aws

管理员指南

Amazon WorkSpaces 瘦客户机

Amazon WorkSpaces 瘦客户机: 管理员指南

Table of Contents

什么是 Amazon WorkSpaces 瘦客户机管理员控制台？

借助 Amazon WorkSpaces 瘦客户机管理员控制台，管理员可以通过 WorkSpaces 瘦客户机门户管理 WorkSpaces 瘦客户机环境和设备。通过此 Web 控制台，管理员可以在其网络中为 WorkSpaces 瘦客户机用户创建环境、管理设备和设置参数。

用于 WorkSpaces 瘦客户机的虚拟桌面环境必须在其自己的控制台中创建或修改。

> **Important**
>
> 要使 WorkSpaces 瘦客户机管理员控制台正常运行，您的系统必须首先满足特定要求。这些要求列在先决条件和配置中。

主题

您是 新用户吗？

如果您是首次使用 WorkSpaces 瘦客户机管理员控制台的用户，我们建议您先阅读以下章节：

- 启动 WorkSpaces 瘦客户机管理员控制台
- 使用 WorkSpaces 瘦客户机管理员控制台

架构

每个 WorkSpaces 瘦客户机都与一个虚拟桌面接口 (VDI) 提供商相关联。 WorkSpaces 瘦客户机支持三个 VDI 提供商：

- Amazon WorkSpaces
- AppStream 2.0
- Amazon WorkSpaces 安全浏览器

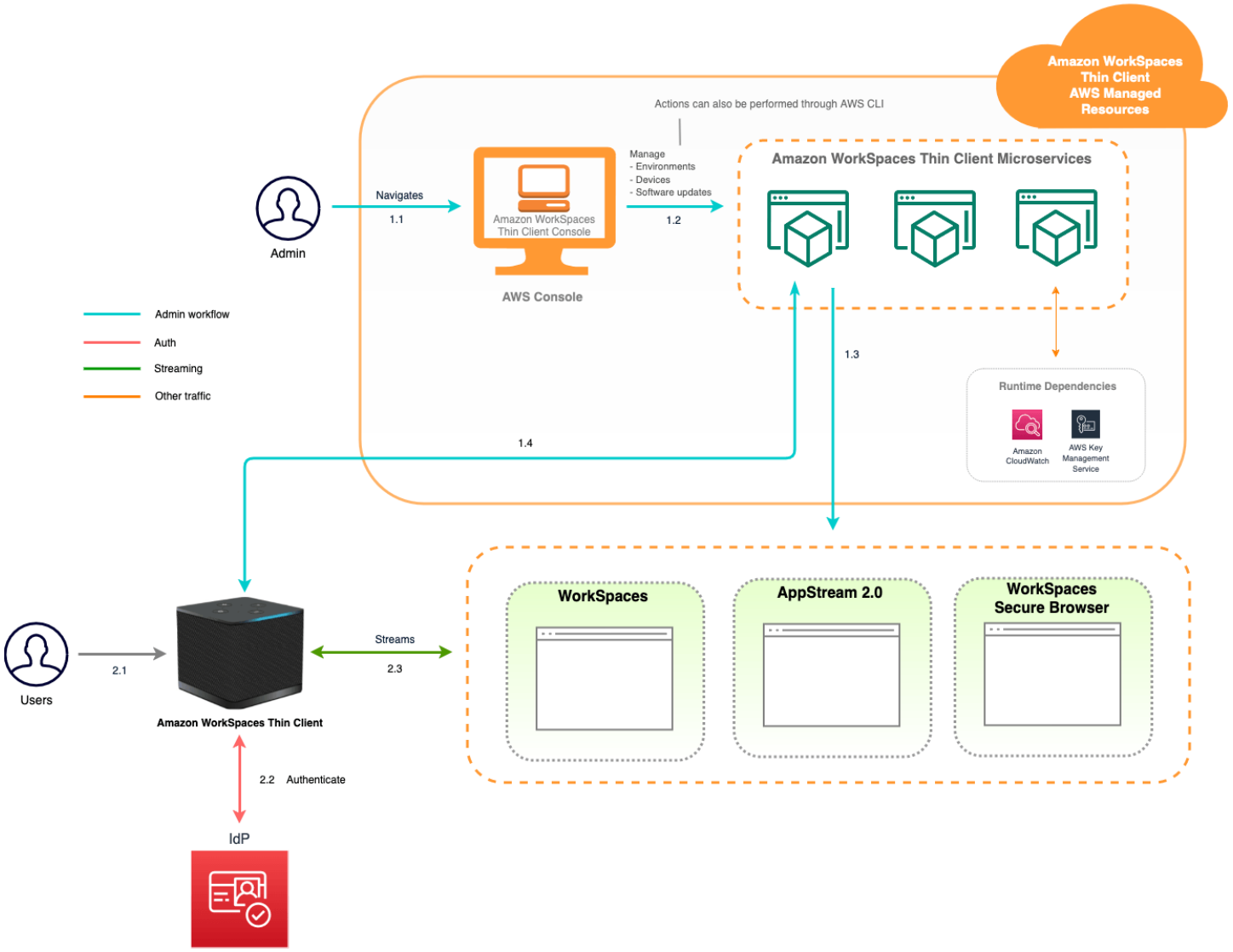
根据所使用的 VDI，您的 WorkSpaces 瘦客户机的信息可通过目录 WorkSpaces、 AppStream 2.0 的堆栈和 WorkSpaces 安全浏览器的门户端点进行访问和管理。

有关 Amazon 的更多信息 WorkSpaces，请参阅 WorkSpaces 快速设置入门。目录通过管理 AWS Directory Service，它提供以下选项：Simple AD、AD Connector 或 AWS Directory Service 微软 Active Directory（也称为 AWS 托管微软 AD）。有关更多信息，请参阅 AWS Directory Service 管理指南。

有关 AppStream 2.0 的更多信息，请参阅 Amazon AppStream 2.0 入门：使用示例应用程序进行设置。 AppStream 2.0 管理托管和运行应用程序所需的 AWS 资源，自动扩展，并按需向用户提供访问权限。 AppStream 2.0 允许用户在自己选择的设备上访问他们需要的应用程序，并提供响应灵敏、流畅的用户体验，与本机安装的应用程序没有区别。

有关 WorkSpaces 安全浏览器的信息，请参阅 Amazon WorkSpaces 安全浏览器入门。Amazon S WorkSpaces ecure Browser 是一项按需提供、完全托管的、基于 Linux 的服务，旨在促进浏览器安全访问内部网站和 (software-as-a-service SaaS) 应用程序。通过现有的 Web 浏览器访问服务，无需承担基础设施管理、专用客户端软件或虚拟专用网络（VPN）解决方案的管理负担。

下图显示了 WorkSpaces 瘦客户机的架构。


Amazon WorkSpaces Thin Client AWS Managed Resources
Actions can also be performed through AWS CLI
Admin
Navigates
1.1
Amazon WorkSpaces Thin Client Console
AWS Console
Manage
- Environments
- Devices
- Software updates
1.2
Amazon WorkSpaces Thin Client Microservices
1.3
Runtime Dependencies
Amazon CloudWatch
AWS Key Management Service
Admin workflow
Auth
Streaming
Other traffic
1.4
Users
2.1
Amazon WorkSpaces Thin Client
Streams
2.3
WorkSpaces
AppStream 2.0
WorkSpaces Secure Browser
2.2 Authenticate
IdP

设置 Amazon WorkSpaces 瘦客户机管理员控制台

主题

注册亚马逊云科技

如果您没有 AWS 账户，请完成以下步骤来创建一个。

报名参加 AWS 账户

1. 打开 https://portal.aws.amazon.com/billing/signup。
2. 按照屏幕上的说明进行操作。

   在注册时，将接到一通电话，要求使用电话键盘输入一个验证码。

   当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务 和资源。作为安全最佳实践，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。

创建 IAM 用户

要创建管理员用户，请选择以下选项之一。

选择一种方法来管理您的管理员	目的	方式	您也可以
在 IAM Identity Center 中	使用短期凭证访问 AWS。 这符合安全最佳实操。有关最佳实践的信息，	有关说明，请参阅《AWS IAM Identity Center 用户指南》中的入门。	通过在《AWS Command Line Interface 用户指南》 AWS IAM Identity Center中配置

选择一种方法来管理您的管理员	目的	方式	您也可以
（建议）	请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。		AWS CLI 要使用的来配置编程访问权限。
在 IAM 中 （不推荐使用）	使用长期凭证访问 AWS。	按照《IAM 用户指南》中的创建您的首个 IAM 管理员用户和组的说明操作。	按照《IAM 用户指南》中的管理 IAM 用户的访问密钥，配置编程式访问。

开始使用适用于 Amazon WorkSpaces 瘦客户机的 VDI

Amazon Th WorkSpaces in Client 是一款经济实惠的瘦客户机设备，专为与 AWS 最终用户计算服务配合使用而设计，可让您安全、即时地访问应用程序和虚拟桌面。

选择虚拟桌面基础架构 (VDI)，并将其配置为与 WorkSpaces 瘦客户机配合使用。

> **Important**
>
> 要使 WorkSpaces 瘦客户机管理员控制台正常运行，您的系统必须首先满足特定要求。这些要求列在每个虚拟桌面提供商的配置步骤中。

WorkSpaces 瘦客户机需要特定的软件配置，具体取决于您的虚拟桌面提供商。

主题

为 Amazon WorkSpaces 瘦客户机 WorkSpaces 进行配置

要在 Amazon 上使用 WorkSpaces 瘦客户机 WorkSpaces，需要将您的服务配置为访问 WorkSpaces 目录。Amazon WorkSpaces 是根据其在 AWS 控制台中的 WorkSpaces 瘦客户机创建环境页面上的目录名称列出的。

> **Note**
>
> 首次使用控制台之前必须进行配置。不建议您在开始使用控制台后修改任何必备功能。

开始前的准备工作

请确保您有一个可以创建或管理的 AWS 帐户 WorkSpace。但是，设备用户不需要 AWS 帐户即可连接和使用他们的 WorkSpaces。

在继续配置之前，请查看并理解以下概念：

- 启动时 WorkSpace，请选择一个 WorkSpace 捆绑包。有关更多信息，请参阅 Amazon WorkSpaces 捆绑包。
- 启动时 WorkSpace，请选择要与捆绑包一起使用的协议。有关更多信息，请参阅 Amazon 协议 WorkSpaces。
- 启动时 WorkSpace，请为每个用户指定个人资料信息，包括用户名和电子邮件地址。用户通过创建密码来完成其个人资料。有关 WorkSpaces 和用户的信息存储在目录中。有关更多信息，请参阅管理目录 WorkSpaces。
- 启动时 WorkSpace，请启用并配置 WorkSpaces Web 访问权限。有关更多信息，请参阅启用和配置 Amazon WorkSpaces Web Access

步骤 1：验证您的系统是否满足 WorkSpaces 所需功能

为了使 WorkSpaces 瘦客户机管理员控制台能够在 Amazon 上正常运行 WorkSpaces，您的系统必须满足以下特定要求。下表列出了所有这些支持的功能及其要求。

功能	要求
Web 访问	已启用
支持的操作系统	• Windows 10 • Windows 10（自带许可证） • Windows 11 • Windows 11（自带许可证）
支持的捆绑包	• 微软 Power 搭载 Windows 10（基于 2016 年、2019 年和 2022 年的服务器） • 微软 Power 搭载 Windows 10（基于 2016 年、2019 年和 2022 年的服务器）w Office • 微软 PowerPro 搭载 Windows 10（基于 2016 年、2019 年和 2022 年的服务器） • 微软 PowerPro 搭载 Windows 10（基于 2016 年、2019 年和 2022 年的服务器）w Office • 微软在 Windows 10 上的性能（基于 2016 年、2019 年和 2022 年的服务器）

功能	要求
	• 微软在 Windows 10 上的性能（基于 2016 年、2019 年和 2022 年的服务器）w Office
支持的协议	仅限 WSP

第 2 步：使用高级设置启动你的 WorkSpace

使用高级设置启动你的 WorkSpace

1. 打开 WorkSpaces 控制台，网址为https://console.aws.amazon.com/workspaces/。
2. 选择以下目录类型之一，然后选择下一步：
   - 亚马逊云科技的 Microsoft AD
   - Simple AD
   - AD Connector
3. 输入目录信息。
4. 从两个不同的可用区选择 VPC 中的两个子网。有关更多信息，请参阅配置具有公有子网的 VPC。
5. 查看您的目录信息，然后选择创建目录。

