务账户页面底部的令牌。
3. 如果您在保存令牌之前关闭了添加服务账户页面，则必须编辑您的服务账户，生成新的令牌并进行保存。

配置Azure Monitor为 AppFabric

Azure Monitor是一款全面的监控解决方案，用于收集、分析和响应来自云端和本地环境的监控数据。您可以使用Azure Monitor来最大限度地提高应用程序和服务的可用性和性能。它可以帮助您了解应用程序的性能，并允许您手动和以编程方式响应系统事件。

Azure Monitor跨多个 Azure 和非 Azure 订阅和租户收集和聚合来自系统每个层和组件的数据。它将其存储在通用数据平台中，供一组常用工具使用，这些工具可以关联、分析、可视化和 and/or 响应数据。你也可以集成其他微软和非微软工具。Azure Monitor活动日志是一种平台日志，可提供对订阅级别事件的见解。活动日志包含诸如资源何时修改或虚拟机何时启动之类的信息。

AWS AppFabric 出于安全考虑，您可以使用来审核来自的日志和用户数据Azure Monitor，将数据标准化为开放网络安全架构框架 (OCSF) 格式，并将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

- AppFabric 支持 Azure Monitor
- 正在 AppFabric 连接您的Azure Monitor账户

AppFabric 支持 Azure Monitor

AppFabric 能够从以下Azure Monitor服务接收用户信息和审核日志：

- Azure Monitor
- API Management
- Microsoft Sentinel
- Security Center

先决条件

AppFabric 要使用将审核日志从支持的目标传输Azure Monitor到支持的目的地，您必须满足以下要求：

- 您需要拥有一个可以免费试用或 pay-as-you-go订阅的Microsoft Azure帐户。
- 至少需要一次订阅才能获取该订阅中的事件。

速率限制注意事项

Azure Monitor对提出请求的安全主体（用户或应用程序）以及订阅 ID 或租户 ID 施加速率限制。有关 Azure Monitor API 速率限制的更多信息，请参阅Azure Monitor开发者网站上的 “了解Azure Resource Manager如何限制请求”。

数据延迟注意事项

审计事件发送到目标位置的时间可能会延迟多达 30 分钟。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。不过，这可以在账户级别进行自定义。如需帮助，请联系 支持。

正在 AppFabric 连接您的Azure Monitor账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric使用进行授权Azure Monitor。要查找授权所需的信息 Azure Monitor AppFabric，请使用以下步骤。

创建 OAuth 应用程序

AppFabric 与Azure Monitor使用集成 OAuth2。要在中创建 OAuth2 应用程序，请完成以下步骤Azure Monitor：

1. 导航到Microsoft Azure门户网站并登录。
2. 导航到 Microsoft EntraID。
3. 选择 “应用程序注册”。
4. 选择 “新注册”。

5. 输入客户机的名称，例如Azure Monitor OAuth客户端。这将是已注册应用程序的名称。
6. 验证 “支持的账户类型” 是否设置为 “单租户”。
7. 对于重定向 URI，选择 Web 作为平台并添加重定向 URI。使用以下格式作为重定向 URI：

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   该地址中*<region>*是您在其中配置 AppFabric 应用程序包的代码。 AWS 区域 例如，美国东部（弗吉尼亚州北部）区域的代码为 us-east-1。对于该区域，重定向 URL 为 https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。

   成功对用户进行身份验证后，身份验证响应将发送到提供的 URI。现在提供此值是可选的，以后可以更改，但是大多数身份验证方案都需要一个值。
8. 选择注册。
9. 在已注册的应用程序中，选择 “证书和机密”，然后选择 “新建客户机密”。
10. 为密钥添加描述。
11. 选择密钥到期时间。您可以从下拉列表中选择任何预设持续时间或设置自定义持续时间。
12. 选择添加。客户端密钥值只能在创建后立即查看。离开页面之前，请务必将密钥保存在安全的地方。

所需的权限

您必须向 OAuth 应用程序添加以下权限。要添加权限，请按照《Microsoft Entra开发者指南》的 “添加访问您的 Web API 的权限” 部分中的说明进行操作。

- Microsoft Graph用户访问 API > User.Read.All（选择委托类型）
- Microsoft Graph用户访问 API > offline_access（选择委托类型）
- Azure服务管理审计日志 API > user_impersonation（选择委托类型）

添加权限后，要授予管理员对这些权限的同意，请按照《Microsoft Entra开发者指南》的 “管理员同意” 按钮部分中的说明进行操作。

应用程序授权

AppFabric 支持从您的Azure Monitor账户接收用户信息和审核日志。要同时接收来自的审核日志和用户数据Azure Monitor，您必须创建两个应用程序授权，一个在应用程序授权下拉列表Azure Monitor中命名，另一个在应用程序授权下拉列表中命名为 Azure Monitor Audit L ogs。您可以为两个应用程序授

权使用相同的租户 ID、客户端 ID 和客户端密钥。要接收来自的审核日志，Azure Monitor您需要同时获得审核日志应用程序Azure Monitor和 Audi Azure Monitort Logs 应用程序的授权。要单独使用用户访问工具，只需要Azure Monitor应用程序授权。

租户编号

AppFabric 将请求您的租户 ID。完成以下步骤，在 Azure 监视器中查找你的客户端 ID：

1. 导航到门Microsoft Azure户。
2. 导航到 Azure 活动目录。
3. 在“应用程序注册”部分，选择之前创建的应用程序。
4. 在“概述”部分，从“目录（租户）ID”字段中复制租户 ID。

租户名称

输入标识此唯一Azure Monitor订阅的名称。 AppFabric 使用租户名称来标记应用程序授权和通过应用程序授权创建的任何摄取。

> **Note**
>
> 租户名称最多应为 2,048 个字符，由数字、 lower/upper 大小写字母和以下特殊字符组成：句点 (.)、下划线 (_)、破折号 (-) 和空格。

客户端 ID

AppFabric 将请求客户端 ID。完成以下步骤以在中查找您的客户端 IDAzure Monitor：

1. 导航到门Microsoft Azure户。
2. 导航到 Azure 活动目录。
3. 在“应用程序注册”部分，选择之前创建的应用程序。
4. 在“概述”部分，从“应用程序（客户端）ID”字段中复制客户端 ID。

客户端密钥

AppFabric 将请求客户机密钥。注册 OAuth 应用程序的客户端密钥是您在 OAuth 应用程序创建部分的步骤 11 中生成的密钥。如果您放错了在应用程序创建期间生成的客户端密钥，请重复 OAuth OAuth 应用程序创建部分中的步骤 8-11 以重新生成一个新的密钥。

App 授权

在中创建应用程序授权后 AppFabric，您将收到一个Microsoft Azure用于批准授权的弹出窗口。从窗口登录您的帐户，然后选择 “允许” 以批准 AppFabric 授权。

配置Atlassian Confluence为 AppFabric

在一个地方创建、协作和整理所有工作。Confluence 是一个团队工作区，知识和协作在这里交汇。动态页面为您的团队提供了一个创建、捕获和协作处理任何项目或想法的地方。Spaces 可帮助您的团队构建、组织和共享工作，因此每个团队成员都可以了解机构知识，并可以访问他们最佳完成工作所需的信息。

AWS AppFabric 为了安全起见，您可以使用接收来自的审计日志和用户数据Confluence，将数据标准化为开放网络安全架构框架 (OCSF) 格式，然后将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

AppFabric 支持 Atlassian Confluence

AppFabric 支持从接收审核日志Atlassian Confluence。

先决条件

AppFabric 要使用将审核日志从支持的目标传输Atlassian Confluence到支持的目的地，您必须满足以下要求：

- 要访问审计日志，您需要拥有一个标准帐户、高级帐户或企业帐户。如需详细了解如何创建或升级到适用的 Confluence 计划类型，请参阅 Atlassian 网站上的 Confluence 定价。
- 要访问审计日志，您需要对您的帐户拥有管理员权限。有关角色的详细信息，请参阅在 Atlassian 支持网站上的向用户授予管理员权限。

速率限制注意事项

Confluence 对 Atlassian Confluence API 施加速率限制。如果您的现有 API 应用程序 AppFabric 和您的现有 Atlassian Confluence API 应用程序Atlassian Confluence的组合超出限制，则显示在中的审核日志 AppFabric 可能会延迟。

数据延迟注意事项

审计事件发送到目标位置的时间可能会延迟多达 30 分钟。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。不过，这可以在账户级别进行自定义。如需帮助，请联系 支持。

正在 AppFabric 连接您的Atlassian Confluence账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric使用进行授权Atlassian Confluence。要查找授权所需的信息 Atlassian Confluence AppFabric，请使用以下步骤。

创建 OAuth 应用程序

AppFabric 与Atlassian Confluence使用集成 OAuth。要在中创建 OAuth 应用程序Atlassian Confluence，请使用以下步骤。

1. 导航到 Atlassian 开发人员控制台。
2. 在右上角选择您的个人资料图标，然后选择开发人员控制台。
3. 在 “我的应用程序” 旁边，选择 “创建，OAuth 2.0 集成”。
4. 在左侧导航窗格中选择权限，然后选择 Confluence API 旁边的添加。
5. 在经典范围下，选择读取用户 (`read:confluence-user`)。
6. 在精细范围下，选择查看审计记录 (`read:audit-log:confluence`)。
7. 在左侧导航窗格中选择 “授权”，然后选择 OAuth 2.0 (3LO) 旁边的 “添加”。
8. 在回调 URL 文本框中使用以下格式的重定向 URL，然后选择保存更改。

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   此 URL AWS 区域 中*<region>*是您在其中配置 AppFabric 应用程序包的代码。例如，美国东部（弗吉尼亚州北部）区域的代码为 `us-east-1`。对于该区域，重定向 URL 为 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`。

所需范围

您必须向Atlassian Confluence OAuth 应用程序添加以下范围之一。有关范围的更多信息，请参阅Atlassian开发者网站上的适用于 OAuth 2.0 (3LO) 和 Forge 应用程序的范围。如果可用，请使用经典范围。

- 经典范围：

  - `read:confluence-user`
- 精细范围：
  - `read:audit-log:confluence`

应用程序授权

租户编号

AppFabric 将请求您的租户 ID。中的租户 ID AppFabric 是您的Atlassian Confluence实例子域。您可以在浏览器地址栏 https:// 和 .atlassian.net 之间找到您的 Atlassian Confluence 实例子域。

租户名称

输入标识此唯一Atlassian Confluence组织的名称。 AppFabric 使用租户名称来标记应用程序授权和通过应用程序授权创建的任何摄取。

客户端 ID

AppFabric 将请求客户端 ID。要在 Atlassian Confluence 中查找您的客户端 ID，请按以下步骤操作：

1. 导航到 Atlassian 开发人员控制台。
2. 在右上角选择您的个人资料图标，然后选择开发人员控制台、我的应用程序。
3. 选择用于连接的 OAuth 应用程序 AppFabric。
4. 在 “设置” 页面的 “客户端 ID” 字段中输入客户端 ID AppFabric。

客户端密钥

AppFabric 将请求客户机密钥。要在 Atlassian Confluence 中查找您的客户端密钥，请执行以下步骤：

1. 导航到 Atlassian 开发人员控制台。
2. 在右上角选择您的个人资料图标，然后选择开发人员控制台、我的应用程序。
3. 选择用于连接的 OAuth 应用程序 AppFabric。
4. 在 “设置” 页面的 “客户机密” 字段中输入密钥 AppFabric。

批准授权

在中创建应用程序授权后 AppFabric，您将收到一个Atlassian Confluence用于批准授权的弹出窗口。要批准 AppFabric 授权，请选择允许。

配置Atlassian Jira suite为 AppFabric

Atlassian 可以释放每个团队的潜力。他们敏捷 DevOps的 IT 服务管理和工作管理软件可帮助团队组织、讨论和完成共享工作。财富 500 强中的大多数企业和全球逾 240,000 家各种规模的公司（包括美国国家航空航天局 (NASA)、Kiva、Deutsche Bank 和 Salesforce）都依靠 Atlassian 解决方案来帮助其团队更好地协同工作，按时交付高质量的成果。在 Atlassian 中了解更多 Atlassian 产品信息，包括 Jira Software、Confluence、Jira Service Management、Trello、Bitbucket 和 Jira Align。

AWS AppFabric 为了安全起见，您可以使用来审计来自Jira suite（除外Jira Align）的日志和用户数据，将数据标准化为开放网络安全架构框架 (OCSF) 格式，然后将数据输出到亚马逊简单存储服务 (Amazon S3) Simple S3 存储桶或亚马逊数据 Firehose 流。

主题

- AppFabric 支持 Jira suite
- 正在 AppFabric 连接您的Jira账户

AppFabric 支持 Jira suite

AppFabric 支持从接收用户信息和审核日志Jira suite，但除外Jira Align。

先决条件

AppFabric 要使用将审核日志从传输Jira suite到支持的目的地，您必须满足以下要求：

- 您必须购买 Jira 标准套餐或更高级的套餐。有关 Jira 套餐功能的更多信息，请参阅 Jira 软件、Jira 服务管理、Jira 工作管理和 Jira 产品发现定价页面。
- 您的 Jira 账户中必须有具有组织管理员角色的用户。有关角色的详细信息，请参阅在 Atlassian 支持网站上的向用户授予管理员权限。

速率限制注意事项

该 Jira 套件对 Jira API 施加了速率限制。有关 Jira suite API 速率限制的更多信息，请参阅 Atlassian 开发人员指南 网站上的速率限制。如果 AppFabric 和您的现有 Jira API 应用程序的组合超过限制，则显示在中的审核日志 AppFabric 可能会延迟。

数据延迟注意事项

审计事件发送到目标位置的时间可能会延迟多达 30 分钟。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。不过，这可以在账户级别进行自定义。如需帮助，请联系 支持。

正在 AppFabric 连接您的Jira账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric使用进行授权Jira。要查找授权所需的信息 Jira AppFabric，请使用以下步骤。

创建 OAuth 应用程序

AppFabric 与Jira suite使用集成 OAuth。要在中创建 OAuth 应用程序Jira，请按以下步骤操作：

1. 导航到 Atlassian 开发人员控制台。
2. 在 “我的应用程序” 旁边，选择 “创建，OAuth 2.0 集成”。
3. 为您的应用程序提供一个名称，然后选择创建。
4. 导航到 “授权” 部分，然后选择 OAuth 2.0 旁边的 “添加”。
5. 在回调 URL 字段中使用以下格式的 URL，然后选择保存更改。

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   此 URL 中*<region>*是您在其中配置 AppFabric 应用程序包的代码。 AWS 区域 例如，美国东部（弗吉尼亚州北部）区域的代码为 `us-east-1`。对于该区域，重定向 URL 为 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`。
6. 导航至 “设置” 部分，复制您的客户端 ID 和客户端密钥，然后将其保存以用于 AppFabric 应用程序授权。

所需范围

您必须将以下范围添加到Jira OAuth 应用程序的 “权限” 页面：

- 在经典范围 (Classic Scopes) 下：
  - Jira API > `read:jira-user`
- 在精细范围 (Granular Scopes) 下：
  - Jira API > `read:audit-log:jira`
  - Jira API > `read:user:jira`

应用程序授权

租户编号

AppFabric 将请求您的租户 ID。中的租户 ID AppFabric 是您的Jira实例子域。您可以在浏览器地址栏 https:// 和 .atlassian.net 之间找到您的 Jira 实例子域。

租户名称

输入标识此唯一Jira服务器的名称。 AppFabric使用租户名称来标记应用程序授权和通过应用程序授权创建的任何摄取。

客户端 ID

AppFabric 将要求您提供客户端 ID。要在 Jira 中查找您的客户端 ID，请按以下步骤操作：

1. 导航到 Atlassian 开发人员控制台。
2. 选择用于连接的 OAuth 应用程序 AppFabric。
3. 在 “设置” 页面的 “客户端 ID” 字段中输入客户端 ID AppFabric。

客户端密钥

AppFabric 将请求您的客户机密钥。中的客户端密钥 AppFabric 是中的密钥Jira。要在 Jira 中查找您的密钥，请按以下步骤操作：

1. 导航到 Atlassian 开发人员控制台。
2. 选择用于连接的 OAuth 应用程序 AppFabric。
3. 在 “设置” 页面的 “客户机密” 字段中输入密钥 AppFabric。

批准授权

在中创建应用程序授权后， AppFabric 您将收到一个Jira用于批准授权的弹出窗口。要批准 AppFabric 授权，请选择允许。

配置Box为 AppFabric

Box是领先的 Content Cloud，它是一个单一平台，使组织能够管理整个内容生命周期、随时随地安全工作以及跨 best-of-breed应用程序集成。

您可以使用 AWS AppFabric 接收来自的审计日志和用户数据Box，将数据标准化为开放网络安全架构框架 (OCSF) 格式，然后将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

AppFabric 支持 Box

AppFabric 支持接收来自的用户信息和审核日志Box。

先决条件

AppFabric 要使用将审核日志从支持的目标传输Box到支持的目的地，您必须满足以下要求：

- 要访问审核日志，您需要有效付费订阅商务版、商务增强版、企业版或企业增强版套餐。
- 您必须拥有具有管理员权限的用户。
- 您的Box账户必须启用双重身份验证，才能从 “配置” 选项卡中查看和复制应用程序的客户端密钥。

速率限制注意事项

Box 对 Box API 施加速率限制。有关 Box API 速率限制的更多信息，请参阅《Box开发者指南》网站上的速率限制。如果 AppFabric 和您的现有Box应用程序的组合超过限制，则显示在中的审核日志 AppFabric 可能会延迟。

数据延迟注意事项

在审核事件中，您可能会看到最长延迟 30 分钟才能送达目的地。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。但是，这可以在账户级别上进行自定义。如需帮助，请联系支持。

正在 AppFabric 连接您的Box账户

在 AppFabric 服务中创建应用程序包后，需要 AppFabric使用进行授权Box。要查找授权所需的信息 Box AppFabric，请按以下步骤操作。

创建 OAuth 应用程序

AppFabric 与Box使用集成 OAuth。使用以下步骤在中Box创建 OAuth 应用程序。有关更多信息，请参阅在Box网站上创建 OAuth 应用程序。

1. 登录Box并进入开发者控制台。
2. 选择创建新的应用程序。
3. 从应用程序类型列表中选择 “自定义应用程序”。将出现一个模态，提示您选择下一步操作。
4. 输入应用程序名称和描述。
5. 从 “目的” 下拉列表中选择 “集成”。
   a. 从 “类别” 下拉列表中选择 “安全与合规”。
   b. 输入AWS AppFabric Secure您要与哪个外部系统集成？ 文本框。
6. 如果您想使用客户端 ID 和客户端密钥验证应用程序身份，请选择服务器身份验证（授予客户端凭证）。
7. 选择 Create App（创建应用程序）。
8. 选择配置选项卡。
9. 在该页面的 “应用程序访问级别” 部分，选择 “应用程序 + 企业访问权限”。
10. 在页面的 “应用程序范围” 部分，选择 “管理用户” 和 “管理企业属性”。
11. 选择保存更改。

    Box管理员需要先在Box管理员控制台中对应用程序进行授权，然后才能使用该应用程序。要申请授权，请完成以下步骤。

    a. 在开发者控制台中为您的应用程序选择 “授权” 选项卡。
    b. 选择 “查看并提交”，向您的Box企业管理员发送一封电子邮件以供审批。有关更多信息，请参阅Box指南中的授权。

> **Note**
>
> 如果提交后有任何更改，则必须重新提交应用程序。

所需范围

以下应用程序范围是必需的。有关作用域的更多信息，请参阅 Box 文档网站上的作用域。

- 管理企业财产 (manage_enterprise_properties)
- 管理用户 (manage_managed_users)

应用程序授权

租户编号

AppFabric 将请求租户 ID。中的租户 ID AppFabric 是Box企业 ID。Box企业 ID 可在管理员控制台的“账户和账单” > “账户信息” > “企业 ID” 下找到。有关更多信息，请参阅 Box 文档网站上的企业 ID。

租户名称

输入标识此唯一Box组织的名称。 AppFabric 使用租户名称来标记应用程序授权以及通过应用程序授权创建的任何摄取。

客户端 ID 和客户端密钥

1. 登录Box并进入开发者控制台。
2. 在导航菜单中选择 “我的应用程序”。
3. 选择用于连接的 OAuth 应用程序 AppFabric。
4. 选择配置选项卡。
5. 滚动至该页面的 Oauth 2.0 凭据部分。
6. 将您的客户 ID 中的客户 OAuth 端 ID 输入到的 “客户端 ID” 字段中 AppFabric。
7. 选择 “获取客户机密钥”。
8. 在的 “客户密钥” 字段中输入来自您的 OAuth 客户密钥的客户密钥 AppFabric。

配置Cisco Duo为 AppFabric

Cisco Duo使用领先的访问管理套件来防范漏洞，该套件提供强大的多层防御和创新功能，允许合法用户进入并将不良行为者拒之门外。对于任何担心被入侵并需要快速解决方案的组织，可以Cisco Duo快速实现强大的安全性，同时还可以提高用户的工作效率。

AWS AppFabric 为了安全起见，您可以使用接收来自的审计日志和用户数据Cisco Duo，将数据标准化为开放网络安全架构框架 (OCSF) 格式，然后将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

AppFabric 支持 Cisco Duo

AppFabric 支持接收来自的用户信息和审核日志Cisco Duo。

先决条件

AppFabric 要使用将审核日志从支持的目标传输Cisco Duo到支持的目的地，您必须满足以下要求：

- 要访问审核日志，你需要有效订阅 Duo Essentials、Duo Advantage 或 Duo Premier 版。或者，拥有 Advantage 或 Premier 试用版的新客户也可以访问。有关Cisco Duo版本的更多信息，请参阅版本和定价。
- 您需要是具有所有者角色的管理员才能创建或修改管理员 API。
- 您需要添加 “授予读取日志资源” 权限，才能在管理员 API 中访问审核日志。

速率限制注意事项

Cisco Duo 对 Cisco Duo API 施加速率限制。有关 Cisco Duo API 速率限制的更多信息，请参阅身份验证日志下的速率限制。如果您的现有 API 应用程序 AppFabric 和您的现有 Cisco Duo API 应用程序Cisco Duo的组合超出限制，则显示在中的审核日志 AppFabric 可能会延迟。如果您需要提高速率限制，请联系 Cisco Duo。

数据延迟注意事项

审计事件发送到目标位置的时间可能会延迟多达 30 分钟。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。不过，这可以在账户级别进行自定义。如需帮助，请联系 支持。

Connect AppFabric 到你的Cisco Duo账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric使用进行授权Cisco Duo。要查找授权所需的信息 Cisco Duo AppFabric，请按以下步骤操作。

创建Cisco Duo管理 API 应用程序

AppFabric 与Cisco Duo使用 API 服务令牌集成。要在中创建应用程序Cisco Duo，请使用以下步骤。

- 要创建Cisco Duo管理员 API 应用程序，请按照Cisco Duo管理 API 中的第一步中的说明进行操作。

所需的权限

您必须将以下范围添加到您的Cisco Duo应用程序中：

- 授予读取日志
- 授予读取资源

应用程序授权

租户编号

AppFabric 将请求租户 ID。您可以在Cisco Duo主机名中找到租户 ID。要在中查找主机名Cisco Duo，请按照以下步骤操作。

1. 导航到 “Cisco Duo管理员登录” 页面并登录。
2. 导航到 “应用程序”，然后选择 “保护应用程序”。
3. 在应用程序列表中找到 Admin API 的条目，然后选择最右边的 Prot ec t 来配置您的应用程序并获取 API 主机名。
4. API 主机名的格式为`api-<tenant-id>.duosecurity.com`，其中*<tenant-id>*是租户 ID。

租户名称

输入标识此唯一Cisco Duo组织的名称。 AppFabric 使用租户名称来标记应用程序授权和通过应用程序授权创建的任何摄取。

服务令牌

AppFabric 将请求服务令牌。服务令牌是以冒号分隔的集成密钥和密钥，格式如下。

```
integrationkey:secretkey
```

要在中查找您的集成密钥和密钥Cisco Duo，请使用以下步骤。

1. 导航到 “Cisco Duo管理员登录” 页面并登录。
2. 导航到 “应用程序”，然后选择 “保护应用程序”。
3. “单击 “保护应用程序”，然后在应用程序列表中找到 Admin API 的条目。单击最右侧的 “保护” 以配置应用程序。向下滚动到范围部分并添加**`Grant read log`**和**`Grant read resource`**。

配置Dropbox为 AppFabric

Dropbox 通过将您的员工聚集在一起，帮助您的组织更快更好地完成工作，无论他们在做什么，在哪里工作，或者碰巧在使用什么样的工具。它通过提供一种简单、安全的内容共享方式，使用户能够加快创新和提高效率。Dropbox 是保持生活井然有序和保持工作顺利进行的地方。在 180 个国家/地区拥有超过 7 亿注册用户，Dropbox 的使命是设计一种更开明的工作方式。

AWS AppFabric 出于安全考虑，您可以使用来审核来自的日志和用户数据Dropbox，将数据标准化为开放网络安全架构框架 (OCSF) 格式，并将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

AppFabric 支持 Dropbox

AppFabric 支持接收来自的用户信息和审核日志Dropbox。

先决条件

AppFabric 要使用将审核日志从支持的目标传输Dropbox到支持的目的地，您必须满足以下要求：

- 您必须拥有 Dropbox 企业账户。如需详细了解如何创建或升级到 Dropbox 企业账户，请参阅 Dropbox 网站上的 Dropbox Business。
- 您的 Dropbox 账户中必须有具有团队管理员角色的用户。有关角色的更多信息，请参阅 Dropbox 帮助中心网站上的如何更改 Dropbox 团队的管理员权限。

速率限制注意事项

Dropbox 对 Dropbox API 施加速率限制。有关 Dropbox API 速率限制的更多信息，请参阅 Dropbox 性能指南网站上的速率限制。如果 AppFabric 和您的现有 Dropbox API 应用程序的组合超过限制，则显示在中的审核日志 AppFabric 可能会延迟。

数据延迟注意事项

审计事件发送到目标位置的时间可能会延迟多达 30 分钟。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。不过，这可以在账户级别进行自定义。如需帮助，请联系 支持。

正在 AppFabric 连接您的Dropbox账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric使用进行授权Dropbox。要查找授权所需的信息 Dropbox AppFabric，请使用以下步骤。

创建 OAuth 应用程序

AppFabric 与Dropbox使用集成 OAuth。要在中创建 OAuth应用程序Dropbox，请按以下步骤操作：

1. 在应用程序控制台的Dropbox应用程序中选择 “创建https://www.dropbox.com/developers/应用程序”。
2. 在新的应用程序配置页面上，选择 API 的作用域访问权限。
3. 接下来，为访问类型选择完整 Dropbox。
4. 为您的 OAuth 应用程序命名，然后选择创建应用程序以完成 OAuth 应用程序的初始设置。
5. 在应用程序信息页面上，在重定向 URIs 字段中添加采用以下格式的 OAuth2 重定向 URL。

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   此 URL 中*<region>*是您在其中配置 AppFabric 应用程序包的代码。 AWS 区域 例如，美国东部（弗吉尼亚州北部）区域的代码为 us-east-1。对于该区域，重定向 URL 为 https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。
6. 选择添加。
7. 复制并保存您的应用程序密钥和应用程序密钥，以便在 AppFabric 应用程序授权中使用。
8. 您可以将设置选项卡上的所有其他字段保留为默认值。

所需范围

您必须使用应用程序信息屏幕上的权限选项卡向 Dropbox 应用程序添加以下范围：

- account_info.read
- team_data.member
- events.read
- members.read
- team_info.read

完成后选择提交。

应用程序授权

租户编号

AppFabric 将请求您的租户 ID。输入任意一个可以唯一地标识您 Dropbox 账户的值，例如团队名称。

租户名称

输入标识此唯一Dropbox帐户的名称。 AppFabric使用租户名称来标记应用程序授权和通过应用程序授权创建的任何摄取。

客户端 ID

AppFabric 将请求客户端 ID。中的客户端 ID AppFabric 是您的Dropbox应用程序密钥。要查找您的 Dropbox 应用密钥，请按照以下步骤进行操作：

1. 在Dropbox应用程序中导航到应用程序控制台。https://www.dropbox.com/developers/
2. 找到你用来连接的应用程序 AppFabric。
3. 在应用程序信息页面的状态部分中找到应用程序密钥。
4. 在的 “客户端 ID” 字段中输入Dropbox应用程序的应用程序密钥 AppFabric。

客户端密钥

AppFabric 将请求客户机密钥。中的客户端密钥 AppFabric 是您的Dropbox应用程序密钥。要查找您的 Dropbox 应用程序私匙，请按照以下步骤进行操作：

1. 在Dropbox应用程序中导航到应用程序控制台。https://www.dropbox.com/developers/
2. 找到你用来连接的应用程序 AppFabric。
3. 在应用程序信息页面的状态部分中找到应用程序私匙。
4. 在的 “客户端密钥” 字段中输入Dropbox应用程序的应用程序密钥 AppFabric。

批准授权

在中创建应用程序授权后 AppFabric，您将收到一个Dropbox用于批准授权的弹出窗口。要批准 AppFabric 授权，请选择允许。

配置Genesys Cloud为 AppFabric

Genesys Cloud通过简单的 all-in-one界面在数字和语音渠道上创建流畅的对话。这使公司能够为员工和客户提供卓越的体验，并从快速部署、降低复杂性和简单管理中获益。

AWS AppFabric 为了安全起见，您可以使用接收来自的审计日志和用户数据Genesys Cloud，将数据标准化为开放网络安全架构框架 (OCSF) 格式，然后将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

AppFabric 支持 Genesys Cloud

AppFabric 支持接收来自的用户信息和审核日志Genesys Cloud。

先决条件

AppFabric 要使用将审核日志从支持的目标传输Genesys Cloud到支持的目的地，您必须满足以下要求：

- 您必须具有 Genesys Cloud 账户。
- 您的 Genesys Cloud 账户中必须有具有管理员角色的用户。

速率限制注意事项

Genesys Cloud 对 Genesys Cloud API 施加速率限制。有关 Genesys Cloud API 速率限制的更多信息，请参阅 Genesys Cloud Developer 网站上的速率限制。

数据延迟注意事项

审计事件发送到目标位置的时间可能会延迟多达 30 分钟。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。不过，这可以在账户级别进行自定义。如需帮助，请联系 支持。

正在 AppFabric 连接您的Genesys Cloud账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric使用进行授权Genesys Cloud。要查找授权所需的信息 Genesys Cloud AppFabric，请使用以下步骤。

创建 OAuth 应用程序

AppFabric 与Genesys Cloud使用集成 OAuth。要在中创建 OAuth应用程序Genesys Cloud，请按以下步骤操作：

1. 按照Genesys Cloud资源中心网站的 “创建 OAuth 客户端” 中的说明进行操作。

   对于授权类型，选择代码授权。
2. 使用以下格式的重定向 URL 作为授权重定向 URIs。

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   此 URL AWS 区域 中*<region>*是您在其中配置 AppFabric 应用程序包的代码。例如，美国东部（弗吉尼亚州北部）区域的代码为 us-east-1。对于该区域，重定向 URL 为 https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。
3. 选择范围框以显示您的应用程序可用的范围列表。选择范围audits:readonly然后users:readonly。有关范围的信息，请参阅Genesys Cloud开发人员中心中的OAuth 作用域。
4. 选择保存。Genesys Cloud 会创建客户端 ID 和客户端密钥（令牌）。

所需范围

您必须在Genesys Cloud OAuth应用程序中添加以下范围：

- audits:readonly
- users:readonly

应用程序授权

租户编号

AppFabric 将请求您的租户 ID。中的租户 ID AppFabric 是您的Genesys Cloud实例名称。您可以在浏览器的地址栏中找到租户 ID。例如，usw2.pure.cloud 是以下 URL https://login.usw2.pure.cloud 中的租户 ID。

租户名称

输入标识此唯一Genesys Cloud组织的名称。 AppFabric 使用租户名称来标记应用程序授权和通过应用程序授权创建的任何摄取。

客户端 ID

AppFabric 将请求客户端 ID。要在 Genesys Cloud 中查找您的客户端 ID，请按以下步骤操作：

1. 选择管理员。
2. 在 “集成” 下，选择OAuth。
3. 选择要获取 OAuth 客户端 ID 的客户端。

客户端密钥

AppFabric 将请求客户机密钥。要在 Genesys Cloud 中查找您的客户端密钥，请执行以下步骤：

1. 选择管理员。
2. 在 “集成” 下，选择OAuth。
3. 选择要获取 OAuth 客户端密钥的客户端。

配置GitHub为 AppFabric

GitHub 是使用 Git 进行软件开发和版本控制的平台和云服务，允许开发人员存储和管理他们的代码。它为每个项目提供 Git 的分布式版本控制以及访问控制、错误跟踪、软件功能请求、任务管理、持续集成和 Wiki。

AWS AppFabric 为了安全起见，您可以使用接收来自的审计日志和用户数据GitHub，将数据标准化为开放网络安全架构框架 (OCSF) 格式，然后将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

- AppFabric 支持 GitHub
- 正在 AppFabric 连接您的GitHub账户

AppFabric 支持 GitHub

AppFabric 支持接收来自的用户信息和审核日志GitHub。

先决条件

AppFabric 要使用将审核日志从支持的目标传输GitHub到支持的目的地，您必须满足以下要求：

- 要访问审核日志，您需要拥有一个企业账户。
- 要访问企业审核日志，您需要拥有企业账户的管理员角色。

- 要从组织获取审核日志，您需要成为组织所有者。

速率限制注意事项

GitHub 对 GitHub API 施加速率限制。有关 GitHub API 速率限制的更多信息，请参阅 GitHub 网站上的 API 请求限制和分配。如果您的现有 API 应用程序 AppFabric 和您的现有 GitHub API 应用程序的组合超过GitHub's限制，则中显示的审核日志 AppFabric 可能会延迟。

数据延迟注意事项

审计事件发送到目标位置的时间可能会延迟多达 30 分钟。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。不过，这可以在账户级别进行自定义。如需帮助，请联系 支持。

正在 AppFabric 连接您的GitHub账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric使用进行授权GitHub。要查找授权所需的信息 GitHub AppFabric，请使用以下步骤。

创建 OAuth 应用程序

AppFabric 与GitHub使用集成 OAuth。使用以下步骤在中创建 OAuth 应用程序GitHub。有关更多信息，请参阅GitHub网站上的创建 GitHubs 应用程序。

1. 选择页面右上角的个人头像，然后选择设置。
2. 在左侧导航窗格中，选择开发人员设置。
3. 在左侧导航窗格中选择OAuth 应用程序。
4. 选择 “新建 OAuth 应用程序”。

> **Note**
>
> 如果您之前没有创建过应用程序，则此按钮将被标记为 “注册新 OAuth应用程序”。

5. 在应用程序名称文本框中输入您的应用程序的名称。
6. 在主页 URL 文本框中输入完整的应用程序实例 URL。
7. （可选）在应用程序描述文本框中输入应用程序描述。用户将看到此描述。
8. 在授权回调 URL 文本框中输入以下格式的 URL。

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

此 URL 中*<region>*是您在其中配置 AppFabric 应用程序包的代码。 AWS 区域 例如，美国东部（弗吉尼亚州北部）区域的代码为 us-east-1。对于该区域，重定向 URL 为 https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。

9. 如果您的 OAuth 应用程序将使用设备流来识别和授权用户，请选择启用设备流。有关设备流程的更多信息，请参阅在GitHub网站上对 OAuth 应用程序进行授权。
10. 选择注册应用程序。

应用程序授权

租户编号

AppFabric 将请求您的租户 ID。应使用以下任一格式提供租户 ID：

企业审核日志：

如果您想了解企业账户拥有的所有组织的汇总操作，请使用企业的审核日志。

使用企业审核日志时，租户 ID 就是您账户的企业 ID。您可以在浏览器的地址栏中找到企业 ID。例如，*exampleenterprise* 是以下 URL https://github.com/settings/enterprises/*examplenterprise* 中的企业 ID。

为企业审核日志指定租户 ID 时，前缀必须为 enterprise:。因此，将前面的示例指定为 enterprise:examplenterprise。

组织审核日志：

如果您想了解组织成员执行的操作，请以组织管理员的身份使用组织审核日志。它包括谁执行了操作、操作是什么以及何时执行等详细信息。

使用组织审核日志时，租户 ID 就是您的组织 ID。您可以在浏览器的地址栏中找到组织 ID。例如，*exampleorganization* 是以下 URL https://github.com/settings/organizations/*exampleorganization* 中的组织 ID。

在为组织审核日志指定租户 ID 时，前缀必须为 organization:。因此，将前面的示例指定为 organization:exampleorganization。

租户名称

输入标识此唯一GitHub企业或组织的名称。 AppFabric 使用租户名称来标记应用程序授权和通过应用程序授权创建的任何摄取。

客户端 ID

AppFabric 将请求客户端 ID。使用以下步骤在 GitHub 中查找您的客户端 ID，

1. 选择页面右上角的个人头像，然后选择设置。
2. 在左侧导航窗格中，选择开发人员设置。
3. 在左侧导航窗格中选择OAuth 应用程序。
4. 选择特定的 OAuth 应用程序，然后查找客户端 ID 值。

客户端密钥

AppFabric 将请求客户机密钥。使用以下步骤在 GitHub 中查找您的客户端密钥。

1. 选择页面右上角的个人头像，然后选择设置。
2. 在左侧导航窗格中，选择开发人员设置。
3. 在左侧导航窗格中选择OAuth 应用程序。
4. 选择特定的 OAuth 应用程序，然后查找 “客户端密钥” 值。如果您找不到现有的客户端密钥，则可能需要生成一个新的客户端密钥。

批准授权

在中创建应用程序授权后 AppFabric，您将收到一个GitHub用于批准授权的弹出窗口。要批准 AppFabric 授权，请选择允许。

如果启用了 OAuth 应用程序访问限制，请确保您的组织已授予对OAuth 应用程序的访问权限。

配置Google Analytics为 AppFabric

Google Analytics是一项网络分析服务，为搜索引擎优化 (SEO) 和营销目的提供统计数据和基本分析工具。 Google Analytics用于跟踪网站性能和收集访客见解。它可以帮助组织确定用户流量的主要来源，衡量其营销活动和活动的成功，跟踪目标完成情况（例如购买、将产品添加到购物车），发现用户参与的模式和趋势，并获取其他访客信息，例如人口统计信息。中小型零售网站通常用于Google Analytics获取和分析各种客户行为分析，这些分析可用于改善营销活动、增加网站流量和更好地留住访客。

AWS AppFabric 出于安全考虑，您可以使用来审核来自的日志和用户数据Azure Monitor，将数据标准化为开放网络安全架构框架 (OCSF) 格式，并将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

AppFabric 支持 Google Analytics

AppFabric 支持从接收审核日志Google Analytics。

先决条件

AppFabric 要使用将审核日志从支持的目标传输Google Analytics到支持的目的地，您必须满足以下要求：

- 您必须是该Google Analytics账户的管理员。
- AppFabric 要传送日志，您需要在Google Cloud项目上启用Google Analytics管理员 API。设置 Google Analytics OAuth 应用程序时，请务必使用新项目。

速率限制注意事项

Google Analytics 对 Google Analytics API 施加速率限制。有关 Google Analytics API 速率限制的更多信息，请参阅 Google Analytics（分析）网站上的限制和配额。如果 AppFabric 与您现有的 Google Analytics API 应用程序组合超过限制，则显示在中的审核日志 AppFabric 可能会延迟。

数据延迟注意事项

审计事件发送到目标位置的时间可能会延迟多达 30 分钟。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。不过，这可以在账户级别进行自定义。如需帮助，请联系 支持。

正在 AppFabric 连接您的Google Analytics账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric使用进行授权Google Analytics。使用以下步骤查找授权Google Analytics所需的信息 AppFabric。

创建 OAuth 应用程序

AppFabric 与Google Analytics使用集成 OAuth。要在中创建 OAuth 应用程序，请完成以下步骤 Google Analytics：

1. 要配置您的 OAuth 同意屏幕，请按照 Google 网站上《Google 开发者指南》中配置 OAuth 同意屏幕中的说明进行操作。

2. 选择 “外部” 作为 “用户” 类型
3. 要为配置 OAuth 凭据 AppFabric，请按照《Google 开发者指南》中 “创建访问凭据” 页面的 “ OAuth 客户端 ID 凭据” 部分中的说明进行操作。
4. 使用以下格式的重定向 URL。

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

该地址中*<region>*是您在其中配置 AppFabric 应用程序包的代码。 AWS 区域 例如，美国东部（弗吉尼亚州北部）区域的代码为 us-east-1。对于该区域，重定向 URL 为 https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。

