aws

用户指南

AWS 数据传输终端

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS 数据传输终端: 用户指南

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

什么是数据传输终端？

AWS 数据传输终端是一个网络就绪的物理位置，您可以将数据存储设备带到这里，以将数据快速传入和传出 AWS Cloud 服务。上传远程采集的数据，使访问这些数据变得更轻松。

通过 AWS 管理控制台在我们的物理数据传输终端设施之一安排预留，在安排的时间到达，然后使用自己的设备将数据上传到您的 AWS Cloud 云服务。完成安排的预留并离开后，该设施将重新获得安保，并为安排的下一次预留做好准备。

> **Note**
>
> AWS 数据传输终端目前仅适用于 AWS Enterprise 客户。

访问数据传输终端：

- AWS 数据传输终端控制台：https://console.aws.amazon.com/datatransferterminal
- 数据传输终端设施：数据传输终端设施的位置将在控制台进行预留立即后提供。有关更多信息，请参阅进行数据传输。

特征

使用 AWS 数据传输终端，可以更轻松地将数据从远程位置传输到 AWS Cloud 服务。以下是数据传输终端在满足远程数据上传需求方面的一些优势：

安全、私密、专属

每个数据传输终端设施都是一个安全、私密的场所，可供您通过快速网络连接在数据存储设备与 AWS 服务之间进行大型数据传输。

专用预留控制台

将经批准的人员添加到您的传输团队，并使用 AWS 数据传输终端控制台安排数据传输终端预留。

光纤网络连接

每个数据传输终端设施包含两个 100 千兆位（Gbps）光纤（LR4）连接，可实现快速数据上传和冗余。

控制数据存储设备

无需运送 Snowball 设备和等待数据上传到 AWS Cloud 服务。您可以在整个数据传输过程中控制物理数据存储设备，从而更快地将数据传输到需要的位置。

重要概念

使用 AWS 数据传输终端需要流程负责人安排预留，以使数据传输专家能够访问数据传输终端设施。请参阅以下各节，了解有关数据传输终端术语的更多信息。

主题

传输团队

传输团队是由 AWS 账户拥有者确定的一组人员，可以选择他们代表您的组织进行数据传输。组建传输团队包括为传输团队命名和指定该团队的人员。建议单次预留的数据传输专家团队不超过四人。

有关更多信息，请参阅安排数据传输终端预留。

人员

人员是指可以进行预留和管理预留，或者可以前往和使用数据传输终端设施的个人。人员可以是流程负责人或数据传输专家，或者两者兼而有之。

流程负责人

- 流程负责人是 AWS 账户所有者，可以在其 AWS 数据传输终端账户中添加、编辑和删除人员。

数据传输专家

- 数据传输专家是可以前往数据传输终端设施进行数据上传事务的人员。这些人员必须获得流程负责人的授权，并添加到您的 AWS 数据传输终端账户。访问数据传输终端设施时，需要出示政府颁发的身份证件。

设施

数据传输终端设施是由一个或多个服务提供商共同拥有和管理的数据中心。每个设施都要求数据传输终端数据传输专家提供政府颁发的身份证明，该证明必须匹配其预留记录才能访问数据传输终端套房。

时间安排注意事项

您可以在数据传输终端控制台中进行时长为一至六小时的预留，预留时间为一周中的任何一天，全年无休。单次预留可以连续安排，但两次预留之间需至少间隔一小时。所有预留必须至少提前 24 小时进行。

进行数据传输所需的时间会有所不同，具体视上传性能速度而定。计划和安排数据传输终端预留时，请考虑以下影响上传性能的因素。

设备

- 某些设备可能包含影响上传性能的设置。请参阅设备规格以了解建议的上传性能速度。

网络状况

- 网络流量过大的时段会影响数据上传速度，因此选择数据传输会话时间时应考虑这一点。将数据传输会话安排在非高峰时段或网络活动较少的时段可提高上传速度。

数据传输大小

- 数据传输终端网络连接专为大型数据传输而设计。但是，所传输数据的大小将影响会话所需的时间。

使用案例

虽然任何 AWS Enterprise 客户都可以访问数据传输终端系统，但某些使用案例场景可能会从中获益更多。

自动驾驶和高级驾驶辅助系统（AD/ADAS）：汽车原始设备制造商（OEM）和供应商通过其在北美、欧洲和东盟的许多大都市运营和收集数据的自动驾驶汽车车队生成大量数据集。借助数据传输终端，这些车队车辆收集的数据可以上传到 AWS Cloud 服务中，并用于训练 AD/ADAS 模型。

媒体和娱乐：影视制作公司和其他内容创作者经常在远程地点生成数字视频和音频（AV）文件。及时将这些 AV 文件上传到云上非常重要，这样分散在各地的制作和编辑团队就可以并行、实时地开始工作流程。通过使用数据传输终端远程上传数据，可以缩短制作时间，从而降低制作成本。

地图、摄影测量和 3D 图像：使用制图或影像应用程序的组织在远程地点收集数据，并需要将这些可视化文件上传到 AWS Cloud 进行分析或训练。数据传输终端最大限度地缩短了从收集到分析这些大型数据集之间的时间，这有助于为驾驶员、农民和其他信息用户提供最新的地理空间数据。

相关服务

以下 AWS 服务在使用数据传输终端时可提供最佳体验。

AWS 服务	描述
AWS Snowball Edge	AWS 数据传输终端是对 Snowball 产品的补充，它提供了一个可以更快上传到 AWS 云的位置，从而最大限度地减少了访问数据的等待时间。
Amazon S3 ()	将您自己的设备带到数据传输终端，以便快速安全地将数据上传到 Amazon S3 服务。

使用数据传输终端的技术要求

在数据传输终端安排预留之前，您需要确保拥有连接网络所需的设备和配置。要获得最佳网络连接和体验，请参阅以下指南。

设备

您必须携带用于连接的便携式设备（包括显示器、键盘、鼠标、计算机或笔记本电脑）前往数据传输终端设施进行安排的预留。

您的硬件必须能够支持光纤（L4）连接

> **Note**
>
> 作为数据安全最佳实践，请确保您带到数据传输终端的存储设备上的数据已经过加密并受到保护，且在使用数据传输终端设施时应用数据加密策略。有关更多信息，请参阅 AWS 数据传输终端安全性

网络要求

确保您的上传设备、服务器或装置（笔记本电脑）已准备好连接到网络并支持 DHCP。您应具备以下条件才能获得最佳数据上传体验：

- 100G QSFP28 LR4（100GBASE-LR4）光学 QSFP 收发器，与数据传输终端设施中提供的用于光纤电缆连接的 NIC 和 LC 连接器兼容。
- 启用 IP 地址自动配置 DHCP。DNS 服务器将通过 DHCP 自动分配。
- 最新的软件和 NIC 驱动程序。