为 Amazon WorkSpaces 瘦客户机配置 AppStream 2.0

AppStream 2.0 实例将根据堆栈名称列出，并且需要在创建环境页面上配置 IdP 登录 URL。由于 AppStream 2.0 版 SAML 身份验证仅支持初始身份验证，因此管理员必须手动输入正确的登录 URL。

> **Note**
>
> 首次使用控制台之前必须进行配置。不建议您在开始使用控制台后修改任何必备功能。

步骤 1：验证您的系统是否满足 AppStream 2.0 要求的功能

为了使 WorkSpaces 瘦客户机管理员控制台能够正常使用 AppStream 2.0，您的系统必须满足以下特定要求。下表列出了所有这些支持的功能及其要求。

功能	要求
身份提供商	转到《AppStream 2.0 管理员指南》中的 “设置 SAML”，创建身份提供商。 当提示创建环境控制台时，输入您的 IDP 登录 URL。
操作系统	Windows
平台类型	Windows Server（2012 R2、2016 或 2019）
流协议	TCP 流式传输 提供 UDP 不可用时自动回退到 TCP 的机制。
本地复制和粘贴	禁用 在 AppStream 2.0 堆栈级别进行配置
本地文件夹共享	禁用 在 AppStream 2.0 堆栈级别进行配置
本地打印	禁用 在 AppStream 2.0 堆栈级别进行配置

还支持在 AppStream 2.0 上通过 SAML 身份验证实现屏幕锁定要求。 WorkSpaces 瘦客户机不支持用户池和编程身份验证机制。

第 2 步：设置 AppStream 2.0 堆栈

要流式传输应用程序， AppStream 2.0 需要一个包含与堆栈关联的队列以及至少一个应用程序映像的环境。按照以下步骤设置队列和堆栈，并允许用户访问堆栈。如果您尚未这样做，我们建议您尝试使用 AppStream 2.0 入门：使用示例应用程序进行设置中的步骤。

如果要创建要使用的映像，请参阅教程：使用 2.0 控制台创建自定义 AppStream AppStream 2.0 镜像。

如果您计划将实例集加入到 Active Directory 域中，请先配置您的 Active Directory 域，然后完成下列步骤。有关更多信息，请参阅 AppStream 2.0 中使用 Active Directory。

任务

- 创建实例集
- 创建堆栈
- 向用户提供访问权
- 清理资源

为亚马逊 WorkSpaces 瘦客户机配置亚马逊 WorkSpaces 安全浏览器

Amazon WorkSpaces Secure Browser 基于其在 AWS 控制台中的 WorkSpaces 瘦客户机创建环境页面上的门户终端节点。

> **Note**
>
> 首次使用控制台之前必须进行配置。不建议您在开始使用控制台后修改任何必备功能。

第 1 步：验证您的系统是否满足 Amazon WorkSpaces 安全浏览器所需的功能

要使 WorkSpaces 瘦客户机管理员控制台与 Amazon WorkSpaces 安全浏览器一起正常运行，您的系统必须满足以下特定要求。下表列出了所有这些支持的功能及其要求。

功能	要求
本地复制和粘贴	禁用
本地文件夹共享	禁用

> **Note**
>
> WorkSpaces 瘦客户机目前不支持用于单点登录 WorkSpaces 的安全浏览器扩展。

步骤 2：设置 WorkSpaces 安全浏览器门户

WorkSpaces 瘦客户机在特定配置下与 WorkSpaces 安全浏览器 VPC 配合使用：

1. 使用 AWS CodeBuild Cloudformation 模板创建 VPC。
2. 设置身份提供程序。
3. 创建 Amazon WorkSpaces 安全浏览器门户。
4. 测试您的新 Amazon WorkSpaces 安全浏览器门户。

启动 WorkSpaces 瘦客户机管理员控制台

WorkSpaces 瘦客户机是一款经济实惠的瘦客户机设备，专为与 AWS 最终用户计算服务配合使用而设计，可让您安全、即时地访问应用程序和虚拟桌面。

主题

覆盖区域

WorkSpaces 瘦客户机在以下区域可用。

这些区域中只有 WorkSpaces 瘦客户机管理员控制台可用。 WorkSpaces 瘦客户机设备目前仅在美国、德国、法国、意大利和西班牙上市。

区域名称	区域	终端节点	控制台链接
美国东部（弗吉尼亚州北部）	us-east-1	thinclient.us-east-1.amazonaws.com	https://us-east-1.console.aws.amazon.com/workspaces-thin-client/home
美国西部（俄勒冈州）	us-west-2	thinclient.us-west-2.amazonaws.com	https://us-west-2.console.aws.amazon.com/workspaces-thin-client/home
亚太地区（孟买）	ap-south-1	thinclient.ap-south-1.amazonaws.com	https://ap-south-1.console.aws.amazon.com/workspaces-thin-client/home
欧洲地区（爱尔兰）	eu-west-1	thinclient.eu-west-1.amazonaws.com	https://eu-west-1.console.aws.amazon.com/workspaces-thin-client/home

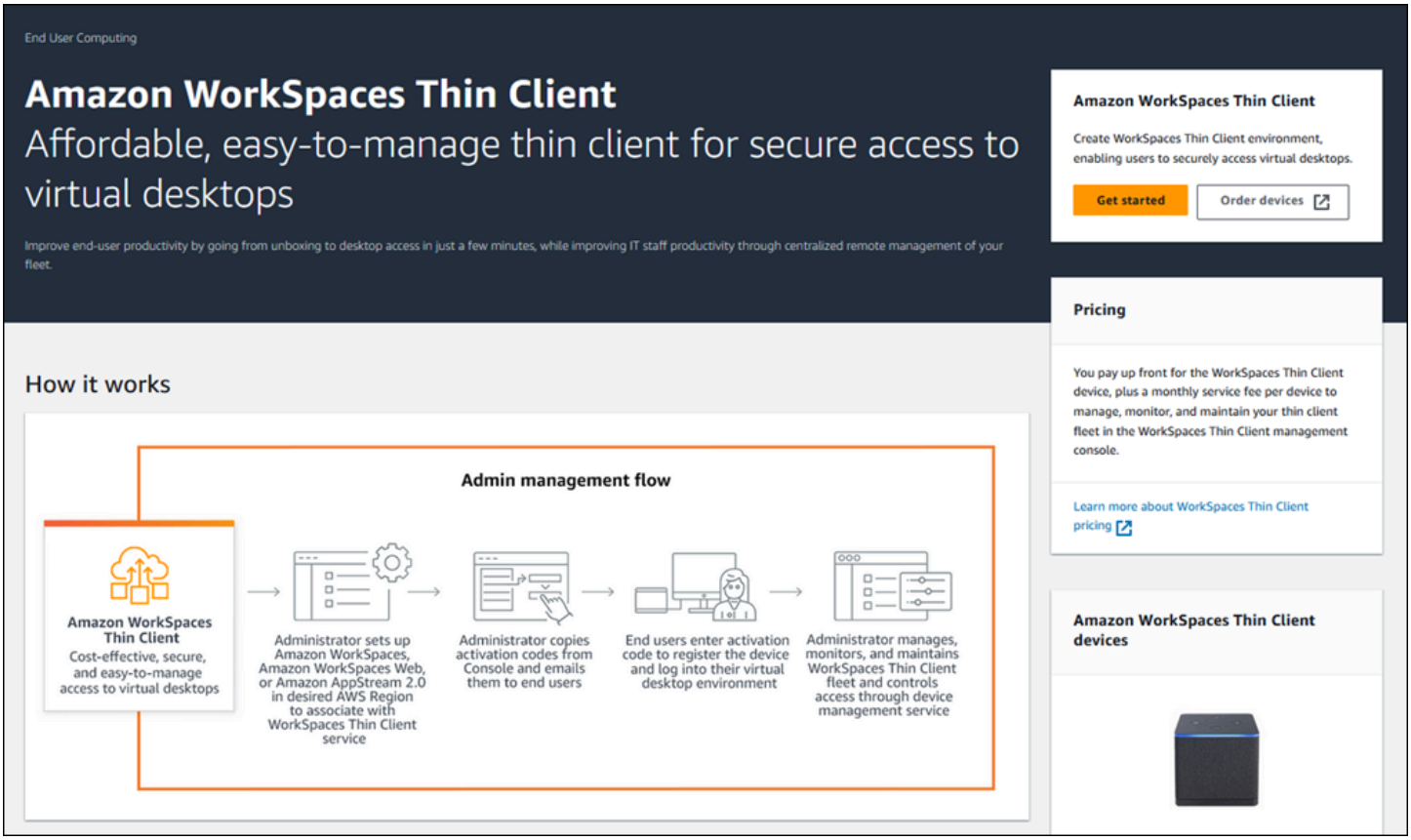
区域名称	区域	终端节点	控制台链接
加拿大（中部）	ca-central-1	thinclient.ca-central-1.amazonaws.com	https://ca-central-1.console.aws.amazon.com/workspaces-thin-client/home
欧洲地区（法兰克福）	eu-central-1	thinclient.eu-central-1.amazonaws.com	https://eu-central-1.console.aws.amazon.com/workspaces-thin-client/home
欧洲地区（伦敦）	eu-west-2	thinclient.eu-west-2.amazonaws.com	https://eu-west-2.console.aws.amazon.com/workspaces-thin-client/home

启动 WorkSpaces 瘦客户机管理员控制台

拥有 AWS 帐户后，您可以启动管理员控制台并转到 WorkSpaces 瘦客户机控制台。要启动控制台，请执行以下操作：

1. 登录您的 AWS 账户。
2. 访问WorkSpaces 瘦客户机控制台。
3. 选择开始使用，您将被定向到环境。

使用 WorkSpaces 瘦客户机管理员控制台



欢迎使用 WorkSpaces 瘦客户机管理员控制台！

在这里，您可以为团队管理您的 WorkSpaces 精简客户机设备和环境。

有关 WorkSpaces 瘦客户机设备的信息，请参阅WorkSpaces 瘦客户机用户指南。

我们开始吧。

主题

- 环境
- 设备
- 软件更新

环境

每台 WorkSpaces 瘦客户机设备都使用单独的虚拟桌面环境来访问其在线资源。用户使用以下虚拟桌面提供商之一访问此环境：

- Amazon WorkSpaces
- AppStream 2.0
- Amazon WorkSpaces 安全浏览器

环境列表

环境列表详细信息

名称 – 与此环境关联的唯一标识符。

虚拟桌面服务 – 此环境使用的虚拟桌面提供程序。

虚拟桌面服务 ID-虚拟桌面服务提供商分配给该环境的唯一标识符。

激活码-最终用户用于访问虚拟桌面环境的代码。

设备计数-访问此环境的 WorkSpaces 瘦客户机设备的数量。

环境列表操作

搜索 – 搜索您管理的所有环境。

刷新 – 刷新环境列表。

查看详细信息 – 显示环境详细信息。

操作-打开一个下拉列表，您可以在其中编辑或删除环境。

创建环境 – 启动创建环境的流程

创建环境 – 启动创建环境的流程。

主题

- 环境详细信息
- 创建环境
- 编辑环境

- 删除环境

环境详细信息

选择环境时，WorkSpaces 瘦客户机控制台会显示该环境的详细信息供您查看。控制台还会显示有关该环境使用的虚拟桌面提供商的详细信息。

主题

- Summary
- 虚拟桌面环境详细信息

Summary

名称 – 与此环境关联的唯一标识符。

虚拟桌面服务 – 此环境使用的虚拟桌面提供程序。

虚拟桌面服务 ID-虚拟桌面服务提供商分配给该环境的唯一标识符。

激活码 – 最终用户使用此代码访问虚拟桌面环境。

始终保留软件 up-to-date-此设置启用软件自动更新。

维护时段开始时间-每周开始自动软件更新的时间。

维护时段结束时间-每周自动软件更新完成的时间。

一周中的维护时段天数 – 软件自动进行更新的天数。

关联设备-访问此环境的 WorkSpaces 瘦客户机设备的数量。

创建时间-创建此环境的日期和时间。

虚拟桌面环境详细信息

Amazon WorkSpaces 目录详情

目录 ID-与此环境关联的 Amazon WorkSpaces 目录。

目录名称-与此 Amazon WorkSpaces 目录关联的唯一标识符。

组织名称-控制 Amazon WorkSpaces 目录的组织名称。

目录类型-Amazon WorkSpaces 目录的格式。

已注册-此 Amazon WorkSpaces 目录是否已注册。

状态-此 Amazon WorkSpaces 目录是否处于活动状态。

Amazon WorkSpaces 安全浏览器门户网站详情

名称-与此 Amazon WorkSpaces 安全浏览器门户相关的唯一标识符。

创建时间-创建此 AppStream 2.0 堆栈的日期和时间。

Web 门户端点 – 用于访问您的虚拟桌面环境的 url。

AppStream 2.0 详情

堆栈名称-与此 AppStream 2.0 堆栈关联的唯一标识符。

IdP 登录网址-用于登录和退出 AppStream 2.0 堆栈的身份提供商网址。

创建时间-创建此 AppStream 2.0 堆栈的日期和时间。

创建环境

首先，每台设备都需要 AWS 最终用户计算服务。 WorkSpaces 瘦客户机使用以下服务：

- Amazon WorkSpaces 通过分配的目录
- AppStream 2.0 通过分配的堆栈
- 通过门户网站地址访问亚马逊 WorkSpaces 安全浏览器