所需范围

您必须在Google Analytics OAuth应用程序中添加以下作用域：

```
https://www.googleapis.com/auth/analytics.edit
```

应用程序授权

租户编号

AppFabric 将请求租户 ID。中的租户 ID AppFabric 是您的Google Analytics账户 ID。

1. 转到Google Analytics主页。
2. 在导航窗格中选择 “管理员”。
3. 您可以在 “账户” > “账户设置” > “账户详情” > “账户 ID” 下找到您的账户 ID。

租户名称

输入标识此唯一Google Analytics组织的名称。 AppFabric 使用租户名称来标记应用程序授权和通过应用程序授权创建的任何摄取。

客户端 ID

AppFabric 将请求客户端 ID。使用以下步骤在中查找您的客户端 IDGoogle Analytics：

1. 转到 “凭证” 页面。
2. 在 “OAuth 2.0 客户端 IDs” 部分，选择您创建的客户端 ID。

3. 客户端 ID 列在页面的 “其他信息” 部分。

客户端密钥

AppFabric 将请求客户机密钥。使用以下步骤在中查找您的客户端密钥Google Analytics：

1. 转到 “凭证” 页面。
2. 在 “OAuth 2.0 客户端 IDs” 部分中，选择客户机名称。
3. 该页面的 “客户机密钥” 部分列出了客户机密钥。

App 授权

在中创建应用程序授权后，AppFabric 您将收到一个Google Analytics用于批准授权的弹出窗口。通过选择 “允许” 来批准 AppFabric 授权。

配置Google Workspace为 AppFabric

Google Workspace 是 Google 开发和销售的云计算、生产力和协作工具、软件和产品的集合。

AWS AppFabric 出于安全考虑，您可以使用来审核来自的日志和用户数据Google Workspace，将数据标准化为开放网络安全架构框架 (OCSF) 格式，并将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

- AppFabric 支持 Google Workspace
- 正在 AppFabric 连接您的Google Workspace账户

AppFabric 支持 Google Workspace

AppFabric 支持接收来自的用户信息和审核日志Google Workspace。

先决条件

AppFabric 要使用将审核日志从支持的目标传输Google Workspace到支持的目的地，您必须满足以下要求：

- 您必须订阅 Google Workspace Enterprise Standard 计划。如需了解如何创建或升级到 Google Workspace Enterprise Standard 计划，请访问 Google Workspace 计划网站。
- 您 Google Workspace 中的用户中必须有具有管理员角色的用户。

- AppFabric 要交付日志，你需要在谷歌云项目上启用 Google Admin SDK API。如需了解详情，请参阅Google Workspace开发者指南 APIs中的启用 Google 工作空间。

速率限制注意事项

Google Workspace 对 Google Workspace API 施加速率限制。有关 Google Workspace API 速率限制的更多信息，请参阅 Google Workspace 网站 Google Workspace 管理员指南中的限制和配额。如果 AppFabric 和您的现有 Google Workspace API 应用程序的组合超过限制，则显示在中的审核日志 AppFabric 可能会延迟。

数据延迟注意事项

大多数审计事件可能会延迟 30 分钟，某些审计事件可能延迟最多 4 小时才能送达目的地。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。有关更多信息，请参阅 Google WorkSpace 管理员帮助网站中的数据保留和延迟时间。不过，这可以在账户级别进行自定义。如需帮助，请联系支持。

正在 AppFabric 连接您的Google Workspace账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric使用进行授权Google Workspace。要查找授权所需的信息 Google Workspace AppFabric，请使用以下步骤。

创建 OAuth 应用程序

AppFabric 与Google Workspace使用集成 OAuth。要在中创建 OAuth 应用程序Google Workspace，请按以下步骤操作：

1. 要配置您的 OAuth 同意屏幕，请按照Google Workspace网站《Google Workspace开发者指南》中配置 OAuth 同意屏幕中的说明进行操作。

   为用户类型选择内部。
2. 要为配置 OAuth 证书 AppFabric，请按照《Google Workspace 开发人员指南》中 “创建访问凭证”页面的 “OAuth 客户端 ID 凭证” 部分中的说明进行操作。
3. 使用以下格式的重定向 URL。

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   此 URL AWS 区域 中*<region>*是您在其中配置 AppFabric 应用程序包的代码。例如，美国东部（弗吉尼亚州北部）区域的代码为 us-east-1。对于该区域，重定向 URL 为 https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。

所需范围

您必须在Google Workspace OAuth应用程序中添加以下范围：

- `https://www.googleapis.com/auth/admin.reports.audit.readonly`
- `https://www.googleapis.com/auth/admin.directory.user`

如果您没有看到这些范围，请将管理软件开发工具包 API 添加到您的 Google Cloud API 库中。

应用程序授权

租户编号

AppFabric 将请求您的租户 ID。中的租户 ID AppFabric 是您的Google Workspace项目 ID。要查找您的项目 ID，请参阅在 Google API 控制台帮助网站上找到项目 ID。

租户名称

输入标识此唯一值的名称Google Workspace。 AppFabric 使用租户名称来标记应用程序授权和通过应用程序授权创建的任何摄取。

客户端 ID

AppFabric 将要求您提供客户端 ID。要查找您的 客户端 ID，请按以下步骤操作：

1. 使用 Google Workspace 开发人员指南中管理凭证页面的查看凭证部分中的信息查找您的客户端 ID。
2. 在的 “客户端 ID” 字段中输入客户的客户端 ID AppFabric。 OAuth

客户端密钥

AppFabric 将请求您的客户机密钥。要查找 客户端密钥，请按以下步骤操作：

1. 使用 Google Workspace开发人员指南 中管理凭证页面的查看凭证部分中的信息查找您的客户端密钥。
2. 如果您需要重置您的客户端密钥，请按照 Google Workspace开发人员指南中管理凭证页面的重置客户端密钥部分中的说明进行操作。
3. 在的客户密钥字段中输入您的客户密钥 AppFabric。

批准授权

在中创建应用程序授权后， AppFabric 您将收到一个Google Workspace用于批准授权的弹出窗口。要批准 AppFabric 授权，请选择允许。

配置HubSpot为 AppFabric

HubSpot 是一个客户平台，包含连接营销、销售、内容管理和客户服务所需的所有软件、集成和资源。HubSpot 的互联平台使您能够专注于最重要的事情：您的客户，从而更快地发展业务。

AWS AppFabric 为了安全起见，您可以使用接收来自的审计日志和用户数据HubSpot，将数据标准化为开放网络安全架构框架 (OCSF) 格式，然后将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

AppFabric 支持 HubSpot

AppFabric 支持接收来自的用户信息和审核日志HubSpot。

先决条件

AppFabric 要使用将审核日志从支持的目标传输HubSpot到支持的目的地，您必须满足以下要求：

- 您必须在 HubSpot 中拥有具有企业订阅的帐户，才能访问访问审计日志。有关 HubSpot 订阅的更多信息，请参阅 HubSpot 知识库上的管理您的 HubSpot 订阅。
- 您必须拥有开发人员账户以及与该账户关联的应用程序。
- 您应该是超级管理员才能在自己的 HubSpot 账户中安装应用程序，或者拥有 App Marketplace 访问权限以及接受应用程序请求的范围的用户权限。

速率限制注意事项

HubSpot 对 HubSpot API 施加速率限制。有关 HubSpot API 速率限制的更多信息，包括应用程序的使用限制 OAuth，请参阅HubSpot网站上的速率限制。如果您的现有 API 应用程序 AppFabric 和您的现有 HubSpot API 应用程序HubSpot的组合超出限制，则显示在中的审核日志 AppFabric 可能会延迟。

数据延迟注意事项

审计事件发送到目标位置的时间可能会延迟多达 30 分钟。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。不过，这可以在账户级别进行自定义。如需帮助，请联系 支持。

正在 AppFabric 连接您的HubSpot账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric使用进行授权HubSpot。要查找授权所需的信息 HubSpot AppFabric，请按以下步骤操作。

创建 OAuth 应用程序

AppFabric 与HubSpot使用集成 OAuth。要在中创建 OAuth应用程序HubSpot，请按以下步骤操作：

1. 按照 HubSpot 网站上的 HubSpot 指南中的创建公共应用程序部分中的说明进行操作。
2. 从身份验证选项卡，添加 所需范围 中列出的三个范围。
3. 在重定向 URL 中使用以下格式的重定向 URL。

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   此 URL AWS 区域 中*<region>*是您在其中配置 AppFabric 应用程序包的代码。例如，美国东部（弗吉尼亚州北部）区域的代码为 us-east-1。对于该区域，重定向 URL 为 https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。
4. 选择创建应用程序。

所需范围

您必须将以下范围添加到您的HubSpot OAuth应用程序中：

- settings.users.read
- crm.objects.owners.read
- account-info.security.read

应用程序授权

租户编号

输入标识此唯一 HubSpot 组织的 ID。例如，输入您的 HubSpot 账户 ID。

租户名称

输入标识此唯一HubSpot组织的名称。 AppFabric 使用租户名称来标记应用程序授权和通过应用程序授权创建的任何摄取。

客户端 ID

AppFabric 将请求客户端 ID。要在 HubSpot 中查找您的客户端 ID，请按以下步骤操作：

1. 导航到 HubSpot 登录页面，并使用您的开发人员账户凭证登录。
2. 从应用程序菜单，选择您的应用程序。
3. 从身份验证选项卡中,查找客户端 ID 值。

客户端密钥

AppFabric 将请求客户机密钥。要在 HubSpot 中查找您的客户端密钥，请执行以下步骤：

1. 导航到 HubSpot 登录页面，并使用您的开发人员账户凭证登录。
2. 从应用程序菜单，选择您的应用程序。
3. 从身份验证选项卡，查找客户端密钥值。

批准授权

在中创建应用程序授权后 AppFabric，您将收到一个HubSpot用于批准授权的弹出窗口。使用您的企业账户凭证（不是您的开发者账户）登录您的账户以批准 AppFabric 授权。选择允许。

配置IBM Security® Verify为 AppFabric

该IBM Security® Verify系列提供自动化、基于云的本地功能，用于管理身份管理、管理员工和消费者的身份和访问权限以及控制特权账户。无论您需要部署云端还是本地解决方案，都可以IBM Security® Verify帮助您建立信任并防范员工和消费者面临的内部威胁。

AWS AppFabric 为了安全起见，您可以使用接收来自的审计日志和用户数据IBM Security® Verify，将数据标准化为开放网络安全架构框架 (OCSF) 格式，然后将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

- AppFabric 支持 IBM Security® Verify
- 正在 AppFabric 连接您的IBM Security® Verify账户

AppFabric 支持 IBM Security® Verify

AppFabric 支持接收来自的用户信息和审核日志IBM Security® Verify。

先决条件

AppFabric 要使用将审核日志从支持的目标传输IBM Security® Verify到支持的目的地，您必须满足以下要求：

- 要访问审核日志，您需要拥有 IBM Security® VerifySaaS 帐户。
- 要访问审核日志，您需要在 IBM Security® Verify SaaS 账户中拥有管理员角色。

速率限制注意事项

IBM Security® Verify 对 IBM Security® Verify API 施加速率限制。有关 IBM Security® Verify API 速率限制的更多信息，请参阅 IBM 条款。如果您的现有 API 应用程序 AppFabric 和您的现有 IBM Security® Verify API 应用程序的组合超过IBM Security® Verify限制，则显示在中的审核日志 AppFabric 可能会延迟。

数据延迟注意事项

在审核事件中，您可能会看到最长延迟 30 分钟才能送达目的地。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。但是，这可以在账户级别上进行自定义。如需帮助，请联系支持。

正在 AppFabric 连接您的IBM Security® Verify账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric使用进行授权IBM Security® Verify。要查找授权所需的信息 IBM Security® Verify AppFabric，请按以下步骤操作。

创建 OAuth 应用程序

AppFabric 与IBM Security® Verify使用集成 OAuth。要在中创建 OAuth 应用程序IBM Security® Verify，请参阅 I BM 文档网站上的创建 API 客户端。

1. 首次登录时，请使用发送到您注册的电子邮件地址的登录 URL 和凭据。
2. 访问管理控制台，网址为`https://<hostname>.verify.ibm.com/ui/admin/`。有关更多信息，请参阅访问 IBM Security® Verify。
3. 在管理控制台中，在安全 < API 访问权限 < API 客户端下，选择添加。
4. 选择以下选项。这些是读取审核日志和用户详细信息所必需的。

- 阅读报告
- 读取用户和组

5. 保留 “客户机身份验证” 方法中的 “默认” 选项。

   请勿编辑 “自定义范围” 字段。

6. 选择下一步。
7. 不要编辑 IP 筛选器字段。
8. 选择下一步。
9. 不要编辑 “其他属性” 字段。
10. 选择下一步。
11. 指定名称和描述。描述是可选的。
12. 选择创建 API 客户端。

应用程序授权

租户编号

AppFabric 将请求您的租户 ID。您可以在IBM Security® Verify标准 URL 中找到租户 ID。例如，在 `https://hostname.verify.ibm.com/` URL 中，租户 ID 是在之前可以找到的`.verify.ibm.com`（`ice.ibmcloud.com`如果您使用*hostname*的是以前的主机名，则在之前找到）。如果您使用的是虚名 URL，请联系您的IBM Security® Verify支持团队以获取标准网址。

租户名称

输入标识此唯一IBM Security® Verify租户的名称。 AppFabric 使用租户名称来标记应用程序授权以及通过应用程序授权创建的任何摄取。

客户端 ID

AppFabric 将请求客户端 ID。要在 IBM Security® Verify 中查找您的客户端 ID，请按以下步骤操作：

1. 首次登录时，请使用发送到您注册的电子邮件地址的登录 URL 和凭据。
2. 访问管理控制台，网址为`https://<hostname>.verify.ibm.com/ui/admin/`。有关更多信息，请参阅访问 IBM Security® Verify。
3. 在管理控制台中，在 “安全 < API Acces s < API 客户端” 下，选择特定 OAuth 应用程序旁边的省略号 (‹)。

4. 选择 “连接详细信息”。
5. 在 API 凭证下找到客户端 ID。

客户端密钥

AppFabric 将请求客户机密钥。要在 IBM Security® Verify 中查找您的客户端密钥，请执行以下步骤：

1. 首次登录时，请使用发送到您注册的电子邮件地址的登录 URL 和凭据。
2. 访问管理控制台，网址为`https://<hostname>.verify.ibm.com/ui/admin/`。有关更多信息，请参阅访问 IBM Security® Verify。
3. 在管理控制台中，在 “安全 < API Acces s < API 客户端” 下，选择特定 OAuth 应用程序旁边的省略号 (‹)。
4. 选择 “连接详细信息”。
5. 在 API 凭据下找到客户端密钥。

配置JumpCloud为 AppFabric

JumpCloud Inc. 是一家美国企业软件公司，为身份管理提供基于云的目录平台。它集中并简化了身份管理，允许用户使用一组凭据安全地访问其系统、应用程序、网络和文件服务器，无论平台、协议、提供商或位置如何。

您可以使用 AWS AppFabric 接收来自的审计日志和用户数据 JumpCloud，将数据标准化为开放网络安全架构框架 (OCSF) 格式，然后将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

- AppFabric 支持 JumpCloud
- 正在 AppFabric 连接您的JumpCloud账户

AppFabric 支持 JumpCloud

AppFabric 支持接收来自的用户信息和审核日志JumpCloud。

先决条件

AppFabric 要使用将审核日志从支持的目标传输JumpCloud到支持的目的地，您必须满足以下要求：

- 您必须拥有有效的付费JumpCloud订阅计划。有关更多信息，请参见Select a package that's right for youJumpCloud网站。
- 您必须具有 “账单管理员” 角色。

速率限制注意事项

JumpCloud 不发布速率限制。您必须创建支持案例或联系您的JumpCloud客户团队。如果您的现有 API 应用程序 AppFabric 和您的现有 JumpCloud API 应用程序的组合超过JumpCloud's限制，则显示在中的审核日志 AppFabric 可能会延迟。

数据延迟注意事项

审计事件发送到目标位置的时间可能会延迟多达 30 分钟。这是由于应用程序提供的审计事件出现延迟，以及为减少数据丢失而采取的预防措施。不过，这可以在账户级别进行自定义。如需帮助，请联系支持。

正在 AppFabric 连接您的JumpCloud账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric 使用进行授权JumpCloud。要查找授权JumpCloud所需的信息 AppFabric，请按照下一节中的步骤操作。

使用该JumpCloud账户创建组织令牌

AppFabric 使用 API 密钥与JumpCloud集成要在中创建 API 密钥 JumpCloud，请按照以下步骤操作：。

1. 以管理员身份登录您的JumpCloud帐户。
2. 在管理门户中，选择右上角的账户首字母缩写，然后从菜单中选择 “我的 API 密钥”。
3. 选择 “生成新 API 密钥”，或选择现有密钥。

> **Note**
>
> JumpCloud只允许使用一个有效的 API 密钥。生成新的 API 密钥将撤消对当前 API 密钥的访问权限。这将导致所有使用之前的 API 密钥的调用都无法访问。您必须使用新的密钥值更新使用先前 API 密钥的所有现有集成。

应用程序授权

租户编号

AppFabric 将请求您的租户 ID。这里的 “组织 ID” 将是租户 ID。要查找 “组织 ID”，请按照以下步骤操作。

1. 登录您的 JumpCloud 账户。
2. 在导航窗格中，依次选择设置、组织配置文件和常规。
3. 选择 “眼睛” 图标以删除模糊的视图。
4. 选择 “双页” 图标以复制身份证。

租户名称

输入标识此唯一JumpCloud组织的名称。 AppFabric 使用租户名称来标记应用程序授权和通过应用程序授权创建的任何摄取。

服务账户令牌

AppFabric 将请求您的服务帐号令牌。在中 AppFabric，这是您在本主题前面部分中创建的使用该 JumpCloud账户创建组织令牌组织 API 令牌。

将 Microsoft 365 配置为 AppFabric

Microsoft 365 是一个由生产力软件、协作工具和基于云的服务组成的产品系列，由 Microsoft 拥有。

AWS AppFabric 为了安全起见，您可以使用来审计来自 Microsoft 365 的日志和用户数据，将数据标准化为开放网络安全架构框架 (OCSF) 格式，并将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

- AppFabric 支持 Microsoft 365
- 正在连接 AppFabric 您的 Microsoft 365 账户

AppFabric 支持 Microsoft 365

AppFabric 支持从 Microsoft 365 接收用户信息和审核日志。

先决条件

AppFabric 要使用将审核日志从 Microsoft 365 传输到支持的目的地，您必须满足以下要求：

- 您必须订阅 Microsoft 365 企业版计划。有关创建或升级到 Microsoft 365 企业版计划的更多信息，请参阅 Microsoft 网站上的 Microsoft 365 企业版计划。
- 您的 Microsoft 365 账户中必须有具有管理员权限的用户。
- 您必须为组织开启审核日志。有关更多信息，请参阅在 Microsoft 网站上开启或关闭审计。

速率限制注意事项

Microsoft 365 对 Microsoft 365 API 施加了速率限制。有关 Microsoft 365 API 速率限制的更多信息，请参阅 Microsoft 网站上 Microsoft Graph 文档中特定于 Microsoft Graph 服务的节流限制。如果 AppFabric 和您现有的 Microsoft 365 API 应用程序的组合超过限制，则显示在中的审核日志 AppFabric 可能会延迟。

数据延迟注意事项

审计事件发送到目标位置的时间可能会延迟多达 30 分钟。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。不过，这可以在账户级别进行自定义。如需帮助，请联系 支持。

正在连接 AppFabric 您的 Microsoft 365 账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric使用 Microsoft 365 进行授权。要查找授权 Microsoft 365 所需的信息 AppFabric，请使用以下步骤。

创建 OAuth 应用程序

AppFabric 使用与 Microsoft 365 集成 OAuth。要在 Microsoft 365 中创建 OAuth应用程序，请使用以下步骤：

1. 按照 Microsoft 网站 Azure Active Directory 开发人员指南中注册应用程序部分中的说明进行操作。

   在支持的账户类型配置中仅选择此组织目录中的账户。
2. 按照 Azure Active Directory 开发人员指南中的添加重定向 URI部分中的说明进行操作。

   选择 Web 平台。

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

此 URL AWS 区域 中*<region>*是您在其中配置 AppFabric 应用程序包的代码。例如，美国东部（弗吉尼亚州北部）区域的代码为 us-east-1。对于该区域，重定向 URL 为 https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。

您可以跳过 Web 平台的其他输入字段。

3. 按照 Azure Active Directory 开发人员指南的添加客户端密钥部分中的说明进行操作。

所需的权限

您必须向 OAuth 应用程序添加以下权限。要添加权限，请按照 Azure Active Directory 开发人员指南的添加用于访问您的 Web API 的权限部分中的说明进行操作。

- Microsoft Graph API > User.Read（自动添加）
- Office 365 Management APIs > ActivityFeed.Read（选择委托类型）
- Office 365 Management APIs > ActivityFeed.ReadDlp（选择委托类型）
- Office 365 Management APIs > ServiceHealth.Read（选择委托类型）

添加权限后，要授予管理员对这些权限的同意，请按照 Azure Active Directory 开发人员指南的管理员同意按钮部分中的说明进行操作。

应用程序授权

AppFabric 支持从您的 Microsoft 365 账户接收用户信息和审核日志。要同时接收来自 Microsoft 365 的审核日志和用户数据，您必须创建两个应用程序授权，一个在应用程序授权下拉列表中名为 Microsoft 365，另一个在应用程序授权下拉列表中名为 Microsoft 365 Audit Log。您可以为两个应用程序授权使用相同的租户 ID、客户端 ID 和客户端密钥。要接收来自 Microsoft 365 的审核日志，您需要同时获得 Microsoft 365 和 Microsoft 365 审核日志应用程序的授权。要单独使用用户访问工具，只需要 Microsoft 365 应用程序授权。

租户编号

AppFabric 将要求您提供租户 ID。中的租户 ID AppFabric 是你的 Azure 活动目录租户 ID。要查找您的 Azure Active Directory 租户 ID，请参阅 Microsoft 网站 Azure 产品文档中的如何查找 Azure Active Directory 租户 ID。

租户名称

输入标识此唯一 Microsoft 365 账户的名称。 AppFabric 使用租户名称来标记应用程序授权和通过应用程序授权创建的任何摄取。

客户端 ID

AppFabric 将要求您提供客户端 ID。中的客户端 ID AppFabric 是 Microsoft 365 应用程序（客户端）ID。要查找您的 Microsoft 365 应用程序（客户端）ID，请使用以下步骤：

1. 打开与您一起使用的 OAuth 应用程序的概述页面 AppFabric。
2. 应用程序（客户端）ID 显示在基本信息下。
3. 在的 “客户端 ID” 字段中输入您的 OAuth 客户的应用程序（客户端）ID AppFabric。

客户端密钥

AppFabric 将请求您的客户机密钥。 Microsoft只有在您最初为 OAuth应用程序创建客户端密钥时，365才会提供此值。要生成新的客户端密钥（如果没有），请按以下步骤操作：

1. 要创建客户端密钥，请按照 Azure Active Directory 开发人员指南的添加客户端密钥部分中的说明进行操作。
2. 在的 “客户机密” 字段中输入 “值” 字段的内容 AppFabric。

批准授权

在中创建应用程序授权后 AppFabric，您将收到来自 Microsoft 365 的弹出窗口，用于批准授权。要批准 AppFabric 授权，请选择允许。

配置Miro为 AppFabric

Miro 是一个用于创新的在线工作空间，能让任何规模的分布式团队共同打造下一件大事。通过该平台的无限画布，团队能够进行引人入胜的研讨会和会议、产品设计、头脑风暴等活动。Miro 公司总部位于旧金山和阿姆斯特丹，全球范围内拥有超过 5000 万用户，其中包括 99% 的财富 100 强公司。Miro 成立于 2011 年，目前在全球 12 个中心拥有超过 1500 名员工。要了解更多信息，请访问 Miro。

Miro 包括一整套专为创新而设计的协作功能，包括绘制图表、线框图、实时数据可视化、研讨会推进以及对敏捷实践、研讨会和交互式演示的内置支持。Miro 近期发布的 Miro AI 扩展了 Miro 的功能，包括 AI 驱动的映射和图表、聚类和摘要以及内容生成。Miro 帮助组织减少独立工具的数量，从而避免信息碎片化和降低成本。

AWS AppFabric 出于安全考虑，您可以使用来审核来自的日志和用户数据Miro，将数据标准化为开放网络安全架构框架 (OCSF) 格式，并将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

AppFabric 支持 Miro

AppFabric 支持接收来自的用户信息和审核日志Miro。

先决条件

AppFabric 要使用将审核日志从支持的目标传输Miro到支持的目的地，您必须满足以下要求：

- 您必须拥有 Miro 企业套餐。有关 Miro 套餐类型的更多信息，请参阅 Miro 网站上的 Miro定价 页面。
- 您的 Miro 账户中必须有具有公司管理员角色的用户。有关角色的更多信息，请参阅 Miro 帮助中心网站上 Miro 中的角色的公司层面部分。
- 您的 Miro 账户中必须有企业开发人员团队。有关创建开发人员团队的信息，请参阅 Miro 帮助中心网站上的企业开发人员团队。

速率限制注意事项

Miro 对 Miro API 施加速率限制。有关 Miro API 速率限制的更多信息，请参阅 Miro 网站上 Miro 开发人员指南中的速率限制。如果 AppFabric 和您的现有 Miro API 应用程序的组合超过限制，则显示在中的审核日志 AppFabric 可能会延迟。

数据延迟注意事项

审计事件发送到目标位置的时间可能会延迟多达 30 分钟。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。不过，这可以在账户级别进行自定义。如需帮助，请联系 支持。

正在 AppFabric 连接您的Miro账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric使用进行授权Miro。要查找授权所需的信息 Miro AppFabric，请使用以下步骤。

创建 OAuth 应用程序

AppFabric 与Miro使用集成 OAuth。要在中创建 OAuth应用程序Miro，请按以下步骤操作：

1. 要创建 OAuth 应用程序，请按照 Miro 帮助中心网站上企业开发者团队文章的 “创建和安装应用程序” 部分中的说明进行操作。
2. 在应用程序创建对话框中，在企业组织中选择开发团队后，选中用户授权令牌过期复选框。

   > **Note**
   >
   > 由于在创建应用程序后无法更改此选项，您必须在创建应用程序之前执行此操作。

3. 在应用程序页面的 “ OAuth 2.0 的重定向 URI” 部分，输入采用以下格式的 UR L。

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   此 URL AWS 区域 中*<region>*是您在其中配置 AppFabric 应用程序包的代码。例如，美国东部（弗吉尼亚州北部）区域的代码为 `us-east-1`。对于该区域，重定向 URL 为 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`。
4. 复制并保存您的客户端 ID 和客户端密钥，以便在 AppFabric 应用程序授权中使用。

所需范围

您必须在Miro OAuth 应用程序页面的`Permissions`部分添加以下范围：

- `auditlogs:read`
- `organizations:read`

应用程序授权

租户编号

AppFabric 将请求您的租户 ID。中的租户 ID AppFabric 是您的Miro团队 ID。有关如何找到您的 Miro 团队 ID 的信息，请参阅我是新 Miro 管理员的常见问题部分。Miro 帮助中心网站上的从哪里开始？

租户名称

输入标识此唯一Miro组织的名称。 AppFabric 使用租户名称来标记应用程序授权和通过应用程序授权创建的任何摄取。

客户端 ID

AppFabric 将要求您提供客户端 ID。要查找您的客户端 ID，请按以下步骤操作：

1. 导航到您的 Miro 个人资料设置。
2. 选择您的应用程序选项卡。
3. 选择您用来连接的应用程序 AppFabric。
4. 在的 “客户端 ID” 字段中输入 “应用程序凭证” 部分中的客户端 ID AppFabric。

客户端密钥

AppFabric 将请求您的客户机密钥。要查找客户端密钥，请按以下步骤操作：

1. 导航到您的 Miro 个人资料设置。
2. 选择您的应用程序选项卡。
3. 选择您用来连接的应用程序 AppFabric。
4. 将应用程序凭证部分中的客户端密钥输入到的客户端密钥字段中 AppFabric。

批准授权

在中创建应用程序授权后 AppFabric，您将收到一个Miro用于批准授权的弹出窗口。要批准 AppFabric 授权，请选择允许。

配置Okta为 AppFabric

Okta 是举世闻名的公司。作为领先的独立身份合作伙伴，Okta 让每个人都可以随时随地在任何设备或应用程序上安全地使用任何技术。最值得信赖的品牌信赖 Okta 能够实现安全访问、身份验证和自动化。灵活性和中立性是 Okta 劳动力身份和客户身份云的核心，借助可定制的解决方案和 7,000 多个预先构建的集成，企业领导者和开发人员可以专注于创新并加快数字化转型。Okta 正在建设一个身份属于您的世界。在 okta .com 上了解更多信息。

AWS AppFabric 出于安全考虑，您可以使用来审核来自的日志和用户数据Okta，将数据标准化为开放网络安全架构框架 (OCSF) 格式，并将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

- AppFabric 支持 Okta

- 正在 AppFabric 连接您的Okta账户

AppFabric 支持 Okta

AppFabric 支持接收来自的用户信息和审核日志Okta。

先决条件

AppFabric 要使用将审核日志从支持的目标传输Okta到支持的目的地，您必须满足以下要求：

- 您可以 AppFabric 与任何Okta计划类型一起使用。
- 您的 Okta 账户中必须有具有超级管理员角色的用户。
- 在中批准应用程序授权的用户还 AppFabric 必须在您的Okta账户中拥有超级管理员角色。

速率限制注意事项

Okta 对 Okta API 施加速率限制。如需详细了解 Okta API 速率限制，请参阅 Okta 网站上 Okta 开发人员指南中的速率限制。如果您的现有 API 应用程序 AppFabric 和您的现有 Okta API 应用程序Okta的组合超出限制，则显示在中的审核日志 AppFabric 可能会延迟。

数据延迟注意事项

审计事件发送到目标位置的时间可能会延迟多达 30 分钟。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。不过，这可以在账户级别进行自定义。如需帮助，请联系 支持。

正在 AppFabric 连接您的Okta账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric使用进行授权Okta。要查找授权所需的信息 Okta AppFabric，请使用以下步骤。

创建 OAuth 应用程序

AppFabric 与Okta使用集成 OAuth。要创建要连接的 OAuth应用程序 AppFabric，请按照Okta帮助中心网站创建 OIDC 应用程序集成中的说明进行操作。以下是以下配置注意事项 AppFabric：

1. 对于应用程序类型，选择 Web 应用程序。
2. 对于授予类型，请选择授权码和刷新令牌。
3. 使用以下格式的重定向 URL 作为登录重定向 URI 和注销重定向 URI。

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

此 URL AWS 区域 中*<region>*是您在其中配置 AppFabric 应用程序包的代码。例如，美国东部（弗吉尼亚州北部）区域的代码为 us-east-1。对于该区域，重定向 URL 为 https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。

4. 您可以跳过可信来源配置。
5. 在受控访问配置中向 Okta 组织中的每个人授予访问权限。

> **Note**
>
> 如果您在初始创建 OAuth 应用程序时跳过此步骤，则可以使用应用程序配置页面上的 “任务” 选项卡将组织中的所有人分配为一个小组。

6. 您可以将所有其他选项保留为默认值。

所需范围

您必须将以下范围添加到您的Okta OAuth应用程序中：

- okta.logs.read
- okta.users.read

应用程序授权

租户编号

AppFabric 将请求租户 ID。中的租户 ID AppFabric 是您的Okta域名。有关查找 Okta 域名的更多信息，请参阅 Okta 网站上 Okta 开发人员指南中的查找您的 Okta 域名。

租户名称

输入标识此唯一Okta组织的名称。 AppFabric 使用租户名称来标记应用程序授权和通过应用程序授权创建的任何摄取。

客户端 ID

AppFabric 将请求客户端 ID。要在 Okta 中查找您的客户端 ID，请按以下步骤操作：

1. 导航到 Okta 开发人员控制台。
2. 选择应用程序选项卡。
3. 选择您的应用程序，然后选择常规选项卡。
4. 滚动至客户端凭证部分。
5. 在的 “客户端 ID” 字段中输入 OAuth 来自客户的客户端 ID AppFabric。

客户端密钥

AppFabric 将请求客户机密钥。要在 Okta 中查找您的客户端密钥，请执行以下步骤：

1. 导航到 Okta 开发人员控制台。
2. 选择应用程序选项卡。
3. 选择您的应用程序，然后选择常规选项卡。
4. 滚动至客户端凭证部分。
5. 在的 “客户机密钥” 字段中输入 OAuth 应用程序中的客户机密钥 AppFabric。

批准授权

在中创建应用程序授权后 AppFabric，您将收到一个Okta用于批准授权的弹出窗口。要批准 AppFabric 授权，请选择允许。批准 Okta 授权的用户必须在 Okta 中拥有超级管理员权限。

配置OneLogin by One Identity为 AppFabric

OneLogin by One Identity 是一款基于云的现代访问管理解决方案，可为您的员工、客户和合作伙伴无缝管理所有数字身份。OneLogin 提供安全的单点登录 (SSO)、多重身份验证 (MFA)、自适应身份验证、桌面级 MFA、与 AD、LDAP、G Suite 和其他外部目录的目录集成、身份生命周期管理等。借OneLogin助，您可以保护您的组织免受最常见的攻击，从而提高安全性、顺畅的用户体验并遵守监管要求。

AWS AppFabric 为了安全起见，您可以使用接收来自的审计日志和用户数据OneLogin，将数据标准化为开放网络安全架构框架 (OCSF) 格式，然后将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

- AppFabric 支持 OneLogin by One Identity
- 正在 AppFabric 连接您的OneLogin by One Identity账户

AppFabric 支持 OneLogin by One Identity

AppFabric 支持接收来自的用户信息和审核日志OneLogin by One Identity。

先决条件

AppFabric 要使用将审核日志从支持的目标传输OneLogin by One Identity到支持的目的地，您必须满足以下要求：

- 您必须拥有 OneLogin 高级或专业账户。
- 您必须拥有具有 Admin/Delegated 管理员权限的用户。

速率限制注意事项

OneLogin by One Identity 对 OneLogin API 施加速率限制。有关 OneLogin API 速率限制的更多信息，请参阅《OneLogin 参考》中的获取速率限制。如果您的现有 API 应用程序 AppFabric 和您的现有 OneLogin API 应用程序OneLogin的组合超出限制，则显示在中的审核日志 AppFabric 可能会延迟。但是，OneLogin 速率限制可以增加。如需帮助，请联系您的 OneLogin by One Identity 客户经理或者联系 One Identity。

数据延迟注意事项

审计事件发送到目标位置的时间可能会延迟多达 30 分钟。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。不过，这可以在账户级别进行自定义。如需帮助，请联系 支持。

正在 AppFabric 连接您的OneLogin by One Identity账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric使用进行授权OneLogin by One Identity。要查找授权所需的信息 OneLogin AppFabric，请使用以下步骤。

创建 OAuth 应用程序

AppFabric 与OneLogin by One Identity使用集成 OAuth。要在中创建 OAuth 应用程序OneLogin，请按以下步骤操作：

1. 导航到 OneLogin 登录页面并登录。
2. 从开发人员菜单中选择 API 凭证。
3. 选择新凭证，输入新凭证的名称，然后选择全部读取。
4. 选择保存。OneLogin 会创建客户端 ID 和客户端密钥。

所需范围

您必须在OneLogin by One Identity OAuth 应用程序中添加以下范围：

- 全部读取。有关范围和客户端凭证的更多信息，请参阅《OneLogin API 参考》中的使用 API 凭证。

应用程序授权

租户编号

AppFabric 将请求租户 ID。中的租户 ID AppFabric 是您的实例子域。您可以在浏览器的地址栏中找到租户 ID。例如，subdomain 是以下 URL `https://subdomain.onelogin.com` 中的租户 ID。

租户名称

输入标识此唯一OneLogin by One Identity组织的名称。 AppFabric 使用租户名称来标记应用程序授权和通过应用程序授权创建的任何摄取。

客户端 ID

AppFabric 将请求客户端 ID。要在 OneLogin by One Identity 中查找您的客户端 ID，请按以下步骤操作：

1. 导航到 OneLogin 登录页面并登录。
2. 从开发人员菜单中选择 API 凭证。
3. 选择 API 凭证以获取客户端 ID。

客户端密钥

AppFabric 将请求客户机密钥。要在 OneLogin by One Identity 中查找您的客户端密钥，请执行以下步骤：

1. 导航到 OneLogin 登录页面并登录。
2. 从开发人员菜单中选择 API 凭证。
3. 选择 API 凭证以获取客户端密钥。

客户端应用程序授权

在中 AppFabric，使用您的租户 ID 和姓名以及您的客户端 ID 和名称创建应用程序授权。选择“连接”以激活授权。

配置PagerDuty为 AppFabric

PagerDuty 是一个数字运营管理平台，可通过将任何信号转化为行动来帮助团队缓解影响客户的问题，从而更快地解决问题并提高运营效率。与 CloudWatch、GuardDuty、CloudTrail 和 Personal Health Dashboard 集成。

AWS AppFabric 为了安全起见，您可以使用接收来自的审计日志和用户数据PagerDuty，将数据标准化为开放网络安全架构框架 (OCSF) 格式，然后将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

AppFabric 支持 PagerDuty

AppFabric 支持接收来自的用户信息和审核日志PagerDuty。

先决条件

AppFabric 要使用将审核日志从支持的目标传输PagerDuty到支持的目的地，您必须满足以下要求：

- 要访问审计日志，您必须制定 PagerDuty 商业或数字运营计划。
- 您应该是 PagerDuty 账户的全球管理员或账户所有者。

速率限制注意事项

PagerDuty 对 PagerDuty API 施加速率限制。有关 PagerDuty API 速率限制的更多信息，请参阅 PagerDuty 开发人员平台上的 REST API 速率限制。如果您的现有 API 应用程序 AppFabric 和您的现有 PagerDuty API 应用程序PagerDuty的组合超出限制，则显示在中的审核日志 AppFabric可能会延迟。

数据延迟注意事项

审计事件发送到目标位置的时间可能会延迟多达 30 分钟。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。不过，这可以在账户级别进行自定义。如需帮助，请联系 支持。

正在 AppFabric 连接您的PagerDuty账户

PagerDuty 平台支持 API 访问密钥。要生成 API 访问密钥，请使用以下步骤。

创建 API 访问密钥

AppFabric 与PagerDuty使用公共客户端的 API 访问密钥集成。要在 PagerDuty 中创建 API 访问密钥，请使用以下步骤：

1. 导航到 PagerDuty 登录页面并登录。
2. 选择集成、API 访问密钥。
3. 选择新建 API 密钥。
4. 输入描述，然后选择只读 API 密钥。
5. 选择创建密钥。
6. 复制并保存 API 密钥。稍后你会需要这个 AppFabric。如果您在保存 API 密钥之前关闭页面，则必须生成新的 API 密钥并将其保存下来。此密钥应专用于 AppFabric 避免与其他集成共享 PagerDuty API 速率限制。

应用程序授权

租户编号

AppFabric 将请求您的租户 ID。您的 PagerDuty 账户的租户 ID 是您账户的基本 URL。要找到它，请登录到 PagerDuty 并从 Web 浏览器的地址栏中进行复制。租户 ID 应采用下列格式之一：

- 对于美国账户为 *subdomain*.pagerduty.com
- 对于欧盟账户为 *subdomain*.eu.pagerduty.com

租户名称

输入标识此唯一PagerDuty组织的名称。 AppFabric 使用租户名称来标记应用程序授权和通过应用程序授权创建的任何摄取。

服务账户令牌

AppFabric 将请求您的服务帐号令牌。中的服务帐号令牌 AppFabric 是您在中创建的 API 访问密钥创建 API 访问密钥。

配置Ping Identity为 AppFabric

在 Ping Identity，我们坚信不妥协地为所有用户提供安全且无缝的数字体验。这就是超过一半的财富 100 强企业选择 Ping Identity 来保护用户的数字互动，同时让体验顺畅无阻的原因。2023 年 8 月 23

日，Ping Identity 和 ForgeRock 携手为客户和合作伙伴提供更多选择、更深入的专业知识和更完整的身份解决方案。

AWS AppFabric 为了安全起见，您可以使用接收来自的审计日志和用户数据Ping Identity，将数据标准化为开放网络安全架构框架 (OCSF) 格式，然后将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