性能优化

要在使用 AWS 数据传输终端时最大限度地提高吞吐量，请考虑以下建议。

- 推荐的硬件：
  - 100Gbps 网络接口卡
  - 16 核 CPU

  - 128 GB RAM
  - RAID 阵列中有多个 NVME SSD 驱动器
- 使用 AWS 通用运行时系统 (AWS CRT) 库通过 AWS 命令行界面或 AWS SDK 进行上传。

  通过配置以下参数优化 Amazon S3 传输设置。在 AWS 配置文件（默认位置 `~/.aws/config`）中的顶层 `s3` 键下设置这些值。

```
[default]
s3 =
    preferred_transfer_client = crt
    target_bandwidth = 100Gb/s
    max_concurrent_requests = 20
    multipart_chunksize = 16MB
```

  请注意，所有 Amazon S3 配置值都会在顶层 `s3` 键下缩进并嵌套。

  - 可选：您可以使用 `aws configure set` 命令以编程方式设置上述值。例如，要为默认配置文件设置上述值，可以改为运行以下命令：

```
aws configure set default.s3.preferred_transfer_client crt
aws configure set default.s3.target_bandwidth 100Gb/s
aws configure set default.s3.max_concurrent_requests 20
aws configure set default.s3.multipart_chunksize 16MB
```

- 要以编程方式为非默认配置文件设置这些值，请提供 `--profile` 标志。例如，要为名为 `test-profile` 的配置文件设置配置，请运行如下例所示的命令。

```
aws configure set s3.max_concurrent_requests 20 --profile test-profile
```

- 在设备上启用 BBR（Linux）以获得更好的吞吐量。

```
sysctl -w net.core.default_qdisc=fq
sysctl -w net.ipv4.tcp_congestion_control=bbr
```

更多信息

有关用于优化网络连接和性能的 AWS 命令行 Amazon S3 配置的更多信息，请参阅以下资源。

- 《AWS 命令参考》中的 AWS CLI Amazon S3 Configuration

- 《Amazon S3Amazon AppStream SDK for Java》中的 Use a performant Amazon S3 client: AWS CRT-based client
- AWS 知识中心 内的如何在使用 AWS CLI 向 Amazon S3 上传大文件时优化性能？

开始使用

通过在其中一个数据传输终端设施进行预留，即可开始向 AWS Cloud 服务进行远程数据传输。首先，需要数据传输终端设施支持的设备和 AWS Enterprise 账户。

在安排数据传输终端预留之前，请查看本指南的使用数据传输终端的技术要求部分，以确保设备具有数据传输的最佳配置。并非所有数据存储设备和网络连接设备都与套房中提供的光纤网络连接兼容。

在注册 AWS 时，将在 AWS 中为您的 AWS 账户自动注册所有服务，包括数据传输终端。您只需为使用的服务付费。

要设置数据传输终端，请使用以下各节中的步骤。

注册 AWS 并设置数据传输终端时，您可以选择在 AWS 管理控制台中更改显示语言。有关更多信息，请参阅《AWS 管理控制台入门指南》中的 Changing the language of the AWS Management Console。

拥有 AWS 账户后，您就可以访问数据传输终端。有关设置和使用 AWS 数据传输终端的更多信息，请参阅安排数据传输终端预留。

注册 AWS 账户

如果您还没有 AWS 账户，请完成以下步骤创建一个。

1. 打开 https://portal.aws.amazon.com/billing/signup。
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 AWS 账户时，系统会创建一个 AWS 账户根用户。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。

注册过程完成后，AWS 会向您发送一封确认电子邮件。在任何时候，您都可以通过转至 https://aws.amazon.com/ 并选择我的账户来查看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 AWS 账户后，保护您的 AWS 账户根用户，启用 AWS IAM Identity Center，并创建一个管理用户，以避免使用根用户执行日常任务。

1. 通过选择根用户并输入您的 AWS 账户电子邮件地址，以账户拥有者身份登录 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《IAM 用户指南》中的为 AWS 账户根用户启用虚拟 MFA 设备（控制台）。
3. 启用 IAM Identity Center。

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

   有关如何使用 IAM Identity Center 目录作为身份源的教程，请参阅《AWS IAM Identity Center 用户指南》中的 Configure user access with the default IAM Identity Center directory。
5. 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。

   要获取使用 IAM Identity Center 用户登录方面的帮助，请参阅《AWS 登录用户指南》中的 Signing in to the AWS access portal。
6. 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。
7. 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。

安排数据传输终端预留

要开始使用 AWS 数据传输终端，您需要拥有一个 AWS 账户并登录到数据传输终端控制台，网址为：https://console.aws.amazon.com/datatransferterminal。登录数据传输终端控制台后，您可以查看现有预留或进行新预留。要安排预留，您需要执行以下操作：

1. 创建传输团队。您需要创建一组指定的用户来创建预留，并访问数据传输终端设施以进行数据传输。要了解有关此主题的更多信息，请参阅创建传输团队。
2. 组建团队后，您需要为其添加人员。如需了解有关向传输团队添加人员的更多信息，请参阅添加人员。
3. 流程负责人可与账户中的团队一起安排数据传输。有关如何安排预留的更多信息，请参阅指定预留详细信息。
4. 在提交请求之前，请确保预留的详细信息正确无误。预留请求提交后，至少 24 小时内无法修改。有关更多信息，请参阅查看和确认预留。

处理并确认您的预留后，您的传输团队将能够在安排的时间访问数据传输终端设施。有关更多信息，请参阅在数据传输终端设施上进行数据传输。

创建传输团队

要访问数据传输终端设施，您需要在 AWS 管理控制台中安排预留。登录您的 AWS 账户以访问数据传输终端控制台，然后完成以下步骤以安排预留。

1. 在数据传输终端的主页上，选择开始使用按钮。
2. 如果您的账户中尚未组建传输团队，则创建预留按钮将被禁用。您需要创建并命名一个传输团队才能开始。
   a. 选择创建传输团队按钮。
   b. 为该团队命名。
      - 名称长度必须介于 2 到 64 个字符之间，以字母或数字开头。
      - 仅使用字母、数字、句点和短划线。特殊字符无法识别。
      - 请勿包含任何敏感的身份识别信息。
   c. 创建传输团队描述。
      - 提供有助于识别团队的描述，例如描述团队在特定时间段、活动或项目中的目的。
   d. 选择创建传输团队按钮。

您将返回到传输团队页面，并且新创建的团队将在传输团队部分下显示。

更新数据传输终端账户中的传输团队

要组建新的传输团队，请参阅本指南的安排数据传输终端预留章节。

要修改或移除传输团队，请执行以下操作：

1. 在传输团队页面上，选择要修改的传输团队。
2. 要修改传输团队的名称和描述，请选择编辑按钮。
3. 要添加或移除人员，请选择人员选项卡，然后完成本常见问题解答如何修改、添加或移除账户中的人员？部分中所述的步骤。
4. 要添加或取消所选传输团队的预留，请参阅本常见问题解答的更新数据传输终端账户中的人员章节。