您必须为现有环境分配服务或创建一个新环境。

> **Note**
>
> WorkSpaces 瘦客户机仅显示同一区域中的虚拟桌面。

主题

步骤 1：输入环境详细信息

1. 在环境详细信息字段中输入环境的名称。
2. 要设置自动软件补丁，请选中 “始终保留软件” 复选框 up-to-date。

> **Note**
>
> 如果未启用自动软件更新，则注册到该环境的设备将不会收到软件更新，除非您手动推送更新，或者软件已过期，系统会强制更新。
> 此外，设备的软件集版本由系统决定。此版本可能不是最新版本。

3. 选择您想要为环境安排维护时段的时间。
   - 应用系统范围的维护窗口-每周在确定的时间自动更新环境软件。
   - 应用自定义维护时段 – 设置希望每周更新环境软件的日期和时间。
4. 选择虚拟桌面服务。
   - Amazon WorkSpaces
   - Amazon WorkSpaces 安全浏览器
   - AppStream 2.0

步骤 2：选择虚拟桌面提供程序

你必须有一项服务才能让你的用户访问他们的虚拟桌面和兼容的资源。

> **Important**
>
> 要使 WorkSpaces 瘦客户机管理员控制台正常运行，您的系统必须满足特定要求。这些要求列在先决条件和配置中。
> 在设置主机之前，请确保您的系统满足这些要求。

使用亚马逊 WorkSpaces

Amazon WorkSpaces 是一项适用于 Windows 的完全托管的桌面虚拟化服务，使您能够从任何支持的设备访问资源。

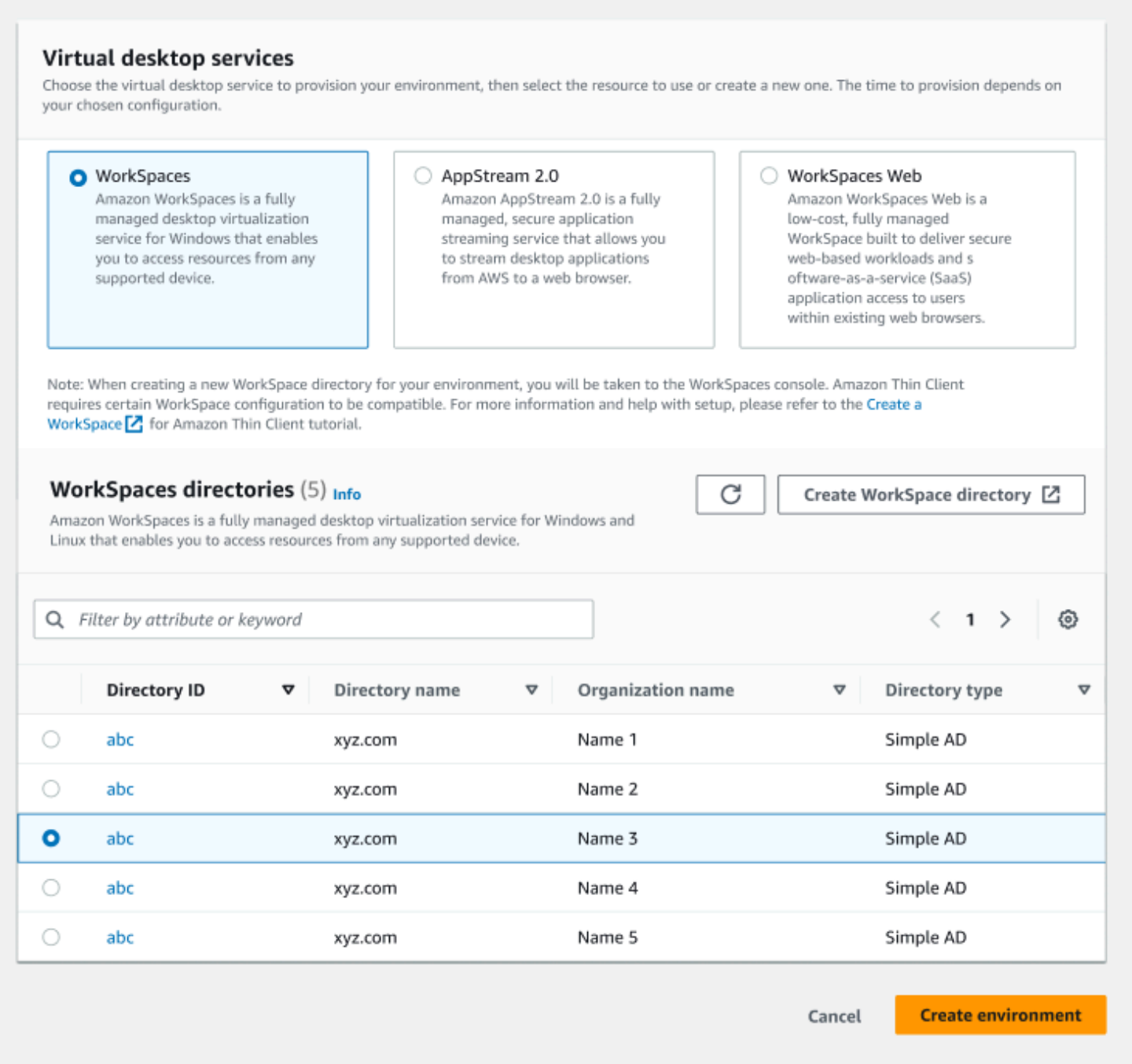
1. 要使用 Amazon WorkSpaces，请执行以下任一操作：

- 选择想要用于您的环境的目录。您可以浏览下拉列表，也可以使用搜索字段搜索目录。

  > **Note**
  >
  > 如果您在列表中看不到现有目录，请在 WorkSpaces 管理控制台中验证其是否符合 WorkSpaces 瘦客户机要求。

- 通过选择 “创建目录” 按钮来创建 WorkSpaces 目录。有关创建 WorkSpaces 目录的更多信息，请参阅管理目录 WorkSpaces。

2. 选择 “创建环境” 按钮。



创建环境时，您仍然可以稍后编辑详细信息。有关更多信息，请参阅编辑环境。

正在使用 AppStream 2.0

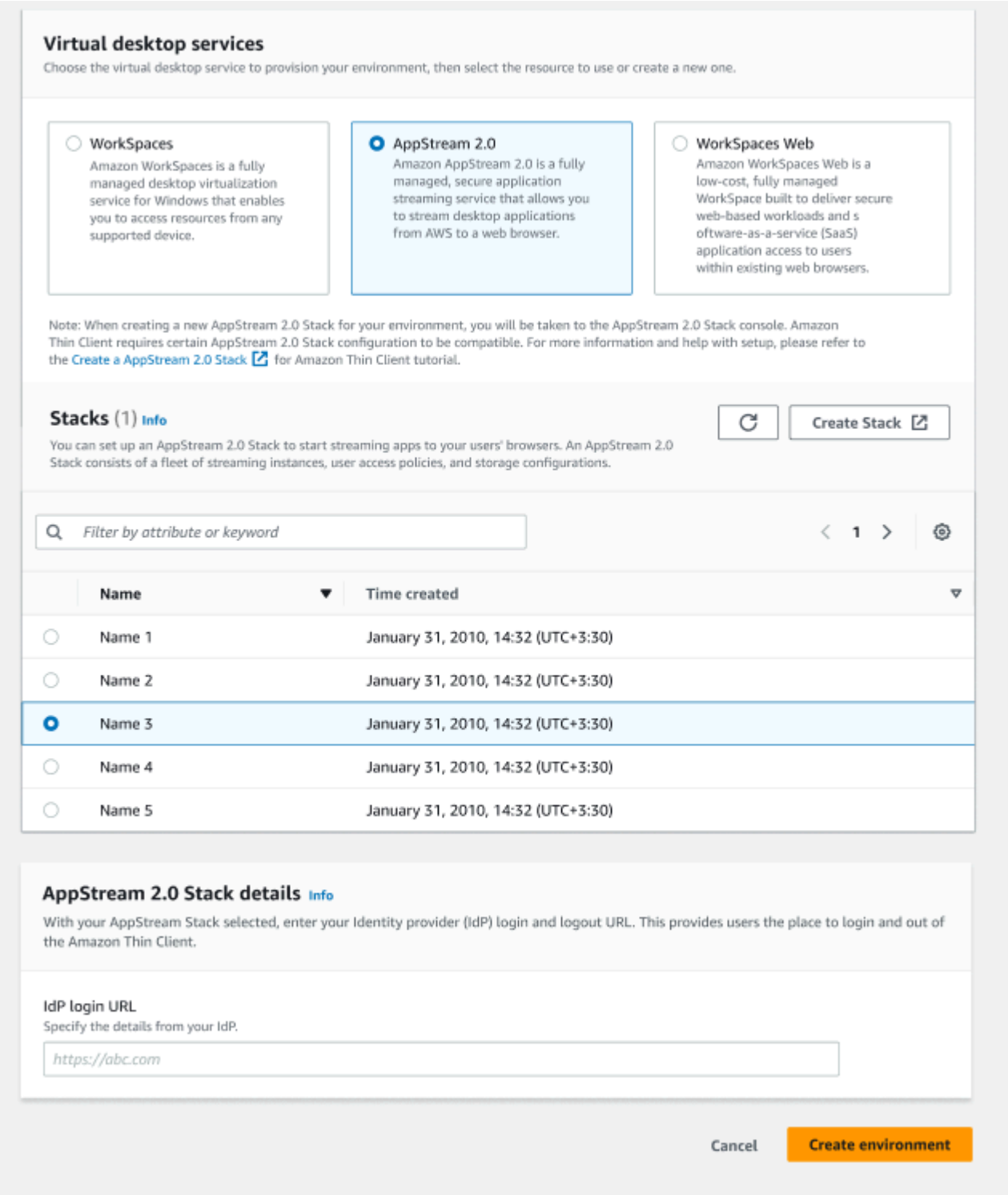
AppStream 2.0 是一项完全托管的安全应用程序流服务，可用于将桌面应用程序从流式传输 AWS 到 Web 浏览器。

> **Warning**
>
> 要创建 AppStream 2.0 环境，必须`cli_follow_urlparam`将设置为`false`。为此，请执行以下操作：
>
> - 对于默认配置文件，运行 `aws configure set cli_follow_urlparam false`。
> - 对于名为 `ProfileName` 的配置文件，运行 `aws configure set cli_follow_urlparam false --profile ProfileName`。

1. 要设置 AppStream 2.0，请执行以下任一操作：
   - 选择想要用于您的环境的堆栈。您可以浏览下拉列表，也可以使用搜索字段搜索堆栈。

     > **Note**
     >
     > 如果您在列表中看不到现有的堆栈，请在 AppStream 2.0 管理控制台中验证它是否符合 WorkSpaces 瘦客户机要求。