AppFabric 支持 Ping Identity

AppFabric 支持接收来自的用户信息和审核日志Ping Identity。

先决条件

AppFabric 要使用将审核日志从支持的目标传输Ping Identity到支持的目的地，您必须满足以下要求：

- 您必须拥有 Essential、Plus 或 Premium Ping Identity 帐户。如需详细了解如何创建或升级到适用 Ping Identity 计划类型，请参阅 Ping Identity 网站上Ping Identity所有功能的定价。
- 您的 Ping Identity 账户中必须具有身份数据只读角色。您可以通过为您的应用程序授予角色来向您的账户添加角色。有关角色的更多信息，请参阅 Ping Identity 支持网站上的角色。

速率限制注意事项

Ping Identity 不发布速率限制。您必须创建支持案例或者联系您的 Ping Identity 客户成功团队。如果您的现有 API 应用程序 AppFabric 和您的现有 Ping Identity API 应用程序Ping Identity的组合超出限制，则显示在中的审核日志 AppFabric 可能会延迟。

数据延迟注意事项

审计事件发送到目标位置的时间可能会延迟多达 30 分钟。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。不过，这可以在账户级别进行自定义。如需帮助，请联系 支持。

正在 AppFabric 连接您的Ping Identity账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric使用进行授权Ping Identity。要查找授权所需的信息 Ping Identity AppFabric，请按以下步骤操作。

创建 OAuth 应用程序

AppFabric 与Ping Identity使用集成 OAuth。要在中创建 OAuth应用程序Ping Identity，请按以下步骤操作：

1. 按照 Ping Identity 网站上的《面向开发人员的 PingOne》指南中的创建应用程序连接部分中的说明进行操作。
2. 在创建应用程序后，自定义授权类型。
   a. 登录应用程序后，选择配置选项卡，然后单击铅笔图标以更改现有配置。
   b. 在授权类型下，选择授权码。将 PKCE 强制执行保留为可选。
   c. 选择刷新令牌并选择刷新持续时间。
3. 在重定向 URL 中使用以下格式的重定向 URL/callback URL。

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

此 URL AWS 区域 中*<region>*是您在其中配置 AppFabric 应用程序包的代码。例如，美国东部（弗吉尼亚州北部）区域的代码为 us-east-1。对于该区域，重定向 URL 为 https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。

应用程序授权

租户编号

AppFabric 将请求您的租户 ID。中的租户 ID AppFabric 是您的Ping Identity实例名称。您可以在浏览器的地址栏中找到租户 ID。例如 *API_PATH*/v1/environments/*environmentID*。其中，*API_PATH* 表示 PingOne 服务器的区域域（例如 api.pingone.com），*environmentID* 代表您的应用程序环境属性中指明的环境 ID。有关环境属性的更多信息，请参阅 Ping Identity 网站上的环境属性。

租户名称

输入标识此唯一Ping Identity组织的名称。 AppFabric 使用租户名称来标记应用程序授权和通过应用程序授权创建的任何摄取。

客户端 ID

AppFabric 将请求客户端 ID。要在 Ping Identity 中查找您的客户端 ID，请按以下步骤操作：

1. 登录 PingOne 管理员控制台并选择应用程序。
2. 从列表中选择应用程序。
3. 选择概述选项卡，然后查找客户端 ID 值。

客户端密钥

AppFabric 将请求客户机密钥。要在 Ping Identity 中查找您的客户端密钥，请执行以下步骤：

1. 登录 PingOne 管理员控制台并选择应用程序。
2. 从列表中选择应用程序。
3. 选择概述选项卡，然后查找客户端密钥值。

批准授权

在中创建应用程序授权后 AppFabric，您将收到一个Ping Identity用于批准授权的弹出窗口。要批准 AppFabric 授权，请选择允许。

配置Salesforce为 AppFabric

Salesforce提供基于云的软件，旨在帮助企业找到更多潜在客户，完成更多交易，并以出色的服务让客户赞叹不已。 Salesforce'sCustomer 360 提供一整套产品，将销售、服务、营销、商务和 IT 团队与客户信息的单一共享视图结合在一起，帮助组织发展与客户和员工的关系。

您可以使用 AWS AppFabric 接收来自的审计日志和用户数据Salesforce，将数据标准化为开放网络安全架构框架 (OCSF) 格式，然后将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

- AppFabric 支持 Salesforce
- 正在 AppFabric 连接您的Salesforce账户

AppFabric 支持 Salesforce

AppFabric 支持接收来自的用户信息和审核日志Salesforce。

先决条件

AppFabric 要使用将审核日志从支持的目标传输Salesforce到支持的目的地，您必须满足以下要求：

- 您必须拥有性能版、企业版或无限版的Salesforce。请联系Salesforce以升级到其中一个版本。
- 如果您想按小时 AppFabric 传输事件日志文件以及来自的全套日志事件Salesforce，则必须订阅“事件监控”，这是 Shield 功能的一部分Salesforce。否则， AppFabric将从Salesforce’s标准每日日志文件中传输有限的事件（即登录 InsecureExternalAssets、注销、API 总使用量、CORS 违规和 HostnameRedirects ELF 事件）。你可以前往 “设置” > “活动管理器”，查看你的Salesforce账户是否已经订阅了 Shield Features。如果您看到列出了 19 个或更多事件，则您的账户已订阅事件监控。如果您没有事件监控，则可以通过联系购买此插件的订阅Salesforce。
- 你需要在Salesforce设置中选择启用生成事件日志文件。
- 您应使用系统管理员配置文件创建 OAuth应用程序，并使用相同的凭据登录 AppFabric。

> **Note**
>
> 在支持的版本中，可以免费获得 API 总使用量、CORS 违规记录、主机名重定向、不安全的外部资产、登录和注销事件。Salesforce联系购买Salesforce其余活动类型。有关Salesforce事件类型的更多信息，请参阅Salesforce网站上的EventLogFile 支持的事件类型。
> AppFabric 每个日志文件实例每种事件类型最多可支持 100,000 个事件（每天或每小时，具体取决于事件监控附加订阅）。超过阈值的日志文件可能会导致整个日志文件被排除在摄取范围之外。

速率限制注意事项

Salesforce 对 Salesforce API 施加速率限制。有关 Salesforce API 速率限制的更多信息，请参阅Salesforce网站上的 API 请求限制和分配。如果 AppFabric 和您的现有 Salesforce API 应用程序的组合超过Salesforce’s限制，则显示在中的审核日志 AppFabric 可能会延迟。

数据延迟注意事项

对于将审核事件传送到目的地，您可能会看到每日日志文件最多延迟 6 小时，或者每小时日志文件最多延迟 29 小时。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。不过，这可以在账户级别进行自定义。如需帮助，请联系 支持。

正在 AppFabric 连接您的Salesforce账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric使用进行授权Salesforce。要查找授权所需的信息 Salesforce AppFabric，请按以下步骤操作。

创建 OAuth 应用程序

AppFabric 与Salesforce使用集成 OAuth。要在中创建 OAuth 应用程序Salesforce，请按以下步骤操作：

1. 登录您的Salesforce账户。
2. 按照Salesforce文档中的说明转到 “设置” 页面。
3. 在快速查找中搜索应用程序管理器。
4. 选择 “新建连接的应用程序”。
5. 在表单字段中输入所需信息。
6. 选择 “启用 OAuth 设置”。
7. 请务必关闭以下选项：
   - 对于支持的授权流程，需要验证密钥才能使用代码交换 (PKCE) 扩展
   - Web 服务器流程需要密钥
   - 刷新令牌流程需要密钥
   - 启用刷新令牌轮换
8. 在回调 URL 文本框中输入以下格式的 URL，然后选择保存更改。

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   此 URL 中*<region>*是您在其中配置 AppFabric 应用程序包的代码。 AWS 区域 例如，美国东部（弗吉尼亚州北部）区域的代码为 us-east-1。对于该区域，重定向 URL 为 https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。
9. 根据需要填写范围（将在下一所需范围节中介绍）。所有其他字段均可保留其默认值。
10. 选择保存。
11. 完成以下步骤以验证新 OAuth 应用程序的刷新令牌策略：
    a. 在 “设置” 页面上，在 “快速查找” 文本框中输入 “关联的应用程序”，然后选择 “管理已连接的应用程序”。
    b. 选择新创建的应用程序旁边的编辑。
    c. 确保 “刷新” 令牌在选中 “撤销” 选项之前一直有效。
    d. 保存更改。
12. 完成以下步骤以验证是否正在生成审核日志：

a. 在设置页面上，在快速查找文本框中输入事件日志文件，然后选择事件日志文件浏览器。

b. 确认事件日志已在事件日志文件浏览器中列出。

13. 导航到已创建的应用程序，然后从下拉列表中选择 “查看”。

14. 选择管理使用者详细信息。

    您将被重定向到一个新选项卡，您需要在其中验证您的身份。在该选项卡上，记下消费者密钥和消费者密钥值。稍后您将需要这些文件才能登录。

所需范围

您必须将以下范围添加到您的Salesforce OAuth应用程序中：

- 通过 APIs (API) 管理用户数据。
- 随时执行请求（`refresh_token`和`offline_access`）。

应用程序授权

租户编号

AppFabric 将请求您的租户 ID。中的租户 ID AppFabric 是您的 “Salesforce我的域” 的子域。你可以在浏览器的地址栏中找到 “我的域名” 子域名，介于`https://`和之间。`.my.salesforce.com`

要查找您的Salesforce我的域名，请在Salesforce主屏幕上按照以下说明进行操作。

1. 按照Salesforce文档中的说明转到 “设置” 页面。
2. 在快速查找中搜索 “公司设置”，然后在结果中选择 “我的域名”。

租户名称

输入标识此唯一Salesforce组织的名称。 AppFabric 使用租户名称来标记应用程序授权和通过应用程序授权创建的任何摄取。

客户端 ID

AppFabric 将请求客户端 ID。要在 Salesforce 中查找您的客户端 ID，请按以下步骤操作：

1. 导航到 “设置” 页面。
2. 选择 “设置”，然后选择 “应用程序管理器”。

3. 选择已创建的应用程序，然后从下拉菜单中选择 “查看”。
4. 选择管理使用者详细信息。您将被重定向到新选项卡。
5. 验证您的身份，然后查找消费者密钥值。
6. 在的 “客户端 ID” 字段中输入消费者密钥 AppFabric。

客户端密钥

AppFabric 将请求您的客户机密钥。中的客户机密 AppFabric 是中的消费者密钥Salesforce。要在中找到你的 SecretSalesforce，请按以下步骤操作：

1. 导航到 “设置” 页面。
2. 选择 “设置”，然后选择 “应用程序管理器”。
3. 选择已创建的应用程序，然后从下拉菜单中选择 “查看”。
4. 选择管理使用者详细信息。您将被重定向到新选项卡。
5. 验证您的身份，然后查找 “消费者机密” 值。
6. 在的客户机密字段中输入消费者密钥 AppFabric。

批准授权

在中创建应用程序授权后 AppFabric，您将收到一个Salesforce用于批准授权的弹出窗口。在批准页面，确保在授权时使用Salesforce系统管理员角色或具Salesforce有 “查看事件日志文件” 和 “启用 API” 用户权限的用户。选择 “允许” 以批准 AppFabric 授权。

配置ServiceNow为 AppFabric

ServiceNow是一家领先的基于云的服务提供商，这些服务可实现企业 IT 运营自动化。 ServiceNow的 ITOM 让企业能够全面了解和控制其整个 IT 环境，包括虚拟化和云基础架构。它简化了服务映射、交付和保障，将 IT 服务和基础设施数据整合到一个记录系统中。它还可以自动化和简化关键流程，包括事件、事故、问题、配置和变更管理。

AWS AppFabric 为了安全起见，您可以使用接收来自的审计日志和用户数据ServiceNow，将数据标准化为开放网络安全架构框架 (OCSF) 格式，然后将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

- AppFabric 支持 ServiceNow

- 数据延迟注意事项
- 正在 AppFabric 连接您的ServiceNow账户

AppFabric 支持 ServiceNow

AppFabric 支持接收来自的用户信息和审核日志ServiceNow。

先决条件

AppFabric 要使用将审核日志从支持的目标传输ServiceNow到支持的目的地，您必须满足以下要求：

- 您可以 AppFabric 与任何ServiceNow计划类型一起使用。
- 您的 ServiceNow 账户中必须有具有管理员角色的用户。
- 你必须有一个 ServiceNow 实例。

速率限制注意事项

ServiceNow 对 ServiceNow API 施加速率限制。有关 ServiceNow API 速率限制的更多信息，请参阅 ServiceNow 网站上的入站 REST API 速率限制。如果您的现有 API 应用程序 AppFabric 和您的现有 ServiceNow API 应用程序的组合超过限制，则中显示的审核日志 AppFabric 可能会延迟。

数据延迟注意事项

审计事件发送到目标位置的时间可能会延迟多达 30 分钟。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。不过，这可以在账户级别进行自定义。如需帮助，请联系 支持。

正在 AppFabric 连接您的ServiceNow账户

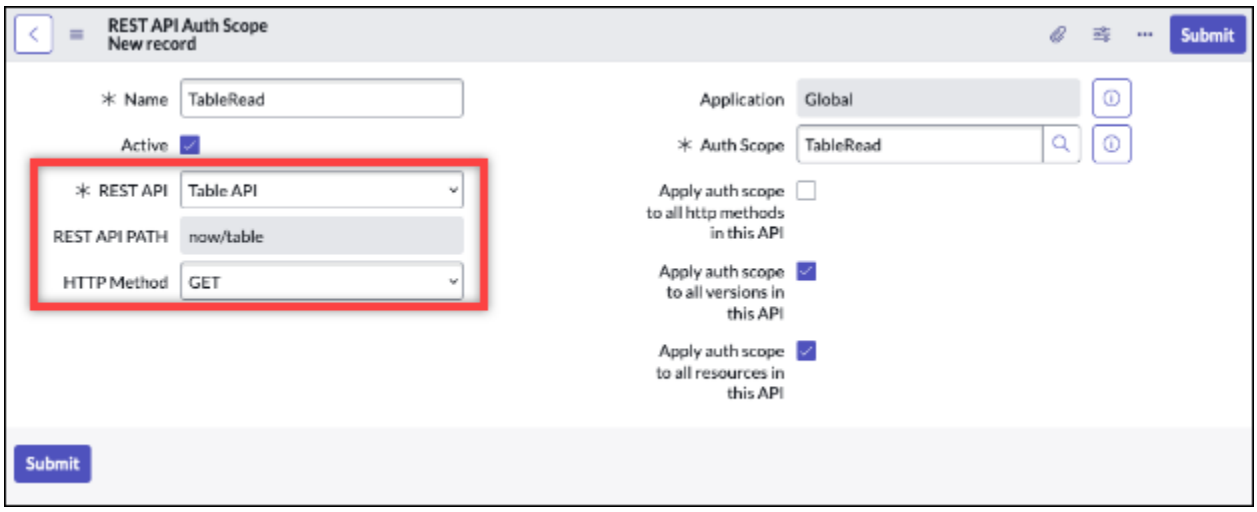
在 AppFabric 服务中创建应用程序包后，必须 AppFabric使用进行授权ServiceNow。使用以下步骤查找授权ServiceNow所需的信息 AppFabric。

创建 OAuth 应用程序

Now Platform支持 OAuth 2.0-授权授予类型，供公共客户端生成访问令牌。

1. 注册您的 OAuth 应用程序。这需要执行以下三个步骤。有关完成这些步骤的更多信息，请参阅 ServiceNow 网站上的 通过 ServiceNow 注册应用程序。

    a. 注册应用程序，并确保 Auth 范围可以访问表 API，REST API 路径为 now/table，HTTP 方法为 GET，如下例所示。



b. 生成授权代码。

c. 使用授权代码生成不记名令牌。

2. 使用以下格式的重定向 URL。

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

此 URL 中*<region>*是您在其中配置 AppFabric 应用程序包的代码。 AWS 区域 例如，美国东部（弗吉尼亚州北部）区域的代码为 `us-east-1`。对于该区域，重定向 URL 为 `https://us-east-1.console.aws.amazon.com/appfabric/oauth2`。

应用程序授权

租户编号

AppFabric 将请求租户 ID。中的租户 ID AppFabric 是您的实例名称。您可以在浏览器的地址栏中找到租户 ID。例如，*example* 是以下 URL `https://example.service-now.com` 中的租户 ID。

租户名称

输入标识此唯一ServiceNow组织的名称。 AppFabric 使用租户的名称来标记应用程序授权和通过应用程序授权创建的任何摄取。

客户端 ID

AppFabric 将请求客户端 ID。请按照以下步骤在 ServiceNow 中查找您的客户端 ID。

1. 导航到 ServiceNow 控制台。

2. 选择 “系统” OAuth，然后选择 “应用程序注册表” 选项卡。
3. 选择您的应用程序。
4. 在的 “客户端 ID” 字段中输入 OAuth 来自客户的客户端 ID AppFabric。

客户端密钥

AppFabric 将请求客户机密钥。使用以下步骤在 ServiceNow 中查找您的客户端密钥。

1. 导航到 ServiceNow 控制台。
2. 选择 “系统” OAuth，然后选择 “应用程序注册表” 选项卡。
3. 选择您的应用程序。
4. 在的 “客户机密钥” 字段中输入 OAuth 应用程序中的客户机密钥 AppFabric。

批准授权

在中创建应用程序授权后 AppFabric，您将收到一个ServiceNow用于批准授权的弹出窗口。选择 “允许” 以批准 AppFabric 授权。

配置Singularity Cloud为 AppFabric

该Singularity Cloud平台可保护您的企业在各个阶段免受所有类别的威胁。其获得专利的人工智能将安全性从已知的签名和模式扩展到最复杂的攻击，例如未修补的漏洞和勒索软件。

您可以使用 AWS AppFabric 接收来自的审计日志和用户数据Singularity Cloud，将数据标准化为开放网络安全架构框架 (OCSF) 格式，然后将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

> **Note**
>
> Singularity Cloud只有在您登录Singularity Cloud账户后才能访问文档。因此，我们无法直接链接到本Singularity Cloud文档中的文档。

主题

- AppFabric 支持 Singularity Cloud
- 正在 AppFabric 连接您的Singularity Cloud账户

AppFabric 支持 Singularity Cloud

AppFabric 支持接收来自的用户信息和审核日志Singularity Cloud。

先决条件

AppFabric 要使用将审核日志从支持的目标传输Singularity Cloud到支持的目的地，您的Singularity Cloud账户中必须具有管理员角色。有关 Singularity Cloud API 速率限制的更多信息，请登录您的 Singularity Cloud 账户，浏览文档部分并搜索角色。

速率限制注意事项

Singularity Cloud 对 Singularity Cloud API 施加速率限制。有关 Singularity Cloud API 速率限制的更多信息，请登录您的 Singularity Cloud 账户，浏览文档部分，然后搜索 API 速率限制。

数据延迟注意事项

您可能会看到审核事件延迟最多 30 分钟才能送达目的地。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。不过，这可以在账户级别进行自定义。如需帮助，请联系 支持。

正在 AppFabric 连接您的Singularity Cloud账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric使用进行授权Singularity Cloud。要查找授权所需的信息 Singularity Cloud AppFabric，请按以下步骤操作。

为创建 API 令牌 Singularity Cloud

完成以下步骤以创建与服务用户关联的 API 令牌。API 令牌不会关联到特定的控制台用户或电子邮件地址。

> **Note**
>
> 在服务用户 API 令牌到期之前或之后，创建新用户或复制服务用户以获取新的 API 令牌。

1. 登录您的 Singularity Cloud 账户。
2. 在 “设置” 工具栏中，选择 “用户”，然后选择 “服务用户”。
3. 选择 “操作”，然后选择 “创建新服务用户”。
4. 在 “创建新服务用户” 页中，输入服务用户的姓名、描述和到期日期。
5. 选择下一步。
6. 在 “选择访问范围” 部分中，选择范围。

- 选择账户作为访问级别。
- 选择要获取其审核日志的账户。

7. 选择 Create User。

   API 令牌已生成。将打开一个窗口，显示令牌字符串，并显示一条消息，指示这是您最后一次可以查看令牌。

8. （可选）选择复制 API 令牌并将其存储在安全的位置。
9. 选择关闭。

应用程序授权

租户编号

AppFabric 将请求您的租户 ID。中的租户 ID AppFabric 将是您登录服务的Sentinel One网站地址的子域。例如，如果您使用该`example-company-1.sentinelone.net`地址登录Singularity Cloud账户，则您的租户 ID 为`example-company-1`。

租户名称

输入标识此唯一Singularity Cloud组织的名称。 AppFabric 使用租户名称来标记应用程序授权和通过应用程序授权创建的任何摄取。

服务账户令牌

使用您按照本指南为创建 API 令牌 Singularity Cloud部分中的步骤生成的令牌。如果您放错了令牌或无法找到令牌，则可以通过再次执行相同的步骤来生成一个新的令牌。

> **Note**
>
> 如果在采集审核日志时在 Singularity Cloud 控制台中生成了新 AppFabric 的 API 令牌，则提取将停止。如果发生这种情况，您需要使用新的 API 令牌更新应用程序授权，以恢复审核日志提取。

配置Slack为 AppFabric

Slack 的使命是让人们的工作生活更简单、更愉快、更富有成效。它是客户公司的生产力平台，通过无代码自动化提高每个人的能力，实现无缝搜索和知识共享，使团队在共同推进工作时保持联系和参与，

从而提高绩效。作为 Salesforce 的一部分，Slack 被深度集成到 Salesforce Customer 360 中，从而提高销售、服务和营销团队的工作效率。要了解更多信息并开始免费使用 Slack，请访问 slack .com。

AWS AppFabric 出于安全考虑，您可以使用来审核来自的日志和用户数据Slack，将数据标准化为开放网络安全架构框架 (OCSF) 格式，并将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

AppFabric 支持 Slack

AppFabric 支持接收来自的用户信息和审核日志Slack。

先决条件

AppFabric 要使用将审核日志从支持的目标传输Slack到支持的目的地，您必须满足以下要求：

- 您必须拥有 Slack 的 Enterprise Grid 计划。有关更多信息，请参阅简介 Slack Enterprise Grid（位于 Slack 网站上）。
- 您必须有一个具有组织拥有者角色的用户在您的 Slack 账户中。有关角色的更多信息，请在 Slack 网站上参阅 Slack 帮助中心的Slack 中的角色类型。

速率限制注意事项

Slack 对 Slack API 施加速率限制。有关 Slack API 速率限制的更多信息，请在 Slack 网站上参阅《Slack API 使用指南》中的速率限制。如果 AppFabric 和您的现有 Slack API 应用程序的组合超过限制，则显示在中的审核日志 AppFabric 可能会延迟。

数据延迟注意事项

审计事件发送到目标位置的时间可能会延迟多达 30 分钟。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。不过，这可以在账户级别进行自定义。如需帮助，请联系 支持。

正在 AppFabric 连接您的Slack账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric使用进行授权Slack。要查找授权所需的信息 Slack AppFabric，请使用以下步骤。

创建 OAuth 应用程序

AppFabric 与Slack使用集成 OAuth。有两种方法可以创建 OAuth 应用程序：使用应用程序清单或从头开始。要在中创建 OAuth 应用程序Slack，请使用以下步骤。

Using an app manifest

1. 在您的浏览器中导航到 Slack 应用程序管理界面。
2. 选择创建新的应用程序。
3. 选择来自应用程序清单。
4. 选择要为其授权的工作空间 AppFabric。
5. 于在下方输入应用程序清单框中，选择 JSON，然后将现有 JSON 替换为以下内容。*<region>*替换为相应的 AWS 区域（例如，*us-east-1*）。

```
{
    "display_information": {
        "name": "AppFabric"
    },
    "oauth_config": {
        "redirect_urls": [
            "https://<region>.console.aws.amazon.com/appfabric/oauth2"
        ],
        "scopes": {
            "user": [
                "auditlogs:read",
                "users:read.email",
                "users:read"
            ]
        }
    },
    "settings": {
        "org_deploy_enabled": false,
        "socket_mode_enabled": false,
        "token_rotation_enabled": true
    }
}
```

6. 从基本信息页面复制并保存客户端 ID 和客户端密钥。
7. 对于 `auditLogs:read` 范围，您必须启用应用程序的公开分发。有关更多信息，请参阅 Slack 网站上的启用公开分发。

From scratch

1. 在创建应用程序屏幕中选择从头开始创建。
2. 为您的应用程序命名并选择工作区。
3. 从基本信息页面复制并保存客户端 ID 和客户端密钥。
4. 在 “OAuth 和权限” 页面上，选择 “通过令牌轮换实现高级令牌安全” 选项。
5. 在 “OAuth 和权限” 页面的 “重定向 URLs” 部分添加以下格式的 URL。

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   此 URL AWS 区域 中*<region>*是您在其中配置 AppFabric 应用程序包的代码。例如，美国东部（弗吉尼亚州北部）区域的代码为 us-east-1。对于该区域，重定向 URL 为 https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。
6. 对于 auditLogs:read 范围，您必须启用应用程序的公开分发。有关更多信息，请参阅 Slack 网站上的启用公开分发。

所需范围

> **Note**
>
> 仅当您选择从头开始创建 OAuth 应用程序时，此部分才适用。如果您选择使用“应用程序清单”来创建应用程序授权，请跳过此部分。

您必须在应用程序的 “OAuth 和权限” 页面上添加以下用户令牌Slack OAuth范围：

- auditlogs:read
- users:read.email
- users:read

应用程序授权

租户编号

AppFabric 将请求您的租户 ID。中的租户 ID AppFabric 是您的Slack工作空间 ID。要获取您的租户 ID，请按照 Slack 网站上的 Slack 帮助中心的找到您的 Slack URL 中的说明进行操作。您的 Slack 工

作区 URL 的格式与 `examplecorp.slack.com` 或 `examplecorp.enterprise.slack.com` 类似。您需要的租户 ID 是 `examplecorp`（不带 `.slack.com` 或 `.enterprise.slack.com`）。

租户名称

输入标识您的Slack工作空间 ID 的名称。 AppFabric使用租户名称来标记应用程序授权以及通过应用程序授权创建的任何摄取

客户端 ID

AppFabric 将从您的Slack OAuth应用程序中请求客户端 ID。要查找客户端 ID，请按以下步骤操作：

1. 在您的浏览器中导航到 Slack 应用程序管理界面。
2. 选择与您一起使用的 OAuth 应用程序 AppFabric。
3. 在 “基本信息” 页面的 “客户端 ID” 字段中输入客户端 ID AppFabric。

客户端密钥

AppFabric 将从您的Slack OAuth应用程序中请求客户端密钥。要查找客户端密钥，请按以下步骤操作：

1. 在您的浏览器中导航到 Slack 应用程序管理界面。
2. 选择与之配合使用的 OAuth 应用程序 AppFabric。
3. 在 “基本信息” 页面的 “客户机密钥” 字段中输入客户机密钥 AppFabric。

批准授权

在中创建应用程序授权后 AppFabric，您将收到一个Slack用于批准授权的弹出窗口。要批准 AppFabric 授权，请选择允许。

配置Smartsheet为 AppFabric

Smartsheet 是一个工作管理平台，可帮助您在整个企业中协调工作、人员和技术。Smartsheet 提供了一组强大的企业级功能，使每个人都能管理项目、自动化工作流程并大规模快速构建解决方案，从而在保持安全性和合规性的同时为创新创造环境。

AWS AppFabric 出于安全考虑，您可以使用来审核来自的日志和用户数据Smartsheet，将数据标准化为开放网络安全架构框架 (OCSF) 格式，并将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

AppFabric 支持 Smartsheet

AppFabric 支持接收来自的用户信息和审核日志Smartsheet。

先决条件

AppFabric 要使用将审核日志从支持的目标传输Smartsheet到支持的目的地，您必须满足以下要求：

- 您必须拥有 Smartsheet 商业、企业或高级账户。如需详细了解如何创建或升级 Smartsheet 账户，请参阅 Smartsheet 网站上的Smartsheet定价或Smartsheet预付款。
- 您必须完成 Smartsheet 开发人员注册流程。

速率限制注意事项

Smartsheet 对 Smartsheet API 施加速率限制。如需详细了解 Smartsheet API 速率限制，请参阅 Smartsheet 网站上《Smartsheet API 参考》中的速率限制。

数据延迟注意事项

审计事件发送到目标位置的时间可能会延迟多达 30 分钟。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。不过，这可以在账户级别进行自定义。如需帮助，请联系 支持。

正在 AppFabric 连接您的Smartsheet账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric使用进行授权Smartsheet。要查找授权所需的信息 Smartsheet AppFabric，请按以下步骤操作。

创建 OAuth 应用程序

AppFabric 与Smartsheet使用集成 OAuth。要在中创建 OAuth应用程序Smartsheet，请按以下步骤操作：

1. 导航到您 Smartsheet 账户中的开发人员工具。
2. 从开发人员工具屏幕中选择创建新应用程序。

3. 在创建新应用程序屏幕上填写所有输入字段。
4. 为应用程序 URL 和应用程序联系人/支持人员使用任意唯一值。
5. 使用以下格式的重定向 URL 作为应用程序重定向 URL。

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

此 URL AWS 区域 中*<region>*是您在其中配置 AppFabric 应用程序包的代码。例如，美国东部（弗吉尼亚州北部）区域的代码为 us-east-1。对于该区域，重定向 URL 为 https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。

6. 选择保存。
7. 复制并保存应用程序客户端 ID 和应用程序私匙。

所需范围

Smartsheet不要求您在 OAuth 配置中明确添加作用域。 AppFabric 将在对您的Smartsheet账户的授权请求中请求以下范围：

- READ_EVENTS
- READ_USERS

应用程序授权

租户编号

AppFabric 将请求您的租户 ID。中的租户 ID AppFabric 是您的Smartsheet账户 ID。

租户名称

AppFabric 将请求您的租户 ID。输入任何可以唯一地标识您 Smartsheet 账户的值。

客户端 ID

AppFabric 将要求您提供客户端 ID。中的客户端 ID AppFabric 是您的Smartsheet应用程序客户端 ID。要在 Smartsheet 中查找您的应用程序客户端 ID，请按以下步骤操作：

1. 导航到您 Smartsheet 账户中的开发人员工具。
2. 选择您用来连接的 OAuth 应用程序 AppFabric。
3. 在“应用程序配置文件”屏幕的“客户端 ID”字段中输入应用程序客户端 ID AppFabric。

客户端密钥

AppFabric 将请求您的客户机密钥。中的客户端密钥 AppFabric 是您的Smartsheet应用程序密钥。要在 Smartsheet 中查找应用程序私匙，请使用以下步骤：

1. 导航到您 Smartsheet 账户中的开发人员工具。
2. 选择您用来连接的 OAuth 应用程序 AppFabric。
3. 在 “应用程序配置文件” 屏幕的 “客户密钥” 字段中输入应用程序密钥 AppFabric。

批准授权

在中创建应用程序授权后 AppFabric，您将收到一个Smartsheet用于批准授权的弹出窗口。要批准 AppFabric 授权，请选择允许。

配置Terraform Cloud为 AppFabric

HashiCorp Terraform Cloud是世界上使用最广泛的多云配置产品。该Terraform生态系统拥有 3,000 多个提供商、14,000 个模块和 2.5 亿次下载量。 Terraform Cloud是最快的采用方式Terraform，它为从业人员、团队和全球企业提供了在基础设施上创建和协作以及管理安全、合规和运营限制风险所需的一切。

AWS AppFabric 为了安全起见，您可以使用接收来自的审计日志和用户数据Terraform Cloud，将数据标准化为开放网络安全架构框架 (OCSF) 格式，然后将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

AppFabric 支持 Terraform Cloud

AppFabric 支持接收来自的用户信息和审核日志Terraform Cloud。

先决条件

AppFabric 要使用将审核日志从支持的目标传输Terraform Cloud到支持的目的地，您必须满足以下要求：

- 要访问审核日志，您必须拥有Terraform Cloud增强版套餐并且是组织的所有者。有关Terraform Cloud套餐的更多信息，请参阅HashiCorp Terraform网站上的Terraform定价。
- TBD 审核日志可供通过该Terraform Cloud账户创建的组织使用。

速率限制注意事项

Terraform Cloud 对 Terraform Cloud API 施加速率限制。有关 Terraform Cloud API 速率限制的更多信息，请参阅Terraform Cloud网站Terraform Cloud开发者管理常规设置中的 API 速率限制。如果您的现有 API 应用程序 AppFabric 和您的现有 Terraform Cloud API 应用程序Terraform Cloud的组合超出限制，则显示在中的审核日志 AppFabric 可能会延迟。

数据延迟注意事项

审计事件发送到目标位置的时间可能会延迟多达 30 分钟。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。不过，这可以在账户级别进行自定义。如需帮助，请联系 支持。

正在 AppFabric 连接您的Terraform Cloud账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric使用进行授权Terraform Cloud。要查找授权所需的信息 Terraform Cloud AppFabric，请按以下步骤操作。

创建组织 API 令牌

AppFabric 与Terraform Cloud使用组织 API 令牌集成。有关Terraform Cloud组织 API 令牌的更多信息，请参阅组织 API 令牌。要创建组织，请按照创建组织中的说明进行操作。要在中创建组织 API 令牌Terraform Cloud，请使用以下步骤。

1. 导航到Terraform Cloud登录页面并登录。
2. 在左侧面板上选择组织、设置，然后选择 API 令牌。
3. 在 “组织令牌” 下，选择 “创建组织令牌”，然后选择 “生成令牌”。
4. （可选）输入令牌的到期日期或时间，或创建永不过期的令牌。
5. 复制并保存令牌。稍后你会需要这个 AppFabric。如果您在保存令牌之前关闭页面，则必须撤消旧令牌并创建一个新令牌。

应用程序授权

租户编号

AppFabric 将请求租户 ID。您账户的租户 ID 是您Terraform Cloud账户的当前组织 URL。您可以通过登录您的Terraform Cloud组织并复制当前的组织 URL 来找到此信息。租户 ID 应采用下列格式之一：

```
https://app.terraform.io/app/organization_URL
```

租户名称

输入标识此唯一Terraform Cloud组织的名称。 AppFabric 使用租户名称来标记应用程序授权和通过应用程序授权创建的任何摄取。

服务账户令牌

AppFabric 将请求您的服务帐号令牌。中的服务帐号令牌 AppFabric 是您在中创建的组织 API 令牌创建组织 API 令牌。

配置Webex by Cisco为 AppFabric

Cisco 是为互联网提供动力的技术领域的全球领导者。Cisco 通过重塑您的应用程序、保护您的数据、改造您的基础架构以及为您的团队赋能，实现全球化和包容性的未来，从而激发新的可能性。

关于 Webex by Cisco

Webex 是基于云的协作解决方案的领先提供商，该解决方案包括视频会议、通话、消息、活动、客户体验解决方案（如联络中心）和专用协作设备。Webex 专注于提供包容性协作体验，这推动了创新，利用人工智能和机器学习来消除地理、语言、个性和对技术熟悉程度等障碍。其解决方案依托于通过设计确保安全性和隐私。Webex 可与世界领先的商业和生产力应用程序配合使用——通过单一应用程序和界面交付。有关更多信息，请参阅 webex.com。

AWS AppFabric 出于安全考虑，您可以使用来审核来自的日志和用户数据Webex，将数据标准化为开放网络安全架构框架 (OCSF) 格式，并将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

- AppFabric 支持 Webex
- 正在 AppFabric 连接您的Webex账户

AppFabric 支持 Webex

AppFabric 支持接收来自的用户信息和审核日志Webex。

先决条件

AppFabric 要使用将审核日志从支持的目标传输Webex到支持的目的地，您必须满足以下要求：

- 您必须有灵活协作计划、会议计划、调用计划或更高级的计划。如需详细了解如何创建或升级到适用 Webex 计划类型，请参阅 Webex 网站上Webex所有功能的定价。
- 您的账户必须拥有 Pro Pack 许可证才能访问思科公司提供的安全审计事件 AuditLog APIs。
- 您必须有具有组织管理员 > 完全管理员角色的用户。
- 您的完全管理员的管理员角色配置必须已启用合规官选项。

速率限制注意事项

Webex 对 Webex API 施加速率限制。如需详细了解 Webex API 速率限制，请参阅 Webex 网站上 Webex 开发人员指南中的速率限制。如果您的现有 API 应用程序 AppFabric 和您的现有 Webex API 应用程序的组合超过限制，则显示在中的审核日志 AppFabric 可能会延迟。

数据延迟注意事项

审计事件发送到目标位置的时间可能会延迟多达 30 分钟。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。不过，这可以在账户级别进行自定义。如需帮助，请联系 支持。

正在 AppFabric 连接您的Webex账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric使用进行授权Webex。要查找授权所需的信息 Webex AppFabric，请按以下步骤操作。

创建 OAuth 应用程序

AppFabric 与Webex使用集成 OAuth。要在中创建 OAuth应用程序Webex，请按以下步骤操作：

1. 按照《Webex开发者指南》的 “集成和授权” 页面的 “注册您的集成” 部分中的说明进行操作。
2. 使用以下格式的重定向 URL。

```
https://<region>.console.aws.amazon.com/appfabric/oauth2
```

此 URL AWS 区域 中*<region>*是您在其中配置 AppFabric 应用程序包的代码。例如，美国东部（弗吉尼亚州北部）区域的代码为 us-east-1。对于该区域，重定向 URL 为 https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。

所需范围

您必须将以下范围添加到您的Webex OAuth应用程序中：

- spark-compliance:events_read
- audit:events_read
- spark-admin:people_read

应用程序授权

租户编号

AppFabric 将请求您的租户 ID。中的租户 ID AppFabric 是您的Webex组织 ID。如需了解如何查找您的 Webex 组织 ID，请参阅 Webex 帮助中心网站的在 CiscoWebex Control Hub 中查找您的组织 ID。

租户名称

输入标识此唯一Webex实例的名称。 AppFabric使用租户名称来标记应用程序授权和通过应用程序授权创建的任何摄取。

客户端 ID

AppFabric 将要求您提供Webex客户端 ID。要查找您的 Webex 客户端 ID，请按以下步骤操作：

1. 登录您的Webex帐户，网址为https://developer.webex.com。
2. 在右上角选择你的头像。
3. 选择我的 Webex 应用程序。
4. 选择您使用的 OAuth2 应用程序 AppFabric。
5. 将此页面上的客户端 ID 输入到中的 “客户端 ID” 字段 AppFabric。

客户端密钥

AppFabric 将请求您的Webex客户机密钥。 Webex在您最初创建 OAuth 应用程序时，只会显示一次您的客户机密钥。要在未保存初始客户端密钥的情况下生成新的客户端密钥，请按照以下步骤进行操作：

1. 登录您的Webex帐户，网址为https://developer.webex.com。
2. 在右上角选择你的头像。
3. 选择我的 Webex 应用程序。
4. 选择您使用的 OAuth2 应用程序 AppFabric。
5. 在此页面上，生成新的客户端密钥。
6. 在的 “客户机密钥” 字段中输入新的客户机密钥 AppFabric。

批准授权

在中创建应用程序授权后， AppFabric 您将收到一个Webex用于批准授权的弹出窗口。要批准AppFabric授权，请选择接受。

配置Zendesk为 AppFabric

Zendesk 于 2007 年开启了客户体验革命，它使世界各地的任何企业都能在线提供客户服务。如今，Zendesk 是为所有人提供优质服务的倡导者，支持数十亿次对话，通过电话、聊天、电子邮件、消息、社交渠道、社区、点评网站和帮助中心，将超过 100,000 个品牌与数亿客户联系起来。Zendesk 产品经过精心打造，深受人们喜爱。该公司在丹麦哥本哈根设想，在加利福尼亚成立和发展，如今在全球拥有 6,000 多名员工。

AWS AppFabric 出于安全考虑，您可以使用来审核来自的日志和用户数据Zendesk，将数据标准化为开放网络安全架构框架 (OCSF) 格式，并将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

- AppFabric 支持 Zendesk
- 正在 AppFabric 连接您的Zendesk账户

AppFabric 支持 Zendesk

AppFabric 支持接收来自的用户信息和审核日志Zendesk。

先决条件

AppFabric 要使用将审核日志从支持的目标传输Zendesk到支持的目的地，您必须满足以下要求：

- 你必须拥有 Zendesk Suite Enterprise 或 Enterprise Plus 账户或 Zendesk Support Enterprise 账户。如需详细了解如何创建或升级到 Zendesk Enterprise 账户，请参阅 Zendesk 网站上检查您的计划类型 Zendesk。
- 您的 Zendesk 账户中必须有具有管理员角色的用户。有关角色的详细信息，请参阅 Zendesk 网站上的了解 Zendesk 支持用户角色。