添加人员

将流程负责人和数据传输专家添加到您的传输团队，以设置数据传输并访问数据传输终端设施。要将人员添加到传输团队，请执行以下操作：

1. 在传输团队页面上，从传输团队部分列出的内容中选择所需的传输团队卡片。将显示传输团队的摘要页面。
2. 选择人员选项卡，然后选择注册人员按钮，将人员添加到传输团队。
3. 在注册人员页面中填写要添加到传输团队的人员的必要信息字段。
   a. 人员别名：创建唯一的别名以识别该人员。
      - 别名用于识别人员，同时保护其身份。
      - 别名最多可包含 64 个字符，包含字母、数字和短划线。
      - 不允许使用特殊字符。
   b. 名字：提供该人员的名字，与其政府颁发身份证件上的名字相同。
   c. 姓氏：提供该人员在其政府颁发身份证件上显示的姓氏。
   d. 电子邮件地址：包含该人员的有效电子邮件地址，以接收预留信息和访问数据传输终端设施的说明。
4. 选择注册人员按钮，完成将该人员添加到传输团队。

更新数据传输终端账户中的人员

目前不支持在数据传输终端控制台中修改账户中的现有人员。AWS数据传输终端流程负责人目前只能添加或删除人员。

要从数据传输终端账户中移除人员，请执行以下操作：

1. 在传输团队页面上，选择与要移除的人员关联的传输团队。
2. 在所选传输团队的摘要页面上，选择人员选项卡。
3. 点击要移除的别名旁边的单选按钮。请注意，只有在删除人员的个人资料时，您才能看到其别名。
4. 选择删除按钮。将出现一条警告，确认对所选人员的预期操作。单击删除按钮继续。控制台顶部将出现一条横幅，确认该人员已成功删除。

指定预留详细信息

以下说明指导您如何在 AWS 管理控制台中安排数据传输终端预留。有关使用数据传输终端设施的信息，请参阅进行数据传输。

1. 在即将进行的预留选项卡中选择进行预留按钮。
2. 填写指定预留详细信息页面上的字段。
   a. 传输团队选择：首先显示默认选择的传输团队。如果想要选择其他团队，请单击下拉箭头从可用的传输团队列表中进行选择。
   b. 流程负责人：选择您希望负责管理预留的人员别名。
      - 一个预留只允许一个流程负责人，并且该负责人必须是您的 AWS 账户的授权人员。

        流程负责人也可以作为数据传输专家之一来执行数据传输活动。
   c. 数据传输专家：选择您想要其访问数据传输终端设施以完成数据传输活动的人员。您可以根据需要选择多名人员。
      - 最佳做法是将您的传输团队限制为不超过四（4）名数据传输专家。
   d. 数据传输终端信息：指定数据传输终端设施、所需的日期以及数据传输会话的具体时间。
      i. 数据传输终端设施：单击下拉箭头选择数据传输终端设施。

> **Note**
>
> 进行预留时仅提供设施描述。其他位置信息将在预留确认电子邮件中提供。

ii. 数据传输终端日期和时间：单击搜索预留的日期和时间字段，查看日历并安排预留。

- 必须至少提前 24 小时进行预留，且距离当前日期不得超过六（6）个月，预留时长最多只能为六（6）个小时。如有必要，单次预留可以跨越一天，以应对过夜的情况。
- 时间以 24 小时制表示，只能以整小时为增量进行预留。
- 要进行连续预留，您必须创建单独的预留，每个数据传输会话之间至少间隔一小时。
- 有关更多信息，请参阅时间安排注意事项。

3. 确认预留详细信息正确无误，然后选择创建按钮继续。这将带您进入确认页面，其中提供预留摘要。

查看和确认预留

指定预留详细信息后，选择下一步按钮继续查看概览页面。在查看并创建页面上查看数据传输终端预留请求的详细信息。

- 如果对请求感到满意，请选择创建按钮。
- 如果需要更改预留，请选择上一步按钮。

提交预留请求后，流程负责人将收到一封电子邮件，确认请求已收到并正在处理。请求获得批准后，将收到另一封电子邮件确认预留，并提供查找和访问数据传输终端设施的说明。有关访问数据传输终端设施的信息，请参阅进行数据传输。

更改您的预留

数据传输终端预留请求有 24 小时的处理期，在此期间无法进行任何更改。

处理期结束后，要查看、编辑或删除您的预留，请在控制台中导航至传输团队页面。

1. 在团队的卡片中找到并选择所需的预留。
2. 单击操作菜单并选择所需的操作。
   - 查看：选择查看选项可以查看预留的详细信息，包括日期、时间、地点和分配的人员。
   - 编辑：您可以修改预留的详细信息，包括日期、时间、地点和分配的人员。请注意，更改必须在所需预留日期前 24 小时进行，并且不会立即接受和应用这些修改。您的流程负责人将收到更新请求的确认。
   - 删除：删除选项可以取消预留。取消请求必须在安排的预留日期前至少 24 小时提出。请求获得批准后，流程负责人将收到取消预留的确认。

在数据传输终端设施上进行数据传输

数据传输终端是一个安全、共同拥有的场所，可以安全访问 AWS 网络。要访问数据传输终端设施，请确保您已收到包含位置描述和访问说明的确认电子邮件。有关访问和使用数据传输终端设施的更多信息，请参阅以下主题。

主题

携带物品

数据传输专家应携带执行数据传输所需的物品，例如笔记本电脑、闪存驱动器、固态硬盘 (SSD) 和 AWS Snowball Edge。确保您的设备已经过优化，可使用数据传输终端设施中的光纤网络电缆。有关最佳设备和配置的更多信息，请参阅使用数据传输终端的技术要求

您负责安装、使用和移除您和随行数据传输专家带入数据传输终端设施的设备和物品。带入套房的任何物品离开时都必须带走。AWS数据传输终端对遗忘或丢失的物品概不负责。

数据传输终端设施的实际地址

不提供数据传输终端设施的实际地址。相反，预留中指定的流程负责人和数据传输专家将收到一封电子邮件，其中包含数据传输终端设施的可搜索公共名称。AWS数据传输终端使用与 AWS Direct Connect 相同的位置识别系统，因此您可以在互联网上搜索公共名称以找到数据传输终端设施。如果您没有收到包含此信息的电子邮件，则请向 AWS 数据传输终端客户经理确认您已加入传输团队，并且您的电子邮件信息正确无误。

进入建筑物

要访问数据传输终端设施，每位数据传输专家都必须提供身份证明或政府颁发的身份证件。进入建筑物后，安保人员将护送您前往数据传输终端套房。

数据传输终端套房中预期的设备

每个数据传输终端设施只能配备两（2）根光纤电缆、一张桌子或书桌和几把椅子。如果房间中还有其他设备或物品，请立即向支持部门报告。

排查网络连接问题

如果您在使用 AWS 数据传输终端时遇到网络连接问题，例如无法连接互联网或连接速度慢，请考虑以下故障排除提示。

主题

设备连接问题

如果您在数据传输终端套房中难以建立物理连接，请考虑以下情况：

- 每个数据传输终端设施都有两（2）根单模 LC 光缆。如果缺少其中一根或两根电缆，则请立即联系 AWS Support。
- 如果一根光纤电缆无法正常工作，则请先尝试调换电缆的两端。如果仍然无法连接第一根电缆，则请尝试使用另一根电缆。

