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？ 1
您是 新用户吗？ 1
架构 1
设置 Amazon WorkSpaces 瘦客户机管理员控制台 4
注册亚马逊云科技 4
创建 IAM 用户 4
开始使用适用于 Amazon WorkSpaces 瘦客户机的 VDI 管理员控制台 6
为 WorkSpaces 瘦客户机配置 WorkSpaces 个人 6
开始前的准备工作 6
步骤 1：验证您的系统是否符合 WorkSpaces个人要求的功能 7
第 2 步：使用高级设置启动你的 WorkSpace 8
业务连续性 8
为 WorkSpaces 瘦客户机配置 WorkSpaces 池 9
开始前的准备工作 10
创建 WorkSpaces 池 10
配置 WorkSpaces 瘦客户机访问权限 12
为 Amazon WorkSpaces 瘦客户机配置 AppStream 2.0 12
步骤 1：验证您的系统是否满足 AppStream 2.0 要求的功能 13
第 2 步：设置 AppStream 2.0 堆栈 14
为亚马逊 WorkSpaces 瘦客户机配置亚马逊 WorkSpaces 安全浏览器 14
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 14
步骤 2：设置 WorkSpaces 安全浏览器门户 15
启动 WorkSpaces 瘦客户机管理员控制台 16
覆盖区域 16
启动 WorkSpaces 瘦客户机管理员控制台 17
使用 WorkSpaces 瘦客户机管理员控制台 18
环境 19
环境列表 19
环境详细信息 20
创建环境 24
编辑环境 27
删除环境 27
设备 28
设备列表 28

设备详细信息 30
编辑设备名称 36
重置和取消注册设备 36
存档设备 37
删除设备 37
导出设备详细信息 37
软件更新 38
更新环境软件 38
更新设备软件 39
WorkSpaces 瘦客户机软件版本 39
在 WorkSpaces 瘦客户机资源上使用标签 46
安全性 49
数据保护 49
数据加密 50
静态加密 51
传输中加密 64
密钥管理 64
互联网工作流量隐私 64
身份和访问管理 65
受众 65
使用身份进行身份验证 66
使用策略管理访问 68
Amazon WorkSpaces 瘦客户机如何与 IAM 配合使用 70
基于身份的策略示例 76
AWS 托管策略 80
故障排除 84
恢复能力 87
漏洞分析和管理 87
监控 88
CloudTrail 日志 88
CloudTrail 数据事件 89
CloudTrail 管理事件 90
CloudTrail 事件示例 90
AWS CloudFormation 资源 94
WorkSpaces 瘦客户机和 AWS CloudFormation 模板 94
了解更多关于 AWS CloudFormation 94

AWS PrivateLink 95
注意事项 95
创建接口端点 95
创建端点策略 95
文档历史记录 97
..... xcix

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？
- 架构

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

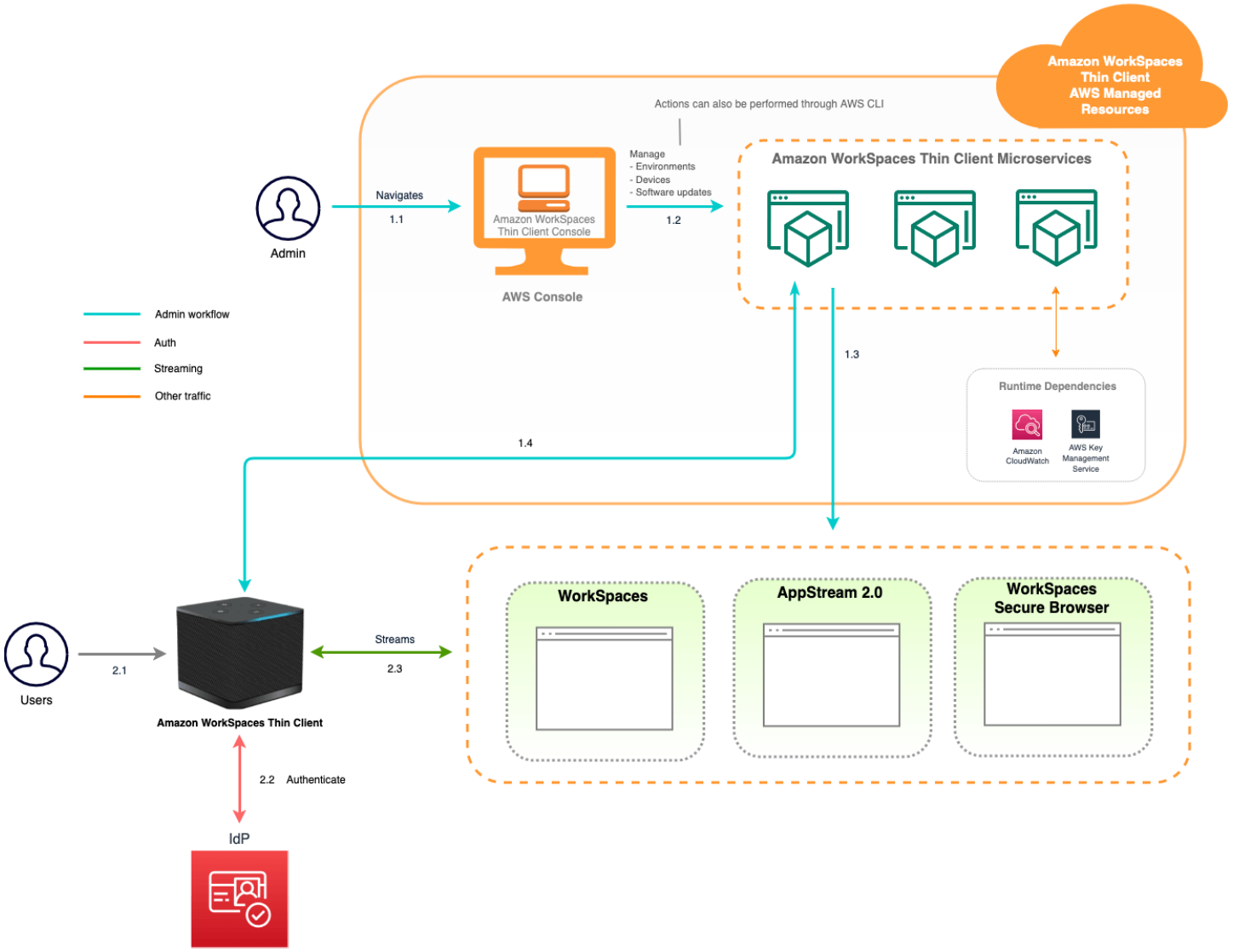
根据所使用的 VDI，您的 WorkSpaces 瘦客户机的信息可通过目录 WorkSpaces、 AppStream 2.0 的堆栈和 WorkSpaces 安全浏览器的门户端点进行访问和管理。

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-serviceSaaS) 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
- 创建 IAM 用户

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/注册。
2. 按照屏幕上的说明操作。

   在注册时，将接到电话或收到短信，要求使用电话键盘输入一个验证码。

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

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》中的创建用于紧急访问的 IAM 用户中的说明进行操作。	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 WorkSpaces 瘦客户机配置 WorkSpaces 个人
- 为 WorkSpaces 瘦客户机配置 WorkSpaces 池
- 为 Amazon WorkSpaces 瘦客户机配置 AppStream 2.0
- 为亚马逊 WorkSpaces 瘦客户机配置亚马逊 WorkSpaces 安全浏览器

为 WorkSpaces 瘦客户机配置 WorkSpaces 个人

要将 WorkSpaces 瘦客户机与 Amazon Person WorkSpaces al 配合使用，需要将您的服务配置为访问 WorkSpaces 目录。Amazon Person WorkSpaces al 目录根据 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。

> **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 WorkSpaces 个人版协议。
- 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 WorkSpaces 个人目录。
- 启动时 WorkSpace，启用并配置 WorkSpaces 瘦客户端 Web 访问权限。有关更多信息，请参阅配置 WorkSpaces 瘦客户机

步骤 1：验证您的系统是否符合 WorkSpaces个人要求的功能

为了使 WorkSpaces 瘦客户机管理员控制台与 Amazon P WorkSpaces ersonal 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
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

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） • 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 DCV

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/v2/home/。
2. 选择以下一种目录类型，然后选择下一步：
   - AWS 微软 AD 托管
   - 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。

业务连续性

WorkSpaces 作为业务连续性计划 (BCP) 的一部分，瘦客户机为业务连续性提供支持。 WorkSpaces 瘦客户机业务连续性仅适用于 WorkSpaces 个人版。有关业务连续性的更多信息，请参阅 Amazon WorkSpaces 管理指南中的 WorkSpaces 个人业务连续性。

先决条件

要使业务连续性在 WorkSpaces 瘦客户机上运行，必须满足以下先决条件：

- 对于 WorkSpaces 跨区域重定向 — 已配置 DNS 服务和路由策略。要进行这些设置，请参阅配置您的 DNS 服务和设置 DNS 路由策略。
- 对于 WorkSpaces 多区域弹性- WorkSpaces 已创建备用副本。要创建它，请参阅创建备用副本 WorkSpace。

- 该区域中使用 WorkSpaces 瘦客户机的连接别名。要验证您的区域，请参阅覆盖区域。

为 WorkSpaces 瘦客户机配置业务连续性

要在 Amazon Th WorkSpaces in Client 上启用 WorkSpaces 个人灾难恢复，您需要使用软件开发工具包配置连接别名以映射到环境。

设置灾难恢复的示例文档说明：

Example

使用 AWS CLI 使用流媒体桌面的 WorkSpaces 连接别名创建新环境的命令示例：

```
aws workspaces-thin-client create-environment --region region --desktop-arn/
arn:aws:workspaces:region:account:connectionalias/wsca-id
```