   - 通过选择 “创建堆栈” 按钮来创建堆栈。有关创建 AppStream 2.0 堆栈的更多信息，请参阅创建堆栈。
2. 在 IdP 登录 URL 字段中输入您的身份提供程序登录和注销 URL。这为用户提供了登录和退出 WorkSpaces 瘦客户机的地方。
3. 选择 “创建环境” 按钮。



创建环境后，您仍然可以稍后编辑详细信息。有关更多信息，请参阅编辑环境。

使用 Amazon WorkSpaces 安全浏览器

Amazon S WorkSpaces ecure Browser 是一款低成本、完全托管的 WorkSpaces 控制台，旨在为使用现有网络浏览器的用户提供安全的基于 Web 的工作负载和软件即服务 (SaaS) 应用程序访问权限。

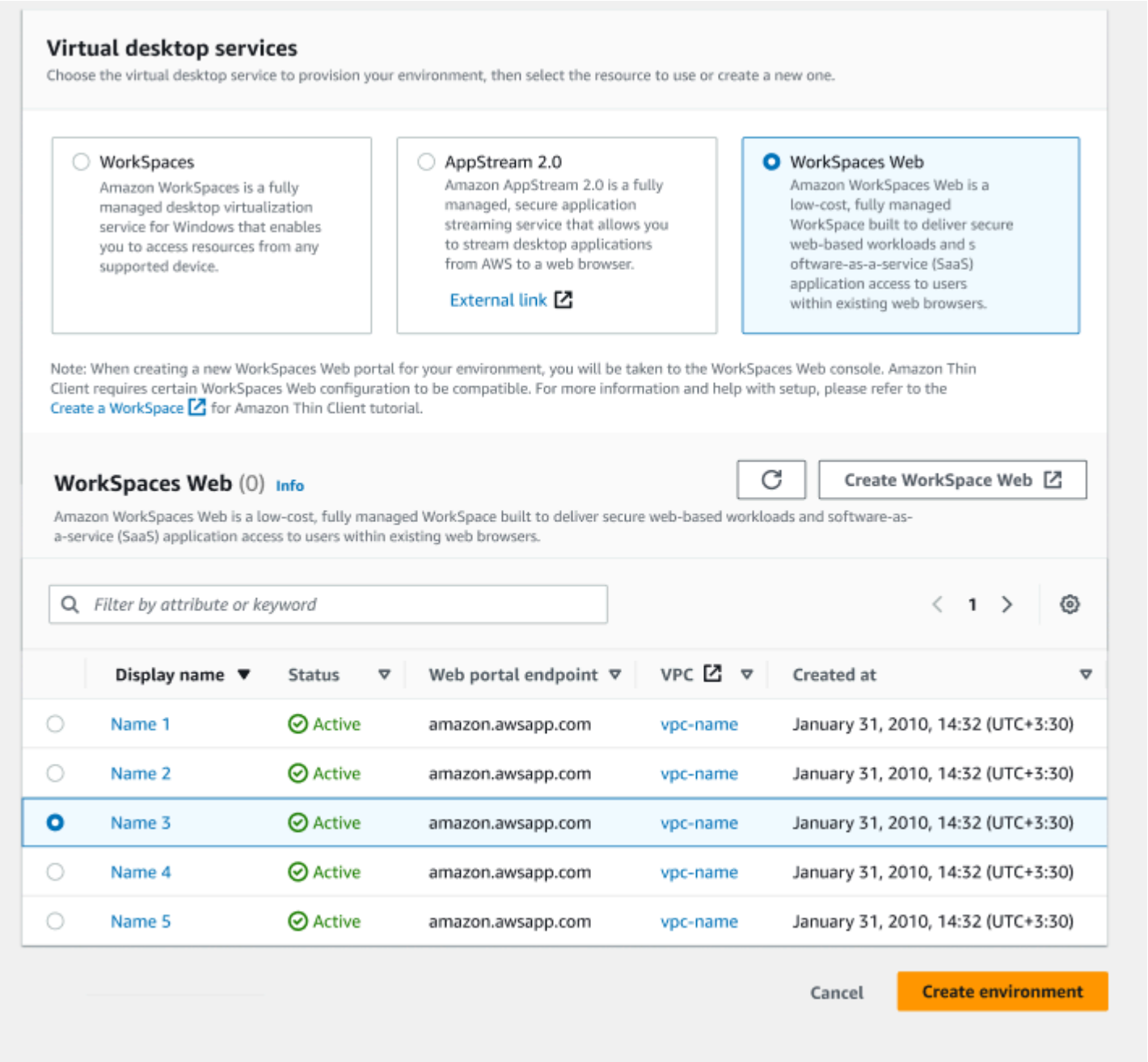
1. 要设置 Amazon WorkSpaces 安全浏览器，请执行以下任一操作：

   - 选择要用于您的环境的 Web 门户。您可以浏览下拉列表，也可以使用搜索字段搜索门户。

     > **Note**
     >
     > 如果您在列表中看不到现有的 Web 门户，请在 WorkSpaces 安全浏览器管理控制台中确认其是否符合 WorkSpaces 瘦客户机要求。

   - 选择 “创建 WorkSpaces 安全浏览器” 按钮创建 Web 门户。有关创建 WorkSpaces 安全浏览器门户的更多信息，请参阅设置 Amazon WorkSpaces 安全浏览器。

2. 选择 “创建环境” 按钮。



创建环境后，您仍然可以稍后编辑详细信息。有关更多信息，请参阅编辑环境。

步骤 3：将激活码发送给您的设备用户

设置环境和虚拟桌面服务后，您将在 AWS 管理控制台上收到一个用于设置的唯一激活码。

向任何 WorkSpaces 瘦客户机设备用户提供此激活码，他们就可以使用它来访问其虚拟桌面。

有关如何帮助您的设备用户设置 Amazon WorkSpaces 瘦客户机的更多信息，请参阅 WorkSpaces 瘦客户机用户指南。

编辑环境

WorkSpaces 瘦客户机管理控制台为个人用户管理虚拟桌面环境。通过此控制台，您可以编辑或删除虚拟桌面环境。

1. 选择想要编辑的环境。

> **Note**
>
> 您可以浏览下拉列表，也可以使用搜索字段搜索环境。

2. 选择 “操作” 按钮。
3. 从下拉列表中选择 “编辑”。您将被定向到 “编辑环境” 窗口。
4. 编辑以下任一项：
   - 在环境名称字段中更改环境的名称。
   - 更改自动软件补丁更新的软件更新详细信息复选框。
   - 更改想要为您的环境安排维护时段的时间。
5. 选择 “编辑环境” 按钮。

删除环境

> **Note**
>
> 如果环境中注册了任何设备，则无法删除该环境。首先，您必须取消注册并删除环境中的所有设备。

1. 选择想要删除的环境。您可以浏览下拉列表，也可以使用搜索字段搜索环境。
2. 选择 “操作” 按钮。
3. 从下拉列表中选择 “删除”。将出现 “删除环境” 确认窗口。
4. 在确认字段中键入“delete”。
5. 选择删除按钮。

设备

每个 WorkSpaces 瘦客户机最终用户都有一台专用设备，用于将他们连接到其虚拟桌面环境和在线资源。这些设备通过AWS 站点上的 WorkSpaces 瘦客户机管理员控制台进行管理。

您可以通过此控制台为您的团队订购设备。

设备列表

设备列表详细信息

设备 ID – 分配给单个设备的标识号。

设备名称-（可选）您为设备提供的唯一名称。

活动状态-设备的当前状态。有两种状态状态：

- 活动 – 过去 7 天内至少连接过一次网络。
- 非活动 – 过去 7 天内未连接到网络。

注册状态-确认设备已设置完毕、已与此 AWS 账户关联且属于特定环境。它可以处于以下状态之一：

- 已注册-这是默认状态。
- 取消注册-设备正处于 “重置和注销” 流程。

> **Note**
>
> 如果设备处于注销状态，则可以将其删除。

- 已取消注册 – 设备已成功取消注册。

> **Note**
>
> 只有当设备处于 “注销注册” 或 “已注销” 状态时，您才能将其删除。

- 已存档 – 设备已存档。

环境 ID – 此设备所连接环境的标识符。

软件合规性 – 设备软件的合规状态。有两种状态状态：

- 合规
- 不合规

设备列表操作

搜索 – 搜索您管理的所有设备。

刷新 – 刷新设备列表。

查看详细信息 – 显示设备详细信息。

操作-打开一个下拉列表，您可以在其中执行以下操作：

- 编辑设备名称
- 取消注册
- 档案
- 删除
- 导出设备详细信息

订购设备 – 开始订购设备的过程。

主题

设备详细信息

Summary

设备序列号-分配给单个设备的标识号。

ARN-设备的唯一标识符，采用亚马逊资源名称 (ARN) 格式。

设备名称-您为设备提供的名称。如果您尚未创建名称，则可以为其命名，否则它将获得默认名称。

设备类型-与账户关联的最终用户设备的类型。

活动状态 – 此设备的当前状态。两种状态状态是：

- 处于活动状态
- Inactive

环境 ID-设备使用的环境的标识号。

注册状态-确认设备已设置完毕、已与此 AWS 账户关联且属于特定环境。它可以处于以下四种状态之一：

- 已注册-这是默认状态。
- 取消注册-设备正处于 “重置和注销” 流程。
- 已取消注册 – 设备已成功取消注册。

> **Note**
>
> 只有当设备处于 “已注销” 或 “已存档” 状态时，您才能将其删除。

- 已存档-管理员已将此设备标记为当前未投入使用。

注册起始时间 – 设备激活的日期。

上次登录 – 最近登录的日期和时间。

上次检查姿势的时间为-最近一次设备签到的日期和时间。

当前软件版本 – 此设备当前使用的软件版本。

计划进行软件更新-设备上预设的软件版本。

软件合规性 – 确认软件集有效。有两种状态状态：

- 合规

- 不合规

用户日志

上次访问设备-上次使用此设备的日期和时间。

编辑设备名称

1. 选择要编辑的设备。您可以浏览下拉列表，也可以使用搜索字段搜索设备。
2. 选择 “操作” 按钮。
3. 从下拉列表中选择 “编辑设备名称”。将出现 “编辑设备名称” 窗口。
4. 在设备名称确认字段中输入新设备名称。
5. 选择保存按钮。

重置和取消注册设备

1. 选择要取消注册的设备。您可以浏览下拉列表，也可以使用搜索字段搜索设备。
2. 选择 “操作” 按钮。
3. 从下拉列表中选择 “取消注册”。将出现 “取消注册” 窗口。
4. 在确认字段中输入“deregister”。
5. 选择取消注册按钮。

> **Note**
>
> 取消注册会强制注销用户，并要求在会话中途重新启动其 WorkSpaces 瘦客户机设备。

存档设备

1. 选择要存档的设备。您可以浏览下拉列表，也可以使用搜索字段搜索设备。
2. 选择 “操作” 按钮。
3. 从下拉列表中选择 “存档”。将出现 “存档” 窗口。
4. 在确认字段中输入“reset and archive”。
5. 选择重置和存档按钮。

> **Note**
>
> 存档设备会强制用户注销，并要求在会话中途重新启动他们的 WorkSpaces 瘦客户机设备。

删除设备

1. 选择要删除的设备。您可以浏览下拉列表，也可以使用搜索字段搜索设备。
2. 选择 “操作” 按钮。
3. 从下拉列表中选择 “删除”。将出现 “删除” 窗口。
4. 在确认字段中键入“delete”。
5. 选择删除按钮。

> **Note**
>
> 成功删除设备后，用户必须将 WorkSpaces 瘦客户机设备退还给 Amazon。

导出设备详细信息

1. 选择要从中导出详细信息的设备。您可以浏览下拉列表，也可以使用搜索字段搜索设备。
2. 选择 “操作” 按钮。
3. 从下拉列表中选择 “导出设备详细信息”。所选设备的详细信息以电子表格格式下载。

