用户指南

AWS 数据传输终端

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS 数据传输终端: 用户指南

Copyright © 2025 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？ 1
特征 1
重要概念 2
转会小组 2
人员 2
设施 3
日程安排注意事项 3
使用案例 3
相关服务 4
技术要求 5
设备 5
网络要求 5
性能优化 5
更多信息 6
入门 8
注册获取 AWS 账户 8
创建具有管理访问权限的用户 9
安排预约 11
创建转会小组 11
在您的数据传输终端账户上更新传输小组 12
添加人员 12
向您的数据传输终端账户中的人员通报最新情况 13
指定预订详情 13
查看并确认您的预订 14
更改您的预订 14
进行数据传输 16
要带什么 16
数据传输终端设施的物理地址 16
进入大楼 16
数据传输终端套件中的预期设备。 17
网络连接疑难解答 18
设备连接问题 18
排除连接性问题 18
Linux/Unix 19

Windows 19
网络吞吐量 20
安全性 21
数据保护 21
数据加密 22
传输中加密 23
密钥管理 23
互联网络流量隐私 23
身份和访问管理 24
受众 24
使用身份进行身份验证 25
使用策略管理访问 27
数据传输终端如何与 IAM 配合使用 29
基于身份的策略示例 34
故障排除 37
API 参考 38
合规性验证 42
恢复能力 42
CloudTrail 日志 43
中的数据传输终端信息 CloudTrail 43
了解数据传输终端日志文件条目 44
基础设施安全性 44
文档历史记录 45
..... xlvi

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，您可以携带数据存储设备，以便在服务之间快速传输数据。 AWS 云 上传远程捕获的数据，以便更轻松地访问远程捕获的数据。

从那里开始在我们的物理数据传输终端设施进行预订 AWS Management Console，在预定时间到达，然后使用自己的设备将您的数据上传到您的 AWS 云 服务。在您的预定预订完成并离开后，该设施将重新获得安全保障，为下一次预定预订做好准备。

> **Note**
>
> AWS 目前，数据传输终端仅适用于 AWS 企业客户。

要访问数据传输终端，请执行以下操作：

- AWS 数据传输终端控制台：https://console.aws.amazon.com/datatransferTerminal
- 数据传输终端设施：一旦在控制台中进行预订，便会提供数据传输终端设施的位置。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 云 服务中。以下是数据传输终端在满足您的远程数据上传需求方面的一些优势：

安全、私密、独家

每个数据传输终端设施都是一个安全、私密的地方，您可以通过快速的网络连接在数据存储设备和 AWS 服务之间进行大量数据传输。

专用的预订控制台

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

光纤网络连接

每个数据传输终端设施包括两个 100 千兆位 (Gbps) 光纤 (LR4) 连接，可实现快速数据上传和冗余。

控制您的数据存储设备

无需运送您的 Snowball 设备并等待数据上传到您的 AWS 云 服务。在整个数据传输过程中，您可以控制物理数据存储设备，从而更快地将数据传输到需要的地方。

重要概念

使用 AWS 数据传输终端需要流程所有者预约数据传输专家访问数据传输终端设施。要了解有关数据传输终端术语的更多信息，请参阅以下部分。

主题

- 转会小组
- 人员
- 设施

转会小组

传输团队是由 AWS 账户 所有者确定的人员组，他们可以被选中代表您的组织进行数据传输。组建转会团队包括为转会小组命名并指定该团队的人员。我们建议由四名或更少的数据传输专家组成的小组进行一次预订。

有关更多信息，请参阅 预约数据传输终端。

人员

人员是指可以进行和管理预订或可以前往和使用数据传输终端设施的个人。人员可以是流程所有者或数据传输专家，或者两者兼而有之。

进程所有者

流程所有 AWS 账户 者是可以从其 AWS 数据传输终端帐户中添加、编辑和删除人员的所有者。

数据传输专家

数据传输专家是指可以前往数据传输终端设施进行数据上传交易的人。这些人员必须获得流程所有者的授权并添加到您的 AWS 数据传输终端帐户中。访问数据传输终端设施时，需要出示政府签发的身份证。

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签发的身份证明，该证明必须与其预订记录相匹配才能访问数据传输终端套件。