*wsca-id*替换为您的 WorkSpaces 个人连接别名。 WorkSpaces 连接别名的 ID 可以在 WorkSpaces 管理控制台或 SDK 中找到。

最终用户体验

配置业务连续性后，设备必须在过去 15 天内注册并处于活动状态。之后，如果 WorkSpaces 瘦客户机管理服务不可用，则用户可以在长达 24 小时内与其会话保持连接。在这种情况下，设备将无法接收软件更新、交换状态信息，也无法激活。 WorkSpaces 瘦客户机控制台中的相应设备条目将不会显示最新信息。

如果 WorkSpaces 瘦客户机设备管理服务在 24 小时后仍然不可用，则会显示以下错误消息：

“发生了错误。请重试。如果问题仍然存在，请联系您的 IT 管理员。（错误代码：3006）。”

为 WorkSpaces 瘦客户机配置 WorkSpaces 池

要将 WorkSpaces 瘦客户机与 Amazon Pools 配合使用，需要将您的 SAML 2.0 身份提供商 (IdP) 配置为访问 WorkSpaces WorkSpaces 池目录。Amazon P WorkSpaces ools 目录是 WorkSpaces 分配给一组用户的非永久池。

> **Note**
>
> 首次使用控制台之前必须进行配置。

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。

在继续进行配置之前，请查看并理解《Amazon WorkSpaces 管理指南》中 Active Directory 与 WorkSpaces 池一起使用之前所列的概念。

创建 WorkSpaces 池

设置并创建一个池，将从该池中启动和流式传输用户应用程序。

> **Note**
>
> 在创建 WorkSpaces 池之前，应先创建一个目录。有关更多信息，请参阅配置 SAML 2.0 和创建 WorkSpaces 池目录目录。

设置和创建池

1. 打开 WorkSpaces 控制台，网址为https://console.aws.amazon.com/workspaces/v2/home/。
2. 在导航窗格中 WorkSpaces，选择 “池”。
3. 选择 “创建 WorkSpaces 池”。
4. 在 Onbo arding（可选）下，您可以根据我的用例选择向我推荐选项，以获取有关 WorkSpaces 您要使用的类型的推荐。如果您知道要使用 P WorkSpaces ools，则可以跳过此步骤。
5. 在 “配置” 下 WorkSpaces，输入以下详细信息：
   - 对于名称，为池输入一个唯一的名称标识符。不允许使用特殊字符。
   - 对于描述，输入池描述（最多 256 个字符）。
   - 对于捆绑包，请从以下选项中选择要用于的捆绑包类型 WorkSpaces。
     - 使用基础 WorkSpaces 捆绑包 — 从下拉列表中选择一个捆绑包。要了解您选择的捆绑包类型的更多信息，请选择捆绑包详细信息。要比较为池提供的捆绑包，请选择比较所有捆绑包。
     - 使用您自己的自定义捆绑包-选择您之前创建的捆绑包。要创建自定义套装，请参阅为 WorkSpaces 个人版创建自定义 WorkSpaces 镜像和捆绑包。

> **Note**
>
> BYOL 目前不适用于资源 WorkSpaces 池。

- 对于最大会话持续时间（分钟），选择流式传输会话可以保持活动状态的最长时间。在达到此限制前的五分钟，如果用户仍连接到流实例，则系统在断开连接之前将会提示用户保存任何打开的文档。在此时间过后，实例将终止并被新的实例取代。您可以在 “ WorkSpaces 池” 控制台中设置的最大会话持续时间为 5760 分钟（96 小时）。您可以使用 WorkSpaces 池 API 和 CLI 设置的最大会话持续时间为 432000 秒（120 小时）。
- 对于 Disconnect timeout in minutes (断开连接超时 (分钟))，请选择在用户断开连接后流式传输会话保持活动状态的时间。如果在此时间间隔内出现连接断开或网络中断的情况后，用户尝试重新连接到流式传输会话，他们将连接到其上一个会话。否则，他们会建立一个新会话，连接到新的流实例。
- 如果用户通过在池工具栏上选择结束会话或注销来结束会话，则不应用断开连接超时。系统而是会提示用户保存任何打开的文档，然后立即断开流实例的连接。用户正在使用的实例随即终止。
- 对于 Idle disconnect timeout in minutes (空闲断开连接超时 (分钟))，请选择用户在与流式传输会话断开连接以及 Disconnect timeout in minutes (断开连接超时 (分钟)) 时间间隔开始之前可以处于空闲（非活动）状态的时间。在由于处于不活动状态而断开连接之前，用户将收到通知。在 Disconnect timeout in minutes (断开连接超时 (分钟)) 中指定的时间间隔过去之前，如果他们尝试重新连接到流式传输会话，则会将他们连接到以前的会话。否则，他们会建立一个新会话，连接到新的流实例。如果将该值设置为 0，则会禁用该值。如果禁用了该值，则不会由于处于不活动状态而断开连接用户。

> **Note**
>
> 如果用户在流式传输会话期间停止提供键盘或鼠标输入，则将其视为处于空闲状态。对于已加入域的池，在用户使用其 Active Directory 域密码或智能卡登录后，空闲断开连接超时的倒计时才会开始。文件上传和下载、音频输入、音频输出以及像素更改不符合用户活动条件。在 Idle disconnect timeout in minutes (空闲断开连接超时 (分钟)) 中的时间间隔过去之后，如果用户继续处于空闲状态，则会将他们断开连接。

- 对于计划容量策略（可选），选择添加新计划容量。根据预期并发用户的最小数量，指明为池预置最小和最大实例数的开始日期和结束日期与时间。
- 对于手动扩展策略（可选），为池指定用于增加和减少池容量的扩展策略。展开手动扩展策略以添加新的扩展策略。

> **Note**
>
> 您的池大小受您指定的最小和最大容量限制。

- 如果指定的容量利用率小于或高于指定的阈值，请选择添加新的横向扩展策略，然后输入用于添加指定实例的值。
- 如果指定的容量利用率小于或高于指定的阈值，请选择添加新的横向缩减策略，然后输入用于删除指定实例的值。

- 对于标签，指定要使用的键对值。键可以是具有特定关联值的一般类别，例如“project”、“owner”或“environment”。

6. 在选择目录页面上，选择您创建的目录。要创建目录，请选择创建目录。有关更多信息，请参阅管理 WorkSpaces 池的目录。
7. 选择 “创建 WorkSpace 池”。

配置 WorkSpaces 瘦客户机访问权限

为 WorkSpaces 池配置 Web 访问权限以使用 WorkSpaces 瘦客户机，你需要使用 AWS 命令登陆界面。

1. 安装或更新 AWS Command Line Interface。
2. 配置您的AWS CLI 设置。
3. 打开 AWS CLI.
4. 使用相应信息替换WORKSPACES_DIRECTORY_ID和REGION运行以下命令：

```
aws workspaces modify-workspace-access-properties --resource-
id WORKSPACES_DIRECTORY_ID  --workspace-access-properties
 '{"DeviceTypeWorkSpacesThinClient":"ALLOW"}' --region REGION
```

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

要使 WorkSpaces 瘦客户机管理员控制台在 AppStream 2.0 中正常运行，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
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）
剪贴板	禁用 在 AppStream 2.0 堆栈级别进行配置
文件传输功能	禁用 在 AppStream 2.0 堆栈级别进行配置
打印到本地设备	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，请参阅在 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
剪贴板	禁用
文件传输功能	禁用
打印到本地设备	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
- 启动 WorkSpaces 瘦客户机管理员控制台