软件更新

WorkSpaces Thin Client 有时需要软件更新以引入新功能并应用安全补丁。这些更新由版本控制的软件集表示。

软件集可以包含 WorkSpaces 瘦客户机设备的软件应用程序或操作系统的更新。通过此控制台，您可以选择立即更新软件，也可以安排在环境维护时段内进行自动更新。

有关已发布的软件集列表，请参阅 WorkSpaces 瘦客户机环境软件集。

主题

- 更新环境软件

- 更新设备软件
- WorkSpaces 瘦客户机软件版本

更新环境软件

WorkSpaces 瘦客户机是一项 AWS 最终用户计算服务，可为用户提供对虚拟桌面的访问权限。这些虚拟桌面会定期使用新的软件集进行更新。要更新环境软件，请执行以下操作：

1. 从可用的软件更新列表中选择软件集。有关软件集的列表，请参阅WorkSpaces 瘦客户机环境软件集。
2. 选择 “安装” 按钮。
3. 选择页面顶部的环境。
4. 从 “环境” 部分的列表中选择要更新的环境。
5. 通过选择以下选项之一，在计划更新中选择何时更新环境：
   - 立即更新软件 – 开始更新所有已注册设备上的环境软件。

     > **Note**
     >
     > 立即更新软件可能会中断任何活跃的用户会话。

   - 在每个环境维护窗口期间更新软件-在环境的计划维护时段内更新环境软件。
6. 选中该复选框以授权更新。必须选中此复选框才能更新软件。
7. 选择 “安装” 按钮。

更新设备软件

WorkSpaces 瘦客户机是一项 AWS 最终用户计算服务，它提供的瘦客户机设备可将用户连接到专用的虚拟桌面。这些设备会定期使用新软件进行更新。要更新设备软件，请执行以下操作：

1. 从可用的软件更新列表中选择软件集。
2. 选择 “安装” 按钮。
3. 选择页面顶部的设备。
4. 从 “设备” 部分的列表中选择要更新的设备。有关软件集的列表，请参阅WorkSpaces 瘦客户机环境软件集。

5. 通过选择以下选项之一，从计划更新选项中选择何时更新环境：

   - 立即更新软件 – 立即更新设备软件。

     > **Note**
     >
     > 立即更新软件可能会中断任何活跃的用户会话。

   - 在每个设备维护时段内更新软件-在设备的预定维护时段内更新环境软件。

6. 选中该复选框以授权更新。必须选中此复选框才能更新软件。
7. 选择 “安装” 按钮。

WorkSpaces 瘦客户机软件版本

WorkSpaces Thin Client 是一项 AWS 最终用户计算服务，它允许用户访问设备上的虚拟桌面。这些设备会定期使用新的软件集进行更新。下表描述了所有已发布的软件集。管理员可以使用AWS 管理控制台查看可用的软件集。

软件套装	发行日期	更改
2.5.0	06-13-2024	• 修复了设备在启动会话之前从睡眠中醒来时会短暂显示键盘和鼠标设置屏幕的问题。 • 设备工具栏上的 “主页” 按钮已重命名为 “登录”。 • 改善会话中音频/视频通话的性能。
2.4.3	05-29-2024	• 修复 Chromium 的 CVE-2024-5274 严重安全问题的未修补程序。
2.4.2	05-17-2024	• 修复 Chromium 的 CVE-2024-4947 严重安全问题的未修补程序。

软件套装	发行日期	更改
2.4.1	05-15-2024	• 修复 Chromium 的 CVE-2024-4671 和 CVE-2024-4761 关键安全问题的未修补漏洞。 • 修复了允许右键单击 WorkSpaces 登录页面上的 AWS 和 Privacy 链接以独立模式打开浏览器的问题。
2.4.0	05-09-2024	• 修复了屏蔽 “accounts .google.com” 并禁止使用 Google Workspace 作为 2.0 会话的 IDP 的问题。AppStream • 只要点击屏幕上的任何区域，设备设置工具栏就会自动折叠。
2.3.0	04-05-2024	• 设备设置显示在折叠的工具栏中，可以更好地利用可见屏幕。 • 现在，最终用户可以配置设备在处于非活动状态时进入睡眠状态之前的等待时间。 • 修复了第二个显示屏上显示 “about: blank” 网址的问题。 • 修复了关闭扩展显示屏时出现白屏的问题。 • 现在，终端用户设置的音量在设备重启后仍然保留。

软件套装	发行日期	更改
2.2.1	02-16-2024	• 修复了登录过程中出现的问题，该问题导致用户无法登录 WorkSpaces 配置了 SAML 2.0 身份验证。
2.2.0	02-08-2024	• 增加了对具有英语（英国）、法语、德语、意大利语、西班牙语区域设置的 ISO 键盘的支持。
2.1.2	01-26-2024	• 修复 Chromium 的 CVE-2024-0519 严重安全问题的未修补程序。 • 改善了与锁定功能相关的最终用户延迟。 • 面向设备的内部端点已切换到 “thinclient*” 域。
2.1.1	12-21-2023	• 修复 Chromium 的 CVE-2023-7024 严重安全问题的未修补程序。
2.1.0	12-20-2023	• 在设备设置中添加主页按钮，并启用对元密钥的支持。这允许终端用户通过按 Meta+L 来调用锁定屏幕。
2.0.1	12-06-2023	• 修复 Chromium 的 CVE-2024-6345 严重安全问题的未修补程序。
2.0.0	11-15-2023	• 初始版本

在 WorkSpaces 瘦客户机资源上使用标签

您可以通过将自己的元数据作为标签分配给每个资源来组织和管理 WorkSpaces 瘦客户机的资源。可为每个标签指定键 和值。键可以是具有特定关联值的一般类别，例如“project”、“owner”或“environment”。您可以使用标签作为管理 AWS 资源和组织数据（包括账单数据）的简单而强大的方式。

向现有资源添加标签时，这些标签直到下个月的第一天才会出现在成本分配报告中。例如，如果您在 7 月 15 日向现有 WorkSpaces 瘦客户机设备添加标签，则这些标签要等到 8 月 1 日才会出现在您的成本分配报告中。有关更多信息，请参阅 AWS 账单用户指南中的使用成本分配标签。

> **Note**
>
> 要在 Cost Explorer 中查看您的 WorkSpaces 瘦客户机资源标签，必须按照用户指南中激活用户定义的成本分配标签中的说明激活已应用于 WorkSpaces 瘦客户机资源的标签。AWS Billing 标签会在激活 24 小时后出现，但与这些标签关联的值可能需要 4-5 天才能显示在 Cost Explorer 中。此外，要在 Cost Explorer 中显示和提供成本数据，已标记的 WorkSpaces 瘦客户机资源必须在此期间产生费用。Cost Explorer 仅显示标签激活时的成本数据。目前没有可用的历史数据。

您可以标记的资源：

- 在创建以下资源时，可以为它们添加标签：WorkSpaces 瘦客户机环境。
- 您可以为以下类型的现有资源添加标签：WorkSpaces 瘦客户机环境、设备和软件集。

标签限制

- 每个资源的标签数上限 – 50
- 最大密钥长度-128 个 Unicode 字符
- 最大值长度-256 个 Unicode 字符
- 标签键和值区分大小写。允许使用的字符包括可用 UTF-8 格式表示的字母、空格和数字，以及以下特殊字符： + - = 。 _ : / @。请不要使用前导空格或尾随空格。
- 请勿在标签名称或值中使用`aws:`前缀，因为它已保留供 AWS 使用。您无法编辑或删除带此前缀的标签名称或值。

使用控制台更新现有环境的标签

1. 打开WorkSpaces 瘦客户机控制台。
2. 选择环境以打开其详细信息页面
3. 选择编辑。
4. 在 “标签” 部分，执行以下一项或多项操作：。
   - 要添加标签，请选择添加新标签，然后编辑键和值的值。
   - 要更新标签，请编辑 “值” 的值。
   - 要删除标签，请选择标签旁边的移除。
5. 更新完标签后，选择 “保存”。

使用控制台更新现有设备的标签

1. 打开WorkSpaces 瘦客户机控制台。
2. 选择设备以打开其详细信息页面。
3. 选择标签。
4. 选择管理标签。
5. 执行以下一个或多个操作：
   - 要添加标签，请选择添加新标签，然后编辑键和值的值。
   - 要更新标签，请编辑 “值” 的值。
   - 要删除标签，请选择标签旁边的移除。
6. 更新完标签后，选择 “保存”。

使用控制台更新软件更新的标签

1. 打开WorkSpaces 瘦客户机控制台。
2. 选择软件更新以打开其详细信息页面。
3. 在标签部分中，选择管理标签。
4. 执行以下一个或多个操作：
   - 要添加标签，请选择添加新标签，然后编辑键和值的值。
   - 要更新标签，请编辑 “值” 的值。

- 要删除标签，请选择标签旁边的移除。

5. 更新完标签后，选择 “保存”。

Amazon WorkSpaces 瘦客户机中的安全

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 Cloud。 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 Amazon Th WorkSpaces in Client 的合规计划，请参阅按合规计划提供的范围内的AWSAWS 服务按合规计划服务。
- 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 WorkSpaces 瘦客户机时如何应用分担责任模型。以下主题向您介绍如何配置 WorkSpaces 瘦客户机以满足您的安全和合规性目标。您还可以学习如何使用其他 AWS 服务来帮助您监控和保护您的 WorkSpaces 瘦客户机资源。

主题

Amazon WorkSpaces 瘦客户机中的数据保护

AWS 分担责任模型分担责任模型适用于 Amazon Th WorkSpaces in Client 中的数据保护。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 Cloud。您负责维护对托管在此基础设施上的内容的控制。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 安全性博客 上的 AWS 责任共担模式和 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。我们还建议您通过以下方式保护数据：

- 对每个账户使用 multi-factor authentication（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。
- 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 140-2 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 140-2 版》。

我们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 SDK AWS 服务 使用 WorkSpaces 瘦客户机或其他客户端时。 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。

Amazon Th WorkSpaces in Client 收集并提供有关用户使用 WorkSpaces 瘦客户机设备及其与虚拟桌面服务交互的信息。例如，可用内存、网络诊断、网络信息、设备连接、SAML 凭据、设备识别信息和崩溃报告。这些信息用于为您提供服务，并可能用于改善用户对服务的体验。此外，仅为了向您提供服务，信息可能会转移到用户使用该服务的 AWS 地区之外。我们根据AWS 隐私声明处理这些信息。

主题

数据加密

WorkSpaces 瘦客户机收集环境和设备自定义数据，例如用户设置、设备标识符、身份提供商信息和流式桌面标识符。 WorkSpaces 瘦客户机还会收集会话时间戳。收集的数据存储在亚马逊 DynamoDB 和亚马逊 S3 中。 WorkSpaces 瘦客户机使用 AWS 密钥管理服务 (KMS) Management Service 进行加密。

要保护您的内容，请遵循以下指南进行操作：

- 实现最低权限访问权限并创建用于 WorkSpaces 瘦客户机操作的特定角色。
- end-to-end 通过提供客户管理的密钥来保护数据，这样 Th WorkSpaces in Client 就可以使用您提供的密钥对您的静态数据进行加密。
- 请谨慎共享环境激活码和用户凭证：
  - 管理员需要登录到 WorkSpaces 瘦客户机控制台，用户需要提供激活码，以便 WorkSpaces 瘦客户机设置使用凭据登录流媒体桌面。
  - 任何具有物理访问权限的人都可以设置 WorkSpaces 瘦客户机，但是除非他们拥有有效的激活码和用户凭据可供登录，否则他们无法启动会话。
- 用户可以通过使用设备工具栏选择锁定屏幕、重启或关闭设备来明确结束会话。这将丢弃设备会话并清除会话凭证。

WorkSpaces 默认情况下，瘦客户机通过使用 KMS 加密所有敏感数据来保护内容和元数据。 AWS 如果应用现有设置时出错，则用户将无法访问新会话，设备也无法应用软件更新。

Amazon WorkSpaces 瘦客户机的静态数据加密

Amazon Th WorkSpaces in Client 默认提供加密，通过使用 AWS 自有的加密密钥保护敏感的静态客户数据。

- AWS 自有密钥 — Amazon Th WorkSpaces in Client 默认使用这些密钥来自动加密个人身份数据。您无法查看、管理或使用 AWS 拥有的密钥，也无法审核其使用情况。但是，无需采取任何措施或更改任何计划即可保护用于加密数据的密钥。有关更多信息，请参阅《AWS Key Management Service 开发人员指南》中的 AWS 拥有的密钥。

