aws

管理指南

Amazon WorkSpaces

Amazon WorkSpaces: 管理指南

Table of Contents

什么是亚马逊 WorkSpaces？

亚马逊 WorkSpaces 允许您为用户配置虚拟的、基于云的微软 Windows、亚马逊 Linux 或 Ubuntu Linux 桌面，即。WorkSpaces WorkSpaces 无需购买和部署硬件或安装复杂的软件。您可以根据需求的变更，快速添加或删除用户。用户可以从多个设备或 Web 浏览器访问自己的虚拟桌面。

有关更多信息，请参阅 Amazon WorkSpaces。

功能

- 选择您的操作系统（Windows、Amazon Linux、Ubuntu Linux），然后在一系列硬件配置、软件配置和 AWS 区域中选择。有关更多信息，请参阅 Amazon WorkSpaces 捆绑包和。the section called “创建自定义映像和捆绑包”
- 选择您的协议：PCoIP 或 WorkSpaces 流媒体协议 (WSP)。有关更多信息，请参见 Amazon 协议 WorkSpaces。
- Connect 连接到你的 WorkSpace ，然后从你上次停下来的地方从右边继续前进。 WorkSpaces提供持久的桌面体验。
- WorkSpaces 提供了按月或按小时计费的灵活性 WorkSpaces。有关更多信息，请参阅WorkSpaces 定价。
- 对于 Windows 桌面，您可以自带许可证和应用程序，也可以从适用于桌面应用程序的 AWS Marketplace 中购买应用程序。
- 为您的用户创建独立的托管目录，或者将您的本地目录 WorkSpaces 连接到您的本地目录，以便您的用户可以使用其现有凭证获得对公司资源的无缝访问权限。有关更多信息，请参见 目录。
- 使用与管理 WorkSpaces 本地桌面相同的工具进行管理。
- 使用多重身份验证 (MFA)，以增强安全性。
- 使用 AWS Key Management Service (AWS KMS) 来加密静态数据、磁盘 I/O 和卷快照。
- 控制允许用户访问自己的 IP 地址 WorkSpaces。

架构

对于 Windows 和 Linux WorkSpaces，它们都 WorkSpace 与一个虚拟私有云 (VPC) 以及一个用于存储和管理您 WorkSpaces和用户信息的目录相关联。有关更多信息，请参见 the section called “VPC 要求”。目录通过 AWS Directory Service 来管理，其中提供了以下选项：Simple AD、AD Connector 或

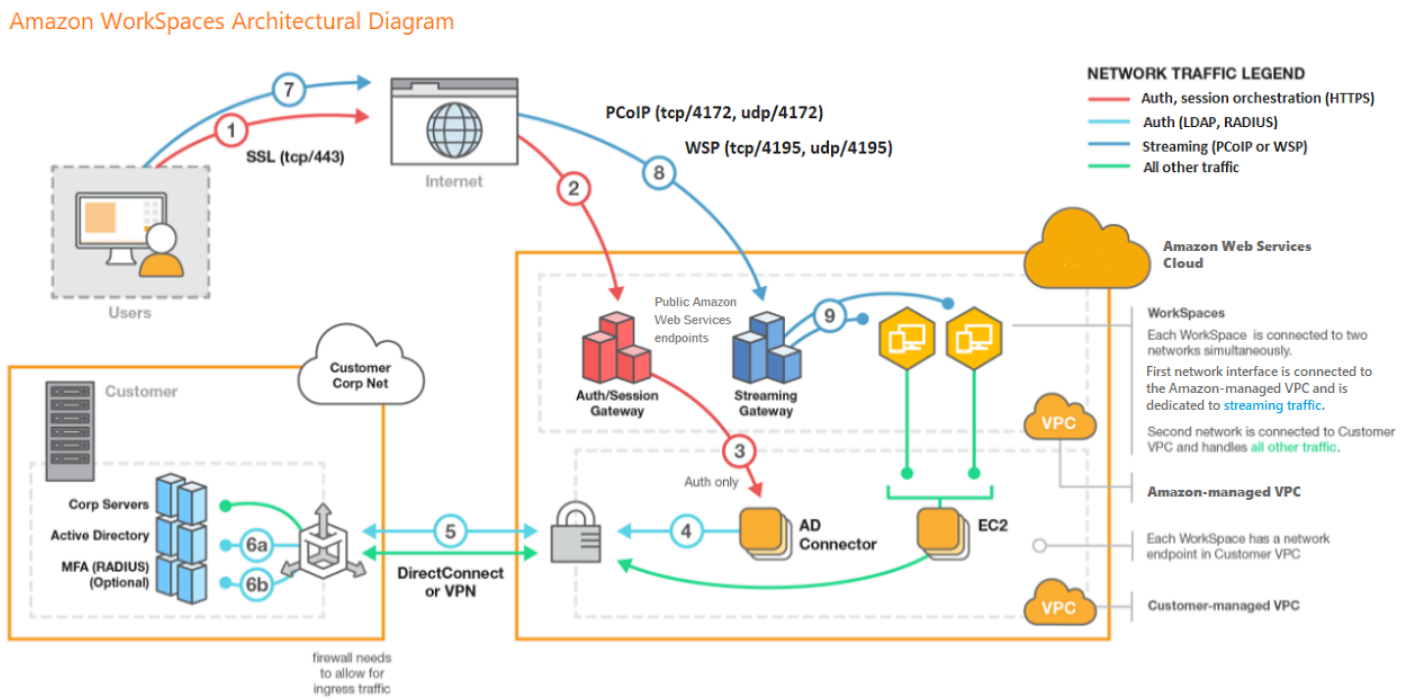
AWS Directory Service for Microsoft Active Directory（也称为 AWS 托管的 Microsoft AD）。有关更多信息，请参阅 AWS Directory Service 管理指南。

WorkSpaces 使用你的 Simple AD、AD Connector 或AWS托管的 Microsoft AD 目录对用户进行身份验证。用户使用 WorkSpaces 支持的设备上的客户端应用程序或者（对于 Windows WorkSpaces，则使用 Web 浏览器）访问他们的，然后使用自己的目录凭据登录。登录信息被发送到身份验证网关，该网关将流量转发到的 WorkSpace目录。用户通过身份验证后，系统会通过流式传输网关来启动流式传输流量。

客户端应用程序使用 HTTPS 通过端口 443 处理所有身份验证及与会话相关的信息，客户端应用程序使用端口 4172 (PCoIP) 和端口 4195 (WSP) 进行像素流式传输，使用端口 4172 WorkSpace 和 4195 进行网络运行状况检查。有关更多信息，请参见 用于客户端应用程序的端口。

每个接口 WorkSpace 都有两个与之关联的弹性网络接口：一个用于管理和流媒体的网络接口 (eth0) 和一个主网络接口 (eth1)。主网络接口的 IP 地址由 VPC（其子网与目录所用的子网相同）提供。这样可以确保来自您的流量 WorkSpace 可以轻松到达该目录。对 VPC 中资源的访问权限由分配给主网络接口的安全组控制。有关更多信息，请参见 网络接口。

下图显示了的架构 WorkSpaces。



访问你的 WorkSpace

您可以在支持的操作系统上使用支持 WorkSpaces 的 Web 浏览器，使用支持设备的客户端应用程序连接到您的。

> **Note**
>
> 您不能使用网络浏览器连接亚马逊 Linux WorkSpaces。

客户端应用程序可用于以下设备：

- Windows 计算机
- macOS 计算机
- Ubuntu Linux 18.04 计算机
- Chromebook
- iPad
- Android 设备
- Fire 平板电脑
- 零客户端设备（只有 PCoIP 支持 Teradici 零客户端设备。）

在 Windows、macOS 和 Linux 电脑上，你可以使用以下网络浏览器连接到 Windows 和 Ubuntu Linux： WorkSpaces

- Chrome 53 及更高版本（仅限 Windows 和 macOS）
- Firefox 49 及更高版本

有关更多信息，请参阅 Amazon WorkSpaces 用户指南中的WorkSpaces 客户。

定价

注册后AWS，您可以使用免费套餐优惠 WorkSpaces 免费开始使用。 WorkSpaces有关更多信息，请参阅WorkSpaces 定价。

使用 WorkSpaces，您只需为实际用量付费。根据捆绑包和您启动的套装数量 WorkSpaces 向您收费。的定价 WorkSpaces 包括使用 Simple AD 和 AD Connector，但不包括使用AWS托管 Microsoft AD。

WorkSpaces 提供按月或按小时计费 WorkSpaces。使用按月计费，您可以为无限使用支付固定费用，这最适合使用 WorkSpaces 全职服务的用户。使用按小时计费，您只需为每小时支付少量固定月费 WorkSpace，再加上每小时的 WorkSpace 低小时费率。有关更多信息，请参阅WorkSpaces 定价。

有关支持的区域的信息，请参阅WorkSpaces 定价。

如何开始

要创建 WorkSpace，请尝试以下教程之一：

- WorkSpaces 快速设置入门
- 启动使用 AWS Managed Microsoft AD 的 WorkSpace
- 启动使用 Simple AD 的 WorkSpace
- 启动使用 AD Connector 的 WorkSpace
- 启动使用受信任域的 WorkSpace

您可能还想浏览以下资源以了解有关 Amazon 的更多信息 WorkSpaces：

- 在云中预调配桌面
- 部署 Amazon 的最佳实践 WorkSpaces
- Amazon WorkSpaces 资源 — 包括白皮书、博客文章、网络研讨会和 re: Invent 会议
- 亚马逊 WorkSpaces 常见问题解答

WorkSpaces 快速设置入门

在本教程中，您将了解如何使用 WorkSpaces 和 AWS Directory Service 预调配基于云的虚拟 Microsoft Windows、Amazon Linux 或 Ubuntu Linux 桌面（也称为 WorkSpace）。

本教程使用快速设置选项启动您的 WorkSpace。只有在您从未启动过 WorkSpace 时该选项才可用。或者，请参阅 使用 WorkSpaces 启动虚拟桌面。

> **Note**
>
> 以下 AWS 区域支持快速设置：
>
> - 美国东部（弗吉尼亚州北部）
> - 美国西部（俄勒冈州）
> - 欧洲地区（爱尔兰）
> - 亚太地区（新加坡）
> - 亚太地区（悉尼）
> - 亚太地区（东京）
>
> 要更改您的区域，请参阅选择区域。

任务

开始前的准备工作

在您开始之前，确保您满足以下要求：

- 您必须拥有 AWS 账户才能创建或管理 WorkSpace。用户连接和使用其 WorkSpaces 不需要 AWS 账户。
- WorkSpaces 并非在所有区域均可用。请确认受支持的区域，并为您的 WorkSpaces 选择一个区域。有关受支持区域的更多信息，请参阅按 AWS 区域划分的 WorkSpaces 定价。

继续操作之前仔细阅读并理解以下内容也很有帮助：

- 启动 WorkSpace 时，您必须选择一个 WorkSpace 服务包。有关更多信息，请参阅 Amazon WorkSpaces 捆绑包和 Amazon WorkSpaces 定价。
- 启动 WorkSpace 时，必须选择要与捆绑包一起使用的协议（PCoIP 或 WorkSpaces Streaming Protocol [WSP]）。有关更多信息，请参阅Amazon 协议 WorkSpaces。
- 当您启动 WorkSpace 时，必须指定用户的配置文件信息，包括用户名和电子邮件地址。用户通过指定密码完成其配置文件。有关 WorkSpace 和用户的信息会存储在目录中。有关更多信息，请参阅目录。

快速设置的用途

快速设置将代表您完成以下任务：

- 创建一个 IAM 角色以允许 WorkSpaces 服务创建弹性网络接口并列出您的 WorkSpaces 目录。此角色的名称为 `workspaces_DefaultRole`。
- 创建虚拟私有云 (VPC)。如果您想改用现有 VPC，请确保其满足为以下项配置 VPC WorkSpaces中提及的要求，然后按照使用 WorkSpaces 启动虚拟桌面中列出的其中一个教程中的步骤进行操作。选择与要使用的 Active Directory 类型对应的教程。
- 在 VPC 中设置一个 Simple AD 目录并针对 Amazon WorkDocs 启用它。此 Simple AD 目录用于存储用户和 WorkSpace 信息。通过快速设置创建的第一个 AWS 账户是您的管理 AWS 账户。† 该目录还有一个管理员账户。有关更多信息，请参阅《AWS Directory Service 管理指南》中的创建的内容。
- 创建指定 AWS 账户并将其添加到目录。
- 创建 WorkSpaces。每个 WorkSpace 都会收到一个公有 IP 地址以提供互联网访问。运行模式为 AlwaysOn。有关更多信息，请参阅管理 WorkSpace 运行模式。
- 向指定的用户发送邀请电子邮件。如果您的用户没有收到邀请电子邮件，请参阅发送邀请电子邮件。

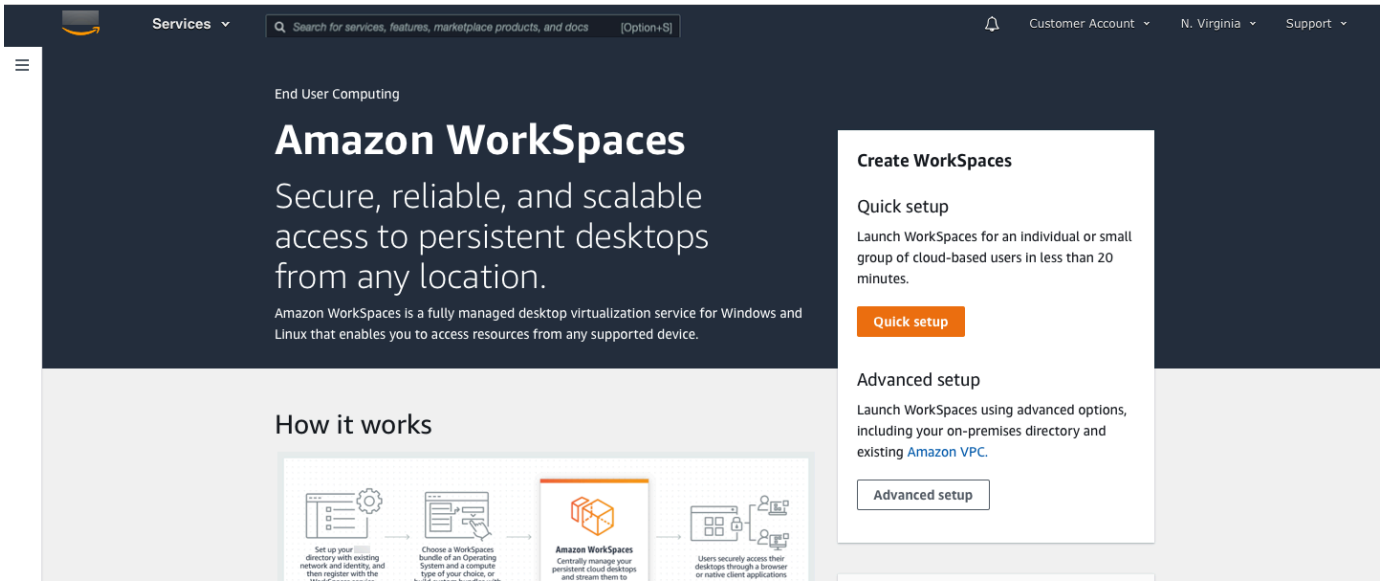
† 通过快速设置创建的第一个 AWS 账户是您的管理 AWS 账户。您无法从 WorkSpaces 控制台更新此 AWS 账户。请勿与任何其他人共享此账户的信息。要邀请其他用户使用 WorkSpaces，请为他们创建新的 AWS 账户。