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

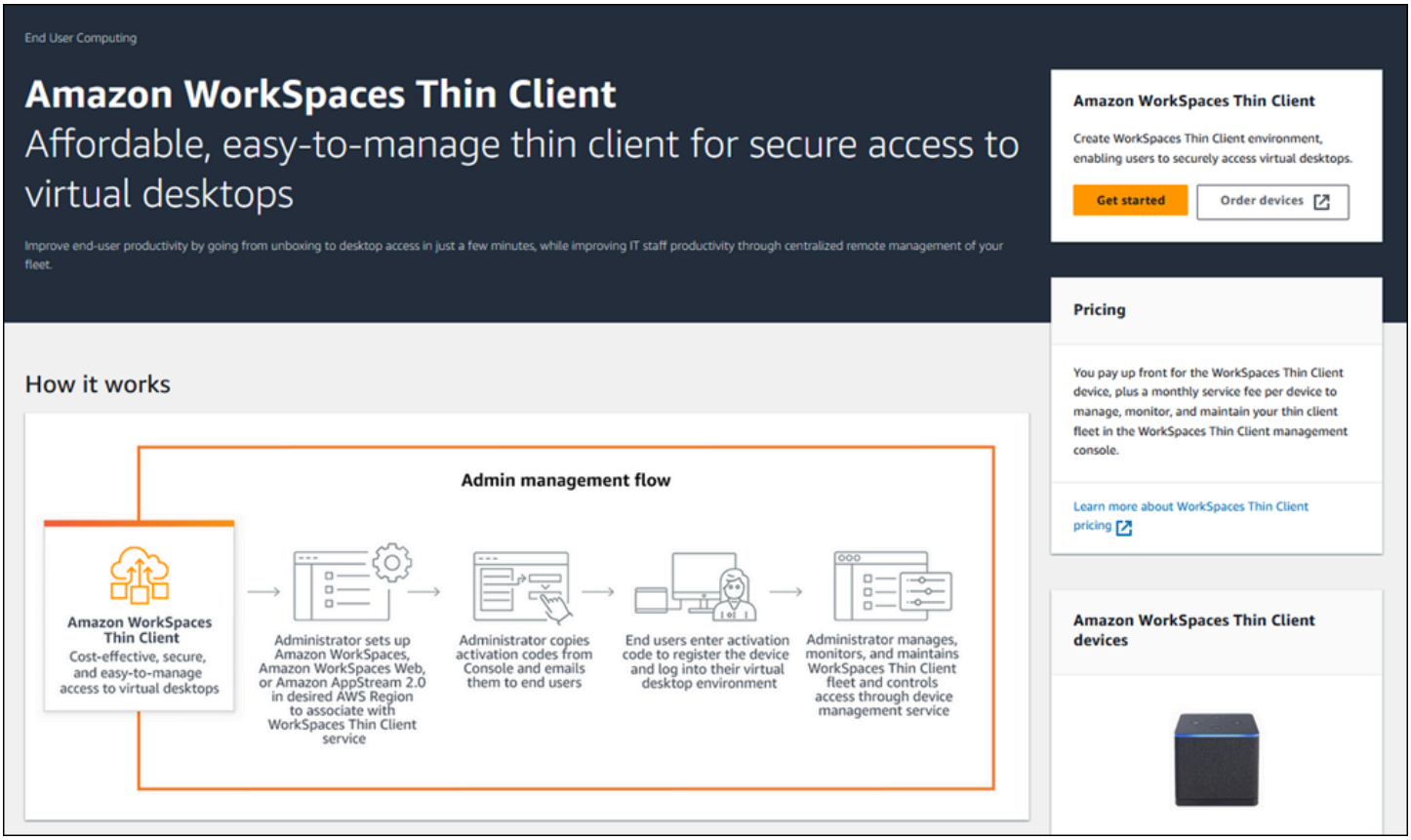
区域名称	区域	终端节点	控制台链接
加拿大（中部）	ca-central-1	thinclient.ca-central-1.amazonaws.com	https://ca-central-1.console.aws.amazon.com/workspaces-thin-client/home
欧洲（法兰克福）	eu-central-1	thinclient.eu-central-1.amazonaws.com	https://eu-central-1.console.aws.amazon.com/workspaces-thin-client/home
欧洲（伦敦）	eu-west-2	thinclient.eu-west-2.amazonaws.com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

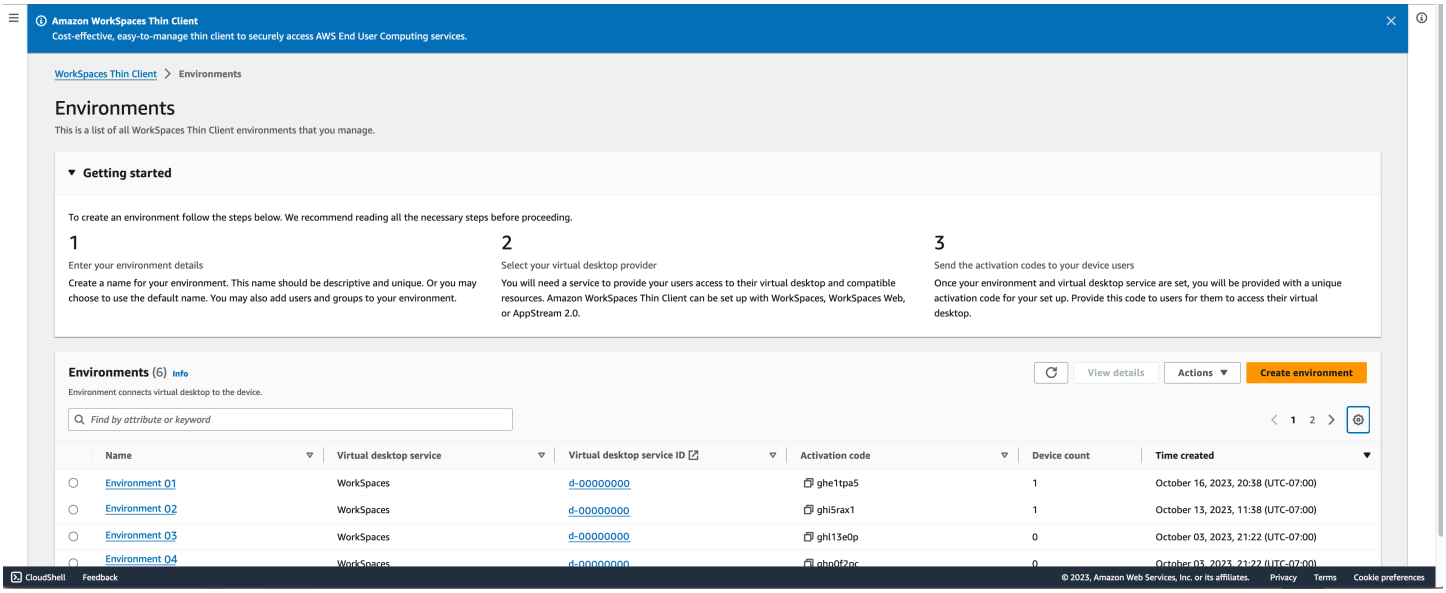
环境

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

您的环境有许多参数可供您查看，还有一些可以采取的措施。



环境列表详细信息

列出了您的环境参数供您查看。下表列出了摘要中的每个元素及其运作方式。

元素	描述
Name	与此环境相关的唯一标识符。
虚拟桌面服务	此环境使用的虚拟桌面提供商。
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。

元素	描述
激活码	最终用户用于访问虚拟桌面环境的代码。
设备数量	访问此环境的 WorkSpaces 瘦客户机设备的数量。
时间已创建	环境的创建日期和时间。

环境列表操作

您可以从此处执行许多操作。选择其中任何一个以执行相应的操作。

元素	描述
Search	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。	开始创建环境的过程。

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

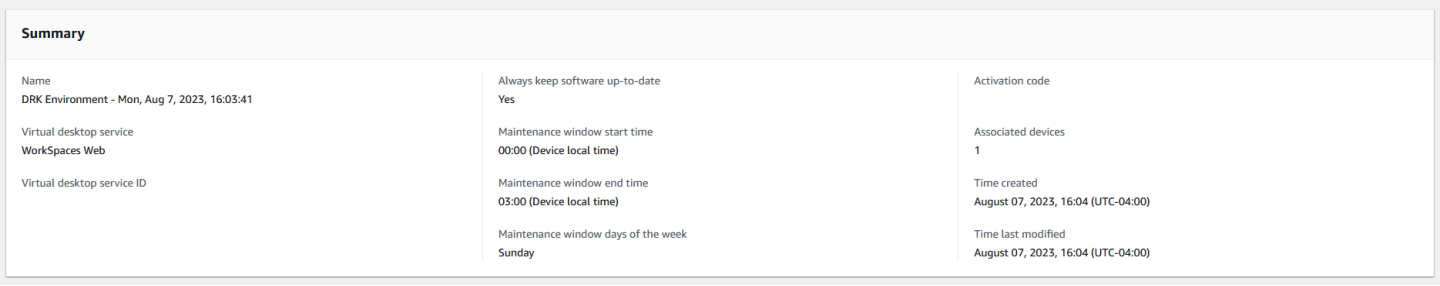
选择环境时，WorkSpaces 瘦客户机控制台会显示该环境的详细信息供您查看。控制台还会显示有关该环境使用的虚拟桌面提供商的详细信息。

主题

- 摘要
- 虚拟桌面环境详细信息

摘要

“摘要” 部分概述了 WorkSpaces 瘦客户机环境的主要功能。下表列出了摘要中的每个元素及其运作方式。



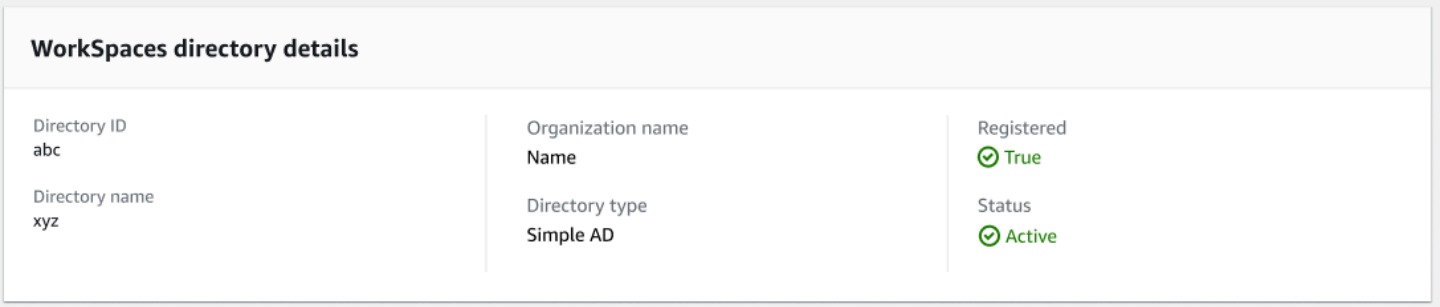
元素	描述
Name	与此环境相关的唯一标识符。
虚拟桌面服务	此环境使用的虚拟桌面提供商。
虚拟桌面服务名称	虚拟桌面服务提供商分配给该环境的唯一标识符。
激活码	最终用户使用此代码访问虚拟桌面环境。
始终保留软件 up-to-date	此设置启用自动软件更新。
维护窗口开始时间	每周开始自动软件更新的时间。
维护窗口结束时间	每周自动软件更新完成的时间。
一周中的维护窗口天数	软件自动更新的日子。
关联的设备	访问此环境的 WorkSpaces 瘦客户机设备的数量。
创建时间	此环境的创建日期和时间。