默认情况下，静态数据加密有助于降低保护敏感数据的操作开销和复杂性。同时，它还支持构建符合严格加密合规性和监管要求的安全应用程序。

虽然您无法禁用此加密层或选择备选加密类型，但您可以在创建 Thin Client 环境时选择客户托管密钥，从而在现有亚马逊云科技拥有的加密密钥上添加第二层加密：

- 客户托管密钥 — Amazon Th WorkSpaces in Client 支持使用您创建、 AWS 拥有和管理的对称客户托管密钥，以便在现有自有加密的基础上添加第二层加密。由于您可以完全控制此加密层，因此可以执行以下任务：
  - 制定和维护关键策略

- 制定和维护 IAM policy 和授权
- 启用和禁用密钥策略
- 轮换密钥加密材料
- 添加标签
- 创建密钥别名
- 计划要删除的密钥

有关更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的客户托管密钥。

下表汇总了 Amazon WorkSpaces 瘦客户机如何加密个人身份数据。

数据类型	AWS 拥有的密钥加密	客户托管密钥加密（可选）
环境名称 WorkSpaces 瘦客户机环境名称	已启用	已启用
设备名称 WorkSpaces 瘦客户机设备名称	已启用	已启用

> **Note**
>
> Amazon Th WorkSpaces in Client 使用 AWS 自有密钥自动启用静态加密，从而免费保护个人身份数据。
> 但是，使用客户托管密钥需支付 AWS KMS 费用。有关定价的更多信息，请参阅 Key Management Service 定价。

Amazon WorkSpaces 瘦客户机如何在 AWS KMS 中使用授权

Amazon Th WorkSpaces in Client 需要您获得授权才能使用您的客户托管密钥。

当您创建使用客户托管密钥加密的 WorkSpaces 瘦客户机环境时，Amazon Th WorkSpaces in Client 会通过向 AWS KMS 发送 CreateGrant 请求来代表您创建授权。 AWS KMS 中的授权用于授予亚马逊 WorkSpaces 瘦客户机访问客户账户中的 KMS 密钥的权限。

当使用客户托管密钥将新的瘦客户机设备注册到 WorkSpaces 瘦客户机加密环境中，并且该设备的名称发生更改时，Amazon Th WorkSpaces in Client 会通过向 AWS KMS 发送 CreateGrant 请求来代表您创建授权。 AWS KMS 中的授权用于授予亚马逊 WorkSpaces 瘦客户机访问客户账户中的 KMS 密钥的权限。

Amazon Th WorkSpaces in Client 需要获得授权，才能使用您的客户托管密钥进行以下内部操作：

- 向 AWS KMS 发送解密请求以解密加密的数据

您可以随时撤消对授权的访问权限，也可以随时删除该服务对客户托管密钥的访问权限。如果您这样做，Amazon Th WorkSpaces in Client 将无法访问由客户托管密钥加密的任何数据，这会影响依赖该数据的操作。例如，如果您尝试获取 Amazon Th WorkSpaces in Client 无法访问的环境详细信息，则该操作会返回`AccessDeniedException`错误。此外， WorkSpaces 瘦客户机设备将无法使用 WorkSpaces 瘦客户机环境。

创建客户托管密钥

您可以使用 AWS 管理控制台或 KMS API 操作创建对称客户托管 AWS 密钥。

创建对称的客户托管式密钥：

根据《AWS Key Management Service 开发人员指南》https://docs.aws.amazon.com/kms/latest/developerguide/overview.html中创建对称的客户托管密钥的步骤操作。

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该密钥以及如何使用该密钥的声明。创建客户托管密钥时，可以指定密钥策略。有关更多信息，请参阅《AWS Key Management Service 开发人员指南》https://docs.aws.amazon.com/kms/latest/developerguide/overview.html中的管理对客户托管密钥的访问权限。

要将您的客户托管密钥用于您的 Amazon WorkSpaces 瘦客户机资源，密钥政策中必须允许以下 API 操作：

- `kms:DescribeKey`— 提供客户托管的密钥详细信息，以便 Amazon T WorkSpaces hin Client 可以验证密钥。

- kms:GenerateDataKey– 允许使用客户托管的密钥对数据进行加密。
- kms:Decrypt– 允许使用客户托管的密钥来解密数据。
- kms:CreateGrant– 向客户托管密钥添加授权。授予对指定 KMS 密钥的控制访问权限，从而允许访问 Amazon Th WorkSpaces in Client 所需的授权操作。有关使用授权的更多信息，请参阅《AWS Key Management Service 开发人员指南》https://docs.aws.amazon.com/kms/latest/developerguide/overview.html。

  这允许 Amazon WorkSpaces 瘦客户机执行以下操作：

  - 调用 Decrypt 以解密加密的数据。

以下是您可以为 Amazon WorkSpaces 瘦客户机添加的政策声明示例：

```
{
    "Statement": [
        {
            "Sid": "Allow access to principals authorized to use Amazon WorkSpaces Thin
 Client",
            "Effect": "Allow",
            "Principal": {"AWS": "*"},
            "Action": [
                "kms:DescribeKey",
                "kms:GenerateDataKey",
                "kms:Decrypt",
                "kms:CreateGrant"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "thinclient.region.amazonaws.com",
                    "kms:CallerAccount": "111122223333"
                }
            }
        },
        {
            "Sid": "Allow access for key administrators",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
            "Action": ["kms:*"],
            "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
        },
        {
```

```
            "Sid": "Allow read-only access to key metadata to the account",
            "Effect": "Allow",
            "Principal": {"AWS": "arn:aws:iam::111122223333:root"},
            "Action": [
                "kms:Describe*",
                "kms:Get*",
                "kms:List*",
                "kms:RevokeGrant"
            ],
            "Resource": "*"
        }
    ]
}
```

有关在策略中指定权限的更多信息，请参阅《AWS Key Management Service 开发人员指南》https://docs.aws.amazon.com/kms/latest/developerguide/overview.html。

有关密钥访问故障排除的更多信息，请参阅《AWS Key Management Service 开发人员指南》https://docs.aws.amazon.com/kms/latest/developerguide/overview.html。

为 WorkSpaces 瘦客户机指定客户管理的密钥

您可以指定客户托管密钥作为以下资源的第二层加密：

- WorkSpaces 瘦客户机环境

创建环境时，您可以通过提供数据密钥来指定数据密钥`kmsKeyArn`，Amazon Th WorkSpaces in Client 使用该密钥来加密可识别的个人数据。

- `kmsKeyArn`— AWS KMS 客户托管密钥的密钥标识符。提供密钥 ARN。

将新的 WorkSpaces 瘦客户机设备添加到使用客户管理密钥加密的 WorkSpaces 瘦客户机环境时，WorkSpaces 瘦客户机设备将继承 WorkSpaces 瘦客户机环境中的客户托管密钥设置。

加密上下文是一组可选的键值对，其中包含有关数据的其他上下文信息。

AWS KMS 使用加密上下文作为额外的经过身份验证的数据来支持经过身份验证的加密。当您在加密数据的请求中包含加密上下文时， AWS KMS 会将加密上下文绑定到加密数据。要解密数据，请在请求中包含相同的加密上下文。

Amazon WorkSpaces 瘦客户机加密上下文

Amazon Th WorkSpaces in Client 在所有 AWS KMS 加密操作中使用相同的加密环境，其中密钥为`aws:thinclient:arn`，值为亚马逊资源名称 (ARN)。

以下是环境加密上下文：

```
"encryptionContext": {
    "aws:thinclient:arn": "arn:aws:thinclient:region:111122223333:environment/
environment_ID"
}
```

以下是设备加密上下文：

```
"encryptionContext": {
    "aws:thinclient:arn": "arn:aws:thinclient:region:111122223333:device/device_ID"
}
```

使用加密上下文进行监控

当您使用对称客户托管密钥加密 WorkSpaces 瘦客户机环境和设备数据时，您还可以使用审计记录和日志中的加密上下文来识别客户托管密钥的使用情况。加密上下文还会显示在 AWS CloudTrail 或 Amazon CloudWatch 日志生成的日志中。

使用加密上下文控制对客户托管密钥的访问

您可以使用密钥策略和 IAM 策略中的加密上下文作为条件来控制对您的对称客户托管密钥的访问。您也可以在授予中使用加密上下文约束。

Amazon Th WorkSpaces in Client 在授权中使用加密上下文限制来控制对您账户或区域中客户托管密钥的访问权限。授权约束要求授权允许的操作使用指定的加密上下文。

以下是密钥策略语句示例，用于授予对特定加密上下文的客户托管密钥的访问权限。此策略语句中的条件要求 `kms:Decrypt` 调用具有指定加密上下文的加密上下文约束。

```
{
    "Sid": "Enable Decrypt to access Thin Client Environment",
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"},
    "Action": "kms:Decrypt",
    "Resource": "*",
    "Condition": {
```

```
        "StringEquals": {"kms:EncryptionContext:aws:thinclient:arn":
 "arn:aws:thinclient:region:111122223333:environment/environment_ID"}
    }
}
```

监控您的 Amazon WorkSpaces 瘦客户机加密密钥

当您在亚马逊 WorkSpaces 瘦客户机资源中使用 AWS KMS 客户托管密钥时，您可以使用 AWS CloudTrail 或 Amazon CloudWatch Logs 来跟踪亚马逊 WorkSpaces 瘦客户端向 AWS KMS 发送的请求。

以下示例是DescribeKey、、、CreateGrantGenerateDataKeyDecrypt、Decrypt（使用Grant）监控 Amazon Th WorkSpaces in Client 为访问由您的客户托管密钥加密的数据而调用的 KMS 操作 AWS CloudTrail 的事件：

在以下示例中，您可以看到encryptionContext WorkSpaces 瘦客户机环境的示例。 WorkSpaces 瘦客户机设备也会记录类似 CloudTrail 的事件。

DescribeKey

Amazon Th WorkSpaces in Client 使用该DescribeKey操作来验证 AWS KMS 客户托管密钥。

以下示例事件记录了 DescribeKey 操作：

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-21T13:43:33Z",
```

```
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:22Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {"keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"},
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

CreateGrant

Amazon Th WorkSpaces in Client 使用该`CreateGrant`操作创建 KMS 授权，允许您在设备访问数据时解密数据。

以下示例事件记录了 `CreateGrant` 操作：

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
```

```
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-21T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:23Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "granteePrincipal": "thinclient.eu-west-1.amazonaws.com",
        "operations": ["Decrypt"],
        "retiringPrincipal": "thinclient.eu-west-1.amazonaws.com",
        "constraints": {
            "encryptionContextSubset": {"aws:thinclient:arn":
 "arn:aws:thinclient:eu-west-1:111122223333:environment/abcSAMPLE"}
        },
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": {
        "grantId":
 "0ab0ac0d0b000f00ea00cc0a0e00fc00bce000c000f0000000c0bc0a0000aaafSAMPLE",
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": false,
```

```
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

GenerateDataKey

Amazon WorkSpaces 瘦客户机使用该GenerateDataKey操作来加密数据。

以下示例事件记录了 GenerateDataKey 操作：

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2024-03-12T12:21:03Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
```

```
    "eventTime": "2024-03-12T13:03:56Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
        },
        "numberOfBytes": 32
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Decrypt

Amazon WorkSpaces 瘦客户机使用该Decrypt操作来解密数据。

以下示例事件记录了 Decrypt 操作：


```
{
    "eventVersion": "1.08",
    "userIdentity": {
```

```
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE:Sampleuser01",
                "arn": "arn:aws:sts::111122223333:assumed-role/Admin/Sampleuser01",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-11-21T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:25Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE",
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
         },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
```

```
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Decrypt (using Grant)

当 WorkSpaces 瘦客户机设备访问环境或设备信息时，将使用该`Decrypt`操作，该操作通过 KMS 密钥`Grant`允许。

以下示例事件记录了通过以下方式授权的`Decrypt`操作`Grant`：

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2023-11-21T13:44:23Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "eu-west-1",
    "sourceIPAddress": "thinclient.amazonaws.com",
    "userAgent": "thinclient.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws-crypto-public-key": "ABC123def4567890abc12345678/90dE/F123abcDEF
+4567890abc123D+ef1==",
            "aws:thinclient:arn": "arn:aws:thinclient:eu-
west-1:111122223333:environment/abcSAMPLE"
        },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
    },
    "responseElements": null,
```

```
    "requestID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:eu-
west-1:111122223333:key/1234abcd-12ab-34cd-56ef-123456SAMPLE"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "ff000af-00eb-00ce-0e00-ea000fb0fba0SAMPLE",
    "eventCategory": "Management"
}
```