日程安排注意事项

全年任何一天，都可以在数据传输终端控制台中进行一到六个小时的预订。个人预订可以连续安排，两次预订之间至少间隔一小时。所有预订必须至少提前 24 小时进行。

传输数据所需的时间因上传性能速度而异。在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。

装备

某些设备可能包含可能会影响上传性能的设置。有关建议的上传性能速度，请参阅您的设备规格。

网络状况

网络流量过大的时间会影响数据上传速度，因此在选择数据传输会话的时间时应将其考虑在内。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能会提高上传速度。

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，传输的数据的大小将影响会话所需的时间。

使用案例

虽然任何 AWS 企业客户都可以访问数据传输终端系统，但某些用例场景可能会从中获得更大的好处。

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) 和供应商从其在北美、欧洲和东盟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 云 服务中，用于训练 AD/ADAS 模型。

媒体和娱乐：工作室和其他内容创作者经常在偏远地区生成数字视频和音频 (AV) 文件。必须及时将这些 AV 文件上传到云端，这样分散在不同地理位置的制作和编辑团队就可以并行和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，可以缩短生产时间，从而降低生产成本。

地图、摄影测量和 3D 影像：使用制图或影像应用程序的组织在远程位置收集数据，需要将这些可视文件上传到 AWS 云 进行分析或培训。Data Transfer Terminal 最大限度地缩短了收集和分析这些大型数据集之间的时间，这有助于 up-to-date为驾驶员、农民和其他信息用户保留地理空间数据。

相关服务

以下内容 AWS 服务 提供了使用数据传输终端时的最佳体验。

AWS 服务	描述
AWS Snowball Edge	AWS 数据传输终端为 Snowball 产品提供了更快上传到 AWS 云端的位置，最大限度地减少了访问数据的等待时间，从而补充了 Snowball 产品。
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您的 Amazon S3 服务。

使用数据传输终端的技术要求

在预约数据传输终端之前，您需要确保拥有连接网络所需的设备和配置。要获得最佳的网络连接和体验，请参阅以下指南。

设备

您必须将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）带到数据传输终端设施进行预约。

您的硬件必须能够使用光纤 (L4) 连接

> **Note**
>
> 作为数据安全最佳实践，请确保您的数据在带到数据传输终端的存储设备上经过加密和保护，并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 数据传输终端的安全

网络要求

确保您的上传设备、服务器或设备（笔记本电脑）已准备好连接到网络并且支持 DHCP。为了获得最佳的数据上传体验，您应该具备以下条件：

- 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。
- IP 地址自动配置 DHCP 已启用。DNS 服务器由 DHCP 自动分配。
- Up-to-date 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。

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

  - 128 GB 内存
  - 一个 RAID 阵列中有多个 NVME 固态硬盘
- 使用 AWS 公共运行时 (AWS CRT) 库使用 AWS Command Line Interface 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 配置文件中的顶级`s3`键下设置这些值，默认位置 `~/.aws/config`。

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

  请注意，所有 Amazon S3 配置值都缩进并嵌套在顶级`s3`密钥下。

  - 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
```

- 要以编程方式为默认配置文件以外的配置文件设置这些值，请提供标`--profile`志。例如，要为名为的配置文件设置配置`test-profile`，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) 以提高吞吐量。

```
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。

- AWSAWS CLI 命令参考中的 CLI Amazon S3 配置

- 在适用于 Java 的 Amazon S3Amazon SDK 中使用高性能的亚马逊 S AppStream 3 客户端： AWS 基于 CRT 的客户端
- 当我使用将大文件上传 AWS CLI 到 Amazon S3 时，如何优化性能？ 在AWS 知识中心

入门

通过在其中一个数据传输终端设施进行预订，即可开始向您的 AWS 云 服务进行远程数据传输。首先，您需要数据传输终端设施支持的设备和 AWS 企业帐户。

在安排数据传输终端预约之前，请查看本指南的使用数据传输终端的技术要求部分，以确保您的设备具有最佳的数据传输配置。并非所有数据存储设备和网络连接设备都与套件中提供的光纤网络连接兼容。

当您注册时 AWS，系统会自动注册使用 AWS 账户 中的所有服务 AWS，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，可以选择更改中的显示语言 AWS Management Console。有关更多信息，请参阅《AWS Management Console 入门指南》中的更改 AWS Management Console的语言。

拥有数据传输终端后， AWS 账户 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，请参阅预约数据传输终端。

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，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 Management Console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 Enabling 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网址。