虚拟桌面环境详细信息

WorkSpaces 瘦客户机环境在虚拟桌面界面上运行。每个接口都有一组不同的参数来控制专用环境。

Amazon WorkSpaces 目录详情

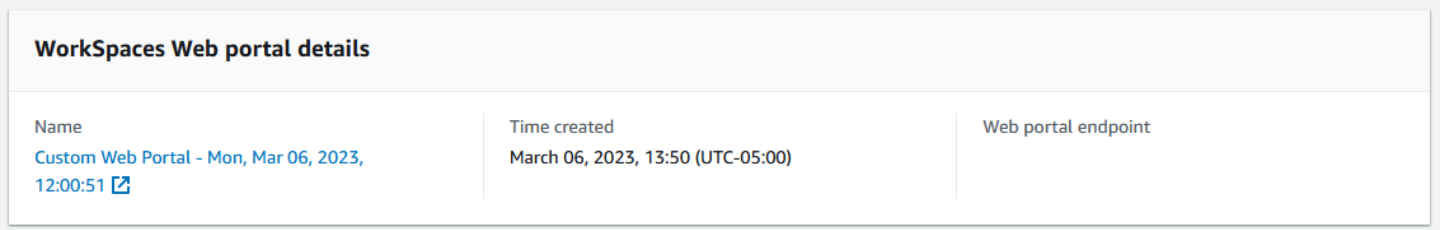
WorkSpaces 在 Amazon 上运行的瘦客户机环境 WorkSpaces 使用目录来创建和运行其虚拟桌面。下表列出了详细信息中的每个元素及其运作方式。



元素	描述
目录 ID	与此环境关联的 Amazon WorkSpaces 目录。
目录名称	与此 Amazon WorkSpaces 目录相关的唯一标识符。
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

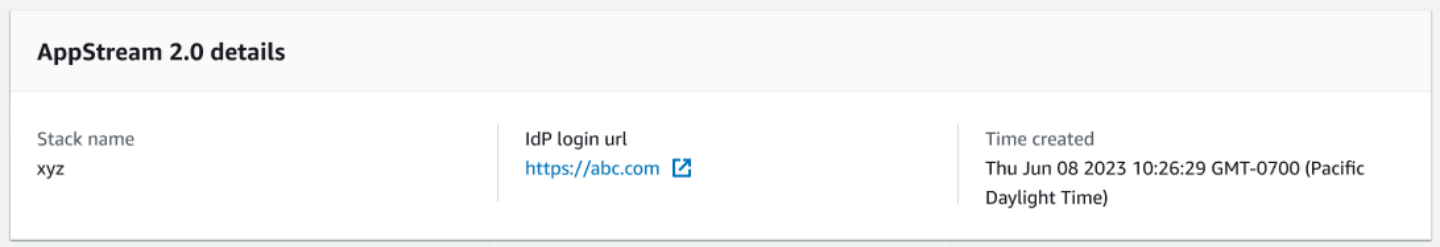
WorkSpaces 在 Amazon WorkSpaces Secure Browser 上运行的瘦客户机环境使用门户来创建和运行其虚拟桌面。下表列出了详细信息中的每个元素及其运作方式。



元素	描述
Name	与此 WorkSpaces 安全浏览器门户相关的唯一标识符。
创建时间	创建此 WorkSpaces 安全浏览器门户的日期和时间。
Web 门户端点	用于访问您的虚拟桌面环境的网址。

AppStream 2.0 详情

WorkSpaces 瘦客户机环境在 AppStream 2.0 信息堆栈上运行，用于创建和运行其虚拟桌面。下表列出了详细信息中的每个元素及其运作方式。



元素	描述
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

您必须将服务分配给现有环境或创建一个新环境。

> **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
- 步骤 2：选择虚拟桌面提供程序
- 步骤 3：将激活码发送给您的设备用户

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。
   - 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。

> **Important**
>
> 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。
   - 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。
   - 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。

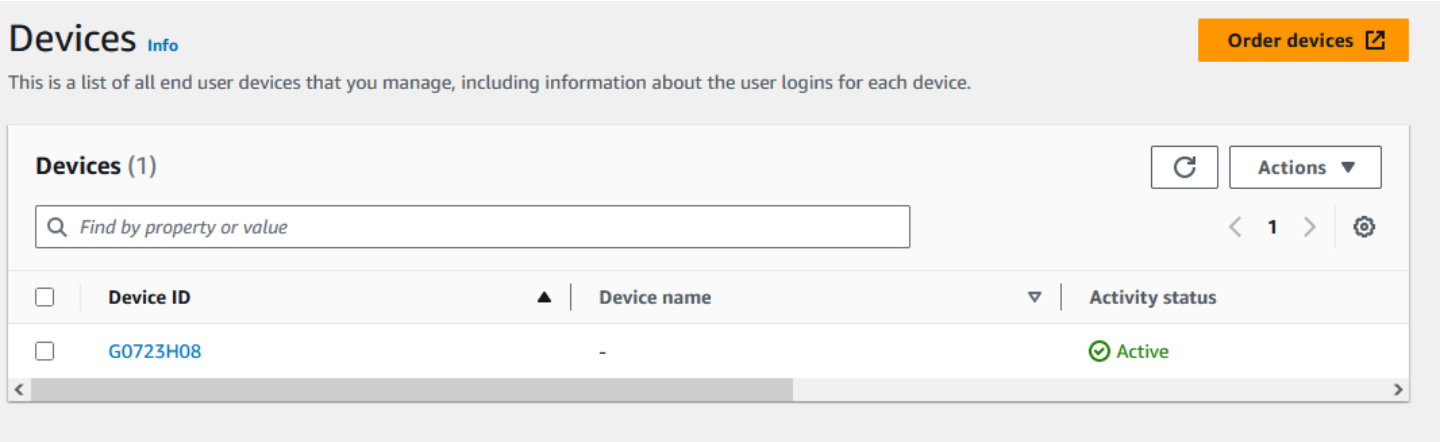
设备

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

网络中的任何设备都有许多参数可供您查看，还有一些可以采取的操作。



设备列表详细信息

您的设备参数已列出供您查看。下表列出了摘要中的每个元素及其运作方式。

元素	描述
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 — 在过去七天内至少连接到网络一次。 • 非活动-在过去七天内未连接到网络。
注册状态	确认设备已设置完毕，已与此 AWS 账户关联，并且属于特定环境。它可以处于以下状态之一： • 已注册-这是默认状态。

元素	描述
	• 取消注册-设备处于 “重置和注销” 过程中。 Note 如果设备处于注销状态，则可以将其删除。 • 已@@ 注销- 设备已成功注销。 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	此设备所连接的环境的标识符。
软件合规性	设备软件的合规性状态。有两种状态状态： • 合规 • 不合规

设备列表操作

您可以从此处执行许多操作。选择其中任何一个以执行相应的操作。

元素	描述
Search	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：

元素	描述
	• 编辑设备名称 • 取消注册 • 存档 • 删除 • 导出设备详细信息
订购设备	开始订购设备的流程。

主题

- 设备详细信息
- 编辑设备名称
- 重置和取消注册设备
- 存档设备
- 删除设备
- 导出设备详细信息

设备详细信息

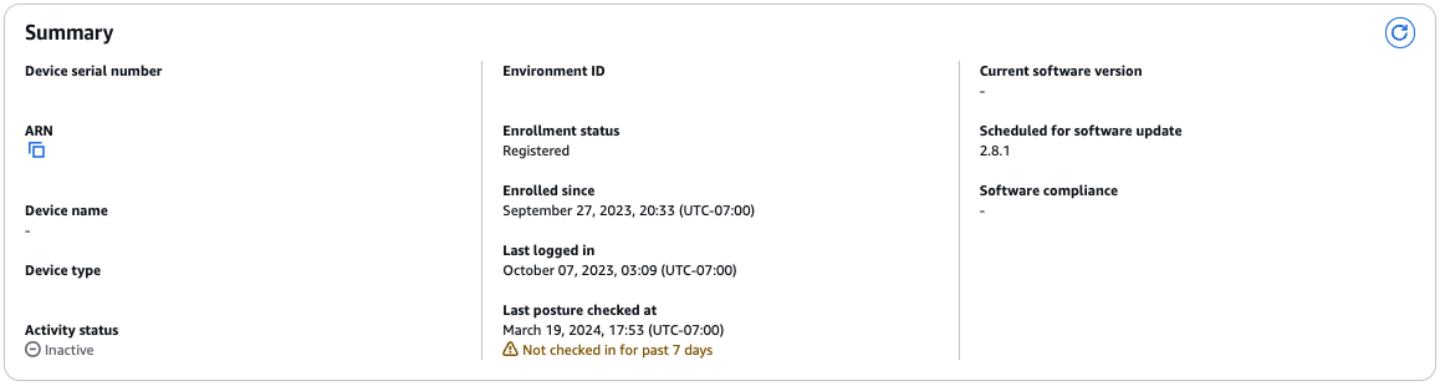
选择设备时，WorkSpaces 瘦客户机控制台会显示该设备的详细信息供您查看。控制台还会显示有关设备网络类型和连接的外围设备的详细信息。