速率限制注意事项

Zendesk 对 Zendesk API 施加速率限制。如需详细了解 Zendesk API 速率限制，请参阅 Zendesk 网站上 Zendesk 开发人员指南中的速率限制。如果 AppFabric 和您的现有 Zendesk API 应用程序的组合超过限制，则显示在中的审核日志 AppFabric 可能会延迟。

数据延迟注意事项

审计事件发送到目标位置的时间可能会延迟多达 30 分钟。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。不过，这可以在账户级别进行自定义。如需帮助，请联系 支持。

正在 AppFabric 连接您的Zendesk账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric使用进行授权Zendesk。要查找授权所需的信息 Zendesk AppFabric，请使用以下步骤。

创建 OAuth 应用程序

AppFabric 与Zendesk使用集成 OAuth。在中Zendesk，必须使用以下设置创建 OAuth 应用程序：

1. 按照 Su Zendesk pport 网站上的 “对应用程序使用 OAuth 身份验证” 一文的 “向 Zendesk 注册应用程序” 部分中的说明进行操作。
2. 使用以下格式的重定向 URL。

   ```
   https://<region>.console.aws.amazon.com/appfabric/oauth2
   ```

   此 URL AWS 区域 中*<region>*是您在其中配置 AppFabric 应用程序包的代码。例如，美国东部（弗吉尼亚州北部）区域的代码为 us-east-1。对于该区域，重定向 URL 为 https://*us-east-1*.console.aws.amazon.com/appfabric/oauth2。

应用程序授权

租户编号

AppFabric 将要求您提供租户 ID。中的租户 ID AppFabric 是您的Zendesk子域。如需详细了解如何查找 Zendesk 子域名，请参阅 Zendesk 支持网站上在哪里可以找到我的 Zendesk 子域名。

租户名称

输入标识此唯一Zendesk组织的名称。 AppFabric 使用租户名称来标记应用程序授权和通过应用程序授权创建的任何摄取。

客户端 ID

AppFabric 将请求客户端 ID。中的客户端 ID AppFabric 是您的 Zendesk API 唯一标识符。要查找您的 Zendesk 唯一标识符，请按照以下步骤进行操作：

1. 在您的 Zendesk 账户中导航到管理中心。
2. 选择应用程序和集成。
3. 选择 APIs，Zendesk APIs。
4. 选择 “OAuth 客户端” 选项卡。
5. 选择您为其创建的 OAuth 应用程序 AppFabric。
6. 在的 “ OAuth 客户 ID” 字段中输入客户的唯一标识符 AppFabric。

客户端密钥

AppFabric 将请求客户机密钥。中的客户端密钥 AppFabric 是您的Zendesk秘密令牌。 Zendesk首次创建Zendesk OAuth应用程序时，仅显示一次您的密钥令牌。要在未保存初始密钥的情况下生成新的密钥令牌，请按照以下步骤进行操作：

1. 在您的 Zendesk 账户中导航到管理中心。
2. 选择应用程序和集成。
3. 选择 APIs，Zendesk APIs。
4. 选择 “OAuth 客户端” 选项卡。
5. 选择您为其创建的 OAuth 应用程序 AppFabric。
6. 选择密钥令牌字段旁边的重新生成按钮。
7. 在的 “客户机密” 字段中输入新的密钥令牌 AppFabric。

批准授权

在中创建应用程序授权后 AppFabric，您将收到一个Zendesk用于批准授权的弹出窗口。要批准 AppFabric 授权，请选择允许。

配置Zoom为 AppFabric

Zoom是一个 all-in-one智能协作平台，可让企业和个人更轻松、更身临其境和更具动态性的连接。Zoom技术以人为本，通过团队聊天、电话、会议、全渠道云联络中心、智能录音、白板等解决方案集于一体，实现有意义的联系，促进现代协作，推动人类创新。

AWS AppFabric 出于安全考虑，您可以使用来审核来自的日志和用户数据Zoom，将数据标准化为开放网络安全架构框架 (OCSF) 格式，并将数据输出到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 流。

主题

AppFabric 支持 Zoom

AppFabric 支持接收来自的用户信息和审核日志Zoom。

先决条件

AppFabric 要使用将审核日志从支持的目标传输Zoom到支持的目的地，您必须满足以下要求：

- 您必须拥有 Zoom 专业版、商务版、教育版或企业版套餐。
- 您的Zoom管理员角色必须具有创建 server-to-server OAuth 应用程序的权限。有关启用 server-to-server OAuth 应用程序的信息，请参阅Zoom网站《Zoom开发人员指南》Server-to-Server OAuth页面的 “启用权限” 部分。
- 您的Zoom管理员角色必须有权查看管理员活动日志和 in/sign 注销审核活动。有关启用查看审核活动的权限的更多信息，请参阅 Zoom 支持网站上的使用角色管理和使用管理员活动日志。

速率限制注意事项

Zoom 对 Zoom API 施加速率限制。有关 Zoom API 速率限制的更多信息，请参阅 Zoom 开发人员指南中的速率限制。如果 AppFabric 和您的现有Zoom应用程序的组合超过限制，则显示在中的审核日志 AppFabric 可能会延迟。

数据延迟注意事项

您可能会看到审核事件延迟大约 24 小时才能送达目标。这是应用程序提供的审核事件延迟或为减少数据丢失而采取的预防措施所致。

正在 AppFabric 连接您的Zoom账户

在 AppFabric 服务中创建应用程序包后，必须 AppFabric 使用进行授权Zoom。要查找授权所需的信息 Zoom AppFabric，请按以下步骤操作。

创建 server-to-server OAuth 应用程序

AppFabric 使用应用程序 server-to-server OAuth 凭据进行集成Zoom。要在中创建 server-to-server OAuth 应用程序Zoom，请按照《Zoom开发者指南》中创建 Server-to-Server OAuth 应用程序中的说明进行操作。 AppFabric 不支持 Zoom webhook，你可以跳过添加 webhook 订阅的部分。

所需范围

Zoom提供两种类型的作用域：粒度作用域（适用于新创建的应用程序）和经典作用域（适用于先前创建的应用程序）。

您必须将以下精细范围添加到您的Zoom server-to-server OAuth 应用程序中：

- `report:read:user_activities:admin`
- `report:read:operation_logs:admin`
- `user:read:email:admin`
- `user:read:user:admin`

如果您使用的是先前创建的应用程序，则需要添加以下经典范围：

- `report:read:admin`
- `user:read:admin`

应用程序授权

租户编号

AppFabric 将要求您提供租户 ID。中的租户 ID AppFabric 是Zoom账户 ID。使用以下步骤查找您的 Zoom 账户 ID：

1. 导航到 Zoom Marketplace。
2. 选择管理。
3. 选择您使用的 server-to-server OAuth 应用程序 AppFabric。
4. 在 “应用程序凭证” 页面的 “租户 ID” 字段中输入账户 ID AppFabric。

租户名称

输入标识此唯一Zoom组织的名称。 AppFabric 使用租户名称来标记应用程序授权和通过应用程序授权创建的任何摄取。

客户端 ID

AppFabric 将要求您提供客户端 ID。要查找您的 Zoom 客户端 ID，请按以下步骤操作：

1. 导航到 Zoom Marketplace。
2. 选择管理。
3. 选择您使用的 server-to-server OAuth 应用程序 AppFabric。
4. 在 “应用程序凭证” 页面的 “客户端 ID” 字段中输入客户端 ID AppFabric。

客户端密钥

AppFabric 将请求您的客户机密钥。要查找 Zoom 客户端密钥，请按以下步骤操作：

1. 导航到 Zoom Marketplace。
2. 选择管理。
3. 选择您使用的 server-to-server OAuth 应用程序 AppFabric。
4. 在 “应用程序凭证” 页面的 “客户端密钥” 字段中输入客户端密钥 AppFabric。

审核日志传输

Zoom 每隔 24 小时访问 API 以提供审核日志。使用 AppFabric查看审核日志时，您看到的数据Zoom是前一天活动的数据。

兼容的安全工具和服务 AppFabric 可确保安全

AWS AppFabric 为了安全起见，支持与以下安全工具和服务集成。选择服务的名称，了解有关如何设置安全性 AppFabric 以连接到该服务的更多信息。

主题

Barracuda XDR

Barracuda Networks 是值得信赖的合作伙伴和云优先安全解决方案的领先提供商，通过创新的解决方案保护电子邮件、网络、数据和应用程序，这些解决方案可以随着企业的发展而增长和调整。Barracuda XDR 是一种开放的扩展检测和响应解决方案，它将复杂的技术与安全运营中心 (SOC) 中的安全分析师团队相结合。Barracuda XDR 平台每天分析来自 40 多个集成数据来源的数十亿个原始事件，再加上映射到 MITRE ATT&CK® 框架的广泛威胁检测规则，它可以更快地检测威胁并缩短响应时间。

AWS AppFabric 审核日志摄取注意事项

以下各节描述了要与一起使用的 AppFabric 输出架构、输出格式和输出目的地Barracuda XDR。

架构和格式

Barracuda XDR支持以下 AppFabric 输出架构和格式：

- OCSF-JSON：使用开放网络安全架构框架 (OCSF) 对数据进行 AppFabric 标准化并以 JSON 格式输出数据。

输出位置

Barracuda XDR 支持从 Amazon Security Lake 接收审计日志。要将数据从发送 AppFabric 到 Barracuda XDR，请按照以下说明进行操作：

1. 将数据发送到亚马逊安全湖：配置 AppFabric 为通过亚马逊数据 Firehose 将数据发送到亚马逊安全湖。有关更多信息，请参阅 Amazon Security Lake。
2. 将数据发送至 Barracuda XDR：配置 Barracuda XDR 以接收来自 Amazon Security Lake 的审计日志。有关更多信息，请参阅设置和使用 Amazon Security Lake。

Dynatrace

Dynatrace® Platform它结合了广泛而深入的可观察性以及持续的运行时应用程序安全性，并提供了 AIOps 基于数据的答案和智能自动化的高级功能。这使创新者能够实现云运营的现代化和自动化，更快、更安全地交付软件，并确保完美的数字体验。

AWS AppFabric 审计日志提取注意事项

以下各节描述了用于的 AppFabric 输出架构、输出格式和输出目的地Dynatrace Platform。

架构和格式

Dynatrace Platform支持以下 AppFabric 输出架构和格式：

- OCSF-JSON：使用开放网络安全架构框架 (OCSF) 对数据进行 AppFabric 标准化并以 JSON 格式输出数据。

输出位置

Dynatrace Platform支持从以下 AppFabric 输出位置接收审核日志。

- Amazon Simple Storage Service（Amazon S3）
  - 要将配置Dynatrace Platform为从包含您的审核日志的 Amazon S3 存储桶接收数据，请按照 Dynatrace 的 S3 日志转发器项目中的说明进行操作。GitHub

Logz.io

Logz.io 通过 Logz.io Open 360 Platform 帮助云原生企业监控和保护其环境——将可观测性和安全性从高成本、低价值的负担转变为高价值、高成本效益的促进因素，从而实现更好的业务成果。

Logz.io Cloud SIEM 通过快速查询、多维检测和深度可自定义的安全内容，直接解决了当今最主要的安全挑战——从数据过载到无处不在的网络技能差距，以帮助监控和调查整个云环境——无论数据量有多大，都不会降低性能。

该 Logz.io 解决方案旨在以更低的复杂性和成本实现高级威胁分析和调查。专门的安全分析师、威胁内容即服务和人工智能支持的功能为客户提供支持，这些功能旨在帮助减少噪声数据并专注于信息，使您的团队能够快速优先处理现实世界中的威胁。

AWS AppFabric 审计日志提取注意事项

以下各节描述了要与一起使用的 AppFabric 输出架构、输出格式和输出目的地Logz.io。

架构和格式

Logz.io支持以下 AppFabric 输出架构和格式：

- Raw - JSON
  - AppFabric 以 JSON 格式输出源应用程序使用的原始架构中的数据。
- OCSF - JSON
  - AppFabric 使用开放网络安全架构框架 (OCSF) 对数据进行标准化并以 JSON 格式输出数据。

输出位置

Logz.io支持以下 AppFabric 输出位置：

- Amazon Data Firehose
  - 要配置您的 Firehose 传输流以使其向其发送数据Logz.io，请按照《亚马逊数据 Firehos e 开发Logz.io者指南》中的 “选择您的目的地” 中的说明进行操作。
- Amazon Simple Storage Service（Amazon S3）
  - 要配置 Logz.io 以从包含审核日志的 Amazon S3 存储桶接收数据，请按照 Logz.io 网站上的配置 Amazon S3 存储桶中的说明进行操作。

Netskope

Netskope，全球网络安全领导者，正在重新定义云、数据和网络安全，帮助组织应用零信任原则来保护数据。该 Netskope 平台快速且易于使用，无论人员、设备和数据身在何处，均可为他们提供经优化的访问和零信任安全。Netskope 帮助客户降低风险、提高性能，并获得对任何云、Web 和私有应用程序活动的无与伦比的可见性。成千上万的客户，包括财富100强中的25家以上的客户，信任Netskope其强大的 NewEdge 网络来应对不断变化的威胁、新的风险、技术转变、组织和网络变革以及新的监管要求。要了解 Netskope 如何帮助客户在其 SASE 旅程中做好一切准备，请访问 netskope .com。

AWS AppFabric 审核日志摄取注意事项

以下各节描述了要与一起使用的 AppFabric 输出架构、输出格式和输出目的地Netskope。

架构和格式

Netskope支持以下 AppFabric 输出架构和格式：

- Raw - JSON
  - AppFabric 以 JSON 格式输出源应用程序使用的原始架构中的数据。
- OCSF - JSON
  - AppFabric 使用开放网络安全架构框架 (OCSF) 对数据进行标准化并以 JSON 格式输出数据。

输出位置

Netskope支持以下 AppFabric 输出位置：

- Amazon Simple Storage Service（Amazon S3）
  - 要配置 Netskope 以从包含您的审核日志的 Amazon S3 存储桶接收数据，请按照 Netskope 网站上 Amazon Web Services S3 数据保护中的说明进行操作。

NetWitness

NetWitness 是扩展检测与响应 (XDR) 软件的领先开发商。他们的全球客户群具有高度的安全意识，依靠 NetWitness XDR 来对抗精明强悍的对手。凭借行业中最完整、集成和成熟的平台来检测、调查和应对数字攻击，NetWitness XDR是现代高效 SOC 的统一基础。

由于架构高度模块化，NetWitness XDR 可以在云端、本地环境、移动和远程工作者及其两者之间检测所发生的威胁。NetWitness XDR 平台提供全面的可见性，结合应用的威胁情报和用户行为分析，以检测威胁、确定活动优先级、调查和自动响应。所有这些都使安全分析人员更好、更快地提高效率，使安全操作远远领先于影响业务的威胁。

AWS AppFabric 审计日志提取注意事项

以下各节描述了要与一起使用的 AppFabric 输出架构、输出格式和输出目的地NetWitness。

架构和格式

NetWitness 支持以下 AppFabric 输出架构和格式：

- Raw - JSON
  - AppFabric 以 JSON 格式输出源应用程序使用的原始架构中的数据。
- OCSF - JSON
  - AppFabric 使用开放网络安全架构框架 (OCSF) 对数据进行标准化并以 JSON 格式输出数据。

输出位置

NetWitness支持以下 AppFabric 输出位置：

- Amazon Simple Storage Service（Amazon S3）
  - 要配置 NetWitness 从包含审核日志的 Amazon S3 存储桶接收数据，请按照 NetWitness 网站 NetWitness 平台集成页面上的 S3 通用连接器事件源日志配置指南中的说明进行操作。

Amazon 快速

Amazon Quick 为数据驱动型组织提供超大规模的统一商业智能 (BI)。借助 Quick，所有用户都可以通过现代交互式仪表板、分页报告、嵌入式分析和自然语言查询，从同一个真实来源满足不同的分析需求。您可以在 Quick 中分析 AWS AppFabric 审核日志数据，方法是选择存储安全日志的亚马逊简单存储服务 (Amazon S3) 存储 AppFabric 桶作为来源。

AppFabric 审核日志摄取注意事项

以下各节描述了与 Quick 配合使用的 AppFabric 输出架构、输出格式和输出目的地。

架构和格式

Quick 支持以下 AppFabric 输出架构和格式：

- Raw - JSON
  - AppFabric 以 JSON 格式输出源应用程序使用的原始架构中的数据。
- OCSF - JSON
  - AppFabric 使用开放网络安全架构框架 (OCSF) 对数据进行标准化并以 JSON 格式输出数据。

输出位置

Quick 支持以下 AppFabric 输出位置：

- Amazon S3

- 您可以使用 Amazon S3 文件创建数据集，直接将数据从 Amazon S 3 提取到 Quick 中。要验证您的目标文件集是否未超过快速数据源配额，请参阅快速用户指南中的数据源配额。
- 如果您的文件集超出了 Amazon S3 数据源的快速配额，则可以使用 Amazon Athena 和表在 AWS Glue Amazon S3 中提取数据。在您的快速数据集中使用 Athena 会产生额外费用。有关 Athena 定价的更多信息，请参阅 Athena 定价页面。

  要使用 Athena，请执行以下操作：

  1. 按照 Athena 用户指南中使用 AWS Glue 连接到 Amazon S3 中的数据来源中的说明进行操作。
  2. 按照快速用户指南中的使用 Athena 数据创建数据集中的说明进行操作。

Rapid7

Rapid7，Inc. 的使命是通过让网络安全变得更简单、更容易获得，从而创造一个更安全的数字世界。Rapid7通过 best-in-class技术、前沿研究和广泛的战略专业知识，使安全专业人员能够管理现代攻击面。 Rapid7的全面安全解决方案可帮助全球 10,000 多家客户将云风险管理和威胁检测结合起来，以减少攻击面并快速精确地消除威胁。

AWS AppFabric 审核日志摄取注意事项

以下各节描述了要与一起使用的 AppFabric 输出架构、输出格式和输出目的地Rapid7。

架构和格式

Rapid7支持以下 AppFabric 输出架构和格式：

- Raw - JSON
  - AppFabric 以 JSON 格式输出源应用程序使用的原始架构中的数据。
- OCSF - JSON
  - AppFabric 使用开放网络安全架构框架 (OCSF) 对数据进行标准化并以 JSON 格式输出数据。

输出位置

Rapid7支持以下 AppFabric 输出位置：

- Amazon Simple Storage Service（Amazon S3）
  - 要配置 Rapid7 以从包含审核日志的 Amazon S3 存储桶接收数据，请按照 Rapid7 博客网站上的 How to Monitor Your Amazon S3 Activity with InsightIDR 博文中的说明进行操作。

Amazon Security Lake

Amazon Security Lake 会自动将来自 AWS 环境、软件即服务 (SaaS) 提供商、本地和云源的安全数据集中到存储在您的专用的数据湖中。 AWS 账户借助 Security Lake，您可以更全面地了解整个组织的安全数据。Security Lake 采用了开放网络安全架构框架（OCSF），这是一种开源安全事件架构。借助 OCSF 的支持，该服务可以标准化 AWS 并合并来自各种企业安全数据源的安全数据。

AppFabric 审核日志摄取注意事项

通过向安全湖添加自定义来源，您可以将 SaaS 审核日志存入您 AWS 账户 的 Amazon 安全湖。以下各节描述了与 Security Lake 配合使用的 AppFabric输出架构、输出格式和输出目的地。

架构和格式

Security Lake 支持以下 AppFabric 输出架构和格式：

- OCSF - JSON
  - AppFabric 使用开放网络安全架构框架 (OCSF) 对数据进行标准化并以 JSON 格式输出数据。

输出位置

Security Lake 支持 AppFabric 将使用 Amazon Data Firehose 传输流作为 AppFabric 提取输出位置作为自定义来源。要配置 AWS Glue 表和 Firehose 交付流，以及在 Security Lake 中设置自定义来源，请使用以下步骤。

创建 AWS Glue 表格

1. 导航到 Amazon Simple Storage Service（Amazon S3），用您选择的名称创建存储桶。
2. 导航到 AWS Glue 控制台。
3. 对于数据目录，转到表部分，然后选择添加表。
4. 为表输入您选择的名称。
5. 请选择您在第 1 步中创建的 Amazon S3 存储桶。
6. 对于数据格式，选择 JSON，然后选择下一步。
7. 在选择或定义架构页面上，选择将架构编辑为 JSON。
8. 输入以下架构，然后完成 AWS Glue 表创建过程。

```
[
    {
```

```
        "Name": "message",
        "Type": "string"
    },
    {
        "Name": "process",
        "Type":
"struct<name:string,pid:int,user:struct<name:string,type:string,domain:string,uid:string,t
    },
    {
        "Name": "status",
        "Type": "string"
    },
    {
        "Name": "time",
        "Type": "bigint"
    },
    {
        "Name": "device",
        "Type":
"struct<name:string,owner:struct<name:string,type:string,uid:string,type_id:int,risk_level
    },
    {
        "Name": "metadata",
        "Type":
"struct<version:string,product:struct<name:string,version:string,uid:string,data_classific
    },
    {
        "Name": "severity",
        "Type": "string"
    },
    {
        "Name": "duration",
        "Type": "int"
    },
    {
        "Name": "type_name",
        "Type": "string"
    },
    {
        "Name": "activity_id",
        "Type": "int"
    },
    {
        "Name": "type_uid",
```

```
        "Type": "int"
    },
    {
        "Name": "observables",
        "Type": "array<struct<name:string,type:string,type_id:int,value:string>>"
    },
    {
        "Name": "category_name",
        "Type": "string"
    },
    {
        "Name": "class_uid",
        "Type": "int"
    },
    {
        "Name": "category_uid",
        "Type": "int"
    },
    {
        "Name": "class_name",
        "Type": "string"
    },
    {
        "Name": "timezone_offset",
        "Type": "int"
    },
    {
        "Name": "end_time",
        "Type": "bigint"
    },
    {
        "Name": "activity_name",
        "Type": "string"
    },
    {
        "Name": "cloud",
        "Type":
"struct<account:struct<name:string,type:string,uid:string,type_id:int>,project_uid:string,
    },
    {
        "Name": "query_info",
        "Type": "struct<name:string,uid:string,query_string:string>"
    },
    {
```

```
        "Name": "query_result",
        "Type": "string"
    },
    {
        "Name": "query_result_id",
        "Type": "int"
    },
    {
        "Name": "severity_id",
        "Type": "int"
    },
    {
        "Name": "status_code",
        "Type": "string"
    },
    {
        "Name": "status_detail",
        "Type": "string"
    },
    {
        "Name": "status_id",
        "Type": "int"
    },
    {
        "Name": "network_interfaces",
        "Type":
"array<struct<name:string,type:string,hostname:string,mac:string,type_id:int,ip:string>>"
    },
    {
        "Name": "file",
        "Type":
"struct<attributes:int,name:string,type:string,path:string,type_id:int,accessor:struct<nam
    },
    {
        "Name": "actor",
        "Type":
"struct<process:struct<pid:int,file:struct<name:string,size:bigint,type:string,version:str
    },
    {
        "Name": "dst_endpoint",
        "Type":
"struct<owner:struct<name:string,type:string,uid:string,type_id:int,full_name:string,risk_
    },
    {
```

```
        "Name": "src_endpoint",
        "Type":
"struct<name:string,owner:struct<name:string,type:string,domain:string,uid:string,org:stru
    },
    {
        "Name": "user",
        "Type":
"struct<name:string,type:string,groups:array<struct<name:string,uid:string>>,type_id:int>"
    },
    {
        "Name": "resource",
        "Type":
"struct<version:string,uid:string,agent_list:array<struct<name:string,type:string,uid:stri
    },
    {
        "Name": "privileges",
        "Type": "array<string>"
    },
    {
        "Name": "action",
        "Type": "string"
    },
    {
        "Name": "action_id",
        "Type": "int"
    },
    {
        "Name": "protocol_ver",
        "Type": "string"
    },
    {
        "Name": "proxy",
        "Type":
"struct<name:string,port:int,type:string,ip:string,hostname:string,uid:string,type_id:int,
    },
    {
        "Name": "client_hassh",
        "Type":
"struct<algorithm:string,fingerprint:struct<value:string,algorithm:string,algorithm_id:int
    },
    {
        "Name": "authorizations",
        "Type": "array<string>"
    },
```

```
    {
        "Name": "proxy_tls",
        "Type":
"struct<version:string,certificate:struct<version:string,uid:string,subject:string,issuer:
    },
    {
        "Name": "load_balancer",
        "Type":
"struct<name:string,classification:string,dst_endpoint:struct<owner:struct<type:string,dom
    },
    {
        "Name": "disposition_id",
        "Type": "int"
    },
    {
        "Name": "disposition",
        "Type": "string"
    },
    {
        "Name": "proxy_traffic",
        "Type": "struct<bytes:bigint,packets:int>"
    },
    {
        "Name": "auth_type_id",
        "Type": "int"
    },
    {
        "Name": "proxy_http_response",
        "Type": "struct<code:int,message:string,status:string,length:int>"
    },
    {
        "Name": "server_hassh",
        "Type":
"struct<algorithm:string,fingerprint:struct<value:string,algorithm:string,algorithm_id:int
    },
    {
        "Name": "auth_type",
        "Type": "string"
    },
    {
        "Name": "firewall_rule",
        "Type": "struct<version:string,uid:string>"
    },
    {
```

```
        "Name": "proxy_connection_info",
        "Type":
"struct<direction:string,direction_id:int,protocol_num:int,protocol_ver:string>"
    },
    {
        "Name": "connection_info",
        "Type": "struct<direction:string,direction_id:int>"
    },
    {
        "Name": "api",
        "Type":
"struct<request:struct<data:string,uid:string>,response:struct<error:string,code:int,messa
    },
    {
        "Name": "attacks",
        "Type":
"array<struct<version:string,tactics:array<struct<name:string,uid:string>>,technique:struc
    },
    {
        "Name": "raw_data",
        "Type": "string"
    },
    {
        "Name": "email_uid",
        "Type": "string"
    },
    {
        "Name": "malware",
        "Type":
"array<struct<name:string,path:string,uid:string,classification_ids:array<int>,cves:array<
    },
    {
        "Name": "start_time_dt",
        "Type": "string"
    },
    {
        "Name": "direction",
        "Type": "string"
    },
    {
        "Name": "smtp_hello",
        "Type": "string"
    },
    {
```

```
        "Name": "unmapped",
        "Type": "string"
    },
    {
        "Name": "direction_id",
        "Type": "int"
    },
    {
        "Name": "email_auth",
        "Type":
"struct<spf:string,dkim:string,dkim_domain:string,dkim_signature:string,dmarc:string,dmarc
    },
    {
        "Name": "email",
        "Type":
"struct<uid:string,from:string,to:array<string>,data_classification:struct<category:string
    },
    {
        "Name": "impact_id",
        "Type": "int"
    },
    {
        "Name": "resources",
        "Type":
"array<struct<owner:struct<name:string,type:string,uid:string,type_id:int,full_name:string
    },
    {
        "Name": "finding_info",
        "Type":
"struct<title:string,uid:string,attacks:array<struct<version:string,tactics:array<struct<n
    },
    {
        "Name": "evidences",
        "Type":
"array<struct<process:struct<name:string,pid:int,file:struct<name:string,type:string,versi
    },
    {
        "Name": "impact",
        "Type": "string"
    },
    {
        "Name": "count",
        "Type": "int"
    },
```

```
    {
        "Name": "confidence_id",
        "Type": "int"
    },
    {
        "Name": "enrichments",
        "Type":
"array<struct<data:string,name:string,type:string,value:string,provider:string>>"
    },
    {
        "Name": "rcode",
        "Type": "string"
    },
    {
        "Name": "app_name",
        "Type": "string"
    },
    {
        "Name": "rcode_id",
        "Type": "int"
    },
    {
        "Name": "query",
        "Type":
"struct<type:string,hostname:string,class:string,opcode_id:int,packet_uid:int>"
    },
    {
        "Name": "proxy_endpoint",
        "Type":
"struct<name:string,owner:struct<name:string,type:string,domain:string,uid:string,groups:a
    },
    {
        "Name": "response_time",
        "Type": "bigint"
    },
    {
        "Name": "delay",
        "Type": "int"
    },
    {
        "Name": "start_time",
        "Type": "bigint"
    },
    {
```

```
        "Name": "proxy_http_request",
        "Type":
"struct<version:string,url:struct<port:int,scheme:string,path:string,hostname:string,query
    },
    {
        "Name": "version",
        "Type": "string"
    },
    {
        "Name": "stratum",
        "Type": "string"
    },
    {
        "Name": "stratum_id",
        "Type": "int"
    },
    {
        "Name": "dispersion",
        "Type": "int"
    },
    {
        "Name": "traffic",
        "Type":
"struct<bytes_out:int,chunks:bigint,bytes:int,packets:int,packets_in:bigint>"
    },
    {
        "Name": "precision",
        "Type": "int"
    },
    {
        "Name": "size",
        "Type": "int"
    },
    {
        "Name": "actual_permissions",
        "Type": "int"
    },
    {
        "Name": "base_address",
        "Type": "string"
    },
    {
        "Name": "requested_permissions",
        "Type": "int"
```

```
    },
    {
        "Name": "end_time_dt",
        "Type": "string"
    },
    {
        "Name": "compliance",
        "Type":
"struct<control:string,status:string,standards:array<string>,status_id:int>"
    },
    {
        "Name": "remediation",
        "Type": "struct<desc:string>"
    },
    {
        "Name": "kb_article_list",
        "Type":
"array<struct<os:struct<name:string,type:string,type_id:int,cpe_name:string,edition:string
    },
    {
        "Name": "peripheral_device",
        "Type":
"struct<name:string,class:string,uid:string,model:string,serial_number:string,vendor_name:
    },
    {
        "Name": "time_dt",
        "Type": "string"
    },
    {
        "Name": "group",
        "Type": "struct<name:string,type:string,uid:string>"
    },
    {
        "Name": "users",
        "Type":
"array<struct<name:string,type:string,uid:string,type_id:int,risk_level:string,risk_level_
    },
    {
        "Name": "confidence_score",
        "Type": "int"
    },
    {
        "Name": "state",
        "Type": "string"
```

```
    },
    {
        "Name": "state_id",
        "Type": "int"
    },
    {
        "Name": "evidence",
        "Type": "string"
    },
    {
        "Name": "confidence",
        "Type": "string"
    },
    {
        "Name": "risk_level",
        "Type": "string"
    },
    {
        "Name": "risk_score",
        "Type": "int"
    },
    {
        "Name": "impact_score",
        "Type": "int"
    },
    {
        "Name": "risk_level_id",
        "Type": "int"
    },
    {
        "Name": "finding",
        "Type":
"struct<title:string,uid:string,modified_time:bigint,modified_time_dt:string,first_seen_ti
    },
    {
        "Name": "user_result",
        "Type":
"struct<name:string,type:string,uid:string,type_id:int,account:struct<name:string,uid:stri
    },
    {
        "Name": "codes",
        "Type": "array<int>"
    },
    {
```

```
        "Name": "command",
        "Type": "string"
    },
    {
        "Name": "type",
        "Type": "string"
    },
    {
        "Name": "kernel",
        "Type": "struct<name:string,type:string,type_id:int>"
    },
    {
        "Name": "http_response",
        "Type":
"struct<code:int,status:string,http_headers:array<struct<name:string,value:string>>>"
    },
    {
        "Name": "http_request",
        "Type":
"struct<url:struct<scheme:string,path:string,hostname:string,query_string:string,category_
    },
    {
        "Name": "tls",
        "Type":
"struct<version:string,certificate:struct<subject:string,issuer:string,fingerprints:array<
    },
    {
        "Name": "web_resources",
        "Type":
"array<struct<name:string,type:string,data_classification:struct<category:string,category_
    },
    {
        "Name": "http_cookies",
        "Type":
"array<struct<name:string,value:string,is_http_only:boolean,is_secure:boolean,samesite:str
    },
    {
        "Name": "type_id",
        "Type": "int"
    },
    {
        "Name": "databucket",
        "Type":
"struct<name:string,type:string,file:struct<attributes:int,name:string,owner:struct<name:s
```

```
    },
    {
        "Name": "table",
        "Type": "struct<uid:string,created_time_dt:string>"
    },
    {
        "Name": "session",
        "Type":
"struct<count:int,uid:string,uuid:string,issuer:string,created_time:bigint,is_remote:boole
    },
    {
        "Name": "certificate",
        "Type":
"struct<version:string,uid:string,subject:string,issuer:string,fingerprints:array<struct<v
    },
    {
        "Name": "is_mfa",
        "Type": "boolean"
    },
    {
        "Name": "logon_type_id",
        "Type": "int"
    },
    {
        "Name": "auth_protocol_id",
        "Type": "int"
    },
    {
        "Name": "logon_type",
        "Type": "string"
    },
    {
        "Name": "is_remote",
        "Type": "boolean"
    },
    {
        "Name": "is_cleartext",
        "Type": "boolean"
    },
    {
        "Name": "auth_protocol",
        "Type": "string"
    },
    {
```

```
        "Name": "is_renewal",
        "Type": "boolean"
    },
    {
        "Name": "lease_dur",
        "Type": "int"
    },
    {
        "Name": "relay",
        "Type":
"struct<name:string,type:string,ip:string,mac:string,namespace:string,type_id:int>"
    },
    {
        "Name": "transaction_uid",
        "Type": "string"
    },
    {
        "Name": "file_result",
        "Type":
"struct<name:string,size:int,type:string,path:string,desc:string,product:struct<name:strin
    },
    {
        "Name": "file_diff",
        "Type": "string"
    },
    {
        "Name": "create_mask",
        "Type": "string"
    },
    {
        "Name": "web_resources_result",
        "Type":
"array<struct<type:string,data_classification:struct<category:string,category_id:int,confi
    },
    {
        "Name": "app",
        "Type":
"struct<name:string,version:string,uid:string,data_classification:struct<category:string,c
    },
    {
        "Name": "src_url",
        "Type": "string"
    },
    {
```

```
        "Name": "priority_id",
        "Type": "int"
    },
    {
        "Name": "verdict",
        "Type": "string"
    },
    {
        "Name": "desc",
        "Type": "string"
    },
    {
        "Name": "verdict_id",
        "Type": "int"
    },
    {
        "Name": "priority",
        "Type": "string"
    },
    {
        "Name": "finding_info_list",
        "Type":
"array<struct<title:string,uid:string,attacks:array<struct<version:string,tactics:array<st
    },
    {
        "Name": "expiration_time_dt",
        "Type": "string"
    },
    {
        "Name": "expiration_time",
        "Type": "bigint"
    },
    {
        "Name": "comment",
        "Type": "string"
    },
    {
        "Name": "entity",
        "Type": "struct<data:string,name:string,version:string,uid:string>"
    },
    {
        "Name": "entity_result",
        "Type":
"struct<data:string,name:string,type:string,version:string,uid:string>"
```

```
    },
    {
        "Name": "module",
        "Type":
"struct<type:string,file:struct<name:string,type:string,path:string,desc:string,type_id:in
    },
    {
        "Name": "exit_code",
        "Type": "int"
    },
    {
        "Name": "injection_type",
        "Type": "string"
    },
    {
        "Name": "injection_type_id",
        "Type": "int"
    },
    {
        "Name": "request",
        "Type": "struct<uid:string>"
    },
    {
        "Name": "response",
        "Type": "struct<error:string,code:int,message:string,error_message:string>"
    },
    {
        "Name": "driver",
        "Type":
"struct<file:struct<name:string,type:string,version:string,path:string,type_id:int,parent_
    },
    {
        "Name": "prev_security_states",
        "Type": "array<string>"
    },
    {
        "Name": "security_states",
        "Type": "array<string>"
    },
    {
        "Name": "folder",
        "Type":
"struct<name:string,type:string,path:string,desc:string,type_id:int,mime_type:string,paren
    },
```

```
    {
        "Name": "url",
        "Type":
"struct<port:int,scheme:string,path:string,hostname:string,query_string:string,resource_ty
    },
    {
        "Name": "tunnel_type_id",
        "Type": "int"
    },
    {
        "Name": "tunnel_type",
        "Type": "string"
    },
    {
        "Name": "protocol_name",
        "Type": "string"
    },
    {
        "Name": "job",
        "Type":
"struct<name:string,file:struct<name:string,type:string,path:string,signature:struct<certi
    },
    {
        "Name": "num_trusted_items",
        "Type": "int"
    },
    {
        "Name": "command_uid",
        "Type": "string"
    },
    {
        "Name": "num_registry_items",
        "Type": "int"
    },
    {
        "Name": "num_network_items",
        "Type": "int"
    },
    {
        "Name": "schedule_uid",
        "Type": "string"
    },
    {
        "Name": "num_resolutions",
```

```
        "Type": "int"
    },
    {
        "Name": "scan",
        "Type": "struct<name:string,type:string,type_id:int>"
    },
    {
        "Name": "num_detections",
        "Type": "int"
    },
    {
        "Name": "num_processes",
        "Type": "int"
    },
    {
        "Name": "num_files",
        "Type": "int"
    },
    {
        "Name": "total",
        "Type": "int"
    },
    {
        "Name": "num_folders",
        "Type": "int"
    },
    {
        "Name": "dce_rpc",
        "Type":
"struct<command:string,flags:array<string>,command_response:string,opnum:int,rpc_interface
    },
    {
        "Name": "share",
        "Type": "string"
    },
    {
        "Name": "client_dialects",
        "Type": "array<string>"
    },
    {
        "Name": "open_type",
        "Type": "string"
    },
    {
```

```
        "Name": "tree_uid",
        "Type": "string"
    },
    {
        "Name": "share_type_id",
        "Type": "int"
    },
    {
        "Name": "share_type",
        "Type": "string"
    },
    {
        "Name": "dialect",
        "Type": "string"
    },
    {
        "Name": "cis_benchmark_result",
        "Type": "struct<name:string>"
    },
    {
        "Name": "vulnerabilities",
        "Type":
 "array<struct<references:array<string>,severity:string,affected_packages:array<struct<name
    },
    {
        "Name": "service",
        "Type": "struct<name:string,uid:string>"
    },
    {
        "Name": "data_security",
        "Type":
 "struct<category:string,pattern_match:string,category_id:int,confidentiality:string,confid
    },
    {
        "Name": "database",
        "Type":
 "struct<name:string,type:string,uid:string,type_id:int,data_classification:struct<category
    }
]
```

在 Security Lake 中创建自定义来源

1. 导航到 Amazon Security Lake 控制台。

2. 在导航窗格中选择自定义来源。
3. 选择创建自定义源。
4. 为自定义源输入名称，然后选择适用的 OCSF 事件类别。

> **Note**
>
> AppFabric 使用 “帐户更改”、“身份验证”、“用户访问管理”、“组管理”、“Web 资源活动” 和 “Web 资源访问活动” 事件类。

5. 对于 AWS 账户 ID 和外部 ID，请输入您的 AWS 账户 ID。然后选择 Create。
6. 保存自定义源的 Amazon S3 位置。您将使用它来设置 Amazon Data Firehose 传送流。

在 Firehose 中创建传送流

1. 导航到亚马逊 Data Firehose 控制台。
2. 选择创建传输流。
3. 对于来源，选择直接 PUT。
4. 对于目标，选择 S3。
5. 在转换记录部分，选择启用记录格式转换，然后选择 Apache Parquet 作为输出格式。
6. 对于AWS Glue 表，请选择您在上一个过程中创建的 AWS Glue 表，然后选择最新版本。
7. 对于目标设置，请选择您使用 Security Lake 自定义源创建的 Amazon S3 存储桶。
8. 对于动态分区，请选择启用。
9. 要进行 JSON 的内联解析，请选择启用。
   - 对于 Keyname，输入 `eventDayValue`。
   - 对于 JQ 表达式，输入 `(.time/1000)|strftime("%Y%m%d")`。
10. 对于 S3 存储桶前缀，输入以下值。

```
ext/<custom source name>/region=<region>/accountId=<account_id>/eventDay=!
{partitionKeyFromQuery:eventDayValue}/
```

将*<custom source name><region>*、*<account_id>*替换为您的 Security Lake 自定义来源名称 AWS 区域 和 AWS 账户 ID。

11. 对于 S3 存储桶错误输出前缀，请输入以下值。

```
ext/AppFabric/error/
```

12. 对于重试持续时间，请选择 300。
13. 对于缓冲区大小，请选择 128 MiB。
14. 对于缓冲区间隔，请选择 60 秒。
15. 完成 Firehose 交付流的创建过程。

创建 AppFabric 摄取

要将数据发送到 Amazon Security Lake，您必须在 AppFabric控制台中创建一个提取，使用您之前创建的 Firehose 传输流作为输出位置。有关将 AppFabric 提取配置为使用 Firehose 作为输出位置的更多信息，请参阅创建输出位置。