  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。

预约数据传输终端

要开始使用 AWS 数据传输终端，你需要在 https://console.aws.amazon.com/dat transferterminal 上拥有 AWS 账户 并登录到数据传输终端控制台。登录数据传输终端控制台后，您可以查看现有预订或进行新的预订。要安排预订，您需要执行以下操作：

1. 创建一支转会小组。您需要创建一组指定的用户来创建预订，并访问数据传输终端设施进行数据传输。要了解有关此主题的更多信息，请参阅创建转会小组。
2. 组建完团队后，您需要为其增加人员。要了解有关向您的转会团队添加人员的更多信息，请参阅添加人员。
3. 流程所有者可以与账户中的团队一起安排数据传输。有关如何安排预订的更多信息，请参阅指定预订详情。
4. 在提交申请之前，请确保预订的详细信息正确无误。预订申请一经提交，至少在 24 小时内无法修改。有关更多信息，请参阅 查看并确认您的预订。

处理并确认您的预订后，您的传输团队将能够在预定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进行数据传输。

创建转会小组

要访问数据传输终端设施，您需要在中安排预订 AWS Management Console。登录您的 AWS 账户 以访问数据传输终端控制台，并完成以下步骤来安排您的预订。

1. 在数据传输终端的主页上，选择开始按钮。
2. 如果您的账户中尚未设置转会小组，则创建预订按钮将被禁用。首先，你需要创建并命名一支转会小组。
   a. 选择 “创建转会小组” 按钮。
   b. 给队伍起个名字。
      - 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、句点和破折号。无法识别特殊字符。
      - 请勿包含任何敏感的识别信息。
   c. 创建转会队伍描述。
      - 提供有助于识别团队的描述，例如描述团队在特定时间段、活动或项目的目的。

d. 选择 “创建转会小组” 按钮。

您将返回到转会团队页面，您新创建的球队将显示在转会队伍部分下。

在您的数据传输终端账户上更新传输小组

要组建新的转会小组，请参阅本指南的预约数据传输终端章节。

要修改或移除转会小组，请执行以下操作：

1. 在转会队伍页面上，选择您要修改的转会球队。
2. 要修改转会队的名称和描述，请选择编辑按钮。
3. 要添加或删除人员，请选择人员选项卡，然后完成如何修改、添加或删除账户中的人员？中描述的步骤 本常见问题解答部分。
4. 要为所选转会团队添加或取消预订，请参阅本常见问题解答向您的数据传输终端账户中的人员通报最新情况部分。

添加人员

将流程所有者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。要向您的转会团队添加人员，请执行以下操作：

1. 在转会队伍页面上，从转会队伍部分列出的转会队卡片中选择所需的转会队卡。将会出现转会小组的摘要页面。
2. 选择 “人员” 选项卡，然后选择 “注册人员” 按钮，将人员添加到调动小组。
3. 在 “注册人员” 页面上填写有关您要加入转会团队的人员的必要信息。

   a. 人员别名：创建唯一的别名来识别该人员。

      - 该别名用于识别人员，同时保护他们的身份。
      - 它可以长达 64 个字符，包括字母、数字和破折号。
      - 不允许使用特殊字符。

   b. 名字：提供该人的名字，与其政府签发的身份证件上的名字相同。

   c. 姓氏：提供该人的姓氏或姓氏，该姓氏出现在其政府签发的身份证件上。

   d. 电子邮件地址：包括一个好的电子邮件地址，以便该人接收预订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，完成将该人添加到您的转接团队的操作。

向您的数据传输终端账户中的人员通报最新情况

目前不支持在数据传输终端控制台中修改您账户中的现有人员。 AWS 数据传输终端进程所有者目前只能添加或删除人员。

要从您的数据传输终端账户中删除人员，请执行以下操作：

1. 在转会小组页面上，选择与您要移除的人员相关的转会小组。
2. 在所选转会小组的摘要页面上，选择人员选项卡。
3. 点击您要删除的别名旁边的单选按钮。请注意，只有在删除该人的个人资料时，您才能看到他们的别名。
4. 选择 “删除” 按钮。将出现一条警告，确认所选人员的预期行动。单击 “删除” 按钮继续。控制台顶部将显示一条横幅，确认该人员已成功删除。