如果仍然无法使用电缆进行连接，请立即联系 AWS Support。

排除连接性问题

如果您能够连接设备但无法连接到网络，请尝试以下故障排除建议。

- 请确认设备配置符合指定的网络要求。有关更多信息，请参阅使用数据传输终端的技术要求
- 切换到另一根光纤电缆进行连接。
- 在保持光纤电缆连接的同时重启设备。
- 对设备执行基本网络诊断，确保满足以下要求：
  - DHCP 已启用
  - 已为连接的网络接口分配 IP 地址
  - DNS 服务器已配置
  - 系统时钟与 NTP 已同步

如果仍然无法连接，请联系 AWS Support，并根据您设备上运行的操作系统 (OS) 向其提供以下输出内容。

Linux/Unix

- 在终端或命令行界面（CLI）中获取 IP 地址和路由信息。验证网络接口是否已分配 IP 地址，以及路由表中是否已添加含有默认网关地址的默认路由。

```
ip address show
ip route show
```

  - 或者，如果设备上未安装 `iproute2` 且 `ip` 命令不可用，请使用以下命令：

```
ifconfig
netstat -rn
```

- 收集 DNS 服务器信息。此命令应显示两个以 `nameserver` 关键字开头的 IP 地址。

```
cat /etc/resolv.conf
```

- 收集基本连接测试的输出。将 `default_gateway_address` 替换为分配的默认网关的 IP 地址。

```
ping -c 5 <default_gateway_address>
ping -c 5 s3.amazonaws.com
traceroute s3.amazonaws.com
```

- 收集 HTTPS 连接测试的输出。以下命令应显示来自 Amazon S3 的 `HTTP 200 OK` 响应。

```
curl -i https://s3.amazonaws.com/ping
```

Windows

- 在命令提示符下获取 IP 地址、路由和 DNS 服务器信息。验证网络接口是否已分配 IP 地址、是否已分配两个 DNS 服务器，以及路由表中是否已添加含有默认网关地址的默认路由。

```
ipconfig /all
route print
```

- 在命令提示符下收集基本连接测试的输出。将 default_gateway_address 替换为分配的默认网关的 IP 地址。

```
ping <default_gateway_address>
ping s3.amazonaws.com
tracert s3.amazonaws.com
```

- 在 PowerShell 中收集 HTTPS 连接测试的输出。以下命令应显示 HTTP 200 OK 响应。

```
Invoke-WebRequest -Uri "https://s3.amazonaws.com/ping"
```

网络吞吐量

网络吞吐量衡量的是网络中的实际数据传输速率，可能受到多种因素的影响。以下因素可能会影响数据传输速度：

- 硬件：设备的硬件组件可能会导致上传数据时的连接速度降低。设备中使用的 CPU 和磁盘可能已达到其性能极限。考虑在 RAID 阵列中使用 NVME SSD。请务必使用 AWS CRT 库以获得更好的性能并降低 CPU 使用率。
- 加密开销：HTTPS 等安全传输会由于加密开销而增加处理时间。
- 延迟：延迟是指数据包从源传输到目标所需的时间。上传到不同地理区域的 Amazon S3 存储桶时，可能会出现高延迟，从而可能导致数据传输延迟和吞吐量降低。最佳实践是尽可能在同一区域内进行数据传输。
- 数据包丢失：丢失的数据包需要重新传输，这会减慢数据传输速度。

AWS 数据传输终端安全性

AWS 数据传输终端为将数据传入和传出 AWS Cloud 提供一个安全的环境。与任何其他物理网络光纤连接一样，数据传输终端连接不提供默认加密。因此，您将负责实施数据加密最佳实践，以确保数据传输安全。

AWS 的云安全性的优先级最高。为了满足对安全性最敏感的组织的需求，我们打造了具有超高安全性的数据中心和网络架构。作为 AWS 的客户，您也可以从这些数据中心和网络架构受益。

安全性是 AWS 和您的共同责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云的安全性 – AWS 负责保护在 AWS 云中运行 AWS 服务的基础架构。AWS 还向您提供可安全使用的服务。作为 AWS 合规性计划的一部分，第三方审核人员将定期测试和验证安全性的有效性。要了解适用于 AWS 数据传输终端的合规性计划，请参阅 AWS 按合规性计划提供的范围内服务。
- 云中的安全性：您的责任由您使用的 AWS 服务决定。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。

此文档可帮助您了解如何在使用数据传输终端时应用责任共担模式。以下主题将向您展示如何在使用数据传输终端服务时保护您的数据。您还将了解如何使用其他 AWS 服务来帮助您监控和保护数据传输终端资源。

主题

AWS 数据传输终端中的数据保护

AWS 责任共担模式将应用于 AWS 数据传输终端中的数据保护。如该模式中所述，AWS负责保护运行所有AWS云的全球基础设施。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 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 安全性博客上的 AWS Shared Responsibility Model and GDPR 博客文章。

出于数据保护目的，建议您保护 AWS 账户凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置单独的用户。这样，每个用户只获得履行其工作职责所需的权限。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。
- 使用 SSL/TLS 与 AWS 资源进行通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用 AWS CloudTrail 设置 API 和用户活动日志记录。有关使用 CloudTrail 跟踪来捕获 AWS 活动的信息，请参阅《AWS CloudTrail 用户指南》中的 Working with CloudTrail trails。
- 使用 AWS 加密解决方案以及 AWS 服务中的所有默认安全控制。
- 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。
- 如果在通过命令行界面或 API 访问 AWS 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）。这包括当您通过控制台、API、AWS CLI 或 AWS SDK 使用数据传输终端或其他 AWS 服务时。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。

数据加密

AWS 数据传输终端为您提供高速网络连接访问，以在自管理存储系统与 AWS 存储服务之间安全传输数据。存储数据在传输过程中如何加密部分取决于设备上启用的策略以及数据传输到的服务。数据管理和传输中的加密由使用数据传输终端的个人负责。

静态加密

AWS 数据传输终端会加密所有静态数据。

数据传输终端仅捕获预留所需的数据，包括指定参加和安排预留的个人的姓名和电子邮件地址。收集这些数据的目的是确认预留详细信息，并确保能够进入房间进行数据传输。这些事务信息的备份时间不超过 35 天，但 AWS 账户信息将保留 10 年。

传输中加密

AWS 数据传输终端不加密传输中数据。当您与数据传输终端 API 端点交互以在控制台中设置传输团队、添加人员和安排预留时，数据将在传输过程中加密。作为 AWS 责任共担模式的一部分，您可以选择通过数据传输终端连接到 AWS 服务的方式。强烈建议您选择使用强传输加密（例如 TLS 1.2 和 1.3）连接到 AWS 服务。

例如，通过在 Amazon S3 存储桶策略中使用 aws:SecureTransport 条件，仅使用通过 HTTPS (TLS) 进行加密的连接，如下面的存储桶策略中所示。