主题

- 摘要
- 设备设置
- 用户活动

摘要

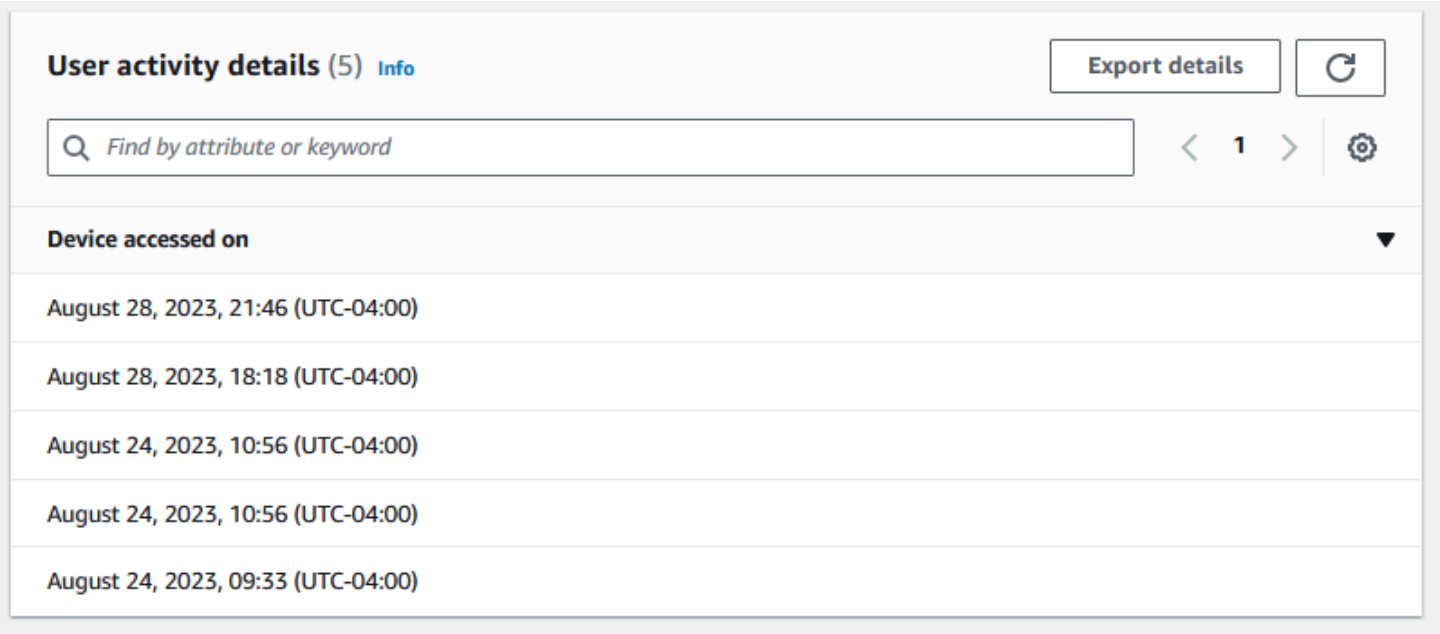
“摘要” 部分概述了 WorkSpaces 瘦客户机设备的主要功能。下表列出了摘要中的每个元素及其运作方式。



元素	描述
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 Amazon 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： • 活动 • 非活动
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，并且属于特定环境。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-设备处于 “重置和注销” 过程中。 • 已注销-设备已成功注销。

元素	描述
	> **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。
此后入学	设备激活的日期。
上次登录	最近一次登录的日期和时间。
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	设备上的计划软件版本。
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



元素	描述
上次访问设备	上次使用此设备的日期和时间。

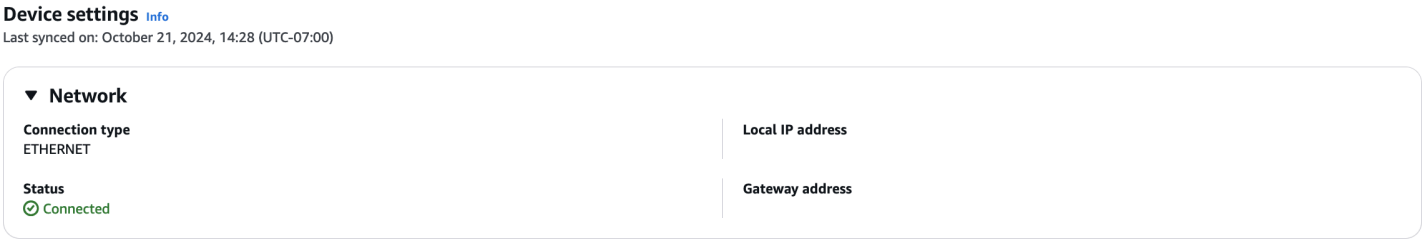
设备设置

您的设备参数已列出供您查看。下表列出了每个元素及其工作原理。

> **Note**
>
> 只有当设备处于联机状态时，设备设置信息才会更新。如果设备处于离线状态，则某些信息可能已过期。

标题和网络

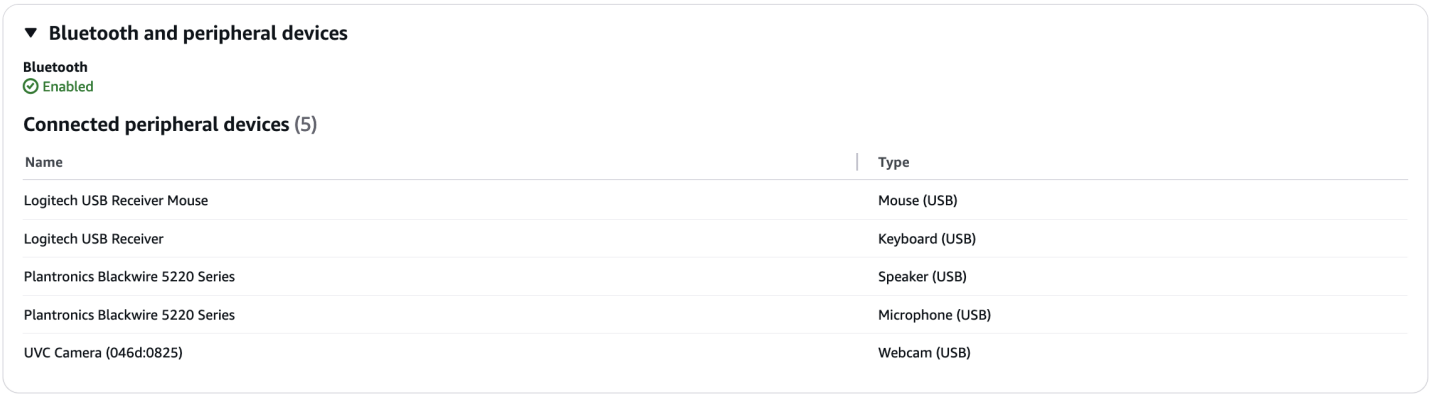
WorkSpaces 瘦客户机设备详细信息概述了设备的网络连接。下表列出了每个元素及其工作原理。



元素	描述
上次同步时间为	最新设备设置的日期和时间与主机同步。
连接类型	设备使用的网络连接类型。连接类型可以是以太网或 Wifi。
状态	网络的状态。如果设备当前处于连接状态，或者在过去 20 分钟内已连接，则状态将显示为 “已连接”。如果网络断开连接的时间超过 20 分钟，则状态将更改为显示自设备上次连接互联网以来经过的时间，例如 “上次连接时间 20 分钟前”。
本地 IP 地址	所连接网络的本地 IP 地址。
网关地址	所连接网络的网关地址。

蓝牙和外围设备

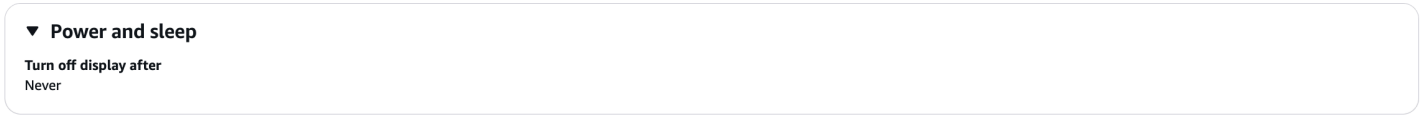
WorkSpaces 瘦客户机设备详细信息提供了连接到设备的所有已连接外围设备的列表。下表列出了每个元素及其工作原理。



元素	描述
蓝牙	设备的蓝牙状态。两种状态状态是： • 已启用 • 已禁用
连接的外围设备	所连接外围设备的名称列表，例如罗技鼠标，以及所连接外围设备的类型，例如鼠标 (USB)。

电源和睡眠

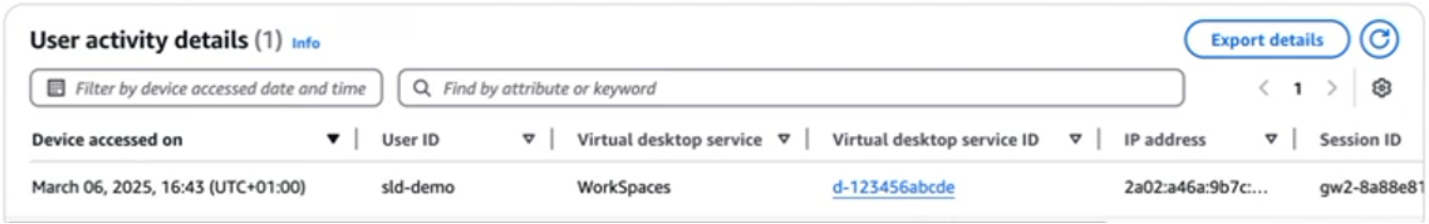
每台 WorkSpaces 瘦客户机设备都有省电模式。下表列出了此模式的状态。



元素	描述
之后关闭显示屏	设备关闭显示屏的非活动时间段。

用户活动

此选项卡显示特定设备的设置和使用信息的日志。下表列出了此日志的每个元素。



元素	描述
访问设备时使用的	设备激活的日期和时间。
用户 ID	访问设备的用户的标识号。

元素	描述
虚拟桌面服务	设备使用的虚拟桌面服务。
虚拟桌面服务 ID	与用户关联的虚拟桌面服务 ID 号。
IP 地址	访问设备的 IP 的标识号。
事件类型	有关设备使用方式的详细信息。