指定预订详情

以下说明将引导您了解如何在中安排数据传输终端的预订 AWS Management Console。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 “即将进行的预订” 选项卡中选择 “进行预订” 按钮。
2. 填写 “指定预订详情” 页面上的字段。

   a. 转会球队选择：选为默认的转会队伍首先出现。如果您想选择其他球队，请点击下拉箭头从可用的转会队伍列表中进行选择。

   b. 流程所有者：选择您要负责管理预订的人员别名。

      - 只允许一个流程所有者进行预订，并且他们必须是您的授权人员 AWS 账户。

        流程所有者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：选择您想要访问数据传输终端设施的人员，以完成数据传输活动。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) 位数据传输专家。

   d. 数据传输终端信息：指定数据传输终端设施、所需的日期和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**
>
> 预订时仅提供设施描述。预订确认电子邮件中将提供其他位置信息。

ii. 数据传输终端日期和时间：单击 “搜索预订的日期和时间” 字段，查看日历并安排预订。

- 必须至少提前 24 小时进行预订，预订时间不得超过六 (6) 个月，且最多只能提前六 (6) 个小时。如有必要，一次预订可能持续一天以上，以考虑到过夜的情况。
- 时间以 24 小时制表示，只能以整小时为增量进行预订。
- 要进行连续预约，您必须创建单独的预留，每次数据传输会话之间至少有一小时的间隔。
- 有关更多信息，请参阅 日程安排注意事项。

3. 确认预订详情正确无误，然后选择 “创建” 按钮继续。这将带您进入确认页面，其中提供了您的预订摘要。

查看并确认您的预订

指定预订详情后，选择 “下一步” 按钮继续查看概览页面。在 “查看并创建” 页面上查看您的数据传输终端预订请求的详细信息。

- 如果您对请求感到满意，请选择 “创建” 按钮。
- 如果您需要更改预订，请选择 “上一步” 按钮。

提交预订申请后，流程所有者将收到一封电子邮件，确认申请已收到并正在处理中。申请获得批准后，将通过另一封电子邮件确认预订，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。

更改您的预订

在对您的数据传输终端预订请求进行任何更改之前，有 24 小时的处理期。

处理期结束后，要查看、编辑或删除您的预订，请在控制台中导航至转会队伍页面。

1. 在球队的卡片上找到并选择所需的预约。

2. 单击 “操作” 菜单并选择所需的操作。
   - 查看：选择 “查看” 选项允许您查看预订的详细信息，包括日期、时间、地点和分配的人员。
   - 编辑：您可以修改预订的详细信息，包括日期、时间、地点和分配的人员。请注意，更改必须在所需的预订日期前 24 小时进行，并且不会立即接受和应用修改。您的流程所有者将收到更新请求的确认。
   - 删除：删除选项允许您取消预订。取消申请必须在预定预订日期前至少 24 小时提出。申请获得批准后，流程所有者将收到已取消预订的确认信息。

在数据传输终端设施进行数据传输

数据传输终端是一个安全的共享场所，可提供对 AWS 网络的安全访问。要访问数据传输终端设施，请确保您有一封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

- 要带什么
- 数据传输终端设施的物理地址
- 进入大楼
- 数据传输终端套件中的预期设备。

要带什么

数据传输专家应带上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 (SSDs) 和AWS Snowball Edge。确保您的设备经过优化，以便在数据传输终端设施中使用光纤网络电缆。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、使用和拆除您和随行的数据传输专家带入数据传输终端设施的设备和物品。任何带入套房的物品在离开时都必须移走。 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物理地址

将不提供数据传输终端设施的实际地址。相反，预订中指定的流程所有者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之相同的位置识别系统， AWS Direct Connect 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，请向您的 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。

进入大楼

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签发的身份证件。进入大楼后，保安人员将护送您前往您的数据传输终端套件。

数据传输终端套件中的预期设备。

每个数据传输终端设施只能有两 (2) 根光纤电缆、一张桌子或一张桌子和椅子。如果房间里还有其他设备或物品，请支持立即报告。

网络连接问题疑难解答

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
- 排除连接性问题
- 网络吞吐量

设备连接问题

如果您在使用数据传输终端套件时难以建立物理连接，请考虑以下几点：

- 每个数据传输终端设施将有两 (2) 根单模 LC 光缆。如果缺少其中一根或两根电缆，请立即联系 Su AWS pp ort。
- 如果一根光纤电缆无法正常工作，请尝试先滚动电缆。如果仍然无法连接第一根电缆，请尝试使用另一根电缆。

如果您仍然无法使用电缆进行连接，请立即联系 Supp AWS or t。

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。

- 确认您的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。
- 对设备执行基本的网络诊断，以确保满足以下要求：
  - DHCP 已启用
  - 已为连接的网络接口分配一个 IP 地址
  - 已配置 DNS 服务器
  - 系统时钟与 NTP 同步