Singularity Cloud

该Singularity Cloud平台可保护您的企业在各个阶段免受所有类别的威胁。其获得专利的人工智能（人工智能）将安全性从已知的签名和模式扩展到最复杂的攻击，例如未修补的漏洞和勒索软件。

AWS AppFabric 审计日志提取注意事项

以下各节描述了要与一起使用的 AppFabric 输出架构、输出格式和输出目的地Singularity Cloud。

架构和格式

Singularity Cloud支持以下 AppFabric 输出架构和格式：

OCSF-JSON：使用开放网络安全架构框架 (OCSF) 对数据进行 AppFabric 标准化并以 JSON 格式输出数据。

输出位置

Singularity Cloud支持从以下 AppFabric 输出位置接收审核日志。

- Amazon Simple Storage Service（Amazon S3）
  - Singularity Cloud要配置为从包含您的审计日志的 Amazon S3 存储桶接收数据，请按照Singularity Cloud’s文档中的说明进行操作。

Splunk

Splunk 有助于提高组织弹性。领先的组织使用 Splunk 的统一的安全和可观测性平台来确保其数字系统的安全性和可靠性。组织依赖 Splunk 来防止安全、基础设施和应用程序问题变成重大事件，吸收数字颠覆带来的冲击，并加速数字化转型。

AWS AppFabric 审核日志摄取注意事项

以下各节描述了要与一起使用的 AppFabric 输出架构、输出格式和输出目的地Splunk。

架构和格式

Splunk 支持以下 AppFabric 输出架构和格式：

- Raw - JSON
  - AppFabric 以 JSON 格式输出源应用程序使用的原始架构中的数据。
- OCSF - JSON
  - AppFabric 使用开放网络安全架构框架 (OCSF) 对数据进行标准化并以 JSON 格式输出数据。
- OCSF - Parquet
  - AppFabric 使用开放网络安全架构框架 (OCSF) 对数据进行标准化并以该格式输出数据。Apache Parquet

输出位置

Splunk支持以下 AppFabric 输出位置：

- Amazon Data Firehose
  - Splunk要配置为从包含您的审核日志的 Firehose 流中接收审核日志，请按照网站上的亚马逊数据 Firehose Splunk 附加组件中的说明进行操作。Splunk
- Amazon Simple Storage Service（Amazon S3）
  - 要把 Splunk 配置为从包含您的审核日志的 Amazon S3 存储桶接收数据，请按照 Splunk 网站上为 AWS的 Splunk 插件配置基于 SQS 的 S3 输入中的说明进行操作。

AWS AppFabric 为安全资源删除

为了安全起见，如果您不想继续使用 AWS AppFabric ，请务必删除您在设置期间创建的输出位置中的数据以及 AppFabric 用于安全资源的输出位置中的数据，以免产生额外费用。要清理 AppFabric 资

源，必须按照为每个软件即服务 (SaaS) 应用程序创建资源的顺序相反地删除资源：摄取目标 > 接入 > 应用程序授权 > 应用程序捆绑包

删除最终的应用程序授权后，您可以删除应用程序捆绑包。

主题

删除摄取目标

如果您在创建摄取时选择输出位置，则 AppFabric 出于安全考虑，会代表您创建接收目的地。要删除摄取目标，请按照以下步骤进行操作：

1. 打开 AppFabric 控制台，网址为https://console.aws.amazon.com/appfabric/。
2. 在入门页面中，展开左侧的菜单。
3. 选择摄取。
4. 选择应用程序授权。
5. 选择要删除的目标旁边的选项按钮，然后选择删除。
6. 在删除目标对话框中选择删除进行确认。
7. 对所有目标重复上述步骤。

删除摄取

要删除摄取，请遵循以下步骤：

1. 在入门页面中，展开左侧的菜单。
2. 选择摄取。
3. 选择您的应用程序授权旁边的选项按钮。
4. 从操作下拉菜单中选择 。
5. 选择删除。
6. 在删除摄取对话框中选择删除进行确认。

删除应用程序授权

要删除应用程序授权，请按照以下步骤进行操作：

1. 在入门页面中，展开左侧的菜单。
2. 选择应用程序授权。
3. 选择要删除的应用程序授权旁边的选项按钮。
4. 从操作下拉菜单中选择 。
5. 选择删除。
6. 在删除摄取对话框中选择删除进行确认。

删除应用程序捆绑包

要删除您的应用程序捆绑包，请遵循以下步骤：

1. 在入门页面中，展开左侧的菜单。
2. 选择应用程序捆绑包。
3. 选择删除按钮。
4. 键入 `delete` 进行确认，然后选择删除。

什么才是 AWS AppFabric 为了提高工作效率？

“ AWS AppFabric 提高生产力” 功能处于预览阶段，可能会发生变化。

> **Note**
>
> 由 Amazon Bedrock 提供支持： AWS 实现自动滥用检测。由于 AWS AppFabric 工作效率建立在 Amazon Bedrock 之上，因此用户继承了 Amazon Bedrock 中实施的控制措施，以强制执行安全、安保和负责任地使用人工智能。

AWS AppFabric for productive（预览版）通过从多个应用程序中生成基于上下文的见解和操作，帮助重新构想第三方应用程序中最终用户的工作效率。应用程序开发人员认识到，从其他应用程序访问用户数据对于创建更高效的应用程序体验很重要，但他们不想构建和管理与每个应用程序的集成。AppFabric 为了提高工作效率，应用程序开发人员可以访问生成式人工智能，这些生成式人工智能 APIs 可以生成跨应用程序的数据见解和操作，因此他们可以通过新的或现有的生成式人工智能助手提供更丰富的最终用户体验。 AppFabric 为了提高工作效率，可以集成来自多个应用程序的数据，开发人员无需构建或维护 point-to-point集成。 AppFabric 为了提高工作效率，应用程序开发人员可以直接嵌入到其应用程序的用户界面中，为最终用户保持一致的体验，同时显示来自其他应用程序的相关上下文。

AppFabric 为了提高工作效率，可以连接来自常用应用程序（例如AsanaAtlassian Jira Suite、Google Workspace、Microsoft 365、Miro、Slack、Smartsheet、等）的数据。 AppFabric 提高生产力为应用程序开发者提供了一种更轻松的方法来构建更加个性化的应用程序体验，从而提高用户采用率、满意度和忠诚度。同时，最终用户可以在不中断工作流程的情况下，从应用程序中访问所需的见解，从而从中受益。

主题

- 优势
- 使用案例
- 访问 AppFabric 以提高工作效率
- AppFabric 面向应用程序开发人员的生产力入门（预览版）
- 开始使用 AppFabric 提高最终用户的工作效率（预览版）
- AppFabric 提高工作效率 APIs （预览）

- 中的数据处理 AppFabric

优势

AppFabric 为了提高工作效率，应用程序开发人员可以访问生成跨应用程序数据见解和操作的信息，这样他们就可以通过新的或现有的生成式 AI 助手提供更丰富的最终用户体验。 APIs

- 跨应用程序用户数据的单一来源： AppFabric 为了提高工作效率，可以集成来自多个应用程序的数据，开发人员无需构建或维护 point-to-point集成。通过自动将不同的数据类型标准化为任何应用程序都能理解的格式，从而处理 SaaS 应用程序数据以供其他应用程序使用，这样让应用程序开发人员能够整合更多数据，从而真正提高最终用户的工作效率。
- 完全控制用户体验：开发人员将工作效率直接嵌入 AppFabric 到其应用程序的用户界面中，保持对用户体验的完全控制，同时向最终用户提供个性化的见解和操作建议，并提供来自整个应用程序的上下文。这使得 AppFabric 最终用户首选的 SaaS 应用程序可以提高工作效率，也可以在他们想要完成任务的应用程序中进行访问。最终用户花在应用程序之间切换的时间更少，并且可以保持在工作流程中。
- 加快上市时间：在单个 API 调用中，应用开发者无需微调模型、编写自定义提示或跨多个应用程序构建集成，即可获得对用户生成的数据的用户级见解。 AppFabric 将这种复杂性抽象出来，使应用程序开发者能够更快地构建、嵌入或丰富生成式 AI 功能。这使应用程序开发人员能够将资源集中在最重要的任务上。
- A@@ rtifactic 引用以建立用户信任：作为产出的一部分， AppFabric 为了提高工作效率，将显示相关的工件或源文件，这些工件或源文件用于生成见解，从而建立最终用户对LLM输出的信任。
- 简化的用户权限：用于生成见解的用户构件基于用户有权访问的内容。 AppFabric 为了提高工作效率，使用 ISV 的权限和访问控制作为事实来源。

使用案例

应用程序开发人员可以利用提高 AppFabric 工作效率来重新构想其应用程序内部的生产力。 AppFabric for productivity 提供了两个 APIs 侧重于以下用例的内容，以帮助最终用户提高工作效率：

- 优先安排您的一天
  - 可操作的见解 API 通过显示来自其应用程序（包括电子邮件、日历、消息、任务等）的及时见解，帮助用户更好地管理自己的一天。此外，用户还可以通过其首选应用程序执行跨应用程序操作，例如创建电子邮件、安排会议和创建操作项目。例如，在一夜之间进行客户上报的员工不仅可以看到一夜之间对话的摘要，还可以看到安排与客户的客户经理召开会议的建议操作。操作预先填

充了必填字段（如任务名称和所有者，或电子邮件发件人/收件人），可以在执行操作之前编辑预先填充的内容。

- 为即将召开的会议做准备
  - 会议准备 API 通过总结会议目的并显示相关的跨应用程序构件（如电子邮件、消息等），帮助用户为会议做好最充分的准备。用户现在可以快速为会议做准备，不用浪费时间在应用程序之间切换来查找内容。

访问 AppFabric 以提高工作效率

AppFabric for productive 目前已作为预览版推出，并在美国东部（弗吉尼亚北部）推出 AWS 区域。有关的更多信息 AWS 区域，请参阅中的AWS AppFabric 终端节点和配额AWS 一般参考。

在每个区域，您可以通过以下任何一种方式 AppFabric 进行访问以提高工作效率：

- 作为应用程序开发人员
  - AppFabric 面向应用程序开发人员的生产力入门（预览版）
- 作为最终用户
  - 开始使用 AppFabric 提高最终用户的工作效率（预览版）

AppFabric 面向应用程序开发人员的生产力入门（预览版）

“ AWS AppFabric 提高生产力” 功能处于预览阶段，可能会发生变化。

本节帮助应用程序开发者将提高 AWS AppFabric 工作效率（预览）集成到他们的应用程序中。 AWS AppFabric 提高生产力使开发人员能够通过跨多个应用程序的电子邮件、日历事件、任务、消息等生成人工智能驱动的见解和操作，从而为用户打造更丰富的应用程序体验。有关支持的应用程序的列表，请参阅AWS AppFabric 支持的应用程序。

AppFabric 提高工作效率为应用程序开发者提供了在安全可控的环境中进行构建和实验的权限。当你第一次开始使用提高 AppFabric 工作效率时，你需要创建一个 AppClient 并注册一个测试用户。此方法旨在帮助您了解和测试应用程序与之间的身份验证和通信流 AppFabric。在对单个用户进行测试后，您可以先将申请提交给 AppFabric 进行验证，然后再将访问权限扩展到其他用户（请参阅步骤 5。AppFabric 请求验证您的申请）。 AppFabric 将在实现广泛采用之前验证应用程序信息，以帮助保护应用程序开发人员、最终用户及其数据，从而为以负责任的方式扩大用户采用率铺平道路。

主题

先决条件

在开始之前，你需要创建一个 AWS 账户。有关更多信息，请参阅 注册获取 AWS 账户。您还需要创建至少一个有权访问下面列出"appfabric:CreateAppClient"的 IAM 策略的用户，该策略允许该用户注册您的应用程序 AppFabric。有关为生产力功能授予权限 AppFabric 的更多信息，请参阅AppFabric 有关生产力 IAM 策略示例。虽然拥有管理用户是有益的，但对于初始设置来说，这不是强制性的。有关更多信息，请参阅 创建具有管理访问权限的用户。

AppFabric 因为在预览期间，只有美国东部（弗吉尼亚北部）才有生产力。在开始以下步骤之前，请确保您位于此区域。

步骤 1：为提高工作效率 AppFabric 而创建 AppClient

在开始在应用程序中浮出水面 AppFabric 以获取生产力见解之前，您需要创建一个 AppFabric AppClient. 本质上 AppClient 是您提高工作效率 AppFabric 的门户，它充当安全的 OAuth 应用程序客户端，可实现应用程序与之间的安全通信 AppFabric。当你创建时 AppClient，你会得到一个 AppClient ID，这是一个唯一的标识符，对于确保它 AppFabric 知道它正在与你的应用程序和你的应用程序一起使用至关重要 AWS 账户。

AppFabric 提高工作效率为应用程序开发者提供了在安全可控的环境中进行构建和实验的权限。当你第一次开始使用提高 AppFabric 工作效率时，你需要创建一个 AppClient并注册一个测试用户。此方法旨在帮助您了解和测试应用程序与之间的身份验证和通信流 AppFabric。在对单个用户进行测试后，您可以先将申请提交给 AppFabric 进行验证，然后再将访问权限扩展到其他用户（请参阅步骤 5。 AppFabric 请求验证您的申请）。 AppFabric 将在实现广泛采用之前验证应用程序信息，以帮助保护应用程序开发人员、最终用户及其数据，从而为以负责任的方式扩大用户采用率铺平道路。

要创建 AppClient，请使用 AWS AppFabric `CreateAppClient` API 操作。如果您需要更新 AppClient 后面的内容，则可以使用 `UpdateAppClient` API 操作仅更改 redirectURL。如果您需要更改与您的关联的任何其他参数（ AppClient 例如 AppName 或描述），则必须删除 AppClient 并创建一个新参数。有关更多信息，请参阅 CreateAppClient。

你可以使用 `CreateAppClient` API 使用多种编程语言（包括 Python、Node.js、Java、C#、Go 和 Rust）向 AWS 服务注册应用程序。有关更多信息，请参阅《IAM 用户指南》中的请求签名示例。您需要使用账户签名版本 4 凭证才能执行此 API 操作。有关签名版本 4 的更多信息，请参阅 I AM 用户指南中的签署 AWS API 请求。

请求字段

- `appName`-将在用户门户的同意页面上向用户显示的应用程序的 AppFabric 名称。用户意见征求页面要求最终用户允许在您的应用程序中显示 AppFabric 见解。有关同意页面的详细信息，请参阅 步骤 2：同意应用程序显示见解。
- `description` - 应用程序的描述。
- `redirectUrls` - 授权后要将最终用户重定向到的 URI。您最多可以添加 5 个 redirectUrl。例如 `https://localhost:8080`。
- `starterUserEmails` - 在应用程序通过验证之前允许访问以接收见解的用户电子邮件地址。只允许使用一个电子邮件地址。例如，`anyuser@example.com`
- `customerManagedKeyIdentifier`（可选）- 用于加密数据的客户托管密钥（由 KMS 生成）的 ARN。如果未指定，则将使用 AWS AppFabric 托管密钥。有关 AWS 拥有的密钥 和客户托管密钥的更多信息，请参阅 AWS Key Management Service 开发人员指南中的客户端密钥和 AWS 密钥。

响应字段

- `appClientArn`-包含编号的亚马逊资源名称 (ARN)。 AppClient 例如， AppClient ID 是`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`。
- `verificationStatus`- AppClient 验证状态。
  - `pending_verification`-的验证 AppClient仍在进行中 AppFabric。在 AppClient 验证之前，只有一个用户（在中指定`starterUserEmails`）可以使用 AppClient。用户将在 AppFabric 用户门户中看到一条通知（如中所述）步骤 3：将 AppFabric 用户门户 URL 添加到您的应用程序，表示该应用程序未通过验证。
  - `verified`-验证过程已成功完成 AppFabric ，现 AppClient 已完全验证。
  - `rejected`-的验证过程 AppClient 被拒绝 AppFabric。在重新启动并成功完成验证过程之前，其他用户 AppClient 无法使用。

```
curl --request POST \
  --header "Content-Type: application/json" \
  --header "X-Amz-Content-Sha256: <sha256_payload>" \
  --header "X-Amz-Security-Token: <security_token>" \
  --header "X-Amz-Date: 20230922T172215Z" \
  --header "Authorization: AWS4-HMAC-SHA256 ..." \
  --url https://appfabric.<region>.amazonaws.com/appclients/ \
  --data '{
    "appName": "Test App",
    "description": "This is a test app",
    "redirectUrls": ["https://localhost:8080"],
    "starterUserEmails": ["anyuser@example.com"],
    "customerManagedKeyIdentifier": "arn:aws:kms:<region>:<account>:key/<key>"
}'
```

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

```
{
    "appClientConfigSummary": {
        "appClientArn": "arn:aws:appfabric:<region>:<account>:appclient/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "verificationStatus": "pending_verification"
    }
}
```

步骤 2：对您的应用程序进行身份验证和授权

通过建立 OAuth 2.0 授权流程，使您的应用程序能够安全地集成 AppFabric 见解。首先，您需要创建一个授权码，用于验证您的应用程序身份。有关更多信息，请参阅 授权。然后，您将使用此授权码兑换访问令牌，该令牌授予您的应用程序在应用程序中获取和显示 AppFabric见解的权限。有关更多信息，请参阅 令牌。

有关授予应用程序授权权限的更多信息，请参阅 允许访问以授权应用程序。

1. 要创建授权码，请使用 AWS AppFabric `oauth2/authorize` API 操作。

   请求字段

   - `app_client_id`（必填）-步骤 1 中 AWS 账户 创建的 AppClient ID。创建一个 AppClient. 例如 `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`。

- redirect_uri（必填）- 在步骤 1 中使用授权后，最终用户要重定向到的 URI。创建一个 AppClient. 例如 https://localhost:8080。
- state（必填）- 用于维护请求和回调之间状态的唯一值。例如 a8904edc-890c-1005-1996-29a757272a44。

```
GET https://productivity.appfabric.<region>.amazonaws.com/oauth2/authorize?
app_client_id=a1b2c3d4-5678-90ab-cdef-EXAMPLE11111\
redirect_uri=https://localhost:8080&state=a8904edc-890c-1005-1996-29a757272a44
```

2. 身份验证后，您将被重定向到指定的 URI，并以查询参数形式返回授权码。例如，其中 code=mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-oampc。

```
https://localhost:8080/?code=mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-
sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-
oampc&state=a8904edc-890c-1005-1996-29a757272a44
```

3. 使用 AppFabric oauth2/token API 操作将此授权码交换为访问令牌。

   此令牌用于 API 请求，最初在验证starterUserEmails之前一直有效。 AppClient 验证后，该令牌可用于任何用户。 AppClient 您需要使用账户签名版本 4 凭证才能执行此 API 操作。有关签名版本 4 的更多信息，请参阅 I AM 用户指南中的签署 AWS API 请求。

   请求字段

   - code（必填）- 您在最后一步中进行身份验证后收到的授权码。例如 mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-sxTAdRF-gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-oampc。
   - app_client_id（必填）-步骤 1 中 AWS 账户 创建的 AppClient ID。创建一个 AppClient. 例如 a1b2c3d4-5678-90ab-cdef-EXAMPLE11111。
   - grant_type（必填）- 值必须为 authorization_code。
   - redirect_uri（必填）- 在步骤 1 中使用授权后，用户要重定向到的 URI。创建一个 AppClient. 这必须与用于创建授权码的重定向 URI 相同。例如 https://localhost:8080。

   响应字段

   - expires_in - 在令牌过期之前多久。默认过期时间为 12 小时。

- refresh_token - 从初始 /token 请求接收的刷新令牌。
- token - 从初始 /token 请求接收的令牌。
- token_type - 该值将是 Bearer。
- appfabric_user_id- AppFabric 用户 ID。只有使用 authorization_code 授予类型的请求才会返回此值。

```
curl --location \
"https://appfabric.<region>.amazonaws.com/oauth2/token" \
--header "Content-Type: application/json" \
--header "X-Amz-Content-Sha256: <sha256_payload>" \
--header "X-Amz-Security-Token: <security_token>" \
--header "X-Amz-Date: 20230922T172215Z" \
--header "Authorization: AWS4-HMAC-SHA256 ..." \
--data "{
    \"code\": \"mM0NyJ9.MEUCIHQQgV3ChXGs2LRwxLtpsgya3ybfPYXfX-sxTAdRF-
gDAiEAxX7BYKlD9krG3J2VtprOjVXZ0FSUX9whdekqJ-oampc",
    \"app_client_id\": \"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111\",
    \"grant_type\": \"authorization_code\",
    \"redirect_uri\": \"https://localhost:8080\"
}"
```

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

```
{
    "expires_in": 43200,
    "refresh_token": "apkaeibaerjr2example",
    "token": "apkaeibaerjr2example",
    "token_type": "Bearer",
    "appfabric_user_id" : "<userId>"
}
```

步骤 3：将 AppFabric 用户门户 URL 添加到您的应用程序

最终用户需要获得授权 AppFabric ，才能访问其应用程序中用于生成见解的数据。 AppFabric 通过构建专门的用户门户（弹出式屏幕）供最终用户授权其应用程序，消除了应用程序开发者拥有此流程的复杂性。当用户准备好提高工作效率时，他们将被带到用户门户，该门户使他们能够连接和管理用于生成见解和跨应用程序操作的应用程序。 AppFabric 登录后，用户可以将应用程序连接到 AppFabric 以提高工作效率，然后返回到您的应用程序以探索见解和操作。要将应用程序与集成 AppFabric 以提高工

作效率，您需要在应用程序中添加特定 AppFabric 的 URL。此步骤对于使用户能够直接从您的应用程序访问 AppFabric 用户门户至关重要。

1. 导航到应用程序的设置并找到用于添加重定向的部分 URLs。
2. 找到相应区域后，将以下 AppFabric URL 作为重定向 URL 添加到您的应用程序：

```
https://userportal.appfabric.<region>.amazonaws.com/eup_login
```

添加 URL 后，您的应用程序将设置为将用户定向到 AppFabric用户门户。在这里，用户可以登录并连接和管理 AppFabric 用于生成生产力见解的应用程序。

步骤 4： AppFabric 用于显示跨应用程序的见解和操作

用户连接应用程序后，您可以利用用户的见解，通过帮助减少应用程序和上下文切换来提高他们的工作效率。 AppFabric 仅根据用户有权访问的内容为用户生成见解。 AppFabric 将用户数据存储在 AWS 账户 所有者中 AppFabric。有关如何 AppFabric 使用您的数据的信息，请参阅中的数据处理 AppFabric。

您可以使用 APIs 以下 AI 驱动的工具在应用程序中生成和显示用户级见解和操作：

- `ListActionableInsights` — 有关更多信息，请参阅下面的可操作的见解部分。
- `ListMeetingInsights` — 有关更多信息，请参阅本指南后面的会议准备部分。

可操作的见解 (`ListActionableInsights`)

`ListActionableInsights` API 可帮助用户根据其应用程序（包括电子邮件、日历、消息、任务等）中的活动显示可操作的见解，帮助用户更好地管理自己的一天。返回的见解还将显示指向用于生成见解的构件的嵌入式链接，从而帮助用户快速查看生成见解时使用了哪些数据。此外，API 可能会根据见解返回建议的操作，并允许用户从您的应用程序执行跨应用程序操作。具体而言，API 与 Asana、Google Workspace、Microsoft 365 和 Smartsheet 等平台集成，使用户能够发送电子邮件、创建日历事件和创建任务。大型语言模型 (LLMs) 可以在建议的操作（例如电子邮件正文或任务名称）中预先填充详细信息，用户可以在执行前对其进行自定义，从而简化决策并提高工作效率。与最终用户授权应用程序的体验类似， AppFabric 使用相同的专用门户供用户查看、编辑和执行跨应用程序操作。要执行操作， AppFabric 需要 ISVs 将用户重定向到 AppFabric 用户门户，他们可以在其中查看操作详细信息并执行这些操作。生成的每个操作都 AppFabric 有一个唯一的 URL。此 URL 在 `ListActionableInsights` API 响应的响应中可用。

以下是支持的跨应用程序操作以及哪些应用程序的摘要：

- 发送电子邮件（Google Workspace、Microsoft 365）
- 创建日历事件（Google Workspace、Microsoft 365）
- 创建任务（Asana、Smartsheet）

请求字段

- nextToken（可选）- 用于获取下一组见解的分页令牌。
- includeActionExecutionStatus - 接受操作执行状态列表的筛选条件。操作将根据传入的状态值进行筛选。可能的值：NOT_EXECUTED | EXECUTED

请求标头

- 授权标头需要与 Bearer Token 值一起传入。

响应字段

- insightId - 生成的见解的唯一 ID。
- insightContent - 这将返回见解摘要以及用于生成见解的构件的嵌入式链接。注意：这将是一个包含嵌入式链接（<a> 标签）的 HTML 内容。
- insightTitle - 生成的见解的标题。
- createdAt - 生成的见解的时间。
- actions - 为生成的见解建议的操作列表。操作对象:
  - actionId - 生成的操作的唯一 ID。
  - actionIconUrl - 建议在其中执行操作的应用程序的图标 URL。
  - actionTitle - 生成的操作的标题。
  - actionUrl-供最终用户在用户门户中查看和执行操作 AppFabric的唯一 URL。注意：为了执行操作，ISV 应用程序将使用此 URL 将用户重定向到 AppFabric 用户门户（弹出屏幕）。
  - actionExecutionStatus - 指示操作状态的枚举。可能的值包括：EXECUTED | NOT_EXECUTED
- nextToken（可选）- 用于获取下一组见解的分页令牌。这是一个可选字段，如果返回 null，则表示没有更多的见解可供加载。

有关更多信息，请参阅 ActionableInsights。

```
curl -v --location \
  "https://productivity.appfabric.<region>.amazonaws.com"\
"/actionableInsights" \
  --header "Authorization: Bearer <token>"
```

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

```
200 OK

{
    "insights": [
        {
            "insightId": "7tff3412-33b4-479a-8812-30EXAMPLE1111",
            "insightContent": "You received an email from James
            regarding providing feedback
            for upcoming performance reviews.",
            "insightTitle": "New feedback request",
            "createdAt": 2022-10-08T00:46:31.378493Z,
            "actions": [
                {
                    "actionId": "5b4f3412-33b4-479a-8812-3EXAMPLE2222",
                    "actionIconUrl": "https://d3gdwnnn63ow7w.cloudfront.net/
eup/123.svg",
                    "actionTitle": "Send feedback request email",
                    "actionUrl": "https://userportal.appfabric.us-east-1.amazonaws.com/
action/action_id_1"
                    "actionExecutionStatus": "NOT_EXECUTED"
                }
            ]
        },
        {
            "insightId": "2dff3412-33b4-479a-8812-30bEXAMPLE3333",
            "insightContent":"Steve sent you an email asking for details on project.
 Consider replying to the email.",
            "insightTitle": "New team launch discussion",
            "createdAt": 2022-10-08T00:46:31.378493Z,
            "actions": [
                {
                    "actionId": "74251e31-5962-49d2-9ca3-1EXAMPLE1111",
                    "actionIconUrl": "https://d3gdwnnn63ow7w.cloudfront.net/
eup/123.svg",
                    "actionTitle": "Reply to team launch email",
```

```
                    "actionUrl": "https://userportal.appfabric.us-east-1.amazonaws.com/
action/action_id_2"
                    "actionExecutionStatus": "NOT_EXECUTED"
                }
            ]
        }
    ],
    "nextToken": null
}
```

会议准备 (**ListMeetingInsights**)

ListMeetingInsights API 通过总结会议目的并显示相关的跨应用程序构件（如电子邮件、消息等），帮助用户为即将举行的会议做好最充分的准备。用户现在可以快速为会议做准备，不用浪费时间在应用程序之间切换来查找内容。

请求字段

- nextToken（可选）- 用于获取下一组见解的分页令牌。

请求标头

- 授权标头需要与 Bearer Token 值一起传入。

响应字段

- insightId - 生成的见解的唯一 ID。
- insightContent - 见解的描述，以字符串格式突出显示详细信息。例如，为什么这种见解很重要。
- insightTitle - 生成的见解的标题。
- createdAt - 生成的见解的时间。
- calendarEvent - 用户应关注的重要日历事件或会议。日历事件对象：
  - startTime - 事件的开始时间。
  - endTime - 事件的结束时间。
  - eventUrl - ISV 应用程序上日历事件的 URL。
- resources - 包含与生成的见解相关的其他资源的列表。资源对象：
  - appName - 资源所属的应用程序名称。

- resourceTitle - 资源标题。
- resourceType - 资源的类型。可能的值包括：EMAIL | EVENT | MESSAGE | TASK
- resourceUrl - 应用程序中的资源 URL。
- appIconUrl - 资源所属应用程序的图像 URL。

- nextToken（可选）- 用于获取下一组见解的分页令牌。这是一个可选字段，如果返回 null，则表示没有更多的见解可供加载。

有关更多信息，请参阅 MeetingInsights。

```
curl --location \
  "https://productivity.appfabric.<region>.amazonaws.com"\
"/meetingContexts" \
  --header "Authorization: Bearer <token>"
```

如果此操作成功，则该服务将会发送回 HTTP 201 响应。

```
200 OK

{
    "insights": [
        {
            "insightId": "74251e31-5962-49d2-9ca3-15EXAMPLE4444"
            "insightContent": "Project demo meeting coming up soon. Prepare
 accordingly",
            "insightTitle": "Demo meeting next week",
            "createdAt": 2022-10-08T00:46:31.378493Z,
            "calendarEvent": {
                    "startTime": {
                        "timeInUTC": 2023-10-08T10:00:00.000000Z,
                        "timeZone": "UTC"
                     },
                    "endTime": {
                        "timeInUTC": 2023-10-08T11:00:00.000000Z,
                        "timeZone": "UTC"
                     },
                    "eventUrl": "http://someapp.com/events/1234",
            }
            "resources": [
                {
                    "appName": "SOME_EMAIL_APP",
```

```
                    "resourceTitle": "Email for project demo",
                    "resourceType": "EMAIL",
                    "resourceUrl": "http://someapp.com/emails/1234",
                    "appIconUrl":"https://d3gdwnnn63ow7w.cloudfront.net/eup/123.svg"
                }
            ]
        },
        {
            "insightId": "98751e31-5962-49d2-9ca3-15EXAMPLE5555"
            "insightContent": "Important code complete task is now due. Consider
 updating the status.",
            "insightTitle": "Code complete task is due",
            "createdAt": 2022-10-08T00:46:31.378493Z,
            "calendarEvent":{
                    "startTime": {
                        "timeInUTC": 2023-10-08T10:00:00.000000Z,
                        "timeZone": "UTC"
                     },
                    "endTime": {
                        "timeInUTC": 2023-10-08T11:00:00.000000Z,
                        "timeZone": "UTC"
                     },
                    "eventUrl": "http://someapp.com/events/1234",
            },
            "resources": [
                {
                    "appName": "SOME_TASK_APPLICATION",
                    "resourceTitle": "Code Complete task is due",
                    "resourceType": "TASK",
                    "resourceUrl": "http://someapp.com/task/1234",
                    "appIconUrl": "https://d3gdwnnn63ow7w.cloudfront.net/eup/123.svg"
                }
            ]
        }
    ],
    "nextToken": null
}
```


为您的见解或操作提供反馈

使用 AppFabric PutFeedback API 操作为生成的见解和操作提供反馈。您可以将此功能嵌入到您的应用程序中，以提供一种提交给定 InsightId 或的反馈评分（1 到 5，其中评分越高越好）的方法 ActionId。

请求字段

- `id` - 正为其提交反馈的对象的标识符。这可以是 InsightId 或 ActionId。
- `feedbackFor` - 正为其提交反馈的资源类型。可能的值：`ACTIONABLE_INSIGHT | MEETING_INSIGHT | ACTION`
- `feedbackRating` - 反馈评分从 1 到 5。评分越高越好。

响应字段

- 没有响应字段。

有关更多信息，请参阅 PutFeedback。

```
curl --request POST \
  --url "https://productivity.appfabric.<region>.amazonaws.com"\
"/feedback" \
  --header "Authorization: Bearer <token>" \
  --header "Content-Type: application/json" \
  --data '{
    "id": "1234-5678-9012",
    "feedbackFor": "ACTIONABLE_INSIGHT"
    "feedbackRating": 3
}'
```

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 201 响应。

步骤 5。 AppFabric 请求验证您的申请

到目前为止，您已经更新了应用程序界面以嵌入 AppFabric 跨应用程序的见解和操作，并收到了针对单个用户的见解。在您对测试感到满意并希望将 AppFabric丰富的体验扩展到其他用户之后，可以将您的申请提交给以 AppFabric 供审核和验证。 AppFabric 将在实现广泛采用之前验证应用程序信息，以帮助保护应用程序开发人员、最终用户及其数据，从而为以负责任的方式扩大用户采用率铺平道路。

启动验证流程

通过发送电子邮件至 appfabric-appverification@amazon.com 并请求验证您的应用程序，来开始验证流程。

在您的电子邮件中包括以下详细信息：

- 你的 AWS 账户 身份证
- 您正在寻求验证的应用程序的名称
- 你的 AppClient 身份证
- 您的联系信息

此外，请提供以下信息（如果可用），以帮助我们评估优先级和影响：

- 您计划授予访问权限的估计用户数
- 您的目标发布日期

> **Note**
>
> 如果您有 AWS 账户 经理或 AWS 合作伙伴开发经理，请将其复制到您的电子邮件中。包括这些联系人可以帮助加快验证过程。

验证标准

在启动验证过程之前，您必须满足以下标准：

- 为了提高工作效率， AWS 账户 必须使用有效 AppFabric 的

此外，您至少满足下列条件之一：

- 您的组织是至少 AWS Partner Network 具有 “AWS 精选” 级别的 AWS 合作伙伴。有关更多信息，请参阅 AWS 合作伙伴服务等级。
- 在过去三年中，您的组织应该在 AppFabric 服务上花费至少10,000美元。
- 您的应用程序应列在 AWS Marketplace上。有关更多信息，请参阅 AWS Marketplace。

等待验证状态更新

审核您的申请后，我们将通过电子邮件回复，您的申请状态 AppClient 将从变`pending_verification`为`verified`。如果您的申请被拒绝，则需要重新启动验证流程。

通过管理提高 AppFabric 工作效率 AppClients

提高 AWS AppFabric 工作效率功能处于预览阶段，可能会发生变化。

您可以管理您的 AppFabric 生产力 AppClients ，以确保身份验证和授权流程的顺利运行和维护。

获取的详细信息 AppClient

使用 AppFabric `GetAppClient` API 操作查看您的详细信息 AppClient，包括检查 AppClient 状态。有关更多信息，请参阅 GetAppClient。

要获取的详细信息 AppClient，您必须至少拥有 `"appfabric:GetAppClient"` IAM 策略权限。有关更多信息，请参阅 允许访问以获取以下详细信息 AppClients。

请求字段

- `appClientId`- AppClient 身份证。

响应字段

- `appName`-将在用户门户的同意页面上向用户显示的应用程序的 AppFabric 名称。
- `customerManagedKeyIdentifier`（可选）- 用于加密数据的客户托管密钥（由 KMS 生成）的 ARN。如果未指定，则将使用 AWS AppFabric 托管密钥。
- `description` - 应用程序的描述。
- `redirectUrls` - 授权后要将最终用户重定向到的 URI。您最多可以添加 5 个 redirectUrl。例如 `https://localhost:8080`。
- `starterUserEmails` - 在应用程序通过验证之前允许访问以接收见解的用户电子邮件地址。只允许使用一个电子邮件地址。例如 `anyuser@example.com`。
- `verificationStatus`- AppClient 验证状态。
  - `pending_verification`-的验证 AppClient仍在进行中 AppFabric。在 AppClient 验证之前，只有一个用户（在中指定`starterUserEmails`）可以使用 AppClient。
  - `verified`-验证过程已成功完成 AppFabric ，现 AppClient 已完全验证。
  - `rejected`-的验证过程 AppClient 被拒绝 AppFabric。在重新启动并成功完成验证过程之前，其他用户 AppClient 无法使用。

```
curl --request GET \
  --header "Content-Type: application/json" \
  --header "X-Amz-Content-Sha256: <sha256_payload>" \
  --header "X-Amz-Security-Token: <security_token>" \
  --header "X-Amz-Date: 20230922T172215Z" \
  --header "Authorization: AWS4-HMAC-SHA256 ..." \
  --url https://appfabric.<region>.amazonaws.com/appclients/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111
```

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

```
200 OK

{
    "appClient": {
        "appName": "Test App",
        "arn": "arn:aws:appfabric:<region>:111122223333:appclient/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111",
        "customerManagedKeyArn": "arn:aws:kms:<region>:111122223333:key/<key>",
        "description": "This is a test app",
        "redirectUrls": [
            "https://localhost:8080"
        ],
        "starterUserEmails": [
            "anyuser@example.com"
        ],
        "verificationDetails": {
            "verificationStatus": "pending_verification"
        }
    }
}
```

清单 AppClients

使用 AppFabric `ListAppClients` API 操作查看您的列表 AppClients。 AppFabric AppClient 每人只允许一个 AWS 账户。这在未来可能会发生变化。有关更多信息，请参阅 ListAppClients。

要上 AppClients市，您必须至少拥有 `"appfabric:ListAppClients"` IAM 策略权限。有关更多信息，请参阅 允许访问列表 AppClients。

请求字段

- 没有必填字段。

响应字段

- `appClientARN`-包含编号的亚马逊资源名称 (ARN)。 AppClient 例如， AppClient ID 是`a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`。
- `verificationStatus`- AppClient 验证状态。
  - `pending_verification`-的验证 AppClient仍在进行中 AppFabric。在 AppClient 验证之前，只有一个用户（在中指定`starterUserEmails`）可以使用 AppClient。
  - `verified`-验证过程已成功完成 AppFabric ，现 AppClient 已完全验证。
  - `rejected`-的验证过程 AppClient 被拒绝 AppFabric。在重新启动并成功完成验证过程之前，其他用户 AppClient 无法使用。

```
curl --request GET \
  --header "Content-Type: application/json" \
  --header "X-Amz-Content-Sha256: <sha256_payload>" \
  --header "X-Amz-Security-Token: <security_token>" \
  --header "X-Amz-Date: 20230922T172215Z" \
  --header "Authorization: AWS4-HMAC-SHA256 ..." \
  --url https://appfabric.<region>.amazonaws.com/appclients
```

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

```
200 OK

{
    "appClientList": [
        {
            "appClientArn": "arn:aws:appfabric:<region>:111122223333:appclient/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "verificationStatus": "pending_verification"
        }
    ]
}
```

更新一个 AppClient

使用 AppFabric `UpdateAppClient` API 操作更新映射到您的重定向网址。 AppClient如果您需要更改任何其他参数，例如 AppName starterUserEmails、或其他，则必须删除 AppClient 并创建一个新参数。有关更多信息，请参阅 UpdateAppClient。

要更新 AppClient，您必须至少拥有 `"appfabric:UpdateAppClient"` IAM 策略权限。有关更多信息，请参阅 允许访问更新 AppClients。

请求字段

- `appClientId`（必填）-你要更新 redirectURLS 的 AppClient ID。
- `redirectUrls`（必填）- 已更新的 redirectUrl 列表。您最多可以添加 5 个 redirectUrl。

响应字段

- `appName`-将在用户门户的同意页面上向用户显示的应用程序的 AppFabric 名称。
- `customerManagedKeyIdentifier`（可选）- 用于加密数据的客户托管密钥（由 KMS 生成）的 ARN。如果未指定，则将使用 AWS AppFabric 托管密钥。
- `description` - 应用程序的描述。
- `redirectUrls` - 授权后要将最终用户重定向到的 URI。例如 `https://localhost:8080`。
- `starterUserEmails` - 在应用程序通过验证之前允许访问以接收见解的用户电子邮件地址。只允许使用一个电子邮件地址。例如 `anyuser@example.com`。
- `verificationStatus`- AppClient 验证状态。
  - `pending_verification`-的验证 AppClient仍在进行中 AppFabric。在 AppClient 验证之前，只有一个用户（在中指定`starterUserEmails`）可以使用 AppClient。
  - `verified`-验证过程已成功完成 AppFabric ，现 AppClient 已完全验证。
  - `rejected`-的验证过程 AppClient 被拒绝 AppFabric。在重新启动并成功完成验证过程之前，其他用户 AppClient 无法使用。

```
curl --request PATCH \
  --header "Content-Type: application/json" \
  --header "X-Amz-Content-Sha256: <sha256_payload>" \
  --header "X-Amz-Security-Token: <security_token>" \
  --header "X-Amz-Date: 20230922T172215Z" \
  --header "Authorization: AWS4-HMAC-SHA256 ..." \
```

```
  --url https://appfabric.<region>.amazonaws.com/appclients/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111 \
  --data '{
    "redirectUrls": ["https://localhost:8081"]
}'
```