步骤 1：启动 WorkSpace

使用快速设置，可以在几分钟内启动您的第一个 WorkSpace。

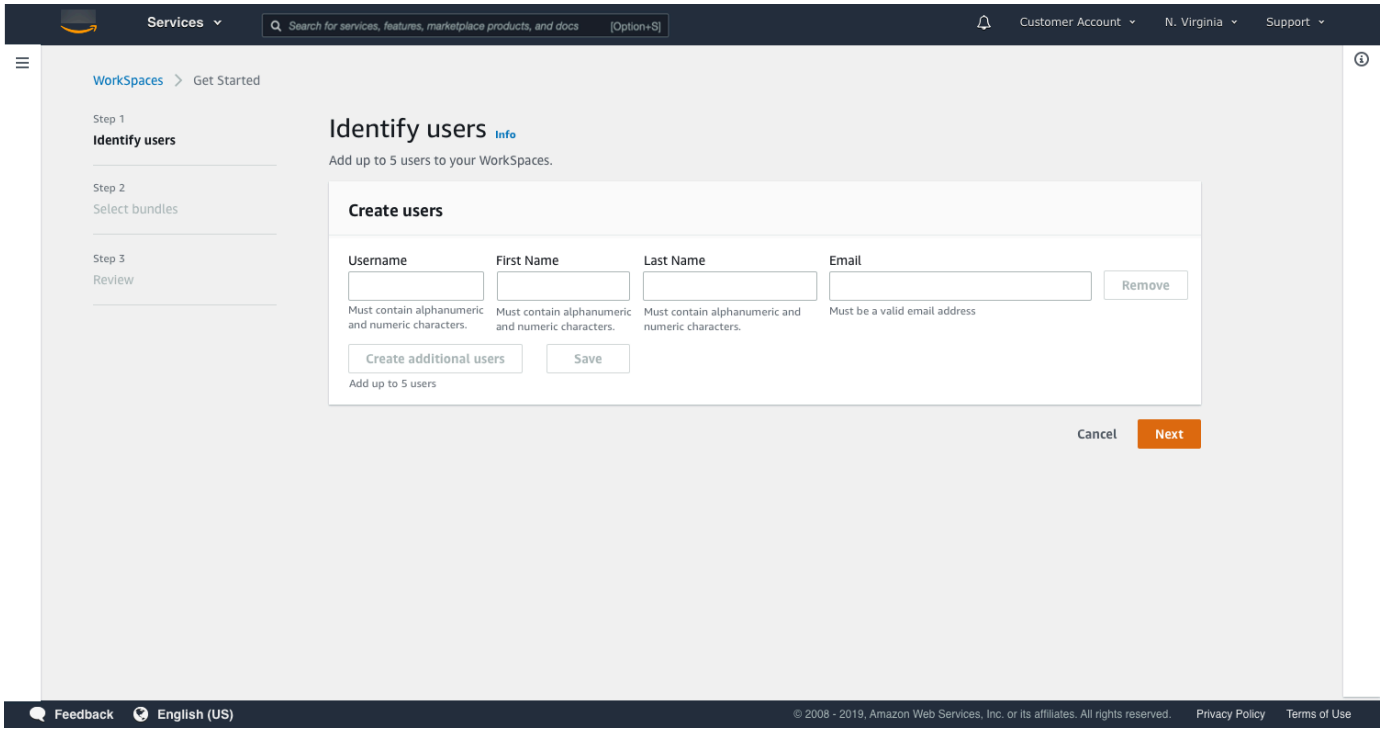
启动 WorkSpace

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。
2. 选择 Quick setup (快速设置)。如果您没有看到此按钮，则表明您已在此区域中启动 WorkSpace，或者您没有使用支持快速设置的区域之一。在这种情况下，请参阅使用 WorkSpaces 启动虚拟桌面。

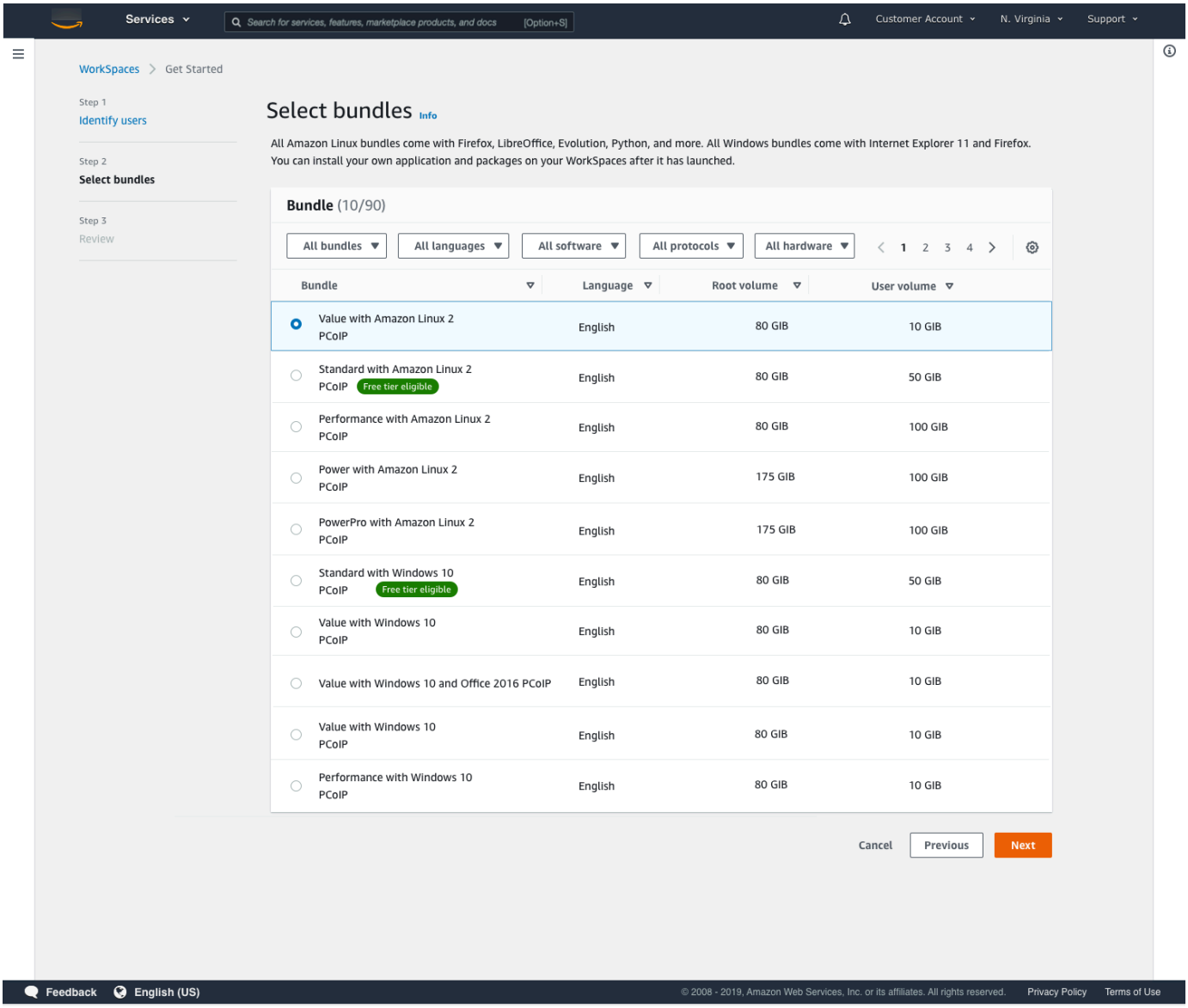


3. 对于识别用户，输入用户名、名字、姓氏和电子邮件。然后选择下一步。

> **Note**
>
> 如果这是您首次使用 WorkSpaces，建议您为自己创建一个用户以进行测试。



4. 对于捆绑包，为用户选择具有相应协议（PCoIP 或 WSP）的捆绑包（硬件和软件）。有关 Amazon WorkSpaces 可用的各种公有捆绑包的更多信息，请参阅 Amazon WorkSpaces 捆绑包。



5. 查看您的信息。然后选择创建 WorkSpace。
6. 您的 WorkSpace 大约需要 20 分钟才能启动。要监控进度，请转到左侧导航窗格并选择目录。您将看到一个目录正在创建，其初始状态为 REQUESTED，然后为 CREATING。

   目录创建完毕且状态变为 ACTIVE 后，您可以在左侧导航窗格中选择 WorkSpaces，来监控 WorkSpace 启动过程的进度。WorkSpace 的初始状态是 PENDING。启动完毕后，状态会变为 AVAILABLE，然后系统会向您为每个用户指定的电子邮件地址发送一封邀请电子邮件。如果您的用户没有收到邀请电子邮件，请参阅发送邀请电子邮件。

步骤 2：连接到 WorkSpace

收到邀请电子邮件后，您可以使用所选的客户端连接到 WorkSpace。登录后，此客户端会显示 WorkSpace 桌面。

连接到 WorkSpace

1. 如果您尚未为用户设置凭证，则打开邀请电子邮件中的链接，按照指示操作。记住您指定的密码，因为您需要它来连接到 WorkSpace。

   > **Note**
   >
   > 密码区分大小写，且长度必须介于 8 到 64 个字符之间 (含 8 和 64)。密码必须至少包含以下每个类别中的一个字符：小写字母 (a-z)、大写字母 (A-Z)、数字 (0-9) 以及字符集 ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/。

2. 查看《Amazon WorkSpaces 用户指南》中的 WorkSpaces 客户端，详细了解每个客户端的要求，然后执行以下一项操作：

   - 根据系统提示，下载一个客户端应用程序或启动 Web Access。
   - 如果系统未提示您且您尚未安装客户端应用程序，请打开 https://clients.amazonworkspaces.com/ ，并下载一个客户端应用程序或启动 Web Access。

   > **Note**
   >
   > 您不能使用 Web 浏览器 (Web Access) 连接到 Amazon Linux WorkSpaces。

3. 启动客户端，输入邀请电子邮件中的注册代码，然后选择 Register。
4. 当系统提示登录时，输入登录凭证，然后选择登录。
5. (可选) 当系统提示您保存凭证时，选择 Yes。

有关使用客户端应用程序（例如设置多台显示器或使用外围设备）的更多信息，请参阅《Amazon WorkSpaces 用户指南》中的 WorkSpaces 客户端和外围设备支持。

步骤 3：清除（可选）

如果您使用完为本教程创建的 WorkSpace，可将其删除。有关更多信息，请参阅the section called “删除 WorkSpace”。

> **Note**
>
> Simple AD 供您免费使用，可用于 WorkSpaces。如果连续 30 天没有一起使用 WorkSpaces 与您的 Simple AD 目录，则系统将自动取消注册该目录，无法再将其用于 Amazon WorkSpaces，而且将根据 AWS Directory Service 定价条款向您收取该目录的费用。要删除空目录，请参阅删除 WorkSpaces 的目录。如果您删除了 Simple AD 目录，则当您想重新开始使用 WorkSpaces 时，可以随时创建一个新的目录。

后续步骤

您可以继续自定义您刚创建的 WorkSpace。例如，您可以安装软件，然后在 WorkSpace 中创建自定义服务包。您还可以对 WorkSpaces 和 WorkSpaces 目录执行各种管理任务。有关更多信息，请参阅以下文档。

- 创建自定义 WorkSpaces 镜像和捆绑包
- 管理你的 WorkSpaces
- 管理 WorkSpaces 目录

要创建其他 WorkSpaces，请执行以下一项操作：

- 如果您想继续使用通过快速设置创建的 VPC 和 Simple AD 目录，则可以按照“使用 Simple AD 启动 WorkSpace”教程步骤 2：创建 WorkSpace部分中的步骤，为其他用户添加 WorkSpaces。
- 如果您需要使用其他目录类型或需要使用现有的 Active Directory，请参阅使用 WorkSpaces 启动虚拟桌面中的相应教程。

有关使用 WorkSpaces 客户端应用程序（例如设置多台显示器或使用外围设备）的更多信息，请参阅《Amazon WorkSpaces 用户指南》中的 WorkSpaces 客户端和外围设备支持。

WorkSpaces 高级设置入门

在本教程中，您将了解如何使用 WorkSpaces 和 AWS Directory Service 预调配基于云的虚拟 Microsoft Windows 或 Amazon Linux 桌面（也称为 WorkSpace）。

本教程使用高级设置选项启动您的 WorkSpace。

> **Note**
>
> 在所有区域中 WorkSpaces 都支持高级设置。

任务

- 开始前的准备工作
- 使用高级设置启动您的 WorkSpace

开始前的准备工作

开始前，请确保您拥有一个可用于创建或管理 WorkSpace 的 AWS 账户。用户连接和使用其 WorkSpaces 不需要 AWS 账户。

在继续之前，请仔细阅读并理解以下概念：

- 启动 WorkSpace 时，您必须选择一个 WorkSpace 服务包。有关更多信息，请参阅 Amazon WorkSpaces 服务包。
- 启动 WorkSpace 时，必须选择要与捆绑包一起使用的协议（PCoIP 或 WorkSpaces Streaming Protocol [WSP]）。有关更多信息，请参阅Amazon 协议 WorkSpaces。
- 当您启动 WorkSpace 时，必须指定用户的配置文件信息，包括用户名和电子邮件地址。用户通过指定密码完成其配置文件。有关 WorkSpace 和用户的信息会存储在目录中。有关更多信息，请参阅目录。

使用高级设置启动您的 WorkSpace

使用高级设置启动 WorkSpace：

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。

2. 选择以下一种目录类型，然后选择下一步：

   - AWS Managed 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。

WorkSpaces 的网络和访问权限

作为 WorkSpace 管理员，您必须了解以下有关 WorkSpaces 网络和访问权限的内容。

目录

Amazon 协议 WorkSpaces

亚马逊 WorkSpaces 支持两种协议：PCoIP 和 WorkSpaces 流媒体协议 (WSP)。您选择的协议取决于多个因素，例如您的用户将 WorkSpaces 从哪种设备访问他们的设备、您使用的操作系统 WorkSpaces、您的用户将面临的网络状况以及您的用户是否需要双向视频支持。

要求

只有满足以下最低要求才支持 WSP WorkSpaces 。

主机代理要求：

- Windows 主机代理版本 2.0.0.312 或更高版本
- Ubuntu 主机代理版本 2.1.0.501 或更高版本
- Amazon Linux 2 主机代理版本 2.0.0.596 或更高版本

客户端要求：

- Windows 原生客户端版本 5.1.0.329 或更高版本
- macOS 原生客户端版本 5.5.0 或更高版本
- Web Access

有关如何检查您的 WorkSpace 客户端版本和主机代理版本的更多信息，请参阅常见问题解答。

何时使用 WSP

- 如果您需要更高的损耗/延迟容忍度来支持您的最终用户网络状况。例如，有些用户正在全球 WorkSpaces 范围内访问或使用不可靠的网络。
- 如果您需要用户使用智能卡进行身份验证或在会话中使用智能卡。
- 如果您在会话中需要网络摄像头支持功能。
- 如果你需要将 Web Access 与支持 Windows Server 2019 的 WorkSpaces 捆绑包一起使用。
- 如果你需要使用 Ubuntu WorkSpaces。
- 如果你需要使用 Windows 11 BYOL WorkSpaces。
- 如果你需要使用基于 Ubuntu GPU 的捆绑包（Graphics.g4dn 和.g4dn）。 GraphicsPro
- 如果你需要你的用户在会话中使用身份验证 WebAuthn 器（例如 YubiKey 或 Windows Hello）进行身份验证。

何时使用 PCoIP

- 如果您要使用 iPad 或 Android Linux 客户端。
- 如果您使用 Teradici 零客户端设备。
- 如果你需要使用基于 GPU 的捆绑包（Graphics.g4dn、.g4dn、Graphics 或）。 GraphicsPro GraphicsPro
- 如果您需要将 Linux 捆绑包用于非智能卡使用案例。

- 如果您需要 WorkSpaces 在中国（宁夏）区域使用。

> **Note**
>
> - 一个目录中可以混合使用 PCoIP 和 WSP WorkSpaces 。
> - 用户可以同时拥有 PCoIP 和 WSP WorkSpace ，前提 WorkSpaces 是两者位于不同的目录中。同一个用户不能将 PCoIP 和 WSP 放在同一个目录 WorkSpace 中。有关为用户创建多个 WorkSpaces 项目的更多信息，请参阅为一个用户创建多个 WorkSpaces。
> - 您可以使用迁移功能在两个协议 WorkSpace 之间 WorkSpaces 迁移，该功能需要重新构建 WorkSpace。有关更多信息，请参阅 迁移 WorkSpace。
> - 如果您 WorkSpace 是使用 PCoIP 捆绑包创建的，则可以修改流媒体协议以在两个协议之间迁移，而无需重建，同时保留根卷。有关更多信息，请参阅修改协议。
> - 为了获得最佳的视频会议体验，我们建议仅使用 Power 或 PowerPro 捆绑包。

为以下项配置 VPC WorkSpaces

WorkSpaces WorkSpaces 在虚拟私有云 (VPC) 中启动你的。

您可以创建一个 VPC，其中包含两个私有子网供您使用， WorkSpaces 并在公有子网中创建一个 NAT 网关。或者，您可以创建一个 VPC，其中包含两个公有子网， WorkSpaces 并将每个子网与每个 WorkSpace子网关联一个公有 IP 地址或弹性 IP 地址。

有关 VPC 设计注意事项的更多信息，请参阅 Amazon WorkSpaces 部署中的 VPC 和联网最佳实践和部署最佳实践 WorkSpaces -VPC 设计。