如果您仍然无法连接，请联系 Su AWS pp ort，并根据您的设备上运行的操作系统 (OS) 向他们提供以下输出。

Linux/Unix

- 在终端或命令行界面 (CLI) 中获取 IP 地址和路由信息。确认已为网络接口分配了 IP 地址，并且路由表中添加了带有默认网关地址的默认路由。

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

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

```
ifconfig
netstat -rn
```

- 收集 DNS 服务器信息。这应该显示两个以`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。确认已为网络接口分配一个 IP 地址，分配了两台 DNS 服务器，并在路由表中添加了带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
```

- 在中收集 HTTPS 连接测试的输出 PowerShell。以下命令应显示响`HTTP 200 OK`应。

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

网络吞吐量

衡量网络中实际数据传输速率的网络吞吐量可能受到多种因素的影响。以下因素可能会影响您的数据传输速度：

- 硬件：上传数据时，设备的硬件组件可能会导致连接速度降低。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 SSDs 中使用 NVME。为了提高性能和降低 CPU 使用率，请务必使用 AWS CRT 库。
- 加密开销：由于加密开销，安全传输（例如 HTTPS）会增加处理时间。
- 延迟：延迟是指数据包从源传输到目的地所花费的时间。上传到不同地理区域的 Amazon S3 存储桶时可能会出现高延迟，这可能导致数据传输延迟和吞吐量降低。最佳做法是尽可能在同一区域内进行数据传输。
- 丢包：丢失的数据包需要重新传输，这会减慢数据传输速度。

AWS 数据传输终端的安全

AWS 数据传输终端为往返传输数据提供了一个安全的环境 AWS 云。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，以确保您的数据传输安全。

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 负责保护在云中运行 AWS 服务的基础架构 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。要了解适用于 AWS 数据传输终端的合规性计划，请参阅AWS 按合规计划划分的范围内AWS 服务按合规计划。
- 云端安全-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。

本文档可帮助您了解在使用数据传输终端时如何应用分担责任模型。以下主题向您介绍如何在使用数据传输终端服务时保护您的数据。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的数据传输终端资源。

主题

- 数据传输终端中的 AWS 数据保护
- 数据传输终端的身份和访问管理
- AWS 数据传输终端的合规性验证
- AWS 数据传输终端的弹性
- 在数据传输终端中记录和监控
- AWS 数据传输终端的基础设施安全

数据传输终端中的 AWS 数据保护

分 AWS 担责任模型适用于数据传输终端中的 AWS 数据保护。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）。
- 使用 SSL/TLS 与资源通信。 AWS 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》。

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）。这包括使用控制台、API 或 AWS 服务 使用数据传输终端或其他终端时 AWS SDKs。 AWS CLI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网址，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 数据传输终端允许您访问高速网络连接，以便在自我管理的存储系统和 AWS 存储服务之间安全地传输数据。存储数据在传输过程中的加密方式在一定程度上取决于设备上启用的策略以及数据传输到的服务。数据管理和传输过程中的加密由使用数据传输终端的个人负责。

静态加密

AWS 数据传输终端对所有静态数据进行加密。

数据传输终端仅捕获预订所需的数据，包括指定参加和安排预订的个人的名字和姓氏以及电子邮件地址。收集数据的目的是确认预订详情，并确保可以进入房间进行数据传输。此交易信息的备份时间不超过 35 天，但是， AWS 账户信息将保留 10 年。

传输中加密

AWS 数据传输终端不对传输中的数据进行加密。数据是 encrypted-in-transit指您与数据传输终端 API 端点进行交互，以便在控制台中设置传输小组、添加人员和安排预约。作为责任 AWS 共担模式的一部分，您可以选择如何 AWS 服务 通过数据传输终端进行连接。我们强烈建议您选择 AWS 服务 使用强连接 encryption-in-transit，例如 TLS 1.2 和 1.3。

例如，使用您的 Amazon S3 存储桶策略中的`aws:SecureTransport`条件，仅使用通过 HTTPS (TLS) 的加密连接，如以下存储桶策略所示。