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

```
200 OK

{
    "appClient": {
        "appName": "Test App",
        "arn": "arn:aws:appfabric:<region>:111122223333:appclient/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111",
        "customerManagedKeyArn": "arn:aws:kms:<region>:111122223333:key/<key>",
        "description": "This is a test app",
        "redirectUrls": [
            "https://localhost:8081"
        ],
        "starterUserEmails": [
            "anyuser@example.com"
        ],
        "verificationDetails": {
            "verificationStatus": "pending_verification"
        }
    }
}
```

删除一个 AppClient

使用 AppFabric `DeleteAppClient` API 操作删除任何不再 AppClients 需要的内容。有关更多信息，请参阅 DeleteAppClient。

要删除 AppClient，您必须至少拥有 `"appfabric:DeleteAppClient"` IAM 策略权限。有关更多信息，请参阅 允许访问删除 AppClients。

请求字段

- `appClientId`- AppClient 身份证。

响应字段

- 没有响应字段。

```
curl --request DELETE \
  --header "Content-Type: application/json" \
  --header "X-Amz-Content-Sha256: <sha256_payload>" \
  --header "X-Amz-Security-Token: <security_token>" \
  --header "X-Amz-Date: 20230922T172215Z" \
  --header "Authorization: AWS4-HMAC-SHA256 ..." \
  --url https://appfabric.<region>.amazonaws.com/appclients/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111
```

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 204 响应。

为最终用户刷新令牌

您为最终用户 AppClient 获取的代币可以在到期时刷新。这可以使用 grant_type 为 `refresh_token` 的 令牌 API 来完成。当 grant_type 为 `refresh_token` 时，要使用的 `authorization_code` 将作为令牌 API 响应的一部分返回。默认到期时间为 12 小时。要调用刷新 API，您必须具有 `"appfabric:Token"` IAM 策略权限。有关更多信息，请参阅令牌和允许访问更新 AppClients。

请求字段

- `refresh_token`（必填）- 从初始 `/token` 请求接收的刷新令牌。
- `app_client_id`（必填）-为创建的 AppClient 资源的 ID AWS 账户。
- `grant_type`（必填）- 这必须是 `refresh_token`。

响应字段

- `expires_in` - 在令牌过期之前多久。默认过期时间为 12 小时。
- `refresh_token` - 从初始 /token 请求接收的刷新令牌。
- `token` - 从初始 /token 请求接收的令牌。
- `token_type` - 该值将是 `Bearer`。
- `appfabric_user_id`- AppFabric 用户 ID。只有使用 `authorization_code` 授予类型的请求才会返回此值。

```
curl --location \
```

```
"https://appfabric.<region>.amazonaws.com/oauth2/token" \
--header "Content-Type: application/json" \
--header "X-Amz-Content-Sha256: <sha256_payload>" \
--header "X-Amz-Security-Token: <security_token>" \
--header "X-Amz-Date: 20230922T172215Z" \
--header "Authorization: AWS4-HMAC-SHA256 ..." \
--data "{
    \"refresh_token\": \"<refresh_token>",
    \"app_client_id\": \"a1b2c3d4-5678-90ab-cdef-EXAMPLE11111\",
    \"grant_type\": \"refresh_token\"
}"
```

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

```
200 OK

{
    "expires_in": 43200,
    "token": "apkaeibaerjr2example",
    "token_type": "Bearer",
    "appfabric_user_id" : "${UserID}"
}
```

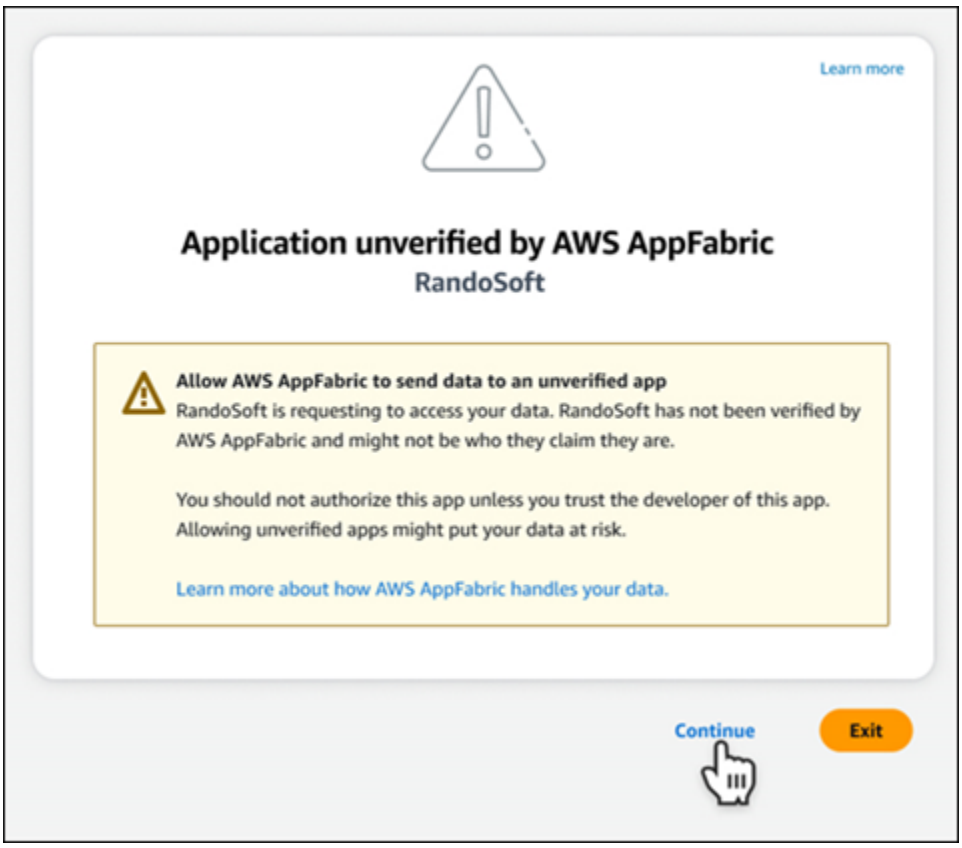
进行故障排除 AppClients AppFabric 以提高工作效率

提高 AWS AppFabric 工作效率功能处于预览阶段，可能会发生变化。

本节介绍常见错误和故障排除， AppFabric 以提高工作效率。

未验证的应用程序

AppFabric 用于提高工作效率来丰富其应用程序体验的应用程序开发者在向最终用户推出其功能之前将经过验证流程。所有应用程序都以未验证状态启动，只有在验证过程完成后才会更改为已验证。这意味着`starterUserEmails`您在创建时使用的 AppClient 将看到此消息。



`CreateAppClient` 错误

ServiceQuotaExceededException

如果您在创建时收到以下异常 AppClient，则说明您已经超过了每个 AppClients 可以创建的数量 AWS 账户。限制为 1。HTTP 状态代码：402

```
ServiceQuotaExceededException / SERVICE_QUOTA_EXCEEDED
You have exceeded the number of AppClients that can be created per AWS Account. The
 limit is 1.
HTTP Status Code: 402
```

`GetAppClient` 错误

ResourceNotFoundException

如果您在获取的详细信息时收到以下异常 AppClient，请确保您输入了正确的 AppClient 标识符。此错误表示未找到指定 AppClient 的。

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
```

```
The specified AppClient is not found. Ensure you've entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

`DeleteAppClient` 错误

ConflictException

如果您在删除时收到以下异常 AppClient，则表示另一个删除请求正在处理中。等待完成，然后重试。HTTP 状态代码：409

```
ConflictException
Another delete request is in progress. Wait until it completes then try again.
HTTP Status Code: 409
```

ResourceNotFoundException

如果您在删除时遇到以下异常 AppClient，请确保输入了正确的标 AppClient 识符。此错误表示未找到指定 AppClient 的。

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
The specified AppClient is not found. Ensure you've entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

`UpdateAppClient` 错误

ResourceNotFoundException

如果您在更新时收到以下异常 AppClient，请确保输入了正确的标 AppClient 识符。此错误表示未找到指定 AppClient 的。

```
ResourceNotFoundException / APP_CLIENT_NOT_FOUND
The specified AppClient is not found. Ensure you've entered the correct AppClient
 identifier.
HTTP Status Code: 404
```

`Authorize` 错误

ValidationException

如果任何 API 参数不满足 API 规范中定义的约束，您可能会收到以下异常。

```
ValidationException
HTTP Status Code: 400
```

原因 1：未指定 AppClient ID 时

请求参数中缺少 `app_client_id`。 AppClient如果尚未创建，请创建，或者使用现有的，`app_client_id`然后重试。要查找 AppClient ID，请使用 ListAppClientAPI 操作。

原因 2：何时 AppFabric 无法访问客户管理的密钥

```
Message: AppFabric couldn't access the customer managed key configured for AppClient.
```

AppFabric 目前无法访问客户托管的密钥，这可能是由于其权限最近发生了变化。验证指定的密钥 AppFabric 是否存在，并确保已授予相应的访问权限。

原因 3：指定的重定向 URL 无效

```
Message: Redirect url invalid
```

确保请求中的重定向 URL 正确。它必须与您在创建或更新时 URLs指定的重定向相匹配 AppClient。要查看允许的重定向列表 URLs，请使用 GetAppClientAPI 操作。

Token 错误

TokenException

您可能会收到以下异常，原因如下。

```
TokenException
HTTP Status Code: 400
```

原因 1：指定了无效的电子邮件时

```
Message: Invalid Email used
```

确保您使用的电子邮件地址与您创建时为该`starterUserEmails`属性列出的电子邮件地址相匹配 AppClient。如果电子邮件不匹配，请更改为匹配的电子邮件地址，然后重试。要查看使用的电子邮件，请使用 GetAppClientAPI 操作。

原因 2：对于 grant_type 为 refresh_token，当未指定令牌时。

```
Message: refresh_token must be non-null for Refresh Token Grant-type
```

请求中指定的刷新令牌为 null 或空。在令牌 API 调用响应中指定接收的有效 `refresh_token`。

ThrottlingException

如果调用 API 的速率超过允许的限额，则可能会收到下列异常。

```
ThrottlingException
HTTP Status Code: 429
```

`ListActionableInsights`、`ListMeetingInsights` 和 `PutFeedback` 错误

ValidationException

如果任何 API 参数不满足 API 规范上定义的约束，则可能会收到以下异常。

```
ValidationException
HTTP Status Code: 400
```

ThrottlingException

如果调用 API 的速率超过允许的限额，则可能会收到下列异常。

```
ThrottlingException
HTTP Status Code: 429
```

开始使用 AppFabric 提高最终用户的工作效率（预览版）

“ AWS AppFabric 提高生产力” 功能处于预览阶段，可能会发生变化。

本部分适用于想要提高工作效率（预览）以 AWS AppFabric 改善任务管理和工作流程效率的 SaaS 应用程序的最终用户。按照以下步骤连接您的应用程序并授权 AppFabric 显示跨应用程序见解，并帮助您通过首选应用程序完成操作（例如发送电子邮件或安排会议）。您可以连接 Asana、Atlassian

Jira Suite、Google Workspace、Microsoft 365、Miro、Slack、Smartsheet 等应用程序。在您授权 AppFabric 访问内容后， AppFabric可以直接在您的首选应用程序中提供跨应用程序的见解和操作，从而帮助您提高工作效率并保持当前的工作流程。

AppFabric 为了提高工作效率，使用由 Amazon Bedrock 提供支持的生成式人工智能。 AppFabric 只有在获得您的明确许可后，才会生成见解和操作。您授权每个应用程序完全控制使用哪些内容。AppFabric 不会使用您的数据来训练或改进用于生成见解的底层大型语言模型。欲了解更多信息，请参阅 Amazon Bedrock FAQs。

主题

先决条件

开始之前，请确保您具备以下内容：

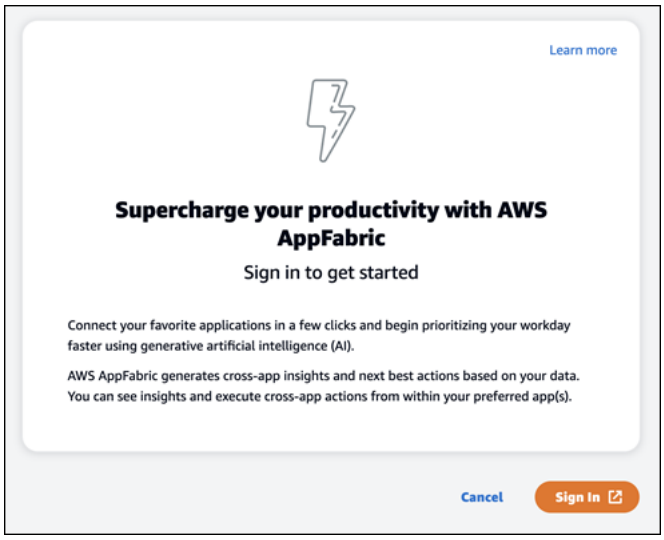
- 登录凭证 AppFabric：要开始使用 AppFabric 以提高工作效率，您需要以下提供商之一的联合登录凭证（用户名和密码）：Asana、Google WorkspaceMicrosoft 365、或Slack。登录以 AppFabric 帮助我们在您为提高工作效率而启用的每个应用程序中将您识别 AppFabric 为用户。登录后，您可以连接您的应用程序以开始生成见解。
- 连接您的应用程序的凭证：仅基于您授权的应用程序生成跨应用程序见解和操作。您要授权的每个应用程序都需要登录凭证（用户名和密码）。支持的应用程序包括 Asana、Atlassian Jira Suite、Google Workspace、Microsoft 365、Miro、Slack 和 Smartsheet。

步骤 1：登录到 AppFabric

将应用程序连接到 AppFabric ，将您的内容和见解直接带到您的首选应用程序中。

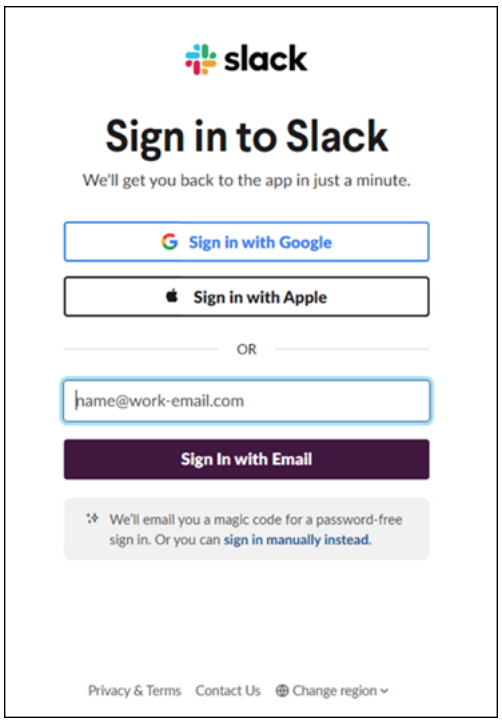
1. 每个应用程序都将以不同的方式 AppFabric 用于提高工作效率，从而为您带来更丰富的应用程序体验。因此，每个应用程序都将有不同的入口点来访问下面的 AppFabric 提高生产力主页。

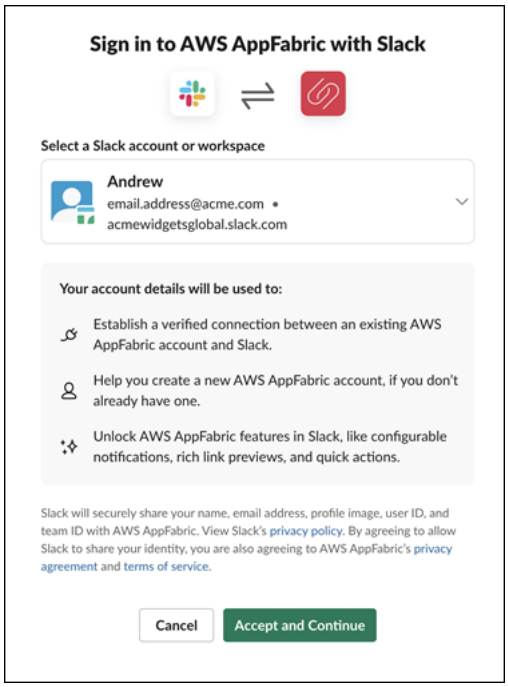
主页会设置要启用的流程的上下文， AppFabric 并首先提示您登录。您要启用的每个应用程序 AppFabric 都将显示此屏幕。



2. 使用以下提供商之一提供的凭证登录：Asana、Google Workspace、Microsoft 365 或 Slack。为了获得最佳体验，我们建议您为启用的每个应用程序使用相同的提供商登 AppFabric 录。例如，如果您在 App1 中选择 Google Workspace 凭证，我们建议您在 App2 中选择 Google Workspace，以及每隔一段时间需要重新登录时进行选择。如果使用其他提供商登录，则您需要重新启动连接应用程序的过程。

3. 如果出现提示，请输入您的登录凭据并接受该提供商 AppFabric 的登录。

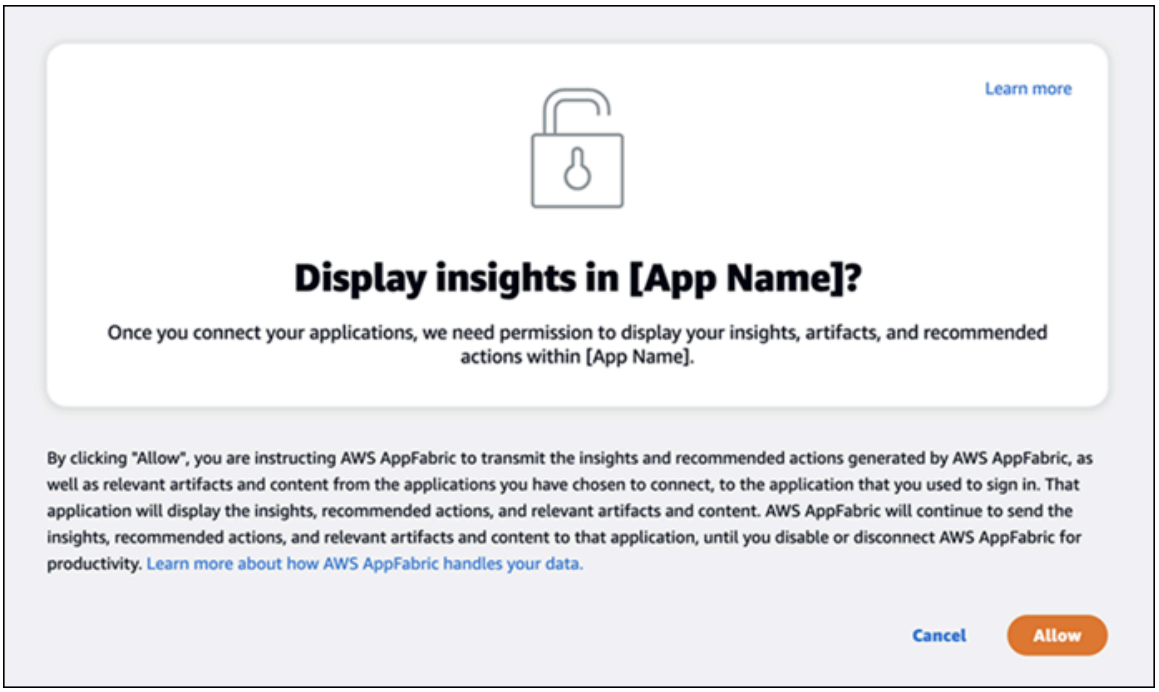




步骤 2：同意应用程序显示见解

登录后， AppFabric 将显示一个同意页面，询问您是否允许在 AppFabric 为提高工作效率而启用的应用程序中显示跨应用程序 AppFabric 的见解和操作。例如，您是否 AppFabric 允许Google Workspace

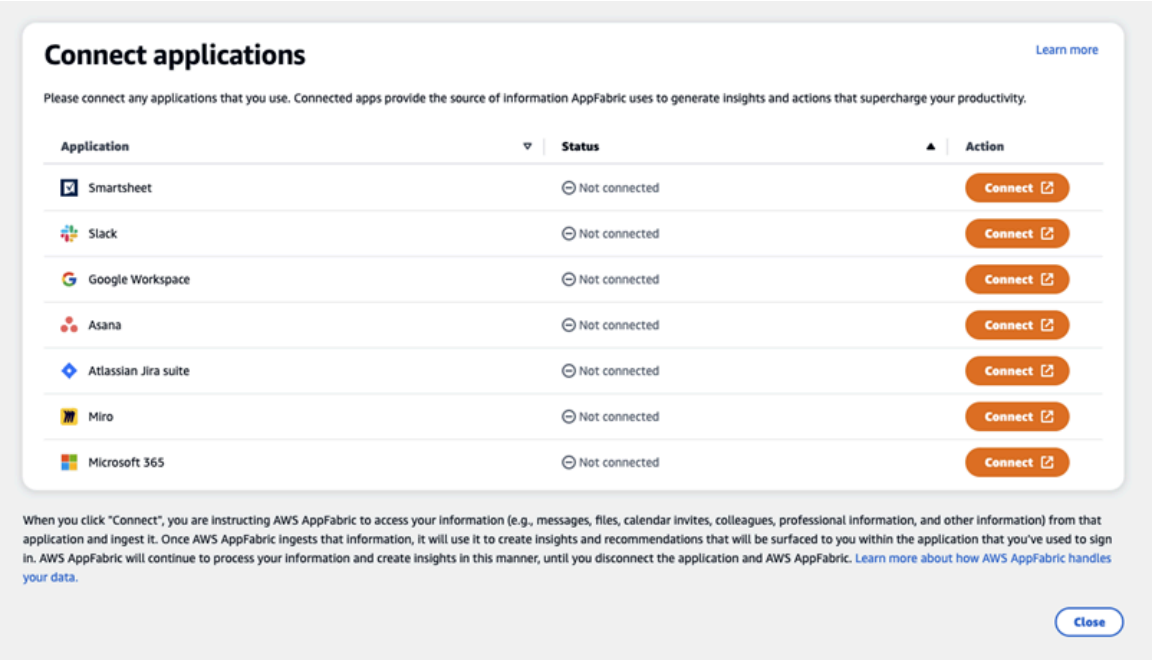
接收您的电子邮件和日历活动并将其显示在中Asana。对于您在中启 AppFabric 用的每个应用程序，您只需完成一次此同意步骤即可。



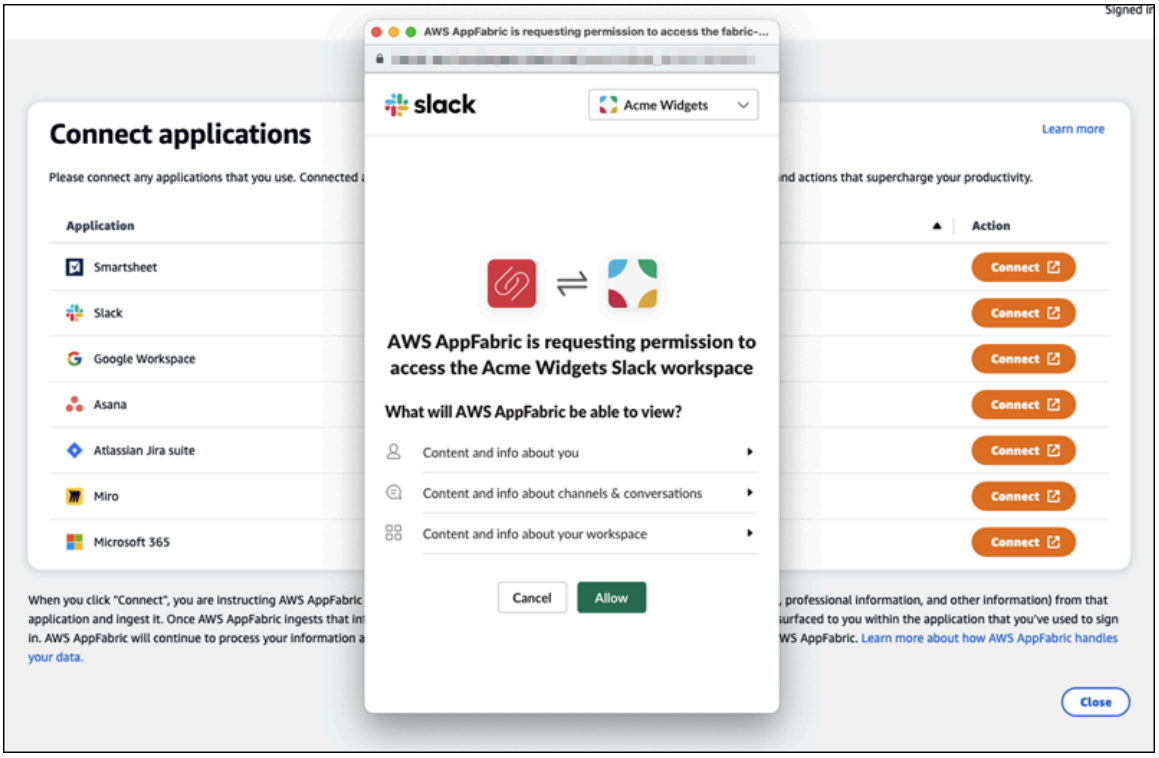
步骤 3：连接您的应用程序以生成见解和操作

完成同意页面后，您将进入连接应用程序页面，您可以在其中连接、断开连接或重新连接各个应用程序，这些应用程序最终用于生成跨应用程序见解和操作。大多数情况下，在您登录并提供同意后，您将继续使用此页面来管理已连接的应用程序。

要连接应用程序，请选择您使用的任意应用程序旁边的连接按钮。



您需要提供应用程序的登录凭证，并 AppFabric允许访问您的数据以生成见解和完成操作。

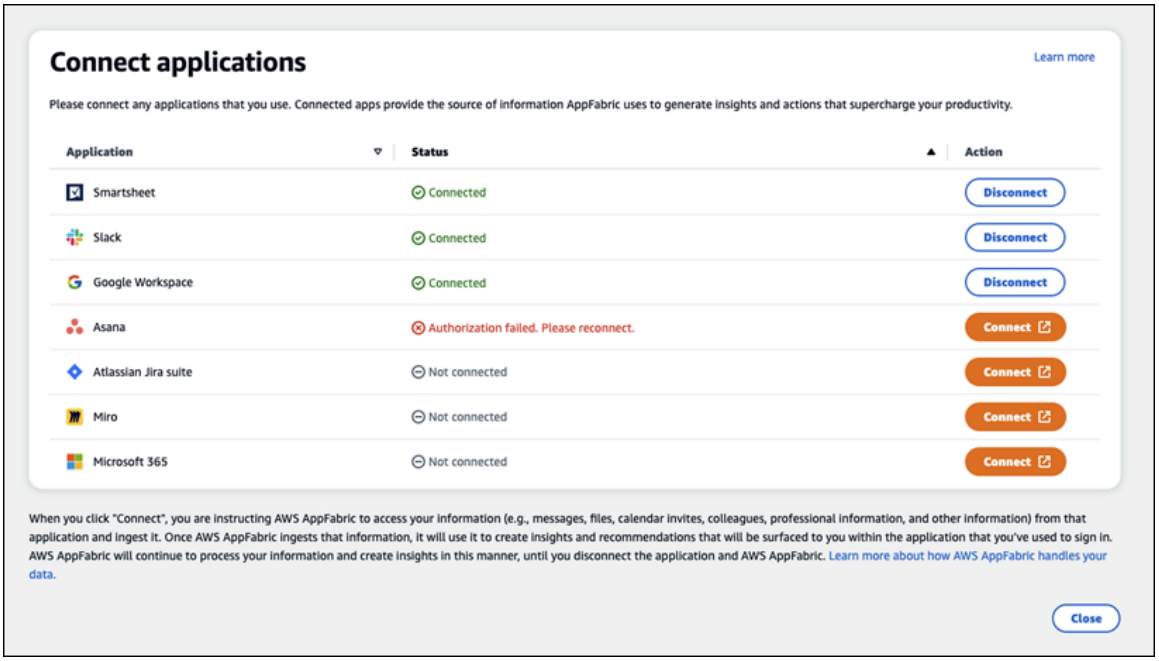


成功连接应用程序后，该应用程序的状态将从“未连接”更改为“已连接”。提醒：您需要为每个要用于生成见解和操作的应用程序完成此授权步骤。

连接应用程序后，它不会永远连接。您需要定期重新连接应用程序。我们这样做是为了确保我们仍然可以获得您的许可来生成见解。

可能的应用程序状态包括：

- Connec AppFabric ted-已获得授权，正在使用您来自此应用程序的数据生成见解。
- 未连接- AppFabric 未使用此应用程序中的数据生成见解。您可以连接以开始生成见解。
- 授权失败。请重新连接。- 特定应用程序可能存在授权失败。如果看到此错误，请尝试使用连接按钮重新连接您的应用程序。



设置已完成，您可以返回到您的应用程序。开始查看应用程序内部的见解可能至少需要几个小时。

根据需要，您可以导航回此页面以管理已连接的应用程序。如果您选择断开应用程序连接， AppFabric 将停止使用该应用程序中的数据或收集新数据来生成新的见解。如果您选择在 7 天内不重新连接应用程序，则断开连接的应用程序中的数据在该时间段后将自动删除。

步骤 4：开始查看见解并在您的应用程序中执行跨应用程序操作

将应用程序与连接后 AppFabric，您将可以访问宝贵的见解，并能够直接从首选应用程序中执行跨应用程序操作。注意：并非每个应用程序都保证此功能，并且完全取决于应用程序开发者选择启用哪种 AppFabric 生产力功能。

跨应用程序见解

AppFabric 提高生产力提供了两种类型的见解：

- 切实可行的见解： AppFabric 分析来自互联应用程序中的电子邮件、日历事件、任务和消息的信息，并生成可能对您重要的关键见解，以确定优先顺序。此外， AppFabric 可能会生成建议的操作（例如发送电子邮件、安排会议和创建任务），您可以在停留在首选应用程序中时编辑和执行这些操作。例如，您可能会收到一条见解，说有客户上报需要处理，并建议您采取下一步行动安排与客户的会议。
- 会议准备见解：此功能可帮助您为即将举行的会议做好最充分的准备。 AppFabric 将分析您即将举行的会议，并生成有关会议目的的简要摘要。此外，它还会显示已连接的应用程序中的相关构件（例如，电子邮件、消息和任务），这将有助于您高效地为会议做准备，而无需在应用程序之间切换来查找内容。

跨应用程序操作

对于某些见解，还 AppFabric 可能生成建议的操作，例如发送电子邮件、安排会议或创建任务。生成操作时， AppFabric 可能会根据所连接应用程序的内容和上下文预先填充某些字段。例如， AppFabric 可能会根据见解生成建议的电子邮件回复或任务名称。当你点击建议的操作时，你将被带到一个 AppFabric 拥有的用户界面，在执行操作之前，你可以在其中编辑预先填充的内容。 AppFabric 由于生成式人工智能和底层的大型语言模型 (LLM) 可能会不时产生幻觉，因此在没有用户审查和输入的情况下不会执行操作。

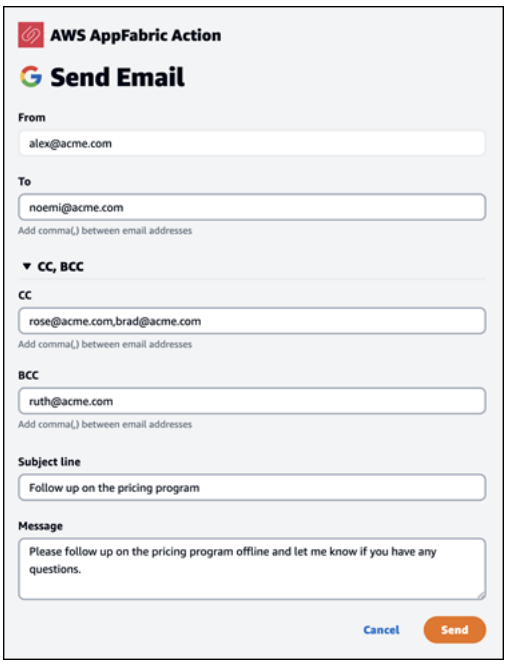
> **Note**
>
> 您有责任验证和确认 AppFabric LLM 的输出。 AppFabric 不保证其 LLM 输出的准确性或质量。有关更多信息，请参阅 AWS 负责任 AI 策略。

创建电子邮件（Google Workspace、Microsoft 365）

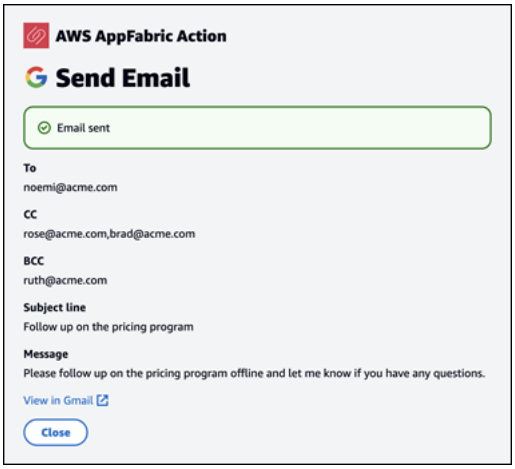
AppFabric 允许您在首选应用程序中编辑和发送电子邮件。我们支持基本的电子邮件字段，包括 “发件人”、“收件人”、“抄送/密送”、“电子邮件主题行” 和 “电子邮件正文”。 AppFabric 可能会在这些字段中生成内容，以帮助您缩短完成任务的时间。编辑完电子邮件后，选择发送以发送电子邮件。

发送电子邮件需要下列字段：

- 至少需要一封收件人电子邮件（收件人、抄送和密件抄送），并且必须是有效的电子邮件地址。
- 主题行和消息字段。



发送电子邮件后，您将看到电子邮件已发送的确认信息。此外，您还会在指定的应用程序中看到用于查看电子邮件的链接。您可以使用此链接快速导航到应用程序，并确认电子邮件已发送。



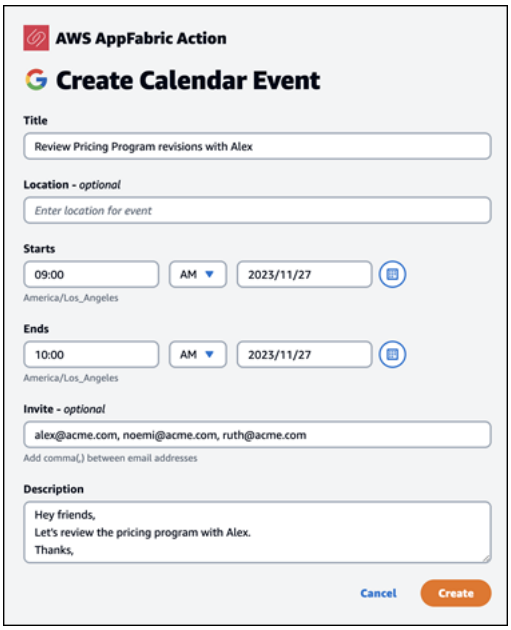
创建日历事件（Google Workspace、Microsoft 365）

AppFabric 允许您在首选应用程序中编辑和创建日历事件。我们支持基本的日历活动字段，包括活动标题、地点、 Start/End 时间和日期、受邀者列表和活动详情。 AppFabric 可能会在这些字段中生成内容，以帮助您缩短完成任务的时间。编辑完日历事件后，选择创建以创建事件。

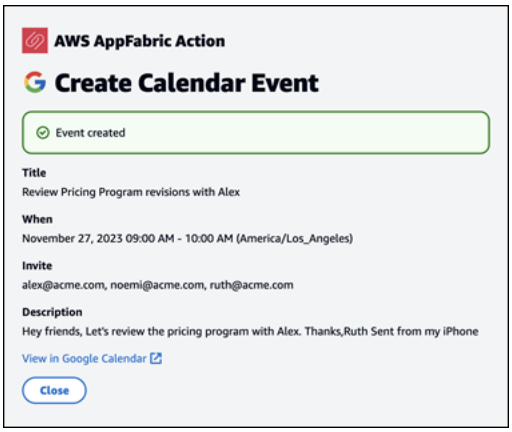
要创建日历事件，必须填写以下字段：

- “标题”、“开始”、“结束”和“描述”字段。

- 开始时间和日期不得早于结束时间和日期。
- “邀请”字段是可选的，但需要有效的电子邮件地址（如果提供）。



发送日历事件后，您将看到事件已创建的确认信息。此外，您还会在指定的应用程序中看到用于查看事件的链接。您可以使用此链接快速导航到应用程序，并验证事件是否已创建。

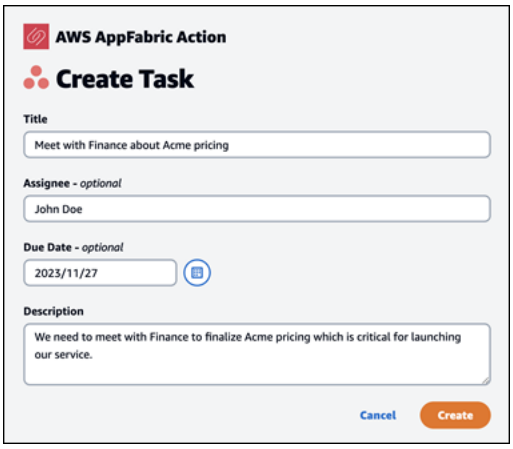


创建任务 (Asana)

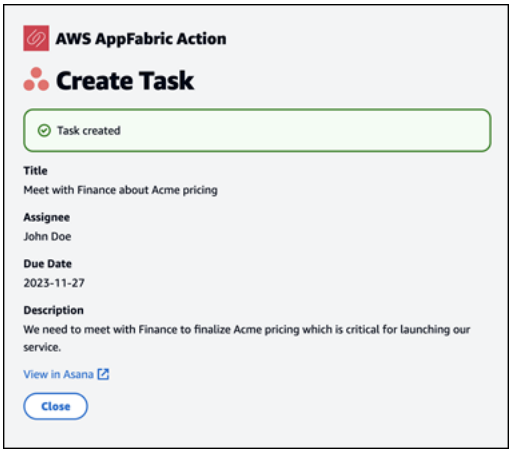
AppFabric 允许您在首选应用程序Asana中编辑和创建任务。我们支持基本任务字段，例如任务名称、任务所有者、截止日期和任务描述。 AppFabric 可能会在这些字段中生成内容，以帮助您缩短创建任务的时间。编辑完任务后，选择创建以创建任务。按照 LLM 的建议，在相应 Asana 的工作区或项目或任务中创建任务。

创建 Asana 任务时必须填写以下字段：

- “标题”和“描述”字段。
- 如果修改，则受让人必须是有效的电子邮件地址。



创建任务后，您将看到一条确认消息，表明已在 Asana 中创建任务。此外，您将在 Asana 中看到一个查看任务的链接。您可以使用此链接快速导航到应用程序以验证任务是否已创建，或者将其移动到相应的 Asana 工作区、项目或任务。



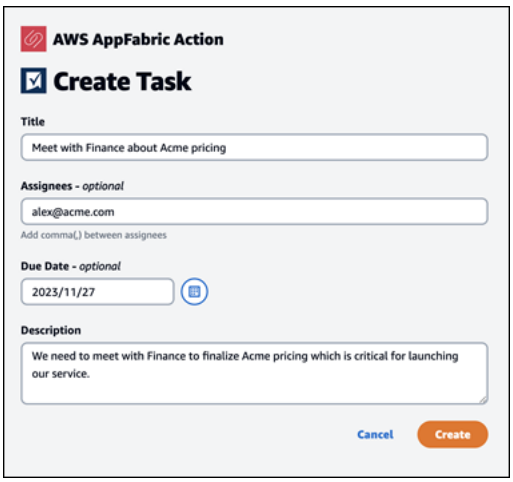
创建任务 (Smartsheet)

AppFabric 允许您在首选应用程序Smartsheet中编辑和创建任务。我们支持基本任务字段，例如任务名称、任务所有者、截止日期和任务描述。 AppFabric 可能会在这些字段中生成内容，以帮助您缩短创建任务的时间。编辑完任务后，选择创建以创建任务。对于Smartsheet任务， AppFabric 将创建一个新的私人Smartsheet工作表并填充所有已创建的任务。这样做是为了帮助以结构化的方式将 AppFabric 生成的操作集中在一个地方。