要了解有关使用其他 AWS 服务（如 Amazon S3）进行传输中数据加密的更多信息，请参阅《Amazon S3 用户指南》中的使用服务器端加密保护数据。

密钥管理

AWS 数据传输终端不直接支持客户自主管理型密钥。请使用您在数据传输终端预留期间连接的 AWS 服务提供的客户自主管理型密钥。在《AWS Key Management Service Developer Guide》https://docs.aws.amazon.com/kms/latest/developerguide/overview.html#customer-cmk#IMUpdateThresholdFromMap的 AWS KMS keys 章节中，了解有关客户自主管理型密钥以及如何加密静态数据的更多信息。

互联网络流量隐私

通过已发布的服务 API 访问数据传输终端控制台。数据传输终端资源独立于虚拟私有云（VPC）。

数据传输终端的身份和访问管理

AWS Identity and Access Management（IAM）是一项 AWS 服务，可帮助管理员安全地控制对 AWS 资源的访问。IAM 管理员控制谁可以通过身份验证（登录）和授权（具有权限）使用数据传输终端资源。IAM 是一项可以免费使用的 AWS 服务。

主题

受众

如何使用 AWS Identity and Access Management (IAM) 因在数据传输终端中执行的操作而异。

服务用户：如果您使用数据传输终端服务来完成工作，则您的管理员会为您提供所需的凭证和权限。随着您使用更多数据传输终端功能来完成工作，您可能需要额外的权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果无法访问数据传输终端中的功能，请参阅 AWS 数据传输终端身份和访问故障排除。

服务管理员 – 如果您在公司负责管理数据传输终端资源，您可能对数据传输终端具有完全访问权限。您有责任确定您的服务用户应访问哪些数据传输终端功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要了解有关您的公司如何将 IAM 与数据传输终端搭配使用的更多信息，请参阅数据传输终端如何与 IAM 配合使用。

IAM 管理员 – 如果您是 IAM 管理员，则可能需要了解如何编写策略以管理对数据传输终端的访问的详细信息。要查看可在 IAM 中使用的基于身份的数据传输终端策略示例，请参阅 AWS 数据传输终端基于身份的策略示例。

使用身份进行身份验证

身份验证是您使用身份凭证登录 AWS 的方法。您必须作为 AWS 账户根用户、IAM 用户或通过代入 IAM 角色进行身份验证（登录到 AWS）。

您可以使用通过身份源提供的凭证以联合身份登录到 AWS。AWSIAM Identity Center（IAM Identity Center）用户、您公司的单点登录身份验证以及您的 Google 或 Facebook 凭证都是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当您使用联合身份验证访问 AWS 时，您就是在间接代入角色。

根据您的用户类型，您可以登录 AWS 管理控制台或 AWS 访问门户。有关登录到 AWS 的更多信息，请参阅《AWS Sign-In 用户指南》中的如何登录到您的 AWS 账户。

如果您以编程方式访问 AWS，则 AWS 将提供软件开发工具包（SDK）和命令行界面（CLI），以便使用您的凭证以加密方式签署您的请求。如果您不使用 AWS 工具，则必须自行对请求签名。有关使用推荐的方法自行签署请求的更多信息，请参阅《IAM 用户指南》中的用于签署 API 请求的 AWS 签名版本 4。

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

AWS 账户根用户

在创建 AWS 账户时，您首先需要使用一个对账户中所有 AWS 服务和资源拥有完全访问权限的登录身份。此身份称为AWS账户根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅 IAM 用户指南中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）结合使用联合身份验证和身份提供者，以使用临时凭证来访问 AWS 服务。

联合身份是来自企业用户目录、Web 身份提供程序、AWS Identity Service 的用户，或任何使用通过身份源提供的凭证来访问 AWS 服务的用户。当联合身份访问 AWS 账户时，他们会代入角色，而角色会提供临时凭证。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和组，也可以连接并同步到您自己的身份源中的一组用户和组以跨所有 AWS 账户和应用程序使用。有关 IAM Identity Center 的信息，请参阅《AWS IAM Identity Center 用户指南》中的 What is IAM Identity Center?。

IAM 用户和群组

IAM 用户是 AWS 账户内对某个人员或应用程序具有特定权限的一个身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用案例需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的使用案例，应在需要时更新访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

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

IAM 角色

IAM 角色是 AWS 账户中具有特定权限的实体。它类似于 IAM 用户，但与特定人员不关联。要在 AWS 管理控制台中临时代入 IAM 角色，可以从用户切换到 IAM 角色（控制台）。可以通过调用 AWS CLI

或 AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的代入角色的方法。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问：要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关用于联合身份验证的角色的信息，请参阅《IAM 用户指南》中的针对第三方身份提供者创建角色（联合身份验证）。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关更多信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。
- 临时 IAM 用户权限：IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户访问：您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅 IAM 用户指南中的 IAM 中的跨账户资源访问。
- 跨服务访问：某些 AWS 服务使用其它 AWS 服务中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Simple Storage Service（Amazon S3）中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话（FAS）：当您使用 IAM 用户或角色在 AWS 中执行操作时，您将被视为主体。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用主体调用 AWS 服务的权限，结合请求的 AWS 服务，向下游服务发出请求。只有在服务收到需要与其它 AWS 服务或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两项操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。
  - 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。
  - 服务相关角色：服务相关角色是与 AWS 服务关联的一种服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 AWS 账户中，并由该服务拥有。IAM 管理员可以查看但不能编辑服务关联角色的权限。
- 在 Amazon EC2 上运行的应用程序：您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时凭证。这优先于在 EC2 实例中存储访问密钥。要将 AWS 角色分配给 EC2 实例并使其对该实例的所有应用程序可用，您可以创建一个附加到实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM 角色向在 Amazon EC2 实例上运行的应用程序授予权限。

使用策略管理访问

您将创建策略并将其附加到 AWS 身份或资源，以控制 AWS 中的访问。策略是 AWS 中的对象；在与身份或资源相关联时，策略定义它们的权限。在主体（用户、根用户或角色会话）发出请求时，AWS 将评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略在 AWS 中存储为 JSON 文档。有关 JSON 策略文档的结构和内容的更多信息，请参阅 IAM 用户指南中的 JSON 策略概览。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

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

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管策略是可以附加到 AWS 账户中的多个用户、组和角色的独立策略。托管式策略包括 AWS 托管式策略和客户托管策略。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。主体可以包括账户、用户、角色、联合用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用来自 IAM 的 AWS 托管式策略。

访问控制列表（ACL）

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

Amazon S3、AWS WAF 和 Amazon VPC 是支持 ACL 的服务示例。要了解有关 ACL 的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的访问控制列表（ACL）概览。