```
{
 "Version": "2012-10-17",
    "Statement": [{
        "Sid": "RestrictToTLSRequestsOnly",
        "Action": "s3:",
        "Effect": "Deny",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket",
            "arn:aws:s3:::amzn-s3-demo-bucket/"
        ],
        "Condition": {
            "Bool": {
                "aws:SecureTransport": "false"
            }
        },
        "Principal": "*"
    }]
}
```

要详细了解与其他 AWS 服务（例如 Amazon S3）传输的数据加密，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管理的密钥。在预订数据传输终端期间，使用适用于您连接的 AWS 服务的客户托管密钥支持。在《密钥管理服务开发人员指南》的 AWS KMS 密钥部分，详细了解客户托管密钥以及如何加密静态数据。AWS

互联网络流量隐私

通过已发布的服务访问数据传输终端控制台 APIs。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) 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）使用数据传输终端资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- 数据传输终端如何与 IAM 配合使用
- AWS 数据传输终端基于身份的策略示例
- AWS 数据传输终端身份和访问疑难解答
- 数据传输终端 API 参考：操作和资源

受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您在数据传输终端中所做的工作。

服务用户-如果您使用数据传输终端服务完成工作，则您的管理员会为您提供所需的凭据和权限。当你使用更多的数据传输终端功能来完成工作时，你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。如果您无法访问数据传输终端中的某项功能，请参阅AWS 数据传输终端身份和访问疑难解答。

服务管理员-如果您负责公司的数据传输终端资源，则可能拥有对数据传输终端的完全访问权限。您的工作是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。要详细了解贵公司如何将 IAM 与数据传输终端一起使用，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，则可能需要详细了解如何编写策略来管理对数据传输终端的访问权限。要查看您可以在 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 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （IAM Identity Center）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅《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》中的多重身份验证和《IAM 用户指南》中的 IAM 中的AWS 多重身份验证。

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问该身份。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）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C enter 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。 AWS Directory Service当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

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 中创建用户和群组，也可以连接并同步到您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户 和

应用程序中使用。有关 IAM Identity Center 的信息，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

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。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场景需要长期凭证以及 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用例，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，您可以拥有一个名为的群组，IAMAdmins并向该群组授予管理 IAM 资源的权限。

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

IAM 角色

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。要在中临时担任 IAM 角色 AWS Management Console，您可以从用户切换到 IAM 角色（控制台）。您可以通过调用 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商创建角色（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。有关权限集的信息，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。
- 跨账户存取：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，对于某些资源 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 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在服务中拨打电话时，该服务通常会在 Amazon 中运行应用程序 EC2 或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。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 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 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-服务相关角色是一种与服务相关联的服务角色。 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相关角色的权限。
- 在 A@@ mazon 上运行的应用程序 EC2 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这比在 EC2 实例中存储访问密钥更可取。要为 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建一个附加到该实例的实例配置文件。实例配置文件包含角色并允许在 EC2 实例上运行的程序获得临时证书。有关更多信息，请参阅 IAM 用户指南中的使用 IAM 角色向在 A mazon EC2 实例上运行的应用程序授予权限。

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。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 AWS 形式存储在中。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。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。拥有该策略的用户可以从 AWS Management Console 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》中的使用客户托管策略定义自定义 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。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管策略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。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

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

访问控制列表 (ACLs)

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

Amazon S3 和 Amazon VPC 就是支持的服务示例 ACLs。 AWS WAF要了解更多信息 ACLs，请参阅《亚马逊简单存储服务开发者指南》中的访问控制列表 (ACL) 概述。

其他策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界：权限边界是一个高级特征，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 (SCPs) — SCPs 是 JSON 策略，用于指定中组织或组织单位 (OU) 的最大权限 AWS Organizations。 AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中

管理的服务。如果您启用组织中的所有功能，则可以将服务控制策略 (SCPs) 应用于您的任何或所有帐户。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organization SCPs s 和的更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略。

- 资源控制策略 (RCPs) — RCPs 是 JSON 策略，您可以使用它来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 限制成员账户中资源的权限，并可能影响身份（包括身份）的有效权限 AWS 账户根用户，无论这些身份是否属于您的组织。有关 Organizations 的更多信息 RCPs，包括 AWS 服务 该支持的列表 RCPs，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。

数据传输终端如何与 IAM 配合使用

在使用 IAM 管理数据传输终端的访问权限之前，请先了解哪些可用于数据传输终端的 IAM 功能。

IAM 特征	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
ACLs	否
ABAC（策略中的标签）	否
临时凭证	是

IAM 特征	数据传输终端支持
主体权限	否
服务角色	否
服务相关角色	否

要全面了解数据传输终端和其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中的与 IAM 配合使用的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

要查看数据传输终端基于身份的策略示例，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。当委托人和资源处于不同位置时

AWS 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

数据传输终端的政策措施

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。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列表，请参阅《服务授权参考》中的 “ AWS 数据传输终端定义的操作”。

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"
         ]
```