内容

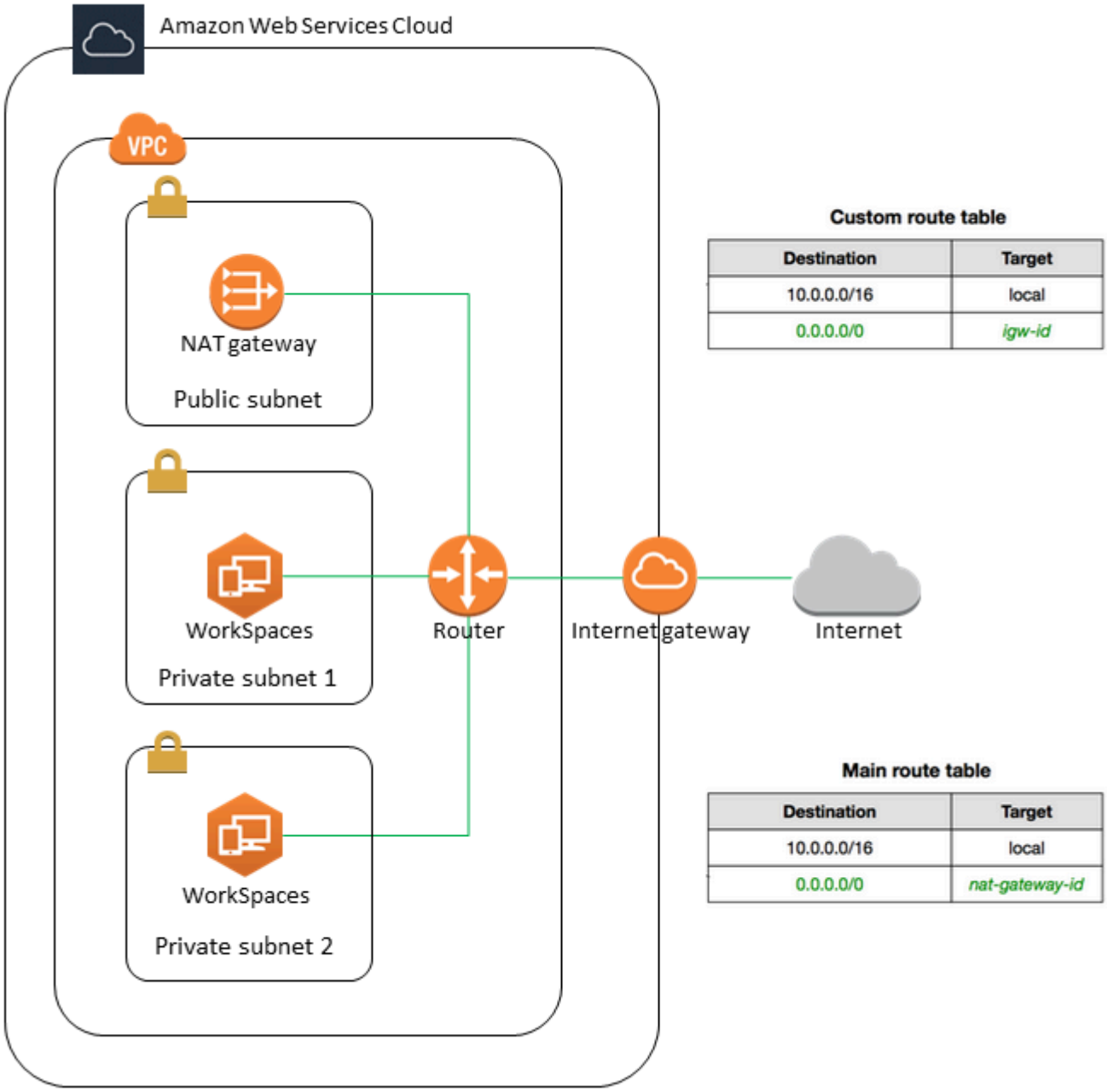
要求

您的 VPC 的子网必须位于您要启动 WorkSpaces的区域的不同可用区中。可用区是被设计为可以隔离其他可用区的故障的不同位置。通过启动独立可用区内的实例，您可以保护您的应用程序不受单一位置故障的影响。每个子网都必须完全位于一个可用区之内，不能跨越多个可用区。

> **Note**
>
> WorkSpaces Amazon 在每个受支持区域的部分可用区域中可用。要确定您可以将哪些可用区域用于您所使用的 VPC 的子网 WorkSpaces，请参阅Amazon 的可用区域 WorkSpaces。

配置具有私有子网和 NAT 网关的 VPC

如果您使用 AWS Directory Service 创建 AWS 托管 Microsoft 或 Simple AD，我们建议您为该 VPC 配置一个公有子网和两个私有子网。将您的目录配置为在私有子网 WorkSpaces 中启动您的目录。要在私有子网 WorkSpaces 中提供互联网访问权限，请在公有子网中配置 NAT 网关。



创建具有一个公有子网和两个私有子网的 VPC

1. 通过 https://console.aws.amazon.com/vpc/ 打开 Amazon VPC 控制台。
2. 选择创建 VPC。
3. 在要创建的 Resources（资源）下，选择 VPC and more（VPC 等）。
4. 对于 Name tag auto-generation（名称标签自动生成），为 VPC 输入名称。

5. 若要配置子网，请执行以下操作：

   a. 对于 Number of Availability Zones（可用区域数量），根据您的需求选择 1 或 2。

   b. 展开自定义 AZ，然后选择您的可用区。否则，请为您 AWS 选择它们。要做出适当的选择，请参阅 Amazon 的可用区域 WorkSpaces。

   c. 对于 Number of public subnets（公有子网数量），确保每个可用区有一个公有子网。

   d. 对于私有子网数量，确保每个可用区至少有一个私有子网。

   e. 为每个子网输入一个 CIDR 块。有关更多信息，请参阅《Amazon VPC 用户指南》中的子网大小调整。

6. 对于 NAT 网关，请选择每个 AZ 1 个。

7. 选择创建 VPC。

IPv6 CIDR 块

您可以将 IPv6 CIDR 块与您的 VPC 和子网关联。但是，如果您将子网配置为自动向子网中启动的实例分配 IPv6 地址，则无法使用 Graphics 服务包。（但是，你可以使用 Graphics.g4dn、GraphicsPro .g4dn 和捆绑包。）GraphicsPro 此限制来自不支持 IPv6 的上一代实例类型的硬件限制。

要解决此问题，可以在启动 Graphics 捆绑包之前暂时禁用 WorkSpaces 子网上的自动分配 IPv6 地址设置，然后在启动 Graphics 捆绑包后重新启用此设置（如果需要），以便任何其他分发包都能获得所需的 IP 地址。

默认情况下，禁用自动分配 IPv6 地址设置。要从 Amazon VPC 控制台检查此设置，请在导航窗格中选择子网。选择子网，然后依次选择操作、修改自动分配公有 IP。

通过公有子网配置 VPC

如果您愿意，您可以创建具有两个公有子网的 VPC。要为公有子网提供互联网访问权限，请将目录配置为自动分配弹性 IP 地址或手动为每个 WorkSpace子网分配弹性 IP 地址。 WorkSpaces

任务

- 第 1 步：创建 VPC
- 第 2 步：为您的 IP 地址分配公有 IP 地址 WorkSpaces

第 1 步：创建 VPC

如下所示创建具有一个公有子网的 VPC。

创建 VPC

1. 通过 https://console.aws.amazon.com/vpc/ 打开 Amazon VPC 控制台。
2. 选择创建 VPC。
3. 在要创建的 Resources（资源）下，选择 VPC and more（VPC 等）。
4. 对于 Name tag auto-generation（名称标签自动生成），为 VPC 输入名称。
5. 若要配置子网，请执行以下操作：
   a. 对于可用区数量，选择 2。
   b. 展开自定义 AZ，然后选择您的可用区。否则，请为您 AWS 选择它们。要做出适当的选择，请参阅 Amazon 的可用区域 WorkSpaces。
   c. 对于Number of public subnets（公有子网数量），选择 2。
   d. 对于 Number of private subnets（私有子网数量），选择 0。
   e. 为每个公有子网输入 CIDR 块。有关更多信息，请参阅《Amazon VPC 用户指南》中的子网大小调整。
6. 选择创建 VPC。

IPv6 CIDR 块

您可以将 IPv6 CIDR 块与您的 VPC 和子网关联。但是，如果您将子网配置为自动向子网中启动的实例分配 IPv6 地址，则无法使用 Graphics 服务包。（但是，你可以使用 GraphicsPro 捆绑包。）此限制来自不支持 IPv6 的上一代实例类型的硬件限制。

要解决此问题，可以在启动 Graphics 捆绑包之前暂时禁用 WorkSpaces 子网上的自动分配 IPv6 地址设置，然后在启动 Graphics 捆绑包后重新启用此设置（如果需要），以便任何其他分发包都能获得所需的 IP 地址。

默认情况下，禁用自动分配 IPv6 地址设置。要从 Amazon VPC 控制台检查此设置，请在导航窗格中选择子网。选择子网，然后依次选择操作、修改自动分配公有 IP。

第 2 步：为您的 IP 地址分配公有 IP 地址 WorkSpaces

您可以 WorkSpaces 自动或手动为您的分配公有 IP 地址。要使用自动分配，请参阅the section called “配置自动公有 IP 地址”。要手动分配公有 IP 地址，请使用以下过程。

WorkSpace 手动为分配公有 IP 地址

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 展开对的行（选择箭头图标），WorkSpace 并记下 WorkSpace IP 的值。这是的主私有 IP 地址 WorkSpace。
4. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
5. 在导航窗格中，选择弹性 IP。如果您没有可用的弹性 IP 地址，请选择分配弹性 IP 地址，并选择 Amazon 的 IPv4 地址池或客户拥有的 IPv4 地址池，然后选择分配。记下新的 IP 地址。
6. 在导航窗格中，选择网络接口。
7. 选择适合您的网络接口 WorkSpace。要查找您的网络接口 WorkSpace，请在搜索框中输入 WorkSpace IP 值（您之前记下的），然后按 Enter。WorkSpace IP 值与网络接口的主私有 IPv4 地址相匹配。请注意，网络接口的 VPC ID 与您的 WorkSpaces VPC 的 ID 相匹配。
8. 依次选择操作、管理 IP 地址。选择分配新 IP，然后选择是，更新。记下新的 IP 地址。
9. 依次选择 Actions、Associate Address。
10. 在关联弹性 IP 地址页面上，从地址中选择一个弹性 IP 地址。对于关联到私有 IP 地址，请指定新的私有 IP 地址，然后选择关联地址。

Amazon 的可用区域 WorkSpaces

当您创建用于 Amazon 的虚拟私有云 (VPC) 时 WorkSpaces，您的 VPC 的子网必须位于您启动 WorkSpaces的地区的不同可用区中。可用区是被设计为可以隔离其他可用区的故障的不同位置。通过启动独立可用区内的实例，您可以保护您的应用程序不受单一位置故障的影响。每个子网都必须完全位于一个可用区之内，不能跨越多个可用区。

可用区由区域代码后跟一个字母标识符表示；例如，us-east-1a。为了确保资源分布在某个地区的可用区中，我们独立地将可用区映射到每个 AWS 账户的名称。例如，您 AWS 账户的可用区us-east-1a可能与其他 AWS 账户的可用区不同。us-east-1a

要跨账户协调可用区，您必须使用 AZ ID（可用区的唯一、一致的标识符）。例如，use1-az2是该us-east-1区域的可用区 ID，它在每个 AWS 账户中的位置都相同。

通过查看 AZ ID，您可以确定一个账户中的资源相对于另一个账户中的资源所在的位置。例如，如果您在 AZ ID 为 use1-az2 的可用区中与另一个账户共享一个子网，则在 AZ ID 也为 use1-az2 的可用区中该账户便可使用这一子网。每个 VPC 和子网的 AZ ID 均显示在 Amazon VPC 控制台中。

Amazon WorkSpaces 仅在每个受支持区域的部分可用区域中可用。下表列出了每个区域中您可以使用的可用区 ID 列表。要查看您账户中可用区 ID 到可用区的映射，请参阅《AWS RAM 用户指南》中的您的资源的 AZ ID。

区域名称	区域代码	支持的 AZ ID
美国东部（弗吉尼亚州北部）	us-east-1	use1-az2, use1-az4, use1-az6
美国西部（俄勒冈州）	us-west-2	usw2-az1, usw2-az2, usw2-az3
亚太地区（孟买）	ap-south-1	aps1-az1, aps1-az2, aps1-az3
亚太地区（首尔）	ap-northeast-2	apne2-az1 , apne2-az3
亚太地区（新加坡）	ap-southeast-1	apse1-az1 , apse1-az2
亚太地区（悉尼）	ap-southeast-2	apse2-az1 , apse2-az3
亚太地区（东京）	ap-northeast-1	apne1-az1 , apne1-az4
加拿大（中部）	ca-central-1	cac1-az1, cac1-az2
欧洲地区（法兰克福）	eu-central-1	euc1-az2, euc1-az3
欧洲地区（爱尔兰）	eu-west-1	euw1-az1, euw1-az2, euw1-az3
欧洲地区（伦敦）	eu-west-2	euw2-az2, euw2-az3
南美洲（圣保罗）	sa-east-1	sae1-az1, sae1-az3
非洲（开普敦）	af-south-1	afs1-az1, afs1-az2, afs1-az3
以色列（特拉维夫）	il-central-1	ilc1-az1, ilc1-az2, ilc1-az3

区域名称	区域代码	支持的 AZ ID
AWS GovCloud （美国西部）	us-gov-west-1	usgw1-az1 ，usgw1-az2 ，usgw1-az3
AWS GovCloud （美国东部）	us-gov-east-1	usge1-az1 ，usge1-az2 ，usge1-az3

有关可用区和可用区 ID 的更多信息，请参阅 A mazon EC2 用户指南中的区域、可用区和本地区域。

的 IP 地址和端口要求 WorkSpaces

要连接到您的 WorkSpaces，您的 WorkSpaces 客户端所连接的网络必须为各种AWS服务的 IP 地址范围（按子集分组）开放某些端口。这些地址范围因 AWS 区域而异。这些相同端口还必须在客户端上运行的任何防火墙上处于打开状态。有关不同区域的 AWS IP 地址范围的更多信息，请参阅 Amazon Web Services 一般参考 中的 AWS IP 地址范围。

有关架构图，请参阅WorkSpaces 架构。有关其他架构图，请参阅部署 Amazon 的最佳实践 WorkSpaces。

用于客户端应用程序的端口

WorkSpaces 客户端应用程序需要通过以下端口进行出站访问：

端口 53 (UDP)

此端口用于访问 DNS 服务器。它必须对您的 DNS 服务器 IP 地址开放，以使客户端可以解析公有域名。如果您不使用 DNS 服务器进行域名解析，则此端口要求是可选的。

端口 443 (TCP)

此端口用于客户端应用程序更新、注册和身份验证。桌面客户端应用程序支持使用代理服务器处理端口 443 (HTTPS) 流量。要允许使用代理服务器，请打开客户端应用程序，依次选择 Advanced Settings 和 Use Proxy Server，指定代理服务器的地址和端口，然后选择 Save。

此端口必须对以下 IP 地址范围开放：

- GLOBAL 区域中的 AMAZON 子集。
- 所在区域中的AMAZON WorkSpace 子集。

- us-east-1 区域中的 AMAZON 子集。
- us-west-2 区域中的 AMAZON 子集。
- us-west-2 区域中的 S3 子集。

端口 4172 (UDP 和 TCP)

此端口用于流式传输 WorkSpace 桌面和 PCo WorkSpaces IP 的运行状况检查。此端口必须向 PCoIP 网关及其所在区域的运行状况检查服务器开放。 WorkSpace 有关更多信息，请参阅 运行状况检查服务器和 PCoIP 网关服务器：

对于 PCoIP WorkSpaces，桌面客户端应用程序不支持使用代理服务器，也不支持 TLS 解密和检查 UDP 中的端口 4172 流量（用于桌面流量）。它们需要直接连接到端口 4172。

端口 4195（UDP 和 TCP）

此端口用于流式传输 WorkSpace 桌面和流 WorkSpaces 媒体协议 (WSP) WorkSpaces 的运行状况检查。此端口必须向 WSP 网关 IP 地址范围和所在区域中的运行状况检查服务器开放。 WorkSpace 有关更多信息，请参阅 运行状况检查服务器和 WSP 网关服务器：

对于 WSP WorkSpaces， WorkSpaces Windows 客户端应用程序（版本 5.1 及更高版本）和 macOS 客户端应用程序（版本 5.4 及更高版本）支持对端口 4195 的 TCP 流量使用 HTTP 代理服务器，但不建议使用代理。不支持 TLS 解密和检查。有关更多信息，请参阅为 Windows WorkSpaces、Amazon Linux WorkSpaces 和 Ubuntu WorkSpaces 配置用于互联网访问的设备代理服务器设置。