了解更多

以下资源提供有关静态数据加密的更多信息：

- 有关 Amazon Key Management Service 基本概念的更多信息，请参阅《AWS Key Management Service 开发人员指南》https://docs.aws.amazon.com/kms/latest/developerguide/overview.html。
- 有关 AWS Key Management Service 安全最佳实践的更多信息，请参阅AWS 密钥管理服务开发人员指南。

传输中加密

WorkSpaces 瘦客户机对通过 HTTPS 和 TLS 1.2 传输的数据进行加密。您可以使用控制台或直接 API 调用向 WorkSpaces 瘦客户机发送请求。传输的请求数据通过通过 HTTPS 或 TLS 连接发送进行加密。请求数据可以从 AWS 控制台、 AWS 命令行界面或 AWS SDK 传输到 WorkSpaces 瘦客户端。这还包括设备上的任何软件更新。

默认配置传输中的加密，默认配置安全连接（HTTPS、TLS）。

密钥管理

您可以提供自己的客户托管 AWS KMS 密钥来加密您的客户信息。如果您不提供密钥， WorkSpaces 瘦客户机将使用 AWS 自有密钥。您可以使用 AWS SDK 设置密钥。

互联网工作流量隐私

管理员可以查看 WorkSpaces 瘦客户机会话事件，包括启动时间和待处理的软件更新信息。这些日志经过加密，并在 WorkSpaces 瘦客户机控制台中安全地传送给客户。用户信息和有关单个流式桌面会话的更多详细信息由桌面服务记录。有关更多信息，请参阅监控您的 WorkSpaces、 AppStream 2.0 版的监控和报告或适用于 WorkSpaces Web 的用户访问日志记录。

Amazon WorkSpaces 瘦客户机的身份和访问管理

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 WorkSpaces 瘦客户端资源。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) 会有所不同，具体取决于您在 WorkSpaces 瘦客户机中所做的工作。

服务用户-如果您使用 WorkSpaces 瘦客户机服务完成工作，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 WorkSpaces 瘦客户机功能来完成工作时，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 WorkSpaces 瘦客户机中的某项功能，请参阅对 Amazon WorkSpaces 瘦客户机身份和访问进行故障排除。

服务管理员-如果您负责公司的 WorkSpaces 瘦客户机资源，则可能拥有对 WorkSpaces 瘦客户机的完全访问权限。您的工作是确定您的服务用户应访问哪些 WorkSpaces 瘦客户机功能和资源。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 WorkSpaces 瘦客户端一起使用，请参阅Amazon WorkSpaces 瘦客户机如何与 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 WorkSpaces 瘦客户端的访问权限。要查看您可以在 IAM 中使用的基于 WorkSpaces 瘦客户端身份的策略示例，请参阅。Ama WorkSpaces zon 瘦客户机的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，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 用户指南中的签署 AWS API 请求。

无论使用何种身份验证方法，您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》中的在 AWS中使用多重身份验证（MFA）。

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，我们建议您使用 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，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，如果有一些特定的使用场景需要长期凭证以及 IAM 用户，我们建议轮换访问密钥。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场景定期轮换访问密钥。

IAM 组是一个用于指定一组 IAM 用户的身份。您不能使用群组的身份登录。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担任。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》中的何时创建 IAM 用户（而不是角色）。

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。您可以 AWS Management Console 通过切换角色在中临时担任 IAM 角色。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》中的使用 IAM 角色。

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。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制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 用户或角色可代入 IAM 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）访问账户中的资源。角色是授予跨账户存取权限的主要方式。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 角色与基于资源的策略有何不同。

- 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 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，此操作然后在不同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个操作的权限。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 服务服务可以担任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 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证书。这优先于在 EC2 实例中存储访问密钥。要向 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建附加到该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 角色为 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是 IAM 用户，请参阅《IAM 用户指南》中的何时创建 IAM 角色（而不是用户）。

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 策略概述。

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 policy。然后，管理员可以向角色添加 IAM policy，并且用户可以代入角色。

IAM policy 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、用户群组或角色）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 创建 IAM policy。

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、群组或角色中。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。要了解如何在托管式策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管式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 (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，尽管它们不使用 JSON 策略文档格式。

Amazon S3 和 Amazon VPC 就是支持 ACL 的服务示例。 AWS WAF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。您可以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 JSON 策略，用于指定组织或组织单位 (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。如果您在组织内启用了特征，则可对任意或全部账户应用服务控制策略 (SCP)。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关组织和 SCP 的更多信息，请参阅《AWS Organizations 用户指南》中的 SCP 的工作原理。
- 会话策略——会话策略是当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。

Amazon WorkSpaces 瘦客户机如何与 IAM 配合使用

在使用 IAM 管理 WorkSpaces 瘦客户端访问权限之前，请先了解有哪些 IAM 功能可用于 WorkSpaces 瘦客户端。

您可以在 Amazon WorkSpaces 瘦客户机上使用的 IAM 功能

IAM 功能	WorkSpaces 瘦客户机支持
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	支持
ACL	否
ABAC（策略中的标签）	支持

IAM 功能	WorkSpaces 瘦客户机支持
临时凭证	是
主体权限	支持
服务角色	否
服务相关角色	不支持

要全面了解 WorkSpaces 瘦客户端和其他 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。

瘦客户机的基于身份的 WorkSpaces 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》中的创建 IAM 策略。

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。

瘦客户机的基于身份的 WorkSpaces 策略示例

要查看 WorkSpaces 瘦客户机基于身份的策略的示例，请参阅。Ama WorkSpaces zon 瘦客户机的基于身份的策略示例

WorkSpaces 瘦客户机中基于资源的策略

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。

要启用跨账户存取，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 角色与基于资源的策略有何不同。

WorkSpaces 瘦客户机的策略操作

支持策略操作	支持

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 WorkSpaces 瘦客户机操作列表，请参阅《服务授权参考》中的 Amazon WorkSpaces 瘦客户机定义的操作。

WorkSpaces 瘦客户机中的策略操作在操作前使用以下前缀：

```
workspaces-thin-client
```

要在单个语句中指定多个操作，请用逗号分隔它们，如以下示例所示：

```
"Action": [
      "workspaces-thin-client:action1",
      "workspaces-thin-client:action2"
         ]
```

要查看 WorkSpaces 瘦客户机基于身份的策略的示例，请参阅。Ama WorkSpaces zon 瘦客户机的基于身份的策略示例

WorkSpaces 瘦客户机的策略资源

支持策略资源	支持

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 WorkSpaces 瘦客户机资源类型及其 ARN 的列表，请参阅《服务授权参考》中的 Amazon WorkSpaces 瘦客户机定义的资源。要了解您可以使用哪些操作来指定每种资源的 ARN，请参阅 Amazon Th WorkSpaces in Client 定义的操作。

要查看 WorkSpaces 瘦客户机基于身份的策略的示例，请参阅。Ama WorkSpaces zon 瘦客户机的基于身份的策略示例

WorkSpaces 瘦客户机的策略条件密钥

支持特定于服务的策略条件键	支持

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，您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 元素中指定多个密钥，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。

您也可以在指定条件时使用占位符变量。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 WorkSpaces 瘦客户机条件密钥列表，请参阅《服务授权参考》中的 Amazon WorkSpaces 瘦客户机条件密钥。要了解您可以使用条件键的操作和资源，请参阅 Amazon Th WorkSpaces in Client 定义的操作。

要查看 WorkSpaces 瘦客户机基于身份的策略的示例，请参阅。Ama WorkSpaces zon 瘦客户机的基于身份的策略示例

WorkSpaces 瘦客户机中的 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，尽管它们不使用 JSON 策略文档格式。

带 WorkSpaces 瘦客户机的 ABAC

支持 ABAC（策略中的标签）	支持

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。在中 AWS，这些属性称为标签。您可以向 IAM 实体（用户或角色）和许多 AWS 资源附加标签。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，需要使用 aws:ResourceTag/*key-name*、aws:RequestTag/*key-name* 或 aws:TagKeys 条件密钥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密钥，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密钥，则该值为部分。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的什么是 ABAC？。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 WorkSpaces 瘦客户机上使用临时证书

支持临时凭证	支持

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，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》中的切换到角色（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。

WorkSpaces 瘦客户机的跨服务主体权限

支持转发访问会话 (FAS)	支持

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，此操作然后在不同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个操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

WorkSpaces 瘦客户机的服务角色

支持服务角色	否

服务角色是由一项服务代入、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 WorkSpaces 瘦客户机的功能。只有在 Th WorkSpaces in Client 提供相关指导时才编辑服务角色。

WorkSpaces 瘦客户机的服务相关角色

支持服务相关角色	不支持

服务相关角色是一种与服务相关联的 AWS 服务服务角色。服务可以担任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。

Ama WorkSpaces zon 瘦客户机的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 WorkSpaces 瘦客户机资源。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 policy。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。

有关 WorkSpaces 瘦客户机定义的操作和资源类型（包括每种资源类型的 ARN 格式）的详细信息，请参阅《服务授权参考》中的 Amazon WorkSpaces 瘦客户端操作、资源和条件密钥。

主题

- 策略最佳实践
- 使用 WorkSpaces 瘦客户机控制台

- 授予对 WorkSpaces 瘦客户机的只读访问权限
- 允许用户查看他们自己的权限
- 授予对 WorkSpaces 瘦客户机的完全访问权限

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 WorkSpaces 瘦客户机资源。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，请遵循以下准则和建议：

- 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 policy 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 policy 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 AWS 服务的（例如）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 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 IAM policy，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，确保策略符合 IAM policy 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，有助于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 IAM Access Analyzer 策略验证。
- 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。要在调用 API 操作时需要 MFA，请将 MFA 条件添加到策略中。有关更多信息，请参阅《IAM 用户指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html中的配置受 MFA 保护的 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 中的安全最佳实操。

使用 WorkSpaces 瘦客户机控制台

要访问 Amazon WorkSpaces 瘦客户机控制台，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 WorkSpaces 瘦客户机资源的详细信息 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。

授予对 WorkSpaces 瘦客户机的只读访问权限

此示例说明如何创建策略，允许 IAM 用户查看 WorkSpaces 瘦客户端配置，但不能进行更改。此策略包括使用 AWS CLI 或 AWS API 在控制台或程序上完成此操作的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "thinclient:GetEnvironment",
                "thinclient:ListEnvironments",
                "thinclient:GetDevice",
                "thinclient:ListDevices",
                "thinclient:ListDeviceSessions",
                "thinclient:GetSoftwareSet",
                "thinclient:ListSoftwareSets",
                "thinclient:ListTagsForResource"
            ],
            "Resource": "arn:aws:thinclient:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces:DescribeWorkspaceDirectories"],
            "Resource": "arn:aws:workspaces:*:*:directory/*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetPortal"],
            "Resource": ["arn:aws:workspaces-web:*:*:portal/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetUserSettings"],
            "Resource": ["arn:aws:workspaces-web:*:*:userSettings/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["appstream:DescribeStacks"],
```

```
            "Resource": ["arn:aws:appstream:*:*:stack/*"]
        }
    ]
}
```

允许用户查看他们自己的权限

该示例说明了如何创建策略，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": "*"
        }
    ]
}
```