要查看数据传输终端基于身份的策略示例，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。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资源类型及其列表 ARNs，请参阅《服务授权参考》中的 “ AWS 数据传输终端定义的资源”。要了解您可以使用哪些操作来指定每种资源的 ARN，请参阅AWS 数据传输终端定义的操作。

要查看数据传输终端基于身份的策略示例，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密钥

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。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素（或 Condition 块）中，可以指定语句生效的条件。Condition 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 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，则使用逻辑OR运算来 AWS 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 支持全局条件密钥和特定于服务的条件密钥。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。

要查看数据传输终端条件键列表，请参阅《服务授权参考》中的 “AWS 数据传输终端条件密钥”。要了解可以使用条件键的操作和资源，请参阅AWS 数据传输终端定义的操作。

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

ACLs 在数据传输终端中

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。

带有数据传输终端的 ABAC

支持 ABAC（策略中的标签）：否

基于属性的访问控制（ABAC）是一种授权策略，该策略基于属性来定义权限。在中 AWS，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）和许多 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，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）。

在数据传输终端上使用临时证书

支持临时凭证：是

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关更多信息，包括哪些 AWS 服务 适用于临时证书，请参阅 IAM 用户指南中的AWS 服务 与 IAM 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的从用户切换到 IAM 角色（控制台）。

您可以使用 AWS CLI 或 AWS API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 AWS。 AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 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 用户或角色在中执行操作时 AWS，您被视为委托人。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 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 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中断数据传输终端的功能。只有在数据传输终端提供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服务相关联的 AWS 服务服务角色。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相关角色的权限。

有关创建或管理服务相关角色的详细信息，请参阅能够与 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，用户和角色无权创建或修改数据传输终端资源。他们也无法使用 AWS Management Console、 AWS Command Line Interface (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）。

有关由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》中的“AWS 数据传输终端的操作、资源和条件密钥”。 ARNs

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

基于身份的策略决定了某人是否可以在您的账户中创建、访问或删除数据传输终端资源。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：