> **Note**
>
> 除 “ WorkSpaces 个人” 之外， VDIs 仅显示已启动登录的事件。

您可以使用表格上方的搜索栏在表格中查找特定信息。您也可以按日期和时间筛选表格结果。

您可以通过选择导出详细信息按钮将表格导出到 csv 文件。

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。

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 瘦客户机是一项 AWS 最终用户计算服务，可让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
2.16.1	7-3-2025	• 已修复 Chromium 的 CVE-2025-6554 严重安全问题。
2.16.0	6-27-2025	• 添加了网络延迟通知。 • 增加了在会话期间从第二台显示器变暗中恢复的功能。

软件套装	发行日期	更改
		• 修复了设备从睡眠模式恢复后显示器显示白屏或不自动延伸的问题。
2.15.0	6-19-2025	• 增加了对拉丁美洲西班牙语和国际英语键盘的支持。 • 当设备长时间未检测到键盘或鼠标活动时，最终用户会看到通知。
2.14.1	6-09-2025	• 修复了 Chromium 的 CVE-2025-5419 关键安全问题。
2.13.0	3-31-2025	• 最终用户将以通知的形式看到产品满意度反馈调查。 • 增加了对 FIDO2 身份验证流程的预发行功能支持。查看FIDO2 会前详情。 • 如果设备正在会话中播放，audio/video 则不会进入睡眠状态。 • 当显示器连接和断开连接时，最终用户会看到通知。 • 设备从操作系统收集诊断信息，以改进服务。 • 修复了软件安装日期的 “设置” 中显示的日期不正确的问题。
emrfs	4-29-2025	• 可用性改进和错误修复。

软件套装	发行日期	更改
2.13.0	3-31-2025	• 最终用户将以通知的形式看到产品满意度反馈调查。 • 增加了对 FIDO2 身份验证流程的预发行功能支持。查看FIDO2 会前详情。 • 如果设备正在会话中播放，audio/video 则不会进入睡眠状态。 • 当显示器连接和断开连接时，最终用户会看到通知。 • 设备从操作系统收集诊断信息，以改进服务。 • 修复了软件安装日期的 “设置” 中显示的日期不正确的问题。
2.12.0	1-30-2025	• 修复了最终用户在按下鼠标后退按钮后退出会话的问题。
2.11.2	1-24-2025	• 修复了鼠标在显示器上移动时，通话期间音频会嘎吱作响的问题。
2.11.1	12-27-2024	• 修复了双显示器自动扩展问题。 • 对 VoiceView 标签进行了细微改进。
2.11.0	12-19-2024	• WorkSpaces 瘦客户机现在支持 VoiceView 和放大镜。
2.10.0	11-22-2024	• 最终用户可以使用键盘快捷键来折叠设备工具栏。

软件套装	发行日期	更改
2.9.0	10-28-2024	• 管理员现在可以在 AWS 控制台中特定设备的设备详细信息页面下查看其最终用户的设备设置。 • WorkSpaces 瘦客户机现在支持单屏分辨率为 2K 的显示器。 • 最终用户可以在 WorkSpaces 瘦客户机设备上看到与网络诊断相关的通知。 • 现在，最终用户可以根据自己的喜好选择将设备工具栏放置在左侧或右侧。 • 修复了设备在睡眠或空闲时间未安装软件更新的问题。
2.8.1	09-26-2024	• 修复了设备从睡眠状态醒来后无法开启第二台显示器的严重问题。
2.8.0	09-06-2024	• 瘦客户机支持 4K 分辨率的显示器。 • 即使 WorkSpaces 瘦客户机设备管理服务暂时不可用，用户也可以连接到 VDI 会话。 • 修复了 AWS 控制台中的用户活动详情部分显示重复条目的问题。 • 最终用户可以在 WorkSpaces 瘦客户机 WorkSpaces 上流式传输时使用 PrintScreen 选项。

软件套装	发行日期	更改
2.7.1	08-27-2024	• 修复 Chromium 的 CVE-2024-7971 和 CVE-2024-7965 关键安全问题的未修补漏洞。
2.7.0	07-29-2024	• 提高了第二台显示器的性能。 • 修复了更改设备语言时工具栏语言不受影响的问题。 • 设备现在可以收集诊断信息以改进服务。
2.6.0	07-09-2024	• 用户可以推迟传入的软件更新，这样他们就可以不间断地完成工作。 • 设备设置允许用户忘记保存的 WiFi 网络。 • 改善会 audio/video 话中呼叫的性能。 • VDI 会话的某些用户设置在设备重新启动后仍会保留。
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 audio/video 话中呼叫的性能。
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。

软件套装	发行日期	更改
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。
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存在。

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 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。
- 您可以为环境中的设备配置标签，使其在注册设备时自动应用。

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。

使用控制台管理现有环境的标签

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。

使用控制台管理现有设备的标签

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。

使用控制台管理新设备的标签

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. 在设备创建标签部分，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。

设备创建后，将在环境中注册并应用设备创建标签。这仅在新设备注册期间发生。此外，应用`aws:thinclient:environment-id`系统标签时使用环境 ID 作为值。

使用控制台管理软件更新的标签

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，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 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 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
- Amazon WorkSpaces 瘦客户机的身份和访问管理
- Amazon WorkSpaces 瘦客户机的弹性
- Amazon WorkSpaces 瘦客户机中的漏洞分析和管理

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 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）。这包括您使用控制台、API 或 AWS 服务 使用 WorkSpaces 瘦客户机或其他客户机时 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。

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
- Amazon WorkSpaces 瘦客户机的静态数据加密
- 传输中加密
- 密钥管理
- 互联网工作流量隐私

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
  - 建立和维护 IAM 策略
  - 启用和禁用密钥政策
  - 轮换加密材料
  - 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
设备设置 WorkSpaces 瘦客户机设备设置	已启用	已启用
设备创建标签 WorkSpaces 瘦客户机环境设备创建标签	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。

亚马逊 WorkSpaces 瘦客户机如何使用 AWS KMS

Amazon Th WorkSpaces in Client 需要密钥策略才能使用您的客户托管密钥。

Amazon Th WorkSpaces in Client 要求密钥策略使用您的客户托管密钥进行以下内部操作：

- 向 AWS KMS 发送`GenerateDataKey`请求以加密数据。
- 向 AWS KMS 发送`Decrypt`请求以解密加密数据。

您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 WorkSpaces 瘦客户机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自主管理型密钥的访问。每个客户托管式密钥必须只有一个密钥策略，其中包含确定谁可以使用密钥以及如何使用密钥的声明。创建客户托管式密钥时，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。

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"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "thinclient.region.amazonaws.com",
                    "kms:CallerAccount": "111122223333"
                }
            }
        },
        {
            "Sid": "Allow Amazon WorkSpaces Thin Client service to encrypt and decrypt
 data",
            "Effect": "Allow",
            "Principal": {"Service": "thinclient.amazonaws.com"},
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:SourceArn":
                         "arn:aws:thinclient:region:111122223333:*",
```

```
                    "kms:EncryptionContext:aws:thinclient:arn":
                        "arn:aws:thinclient:region: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*"
            ],
            "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您的 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

您可以使用密钥政策和 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。

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、、GenerateDataKeyDecrypt、监控 Amazon Th WorkSpaces in Client 为访问由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": "1.09",
    "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"
            },
```

```
            "attributes": {
                "creationDate": "2024-04-08T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:44:22Z",
    "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"
}
```

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": "1.09",
    "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"
            },
            "attributes": {
                "creationDate": "2024-04-08T12:21:03Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:03:56Z",
    "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",
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "eventCategory": "Management"
}
```

GenerateDataKey (by service)

当 Amazon Th WorkSpaces in Client 使用GenerateDataKey保存的设备信息时，该GenerateDataKey操作用于加密数据。

在 KMS 密钥策略声明中允许该GenerateDataKey操作，Sid 为 “允许 Amazon WorkSpaces 瘦客户机服务加密和解密数据”。

以下示例事件记录了该 GenerateDataKey 操作：

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:03:56Z",
    "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",
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "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": "1.09",
    "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"
```

```
            },
            "attributes": {
                "creationDate": "2024-04-08T13:43:33Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:44:25Z",
    "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",
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "eventCategory": "Management"
```

```
}
```

Decrypt (by service)

当 WorkSpaces 瘦客户机设备访问环境或设备信息时，该Decrypt操作用于解密数据。在 KMS 密钥策略声明中允许该Decrypt操作，Sid 为 “允许 Amazon WorkSpaces 瘦客户机服务加密和解密数据”。

以下示例事件记录了通过以下方式授权的Decrypt操作Grant：

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "thinclient.amazonaws.com"
    },
    "eventTime": "2024-04-08T13:44:25Z",
    "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",
    "sharedEventID": "1234abcd-12ab-34cd-56ef-123456SAMPLE",
    "vpcEndpointId": "vpce-1234abcd567SAMPLE",
    "vpcEndpointAccountId": "thinclient.amazonaws.com",
    "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 Amazon Key Management Service 的安全最佳实践的更多信息，请参阅《AWS Key Management Service 开发人员指南》https://docs.aws.amazon.com/kms/latest/developerguide/overview.html。

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
- 使用身份进行身份验证
- 使用策略管理访问
- Amazon WorkSpaces 瘦客户机如何与 IAM 配合使用
- Ama WorkSpaces zon 瘦客户机的基于身份的策略示例
- AWS Amazon WorkSpaces 瘦客户机的托管策略
- 对 Amazon WorkSpaces 瘦客户机身份和访问进行故障排除

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，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。实例配置文件包含该角色，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 是指定组织或组织单位 (OU) 的最大权限的 JSON 策略 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。

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 特征	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	是
ACLs	否
ABAC（策略中的标签）	是

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

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。

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。

WorkSpaces 瘦客户机的策略操作

支持策略操作：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。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：