> **Note**
>
> - 如果防火墙使用有状态筛选功能，则会自动打开临时（也称为动态）端口，以便允许返回通信。如果您的防火墙使用无状态筛选功能，则需要明确打开临时端口，以便允许返回通信。根据您的配置，需要打开的临时端口范围有所不同。
> - UDP 流量不支持代理服务器功能。如果您选择使用代理服务器，则客户端应用程序对 Amazon WorkSpaces 服务进行的 API 调用也会被代理。API 调用和桌面流量都应通过同一个代理服务器。

用于 Web Access 的端口

WorkSpaces Web 访问需要以下端口的出站访问权限：

端口 53 (UDP)

此端口用于访问 DNS 服务器。它必须对您的 DNS 服务器 IP 地址开放，以使客户端可以解析公有域名。如果您不使用 DNS 服务器进行域名解析，则此端口要求是可选的。

端口 80 (UDP 和 TCP)

此端口用于与 `https://clients.amazonworkspaces.com` 的初始连接，该连接之后切换为 HTTPS。它必须向所在区域EC2子集中的所有 IP 地址范围开放。 WorkSpace

端口 443 (UDP 和 TCP)

此端口用于使用 HTTPS 进行注册和身份验证。它必须向所在区域EC2子集中的所有 IP 地址范围开放。 WorkSpace

端口 4195（UDP 和 TCP）

WorkSpaces 对于配置为 WorkSpaces 流式传输协议 (WSP) 的端口，此端口用于流式传输 WorkSpaces 桌面流量。此端口必须对 WSP 网关 IP 地址范围开放。有关更多信息，请参见 WSP 网关服务器。

WSP Web 访问支持使用代理服务器处理端口 4195 TCP 流量，但不建议这样做。有关更多信息，请参阅为 Windows WorkSpaces、Amazon Linux WorkSpaces 和 Ubuntu WorkSpaces 配置用于互联网访问的设备代理服务器设置。

> **Note**
>
> 如果防火墙使用有状态筛选功能，则会自动打开临时（也称为动态）端口，以便允许返回通信。如果您的防火墙使用无状态筛选功能，则需要明确打开临时端口，以便允许返回通信。根据您的配置，必须打开的临时端口的范围有所不同。

通常，Web 浏览器会随机选择高范围内的源端口，用于流式传输流量。 WorkSpaces Web Access 无法控制浏览器选择的端口。您必须确保允许流量返回到该端口。

要添加到允许列表的域和 IP 地址

要使 WorkSpaces 客户端应用程序能够访问该 WorkSpaces 服务，必须将以下域和 IP 地址添加到客户端尝试访问服务的网络上的允许列表中。

要添加到允许列表的域和 IP 地址

类别	域或 IP 地址
验证码	https://opfcaptcha-prod.s3.amazonaws.com/
客户端自动更新	• https://d2td7dqidlhjx7.cloudfront.net/ • 在 AWS GovCloud （美国西部）区域： https://d2td7dqidlhjx7.cloudfront.net/prod/pdt/windows/ WorkSpacesAppCastx 64.xml
连接检查	https://connectivity.amazonworkspaces.com/
客户端指标（适用于 3.0 及以上的 WorkSpaces 客户端应用程序）	域: • https://skylight-client-ds.us-east-1.amazonaws • https://skylight-client-ds.us-west-2.amazonaws • https://skylight-client-ds.ap-south-1.amazonaw • https://skylight-client-ds.ap-northeast-2.amazonaws • https://skylight-client-ds.ap-southeast-1.amazonaws • https://skylight-client-ds.ap-southeast-2.amazonaws • https:// skylight-client-ds .ap-northeast-1.amazonaws • https://skylight-client-ds.ca-central-1.amazonaw • https://skylight-client-ds.eu-central-1.amazonaw • https://skylight-client-ds.eu-West-1.amazonaws.com

类别	域或 IP 地址
	• https://skylight-client-ds.eu-West-2 .amazonaws.com • https:// skylight-client-ds .sa-east-1.amazona ws.co • https://skylight-client-ds.af-south-1.amazona • https://skylight-client-ds.il-central-1.amazona • 在 AWS GovCloud （美国西部）区域： https://skylight-client-ds。 us-gov-we st-1.amazonaws.com • 在 AWS GovCloud （美国东部）区域： https://skylight-client-ds。 us-gov-ea st-1.amazonaws.com

类别	域或 IP 地址
动态消息服务（适用于 3.0 以上的 WorkSpaces 客户端应用程序）	域: • https://ws-client-service.us-east-1.amazonaws • https://ws-client-service.us-west-2.amazonaws • https://ws-client-service.ap-south-1.amazonaw • https://ws-client-service.ap-northeast-2.amazonaws • https://ws-client-service.ap-southeast-1.amazonaws • https://ws-client-service.ap-southeast-2.amazonaws • https:// ws-client-service .ap-northeast-1.amazonaws • https://ws-client-service.ca-central-1.amazonaw • https://ws-client-service.eu-central-1.amazonaw • https://ws-client-service.eu-West-1.amazonaws.com • https://ws-client-service.eu-West-2.amazonaws.com • https:// ws-client-service .sa-east-1.amazonaws.co • https://ws-client-service.af-south-1.amazona • https://ws-client-service.il-central-1.amazona • 在 AWS GovCloud （美国西部）区域： https://ws-client-service。 us-gov-west-1.amazonaws.com

类别	域或 IP 地址
	• 在 AWS GovCloud （美国东部）区域： https://ws-client-service。 us-gov-east-1.amazonaws.com

类别	域或 IP 地址
目录设置	在登录到客户目录之前，从客户机到客户目录进行身份验证 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<##>/<## ID> 从 macOS 客户端进行的连接： • https://d32i4gd7pg4909.cloudfront.net/ 客户目录设置： • https://d21ui22avrxoh6.cloudfront.net/prod/<区域>/<目录 ID> 客户目录级别联合品牌的登录页面图形： • 传统 — https://d1cbg795sa4g1u.cloudfront.net/prod/<区域>/<目录 ID> • 美国东部（弗吉尼亚州北部）— https://d2h1yryv1jxiq.cloudfront.net/ • 美国西部（俄勒冈州）— https://d1fq42e1gi7rtq.cloudfront.net/ • 亚太地区（孟买）— https://d1ctsk4u02kky7.cloudfront.net/ • 亚太地区（首尔）— https://dyoj3cw6iktvg.cloudfront.net • 亚太地区（新加坡）— https://d1525ef92caquk.cloudfront.net/ • 亚太地区（悉尼）— https://dodwxjr2amr8p.cloudfront.net/ • 亚太地区（东京）— https://d3v7kcib8ir2e1.cloudfront.net/

类别	域或 IP 地址
	• 加拿大（中部）— https://d1ebdk07rro1qy.cloudfront.net/ • 欧洲地区（法兰克福）— https://d39q4y7cndearu.cloudfront.net/ • 欧洲地区（爱尔兰）— https://d2127w6wvrc6l3.cloudfront.net/ • 欧洲地区（伦敦）— https://df4ahgpxbxqy2.cloudfront.net/ • 南美洲（圣保罗）— https://d2nezqurrjvain.cloudfront.net/ • 非洲（开普敦）— https://dr6ry0pwaoy23.cloudfront.net • 以色列（特拉维夫）— https://d2kmf63k5sit88.cloudfront.net 用于设计登录页面的 CSS 文件： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 登录页面的文件： • 美国东部（弗吉尼亚州北部）— https://d32i4gd7pg4909.cloudfront.net/ • 美国西部（俄勒冈州）— https://d18af777lco7lp.cloudfront.net/ • 亚太地区（孟买）— https://d78hovzzqqtsb.cloudfront.net/ • 亚太地区（首尔）— https://dtyv4uwoh7ynt.cloudfront.net/ • 亚太地区（新加坡）— https://d3qzmd7y07pz0i.cloudfront.net/

类别	域或 IP 地址
	• 亚太地区（悉尼）— https://dwcpoxuuza83q.cloudfront.net/ • 亚太地区（东京）— https://d2c2t8mxjhq5z1.cloudfront.net/ • 加拿大（中部）— https://d2wfbsypmqjmog.cloudfront.net/ • 欧洲地区（法兰克福）— https://d1whcm49570jjw.cloudfront.net/ • 欧洲地区（爱尔兰）— https://d3pgffbf39h4k4.cloudfront.net/ • 欧洲地区（伦敦）— https://d16q6638mh01s7.cloudfront.net/ • 南美洲（圣保罗）— https://d2lh2qc5bdoq4b.cloudfront.net/ • 非洲（开普敦）— https://di5ygl2cs0mrh.cloudfront.net/ • 以色列（特拉维夫）— https://d1a3pnge9on3sx.cloudfront.net 在 AWS GovCloud （美国西部）区域： • 客户目录设置： https://s3.amazonaws.com/ workspaces-client-properties /prod/pdt/ <directory ID> • 客户目录级别联合品牌的登录页面图形： https://workspace-client-assets-pdt.s3--us-gov-west 1.amazonaws.com • 用于设计登录页面的 CSS 文件： https://s3.amazonaws.com/ workspaces-clients-css /workspaces_v2.css • JavaScript 登录页面的文件：

类别	域或 IP 地址
	不适用 在 AWS GovCloud （美国东部）区域： • 客户目录设置： https://s3.amazonaws.com/ workspaces-client-properties /prod/osu/ <directory ID> • 客户目录级别联合品牌的登录页面图形： https://workspace-client-assets-pdt.s3--us-gov-east 1.amazonaws.com • 用于设计登录页面的 CSS 文件： https://s3.amazonaws.com/ workspaces-clients-css /workspaces_v2.css • JavaScript 登录页面的文件： 不适用
Forrester 日志服务	https://fls-na.amazon.com/
运行状况检查 (DRP) 服务器	运行状况检查服务器
会话前智能卡身份验证端点	• https://smartcard.us-east-1.signin.aws • https://smartcard.us-west-2.signin.aws • https://smartcard.ap-southeast-2.signin.aws • https://smartcard.ap-northeast-1.signin.aws • https://smartcard.eu-west-1.signin.aws • https://smartcard.signin。 amazonaws-us-gov.com

类别	域或 IP 地址
用户登录页面	https://<directory id>.awsapps.com/（其中，<目录 id> 是客户域） 在 AWS GovCloud（美国西部）和 AWS GovCloud（美国东部）区域： https://login。 us-gov-home<directory id><directory id>.awsapps.com/directory//（客户的域名在哪里）

类别	域或 IP 地址
WS 代理	域: • https://ws-broker-service.us-east-1.amazonaws • https://ws-broker-service-fips.us-east-1.amazonaws • https://ws-broker-service.us-west-2.amazonaws • https://ws-broker-service-fips.us-west-2.amazonaws • https://ws-broker-service.ap-south-1.amazonaw • https://ws-broker-service.ap-northeast-2.amazonaws • https://ws-broker-service.ap-southeast-1.amazonaws • https://ws-broker-service.ap-southeast-2.amazonaws • https:// ws-broker-service .ap-northeast-1.amazonaws • https://ws-broker-service.ca-central-1.amazonaw • https://ws-broker-service.eu-central-1.amazonaw • https://ws-broker-service.eu-West-1.amazonaws.com • https://ws-broker-service.eu-West-2.amazonaws.com • https:// ws-broker-service .sa-east-1.amazonaws.co • https://ws-broker-service.af-south-1.amazona

类别	域或 IP 地址
	• https://ws-broker-service.il-central-1.amazona • https://ws-broker-service。 us-gov-west-1.amazonaws.com • https://ws-broker-service-fips。 us-gov-west-1.amazonaws.com • https://ws-broker-service。 us-gov-east-1.amazonaws.com • https://ws-broker-service-fips。 us-gov-east-1.amazonaws.com

类别	域或 IP 地址
WorkSpaces API 端点	域: • https://workspaces.us-east-1.amazonaws.com • https://workspaces-fips.us-east-1.amazonaws.com • https://workspaces.us-west-2.amazonaws.com • https://workspaces-fips.us-west-2.amazonaws.com • https://workspaces.ap-south-1.amazonaws.com • https://workspaces.ap-northeast-2.amazonaws.com • https://workspaces.ap-southeast-1.amazonaws.com • https://workspaces.ap-southeast-2.amazonaws.com • https://workspaces.ap-northeast-1.amazonaws.com • https://workspaces.ca-central-1.amazonaws.com • https://workspaces.eu-central-1.amazonaws.com • https://workspaces.eu-west-1.amazonaws.com • https://workspaces.eu-west-2.amazonaws.com • https://workspaces.sa-east-1.amazonaws.com • https://workspaces.af-south-1.amazonaws.com

类别	域或 IP 地址
	• https://workspaces.il-central-1.amazonaws.com • https://workspaces。 us-gov-west-1.amazonaws.com • https://workspaces-fips。 us-gov-west-1.amazonaws.com • https://workspaces。 us-gov-east-1.amazonaws.com • https://workspaces-fips。 us-gov-east-1.amazonaws.com

类别	域或 IP 地址
WorkSpaces SAML 单点登录 (SSO) 的终端节点	域: • https://euc-sso-sm.us-east-1.amazonaws.com/v1/report-heartbe • https://euc-sso-sm-fips.us-east-1.amazonaws.com/v1/report-heartbe • https://euc-sso-sm.us-west-2.amazonaws.com/v1/report-heartbe • https://euc-sso-sm-fips.us-west-2.amazonaws.com/v1/report-heartbe • https://euc-sso-sm.ap-south-1.amazonaws.com/v1/report-heartb • https://euc-sso-sm.ap-northeast-2.amazonaws.com/v1/report-heartbe • https://euc-sso-sm.ap-southeast-1.amazonaws.com/v1/report-heartbe • https://euc-sso-sm.ap-southeast-2.amazonaws.com/v1/report-heartbe • https://euc-sso-sm.ap-northeast-1.amazonaws.com/v1/report-heartbe • https://euc-sso-sm.eu-central-1.amazonaws.com/v1/report-heartb • https://euc-sso-sm.eu-west-2.amazonaws.com/v1/report-heartbea • https://euc-sso-sm.af-south-1.amazonaws.com/v1/report-heart • https://euc-sso-sm.il-central-1.amazonaws.com/v1/report-heart • https://euc-sso-sm。 us-gov-west-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm-fips。 us-gov-west-1.amazonaws.com/v1/report-heartbeat

类别	域或 IP 地址
	• https://euc-sso-sm。 us-gov-east-1.amazonaws.com/v1/report-heartbeat • https://euc-sso-sm-fips。 us-gov-east-1.amazonaws.com/v1/report-heartbeat

要添加到 PCoIP 允许列表的域和 IP 地址

类别	域或 IP 地址
PCoIP 会话网关 (PSG)	PCoIP 网关服务器
会话代理 (PCM)	域: • https://skylight-cm.us-east-1.amazonaws.com • https://skylight-cm-fips.us-east-1.amazonaws • https://skylight-cm.us-west-2.amazonaws.com • https://skylight-cm-fips.us-west-2.amazonaws • https://skylight-cm.ap-south-1.amazonaws.com • https://skylight-cm.ap-northeast-2.amazonaws.com • https://skylight-cm.ap-southeast-1.amazonaws.com • https://skylight-cm.ap-southeast-2.amazonaws.com • https://skylight-cm.ap-northeast-1.amazonaws.com • https://skylight-cm.ca-central-1.amazonaws.com • https://skylight-cm.eu-central-1.amazonaws.com

类别	域或 IP 地址
	• https://skylight-cm.eu-west-1.amazonaws.com • https://skylight-cm.eu-west-2.amazonaws.com • https://skylight-cm.sa-east-1.amazonaws.com • https://skylight-cm.af-south-1.amazonaws.com • https://skylight-cm.il-central-1.amazonaws.com • https://skylight-cm。 us-gov-west-1.amazonaws.com • https://skylight-cm-fips。 us-gov-west-1.amazonaws.com • https://skylight-cm。 us-gov-east-1.amazonaws.com • https://skylight-cm-fips。 us-gov-east-1.amazonaws.com