- 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 托管式策略或工作职能的AWS 托管式策略。
- 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 AWS 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，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您的数据传输终端资源的详细信息 AWS 账户。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。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。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然可以使用数据传输终端控制台，还要将数据传输终端*ConsoleAccess*或*ReadOnly* AWS 托管策略附加到实体。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": "*"
        }
    ]
}
```

AWS 数据传输终端身份和访问疑难解答

使用以下信息来帮助您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
- 我想允许我以外的人 AWS 账户 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约，则可能没有所需的权限。请联系您的账户管理员配置授予您访问权限和相应权限的 IAM 身份策略。

我想允许我以外的人 AWS 账户 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 (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。

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，此页面可以帮助您了解 AWS 数据传输终端 API 操作、您可以授予权限的相应操作以及您可以为其授予权限的 AWS 资源之间的关系。

通常，以下是向策略中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。

您也可以在数据传输终端策略中使用 AWS 条件密钥。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 操作和相应操作

CreateTransferTeam

操作：`datatransferterminal:CreateTransferTeam`

资源： `None`

GetTransferTeam

操作：`datatransferterminal:GetTransferTeam`

资源： `arn:aws::$Partition:datatransferterminal:$Region:$Account:transfer-team/$TransferTeamId`

UpdateTransferTeam

操作：`datatransferterminal:UpdateTransferTeam`

资源： `arn:aws::$Partition:datatransferterminal:$Region:$Account:transfer-team/$TransferTeamId`

DeleteTransferTeam

操作：`datatransferterminal:DeleteTransferTeam`

资源： arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*

ListTransferTeams

操作：datatransferterminal:ListTransferTeams

资源： None

RegisterPerson

操作：datatransferterminal:RegisterPerson

资源： arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*

GetPerson

操作：datatransferterminal:GetPerson

资源： arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*/person/$*PersonId*

依赖操作：datatransferterminal:GetTransferTeam

依赖资源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*

DeregisterPerson

操作：datatransferterminal:DeregisterPerson

资源： arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*/person/$*PersonId*

依赖操作：datatransferterminal:GetTransferTeam

依赖资源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*

ListPersons

操作：datatransferterminal:ListPersons

资源： arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*

CreateReservation

操作：datatransferterminal:CreateReservation

资源： arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*

依赖操作：datatransferterminal:GetTransferTeam

依赖资源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*

依赖操作：datatransferterminal:GetPerson

依赖资源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*/person/$*PersonId*

依赖操作：datatransferterminal:GetFacility

依赖资源：arn:aws::$*Partition*:datatransferterminal:::facility/$*FacilityId*

GetReservation

操作：datatransferterminal:GetReservation

资源： arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*/reservation/$*ReservationId*

依赖操作：datatransferterminal:GetTransferTeam

依赖资源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*

UpdateReservation

操作：datatransferterminal:UpdateReservation

资源： arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*/reservation/$*ReservationId*

依赖操作：datatransferterminal:GetTransferTeam

依赖资源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*

依赖操作：datatransferterminal:GetPerson

依赖资源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*/person/$*PersonId*

DeleteReservation

操作：datatransferterminal:DeleteReservation

资源： arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*/person/$*PersonId*

依赖操作：datatransferterminal:GetTransferTeam

依赖资源：arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*

ListReservations

操作：datatransferterminal:ListReservations

资源： arn:aws::$*Partition*:datatransferterminal:$*Region*:$*Account*:transfer-team/$*TransferTeamId*

ListFacilities

操作：datatransferterminal:ListFacilities

资源： None

GetFacility

操作：datatransferterminal:GetFacility

资源： arn:aws::$*Partition*:datatransferterminal:::facility/$*FacilityId*

GetFacilityAvailability

操作：datatransferterminal:GetFacilityAvailability

资源： arn:aws::$*Partition*:datatransferterminal:::facility/$*FacilityId*/availability

依赖操作：datatransferterminal:GetFacility

依赖资源：arn:aws::$*Partition*:datatransferterminal:::facility/$*FacilityId*/availability

AWS 数据传输终端的合规性验证

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。 AWS 提供了以下资源来帮助实现合规性：

- 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 人都符合 HIPAA 资格。
- AWS 合AWS 规资源 — 此工作簿和指南集合可能适用于您的行业和所在地区。
- 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的最佳实践， AWS 服务 并将指南映射到跨多个框架（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)）的安全控制。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub— 这 AWS 服务 提供了您内部安全状态的全面视图 AWS。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 — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务 检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

AWS 数据传输终端的弹性

AWS 全球基础设施是围绕 AWS 区域 可用区构建的。 AWS 区域 提供多个物理隔离和隔离的可用区，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结构相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域 和可用区的更多信息，请参阅AWS 全球基础设施。

AWS 数据传输终端可在世界各地使用。您可以连接到任何 AWS 区域 可通过互联网访问的内容。

在数据传输终端中记录和监控

AWS 数据传输终端与 AWS CloudTrail一项服务集成，该服务提供用户、角色或 AWS 服务在数据传输终端中采取的操作的记录。 CloudTrail 将数据传输终端的所有 API 调用捕获为事件。捕获的调用包括来自数据传输终端控制台的调用和对数据传输终端 API 操作的代码调用。如果您创建跟踪，则可以将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括数据传输终端的事件。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，您可以确定向数据传输终端发出的请求、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。

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

中的数据传输终端信息 CloudTrail

CloudTrail 在您创建账户 AWS 账户 时已在您的账户上启用。当数据传输终端中发生活动时，该活动与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在中查看、搜索和下载最近发生的事件 AWS 账户。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

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

- 创建跟踪记录概述
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个地区的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail 日志文件

所有数据传输终端操作均由本指南的数据传输终端 API 参考：操作和资源部分记录 CloudTrail 并记录在案。

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 CloudTrail userIdentity 元素。

了解数据传输终端日志文件条目

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

AWS 数据传输终端的基础设施安全

作为一项托管服务， AWS 数据传输终端受到《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）生成临时安全凭证来对请求进行签名。

《数据传输终端用户指南》的文档历史记录

下表描述了《 AWS 数据传输终端用户指南》每个版本中的重要更改。如需对此文档更新的通知，您可以订阅 RSS 源。

更改	描述	日期
初次发布	原始文档发布日期。	2024 年 12 月
更新布局	更新了文档布局，并对措辞和内容进行了少量编辑。	2025 年 1 月

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。