```
thinclient
```

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": [
      "thinclient:action1",
      "thinclient: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：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 WorkSpaces 瘦客户机资源类型及其列表 ARNs，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：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 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

ACLs 在 WorkSpaces 瘦客户机中

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 WorkSpaces 瘦客户机的 ABAC

支持 ABAC（策略中的标签）：是

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，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 WorkSpaces 瘦客户机上使用临时证书

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 IA M 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。

WorkSpaces 瘦客户机的跨服务主体权限

支持转发访问会话（FAS）：是

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。

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 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：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。

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 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 WorkSpaces 瘦客户机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 Amazon Th WorkSpaces in Client 操作、资源和条件密钥。 ARNs

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 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 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。

JSON

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

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。

JSON

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

AWS Amazon WorkSpaces 瘦客户机的托管策略

AWS 托管策略是由创建和管理的独立策略 AWS。 AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于您的使用场景的客户管理型策略来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务 的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管策略。

AWS 托管策略： AmazonWorkSpacesThinClientReadOnlyAccess

您可以将 `AmazonWorkSpacesThinClientReadOnlyAccess` 策略附加到 IAM 身份。此策略授予对 WorkSpaces 瘦客户机服务及其依赖项的完全访问权限。有关此托管策略的更多信息，请参阅《AWS 托管策略参考指南》 AmazonWorkSpacesThinClientReadOnlyAccess中的。

权限详细信息

该策略包含以下权限。

- `thinclient`（WorkSpaces 瘦客户机）-允许对所有 WorkSpaces 瘦客户机操作进行只读访问。
- `workspaces`(WorkSpaces)-允许描述 WorkSpaces 目录和连接别名的权限。这用于检查您的 WorkSpaces 资源是否与 WorkSpaces 瘦客户机兼容。它还用于在 WorkSpaces 瘦客户机 AWS 控制台中显示这些资源。
- `workspaces-web`(WorkSpaces Secure Browser)-允许描述 WorkSpaces Secure Browser门户和用户设置的权限。这用于检查您的 WorkSpaces Secure Browser资源是否与 WorkSpaces 瘦客户机兼容。它还用于在 WorkSpaces 瘦客户机 AWS 控制台中显示这些资源。
- `appstream`(AppStream 2.0)-允许描述 AppStream 2.0 堆栈的权限。这用于检查您的 AppStream 2.0 资源是否与 WorkSpaces 瘦客户机兼容。它还用于在 WorkSpaces 瘦客户机 AWS 控制台中显示这些资源。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowThinClientReadAccess",
      "Effect": "Allow",
      "Action": [
        "thinclient:GetDevice",
        "thinclient:GetDeviceDetails",
        "thinclient:GetEnvironment",
        "thinclient:GetSoftwareSet",
        "thinclient:ListDevices",
        "thinclient:ListDeviceSessions",
        "thinclient:ListEnvironments",
        "thinclient:ListSoftwareSets",
        "thinclient:ListTagsForResource"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource": "*"
```

```
    },
    {
      "Sid": "AllowWorkSpacesSecureBrowserAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces-web:GetPortal",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListPortals"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowAppStreamAccess",
      "Effect": "Allow",
      "Action": [
        "appstream:DescribeStacks"
      ],
      "Resource": "*"
    }
  ]
}
}
```

AWS 托管策略： AmazonWorkSpacesThinClientFullAccess

您可以将 AmazonWorkSpacesThinClientFullAccess 策略附加到 IAM 身份。此策略授予对 WorkSpaces 瘦客户机服务及其依赖项的完全访问权限。有关此托管策略的更多信息，请参阅 AmazonWorkSpacesThinClientFullAccess《AWS 托管策略参考指南》。

权限详细信息

该策略包含以下权限：

- thinclient（WorkSpaces 瘦客户机）-允许完全访问所有 WorkSpaces 瘦客户机操作。
- workspaces(WorkSpaces)-允许描述 WorkSpaces 目录和连接别名的权限。这用于检查您的 WorkSpaces 资源是否与 WorkSpaces 瘦客户机兼容。它还用于在 WorkSpaces 瘦客户机 AWS 控制台中显示这些资源。
- workspaces-web(WorkSpaces Secure Browser)-允许描述 WorkSpaces Secure Browser门户和用户设置的权限。这用于检查您的 WorkSpaces Secure Browser资源是否与 WorkSpaces 瘦客户机兼容。它还用于在 WorkSpaces 瘦客户机 AWS 控制台中显示这些资源。

- appstream(AppStream 2.0)-允许描述 AppStream 2.0 堆栈的权限。这用于检查您的 AppStream 2.0 资源是否与 WorkSpaces 瘦客户机兼容。它还用于在 WorkSpaces 瘦客户机 AWS 控制台中显示这些资源。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowThinClientFullAccess",
      "Effect": "Allow",
      "Action": [
        "thinclient:*"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeConnectionAliases",
        "workspaces:DescribeWorkspaceDirectories"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowWorkSpacesSecureBrowserAccess",
      "Effect": "Allow",
      "Action": [
        "workspaces-web:GetPortal",
        "workspaces-web:GetUserSettings",
        "workspaces-web:ListPortals"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowAppStreamAccess",
      "Effect": "Allow",
      "Action": [
        "appstream:DescribeStacks"
      ],
      "Resource": "*"
    }
```

```
  ]
}
}
```

WorkSpaces AWS 托管策略的瘦客户机更新

更改	描述	日期
AmazonWorkSpacesThinClientReadOnlyAccess - 更新的策略	WorkSpaces Thin Client 更新了政策，增加了对设备详细信息和 WorkSpaces 连接别名的有限读取权限。	2025 年 1 月 9 日
AmazonWorkSpacesThinClientFullAccess - 更新的策略	WorkSpaces Thin Client 更新了策略，增加了 WorkSpaces 连接别名的有限读取权限。	2025 年 1 月 9 日
AmazonWorkSpacesThinClientReadOnlyAccess - 更新的策略	WorkSpaces 瘦客户机更新了策略，增加了对 AppStream 2.0、 WorkSpaces Web 和的有限读取权限 WorkSpaces。	2024 年 8 月 9 日
AmazonWorkSpacesThinClientFullAccess：新策略	提供对 Amazon Th WorkSpaces in Client 的完全访问权限以及对所需相关服务的有限访问权限。	2024 年 8 月 9 日
AmazonWorkSpacesThinClientReadOnlyAccess：新策略	提供对 Amazon WorkSpaces 瘦客户机及其依赖项的只读访问权限。	2024 年 7 月 19 日
WorkSpaces 瘦客户机开始跟踪更改	WorkSpaces 瘦客户机开始跟踪其 AWS 托管策略的更改。	2024 年 7 月 19 日

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 `thinclient:`*`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:
 thinclient: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`thinclient:`*`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 瘦客户机，您必须向需要访问的人员或应用程序授予权限。如果使用 AWS IAM Identity Center 管理人员和应用程序，则可以向用户或组分配权限集来定义其访问权限级别。权限集会自动创建 IAM 策略并将其分配给与人员或应用程序关联的 IAM 角色。有关更多信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。

如果未使用 IAM Identity Center，则必须为需要访问的人员或应用程序创建 IAM 实体（用户或角色）。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。授予权限后，向用户或应用程序开发人员提供凭证。他们将使用这些凭证访问 AWS。要了解有关创建 IAM 用户、组、策略和权限的更多信息，请参阅《IAM 用户指南》中的 IAM 身份和 IAM 中的策略和权限。

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 (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 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 中的跨账户资源访问。

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架构相比，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。

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。

主题

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

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，该服务提供用户、角色或角色所执行操作的记录 AWS 服务。 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。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、发出请求的时间以及其他详细信息。

所有亚马逊 WorkSpaces 瘦客户机操作均由《亚马逊瘦客户端 API 参考》记录 CloudTrail 并记录在《亚马逊 WorkSpaces 瘦客户端 API 参考》中。例如，调用`DeleteDevice`和`GetSoftwareSet`操作会在 CloudTrail 日志文件中生成条目。`CreateEnvironment`

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：

- 请求是使用根用户凭证还是用户凭证发出的。
- 请求是否代表 IAM Identity Center 用户发出。
- 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。

CloudTrail 在您创建账户 AWS 账户 时在您的账户中处于活动状态，并且您自动可以访问 CloudTrail 活动历史记录。 CloudTrail 事件历史记录提供了过去 90 天中记录的管理事件的可查看、可搜索、可下载且不可变的记录。 AWS 区域有关更多信息，请参阅《AWS CloudTrail 用户指南》中的 “使用 CloudTrail 事件历史记录”。查看活动历史记录不 CloudTrail收取任何费用。

要持续记录 AWS 账户 过去 90 天内的事件，请创建跟踪或 CloudTrailLake 事件数据存储。

CloudTrail 步道

跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。使用创建的所有跟踪 AWS Management Console 都是多区域的。您可以通过使用 AWS CLI创建单区域或多区域跟踪。建议创建多区域跟踪，因为您可以捕获账户 AWS 区域 中的所有活动。如果您创建单区域跟踪，则只能查看跟踪的 AWS 区域中记录的事件。有关跟踪的更多信息，请参阅《AWS CloudTrail 用户指南》中的为您的 AWS 账户创建跟踪和为组织创建跟踪。

通过创建跟踪，您可以免费将正在进行的管理事件的一份副本传送到您的 Amazon S3 存储桶，但会收取 Amazon S3 存储费用。 CloudTrail 有关 CloudTrail 定价的更多信息，请参阅AWS CloudTrail 定价。有关 Amazon S3 定价的信息，请参阅 Amazon S3 定价。

CloudTrail 湖泊事件数据存储

CloudTrail L@@ ak e 允许你对自己的事件运行基于 SQL 的查询。 CloudTrail Lake 将基于行的 JSON 格式的现有事件转换为 Apache ORC 格式。ORC 是一种针对快速检索数据进行优化的列式存储格式。事件将被聚合到事件数据存储中，它是基于您通过应用高级事件选择器选择的条件的不可变的事件集合。应用于事件数据存储的选择器用于控制哪些事件持续存在并可供您查询。有关 CloudTrail Lake 的更多信息，请参阅AWS CloudTrail 用户指南中的使用 AWS CloudTrail Lake。

CloudTrail 湖泊事件数据存储和查询会产生费用。创建事件数据存储时，您可以选择要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。有关 CloudTrail 定价的更多信息，请参阅AWS CloudTrail 定价。

WorkSpaces 中的瘦客户机数据事件 CloudTrail

数据事件提供有关在资源上或资源中执行的资源操作的信息（例如，最终用户注册设备）。这些也称为数据层面操作。数据事件通常是高容量活动。默认情况下， CloudTrail 不记录数据事件。 CloudTrail 事件历史记录不记录数据事件。

记录数据事件将收取额外费用。有关 CloudTrail 定价的更多信息，请参阅AWS CloudTrail 定价。

您可以使用 CloudTrail 控制台、 AWS CLI或 CloudTrail API 操作记录 WorkSpaces 瘦客户机资源类型的数据事件。有关如何记录数据事件的更多信息，请参阅《AWS CloudTrail 用户指南》中的使用 AWS Management Console记录数据事件和使用 AWS Command Line Interface记录数据事件。

下表列出了您可以记录数据事件的 WorkSpaces 瘦客户机资源类型。数据事件类型（控制台）列显示要从控制 CloudTrail 台上的数据事件类型列表中选择的值。res ources.type 值列显示

该resources.type值，您将在使用或配置高级事件选择器时指定该值。 AWS CLI CloudTrail APIs“ APIs 记录到的数据 CloudTrail” 列显示了 CloudTrail 针对该资源类型记录的 API 调用。

数据事件类型（控制台）	resources.type 值	数据 APIs 已记录到 CloudTrail
ThinClientDevice	AWS::WorkSpacesThinClient::Device	• RegisterDevice • UpdateDeviceDetails

您可以将高级事件选择器配置为在 eventName、readOnly 和 resources.ARN 字段上进行筛选，从而仅记录那些对您很重要的事件。有关这些字段的更多信息，请参阅 AdvancedFieldSelector《AWS CloudTrail API 参考》中的 。

WorkSpaces 中的瘦客户机管理事件 CloudTrail

管理事件提供有关对中的资源执行的管理操作的信息 AWS 账户。这些也称为控制面板操作。默认情况下， CloudTrail 记录管理事件。

Amazon WorkSpaces 瘦客户机将所有 WorkSpaces 瘦客户机控制平面操作记录为管理事件。有关瘦客户机登录的 Amazon WorkSpaces 瘦客户机控制平面操作的列表 CloudTrail，请参阅《亚马逊 WorkSpaces 瘦客户机 API 参考》。 WorkSpaces

WorkSpaces 瘦客户机事件示例

事件代表来自任何来源的单个请求，包括有关所请求的 API 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，因此事件不会按任何特定顺序出现。

以下示例显示了一个演示该RegisterDevice操作 CloudTrail 的事件。