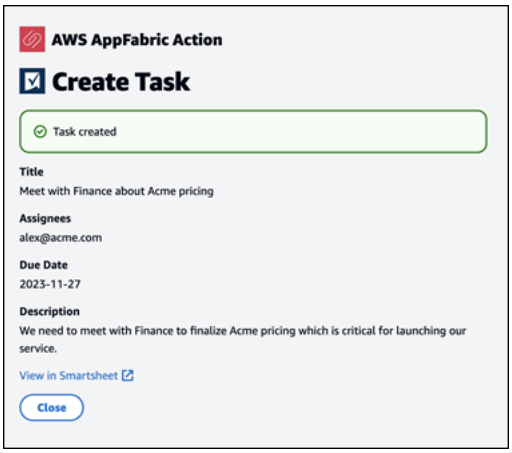
创建 Smartsheet 任务时必须填写以下字段：

- “标题”和“描述”字段。

- 受让人必须是有效的电子邮件地址（如果提供）。



创建任务后，您将看到一条确认消息，表明已在 Smartsheet 中创建任务。此外，您将在 Smartsheet 中看到一个查看任务的链接。您可以使用此链接快速导航到应用程序，以便在创建的 Smartsheet 工作表中查看任务。所有未来的 Smartsheet 任务都将填充在此工作表中。如果工作表被删除， AppFabric 将创建一个新工作表。



管理 IT 和安全管理员 AppFabric 对提高工作效率（预览）功能的访问权限

“ AWS AppFabric 提高生产力” 功能处于预览阶段，可能会发生变化。

所有集成 AppFabric 了提高生产力（预览）功能的 SaaS 应用程序用户均可公开访问生产力用户门户。 AppFabric 如果您是一名 IT 管理员，想要管理组织内对这些生成式人工智能功能的访问权限，请考虑以下选项：

- 限制身份提供者 (IdP) 登录：您可以通过身份提供者阻止登录访问权限，以控制用户对生成式人工智能功能的访问。
- OAuth 对特定应用程序禁用：通过禁用来实现下游限制 OAuth。此操作可防止用户将需要 OAuth 身份验证的应用程序连接到公司的工作区。

对最终用户错误进行故障排除，提高 AppFabric 工作效率

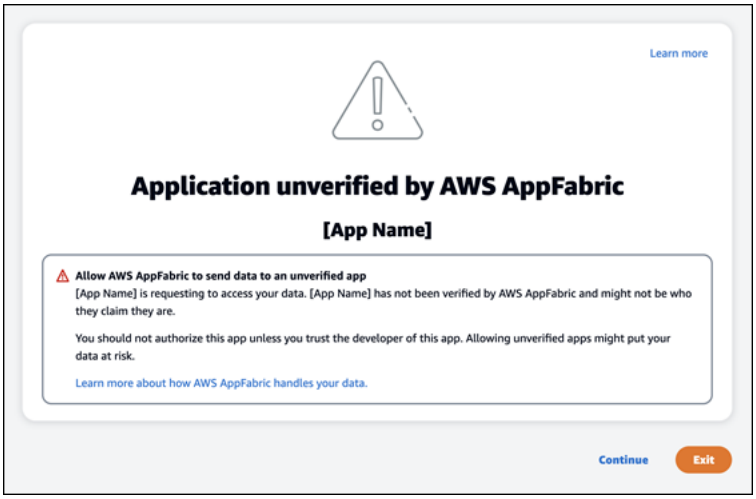
“ AWS AppFabric 提高生产力” 功能处于预览阶段，可能会发生变化。

本节介绍常见错误和故障排除， AppFabric 以提高工作效率。

未验证的应用程序

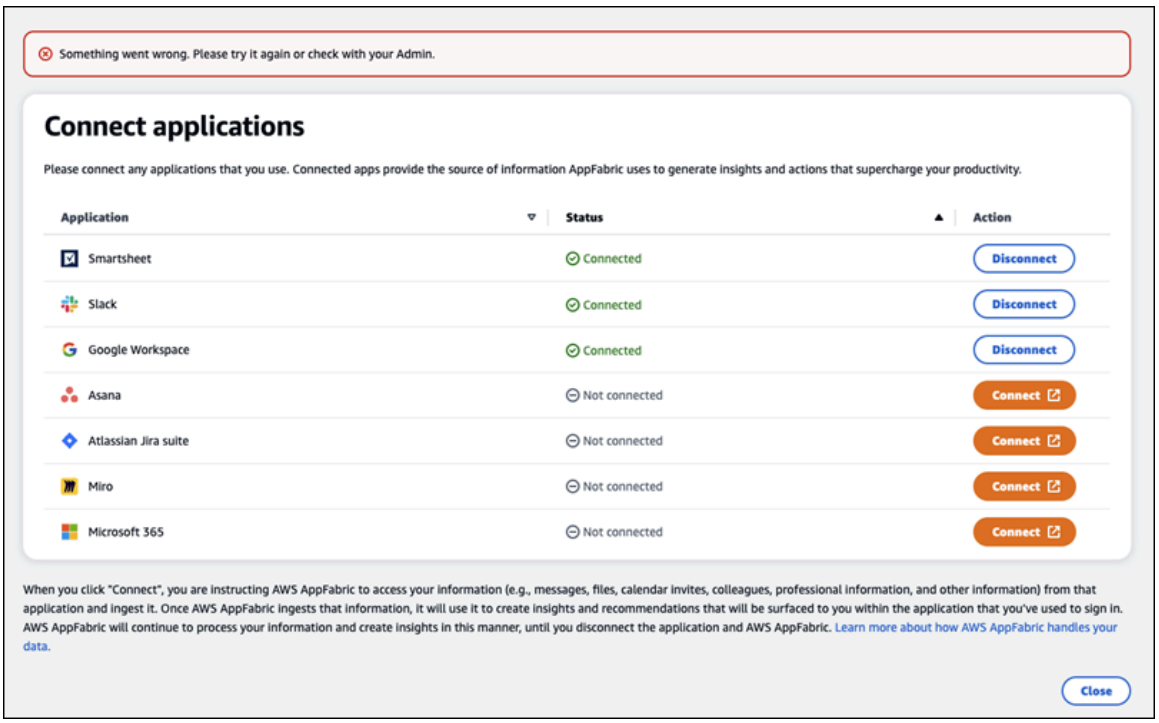
AppFabric 用于提高工作效率以丰富其应用程序体验的应用程序在向最终用户推出其功能之前将经过验证过程。如果您在尝试登录时遇到 “未验证” 横幅 AppFabric，则表示该应用程序尚未经过 AppFabric确认应用程序开发者的身份和应用程序注册信息的准确性的验证过程。所有应用程序都以未验证状态启动，只有在验证过程完成后才会更改为已验证。

使用未经验证的应用程序时要小心。如果不确定应用程序开发人员，则可以等到应用程序获得已验证状态后再继续。



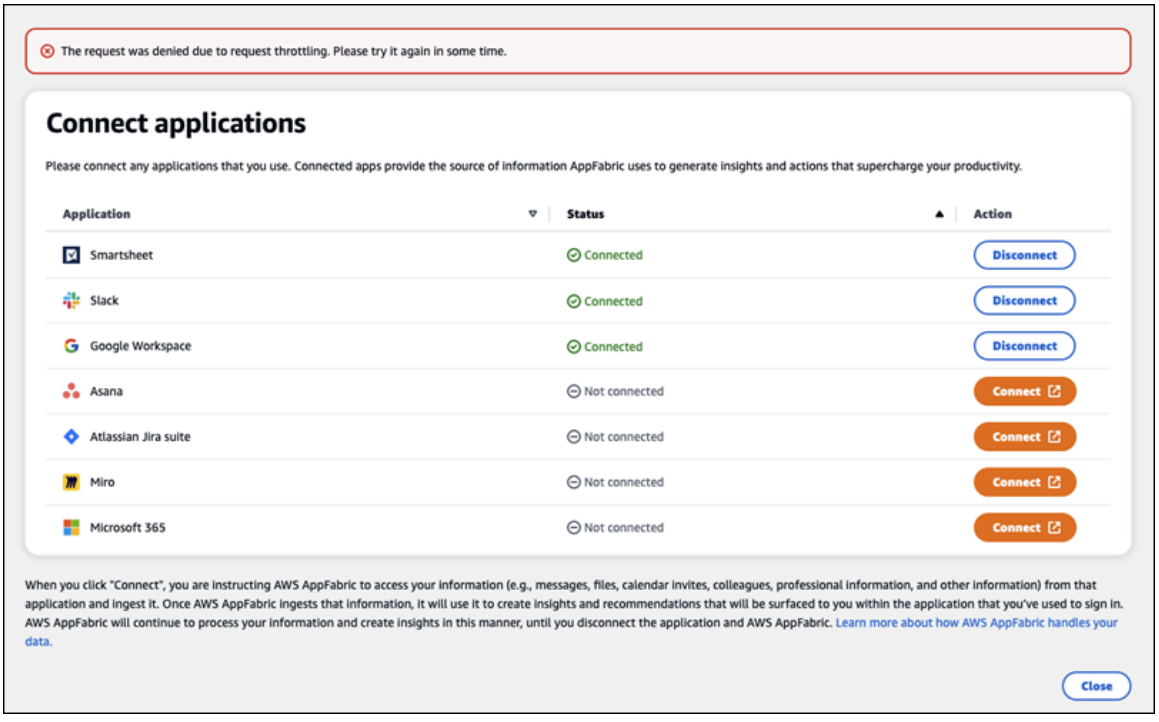
出了问题。请重试或者咨询您的管理员 (`InternalServerException`)

当 AppFabric 用户门户无法列出应用程序或由于未知错误、异常或故障而断开应用程序连接时，您可能会收到此消息。请稍后重试。



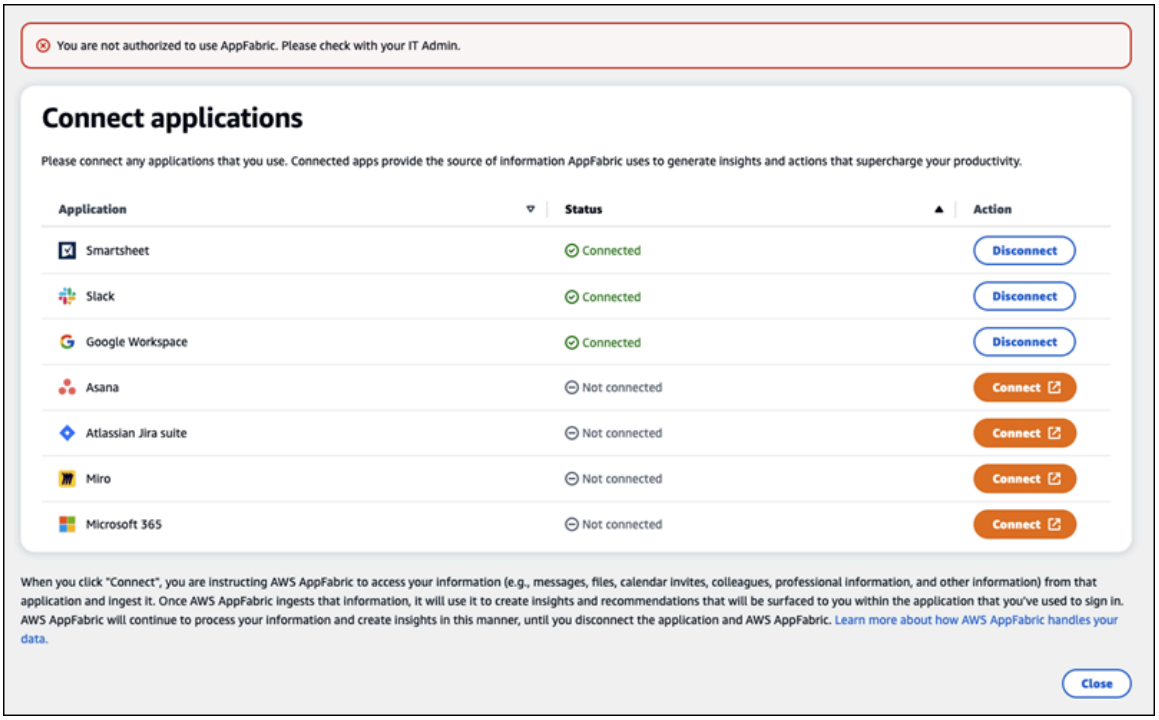
由于请求限制而导致请求被拒绝。请稍后再试 (**ThrottlingException**)

当 AppFabric 用户门户无法列出应用程序或由于限制问题而断开应用程序连接时，您可能会收到此消息。请稍后重试。



您无权使用 AppFabric。请 AppFabric 重新登录 (**`AccessDeniedException`**)

当 AppFabric 用户门户无法列出应用程序或由于访问被拒绝异常而断开应用程序连接时，您可能会收到此消息。 AppFabric 再次登录到。



AppFabric 提高工作效率 APIs （预览）

提高 AWS AppFabric 工作效率功能处于预览阶段，可能会发生变化。

本节提供 AWS AppFabric生产力功能的 API 操作、数据类型和常见错误。

> **Note**
>
> 有关所有其他信息 AppFabric APIs，请参阅 AWS AppFabric API 参考。

主题

- 提高工作效率 AppFabric 的 API 操作（预览版）
- 提高工作效率的 API 数据类型（预览版） AppFabric
- 提高工作效率的 AppFabric 常见 API 错误（预览版）

提高工作效率 AppFabric 的 API 操作（预览版）

提高 AWS AppFabric 工作效率功能处于预览阶段，可能会发生变化。

提高工作效率功能 AppFabric 支持以下操作。

有关所有其他 AppFabric API 操作，请参阅 AWS AppFabric API 操作。

主题

- 授权
- CreateAppClient
- DeleteAppClient
- GetAppClient
- ListActionableInsights
- ListAppClients
- ListMeetingInsights
- PutFeedback
- 令牌
- UpdateAppClient

授权

提高 AWS AppFabric 工作效率功能处于预览阶段，可能会发生变化。

授权. AppClient

主题

- 请求正文

请求正文

请求接受采用 JSON 格式的以下数据。

参数	说明
app_client_id	AppClient 要授权的 ID。
redirect_uri	授权后要将最终用户重定向到的 URI。
state	用于维护请求和回调之间状态的唯一值。

CreateAppClient

提高 AWS AppFabric 工作效率功能处于预览阶段，可能会发生变化。

创建一个 AppClient.

主题

- 请求正文
- 响应元素

请求正文

请求接受采用 JSON 格式的以下数据。

参数	说明
appName	应用程序的名称。 类型：字符串 长度限制：最小长度为 1。最大长度为 255。 是否必需：是
clientToken	指定为确保请求的幂等性而提供的唯一、区分大小写的标识符。这使您可以安全地重试请求，而不会意外地再次执行相同的操作。要将相同值传递给以后对操作的调用，则还需要为所有其他参数传递相同的值。我们建议您使用 UUID 类型的值。

参数	说明
	如果您不提供此值，则 AWS 会为您生成一个随机值。 如果您使用相同 `ClientToken` 但不同的参数重试该操作，则重试将失败并显示 `IdempotentParameterMismatch` 错误。 类型：字符串 模式：`[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 必需：否
customerManagedKey标识符	由 客户托管式密钥 生成的 ARN。 AWS Key Management Service密钥用于加密数据。 如果未指定密钥， AWS 托管式密钥 则使用。要分配给资源的一个或多个标记的键值对的映射。 有关客户托管密钥 AWS 拥有的密钥 的更多信息，请参阅《AWS Key Management Service 开发人员指南》中的客户 AWS 密钥和密钥。 类型：字符串 长度限制：最小长度为 1。最大长度为 1011。 模式：`arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 必需：否
描述	应用的描述。 类型：字符串 是否必需：是

参数	说明
iconUrl	的图标或徽标的网址 AppClient。 类型：字符串 必需：否
redirectUrls	授权后要将最终用户重定向到的 URI。您最多可以添加 5 个 redirectUrl。例如 `https://localhost:8080` 。 类型：字符串数组 数组成员：最少 1 个物品。最多 5 项。 长度限制：最小长度为 1。最大长度为 2048。 模式：`(http|https):\/\/[-a-zA-Z0-9_:.\/]+` 是否必需：是
starterUserEmails	入门电子邮件地址，这些用户在验证之前有权接收见解。AppClient 类型：字符串数组 数组成员：固定数量为 1 项。 长度限制：最小长度为 0。长度上限为 320。 模式：`[a-zA-Z0-9.!#$%&'*+/=?^_`{|}~-]+@[a-zA-Z0-9-]+(?:\.[a-zA-Z0-9-]+)*` 是否必需：是
tags	要分配给资源的一个或多个标记的键值对的映射。 类型：标签对象数组 数组成员：最少 0 个物品。最多 50 项。 必需：否

响应元素

如果此操作成功，则该服务将会发送回 HTTP 201 响应。

服务以 JSON 格式返回的以下数据。

参数	说明
appClientSummary	包含的摘要 AppClient。 类型：AppClientSummary 对象

DeleteAppClient

提高 AWS AppFabric 工作效率功能处于预览阶段，可能会发生变化。

删除应用程序客户端。

主题

- 请求正文
- 响应元素

请求正文

请求接受采用 JSON 格式的以下数据。

参数	说明
appClientIdentifier	用于请求的亚马逊资源名称 (ARN) 或通用唯一标识符 (UUID)。AppClient 长度限制：最小长度为 1。最大长度为 1011。 模式：`arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 是否必需：是

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 204 响应。

GetAppClient

提高 AWS AppFabric 工作效率功能处于预览阶段，可能会发生变化。

返回有关的信息 AppClient。

主题

请求正文

请求接受采用 JSON 格式的以下数据。

参数	说明
appClientIdentifier	用于请求的亚马逊资源名称 (ARN) 或通用唯一标识符 (UUID)。AppClient 长度限制：最小长度为 1。最大长度为 1011。 模式：`arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 是否必需：是

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

参数	说明
appClient	包含有关的信息 AppClient。 类型：AppClient 对象

ListActionableInsights

提高 AWS AppFabric 工作效率功能处于预览阶段，可能会发生变化。

列出最重要的可操作电子邮件、任务和其他更新。

主题

- 请求正文
- 响应元素

请求正文

请求接受采用 JSON 格式的以下数据。

参数	说明
nextToken	如果返回 `nextToken` ，则会有更多可用结果。`nextToken` 的值是每个页面的唯一分页令牌。使用返回的令牌再次调用以检索下一页。保留所有其他参数不变。每个分页令牌将在 24 小时后过期。使用过期的分页令牌将返回 HTTP 400 InvalidToken 错误。

响应元素

如果此操作成功，则该服务将会发送回 HTTP 201 响应。

服务以 JSON 格式返回的以下数据。

参数	说明
ActionableInsightsList	列出可操作的见解，包括标题、描述、操作和创建的时间戳。有关更多信息，请参阅 ActionableInsights。
nextToken	如果返回 nextToken ，则会有更多可用结果。nextToken 的值是每个页面的唯一分页令牌。使用返回的令牌再次调用以检索下一页。保留所有其他参数不变。每个分页令牌将在 24 小时后过期。使用过期的分页令牌将返回 HTTP 400 InvalidToken 错误。 类型：字符串

ListAppClients

提高 AWS AppFabric 工作效率功能处于预览阶段，可能会发生变化。

返回所有列表 AppClients。

主题

- 请求正文
- 响应元素

请求正文

请求接受采用 JSON 格式的以下数据。

参数	说明
maxResults	每个调用返回的最大结果数。您可以使用 nextToken 获取更多的结果页面。 这只是一个上限。每次调用返回的实际结果数可能少于指定的最大值。 有效范围：最小值为 1。最大值为 100。

参数	说明
nextToken	如果返回 nextToken ，则会有更多可用结果。nextToken 的值是每个页面的唯一分页令牌。使用返回的令牌再次调用以检索下一页。保留所有其他参数不变。每个分页令牌将在 24 小时后过期。使用过期的分页令牌将返回 HTTP 400 InvalidToken 错误。

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

参数	说明
appClientList	包含 AppClient 结果列表。 类型：AppClientSummary 对象数组
nextToken	如果返回 nextToken ，则会有更多可用结果。nextToken 的值是每个页面的唯一分页令牌。使用返回的令牌再次调用以检索下一页。保留所有其他参数不变。每个分页令牌将在 24 小时后过期。使用过期的分页令牌将返回 HTTP 400 InvalidToken 错误。 类型：字符串

ListMeetingInsights

提高 AWS AppFabric 工作效率功能处于预览阶段，可能会发生变化。

列出最重要的可操作的日历事件。

主题

- 请求正文
- 响应元素

请求正文

请求接受采用 JSON 格式的以下数据。

参数	说明
nextToken	如果返回 nextToken ，则会有更多可用结果。nextToken 的值是每个页面的唯一分页令牌。使用返回的令牌再次调用以检索下一页。保留所有其他参数不变。每个分页令牌将在 24 小时后过期。使用过期的分页令牌将返回 HTTP 400 InvalidToken 错误。

响应元素

如果此操作成功，则该服务将会发送回 HTTP 201 响应。

服务以 JSON 格式返回的以下数据。

参数	说明
MeetingInsightList	列出可操作的会议见解。有关更多信息，请参阅 MeetingInsights。
nextToken	如果返回 nextToken ，则会有更多可用结果。nextToken 的值是每个页面的唯一分页令牌。使用返回的令牌再次调用以检索下一页。保留所有其他参数不变。每个分页令牌将在 24 小时后过期。使用过期的分页令牌将返回 HTTP 400 InvalidToken 错误。 类型：字符串

PutFeedback

提高 AWS AppFabric 工作效率功能处于预览阶段，可能会发生变化。

允许用户针对给定的见解或操作提交反馈。

主题

- 请求正文
- 响应元素

请求正文

请求接受采用 JSON 格式的以下数据。

参数	说明
id	要提交反馈的对象的 ID。这可以是 InsightId 或 ActionId。
feedbackFor	要提交反馈的见解类型。 可能的值：`ACTIONABLE_INSIGHT | MEETING_INSIGHT | ACTION`
feedbackRating	反馈评分从 1 到 5。评分越高越好。

响应元素

如果此操作成功，则该服务会发送回带有空 HTTP 正文的 HTTP 201 响应。

令牌

提高 AWS AppFabric 工作效率功能处于预览阶段，可能会发生变化。

包含 AppClients 允许将授权码交换为访问令牌的信息。

主题

- 请求正文
- 响应元素

请求正文

请求接受采用 JSON 格式的以下数据。

参数	说明
代码	从授权端点接收的授权码。 类型：字符串 长度限制：最小长度为 1。最大长度为 2048。 必需：否
grant_type	令牌的授予类型。必须是 `authorization_code` 或 `refresh_token` 。 类型：字符串 是否必需：是
app_client_id	AppClient 的 ID。 类型：字符串 模式：`[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 是否必需：是
redirect_uri	传递给授权端点的重定向 URI。 类型：字符串 必需：否
refresh_token	从初始令牌请求接收的刷新令牌。 类型：字符串 长度限制：最小长度为 1。最大长度为 4096。 必需：否

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

参数	说明
appfabric_user_id	令牌的用户 ID。只有使用 `authorization_code` 授予类型的请求才会返回此值。 类型：字符串
expires_in	令牌过期前的秒数。 类型：长整型
refresh_token	用于后续请求的刷新令牌。 类型：字符串 长度限制：最小长度为 1。最大长度为 2048。
token	访问令牌。 类型：字符串 长度限制：最小长度为 1。最大长度为 2048。
token_type	令牌类型。 类型：字符串

UpdateAppClient

提高 AWS AppFabric 工作效率功能处于预览阶段，可能会发生变化。

更新一个 AppClient.

主题

- 请求正文
- 响应元素

请求正文

请求接受采用 JSON 格式的以下数据。

参数	说明
appClientIdentifier	用于请求的亚马逊资源名称 (ARN) 或通用唯一标识符 (UUID)。AppClient 长度限制：最小长度为 1。最大长度为 1011。 模式：`arn:.+$|^[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 是否必需：是
redirectUrls	授权后要将最终用户重定向到的 URI。您最多可以添加 5 个 redirectUrl。例如 `https://localhost:8080` 。 类型：字符串数组 数组成员：最少 1 个物品。最多 5 项。 长度限制：最小长度为 1。最大长度为 2048。 模式：`(http|https):\/\/[-a-zA-Z0-9_:.\/]+`

响应元素

如果此操作成功，则该服务将会发送回 HTTP 200 响应。

服务以 JSON 格式返回以下数据。

参数	说明
appClient	包含有关的信息 AppClient。

参数	说明
	类型：AppClient 对象

提高工作效率的 API 数据类型（预览版） AppFabric

提高 AWS AppFabric 工作效率功能处于预览阶段，可能会发生变化。

AppFabric API 包含各种操作使用的多种数据类型。本节详细描述了提高效率功能的数据类型。AppFabric

有关所有其他 AppFabric API 数据类型，请参阅 AWS AppFabric API 数据类型。

> **Important**
>
> 不能保证数据类型结构中每个元素的顺序。应用程序不应假设特定的顺序。

主题

- ActionableInsights
- AppClient
- AppClientSummary
- MeetingInsights
- VerificationDetails

ActionableInsights

提高 AWS AppFabric 工作效率功能处于预览阶段，可能会发生变化。

根据用户应用程序产品组合中的电子邮件、日历邀请、消息和任务，包含用户的重要且合适的操作摘要。用户可以看到来自各个应用程序的主动见解，以帮助他们最好地调整一天的方向。这些见解为用户为什么应关心见解摘要以及生成见解的各个应用程序和构件的引用（例如嵌入式链接）提供了理由。

参数	说明
insightId	生成的见解的唯一 ID。
insightContent	这将返回见解摘要以及用于生成见解的构件的嵌入式链接。 这将是一个包含嵌入式链接（<a> 标签）的 HTML 内容。
insightTitle	生成的见解的标题。
createdAt	当生成见解时。
actions	为生成的见解建议的操作列表。 操作对象包含下列参数： • actionId — 生成的操作的唯一 ID。 • actionIconUrl — 建议在其中执行操作的应用程序的图标 URL。 • actionTitle — 生成的操作的标题。 • actionUrl — 供最终用户在用户门户中查看和执行操作 AppFabric的唯一 URL。 为了执行操作，ISV 应用程序将使用此 URL 将用户重定向到 AppFabric 用户门户（弹出屏幕）。 • actionExecutionStatus — 指示操作状态的枚举。 可能的值包括：EXECUTED | NOT_EXECUTED

AppClient

提高 AWS AppFabric 工作效率功能处于预览阶段，可能会发生变化。

包含有关的信息 AppClient。

参数	说明
appName	应用程序的名称。 类型：字符串 是否必需：是
arn	AppClient 的 Amazon 资源名称（ARN）。 类型：字符串 长度限制：最小长度为 1。最大长度为 1011。 模式：`arn:.+` 是否必需：是
描述	应用程序的描述。 类型：字符串 是否必需：是
iconUrl	的图标或徽标的网址 AppClient。 类型：字符串 必需：否
redirectUrls	允许的重 URLs 定向 AppClient。 类型：字符串数组 数组成员：最少 1 个物品。最多 5 项。 长度限制：最小长度为 1。最大长度为 2048。 模式：`(http|https):\/\/[-a-zA-Z0-9_:.\/]+` 是否必需：是

参数	说明
starterUserEmails	入门电子邮件地址，这些用户在验证之前有权接收见解。 AppClient 类型：字符串数组 数组成员：固定数量为 1 项。 长度限制：最小长度为 0。长度上限为 320。 模式：`[a-zA-Z0-9.!#$%&'*+/=?^_`{|}~-]+@[a-zA-Z0-9-]+(?:\.[a-zA-Z0-9-]+)*` 是否必需：是
verificationDetails	包含 AppClient验证的状态和原因。 类型：VerificationDetails 对象 是否必需：是
customerManagedKeyArn	为 客户托管式密钥 生成的亚马逊资源名称 (ARN) AWS Key Management Service 。 AppClient 类型：字符串 长度限制：最小长度为 1。最大长度为 1011。 模式：`arn:.+` 必需：否
appClientId	AppClient 的 ID。旨在用于应用程序客户端的 o-auth 流程。 类型：字符串 模式：`[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 必需：否

AppClientSummary

提高 AWS AppFabric 工作效率功能处于预览阶段，可能会发生变化。

包含有关的信息 AppClient。

参数	说明
arn	AppClient 的 Amazon 资源名称（ARN）。 类型：字符串 长度限制：最小长度为 1。最大长度为 1011。 模式：`arn:.+` 是否必需：是
verificationStatus	AppClient 验证状态。 类型：字符串 有效值：`pending_verification | verified | rejected` 是否必需：是
appClientId	AppClient 的 ID。旨在用于应用程序客户端的 o-auth 流程。 类型：字符串 模式：`[a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}` 必需：否

MeetingInsights

提高 AWS AppFabric 工作效率功能处于预览阶段，可能会发生变化。

包含前 3 个会议的摘要，以及会议目的、相关的跨应用程序构件以及来自任务、电子邮件、消息和日历事件的活动。

参数	说明
insightId	生成的见解的唯一 ID。
insightContent	见解的描述，以字符串格式突出显示详细信息。例如，为什么这种见解很重要。
insightTitle	生成的见解的标题。
createdAt	当生成见解时。
calendarEvent	用户应关注的重要日历事件或会议。 日历事件对象： • `startTime` — 事件的开始时间。 • `endTime` — 事件的结束时间。 • `eventUrl` — ISV 应用程序上日历事件的 URL。
resources	包含与生成的见解相关的其他资源的列表。 资源对象： • `appName` — 资源所属的应用程序名称。 • `resourceTitle` — 资源标题。 • `resourceType` — 资源的类型。 可能的值包括：`EMAIL | EVENT | MESSAGE | TASK` • `resourceUrl` — 应用程序中的资源 URL。 • `appIconUrl` — 资源所属应用程序的图像 URL。

参数	说明
nextToken	用于获取下一组见解的分页令牌。这是一个可选字段，如果返回 null，则表示没有更多的见解可供加载。

VerificationDetails

提高 AWS AppFabric 工作效率功能处于预览阶段，可能会发生变化。

包含 AppClient 验证的状态和原因。

参数	说明
verificationStatus	AppClient 验证状态。 类型：字符串 有效值：`pending_verification | verified | rejected` 是否必需：是
statusReason	AppClient 验证状态原因。 类型：字符串 长度限制：最小长度为 1。最大长度为 1024。 必需：否

提高工作效率的 AppFabric 常见 API 错误（预览版）

提高 AWS AppFabric 工作效率功能处于预览阶段，可能会发生变化。

本节列出了 AWS AppFabric 生产力功能的 API 操作中常见的错误。

有关所有其他 AppFabric 常见的 API 错误，请参阅进行故障排除 AppClients AppFabric 以提高工作效率《AWS AppFabric API 参考》中的AWS AppFabric API 常见错误。

异常名称	说明
TokenException	令牌请求无效。 HTTP 状态代码：400

中的数据处理 AppFabric

“ AWS AppFabric 提高生产力” 功能处于预览阶段，可能会发生变化。

AppFabric 采取措施将用户内容单独存储在由 AppFabric和单独管理的 Amazon S3 存储桶中；这有助于确保我们生成用户特定的见解。我们使用合理的保障措施来保护您的内容，包括静态加密和动态加密。我们已将系统配置为在客户内容接收后 30 天内自动删除。 AppFabric 不会使用用户不再有权访问的数据工件生成见解。例如，当用户断开数据源（应用程序）的连接时， AppFabric 停止从该应用程序收集数据，并且不使用断开连接的应用程序中的任何延迟工件来生成见解。 AppFabric的系统配置为在 30 天内删除此类数据。

AppFabric 不使用用户内容来训练或改进用于生成见解的底层大型语言模型。有关生成人工智能功能AppFabric的更多信息，请参阅 A mazon Bedrock FAQs。

静态加密

AWS AppFabric 支持静态加密，这是一种服务器端加密功能，当用户相关的所有数据保存到磁盘时，可以 AppFabric透明地对其进行加密，并在您访问数据时对其进行解密。

传输中加密

AppFabric 使用 TLS 1.2 保护传输中的所有内容，并使用 AWS 签名版本 4 签署 AWS 服务的 API 请求。

中的术语和概念 AppFabric

本主题介绍中的关键术语和概念 AWS AppFabric ，以帮助您入门。

应用程序捆绑包

A AppFabric pp bundle 存储您的所有 AppFabric 应用程序授权和摄取（参见以下摄取定义）。您可以为 AWS 账户 每个应用程序创建一个 App bundle AWS 区域。

AppClient （还有应用程序客户端和应用程序客户端）

OAuth AppClient 适用于数据接收者应用程序。每个数据接收方应用程序都需要注册 AppClient 才能访问 AppFabric 数据。开发者用户需要一个 AWS 账号才能注册 AppClient。每个 AWS 账户只能注册一个 AppClient。 AppFabric 将基于以下内容出售访问令牌。 AppClient AppClient 将包含有关数据接收者应用程序的信息，该应用程序将通过此应用程序访问 AppFabric 数据 AppClient。

App 授权

应用程序授权授予连接您的应用程序并与之交互的 AppFabric 权限。它允许使用 OAuth （开放授权-用于授予应用程序访问权限的访问委托的开放标准）或个人访问令牌 (PAT) 凭证从您的应用程序中提取审核日志。您可以为每个应用程序捆绑包设置多个应用程序授权（最多 50 个）。这 AppFabric 允许根据需要为应用程序的每个租户重复应用程序授权创建步骤，从而从应用程序的多个租户提取审核日志。共享的凭据使用 AWS Key Management Service (AWS KMS) 中的 AWS 拥有的密钥 或客户管理的密钥进行加密，并存储在中 AppFabric。

摄取

AppFabric 摄取使用应用程序授权，通过应用程序的公共应用程序从应用程序中提取审核日志。 APIs 然后，它将审核日志传送到一个或多个（最多五个）目标。

客户端 ID

当您创建应用程序授权以连接使用该 OAuth 流程的应用程序时， AppFabric 可能会要求您提供客户端 ID 和客户端密钥。客户端 ID 和客户端密钥可以在应用程序的身份验证应用程序中找到。有关在给定身份验证应用程序中如何找到客户端 ID 的说明，请参阅支持的应用程序。共享的客户端 ID 和客户端密钥使用 AWS 拥有的密钥 或客户托管密 AWS KMS 钥进行加密并存储在 AppFabric。

客户端密钥

当您创建应用程序授权以连接使用该 OAuth 流程的应用程序时， AppFabric 可能会要求您提供客户端 ID 和客户端密钥。客户端 ID 和客户端密钥可以在应用程序的身份验证应用程序中找到。有关在给定身

份验证应用程序中如何找到客户端密钥的说明，请参阅支持的应用程序。共享的客户端 ID 和客户端密钥使用 AWS 拥有的密钥 或客户托管密 AWS KMS 钥进行加密并存储在 AppFabric。

提取目标

提取目标定义了从提取中获得的审核日志应存储在哪里。每次摄取都可以将审核日志传送到一个或多个目的地（最多五个），即亚马逊简单存储服务 (Amazon S3) Service 存储桶或您中的亚马逊数据 Firehose。 AWS 账户对于每个目标，您可以定义是希望日志采用原始形式还是标准化为开放网络安全架构框架 (OCSF) 架构。选择 OCSF 架构时，您可以定义日志的格式（JSON 或 Apache Parquet）。只有选择 Amazon S3 作为目标时，才能使用 Apache Parquet 格式。

数据接收者应用程序

将调用 AppFabric 以从中获取生成的见解的应用程序 AppFabric。

OAuth

OAuth 是一种开放协议，允许通过 Web、移动和桌面应用程序以简单而标准的方法进行安全授权。AppFabric OAuth 用于创建一些应用程序授权。

开放式网络安全架构框架（OCSF）

开放网络安全架构框架 (OCSF) 是一个开源项目，为开发架构提供了一个可扩展的框架，以及一个与供应商无关的核心安全架构。供应商和其他数据生成工具可以为其特定域采用和扩展架构。目标是提供可在任何环境、应用程序或解决方案中采用的开放标准，同时补充现有的安全标准和流程。 AppFabric 已扩展此架构，以创建以软件即服务 (SaaS) 为中心的事件结构，所有支持的 SaaS 应用程序审核日志都 AppFabric 将标准化为该结构。有关更多信息，请参阅 开放网络安全架构框架 AWS AppFabric。

个人访问令牌 (PAT)

个人访问令牌 (PAT) 是一串字符，可用于访问计算机系统，而不是通常的密码。当您创建应用程序授权以连接使用 PAT 流程的应用程序时， AppFabric 可能会要求您提供 PAT。PAT 可以在应用程序的身份验证应用程序中找到。有关如何在特定身份验证应用程序中找到 PAT 的说明，请参阅支持的应用程序。共享的服务帐号令牌使用 AWS 拥有的密钥 或客户托管密 AWS KMS 钥进行加密并存储在 AppFabric。

服务账户令牌

当您创建 AppFabric 应用程序授权以连接应用程序时，某些应用程序需要创建服务帐户才能进行应用程序身份验证。 AppFabric 作为应用程序授权过程的一部分，可能会要求提供服务帐号令牌。有关如

何在给定身份验证应用程序中找到服务账户令牌的说明，请参阅支持的应用程序。共享的服务帐号令牌使用 AWS 拥有的密钥 或客户托管密 AWS KMS 钥进行加密并存储在 AppFabric。

租户编号

创建应用程序授权时， AppFabric 可能会要求您提供应用程序的租户 ID 和租户名称。租户 ID 是应用程序租户的唯一标识符。每个应用程序可能对租户使用不同的术语，例如 Slack 的WorkSpace ID或 Asana 的域 ID。有关如何在特定应用程序中找到租户 ID 的说明，请参阅支持的应用程序。

租户名称

创建应用程序授权时， AppFabric 可能会要求您提供应用程序的租户 ID 和租户名称。租户名称是您为租户 ID 指定的唯一名称，可在应用程序捆绑包中使用。此值用于标记应用程序授权和任何相关提取。

安全性 AWS AppFabric

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

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

- 云安全 — AWS 负责保护在云 AWS 服务 中运行的基础架构 AWS 云。 AWS 还为您提供可以安全使用的服务。作为AWS 合规计划合规计划合规计划合的一部分，第三方审计师定期测试和验证我们安全的有效性。要了解适用的合规计划 AWS AppFabric，请参阅按合规计划划分的范围内的AWSAWS服务按合规计划。
- 云端安全 — 您的责任由您 AWS 服务 使用的内容决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

本文档可帮助您了解在使用时如何应用分担责任模型 AppFabric。以下主题向您介绍如何进行配置 AppFabric 以满足您的安全和合规性目标。您还将学习如何使用其他 AWS 服务 方法来监控和保护您的 AppFabric 资源。

主题

- 中的数据保护 AWS AppFabric
- 的身份和访问管理 AWS AppFabric
- 合规性验证 AWS AppFabric
- 以下方面的安全最佳实践 AWS AppFabric
- 韧性在 AWS AppFabric
- 中的基础设施安全 AWS AppFabric
- 中的配置和漏洞分析 AWS AppFabric

中的数据保护 AWS AppFabric

分 AWS 担责任模型适用于中的数据保护 AWS AppFabric。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS 云。您负责维护对托管在此基础结构上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS Security Blog 上的 AWS Shared Responsibility Model and GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。
- 用于 SSL/TLS 与 AWS 资源通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。有关使用 CloudTrail 跟踪捕获 AWS 活动的信息，请参阅《AWS CloudTrail 用户指南》中的使用跟 CloudTrail 踪。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-3 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-3 版》https://aws.amazon.com/compliance/fips/。

强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括您使用控制台、API AppFabric 或以其他 AWS 服务 方式使用控制台 AWS CLI、API 或时 AWS SDKs。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供 URL，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

> **Note**
>
> 有关适用于安全性的数据保护的 AppFabric 更多信息，请参阅中的数据处理 AppFabric。

静态加密

AWS AppFabric 支持静态加密，这是一种服务器端加密功能，当与您的应用程序包相关的所有数据保存到磁盘时，可以 AppFabric透明地对其进行加密，并在您访问数据时对其进行解密。默认情况下，使用 from AWS Key Management Service (AWS KMS) AppFabric 加密您的数据。 AWS 拥有的密钥 您也可以选择使用自己的客户托管密钥对数据进行加密 AWS KMS。

当您删除应用程序捆绑包时，其所有元数据都将被永久删除。

传输中加密

配置应用程序包时，您可以选择 AWS 拥有的密钥 或客户托管密钥。在为审计日志摄取收集和规范化数据时，会将数据临时存储在中间亚马逊简单存储服务 (Amazon S3) Service 存储桶中，并使用此密钥对其进行加密。 AppFabric 该临时的存储桶将在 30 天后使用存储桶生命周期策略删除。