其他策略类型

AWS 支持额外的、不太常用的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界：权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅IAM 用户指南中的 IAM 实体的权限边界。
- 服务控制策略 (SCP) – SCP 是指定 AWS Organizations 中的组织或组织单元 (OU) 的最大权限的 JSON 策略。AWSOrganizations 是一个服务，用于对您的企业拥有的多个 AWS 账户进行分组和集中管理。如果在组织内启用了所有特征，则可对任意或全部账户应用服务控制策略（SCP）。SCP 限制成员账户中实体的权限，包括每个AWS账户根用户。有关组织和 SCP 的更多信息，请参阅《AWS Organizations 用户指南》中的 Service control policies。
- 资源控制策略（RCP）– RCP 是 JSON 策略，您可以使用它们设置账户中资源的最大可用权限，而无需更新附加到您拥有的每个资源的 IAM 策略。RCP 限制了成员账户中资源的权限，并可能影响身份（包括 AWS 账户根用户）的有效权限，无论这些身份是否属于您的组织。有关 Organizations 和 RCP（包括支持 RCP 的 AWS 服务列表）的更多信息，请参阅《AWS Organizations 用户指南》中的资源控制策略 (RCPs)。
- 会话策略：会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解 AWS 如何确定在涉及多种策略类型时是否允许请求，请参阅《IAM 用户指南》中的策略评估逻辑。

数据传输终端如何与 IAM 配合使用

在使用 IAM 管理对数据传输终端的访问权限之前，您应该了解哪些 IAM 功能可用于数据传输终端。

IAM 功能	数据传输终端支持
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
策略条件键	是
ACL	否
ABAC（策略中的标签）	否
临时凭证	是
主体权限	否
服务角色	否
服务关联角色	否

要大致了解数据传输终端和其他 AWS 服务如何与大多数 IAM 功能结合使用，请参阅《IAM 用户指南》中的使用 IAM 的 AWS 服务。

数据传输终端基于身份的策略

支持基于身份的策略：是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

数据传输终端基于身份的策略示例

要查看基于身份的数据传输终端策略示例，请参阅 AWS 数据传输终端基于身份的策略示例。

数据传输终端内基于资源的策略

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、联合身份用户或 AWS 服务。

要启用跨账户访问，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当主体和资源位于不同的 AWS 账户中时，受信任账户中的 IAM 管理员还必须授予主体实体（用户或角色）访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

数据传输终端的策略操作

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内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

要查看数据传输终端操作的列表，请参阅《Service Authorization Reference》中的 Actions Defined by AWS Data Transfer Terminal。

数据传输终端中的策略操作在操作前使用以下前缀：

```
datatransferterminal
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
      "datatransferterminal:action1",
      "datatransferterminal:action2"
         ]
```

要查看基于身份的数据传输终端策略示例，请参阅 AWS 数据传输终端基于身份的策略示例。

数据传输终端的策略资源

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内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

Resource JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

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

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

要查看数据传输终端的资源类型及其 ARN 的列表，请参阅《Service Authorization Reference》中的 Resources Defined by AWS Data Transfer Terminal。要了解您可以使用哪些操作指定每个资源的 ARN，请参阅 AWS 数据传输终端定义的操作。

要查看基于身份的数据传输终端策略示例，请参阅 AWS 数据传输终端基于身份的策略示例。

数据传输终端的策略条件键

支持特定于服务的策略条件键：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。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（或 Condition`*block*) lets you specify conditions in which a statement is in effect. The `Condition 元素）是可选项。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

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

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

AWS 支持全局条件键和特定于服务的条件键。要查看所有 AWS 全局条件键，请参阅《IAM 用户指南》中的 AWS 全局条件上下文键。

要查看数据传输终端条件键的列表，请参阅《Service Authorization Reference》中的 Condition Keys for AWS Data Transfer Terminal。要了解您可以对哪些操作和资源使用条件键，请参阅 AWS 数据传输终端定义的操作。

要查看基于身份的数据传输终端策略示例，请参阅 AWS 数据传输终端基于身份的策略示例。

数据传输终端中的 ACL

支持 ACL：否

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

通过数据传输终端进行 ABAC

支持 ABAC（策略中的标签）：否

基于属性的访问权限控制 (ABAC) 是一种授权策略，该策略基于属性来定义权限。在 AWS 中，这些属性称为标签。您可以将标签附加到 IAM 实体（用户或角色）以及 AWS 资源。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，请使用 `aws:ResourceTag/[replaceable]key-name ``, , or aws:TagKeys condition keys.` 在策略的 condition 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）。

在数据传输终端中使用临时凭证

支持临时凭证：是

某些 AWS 服务在您使用临时凭证登录时无法正常工作。有关更多信息，包括AWS服务与临时凭证配合使用，请参阅《IAM 用户指南》中的使用 IAM 的AWS服务。

如果您不使用用户名和密码而用其他方法登录到 AWS 管理控制台，可使用临时凭证。例如，当您使用贵公司的单点登录 (SSO) 链接访问 AWS 时，该过程将自动创建临时凭证。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的从用户切换到 IAM 角色（控制台）。

您可以使用 AWS CLI 或者 AWS API 手动创建临时凭证。之后，您可以使用这些临时凭证访问 AWS。AWS 建议您动态生成临时凭证，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

数据传输终端的跨服务主体权限

支持转发访问会话（FAS）：否

当您使用 IAM 用户或角色在 AWS 中执行操作时，您将被视为主体。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用主体调用 AWS 服务的权限，结合请求的 AWS 服务，向下游服务发出请求。只有在服务收到需要与其它 AWS 服务或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两项操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

数据传输终端的服务角色

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破坏数据传输终端功能。仅当数据传输终端提供相关指导时才编辑服务角色。

数据传输终端的服务相关角色

支持服务相关角色：否

服务相关角色是一种与AWS服务相关的服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 AWS 账户中，并由该服务拥有。IAM 管理员可以查看但不能编辑服务关联角色的权限。

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

AWS 数据传输终端基于身份的策略示例

默认情况下，用户和角色没有创建或修改数据传输终端资源的权限。它们也无法使用 AWS 管理控制台、AWS 命令行界面 (AWS CLI) 或 AWS API 执行任务。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的创建 IAM 策略（控制台）。

有关定义的操作和资源类型的详细信息，包括每种资源类型的 ARN 格式，请参阅服务授权参考中的操作。

主题

- 策略最佳实践
- 使用数据传输终端控制台
- 允许用户查看他们自己的权限

策略最佳实践

基于身份的策略确定某个人是否可以创建、访问或删除您账户中的数据传输终端资源。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：

- AWS 托管策略及转向最低权限许可入门 – 要开始向用户和工作负载授予权限，请使用 AWS 托管式策略来为许多常见使用案例授予权限。您可以在 AWS 账户中找到这些策略。我们建议通过定义特定于您的使用案例的 AWS 客户管理型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。如果通过特定 AWS 服务（例如

AWS CloudFormation）使用服务操作，您还可以使用条件来授予对服务操作的访问权限。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）– 如果您所处的场景要求您的 AWS 账户中有 IAM 用户或根用户，请启用 MFA 来提高安全性。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。