```
{
      "eventVersion": "1.10",
      "userIdentity": {
        "type": "Unknown",
        "accountId": "111111111111",
        "userName": "DSN: G1X11X11111111XX"
      },
      "eventTime": "2024-06-19T17:13:44Z",
      "eventSource": "thinclient.amazonaws.com",
      "eventName": "RegisterDevice",
      "awsRegion": "us-west-2",
```

```
      "sourceIPAddress": "AWS Internal",
      "userAgent": "AWS Internal",
      "requestParameters": {
        "dsn": "G1X11X11111111XX",
        "activationCode": "xxx1xxx1",
        "model": "AFTGAZL"
      },
      "responseElements": null,
      "requestID": "f626fb2b-a841-4b87-9a9b-685a62024058",
      "eventID": "214385d7-9249-4f60-af56-b4c951e0491d",
      "readOnly": false,
      "resources": [
        {
          "type": "AWS::ThinClient::Device",
          "ARN": "arn:aws:thinclient:us-west-2:111111111111:device/DEVICE_ID"
        }
      ],
      "eventType": "AwsApiCall",
      "managementEvent": false,
      "recipientAccountId": "111111111111",
      "eventCategory": "Data"
    }
```

以下示例显示了一个演示该UpdateDeviceDetails操作 CloudTrail 的事件。

```
{
      "eventVersion": "1.10",
      "userIdentity": {
        "type": "Unknown",
        "accountId": "111111111111",
        "userName": "DSN: G1X11X11111111XX"
      },
      "eventTime": "2024-10-21T17:46:27Z",
      "eventSource": "thinclient.amazonaws.com",
      "eventName": "UpdateDeviceDetails",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "AWS Internal",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "7d562fcf-a9ce-40da-9e5c-9ef390b8b83c",
      "eventID": "f294b614-b00c-45ef-b293-cd389121033a",
      "readOnly": false,
```

```
    "resources": [
      {
        "type": "AWS::ThinClient::Device",
        "ARN": "arn:aws:thinclient:us-west-2:111111111111:device/DEVICE_ID"
      }
    ],
    "eventType": "AwsServiceEvent",
    "managementEvent": false,
    "recipientAccountId": "111111111111",
    "serviceEventDetails": {
      "settings": {
        "network": {
          "ethernet": {
            "addresses": [
              {
                "gateway": "gateway",
                "localIp": "localIp",
                "type": "IPV4"
              }
            ],
            "connectionStatus": "NOT_CONNECTED"
          },
          "networkInterfaceInUse": "ETHERNET",
          "wifi": {
            "addresses": [
              {
                "gateway": "gateway",
                "localIp": "localIp",
                "type": "IPV4"
              }
            ],
            "connectionStatus": "NOT_CONNECTED"
          }
        },
        "peripherals": {
          "bluetooth": {
            "enabledStatus": "ENABLED"
          },
          "keyboards": [
            {
              "name": "name",
              "type": "USB"
            }
          ],
```

```
            "mice": [
              {
                "name": "name",
                "type": "BLUETOOTH"
              }
            ],
            "sound": {
              "microphones": [
                {
                  "name": "name",
                  "selectionStatus": "SELECTED",
                  "type": "BUILT_IN"
                }
              ],
              "speakers": [
                {
                  "name": "name",
                  "selectionStatus": "SELECTED",
                  "type": "BUILT_IN"
                }
              ]
            },
            "webcams": [
              {
                "name": "name",
                "selectionStatus": "SELECTED",
                "type": "USB"
              }
            ]
          },
          "powerAndSleep": {
            "sleepAfter": "FIFTEEN_MINUTES"
          }
        },
        "updatedAt": "2024-10-21T17:46:27.624Z"
      },
      "eventCategory": "Data"
    }
```


有关 CloudTrail 录音内容的信息，请参阅《AWS CloudTrail 用户指南》中的CloudTrail录制内容。

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 参考
- 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 VPC 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
AWS 托管策略： AmazonWorkSpacesThinClientFullAccess	Amazon Th WorkSpaces in Client 添加了 AmazonWorkSpacesThinClientFullAccess 托管策略版本 2。	2025 年 1 月 9 日
AWS 托管策略： AmazonWorkSpacesThinClientReadOnlyAccess	Amazon Th WorkSpaces in Client 添加了 AmazonWorkSpacesThinClientReadOnlyAccess 托管策略版本 3。	2025 年 1 月 9 日
使用记录亚马逊 WorkSpaces 瘦客户端 API 调用 AWS CloudTrail 设备设置 Amazon WorkSpaces 瘦客户机的静态数据加密	为数据事件添加了新的章节。 为设备设置添加了新部分。 更新了静态数据加密部分中的 KMS 信息。	2024 年 10 月 28 日
业务连续性	添加了有关业务连续性和灾难恢复的新章节。	2024 年 9 月 6 日
AWS 托管策略： AmazonWorkSpacesThinClientFullAccess	Amazon T WorkSpaces hin Client 添加了 AmazonWorkSpacesThinClientFullAccess 托管策略。	2024 年 8 月 9 日
AWS 托管策略： AmazonWorkSpacesThinClientReadOnlyAccess	Amazon Th WorkSpaces in Client 添加了 AmazonWorkSpacesThinClientR	2024 年 8 月 9 日

更改	描述	日期
	eadOnlyAccess 托管策略版本 2。	
为 WorkSpaces 瘦客户机配置 WorkSpaces 个人	更新了新的 WorkSpaces 个人版。	2024 年 8 月 7 日
为 WorkSpaces 瘦客户机配置 WorkSpaces 池	为新 WorkSpaces 矿池添加了新版块。	2024 年 8 月 7 日
AWS 托管策略： AmazonWorkSpacesThinClientReadOnlyAccess	Amazon T WorkSpaces hin Client 添加了 AmazonWorkSpacesThinClientReadOnlyAccess 托管策略。	2024年7月19日
AWS Amazon WorkSpaces 瘦客户机的托管策略	Amazon Th WorkSpaces in Client 已开始跟踪更改。	2024年7月19日
为 Amazon WorkSpaces 瘦客户机 WorkSpaces 进行配置	更新了操作系统列表。	2024 年 2 月 12 日
为 Amazon WorkSpaces 瘦客户机配置 AppStream 2.0	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。