类别	域或 IP 地址
适用于 PCoIP 的 Web Access TURN 服务器	服务器： • turn:*.us-east-1.rdn.amazonaws.com • turn:*.us-west-2.rdn.amazonaws.com • Web Access 目前在亚太地区（孟买）区域不可用。 • turn:*.ap-northeast-2.rdn.amazonaws.com • turn:*.ap-southeast-1.rdn.amazonaws.com • turn:*.ap-southeast-2.rdn.amazonaws.com • turn:*.ap-northeast-1.rdn.amazonaws.com • turn:*.ca-central-1.rdn.amazonaws.com • turn:*.eu-central-1.rdn.amazonaws.com • turn:*.eu-west-1.rdn.amazonaws.com • turn:*.eu-west-2.rdn.amazonaws.com • turn:*.sa-east-1.rdn.amazonaws.com • Web Access 目前不在非洲（开普敦）区域提供 • Web Access 目前在以色列（特拉维夫）地区不可用。

要添加到 WorkSpaces 直播协议 (WSP) 允许列表中的域和 IP 地址

类别	域或 IP 地址
WSP 会话网关 (WSG)	WSP 网关服务器
适用于 WSP 的 Web Access TURN 服务器	WSP 网关服务器

运行状况检查服务器

WorkSpaces 客户端应用程序通过端口 4172 和 4195 执行运行状况检查。这些检查验证 TCP 还是 UDP 流量是从 WorkSpaces 服务器流向客户端应用程序。要成功完成这些检查，您的防火墙策略必须允许指向以下区域运行状况检查服务器的 IP 地址的出站流量。

区域	运行状况检查主机名	IP 地址
美国东部（弗吉尼亚州北部）	drp-iad.amazonworkspaces.com	3.209.215.252 3.212.50.30 3.225.55.35 3.226.24.234 34.200.29.95 52.200.219.150
美国西部（俄勒冈州）	drp-pdx.amazonworkspaces.com	34.217.248.177 52.34.160.80 54.68.150.54 54.185.4.125 54.188.171.18 54.244.158.140
亚太地区（孟买）	drp-bom.amazonworkspaces.com	13.127.57.82 13.234.250.73
亚太地区（首尔）	drp-icn.amazonworkspaces.com	13.124.44.166 13.124.203.105 52.78.44.253

区域	运行状况检查主机名	IP 地址
		52.79.54.102
亚太地区（新加坡）	drp-sin.amazonworkspaces.com	3.0.212.144 18.138.99.116 18.140.252.123 52.74.175.118
亚太地区（悉尼）	drp-syd.amazonworkspaces.com	3.24.11.127 13.237.232.125
亚太地区（东京）	drp-nrt.amazonworkspaces.com	18.178.102.247 54.64.174.128
加拿大（中部）	drp-yul.amazonworkspaces.com	52.60.69.16 52.60.80.237 52.60.173.117 52.60.201.0
欧洲地区（法兰克福）	drp-fra.amazonworkspaces.com	52.59.191.224 52.59.191.225 52.59.191.226 52.59.191.227
欧洲地区（爱尔兰）	drp-dub.amazonworkspaces.com	18.200.177.86 52.48.86.38 54.76.137.224

区域	运行状况检查主机名	IP 地址
欧洲地区（伦敦）	drp-lhr.amazonworkspaces.com	35.176.62.54 35.177.255.44 52.56.46.102 52.56.111.36
南美洲（圣保罗）	drp-gru.amazonworkspaces.com	18.231.0.105 52.67.55.29 54.233.156.245 54.233.216.234
非洲（开普敦）	drp-cpt.amazonworkspaces.com/	13.244.128.155 13.245.205.255 13.245.216.116
以色列（特拉维夫）	drp-tlv.amazonworkspaces.com/	51.17.52.90 51.17.109.231 51.16.190.43
AWS GovCloud （美国西部）	drp-pdt.amazonworkspaces.com	52.61.60.65 52.61.65.14 52.61.88.170 52.61.137.87 52.61.155.110 52.222.20.88

区域	运行状况检查主机名	IP 地址
AWS GovCloud （美国东部）	drp-osu.amazonworkspaces.com	18.253.251.70 18.254.0.118

PCoIP 网关服务器

WorkSpaces 使用 PCoIP 通过端口 4172 将桌面会话流式传输到客户端。对于其 PCoIP 网关服务器，WorkSpaces 使用少量的 Amazon EC2 公有 IPv4 地址。这样，您可以为用于访问 WorkSpaces 的设备设置更为精细的防火墙策略。请注意， WorkSpaces 客户端目前不支持 IPv6 地址作为连接选项。

区域	公有 IP 地址范围
美国东部（弗吉尼亚州北部）	3.217.228.0 - 3.217.231.255 3.235.112.0 - 3.235.119.255 52.23.61.0 - 52.23.62.255
美国西部（俄勒冈州）	35.80.88.0-35.80.95.255 44.234.54.0 - 44.234.55.255 54.244.46.0 - 54.244.47.255
亚太地区（孟买）	13.126.243.0-13.126.243.255
亚太地区（首尔）	3.34.37.0 - 3.34.37.255 3.34.38.0 - 3.34.39.255 13.124.247.0 - 13.124.247.255
亚太地区（新加坡）	18.141.152.0 - 18.141.152.255 18.141.154.0 - 18.141.155.255 52.76.127.0 - 52.76.127.255
亚太地区（悉尼）	3.25.43.0 - 3.25.43.255

区域	公有 IP 地址范围
	3.25.44.0 - 3.25.45.255 54.153.254.0 - 54.153.254.255
亚太地区（东京）	18.180.178.0 - 18.180.178.255 18.180.180.0 - 18.180.181.255 54.250.251.0 - 54.250.251.255
加拿大（中部）	15.223.100.0 - 15.223.100.255 15.223.102.0 - 15.223.103.255 35.183.255.0 - 35.183.255.255
欧洲地区（法兰克福）	18.156.52.0 - 18.156.52.255 18.156.54.0 - 18.156.55.255 52.59.127.0 - 52.59.127.255
欧洲地区（爱尔兰）	3.249.28.0 - 3.249.29.255 52.19.124.0 - 52.19.125.255
欧洲地区（伦敦）	18.132.21.0 - 18.132.21.255 18.132.22.0 - 18.132.23.255 35.176.32.0 - 35.176.32.255
南美洲（圣保罗）	18.230.103.0 - 18.230.103.255 18.230.104.0 - 18.230.105.255 54.233.204.0 - 54.233.204.255
非洲（开普敦）	13.246.120.0-13.246.123.255
以色列（特拉维夫）	51.17.28.0-51.17.31.255

区域	公有 IP 地址范围
AWS GovCloud （美国西部）	52.61.193.0 - 52.61.193.255
AWS GovCloud （美国东部）	18.254.140.0-18.254.143.255

WSP 网关服务器

> **Important**
>
> 从 2020 年 6 月开始，通过端口 4195 而不是端口 4172 WorkSpaces 将 WSP 的桌面会话 WorkSpaces 流式传输到客户端。如果要使用 WSP WorkSpaces，请确保端口 4195 已通信。

WorkSpaces 为其 WSP 网关服务器使用少量的 Amazon EC2 公有 IPv4 地址。这样，您可以为用于访问 WorkSpaces 的设备设置更为精细的防火墙策略。请注意， WorkSpaces 客户端目前不支持 IPv6 地址作为连接选项。

区域	公有 IP 地址范围
美国东部（弗吉尼亚州北部）	• 3.227.4.0/22 • 44.209.84.0/22
美国西部（俄勒冈州）	34.223.96.0/22
亚太地区（孟买）	65.1.156.0/22
亚太地区（首尔）	3.35.160.0/22
亚太地区（新加坡）	13.212.132.0/22
亚太地区（悉尼）	3.25.248.0/22
亚太地区（东京）	3.114.164.0/22
加拿大（中部）	3.97.20.0/22
欧洲地区（法兰克福）	18.192.216.0/22

区域	公有 IP 地址范围
欧洲地区（爱尔兰）	3.248.176.0/22
欧洲地区（伦敦）	18.134.68.0/22
南美洲（圣保罗）	15.228.64.0/22
非洲（开普敦）	13.246.108.0/22
以色列（特拉维夫）	51.17.72.0/22
AWS GovCloud（美国西部）	• 3.32.139.0/24 • 3.30.129.0/24 • 3.30.130.0/23
AWS GovCloud（美国东部）	18.254.148.0/22

WSP 网关域名

下表列出了 WSP WorkSpace 网关域名。这些域必须是可联系的，WorkSpaces 客户端应用程序才能访问 WorkSpace WSP 服务。

区域	域
美国东部（弗吉尼亚州北部）	*.prod.us-east-1.highlander.aws.a2z.com
美国西部（俄勒冈州）	*.prod.us-west-2.highlander.aws.a2z.com
亚太地区（孟买）	*.prod.ap-south-1.highlander.aws.a2z.com
亚太地区（首尔）	*.prod.ap-northeast-2.highlander.aws.a2z.com
亚太地区（新加坡）	*.prod.ap-southeast-1.highlander.aws.a2z.com
亚太地区（悉尼）	*.prod.ap-southeast-2.highlander.aws.a2z.com
亚太地区（东京）	*.prod.ap-northeast-1.highlander.aws.a2z.com

区域	域
加拿大（中部）	*.prod.ca-central-1.highlander.aws.a2z.com
欧洲地区（法兰克福）	*.prod.eu-central-1.highlander.aws.a2z.com
欧洲地区（爱尔兰）	*.prod.eu-west-1.highlander.aws.a2z.com
欧洲地区（伦敦）	*.prod.eu-west-2.highlander.aws.a2z.com
南美洲（圣保罗）	*.prod.sa-east-1.highlander.aws.a2z.com
非洲（开普敦）	*.prod.af-south-1.highlander.aws.a2z.com
以色列（特拉维夫）	*.prod.il-central-1.highlander.aws.a2z.com
AWS GovCloud （美国西部）	*.prod。 us-gov-west-1.highlander.aws.a2z.com
AWS GovCloud （美国东部）	*.prod。 us-gov-east-1.highlander.aws.a2z.com

网络接口

每个 WorkSpace 都有以下网络接口：

- 主网络接口 (eth1) 提供与您的 VPC 内和互联网上的资源的连接，并用于加入目录。 WorkSpace
- 管理网络接口 (eth0) 已连接到安全的 WorkSpaces 管理网络。它用于将 WorkSpace桌面交互式传输到 WorkSpaces 客户端，并 WorkSpaces 允许管理 WorkSpace。

WorkSpaces 根据创建管理网络接口的区域，从不同的地址范围中选择管理网络接口 WorkSpaces 的 IP 地址。注册目录后， WorkSpaces 测试您的 VPC CIDR 和您的 VPC 中的路由表，以确定这些地址范围是否会造成冲突。如果区域中的所有可用地址范围存在冲突，则会显示一条错误消息，而且目录将无法注册。如果您在目录注册后更改了 VPC 中的路由表，则可能会导致冲突。

> **Warning**
>
> 请勿修改或删除连接到的任何网络接口 WorkSpace。这样做可能会导致无法 WorkSpace 访问或无法访问互联网。例如，如果您在目录级别启用了弹性 IP 地址的自动分配，则会在启动弹性 IP 地址（来自亚马逊提供的地址池） WorkSpace时分配给您。但是，如果您将自己拥有的弹

性 IP 地址关联到 WorkSpace，然后又将该弹性 IP 地址与解除关联 WorkSpace，则该地址将 WorkSpace 丢失其公有 IP 地址，并且不会自动从亚马逊提供的池中获取新的 IP 地址。要将亚马逊提供的资源池中的新公有 IP 地址与相关联 WorkSpace，您必须重新构建。WorkSpace如果您不想重建 WorkSpace，则必须将您拥有的另一个弹性 IP 地址与关联起来 WorkSpace。

管理接口 IP 范围

下表列出了用于管理网络接口的 IP 地址范围。

> **Note**
>
> - 如果您使用的是自带许可证 (BYOL) Windows WorkSpaces，则下表中的 IP 地址范围不适用。相反，PCoIP BYOL WorkSpaces 使用 54.239.224.0/20 IP 地址范围来管理所有区域的管理接口流量。AWS对于 WSP BYOL Windows WorkSpaces，54.239.224.0/20 和 10.0.0.0/8 的 IP 地址范围均适用于所有区域。AWS（除了您为 BY WorkSpaces OL 的管理流量选择的 /16 CIDR 块之外，还会使用这些 IP 地址范围。）
> - 如果您使用的是通过公共捆绑包 WorkSpaces 创建的 WSP，则除了下表所示的 pCoIP/WSP 范围外，IP 地址范围 10.0.0.0/8 还适用于所有AWS区域的管理接口流量。

区域	IP 地址范围
美国东部（弗吉尼亚州北部）	PCoIP/WSP：172.31.0.0/16、192.168.0.0/16、198.19.0.0/16 WSP：10.0.0.0/8
美国西部（俄勒冈州）	PCoIP/WSP：172.31.0.0/16、192.168.0.0/16 和 198.19.0.0/16 WSP：10.0.0.0/8
亚太地区（孟买）	PCoIP/WSP：192.168.0.0/16 WSP：10.0.0.0/8

区域	IP 地址范围
亚太地区（首尔）	PCoIP/WSP：198.19.0.0/16 WSP：10.0.0.0/8
亚太地区（新加坡）	PCoIP/WSP：198.19.0.0/16 WSP：10.0.0.0/8
亚太地区（悉尼）	PCoIP/WSP：172.31.0.0/16、192.168.0.0/16 和 198.19.0.0/16 WSP：10.0.0.0/8
亚太地区（东京）	PCoIP/WSP：198.19.0.0/16 WSP：10.0.0.0/8
加拿大（中部）	PCoIP/WSP：198.19.0.0/16 WSP：10.0.0.0/8
欧洲地区（法兰克福）	PCoIP/WSP：198.19.0.0/16 WSP：10.0.0.0/8
欧洲地区（爱尔兰）	PCoIP/WSP：172.31.0.0/16、192.168.0.0/16 和 198.19.0.0/16 WSP：10.0.0.0/8
欧洲地区（伦敦）	PCoIP/WSP：198.19.0.0/16 WSP：10.0.0.0/8
南美洲（圣保罗）	PCoIP/WSP：198.19.0.0/16 WSP：10.0.0.0/8

区域	IP 地址范围
非洲（开普敦）	PCoIP/WSP：172.31.0.0/16 和 198.19.0.0/16 WSP：10.0.0.0/8
以色列（特拉维夫）	PCoIP/WSP：198.19.0.0/16 WSP：10.0.0.0/8
AWS GovCloud（美国西部）	PCoIP/WSP：198.19.0.0/16 WSP：10.0.0.0/8 和 192.169.0.0/16
AWS GovCloud（美国东部）	PCoIP/WSP：198.19.0.0/16 WSP：10.0.0.0/8

管理接口端口

必须在所有人的管理网络接口上打开以下端口 WorkSpaces：

- 端口 4172 上的入站 TCP。用于基于 PCoIP 协议建立流式连接。
- 端口 4172 上的入站 UDP。用于基于 PCoIP 协议流式传输用户输入。
- 端口 4489 上的入站 TCP。这用于通过 Web 客户端访问。
- 端口 8200 上的入站 TCP。这用于管理和配置 WorkSpace。
- 端口 8201-8250 上的入站 TCP。这些端口用于建立流式连接以及基于 WSP 协议流式传输用户输入。
- 端口 8220 上的入站 UDP。此端口用于建立流式连接以及基于 WSP 协议流式传输用户输入
- 出站 TCP 端口 8443 和 9997。这用于通过 Web 客户端访问。
- 端口 3478、4172 和 4195 上的出站 UDP。这用于通过 Web 客户端访问。
- 端口 50002 和 55002 上的出站 UDP。用于流式传输。如果您的防火墙使用有状态筛选，则临时端口 50002 和 55002 会自动打开以允许返回通信。如果您的防火墙使用无状态筛选，则需要打开临时端口 49152 至 65535，以便允许返回通信。
- 根据管理接口 IP 范围中的定义，端口 80 上的出站 TCP 到 IP 地址 169.254.169.254，用于访问 EC2 元数据服务。分配给您的任何 HTTP 代理还 WorkSpaces 必须排除 169.254.169.254。

- 使用端口 1688 通过出站 TCP 将流量发送到 IP 地址 169.254.169.250 和 169.254.169.251，以允许针对基于公共捆绑包的 Workspaces 通过访问 Microsoft KMS 来激活 Windows。如果你使用的是自带许可证 (BYOL) Windows WorkSpaces，则必须允许访问自己的 KMS 服务器才能激活 Windows。
- 端口 1688 上的出站 TCP 到 IP 地址 54.239.236.220，允许访问微软 KMS 进行 Office 激活 BYOL。WorkSpaces