使用数据传输终端控制台

要访问 AWS 数据传输终端控制台，您必须具有一组最低的权限。这些权限必须允许您列出和查看有关您 AWS 账户中的数据传输终端资源的详细信息。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于只需要调用 AWS CLI 或 AWS API 的用户，您无需为其提供最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保用户和角色仍可使用数据传输终端控制台，请同时将数据传输终端 *ConsoleAccess* 或 *ReadOnly* AWS 托管式策略添加到实体。有关更多信息，请参阅《IAM 用户指南》中的为用户添加权限。

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。此策略包含通过控制台或者使用 AWS CLI 或 AWS API 以编程方式完成此操作所需的权限。

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

AWS 数据传输终端身份和访问故障排除

您可以使用以下信息，帮助诊断和修复在使用数据传输终端和 IAM 时可能遇到的常见问题。

主题

- 我无权在数据传输终端中执行操作
- 我希望允许我的 AWS 账户以外的人访问我的数据传输终端资源

我无权在数据传输终端中执行操作

如果您无法在 AWS 数据传输终端控制台中查看或安排预留，则可能是没有所需的权限。请联系账户管理员配置 IAM 身份策略，授予您访问权限和相应的权限。

我希望允许我的 AWS 账户以外的人访问我的数据传输终端资源

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（ACL）的服务，您可以使用这些策略向人员授予对您的资源的访问权。

要了解更多信息，请参阅以下内容：

- 要了解数据传输终端是否支持这些功能，请参阅数据传输终端如何与 IAM 配合使用。
- 要了解如何为您拥有的 AWS 账户中的资源提供访问权限，请参阅 IAM 用户指南中的为您拥有的另一个 AWS 账户中的 IAM 用户提供访问权限。
- 要了解如何为第三方 AWS 账户提供您的资源的访问权限，请参阅IAM 用户指南中的 为第三方拥有的 AWS 账户提供访问权限。
- 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。

数据传输终端 API 参考：操作和资源

创建 AWS Identity and Access Management (IAM) 策略时，此页面可帮助您了解 AWS 数据传输终端 API 操作、您可授予执行权限的对应操作以及您可授予权限的 AWS 资源之间的关系。

通常，以下是向策略添加数据传输终端权限的方法：

- 在 `Action` 元素中指定操作。该值包括 `datatransferterminal:` 前缀和 API 操作名称。例如 `datatransferterminal:CreateTask`。
- 在 `Resource` 元素中指定与操作相关的 AWS 资源。

您还可以在数据传输终端策略中使用 AWS 的条件键。有关 AWS 的键的完整列表，请参阅 IAM 用户指南中的可用键。

数据传输终端 API 操作及对应的操作

CreateTransferTeam

- 操作：`datatransferterminal:CreateTransferTeam`

  资源：None

GetTransferTeam

- 操作：`datatransferterminal:GetTransferTeam`

  资源：`arn:aws::$[replaceable]分区:datatransferterminal:$[replaceable]区域:$[replaceable]账户:transfer-team/$[replaceable]TransferTeamId````

UpdateTransferTeam

- 操作：datatransferterminal:UpdateTransferTeam

  资源：arn:aws::$[replaceable]分区:datatransferterminal:$[replaceable]区域:$[replaceable]账户:transfer-team/$[replaceable]TransferTeamId````

DeleteTransferTeam

- 操作：datatransferterminal:DeleteTransferTeam

  资源：arn:aws::$[replaceable]分区:datatransferterminal:$[replaceable]区域:$[replaceable]账户:transfer-team/$[replaceable]TransferTeamId````

ListTransferTeams

- 操作：datatransferterminal:ListTransferTeams

  资源：None

RegisterPerson

- 操作：datatransferterminal:RegisterPerson

  资源：arn:aws::$[replaceable]分区:datatransferterminal:$[replaceable]区域:$[replaceable]账户:transfer-team/$[replaceable]TransferTeamId````

GetPerson

- 操作：datatransferterminal:GetPerson

  资源：arn:aws::$[replaceable]分区:datatransferterminal:$[replaceable]区域:$[replaceable]账户:transfer-team/$[replaceable]TransferTeamId/person/$[replaceable]PersonId````

  相关操作：datatransferterminal:GetTransferTeam

  依赖资源：arn:aws::$[replaceable]分区:datatransferterminal:$[replaceable]区域:$[replaceable]账户:transfer-team/$[replaceable]TransferTeamId````

DeregisterPerson

- 操作：datatransferterminal:DeregisterPerson

  资源：arn:aws::$[replaceable]分区:datatransferterminal:$[replaceable]区域:$[replaceable]账户:transfer-team/$[replaceable]TransferTeamId/person/$[replaceable]PersonId````

相关操作：datatransferterminal:GetTransferTeam

依赖资源：arn:aws::$[replaceable]分区:datatransferterminal:
$[replaceable]区域:$[replaceable]账户:transfer-team/
$[replaceable]TransferTeamId````

ListPersons

- 操作：datatransferterminal:ListPersons

  资源：arn:aws::$[replaceable]分区:datatransferterminal:$[replaceable]区域:$[replaceable]账户:transfer-team/$[replaceable]TransferTeamId````

CreateReservation

- 操作：datatransferterminal:CreateReservation

  资源：arn:aws::$[replaceable]分区:datatransferterminal:$[replaceable]区域:$[replaceable]账户:transfer-team/$[replaceable]TransferTeamId````

  相关操作：datatransferterminal:GetTransferTeam

  依赖资源：arn:aws::$[replaceable]分区:datatransferterminal:
  $[replaceable]区域:$[replaceable]账户:transfer-team/
  $[replaceable]TransferTeamId````

  相关操作：datatransferterminal:GetPerson

  依赖资源：arn:aws::$[replaceable]分区:datatransferterminal:
  $[replaceable]区域:$[replaceable]账户:transfer-team/
  $[replaceable]TransferTeamId/person/$[replaceable]PersonId````

  相关操作：datatransferterminal:GetFacility

  依赖资源：arn:aws::$[replaceable]分区:datatransferterminal:::facility/
  $[replaceable]FacilityId````

GetReservation

- 操作：datatransferterminal:GetReservation

  资源：arn:aws::$[replaceable]分区:datatransferterminal:$[replaceable]区域:$[replaceable]账户:transfer-team/$[replaceable]TransferTeamId/
  reservation/$[replaceable]ReservationId````

相关操作：datatransferterminal:GetTransferTeam

依赖资源：arn:aws::$[replaceable]分区:datatransferterminal:
$[replaceable]区域:$[replaceable]账户:transfer-team/
$[replaceable]TransferTeamId````

UpdateReservation

- 操作：datatransferterminal:UpdateReservation

  资源：arn:aws::$[replaceable]分区:datatransferterminal:$[replaceable]区域:$[replaceable]账户:transfer-team/$[replaceable]TransferTeamId/reservation/$[replaceable]ReservationId````

  相关操作：datatransferterminal:GetTransferTeam

  依赖资源：arn:aws::$[replaceable]分区:datatransferterminal:
  $[replaceable]区域:$[replaceable]账户:transfer-team/
  $[replaceable]TransferTeamId````