AppFabric 使用 TLS 1.2 保护传输中的所有数据，并使用 AWS 签名 V4 签名 API 请求。 AWS 服务

密钥管理

AppFabric 支持使用 AWS 拥有的密钥 或客户托管密钥加密数据。我们建议您使用客户托管密钥，因为它能让您完全控制加密数据。当您选择客户托管密钥时，会将资源策略 AppFabric 附加到客户托管密钥，授予其访问客户托管密钥的权限。

客户托管密钥

要创建客户托管密钥，请按照 AWS KMS 开发人员指南的创建对称加密 KMS 密钥中的步骤进行操作。

密钥策略

密钥策略控制对客户托管密钥的访问。每个客户托管密钥必须只有一个密钥策略，其中包含确定谁可以使用密钥以及如何使用密钥的声明。创建客户托管密钥时，可以指定密钥策略。有关创建密钥政策的更多信息，请参阅 AWS KMS 开发人员指南中的创建密钥政策。

要将客户托管密钥与一起使用 AppFabric，创建您的 AppFabric资源的 AWS Identity and Access Management (IAM) 用户或角色必须有权使用您的客户托管密钥。我们建议您创建一个仅与之配合使用的密钥， AppFabric 并将您的 AppFabric 用户添加为该密钥的用户。这种方法限制了访问您数据的范围。您的用户需要的权限如下所示：

- `kms:DescribeKey`
- `kms:CreateGrant`
- `kms:GenerateDataKey`
- `kms:Decrypt`

AWS KMS 控制台将指导您使用相应的密钥策略创建密钥。有关密钥策略的更多信息，请参阅 AWS KMS 开发人员指南的 AWS KMS中的密钥策略。

以下是一个密钥政策示例，它可以：

- 对钥匙的 AWS 账户根用户 完全控制。

- 允许用户使用 AppFabric 您的客户托管密钥 AppFabric。
- us-east-1 中设置的应用程序捆绑包的密钥政策。

如何在中 AppFabric 使用补助金 AWS KMS

AppFabric 需要获得授权才能使用您的客户托管密钥。有关更多信息，请参阅 AWS KMS 开发人员指南的 AWS KMS中的授权。

创建应用程序包时，通过向发送CreateGrant请求来代表您 AppFabric 创建授权 AWS KMS。中的授权 AWS KMS 用于授予对客户账户中 AWS KMS 密钥的 AppFabric 访问权限。 AppFabric 要求授权使用您的客户托管密钥进行以下内部操作：

- 向发送GenerateDataKey请求 AWS KMS 以生成由您的客户托管密钥加密的数据密钥。
- 向发送解密加密数据密钥的Decrypt请求，以便这些密钥可用于加密您的数据和解密传输中的应用程序访问令牌。 AWS KMS
- 向发送Encrypt请求 AWS KMS 以加密传输中的应用程序访问令牌。

以下是授权的示例。

```
{
  "KeyId": "arn:aws:kms:us-east-1:111122223333:key/ff000af-00eb-00ce-0e00-
ea000fb0fba0SAMPLE",
  "GrantId": "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
  "Name": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
  "CreationDate": "2022-10-11T20:35:39+00:00",
  "GranteePrincipal": "appfabric.us-east-1.amazonaws.com",
  "RetiringPrincipal": "appfabric.us-east-1.amazonaws.com",
  "IssuingAccount": "arn:aws:iam::111122223333:root",
  "Operations": [
    "Decrypt",
    "Encrypt",
    "GenerateDataKey"
  ],
  "Constraints": {
    "EncryptionContextSubset": {
      "appBundleArn": "arn:aws:fabric:us-east-1:111122223333:appbundle/
ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE"
    }
  }
```

```
},
```

当您删除应用程序包时，会 AppFabric 停用对您的客户托管密钥发放的授权。

监控您的加密密钥 AppFabric

当您将 AWS KMS 客户托管密钥与一起使用时 AppFabric，您可以使用 AWS CloudTrail 日志来跟踪 AppFabric 发送到的请求 AWS KMS。

以下是 AppFabric 使用`CreateGrant`客户托管密钥时记录 CloudTrail 的事件示例。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:SampleUser",
        "arn": "arn:aws:sts::111122223333:assumed-role/AssumedRole/SampleUser",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/AssumedRole",
                "accountId": "111122223333",
                "userName": "SampleUser"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-04-28T14:01:33Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-04-28T14:05:48Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "appfabric.amazonaws.com",
    "userAgent": "appfabric.amazonaws.com",
    "requestParameters": {
        "granteePrincipal": "appfabric.us-east-1.amazonaws.com",
        "constraints": {
```

```
            "encryptionContextSubset": {
                "appBundleArn": "arn:aws:appfabric:us-east-1:111122223333:appbundle/
ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE"
            }
        },
        "keyId": "arn:aws:kms:us-east-1:111122223333:key/EXAMPLEID",
        "retiringPrincipal": "appfabric.us-east-1.amazonaws.com",
        "operations": [
            "Encrypt",
            "Decrypt",
            "GenerateDataKey"
        ]
    },
    "responseElements": {
        "grantId": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
        "keyId": "arn:aws:kms:us-east-1:111122223333:key/KEY_ID"
    },
    "additionalEventData": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-east-1:111122223333:key/key_ID"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_256_GCM_SHA384",
        "clientProvidedHostHeader": "kms.us-east-1.amazonaws.com"
    }
}
```

的身份和访问管理 AWS AppFabric

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

主题

受众

您的使用方式 AWS Identity and Access Management (IAM) 因您的角色而异：

- 服务用户：如果您无法访问功能，请从管理员处请求权限（请参阅对 AWS AppFabric 身份和访问进行故障排除）
- 服务管理员：确定用户访问权限并提交权限请求（请参阅如何 AWS AppFabric 与 IAM 配合使用）
- IAM 管理员：编写用于管理访问权限的策略（请参阅基于身份的策略示例 AWS AppFabric）

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份进行身份验证 AWS 账户根用户，或者通过担任 IAM 角色进行身份验证。

您可以使用来自身份源的证书 AWS IAM Identity Center （例如（IAM Identity Center）、单点登录身份验证或 Google/Facebook 证书，以联合身份登录。有关登录的更多信息，请参阅《AWS 登录 用户指南》中的如何登录您的 AWS 账户。

对于编程访问， AWS 提供 SDK 和 CLI 来对请求进行加密签名。有关更多信息，请参阅《IAM 用户指南》中的适用于 API 请求的AWS 签名版本 4。

AWS 账户 root 用户

创建时 AWS 账户，首先会有一个名为 AWS 账户 root 用户的登录身份，该身份可以完全访问所有资源 AWS 服务 和资源。我们强烈建议不要使用根用户进行日常任务。有关需要根用户凭证的任务，请参阅《IAM 用户指南》中的需要根用户凭证的任务。

联合身份

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

联合身份是指来自您的企业目录、Web 身份提供商的用户 Directory Service ，或者 AWS 服务 使用来自身份源的凭据进行访问的用户。联合身份代入可提供临时凭证的角色。

要集中管理访问权限，建议使用。 AWS IAM Identity Center有关更多信息，请参阅《AWS IAM Identity Center 用户指南》中的什么是 IAM Identity Center？。

IAM 用户和群组

IAM 用户是对某个人员或应用程序具有特定权限的一个身份。建议使用临时凭证，而非具有长期凭证的 IAM 用户。有关更多信息，请参阅 IAM 用户指南中的要求人类用户使用身份提供商的联合身份验证才能 AWS 使用临时证书进行访问。

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

IAM 角色

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

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

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略定义了与身份或资源关联时的权限。 AWS 在委托人提出请求时评估这些政策。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概述。

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

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

基于身份的策略

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

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

基于资源的策略

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

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

其他策略类型

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

- 权限边界 – 设置基于身份的策略可以授予 IAM 实体的最大权限。有关更多信息，请参阅《 IAM 用户指南》中的 IAM 实体的权限边界。
- 服务控制策略 (SCPs)-在中指定组织或组织单位的最大权限 AWS Organizations。有关更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略。
- 资源控制策略 (RCPs)-设置账户中资源的最大可用权限。有关更多信息，请参阅《AWS Organizations 用户指南》中的资源控制策略 (RCPs)。
- 会话策略 – 在为角色或联合用户创建临时会话时，作为参数传递的高级策略。有关更多信息，请参阅《IAM 用户指南》中的会话策略。

多个策略类型

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

如何 AWS AppFabric 与 IAM 配合使用

在使用 IAM 管理访问权限之前 AppFabric，请先了解哪些可用的 IAM 功能 AppFabric。

您可以搭配使用的 IAM 功能 AWS AppFabric

IAM 功能	AppFabric 支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	是
策略条件密钥	否
ACLs	否
ABAC（策略中的标签）	是
临时凭证	否
主体权限	是
服务角色	否
服务关联角色	是

要全面了解大多数 IAM 功能的使用方式 AppFabric 和其他 AWS 服务 功能，请参阅 IAM 用户指南中的与 IAM 配合使用的AWS 服务。

基于身份的策略 AppFabric

支持基于身份的策略：是

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

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

基于身份的策略示例 AppFabric

要查看 AppFabric 基于身份的策略的示例，请参阅。基于身份的策略示例 AWS AppFabric

内部基于资源的政策 AppFabric

支持基于资源的策略：否

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

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

的政策行动 AppFabric

支持策略操作：是

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

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

要查看 AppFabric 操作列表，请参阅《服务授权参考》 AWS AppFabric中定义的操作。

正在执行的策略操作在操作前 AppFabric 使用以下前缀：

```
appfabric
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

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

您可以使用通配符 (*) 指定多个操作。例如，要指定以单词 List 开头的所有操作，请包括以下操作。

```
"Action": "appfabric:List*"
```

要查看 AppFabric 基于身份的策略的示例，请参阅。基于身份的策略示例 AWS AppFabric

的政策资源 AppFabric

支持策略资源：是

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

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

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

要查看 AppFabric 资源类型及其列表 ARNs，请参阅《服务授权参考》 AWS AppFabric中定义的资源类型。要了解您可以使用哪些操作来指定每种资源的 ARN，请参阅定义的操作。 AWS AppFabric

要查看 AppFabric 基于身份的策略的示例，请参阅。基于身份的策略示例 AWS AppFabric

的策略条件密钥 AppFabric

支持特定于服务的策略条件键：否

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

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

要查看 AppFabric 条件密钥列表，请参阅《服务授权参考》 AWS AppFabric中的条件密钥。要了解可以使用条件键的操作和资源，请参阅由定义的操作 AWS AppFabric。

要查看 AppFabric 基于身份的策略的示例，请参阅。基于身份的策略示例 AWS AppFabric

ACLs in AppFabric

支持 ACLs：否

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。

ABAC with AppFabric

支持 ABAC（策略中的标签）：是

基于属性的访问权限控制（ABAC）是一种授权策略，该策略基于称为标签的属性来定义权限。您可以将标签附加到 IAM 实体和 AWS 资源，然后设计 ABAC 策略以允许在委托人的标签与资源上的标签匹配时进行操作。

要基于标签控制访问，您需要使用 `aws:ResourceTag/`*`key-name`*`aws:RequestTag/`*`key-name`* 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权定义权限。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

将临时凭证与配合使用 AppFabric

支持临时凭证：否

临时证书提供对 AWS 资源的短期访问权限，并且是在您使用联合身份或切换角色时自动创建的。AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的临时安全凭证和使用 IAM 的。AWS 服务

的跨服务主体权限 AppFabric

支持转发访问会话（FAS）：是

转发访问会话 (FAS) 使用调用主体的权限 AWS 服务，再加上 AWS 服务 向下游服务发出请求的请求。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

的服务角色 AppFabric

支持服务角色：否

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。

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

的服务相关角色 AppFabric

支持服务关联角色：是

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

有关创建或管理 AppFabric 服务相关角色的详细信息，请参阅将服务相关角色用于 AppFabric。

基于身份的策略示例 AWS AppFabric

默认情况下，用户和角色没有创建或修改 AppFabric 资源的权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。

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

有关由 AppFabric定义的操作和资源类型（包括每种资源类型的格式）的详细信息，请参阅《服务授权参考》 AWS AppFabric中的操作、资源和条件密钥。 ARNs

目录

- 使用控制 AppFabric 台
- AppFabric 有关安全 IAM 策略示例
  - 允许访问应用程序捆绑包
  - 限制对应用程序捆绑包的访问
  - 限制删除或停止摄取
- AppFabric 有关生产力 IAM 策略示例
  - 允许以只读方式访问生产力功能
  - 允许完全访问生产力功能
  - 允许访问创建 AppClients
  - 允许访问以获取以下详细信息 AppClients
  - 允许访问列表 AppClients
  - 允许访问更新 AppClients
  - 允许访问删除 AppClients
  - 允许访问以授权应用程序
- 其他 IAM 策略示例
  - 允许用户查看他们自己的权限

策略最佳实践

基于身份的策略决定了某人是否可以在您的账户中创建、访问或删除 AppFabric 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管策略或工作职能的AWS 托管策略。
- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。

- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性：IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言（JSON）和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM Access Analyzer 验证策略。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的使用 MFA 保护 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。

使用控制 AppFabric 台

将AWSAppFabricReadOnlyAccess AWS 托管策略附加到您的 IAM 身份，以授予他们对该 AppFabric 服务（包括中的 AppFabric控制台）的只读权限 AWS 管理控制台。或者，您可以将AWSAppFabricFullAccess AWS 托管策略附加到您的 IAM 身份，以授予他们对该 AppFabric 服务的完全管理权限。有关更多信息，请参阅 AWS 的托管策略 AWS AppFabric。

AppFabric 有关安全 IAM 策略示例

以下策略示例 AppFabric 适用于安全功能。

允许访问应用程序捆绑包

以下策略示例授予对 AppFabric服务中应用程序捆绑包的访问权限。

JSON

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

    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:StartUserAccessTasks",
                "appfabric:BatchGetUserAccessTasks"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
        }
    ]
```

```
}
```

限制对应用程序捆绑包的访问

以下策略示例限制了对服务中应用程序捆绑包的 AppFabric访问权限。

JSON

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

    "Statement": [
        {
            "Action": ["appfabric:*"],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "appfabric:StartUserAccessTasks",
                "appfabric:BatchGetUserAccessTasks"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
        }
    ]
}
```

限制删除或停止摄取

以下策略示例限制删除或停止服务中的摄取。 AppFabric

JSON

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

    "Statement": [
        {
            "Action": ["appfabric:*"],
```

```
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "appfabric:StopIngestion",
                "appfabric:DeleteIngestion",
                "appfabric:DeleteIngestionDestination"
            ],
            "Resource": ["arn:aws:appfabric:*:*:appbundle/*"]
        }
    ]
}
```

AppFabric 有关生产力 IAM 策略示例

提高 AWS AppFabric 工作效率功能处于预览阶段，可能会发生变化。

以下策略示例适用于提高工作效率 AppFabric 的功能。

允许以只读方式访问生产力功能

以下策略示例授予生产力功能 AppFabric 的只读访问权限。

> **Important**
>
> 在 IAM 控制台的 JSON 策略编辑器中添加此策略时，您可能会看到一个无效操作错误。这是因为提高生产 AppFabric 力的功能目前处于预览状态。您应该忽略该错误，并继续创建策略。

允许完全访问生产力功能

以下策略示例授予对提高生产力功能 AppFabric 的完全访问权限。

> **Important**
>
> 在 IAM 控制台的 JSON 策略编辑器中添加此策略时，您可能会看到一个无效操作错误。这是因为提高生产 AppFabric 力的功能目前处于预览状态。您应该忽略该错误，并继续创建策略。

允许访问创建 AppClients

以下策略示例授予创建权限 AppClients。有关更多信息，请参阅为提高生产力 AppFabric 而创建 AppClient。

> **Important**
>
> 在 IAM 控制台的 JSON 策略编辑器中添加此策略时，您可能会看到一个无效操作错误。这是因为提高生产 AppFabric 力的功能目前处于预览状态。您应该忽略该错误，并继续创建策略。

允许访问以获取以下详细信息 AppClients

以下策略示例授予访问权限以获取的详细信息 AppClients。有关更多信息，请参阅获取的详细信息 AppClient。

> **Important**
>
> 在 IAM 控制台的 JSON 策略编辑器中添加此策略时，您可能会看到一个无效操作错误。这是因为提高生产 AppFabric 力的功能目前处于预览状态。您应该忽略该错误，并继续创建策略。

允许访问列表 AppClients

以下策略示例授予对列表的访问权限 AppClients。有关更多信息，请参阅获取的详细信息 AppClient。

> **Important**
>
> 在 IAM 控制台的 JSON 策略编辑器中添加此策略时，您可能会看到一个无效操作错误。这是因为提高生产 AppFabric 力的功能目前处于预览状态。您应该忽略该错误，并继续创建策略。

允许访问更新 AppClients

以下策略示例授予更新权限 AppClients。有关更多信息，请参阅更新 AppClient。

> **Important**
>
> 在 IAM 控制台的 JSON 策略编辑器中添加此策略时，您可能会看到一个无效操作错误。这是因为提高生产 AppFabric 力的功能目前处于预览状态。您应该忽略该错误，并继续创建策略。

允许访问删除 AppClients

以下策略示例授予删除权限 AppClients。有关更多信息，请参阅更新 AppClient。

> **Important**
>
> 在 IAM 控制台的 JSON 策略编辑器中添加此策略时，您可能会看到一个无效操作错误。这是因为提高生产 AppFabric 力的功能目前处于预览状态。您应该忽略该错误，并继续创建策略。

允许访问以授权应用程序

以下策略示例使用令牌 API 授予访问权限，以对应用程序进行授权。有关更多信息，请参阅对您的应用程序进行身份验证和授权。

> **Important**
>
> 在 IAM 控制台的 JSON 策略编辑器中添加此策略时，您可能会看到一个无效操作错误。这是因为提高生产 AppFabric 力的功能目前处于预览状态。您应该忽略该错误，并继续创建策略。

其他 IAM 策略示例

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
```

```
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

将服务相关角色用于 AppFabric

AWS AppFabric 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 IAM 角色的独特类型。 AppFabric服务相关角色由服务预定义 AppFabric ，包括该服务代表您呼叫他人 AWS 服务 所需的所有权限。

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

只有在首先删除相关资源后，您才能删除服务关联角色。这样可以保护您的 AppFabric 资源，因为您不能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 IAM 配合使用的AWS 服务，并在服务相关角色列中查找标有 “是” 的服务。选择是和链接，查看该服务的服务关联角色文档。

的服务相关角色权限 AppFabric

AppFabric 使用名为的服务相关角色 `AWSServiceRoleForAppFabric` — AppFabric 允许将数据放入接收目标资源，例如 Amazon S3 存储桶或 Amazon Data Firehose 传输流。它还 AppFabric 允许将 CloudWatch 指标数据放在`AWS/AppFabric`命名空间中。

AWSServiceRoleForAppFabric 服务相关角色信任以下服务代入该角色：

- appfabric.amazonaws.com

名为的角色权限策略AWSAppFabricServiceRolePolicy AppFabric 允许对指定资源完成以下操作：

- 操作：AWS/AppFabric 命名空间中的 cloudwatch:PutMetricData。此操作允许将指标数据放 AppFabric 入 Amazon CloudWatch AWS/AppFabric 命名空间。有关中可用 AppFabric 指标的更多信息 CloudWatch，请参阅AWS AppFabric 使用 Amazon 进行监控 CloudWatch。
- 操作：Amazon S3 存储桶中的 s3:PutObject。此操作允许将提取的数据放入您指定的 Amazon S3 存储桶。 AppFabric
- 操作：firehose:PutRecordBatch在 Amazon Data Firehose 传送流中。此操作允许将提取的数据放 AppFabric 入您指定的 Amazon Data Firehose 传输流中。

有关更多信息，请参阅适用于 AppFabric 的AWS 托管策略。

您必须配置使用户、组或角色能够创建、编辑或删除服务相关角色的权限。有关更多信息，请参阅《IAM 用户指南》中的服务相关角色权限。

为创建服务相关角色 AppFabric

您无需手动创建服务关联角色。当您在 AWS 管理控制台、或 AWS API 中创建 AppFabric 应用程序包时， AppFabric 会为您创建服务相关角色。 AWS CLI

编辑的服务相关角色 AppFabric

AppFabric 不允许您编辑AWSServiceRoleForAppFabric服务相关角色。在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。不过，您可以使用 IAM 编辑角色的说明。有关更多信息，请参阅《IAM 用户指南》中的编辑服务关联角色。

删除的服务相关角色 AppFabric

如果不再需要使用某个需要服务关联角色的功能或服务，我们建议您删除该角色。这样就没有未被主动监控或维护的未使用实体。但是，必须先删除所有 AppFabric 应用程序捆绑包，然后才能删除服务相关角色。

清除服务相关角色

必须先删除服务相关角色使用的所有资源，然后才能使用 IAM 删除该角色。角色使用您在中创建 AppFabric 的应用程序捆绑包。有关更多信息，请参阅 AWS AppFabric 为安全资源删除。

> **Note**
>
> 如果您尝试删除资源时 AppFabric 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。

手动删除 服务相关角色

使用 IAM 控制台 AWS CLI、或 AWS API 删除`AWSServiceRoleForAppFabric`服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的删除服务关联角色。

AppFabric 服务相关角色支持的区域

AppFabric 支持在所有提供服务 AWS 区域 的地方使用服务相关角色。有关更多信息，请参阅 AWS 一般参考 中的 AppFabric 端点和配额。

AWS 的托管策略 AWS AppFabric

要向用户、群组和角色添加权限，使用 AWS 托管策略比自己编写策略要容易得多。创建仅为团队提供所需权限的 IAM 客户管理型策略需要时间和专业知识。要快速入门，您可以使用我们的 AWS 托管策略。这些策略涵盖常见使用案例，可在您的 AWS 账户中使用。有关 AWS 托管策略的更多信息，请参阅 IAM 用户指南中的AWS 托管策略。

AWS 服务 维护和更新 AWS 托管策略。您无法更改 AWS 托管策略中的权限。服务偶尔会向 AWS 托管式策略添加额外权限以支持新特征。此类更新会影响附加策略的所有身份（用户、组和角色）。当启动新特征或新操作可用时，服务最有可能会更新 AWS 托管式策略。服务不会从 AWS 托管策略中移除权限，因此策略更新不会破坏您的现有权限。

此外，还 AWS 支持跨多个服务的工作职能的托管策略。例如，ReadOnlyAccess AWS 托管策略提供对所有资源 AWS 服务 和资源的只读访问权限。当服务启动一项新功能时， AWS 会为新操作和资源添加只读权限。有关工作职能策略的列表和说明，请参阅 IAM 用户指南中的适用于工作职能的AWS 托管式策略。

AWS 托管策略：AWSAppFabricReadOnlyAccess

您可以将 AWSAppFabricReadOnlyAccess 策略附加到 IAM 身份。此策略向 AppFabric 服务授予只读权限。

> **Note**
>
> 该AWSAppFabricReadOnlyAccess策略不授予生产力功能 AppFabric 的只读访问权限。

权限详细信息

该策略包含以下权限：

- appfabric – 授予获取应用捆绑包、列出应用捆绑包、获取应用授权、列出应用授权、获取摄取、列出摄取、获取摄取目标、列出摄取目标和列出资源标签的权限。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "appfabric:GetAppAuthorization",
                "appfabric:GetAppBundle",
                "appfabric:GetIngestion",
                "appfabric:GetIngestionDestination",
                "appfabric:ListAppAuthorizations",
                "appfabric:ListAppBundles",
                "appfabric:ListIngestionDestinations",
                "appfabric:ListIngestions",
                "appfabric:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 托管策略：AWSAppFabricFullAccess

您可以将 AWSAppFabricFullAccess 策略附加到 IAM 身份。此策略向 AppFabric 服务授予管理权限。

> **Important**
>
> 该AWSAppFabricFullAccess政策不授予 AppFabric 对提高生产力功能的访问权限，因为这些功能目前处于预览状态。有关授予生产力功能访问权限的 AppFabric 更多信息，请参阅AppFabric 有关生产力 IAM 策略示例。

权限详细信息

该策略包含以下权限：

- appfabric— 向授予完全管理权限 AppFabric。
- kms – 授予列出别名的权限。
- s3 – 授予列出所有的 Amazon S3 存储桶和获取存储桶位置的权限。
- firehose— 授予列出 Amazon Data Firehose 传输流和描述传输流的权限。
- iam— 授予为创建AWSServiceRoleForAppFabric服务相关角色的 AppFabric权限。有关更多信息，请参阅 将服务相关角色用于 AppFabric。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["appfabric:*"],
            "Resource": "*"
        },
        {
            "Sid": "KMSListAccess",
            "Effect": "Allow",
            "Action": ["kms:ListAliases"],
            "Resource": "*"
```

```
        },
        {
            "Sid": "S3ReadAccess",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*"
        },
        {
            "Sid": "FirehoseReadAccess",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "firehose:ListDeliveryStreams"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowUseOfServiceLinkedRole",
            "Effect": "Allow",
            "Action": ["iam:CreateServiceLinkedRole"],
            "Condition": {
                "StringEquals": {"iam:AWSServiceName": "appfabric.amazonaws.com"}
            },
            "Resource": "arn:aws:iam::*:role/aws-service-role/
appfabric.amazonaws.com/AWSServiceRoleForAppFabric"
        }
    ]
}
```

AWS 托管策略：AWSAppFabricServiceRolePolicy

无法将 AWSAppFabricServiceRolePolicy 策略附加到 IAM 实体。此策略附加到允许代表您执行操作 AppFabric 的服务相关角色。有关更多信息，请参阅 将服务相关角色用于 AppFabric。

权限详细信息

该策略包含以下权限：

- `cloudwatch`— 授予将指标数据放 AppFabric 入 Amazon CloudWatch `AWS/AppFabric` 命名空间的权限。有关中可用 AppFabric 指标的更多信息 CloudWatch，请参阅AWS AppFabric 使用 Amazon 进行监控 CloudWatch。
- `s3`— 授予 AppFabric 将提取的数据放入您指定的 Amazon S3 存储桶的权限。
- `firehose`— 授予将提取的数据放 AppFabric 入您指定的 Amazon Data Firehose 传输流的权限。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CloudWatchEmitMetric",
            "Effect": "Allow",
            "Action": ["cloudwatch:PutMetricData"],
            "Resource": "*",
            "Condition": {
                "StringEquals": {"cloudwatch:namespace": "AWS/AppFabric"}
            }
        },
        {
            "Sid": "S3PutObject",
            "Effect": "Allow",
            "Action": ["s3:PutObject"],
            "Resource": "arn:aws:s3:::*/AWSAppFabric/*",
            "Condition": {
                "StringEquals": {"s3:ResourceAccount": "${aws:PrincipalAccount}"}
            }
        },
        {
            "Sid": "FirehosePutRecord",
            "Effect": "Allow",
            "Action": ["firehose:PutRecordBatch"],
            "Resource": "arn:aws:firehose:*:*:deliverystream/*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/AWSAppFabricManaged":
 "true"}
            }
        }
    ]
```

```
}
```

AppFabric AWS 托管策略的更新

查看 AppFabric 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。有关此页面更改的自动提示，请订阅AppFabric 文档历史记录页面上的 RSS 信息源。

更改	描述	日期
AWSAppFabricReadOnlyAccess - 新策略	AppFabric 添加了向 AppFabric 服务授予只读权限的新策略。	2023 年 6 月 27 日
AWSAppFabricFullAccess：新策略	AppFabric 添加了向 AppFabric 服务授予管理权限的新策略。	2023 年 6 月 27 日
AWSAppFabricServiceRolePolicy：新策略	AppFabric 为`AWSServiceRoleForAppFabric` 服务相关角色添加了新策略。	2023 年 6 月 27 日
AppFabric 已开始跟踪更改	AppFabric 开始跟踪其 AWS 托管策略的更改。	2023 年 6 月 27 日

对 AWS AppFabric 身份和访问进行故障排除

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

主题

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

我无权在以下位置执行操作 AppFabric

如果您收到错误提示，指明您无权执行某个操作，则必须更新策略以允许执行该操作。

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

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

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 appfabric:*GetWidget* 操作访问 *my-example-widget* 资源。

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。

我无权执行 iam:PassRole

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

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

当名为 marymajor 的 IAM 用户尝试使用控制台在 AppFabric 中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

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

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

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人 AWS 账户 访问我的 AppFabric 资源

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

要了解更多信息，请参阅以下内容：

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

- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（身份联合验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

合规性验证 AWS AppFabric

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

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

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。有关您在使用时的合规责任的更多信息 AWS 服务，请参阅AWS 安全文档。

以下方面的安全最佳实践 AWS AppFabric

AWS AppFabric 提供了多种安全功能，供您在制定和实施自己的安全策略时考虑。以下最佳实操是一般准则，并不代表完整的安全解决方案。这些最佳实操可能不适合您的环境或不满足您的环境要求，请将其视为有用的考虑因素而不是惯例。

无需管理员访问权限即可监控应用程序

只要拥有只读 AWS Identity and Access Management (IAM) 权限，任何人都可以 AppFabric 与 Amazon Quick 以及其他安全信息和事件管理 (SIEM) 工具集成，例如Splunk。为了监控应用程序安全，将数据传输到亚马逊简单存储服务 (Amazon S3) 存储桶或亚马逊数据 Firehose 传输流。

监视 AppFabric 事件

您可以 AppFabric 使用 Amazon CloudWatch 指标进行监控。 CloudWatch 从 AppFabric 每分钟收集数据并将其处理为指标。您可以设置警报，以便在指标符合指定阈值时发出通知。有关更多信息，请参阅 AWS AppFabric 使用 Amazon 进行监控 CloudWatch。

韧性在 AWS AppFabric

AWS 全球基础设施是围绕 AWS 区域 可用区构建的。 AWS 区域 提供多个物理分隔和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络连接。利用可用区，您可以设计和操作在可用区之

间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错能力和可扩展性。

有关 AWS 区域 和可用区的更多信息，请参阅AWS 全球基础设施。

中的基础设施安全 AWS AppFabric

作为一项托管服务， AWS AppFabric 受到《Amazon Web Services：安全流程概述》白皮书中描述的 AWS 全球网络安全程序的保护。

您可以使用 AWS 已发布的 API 调用 AppFabric 通过网络进行访问。客户端必须支持 TLS 1.0 或更高版本。建议使用 TLS 1.2 或更高版本。客户端还必须支持具有完全向前保密 (PFS) 的密码套件，例如 DHE (Ephemeral Diffie-Hellman) 或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 主体关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS STS）生成临时安全凭证来对请求进行签名。

中的配置和漏洞分析 AWS AppFabric

配置和 IT 控制由您（我们的客户）共同 AWS 负责。有关更多信息，请参阅责任 AWS 共担模型。

监控 AWS AppFabric

监控是维护和其他 AWS 解决方案的可靠性、可用性和性能的重要组成部分。 AWS AppFabric AWS 提供以下监控工具 AppFabric，供您监视、报告问题并在适当时自动采取措施：

- Amazon 会实时 CloudWatch监控您的 AWS 资源和您运行 AWS 的应用程序。您可以收集和跟踪指标，创建自定义的控制面板，以及设置警报以在指定的指标达到您指定的阈值时通知您或采取措施。例如，您可以 CloudWatch 跟踪您的 Amazon EC2 实例的 CPU 使用率或其他指标，并在需要时自动启动新实例。有关更多信息，请参阅 Amazon CloudWatch 用户指南。
- Amazon Lo CloudWatch gs 使您能够监控、存储和访问来自亚马逊 EC2 实例和其他来源的日志文件。 AWS CloudTrail CloudWatch 日志可以监视日志文件中的信息，并在达到特定阈值时通知您。您还可以在高持久性存储中检索您的日志数据。有关更多信息，请参阅 Amazon CloudWatch 日志用户指南。
- AWS CloudTrail捕获由您或代表您发起的 API 调用和相关事件， 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。有关更多信息，请参阅 AWS CloudTrail 《用户指南》。

AWS AppFabric 使用 Amazon 进行监控 CloudWatch

您可以使用 AWS AppFabric 进行监控 CloudWatch，它收集原始数据并将其处理为可读的近乎实时的指标。这些统计数据会保存 15 个月，从而使您能够访问历史信息，并能够更好地了解您的 Web 应用程序或服务的执行情况。此外，可以设置用于监测特定阈值的警报，并在达到相应阈值时发送通知或执行操作。有关更多信息，请参阅 Amazon CloudWatch 用户指南。

该 AppFabric 服务在`AWS/AppFabric`命名空间中报告以下指标。

指标	说明
AppFabric 应用程序授权状态	应用程序授权的状态（`1`针对已连接；`0`对于任何其他授权）。
AppFabric 数据传输延迟	从 SaaS 应用程序收集审计日志并将其传送 AppFabric 到配置的目标（Amazon S3 或 Amazon Data Firehose）所花费的时间（以秒为单位）。

指标	说明
提取目标状态	摄取目标状态（1 表示“活动”；0 表示“其他”）。
总体数据延迟	事件在 SaaS 应用程序上发生的时间与将相应的审计日志传送到配置的目标（Amazon S3 或 Amazon Data Firehose）的时间之间的时间差（以秒为单位）。 AppFabric
摄取数据量	传输到亚马逊简单存储服务 (Amazon S3) 或亚马逊 Data Firehose 的数据的大小。

AppFabric 指标支持以下维度。

维度	说明
提取目标 Arn	摄取目标的 Amazon 资源名称（ARN）。

使用记录 AWS AppFabric API 调用 AWS CloudTrail

AWS AppFabric 与 AWS CloudTrail一项服务集成，该服务提供用户、角色或角色所执行操作 AWS 服务 的记录 AppFabric。 CloudTrail 将所有 API 调用捕获 AppFabric 为事件。捕获的调用包括来自 AppFabric 控制台的调用和对 AppFabric 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 AppFabric。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 AppFabric、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。

有关的更多信息 CloudTrail，请参阅《AWS CloudTrail 用户指南》。

AppFabric 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 AppFabric，该活动会与其他 CloudTrail 事件一起记录在 AWS 服务 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AWS CloudTrail 用户指南中的使用 CloudTrail 事件历史记录查看事件。

要持续记录您的 AWS 账户事件（包括的事件） AppFabric，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。默认情况下，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《AWS CloudTrail 用户指南》中的以下主题：

- 创建跟踪记录概述
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个区域的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail 日志文件

所有 AppFabric 操作均由《API 参考》记录 CloudTrail 并记录在《AWS AppFabric API 参考》中。例如，对`CreateAppBundle`、`UpdateAppBundle`和`GetAppBundle`操作的调用会在 CloudTrail 日志文件中生成条目。

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

- 请求是使用根证书还是 AWS Identity and Access Management (IAM) 用户凭证发出。
- 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《AWS CloudTrail 用户指南》中的CloudTrail userIdentity元素。

了解 AppFabric 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顺序出现。

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:SampleUser",
        "arn": "arn:aws:sts::111122223333:assumed-role/AssumedRole/SampleUser",
```

```
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAXUFER33B4FVC2GCYR",
                "arn": "arn:aws:iam::111122223333:role/AssumedRole",
                "accountId": "111122223333",
                "userName": "SampleUser"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-05-31T21:11:15Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-05-31T21:22:16Z",
    "eventSource": "appfabric.amazonaws.com",
    "eventName": "CreateAppBundle",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "3.90.81.91",
    "userAgent": "Coral/Apache-HttpClient5",
    "requestParameters": {
        "clientToken": "64d9069f-e565-49a4-9374-6dc8631142e2"
    },
    "responseElements": {
        "appBundle": {
            "arn": "arn:aws:appfabric:us-
east-1:111122223333:appbundle/6aa92da0-5eeb-4ff4-aabf-4db7fd022ad1",
            "idpClientConfiguration": {
                "samlAudience": "urn:amazon:cognito:sp:us-east-1_GEdGiavzr",
                "samlRedirect": "https://6aa92da0-5eeb-4ff4-aabf-4db7fd022ad1.auth.us-
east-1.amazoncognito.com/saml2/idpresponse",
                "oidcRedirect": "https://6aa92da0-5eeb-4ff4-aabf-4db7fd022ad1.auth.us-
east-1.amazoncognito.com/oauth2/idpresponse"
            }
        }
    },
    "requestID": "17e15a5d-8c66-46c7-ad5b-f521004fa9c2",
    "eventID": "ba1dd847-86f6-4386-85be-0398e844a358",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
```

```
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
    "tlsDetails": {
        "clientProvidedHostHeader": "frontend.fabric.us-east-1.amazonaws.com"
    }
}
```

的配额 AppFabric

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。您可以请求增加某些配额，但其他一些配额无法增加。

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

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

下表显示了与 AWS 账户 之相关的配额。 AppFabric

Name	默认值	可调整	说明
应用程序捆绑包	每个受支持的区域：1 个	否	您可以在当前 AWS 区域的账户中创建的最大应用程序捆绑包数量。
应用程序授权	每个受支持的区域：50 个	否	您在当前 AWS 区域的账户中可以创建的最大应用程序授权数量。
提取	每个受支持的区域：50 个	否	你可以在当前 AWS 区域的账户中创建的最大摄取次数。
提取目标	每个受支持的区域：5 个	否	当前 AWS 区域中单个账户每次提取可以创建的最大提取目标数。
AppClient	每个受支持的区域：1 个	否	你可以在当前 AWS 区域 AppClients 的账户中创建的最大数量。

Name	默认值	可调整	说明
			“ AWS AppFabric 提高生产力” 功能处于预览阶段，可能会发生变化。

《 AppFabric 管理指南》的文档历史记录

下表描述了的文档版本 AWS AppFabric。

变更	说明	日期
支持的新应用程序	JumpCloud作为支持的应用程序添加。有关更多信息，请参阅中支持的应用程序 AWS AppFabric。	2024 年 6 月 5 日
新的支持应用程序和安全工具	已添加Azure Monitor和Google Analytics作为支持的应用程序。有关更多信息，请参阅中支持的应用程序 AWS AppFabric。Singularity Cloud作为支持的安全工具添加。有关更多信息，请参阅兼容的安全工具。	2024 年 4 月 30 日
支持的新应用程序	SentinelOne作为支持的应用程序添加。有关更多信息，请参阅中支持的应用程序 AWS AppFabric。	2024 年 4 月 25 日
支持的新应用程序	1Password作为支持的应用程序添加。有关更多信息，请参阅中支持的应用程序 AWS AppFabric。	2024 年 4 月 23 日
支持的新安全工具	Dynatrace作为兼容的安全工具添加。有关更多信息，请参阅兼容的安全工具。	2024 年 3 月 26 日
新指标	添加了 AppFabric 应用程序授权状态指标。有关更多信息，请参阅AWS AppFabric 使用	2024 年 3 月 8 日

	Amazon CloudWatch 日志进行监控。	
支持的新应用程序	IBM Security® Verify作为支持的应用程序添加。有关更多信息，请参阅中支持的应用程序 AWS AppFabric。	2024 年 3 月 6 日
支持的新应用程序	Box作为支持的应用程序添加。有关更多信息，请参阅中支持的应用程序 AWS AppFabric。	2024 年 2 月 28 日
新支持的应用程序和指标	添加了Cisco DuoSalesforce、和Terraform Cloud作为支持的应用程序。有关它们的更多信息，请参阅中支持的应用程序 AWS AppFabric。添加了 AppFabric 数据传输延迟和总体数据延迟指标。有关更多信息，请参阅AWS AppFabric使用 Amazon CloudWatch 日志进行监控。	2024 年 2 月 1 日
添加了 Atlassian Confluence、Genesys Cloud、Hub Spot、OneLogin by One Identity、PagerDuty 和 Ping Identity 作为支持的应用程序，添加了 Barracuda XDR 作为兼容的安全工具	有关新支持应用程序的更多信息，请参阅中支持的应用程序 AWS AppFabric和兼容的安全工具。	2023 年 12 月 15 日
添加了 Atlassian Confluence、Genesys Cloud、Hub Spot、OneLogin by One Identity、PagerDuty 和 Ping Identity 作为支持的应用程序，添加了 Barracuda XDR 作为兼容的安全工具	有关新支持应用程序的更多信息，请参阅中支持的应用程序 AWS AppFabric和兼容的安全工具。	2023 年 12 月 15 日

添加了提高工作效率 AWS AppFabric 的预览文档	有关生产力的 AppFabric 更多信息，AWS AppFabric 请参阅什么是生产力？	2023 年 11 月 27 日
添加了 GitHub 和 ServiceNow 作为支持的应用程序	有关新支持的应用程序的更多信息，请参阅支持的应用程序。	2023 年 10 月 31 日
已开始跟踪的 AWS 托管策略 AWS AppFabric	有关 AWS 托管策略的更多信息 AppFabric，请参阅的AWS 托管策略 AWS AppFabric。	2023 年 6 月 27 日
初始版本	《 AWS AppFabric 管理指南》的初始版本。	2023 年 6 月 27 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。