  如果你通过其中一个 WorkSpaces 公共捆绑包使用 Office，则用于激活 Office 的 Microsoft KMS 的 IP 地址会有所不同。要确定该 IP 地址，请找到的管理接口的 IP 地址 WorkSpace，然后将最后两个八位组替换为。64.250例如，如果管理接口的 IP 地址为 192.168.3.5，则用于激活 Office 的 Microsoft KMS 的 IP 地址为 192.168.64.250。
- 当 WorkSpace 主机配置为使用代理服务器 WorkSpaces 时，WSP 的出站 TCP 到 IP 地址 127.0.0.2。
- 源自环回地址 127.0.01 的通信。

在正常情况下，该 WorkSpaces 服务会为您 WorkSpaces配置这些端口。如果安装了任何安全软件或防火墙软件 WorkSpace 来阻塞其中任何端口，则 WorkSpace 可能无法正常运行或无法访问。

主接口端口

无论您使用哪种类型的目录，都必须在所有主网络接口上打开以下端口 WorkSpaces：

- 要进行互联网连接，以下端口必须开放到所有目的地的出站端口和从 WorkSpaces VPC 入站的端口。如果您想让他们能够访问互联网， WorkSpaces 则需要手动将其添加到您的安全组中。
  - TCP 80 (HTTP)
  - TCP 443 (HTTPS)
- 要与目录控制器通信，必须打开您的 WorkSpaces VPC 和目录控制器之间的以下端口。在 Simple AD 目录中，通过 AWS Directory Service 创建的安全组会正确配置这些端口。对于 AD Connector 目录，您可能需要调整 VPC 的默认安全组才能打开这些端口。
  - TCP/UDP 53 - DNS
  - TCP/UDP 88 - Kerberos 身份验证
  - UDP 123 - NTP
  - TCP 135 - RPC
  - UDP 137-138 - Netlogon
  - TCP 139 - Netlogon
  - TCP/UDP 389 - LDAP

- TCP/UDP 445 - SMB
- TCP/UDP 636-LDAPS（通过 TLS/SSL 的 LDAP）
- TCP 1024-65535 - RPC 动态端口

如果安装了任何安全软件或防火墙软件 WorkSpace 来阻塞其中任何端口，则 WorkSpace 可能无法正常运行或无法访问。

按区域划分的 IP 地址和端口要求

美国东部（弗吉尼亚州北部）

要添加到允许列表的域和 IP 地址

类别	详细信息
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
客户端自动更新	https://d2td7dqidlhjx7.cloudfront.net/
连接检查	https://connectivity.amazonworkspaces.com/
客户端指标（适用于 3.0 及以上的 WorkSpaces 客户端应用程序）	域： https://skylight-client-ds.us-east-1.amazonaws
动态消息服务（适用于 3.0 以上的 WorkSpaces 客户端应用程序）	域： https://ws-client-service.us-east-1.amazonaws
目录设置	在登录到客户目录之前，从客户机到客户目录进行身份验证 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<区域>/<目录 ID> 从 macOS 客户端进行的连接： • https://d32i4gd7pg4909.cloudfront.net/

类别	详细信息
	客户目录设置： • https://d21ui22avrxoh6.cloudfront.net/prod/<区域>/<目录 ID> 客户目录级别联合品牌的登录页面图形： • https://d1cbg795sa4g1u.cloudfront.net/prod/<区域>/<目录 ID> 用于设计登录页面的 CSS 文件： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 登录页面的文件： • 美国东部（弗吉尼亚州北部）— https://d32i4gd7pg4909.cloudfront.net/
Forrester 日志服务	https://fls-na.amazon.com/
运行状况检查 (DRP) 服务器	运行状况检查服务器
会话前智能卡身份验证端点	https://smartcard.us-east-1.signin.aws
注册依赖关系（用于 Web 访问和 Teradici PCoIP 零客户端）	https://s3.amazonaws.com
用户登录页面	https://<目录 ID>.awsapps.com/（其中，<目录 ID> 是客户的域）

类别	详细信息
WS 代理	域: • https://ws-broker-service.us-east-1.amazonaws • https://ws-broker-service-fips.us-east-1.amazonaws
WorkSpaces API 端点	域: https://workspaces.us-east-1.amazonaws.com
会话代理 (PCM)	域: • https://skylight-cm.us-east-1.amazonaws.com • https://skylight-cm-fips.us-east-1.amazonaws
适用于 PCoIP 的 Web Access TURN 服务器	服务器： • turn:*.us-east-1.rdn.amazonaws.com
运行状况检查主机名	drp-iad.amazonworkspaces.com
运行状况检查 IP 地址	• 3.209.215.252 • 3.212.50.30 • 3.225.55.35 • 3.226.24.234 • 34.200.29.95 • 52.200.219.150
PCoIP 网关服务器公有 IP 地址范围	• 3.217.228.0 - 3.217.231.255 • 3.235.112.0 - 3.235.119.255 • 52.23.61.0 - 52.23.62.255
WSP 网关服务器 IP 地址范围	• 3.227.4.0/22 • 44.209.84.0/22

类别	详细信息
WSP 网关域名	*.prod.us-east-1.highlander.aws.a2z.com
管理接口 IP 地址范围	• PCoIP/WSP：172.31.0.0/16、192.168.0.0/16、198.19.0.0/16 • WSP：10.0.0.0/8

美国西部（俄勒冈州）

要添加到允许列表的域和 IP 地址

类别	详细信息
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
客户端自动更新	https://d2td7dqidlhjx7.cloudfront.net/
连接检查	https://connectivity.amazonworkspaces.com/
客户端指标（适用于 3.0 及以上的 WorkSpaces 客户端应用程序）	域： https://skylight-client-ds.us-west-2.amazonaws
动态消息服务（适用于 3.0 以上的 WorkSpaces 客户端应用程序）	域： https://ws-client-service.us-west-2.amazonaws
目录设置	在登录到客户目录之前，从客户机到客户目录进行身份验证 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<区域>/<目录 ID> 从 macOS 客户端进行的连接： • https://d32i4gd7pg4909.cloudfront.net/ 客户目录设置：

类别	详细信息
	• https://d21ui22avrxoh6.cloudfront.net/prod/<区域>/<目录 ID> 客户目录级别联合品牌的登录页面图形： • https://d1cbg795sa4g1u.cloudfront.net/prod/<区域>/<目录 ID> 用于设计登录页面的 CSS 文件： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 登录页面的文件： • 美国西部（俄勒冈州）— https://d18af777lco7lp.cloudfront.net/
Forrester 日志服务	https://fls-na.amazon.com/
运行状况检查 (DRP) 服务器	运行状况检查服务器
会话前智能卡身份验证端点	https://smartcard.us-west-2.signin.aws
注册依赖关系（用于 Web 访问和 Teradici PCoIP 零客户端）	https://s3.amazonaws.com
用户登录页面	https://<目录 ID>.awsapps.com/（其中，<目录 ID> 是客户的域）
WS 代理	域: • https://ws-broker-service.us-west-2.amazonaws • https://ws-broker-service-fips.us-west-2.amazonaws

类别	详细信息
WorkSpaces API 端点	域: • https://workspaces.us-west-2.amazonaws.com • https://workspaces-fips.us-west-2.amazonaws.com
会话代理 (PCM)	域: • https://skylight-cm.us-west-2.amazonaws.com • https://skylight-cm-fips.us-west-2.amazonaws
适用于 PCoIP 的 Web Access TURN 服务器	服务器： • turn:*.us-west-2.rdn.amazonaws.com
运行状况检查主机名	drp-pdx.amazonworkspaces.com
运行状况检查 IP 地址	• 34.217.248.177 • 52.34.160.80 • 54.68.150.54 • 54.185.4.125 • 54.188.171.18 • 54.244.158.140
PCoIP 网关服务器公有 IP 地址范围	• 35.80.88.0-35.80.95.255 • 44.234.54.0 - 44.234.55.255 • 54.244.46.0 - 54.244.47.255
WSP 网关服务器 IP 地址范围	34.223.96.0/22
WSP 网关域名	*.prod.us-west-2.highlander.aws.a2z.com

类别	详细信息
管理接口 IP 地址范围	• PCoIP/WSP：172.31.0.0/16、192.168.0.0/16、198.19.0.0/16 • WSP：10.0.0.0/8

亚太地区（孟买）

要添加到允许列表的域和 IP 地址

类别	详细信息
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
客户端自动更新	https://d2td7dqidlhjx7.cloudfront.net/
连接检查	https://connectivity.amazonworkspaces.com/
客户端指标（适用于 3.0 及以上的 WorkSpaces 客户端应用程序）	域： https://skylight-client-ds.ap-south-1.amazonaw
动态消息服务（适用于 3.0 以上的 WorkSpaces 客户端应用程序）	域： https://ws-client-service.ap-south-1.amazonaw
目录设置	在登录到客户目录之前，从客户机到客户目录进行身份验证 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<区域>/<目录 ID> 从 macOS 客户端进行的连接： • https://d32i4gd7pg4909.cloudfront.net/ 客户目录设置：

类别	详细信息
	• https://d21ui22avrxoh6.cloudfront.net/prod/<区域>/<目录 ID> 客户目录级别联合品牌的登录页面图形： • https://d1cbg795sa4g1u.cloudfront.net/prod/<区域>/<目录 ID> 用于设计登录页面的 CSS 文件： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 登录页面的文件： • 亚太地区（孟买）— https://d78hovzzqqtsb.cloudfront.net/
Forrester 日志服务	https://fls-na.amazon.com/
运行状况检查 (DRP) 服务器	运行状况检查服务器
注册依赖关系（用于 Web 访问和 Teradici PCoIP 零客户端）	https://s3.amazonaws.com
用户登录页面	https://<目录 ID>.awsapps.com/（其中，<目录 ID> 是客户的域）
WS 代理	域： • https://ws-broker-service.ap-south-1.amazonaw
WorkSpaces API 端点	域： • https://workspaces.ap-south-1.amazonaws.com

类别	详细信息
会话代理 (PCM)	域： • https://skylight-cm.ap-south-1.amazonaws.com
适用于 PCoIP 的 Web Access TURN 服务器	Web Access 目前在亚太地区（孟买）区域不可用
运行状况检查主机名	drp-bom.amazonworkspaces.com
运行状况检查 IP 地址	• 13.127.57.82 • 13.234.250.73
PCoIP 网关服务器公有 IP 地址范围	13.126.243.0-13.126.243.255
WSP 网关服务器 IP 地址范围	65.1.156.0/22
WSP 网关域名	*.prod.ap-south-1.highlander.aws.a2z.com
管理接口 IP 地址范围	• PCoIP/WSP：192.168.0.0/16 • WSP：10.0.0.0/8

亚太地区（首尔）

要添加到允许列表的域和 IP 地址

类别	详细信息
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
客户端自动更新	https://d2td7dqidlhjx7.cloudfront.net/
连接检查	https://connectivity.amazonworkspaces.com/
设备指标（适用于 1.0 及更高版本和 2.0 WorkSpaces 及更高版本的客户端应用程序）	https://device-metrics-us-2.amazon.com/

类别	详细信息
客户端指标（适用于 3.0 及以上的 WorkSpaces 客户端应用程序）	域： https://skylight-client-ds.ap-northeast-2.amazonaws
动态消息服务（适用于 3.0 以上的 WorkSpaces 客户端应用程序）	域： https://ws-client-service.ap-northeast-2.amazonaws

类别	详细信息
目录设置	在登录到客户目录之前，从客户机到客户目录进行身份验证 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<区域>/<目录 ID> 从 macOS 客户端进行的连接： • https://d32i4gd7pg4909.cloudfront.net/ 客户目录设置： • https://d21ui22avrxoh6.cloudfront.net/prod/<区域>/<目录 ID> 客户目录级别联合品牌的登录页面图形： • https://d1cbg795sa4g1u.cloudfront.net/prod/<区域>/<目录 ID> 用于设计登录页面的 CSS 文件： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 登录页面的文件： • 亚太地区（首尔）— https://dtyv4uwoh7ynt.cloudfront.net/
Forrester 日志服务	https://fls-na.amazon.com/
运行状况检查 (DRP) 服务器	运行状况检查服务器

类别	详细信息
注册依赖关系（用于 Web 访问和 Teradici PCoIP 零客户端）	https://s3.amazonaws.com
用户登录页面	https://<目录 ID>.awsapps.com/（其中，<目录 ID> 是客户的域）
WS 代理	域： • https://ws-broker-service.ap-northeast-2.amazonaws
WorkSpaces API 端点	域： • https://workspaces.ap-northeast-2.amazonaws.com
会话代理 (PCM)	域： • https://skylight-cm.ap-northeast-2.amazonaws.com
适用于 PCoIP 的 Web Access TURN 服务器	服务器： • turn:*.ap-northeast-2.rdn.amazonaws.com
运行状况检查主机名	drp-icn.amazonworkspaces.com
运行状况检查 IP 地址	• 13.124.44.166 • 13.124.203.105 • 52.78.44.253 • 52.79.54.102
PCoIP 网关服务器公有 IP 地址范围	• 3.34.37.0 - 3.34.37.255 • 3.34.38.0 - 3.34.39.255 • 13.124.247.0 - 13.124.247.255
WSP 网关服务器 IP 地址范围	3.35.160.0/22

类别	详细信息
WSP 网关域名	*.prod.ap-northeast-2.highlander.aws.a2z.com
管理接口 IP 地址范围	• PCoIP/WSP：198.19.0.0/16 • WSP：10.0.0.0/8

亚太地区（新加坡）

要添加到允许列表的域和 IP 地址

类别	详细信息
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
客户端自动更新	https://d2td7dqidlhjx7.cloudfront.net/
连接检查	https://connectivity.amazonworkspaces.com/
客户端指标（适用于 3.0 及以上的 WorkSpaces 客户端应用程序）	域： https://skylight-client-ds.ap-southeast-1.amazonaws
动态消息服务（适用于 3.0 以上的 WorkSpaces 客户端应用程序）	域：https://ws-client-service.ap-southeast-1.amazonaws.com
目录设置	在登录到客户目录之前，从客户机到客户目录进行身份验证 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<区域>/<目录 ID> 从 macOS 客户端进行的连接： • https://d32i4gd7pg4909.cloudfront.net/ 客户目录设置：

类别	详细信息
	• https://d21ui22avrxoh6.cloudfront.net/prod/<区域>/<目录 ID> 客户目录级别联合品牌的登录页面图形： • https://d1cbg795sa4g1u.cloudfront.net/prod/<区域>/<目录 ID> 用于设计登录页面的 CSS 文件： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 登录页面的文件： • 亚太地区（新加坡）— https://d3qzmd7y07pz0i.cloudfront.net/
Forrester 日志服务	https://fls-na.amazon.com/
运行状况检查 (DRP) 服务器	运行状况检查服务器
注册依赖关系（用于 Web 访问和 Teradici PCoIP 零客户端）	https://s3.amazonaws.com
用户登录页面	https://<目录 ID>.awsapps.com/（其中，<目录 ID> 是客户的域）
WS 代理	域： • https://ws-broker-service.ap-southeast-1.amazonaws
WorkSpaces API 端点	域： • https://workspaces.ap-southeast-1.amazonaws.com

类别	详细信息
会话代理 (PCM)	域： • https://skylight-cm.ap-southeast-1.amazonaws.com
适用于 PCoIP 的 Web Access TURN 服务器	服务器： • turn:*.ap-southeast-1.rdn.amazonaws.com
运行状况检查主机名	drp-sin.amazonworkspaces.com
运行状况检查 IP 地址	• 3.0.212.144 • 18.138.99.116 • 18.140.252.123 • 52.74.175.118
PCoIP 网关服务器公有 IP 地址范围	• 18.141.152.0 - 18.141.152.255 • 18.141.154.0 - 18.141.155.255 • 52.76.127.0 - 52.76.127.255
WSP 网关服务器 IP 地址范围	13.212.132.0/22
WSP 网关域名	*.prod.ap-southeast-1.highlander.aws.a2z.com
管理接口 IP 地址范围	• PCoIP/WSP：198.19.0.0/16 • WSP：10.0.0.0/8

亚太地区（悉尼）

要添加到允许列表的域和 IP 地址

类别	详细信息
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
客户端自动更新	https://d2td7dqidlhjx7.cloudfront.net/

类别	详细信息
连接检查	https://connectivity.amazonworkspaces.com/
客户端指标（适用于 3.0 及以上的 WorkSpaces 客户端应用程序）	域： https://skylight-client-ds.ap-southeast-2.amazonaws
动态消息服务（适用于 3.0 以上的 WorkSpaces 客户端应用程序）	域： https://ws-client-service.ap-southeast-2.amazonaws