  相关操作：datatransferterminal:GetPerson

  依赖资源：arn:aws::$[replaceable]分区:datatransferterminal:
  $[replaceable]区域:$[replaceable]账户:transfer-team/
  $[replaceable]TransferTeamId/person/$[replaceable]PersonId````

DeleteReservation

- 操作：datatransferterminal:DeleteReservation

  资源：arn:aws::$[replaceable]分区:datatransferterminal:$[replaceable]区域:$[replaceable]账户:transfer-team/$[replaceable]TransferTeamId/person/$[replaceable]PersonId````

  相关操作：datatransferterminal:GetTransferTeam

  依赖资源：arn:aws::$[replaceable]分区:datatransferterminal:
  $[replaceable]区域:$[replaceable]账户:transfer-team/
  $[replaceable]TransferTeamId````

ListReservations

- 操作：datatransferterminal:ListReservations

资源：arn:aws::$[replaceable]分区:datatransferterminal:$[replaceable]区域:$[replaceable]账户:transfer-team/$[replaceable]TransferTeamId````

ListFacilities

- 操作：datatransferterminal:ListFacilities

  资源：None

GetFacility

- 操作：datatransferterminal:GetFacility

  资源：arn:aws::$[replaceable]分区:datatransferterminal:::facility/$[replaceable]FacilityId````

GetFacilityAvailability

- 操作：datatransferterminal:GetFacilityAvailability

  资源：arn:aws::$[replaceable]分区:datatransferterminal:::facility/$[replaceable]FacilityId/availability

  相关操作：datatransferterminal:GetFacility

  依赖资源：arn:aws::$[replaceable]分区:datatransferterminal:::facility/$[replaceable]FacilityId/availability

AWS 数据传输终端的合规性验证

要了解某个 AWS 服务是否在特定合规性计划范围内，请参阅合规性计划范围内的 AWS 服务，然后选择您感兴趣的合规性计划。有关一般信息，请参阅 AWS合规性计划。

您可以使用 AWS Artifact 下载第三方审计报告。有关更多信息，请参阅下载 AWS Artifact 中的报告。

您在使用 AWS 服务时的合规性责任由您数据的敏感性、贵公司的合规性目标以及适用的法律法规决定。AWS 提供以下资源来帮助满足合规性：

- Security Compliance & Governance：这些解决方案实施指南讨论了架构考虑因素，并提供了部署安全性和合规性功能的步骤。
- 符合 HIPAA 要求的服务参考：列出符合 HIPAA 要求的服务。并非所有 AWS 服务都符合 HIPAA 条件。

- AWS 合规性资源 – 此业务手册和指南集合可能适用于您的行业和位置。
- https://d1-awsstatic-com-whitepapers-compliance-AWS-Customer-Compliance-Guides-pdf[AWS 客户合规指南] – 从合规角度了解责任共担模式。这些指南总结了保护 AWS 服务的最佳实践，并将指南映射到跨多个框架的安全控制，包括美国国家标准与技术研究院（NIST）、支付卡行业安全标准委员会（PCI）和国际标准化组织（ISO）。
- 《AWS Config 开发人员指南》中的使用规则评估资源 – AWS Config 服务评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- AWS Security Hub – 该 AWS 服务向您提供 AWS 中安全状态的全面视图。Security Hub 通过安全控制措施评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控制措施的列表，请参阅 Security Hub 控制措施参考。
- Amazon GuardDuty – 该 AWS 服务通过监控您的环境中是否存在可疑和恶意活动，来检测您的 AWS 账户、工作负载、容器和数据面临的潜在威胁。GuardDuty 可以通过满足某些合规性框架规定的入侵检测要求，来协助您满足各种合规性要求，如 PCI DSS。
- AWS 审计管理器 – 此 AWS 服务可帮助您持续审计 AWS 使用情况，以简化您管理风险和符合法规及行业标准的方式。

AWS 数据传输终端的恢复能力

AWS全球基础架构围绕AWS区域和可用区构建。AWS区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。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 全球基础架构。

AWS 数据传输终端遍布世界各地。您可以连接到可通过互联网访问的任何 AWS 区域。

数据传输终端中的日志记录和监控

AWS 数据传输终端已与 AWS CloudTrail 集成，后者是一项服务，提供数据传输终端中用户、角色或 AWS 服务所执行操作的记录。CloudTrail 将数据传输终端的所有 API 调用作为事件捕获。捕获的调用包括通过数据传输终端控制台的调用以及对数据传输终端 API 操作的代码调用。如果您创建跟踪记录，则可以使 CloudTrail 事件持续传送到 Amazon S3 存储桶，包括数据传输终端的事件。如果您不配置跟踪，则仍可在 CloudTrail 控制台中的事件历史记录中查看最新事件。使用 CloudTrail 收集的信息，您可以确定向数据传输终端发出的请求内容、发出请求的 IP 地址、何人发出的请求、请求的发出时间以及其他详细信息。

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

CloudTrail 中的数据传输终端信息

在您创建 AWS 账户时，将在该账户上启用 CloudTrail。当数据传输终端中发生活动时，该活动将记录在 CloudTrail 事件中，并与其他 AWS 服务事件一同保存在事件历史记录中。您可以在 AWS 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用 CloudTrail 事件历史记录查看事件。

要持续记录 AWS 账户中的事件（包括数据传输终端的事件），请创建跟踪。通过跟踪记录，CloudTrail 可将日志文件传送至 Amazon S3 存储桶。预设情况下，在控制台中创建跟踪时，此跟踪应用于所有 AWS 区域。此跟踪记录在 AWS 分区中记录所有区域中的事件，并将日志文件传送至您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，进一步分析在 CloudTrail 日志中收集的事件数据并采取行动。有关更多信息，请参阅下列内容：

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

所有数据传输终端操作均由 CloudTrail 记录，并记载于本指南的数据传输终端 API 参考：操作和资源章节。

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：

- 发出请求使用的是根凭证还是 AWS Identity and Access Management (IAM) 用户凭证。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

了解数据传输终端日志文件条目

跟踪记录是一种配置，可用于将事件作为日志文件传送到您指定的 Simple Storage Service（Amazon S3）存储桶。CloudTrail 日志文件包含一个或多个记录条目。事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

AWS 数据传输终端的基础设施安全

作为一项托管式服务，AWS 数据传输终端由 {https---d0-awsstatic-com-whitepapers-Security-AWS-Security-Whitepaper-pdf}[Amazon Web Services：安全过程概述] 白皮书中所述的 AWS 全球网络安全程序提供保护。

您可以使用 AWS 发布的 API 调用通过网络访问数据传输终端。客户端必须支持传输层安全性协议（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，对请求进行签名。

数据传输终端用户指南文档历史记录

下表介绍了本指南的文档历史记录。

变更	说明	日期
更新布局	更新文档布局并对措辞和内容进行少量编辑。	2025 年 1 月 1 日
初次发布	原始文档发布日期。	2024 年 12 月 1 日