授予对 WorkSpaces 瘦客户机的完全访问权限

此示例说明如何创建向 WorkSpaces 瘦客户端 IAM 用户授予完全访问权限的策略。该策略包括使用 AWS CLI 或 AWS API 在控制台或程序上完成所有 WorkSpaces 瘦客户机操作的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["thinclient:*"],
            "Resource": "arn:aws:thinclient:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces:DescribeWorkspaceDirectories"],
            "Resource": "arn:aws:workspaces:*:*:directory/*"
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetPortal"],
            "Resource": ["arn:aws:workspaces-web:*:*:portal/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["workspaces-web:GetUserSettings"],
            "Resource": ["arn:aws:workspaces-web:*:*:userSettings/*"]
        },
        {
            "Effect": "Allow",
            "Action": ["appstream:DescribeStacks"],
            "Resource": ["arn:aws:appstream:*:*:stack/*"]
        }
    ]
}
```

对 Amazon WorkSpaces 瘦客户机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 WorkSpaces 瘦客户端和 IAM 时可能遇到的常见问题。

主题

- 我无权在 WorkSpaces 瘦客户机中执行操作
- 我想要查看我的访问密钥
- 我是一名管理员，想允许其他人访问 WorkSpaces 瘦客户机
- 我想允许我以外的人 AWS 账户 访问我的 WorkSpaces 瘦客户机资源

我无权在 WorkSpaces 瘦客户机中执行操作

如果 AWS Management Console 告诉您您无权执行某项操作，则必须联系管理员寻求帮助。管理员是指提供用户名和密码的人员。

当 `mateojackson` IAM 用户尝试使用控制台查看有关虚构 *`my-thin-client-device`* 资源的详细信息，但不拥有虚构 `workspaces-thin-client:`*`ListDevices`* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 workspaces-thin-client:ListDevices on resource: my-thin-client-device
```

在这种情况下，Mateo 会要求其管理员更新其策略，以允许他使用`workspaces-thin-client:`*`ListDevices`*操作访问*`my-thin-client-device`*资源。

我想要查看我的访问密钥

在创建 IAM 用户访问密钥后，您可以随时查看您的访问密钥 ID。但是，您无法再查看您的秘密访问密钥。如果您丢失了私有密钥，则必须创建一个新的访问密钥对。

访问密钥包含两部分：访问密钥 ID（例如 `AKIAIOSFODNN7EXAMPLE`）和秘密访问密钥（例如 `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`）。与用户名和密码一样，您必须同时使用访问密钥 ID 和秘密访问密钥对请求执行身份验证。像对用户名和密码一样，安全地管理访问密钥。

> **Important**
>
> 请不要向第三方提供访问密钥，即便是为了帮助找到您的规范用户 ID 也不行。通过这样做，您可以授予他人永久访问您的权限 AWS 账户。

当您创建访问密钥对时，系统会提示您将访问密钥 ID 和秘密访问密钥保存在一个安全位置。秘密访问密钥仅在您创建它时可用。如果丢失了您的秘密访问密钥，您必须为 IAM 用户添加新的访问密钥。您最多可拥有两个访问密钥。如果您已有两个密钥，则必须删除一个密钥对，然后再创建新的密钥。要查看说明，请参阅 IAM 用户指南中的管理访问密钥。

我是一名管理员，想允许其他人访问 WorkSpaces 瘦客户机

要允许其他人访问 WorkSpaces 瘦客户端，您必须为需要访问的人员或应用程序创建一个 IAM 实体（用户或角色）。它们将使用该实体的凭证访问 AWS。然后，您必须将策略附加到授予他们在 WorkSpaces 瘦客户机中的正确权限的实体。

要立即开始使用，请参阅《IAM 用户指南》中的创建您的第一个 IAM 委派用户和组。

有关更多信息，请参阅 授予对 WorkSpaces 瘦客户机的完全访问权限。

我想允许我以外的人 AWS 账户 访问我的 WorkSpaces 瘦客户机资源

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 WorkSpaces 瘦客户机是否支持这些功能，请参阅Amazon WorkSpaces 瘦客户机如何与 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 角色与基于资源的策略有何不同。

Amazon WorkSpaces 瘦客户机的弹性

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故障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。

除了 AWS 全球基础架构外， WorkSpaces 瘦客户机还提供多项功能来帮助支持您的数据弹性和备份需求。

Amazon WorkSpaces 瘦客户机中的漏洞分析和管理

配置和 IT 控制是您 AWS 和您的共同责任。有关更多信息，请参阅责任 AWS 共担模型。

亚马逊 WorkSpaces 瘦客户机与亚马逊 WorkSpaces、亚马逊 AppStream 2.0 和 WorkSpaces 网络交叉集成。有关每项服务的更新管理的更多信息，请参阅以下链接：

- 亚马逊 AppStream 2.0 中的更新管理
- Amazon 中的更新管理 WorkSpaces
- Amazon WorkSpaces Web 中的配置和漏洞分析

监控 Amazon WorkSpaces 瘦客户机

监控是维护 Amazon Th WorkSpaces in Client 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 提供了以下监控工具，用于监视 WorkSpaces 瘦客户机、报告何时出现问题并在适当时自动采取措施：

- AWS CloudTrail捕获由您的账户或代表您的 AWS 账户进行的 API 调用和相关事件，并将日志文件传输到您指定的 Amazon S3 存储桶。您可以识别呼叫的用户和帐户 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。

使用记录亚马逊 WorkSpaces 瘦客户端 API 调用 AWS CloudTrail

Amazon Th WorkSpaces in Client 与 AWS CloudTrail一项服务集成，可记录用户、角色或 AWS 服务在 WorkSpaces 瘦客户机中执行的操作。 CloudTrail 将 WorkSpaces 瘦客户机的所有 API 调用捕获为事件。捕获的调用包括来自 WorkSpaces 瘦客户机控制台的调用和对 WorkSpaces 瘦客户端 API 操作的代码调用。如果您创建跟踪，则可以允许将 CloudTrail事件持续传输到 Amazon S3 存储桶，包括 WorkSpaces 瘦客户端的事件。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 WorkSpaces 瘦客户机发出的请求、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》。

WorkSpaces 中的瘦客户机信息 CloudTrail

CloudTrail 在您创建账户 AWS 账户 时已在您的账户上启用。在 WorkSpaces 瘦客户机中发生活动时，该活动会与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在 AWS 账户中查看、搜索和下载最新事件。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录您的 AWS 账户事件（包括 WorkSpaces 瘦客户机的事件），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 CloudTrail 日志中收集的事件数据并对其采取行动。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
- 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 WorkSpaces 瘦客户机操作均由《Amazon 瘦客户端 API 参考》记录 CloudTrail 并记录在《亚马逊 WorkSpaces 瘦客户端 API 参考》中。例如，对CreateEnvironmentListDevices、和GetSoftwareSet 操作的调用会在 CloudTrail 日志文件中生成条目。

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

- 请求是使用根证书还是 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 WorkSpaces 瘦客户机日志文件条目

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

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "arn:aws:iam::<arn>",
                "accountId": "<accpimt-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
```

```
            "attributes": {
                "creationDate": "2023-11-18T23:07:01Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-11-18T23:11:57Z",
    "eventSource": "thinclient.amazonaws.com",
    "eventName": "GetDevice",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<source-ip-address>",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0)
 Gecko/20100101 Firefox/115.0",
    "requestParameters": {
        "id": "<ip>"
    },
    "responseElements": null,
    "requestID": "<request-id>",
    "eventID": "<event-id>",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<recipient-account-id>",
    "eventCategory": "Management"
}
```

使用创建 Amazon WorkSpaces 瘦客户机资源 AWS CloudFormation

Amazon Th WorkSpaces in Client 与 AWS CloudFormation一项服务集成，可帮助您对 AWS 资源进行建模和设置。这样，您可以花费更少的时间来创建和管理您的资源和基础设施。您可以创建一个描述所需的所有 AWS 资源（例如环境）的模板，并为您 AWS CloudFormation 预置和配置这些资源。

使用时 AWS CloudFormation，您可以重复使用模板来一致且重复地设置 WorkSpaces 瘦客户机资源。只需描述一次您的资源，然后在多个 AWS 账户 区域中重复配置相同的资源。

WorkSpaces 瘦客户机和 AWS CloudFormation 模板

要为 WorkSpaces 瘦客户机及相关服务配置和配置资源，必须了解AWS CloudFormation 模板。模板是 JSON 或 YAML 格式的格式化文本文件。这些模板描述了您要在 AWS CloudFormation 堆栈中配置的资源。如果您不熟悉 JSON 或 YAML 格式，可以使用 D AWS CloudFormation esigner 来帮助您开始使用 AWS CloudFormation 模板。有关更多信息，请参阅《AWS CloudFormation 用户指南》中的什么是 AWS CloudFormation Designer？。

WorkSpaces 瘦客户机支持在中创建环境 AWS CloudFormation。有关更多信息，包括环境的 JSON 和 YAML 模板示例，请参阅AWS CloudFormation 用户指南中的 Amazon WorkSpaces 瘦客户机资源类型参考。

了解更多关于 AWS CloudFormation

要了解更多信息 AWS CloudFormation，请参阅以下资源：

- AWS CloudFormation
- AWS CloudFormation 用户指南
- AWS CloudFormation API Reference
- AWS CloudFormation 命令行界面用户指南

使用接口终端节点访问 Amazon WorkSpaces 瘦客户端 (AWS PrivateLink)

您可以使用 AWS PrivateLink 在您的 VPC 和 Amazon WorkSpaces 瘦客户端之间创建私有连接。您可以作为 VPC 访问 WorkSpaces 瘦客户机，无需使用互联网网关、NAT 设备、VPN 连接或 AWS Direct Connect 连接。您的 VPC 中的实例不需要公有 IP 地址即可访问 WorkSpaces 瘦客户端。

您可以通过创建由提供支持的接口端点来建立此私有连接 AWS PrivateLink。我们将在您为接口端点启用的每个子网中创建一个端点网络接口。这些是请求者管理的网络接口，用作发往 WorkSpaces 瘦客户机的流量的入口点。

有关更多信息，请参阅《AWS PrivateLink 指南》中的通过 AWS PrivateLink访问 AWS 服务。

WorkSpaces 瘦客户机的注意事项

在为 WorkSpaces 瘦客户机设置接口端点之前，请查看AWS PrivateLink 指南中的注意事项。

WorkSpaces 瘦客户机支持通过接口端点调用其所有 API 操作。

为 WorkSpaces 瘦客户机创建接口端点

您可以使用 Amazon VPC 控制台或 AWS Command Line Interface (AWS CLI) 为 WorkSpaces 瘦客户机创建接口终端节点。有关更多信息，请参阅《AWS PrivateLink 指南》中的创建接口端点。

使用以下服务名称为 WorkSpaces 瘦客户机创建接口端点：

```
com.amazonaws.region.thinclient.api
```

如果您为接口终端节点启用私有 DNS，则可以使用 WorkSpaces 瘦客户端的默认区域 DNS 名称向瘦客户机发出 API 请求。例如，`api.thinclient.us-east-1.amazonaws.com`。

为接口端点创建端点策略

端点策略是一种 IAM 资源，您可以将其附加到接口端点。默认端点策略允许您通过接口端点完全访问 WorkSpaces 瘦客户机。要控制从您的 VPC 授予 WorkSpaces 瘦客户机的访问权限，请将自定义终端节点策略附加到接口终端节点。

端点策略指定以下信息：

- 可执行操作的主体（AWS 账户、IAM 用户和 IAM 角色）。
- 可执行的操作。
- 可对其执行操作的资源。

有关更多信息，请参阅《AWS PrivateLink 指南》中的使用端点策略控制对服务的访问权限。

示例： WorkSpaces 瘦客户机操作的 VPC 终端节点策略

以下是自定义端点策略的示例。当您将此策略附加到接口终端节点时，它会向所有资源的所有委托人授予访问列出的 WorkSpaces 瘦客户机操作的权限。

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "thinclient:ListEnvironments",
            "thinclient:ListDevices",
            "thinclient:ListSoftwareSets"
         ],
         "Resource":"*"
      }
   ]
}
```

《 WorkSpaces 瘦客户机管理员指南》的文档历史记录

下表描述了《 WorkSpaces 瘦客户机管理员指南》版本的文档历史记录。

更改	描述	日期
• 为 Amazon WorkSpaces 瘦客户机 WorkSpaces 进行配置 • 为 Amazon WorkSpaces 瘦客户机配置 AppStream 2.0	• 更新了操作系统列表。 • 更新了身份提供者程序。	2024 年 2 月 12 日
初始版本	初始版本	2023 年 11 月 26 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。