类别	详细信息
目录设置	在登录到客户目录之前，从客户机到客户目录进行身份验证 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<区域>/<目录 ID> 从 macOS 客户端进行的连接： • https://d32i4gd7pg4909.cloudfront.net/ 客户目录设置： • https://d21ui22avrxoh6.cloudfront.net/prod/<区域>/<目录 ID> 客户目录级别联合品牌的登录页面图形： • https://d1cbg795sa4g1u.cloudfront.net/prod/<区域>/<目录 ID> 用于设计登录页面的 CSS 文件： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 登录页面的文件： • 亚太地区（悉尼）— https://dwcpoxuuza83q.cloudfront.net/
Forrester 日志服务	https://fls-na.amazon.com/
运行状况检查 (DRP) 服务器	运行状况检查服务器
会话前智能卡身份验证端点	https://smartcard.ap-southeast-2.signin.aws

类别	详细信息
注册依赖关系（用于 Web 访问和 Teradici PCoIP 零客户端）	https://s3.amazonaws.com
用户登录页面	https://<目录 ID>.awsapps.com/（其中，<目录 ID> 是客户的域）
WS 代理	域： • https://ws-broker-service.ap-southeast-2.amazonaws
WorkSpaces API 端点	域： • https://workspaces.ap-southeast-2.amazonaws.com
会话代理 (PCM)	域： • https://skylight-cm.ap-southeast-2.amazonaws.com
适用于 PCoIP 的 Web Access TURN 服务器	服务器： • turn:*.ap-southeast-2.rdn.amazonaws.com
运行状况检查主机名	drp-syd.amazonworkspaces.com
运行状况检查 IP 地址	• 3.24.11.127 • 13.237.232.125
PCoIP 网关服务器公有 IP 地址范围	• 3.25.43.0 - 3.25.43.255 • 3.25.44.0 - 3.25.45.255 • 54.153.254.0 - 54.153.254.255
WSP 网关服务器 IP 地址范围	3.25.248.0/22
WSP 网关域名	*.prod.ap-southeast-2.highlander.aws.a2z.com

类别	详细信息
管理接口 IP 地址范围	• PCoIP/WSP：172.31.0.0/16、192.168.0.0/16 和 198.19.0.0/16 • WSP：10.0.0.0/8

亚太地区（东京）

要添加到允许列表的域和 IP 地址

类别	详细信息
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
客户端自动更新	https://d2td7dqidlhjx7.cloudfront.net/
连接检查	https://connectivity.amazonworkspaces.com/
客户端指标（适用于 3.0 及以上的 WorkSpaces 客户端应用程序）	域： https:// skylight-client-ds .ap-northeast-1.amazonaws
动态消息服务（适用于 3.0 以上的 WorkSpaces 客户端应用程序）	域： https:// ws-client-service .ap-northeast-1.amazonaws
目录设置	在登录到客户目录之前，从客户机到客户目录进行身份验证 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<区域>/<目录 ID> 从 macOS 客户端进行的连接： • https://d32i4gd7pg4909.cloudfront.net/ 客户目录设置：

类别	详细信息
	• https://d21ui22avrxoh6.cloudfront.net/prod/<区域>/<目录 ID> 客户目录级别联合品牌的登录页面图形： • https://d1cbg795sa4g1u.cloudfront.net/prod/<区域>/<目录 ID> 用于设计登录页面的 CSS 文件： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 登录页面的文件： • 亚太地区（东京）— https://d2c2t8mxjhq5z1.cloudfront.net/
Forrester 日志服务	https://fls-na.amazon.com/
运行状况检查 (DRP) 服务器	运行状况检查服务器
会话前智能卡身份验证端点	https://smartcard.ap-northeast-1.signin.aws
注册依赖关系（用于 Web 访问和 Teradici PCoIP 零客户端）	https://s3.amazonaws.com
用户登录页面	https://<目录 ID>.awsapps.com/（其中，<目录 ID> 是客户的域）
WS 代理	域： • https:// ws-broker-service .ap-northeast-1.amazonaws

类别	详细信息
WorkSpaces API 端点	域： • https://workspaces.ap-northeast-1.amazonaws.com
会话代理 (PCM)	域： • https://skylight-cm.ap-northeast-1.amazonaws.com
适用于 PCoIP 的 Web Access TURN 服务器	服务器： • turn:*.ap-northeast-1.rdn.amazonaws.com
运行状况检查主机名	drp-nrt.amazonworkspaces.com
运行状况检查 IP 地址	• 18.178.102.247 • 54.64.174.128
PCoIP 网关服务器公有 IP 地址范围	• 18.180.178.0 - 18.180.178.255 • 18.180.180.0 - 18.180.181.255 • 54.250.251.0 - 54.250.251.255
WSP 网关服务器 IP 地址范围	3.114.164.0/22
WSP 网关域名	*.prod.ap-northeast-1.highlander.aws.a2z.com
管理接口 IP 地址范围	• PCoIP/WSP：198.19.0.0/16 • WSP：10.0.0.0/8

加拿大（中部）

要添加到允许列表的域和 IP 地址

类别	详细信息
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/

类别	详细信息
客户端自动更新	https://d2td7dqidlhjx7.cloudfront.net/
连接检查	https://connectivity.amazonworkspaces.com/
客户端指标（适用于 3.0 及以上的 WorkSpaces 客户端应用程序）	域： https://skylight-client-ds.ca-central-1.amazonaw
动态消息服务（适用于 3.0 以上的 WorkSpaces 客户端应用程序）	域： https://ws-client-service.ca-central-1.amazonaw

类别	详细信息
目录设置	在登录到客户目录之前，从客户机到客户目录进行身份验证 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<区域>/<目录 ID> 从 macOS 客户端进行的连接： • https://d32i4gd7pg4909.cloudfront.net/ 客户目录设置： • https://d21ui22avrxoh6.cloudfront.net/prod/<区域>/<目录 ID> 客户目录级别联合品牌的登录页面图形： • https://d1cbg795sa4g1u.cloudfront.net/prod/<区域>/<目录 ID> 用于设计登录页面的 CSS 文件： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 登录页面的文件： • 加拿大（中部）— https://d2wfbsypmqjmog.cloudfront.net/
Forrester 日志服务	https://fls-na.amazon.com/
运行状况检查 (DRP) 服务器	运行状况检查服务器

类别	详细信息
注册依赖关系（用于 Web 访问和 Teradici PCoIP 零客户端）	https://s3.amazonaws.com
用户登录页面	https://<目录 ID>.awsapps.com/（其中，<目录 ID> 是客户的域）
WS 代理	域： • https://ws-broker-service.ca-central-1.amazonaw
WorkSpaces API 端点	域： • https://workspaces.ca-central-1.amazonaws.com
会话代理 (PCM)	域： • https://skylight-cm.ca-central-1.amazonaws.com
适用于 PCoIP 的 Web Access TURN 服务器	服务器： • turn:*.ca-central-1.rdn.amazonaws.com
运行状况检查主机名	drp-yul.amazonworkspaces.com
运行状况检查 IP 地址	• 52.60.69.16 • 52.60.80.237 • 52.60.173.117 • 52.60.201.0
PCoIP 网关服务器公有 IP 地址范围	• 15.223.100.0 - 15.223.100.255 • 15.223.102.0 - 15.223.103.255 • 35.183.255.0 - 35.183.255.255
WSP 网关服务器 IP 地址范围	3.97.20.0/22

类别	详细信息
WSP 网关域名	*.prod.ca-central-1.highlander.aws.a2z.com
管理接口 IP 地址范围	• PCoIP/WSP：198.19.0.0/16 • WSP：10.0.0.0/8

欧洲地区（法兰克福）

要添加到允许列表的域和 IP 地址

类别	详细信息
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
客户端自动更新	https://d2td7dqidlhjx7.cloudfront.net/
连接检查	https://connectivity.amazonworkspaces.com/
客户端指标（适用于 3.0 及以上的 WorkSpaces 客户端应用程序）	域： https://skylight-client-ds.eu-central-1.amazonaw
动态消息服务（适用于 3.0 以上的 WorkSpaces 客户端应用程序）	域： https://ws-client-service.eu-central-1.amazonaw
目录设置	在登录到客户目录之前，从客户机到客户目录进行身份验证 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<区域>/<目录 ID> 从 macOS 客户端进行的连接： • https://d32i4gd7pg4909.cloudfront.net/ 客户目录设置：

类别	详细信息
	• https://d21ui22avrxoh6.cloudfront.net/prod/<区域>/<目录 ID> 客户目录级别联合品牌的登录页面图形： • https://d1cbg795sa4g1u.cloudfront.net/prod/<区域>/<目录 ID> 用于设计登录页面的 CSS 文件： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 登录页面的文件： • 欧洲地区（法兰克福）— https://d1whcm49570jjw.cloudfront.net/
Forrester 日志服务	https://fls-na.amazon.com/
运行状况检查 (DRP) 服务器	运行状况检查服务器
注册依赖关系（用于 Web 访问和 Teradici PCoIP 零客户端）	https://s3.amazonaws.com
用户登录页面	https://<目录 ID>.awsapps.com/（其中，<目录 ID> 是客户的域）
WS 代理	域： • https://ws-broker-service.eu-central-1.amazonaw
WorkSpaces API 端点	域： • https://workspaces.eu-central-1.amazonaws.com

类别	详细信息
会话代理 (PCM)	域： • https://skylight-cm.eu-central-1.amazonaws.com
适用于 PCoIP 的 Web Access TURN 服务器	服务器： • turn:*.eu-central-1.rdn.amazonaws.com
运行状况检查主机名	drp-fra.amazonworkspaces.com
运行状况检查 IP 地址	• 52.59.191.224 • 52.59.191.225 • 52.59.191.226 • 52.59.191.227
PCoIP 网关服务器公有 IP 地址范围	• 18.156.52.0 - 18.156.52.255 • 18.156.54.0 - 18.156.55.255 • 52.59.127.0 - 52.59.127.255
WSP 网关服务器 IP 地址范围	18.192.216.0/22
WSP 网关域名	*.prod.eu-central-1.highlander.aws.a2z.com
管理接口 IP 地址范围	• PCoIP/WSP：198.19.0.0/16 • WSP：10.0.0.0/8

欧洲地区（爱尔兰）

要添加到允许列表的域和 IP 地址

类别	详细信息
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
客户端自动更新	https://d2td7dqidlhjx7.cloudfront.net/

类别	详细信息
连接检查	https://connectivity.amazonworkspaces.com/
客户端指标（适用于 3.0 及以上的 WorkSpaces 客户端应用程序）	域： https://skylight-client-ds.eu-West-1.amazonaws.com
动态消息服务（适用于 3.0 以上的 WorkSpaces 客户端应用程序）	域： https://ws-client-service.eu-West-1.amazonaws.com

类别	详细信息
目录设置	在登录到客户目录之前，从客户机到客户目录进行身份验证 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<区域>/<目录 ID> 从 macOS 客户端进行的连接： • https://d32i4gd7pg4909.cloudfront.net/ 客户目录设置： • https://d21ui22avrxoh6.cloudfront.net/prod/<区域>/<目录 ID> 客户目录级别联合品牌的登录页面图形： • https://d1cbg795sa4g1u.cloudfront.net/prod/<区域>/<目录 ID> 用于设计登录页面的 CSS 文件： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 登录页面的文件： • 欧洲地区（爱尔兰）— https://d3pgffbf39h4k4.cloudfront.net/
Forrester 日志服务	https://fls-na.amazon.com/
运行状况检查 (DRP) 服务器	运行状况检查服务器
会话前智能卡身份验证端点	https://smartcard.eu-west-1.signin.aws

类别	详细信息
注册依赖关系（用于 Web 访问和 Teradici PCoIP 零客户端）	https://s3.amazonaws.com
用户登录页面	https://<目录 ID>.awsapps.com/（其中，<目录 ID> 是客户的域）
WS 代理	域： • https://ws-broker-service.eu-West-1.amazonaws.com
WorkSpaces API 端点	域： • https://workspaces.eu-west-1.amazonaws.com
会话代理 (PCM)	域： • https://skylight-cm.eu-west-1.amazonaws.com
适用于 PCoIP 的 Web Access TURN 服务器	服务器： • turn:*.eu-west-1.rdn.amazonaws.com
运行状况检查主机名	drp-dub.amazonworkspaces.com
运行状况检查 IP 地址	• 18.200.177.86 • 52.48.86.38 • 54.76.137.224
PCoIP 网关服务器公有 IP 地址范围	• 3.249.28.0 - 3.249.29.255 • 52.19.124.0 - 52.19.125.255
WSP 网关服务器 IP 地址范围	3.248.176.0/22
WSP 网关域名	*.prod.eu-west-1.highlander.aws.a2z.com

类别	详细信息
管理接口 IP 地址范围	• PCoIP/WSP：172.31.0.0/16、192.168.0.0/16 和 198.19.0.0/16 • WSP：10.0.0.0/8

欧洲地区（伦敦）

要添加到允许列表的域和 IP 地址

类别	详细信息
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
客户端自动更新	https://d2td7dqidlhjx7.cloudfront.net/
连接检查	https://connectivity.amazonworkspaces.com/
客户端指标（适用于 3.0 及以上的 WorkSpaces 客户端应用程序）	域： https://skylight-client-ds.eu-West-2.amazonaws.com
动态消息服务（适用于 3.0 以上的 WorkSpaces 客户端应用程序）	域： https://ws-client-service.eu-West-2.amazonaws.com
目录设置	在登录到客户目录之前，从客户机到客户目录进行身份验证 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<区域>/<目录 ID> 从 macOS 客户端进行的连接： • https://d32i4gd7pg4909.cloudfront.net/ 客户目录设置：

类别	详细信息
	• https://d21ui22avrxoh6.cloudfront.net/prod/<区域>/<目录 ID> 客户目录级别联合品牌的登录页面图形： • https://d1cbg795sa4g1u.cloudfront.net/prod/<区域>/<目录 ID> 用于设计登录页面的 CSS 文件： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 登录页面的文件： • 欧洲地区（伦敦）— https://d16q6638mh01s7.cloudfront.net/
Forrester 日志服务	https://fls-na.amazon.com/
运行状况检查 (DRP) 服务器	运行状况检查服务器
注册依赖关系（用于 Web 访问和 Teradici PCoIP 零客户端）	https://s3.amazonaws.com
用户登录页面	https://<目录 ID>.awsapps.com/（其中，<目录 ID> 是客户的域）
WS 代理	域： • https://ws-broker-service.eu-West-2.amazonaws.com
WorkSpaces API 端点	域： • https://workspaces.eu-west-2.amazonaws.com

类别	详细信息
会话代理 (PCM)	域： • https://skylight-cm.eu-west-2.amazonaws.com
适用于 PCoIP 的 Web Access TURN 服务器	服务器： • turn:*.eu-west-2.rdn.amazonaws.com
运行状况检查主机名	drp-lhr.amazonworkspaces.com
运行状况检查 IP 地址	• 35.176.62.54 • 35.177.255.44 • 52.56.46.102 • 52.56.111.36
PCoIP 网关服务器公有 IP 地址范围	• 18.132.21.0 - 18.132.21.255 • 18.132.22.0 - 18.132.23.255 • 35.176.32.0 - 35.176.32.255
WSP 网关服务器 IP 地址范围	18.134.68.0/22
WSP 网关域名	*.prod.eu-west-2.highlander.aws.a2z.com
管理接口 IP 地址范围	• 198.19.0.0/16 • WSP：10.0.0.0/8

南美洲（圣保罗）

要添加到允许列表的域和 IP 地址

类别	详细信息
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
客户端自动更新	https://d2td7dqidlhjx7.cloudfront.net/

类别	详细信息
连接检查	https://connectivity.amazonworkspaces.com/
客户端指标（适用于 3.0 及以上的 WorkSpaces 客户端应用程序）	域： https:// skylight-client-ds .sa-east-1.amazonaws.co
动态消息服务（适用于 3.0 以上的 WorkSpaces 客户端应用程序）	域： https:// ws-client-service .sa-east-1.amazonaws.co

类别	详细信息
目录设置	在登录到客户目录之前，从客户机到客户目录进行身份验证 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<区域>/<目录 ID> 从 macOS 客户端进行的连接： • https://d32i4gd7pg4909.cloudfront.net/ 客户目录设置： • https://d21ui22avrxoh6.cloudfront.net/prod/<区域>/<目录 ID> 客户目录级别联合品牌的登录页面图形： • https://d1cbg795sa4g1u.cloudfront.net/prod/<区域>/<目录 ID> 用于设计登录页面的 CSS 文件： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 登录页面的文件： • 南美洲（圣保罗）— https://d2lh2qc5bdoq4b.cloudfront.net/
Forrester 日志服务	https://fls-na.amazon.com/
运行状况检查 (DRP) 服务器	运行状况检查服务器

类别	详细信息
注册依赖关系（用于 Web 访问和 Teradici PCoIP 零客户端）	https://s3.amazonaws.com
用户登录页面	https://<目录 ID>.awsapps.com/（其中，<目录 ID> 是客户的域）
WS 代理	域： • https:// ws-broker-service .sa-east-1.amazonaws.co
WorkSpaces API 端点	域： • https://workspaces.sa-east-1.amazonaws.com
会话代理 (PCM)	域： • https://skylight-cm.sa-east-1.amazonaws.com
适用于 PCoIP 的 Web Access TURN 服务器	服务器： • turn:*.sa-east-1.rdn.amazonaws.com
运行状况检查主机名	drp-gru.amazonworkspaces.com
运行状况检查 IP 地址	• 18.231.0.105 • 52.67.55.29 • 54.233.156.245 • 54.233.216.234
PCoIP 网关服务器公有 IP 地址范围	• 18.230.103.0 - 18.230.103.255 • 18.230.104.0 - 18.230.105.255 • 54.233.204.0 - 54.233.204.255
WSP 网关服务器 IP 地址范围	15.228.64.0/22

类别	详细信息
WSP 网关域名	*.prod.sa-east-1.highlander.aws.a2z.com
管理接口 IP 地址范围	• 198.19.0.0/16 • WSP：10.0.0.0/8

非洲（开普敦）

要添加到允许列表的域和 IP 地址

类别	详细信息
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
客户端自动更新	https://d2td7dqidlhjx7.cloudfront.net/
连接检查	https://connectivity.amazonworkspaces.com/
客户端指标（适用于 3.0 及以上的 WorkSpaces 客户端应用程序）	域： https://skylight-client-ds.af-south-1.amazona
动态消息服务（适用于 3.0 以上的 WorkSpaces 客户端应用程序）	域： https://ws-client-service.af-south-1.amazona
目录设置	在登录到客户目录之前，从客户机到客户目录进行身份验证 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<区域>/<目录 ID> 从 macOS 客户端进行的连接： • https://d32i4gd7pg4909.cloudfront.net/ 客户目录设置：

类别	详细信息
	• https://d21ui22avrxoh6.cloudfront.net/prod/<区域>/<目录 ID> 客户目录级别联合品牌的登录页面图形： • https://d1cbg795sa4g1u.cloudfront.net/prod/<区域>/<目录 ID> 用于设计登录页面的 CSS 文件： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 登录页面的文件： • 非洲（开普敦）— https://di5ygl2cs0mrh.cloudfront.net/
Forrester 日志服务	https://fls-na.amazon.com/
运行状况检查 (DRP) 服务器	运行状况检查服务器
注册依赖关系（用于 Web 访问和 Teradici PCoIP 零客户端）	https://s3.amazonaws.com
用户登录页面	https://<目录 ID>.awsapps.com/（其中，<目录 ID> 是客户的域）
WS 代理	域： • https://ws-broker-service.af-south-1.amazona
WorkSpaces API 端点	域： • https://workspaces.af-south-1.amazonaws.com

类别	详细信息
会话代理 (PCM)	域： • https://skylight-cm.af-south-1.amazonaws.com
运行状况检查主机名	drp-cpt.amazonworkspaces.com
运行状况检查 IP 地址	• 18.231.0.105 • 52.67.55.29 • 54.233.156.245 • 54.233.216.234
PCoIP 网关服务器公有 IP 地址范围	• 13.246.120.0-13.246.123.255
WSP 网关服务器 IP 地址范围	15.228.64.0/22
WSP 网关域名	*.prod.af-south-1.highlander.aws.a2z.com
管理接口 IP 地址范围	• 172.31.0.0/16 和 198.19.0.0/16 • WSP：10.0.0.0/8

以色列（特拉维夫）

要添加到允许列表的域和 IP 地址

类别	详细信息
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
客户端自动更新	https://d2td7dqidlhjx7.cloudfront.net/
连接检查	https://connectivity.amazonworkspaces.com/
客户端指标（适用于 3.0 及以上的 WorkSpaces 客户端应用程序）	域： https://skylight-client-ds.il-central-1.amazona

类别	详细信息
动态消息服务（适用于 3.0 以上的 WorkSpaces 客户端应用程序）	域： https://ws-client-service.il-central-1.amazona
目录设置	在登录到客户目录之前，从客户机到客户目录进行身份验证 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<区域>/<目录 ID> 从 macOS 客户端进行的连接： • https://d32i4gd7pg4909.cloudfront.net/ 客户目录设置： • https://d21ui22avrxoh6.cloudfront.net/prod/<区域>/<目录 ID> 客户目录级别联合品牌的登录页面图形： • 用于设计登录页面的 CSS 文件： • https://d3s98kk2h6f4oh.cloudfront.net/ • https://dyqsoz7pkju4e.cloudfront.net/ JavaScript 登录页面的文件： • 以色列（特拉维夫）；—
Forrester 日志服务	https://fls-na.amazon.com/
运行状况检查 (DRP) 服务器	运行状况检查服务器

类别	详细信息
注册依赖关系（用于 Web 访问和 Teradici PCoIP 零客户端）	https://s3.amazonaws.com
用户登录页面	https://<目录 ID>.awsapps.com/（其中，<目录 ID> 是客户的域）
WS 代理	域： • https://ws-broker-service.il-central-1.amazona
WorkSpaces API 端点	域： • https://workspaces.il-central-1.amazonaws.com
会话代理 (PCM)	域： • https://skylight-cm.il-central-1.amazonaws.com
适用于 PCoIP 的 Web Access TURN 服务器	服务器： • 转：*.il-central-1.rdn.amazonaws.com
运行状况检查主机名	drp-tlv.amazonworkspaces.com
运行状况检查 IP 地址	• 51.17.52.90 • 51.17.109.231 • 51.16.190.43
PCoIP 网关服务器公有 IP 地址范围	• 51.17.28.0-51.17.31.255
WSP 网关服务器 IP 地址范围	51.17.72.0/22
WSP 网关域名	*.prod.il-central-1.highlander.aws.a2z.com

类别	详细信息
管理接口 IP 地址范围	• 198.19.0.0/16 • WSP：10.0.0.0/8

AWS GovCloud （美国西部）区域

要添加到允许列表的域和 IP 地址

类别	详细信息
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
客户端自动更新	https://s3.amazonaws.com/ workspaces-client-updates /pdt/windows/ .xm WorkSpace sAppCast l
连接检查	https://connectivity.amazonworkspaces.com/
客户端指标（适用于 3.0 及以上的 WorkSpaces 客户端应用程序）	域： https://skylight-client-ds。 us-gov-west-1.amazonaws.com
动态消息服务（适用于 3.0 以上的 WorkSpaces 客户端应用程序）	域： https://ws-client-service。 us-gov-west-1.amazonaws.com
目录设置	在登录到客户目录之前，从客户机到客户目录进行身份验证 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<区域>/<目录 ID> 从 macOS 客户端进行的连接： • https://d32i4gd7pg4909.cloudfront.net/

类别	详细信息
	客户目录设置： • https://s3.amazonaws.com/ workspaces-client-properties /prod/pdt/ <directory ID> 客户目录级别联合品牌的登录页面图形： • https://s3.amazonaws.com/ workspaces-client-assets /prod/pdt/ <directory ID> 用于设计登录页面的 CSS 文件： • https://s3.amazonaws.com/ workspaces-clients-css /workspaces_v2.css JavaScript 登录页面的文件： • 不适用
Forrester 日志服务	https://fls-na.amazon.com/
运行状况检查 (DRP) 服务器	运行状况检查服务器
会话前智能卡身份验证端点	https://smartcard.signin。 amazonaws-us-gov.com
注册依赖关系（用于 Web 访问和 Teradici PCoIP 零客户端）	https://s3.amazonaws.com
用户登录页面	https://login。 us-gov-home<directory id><directory id>.awsapps.com/directory//（客户的域名在哪里）

类别	详细信息
WS 代理	域： • https://ws-broker-service。 us-gov-west-1.amazonaws.com • https://ws-broker-service-fips。 us-gov-west-1.amazonaws.com
WorkSpaces API 端点	域： • https://workspaces。 us-gov-west-1.amazonaws.com • https://workspaces-fips。 us-gov-west-1.amazonaws.com
会话代理 (PCM)	域： • https://skylight-cm。 us-gov-west-1.amazonaws.com • https://skylight-cm-fips。 us-gov-west-1.amazonaws.com
运行状况检查主机名	drp-pdt.amazonworkspaces.com
运行状况检查 IP 地址	• 52.61.60.65 • 52.61.65.14 • 52.61.88.170 • 52.61.137.87 • 52.61.155.110 • 52.222.20.88
PCoIP 网关服务器公有 IP 地址范围	• 52.61.193.0 - 52.61.193.255
WSP 网关服务器 IP 地址范围	• 3.32.139.0/24 • 3.30.129.0/24 • 3.30.130.0/23

类别	详细信息
WSP 网关域名	*.prod。 us-gov-west-1.highlander.aws.a2z.com
管理接口 IP 地址范围	• 198.19.0.0/16 • WSP：10.0.0.0/8 和 192.169.0.0/16

AWS GovCloud （美国东部）区域

要添加到允许列表的域和 IP 地址

类别	详细信息
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
客户端自动更新	https://s3.amazonaws.com/ workspaces-client-updates /prod/osu/window WorkSpaces AppCast s/ .xml
连接检查	https://connectivity.amazonworkspaces.com/
客户端指标（适用于 3.0 及以上的 WorkSpaces 客户端应用程序）	域： https://skylight-client-ds。 us-gov-east-1.amazonaws.com
动态消息服务（适用于 3.0 以上的 WorkSpaces 客户端应用程序）	域： https://ws-client-service。 us-gov-east-1.amazonaws.com
目录设置	在登录到客户目录之前，从客户机到客户目录进行身份验证 WorkSpace： • https://d32i4gd7pg4909.cloudfront.net/prod/<区域>/<目录 ID> 从 macOS 客户端进行的连接：

类别	详细信息
	• https://d32i4gd7pg4909.cloudfront.net/ 客户目录设置： • https://s3.amazonaws.com/ workspaces-client-properties /prod/osu/ <directory ID> 客户目录级别联合品牌的登录页面图形： • https://s3.amazonaws.com/ workspaces-client-assets /prod/osu/ <directory ID> 用于设计登录页面的 CSS 文件： • https://s3.amazonaws.com/ workspaces-clients-css /workspaces_v2.css JavaScript 登录页面的文件： • 不适用
Forrester 日志服务	https://fls-na.amazon.com/
运行状况检查 (DRP) 服务器	运行状况检查服务器
会话前智能卡身份验证端点	https://smartcard.signin。 amazonaws-us-gov.com
注册依赖关系（用于 Web 访问和 Teradici PCoIP 零客户端）	https://s3.amazonaws.com
用户登录页面	https://login。 us-gov-home<directory id><directory id>.awsapps.com/directory//（客户的域名在哪里）

类别	详细信息
WS 代理	域： • https://ws-broker-service。 us-gov-east-1.amazonaws.com • https://ws-broker-service-fips。 us-gov-east-1.amazonaws.com
WorkSpaces API 端点	域： • https://workspaces。 us-gov-east-1.amazonaws.com • https://workspaces-fips。 us-gov-east-1.amazonaws.com
会话代理 (PCM)	域： • https://skylight-cm。 us-gov-east-1.amazonaws.com • https://skylight-cm-fips。 us-gov-east-1.amazonaws.com
运行状况检查主机名	drp-osu.amazonworkspaces.com
运行状况检查 IP 地址	• 18.253.251.70 • 18.254.0.118
PCoIP 网关服务器公有 IP 地址范围	• 18.254.140.0-18.254.143.255
WSP 网关服务器 IP 地址范围	18.254.148.0/22
WSP 网关域名	*.prod。 us-gov-east-1.highlander.aws.a2z.com
管理接口 IP 地址范围	• 198.19.0.0/16 • WSP：10.0.0.0/8

Amazon WorkSpaces 客户端网络要求

您的 WorkSpaces 用户可使用面向受支持设备的客户端应用程序来连接到其 WorkSpaces。或者，他们可以使用 Web 浏览器连接到支持这种访问形式的 WorkSpaces。有关支持 Web 浏览器访问的 WorkSpaces 的列表，请参阅 客户端访问、Web Access 和用户体验中的“哪些 Amazon WorkSpaces 捆绑包支持 Web Access？”。

> **Note**
>
> Web 浏览器不能用于连接到 Amazon Linux WorkSpaces。

> **Important**
>
> 自 2020 年 10 月 1 日起，客户将无法再使用 Amazon WorkSpaces Web Access 客户端连接到 Windows 7 自定义 WorkSpaces 或 Windows 7 自带许可 (BYOL) WorkSpaces。

要为用户提供良好的 WorkSpace 使用体验，请验证其客户端设备是否符合以下网络要求：

- 客户端设备必须具有宽带互联网连接。建议计划为每个同时观看 480p 视频窗口的用户至少提供 1 Mbps 网速。根据您对视频分辨率的用户质量要求，可能需要更多带宽。
- 对于客户端设备连接到的网络及客户端设备上的任何防火墙，其某些端口必须对各种 AWS 服务的 IP 地址范围开放。有关更多信息，请参阅的 IP 地址和端口要求 WorkSpaces。
- 为了优化 PCoIP 性能，从客户端网络到 WorkSpaces 所在区域之间的往返时间 (RTT) 应小于 100 毫秒。如果 RTT 介于 100 毫秒和 200 毫秒之间，则用户可以访问 WorkSpace，但性能会受到影响。如果 RTT 介于 200 毫秒和 375 毫秒之间，则性能会降低。如果 RTT 超过 375 毫秒，WorkSpaces 客户端连接将终止。

  为了获得 WorkSpaces Streaming Protocol (WSP) 的最佳性能，从客户端网络到 WorkSpaces 所在区域的 RTT 应小于 250 毫秒。如果 RTT 介于 250 毫秒和 400 毫秒之间，则用户可以访问 WorkSpace，但性能会降低。

  要查看从您所在位置到各个 AWS 区域的 RTT，请使用 Amazon WorkSpaces 连接运行状况检查。
- 要将网络摄像头与 WSP 配合使用，建议最低上传带宽为每秒 1.7 兆比特。
- 如果用户通过虚拟专用网络 (VPN) 访问 WorkSpace，则连接必须支持至少 1200 字节的最大传输单位 (MTU)。

> **Note**
>
> 您无法通过连接到虚拟私有云(VPC) 的 VPN 访问 WorkSpaces。要使用 VPN 访问 WorkSpaces，需要互联网连接（通过 VPN 的公有 IP 地址），如 的 IP 地址和端口要求 WorkSpaces中所述。

- 客户端需要通过 HTTPS 访问由该服务和 Amazon Simple Storage Service (Amazon S3) 托管的 WorkSpaces 资源。客户端不支持应用程序级别的代理重定向。HTTPS 访问是必需的，以便用户可以成功完成注册并访问自己的 WorkSpace。
- 要允许从 PCoIP 零客户端设备进行访问，您必须使用适用于 WorkSpaces 的 PCoIP 协议包。您还必须在 Teradici 中启用网络时间协议 (NTP)。有关更多信息，请参阅为 WorkSpaces 设置 PCoIP 零客户端。
- 对于 3.0 及以上版本的客户端，如果您对 Amazon WorkDocs 使用单点登录 (SSO)，则必须按照《AWS Directory Service 管理指南》中的单点登录中的说明操作。

您可以按照以下说明验证客户端设备是否符合网络要求。

验证 3.0+ 客户端的网络要求

1. 打开 WorkSpaces 客户端。如果这是您首次打开客户端，则系统会提示您输入邀请电子邮件中提供的注册代码。
2. 根据您使用的客户端，执行以下操作之一。

如果您使用的是……	请执行该操作
Windows 或 Linux 客户端	在客户端应用程序的右上角，选择 Network (网络) 图标。
macOS 客户端	选择 Connections (连接) 和 Network (网络)。

   客户端应用程序将会测试网络连接、端口以及往返时间，并报告这些测试的结果。
3. 关闭 Network (网络) 对话框以返回到登录页面。

验证 1.0+ 和 2.0+ 客户端的网络要求

1. 打开 WorkSpaces 客户端。如果这是您首次打开客户端，则系统会提示您输入邀请电子邮件中提供的注册代码。
2. 在客户端应用程序右下角，选择 Network (网络)。客户端应用程序将会测试网络连接、端口以及往返时间，并报告这些测试的结果。
3. 选择 Dismiss (关闭)，以返回登录页面。

限制对可信设备的 WorkSpaces 访问

默认情况下，用户可以 WorkSpaces 从任何已连接到互联网的受支持设备进行访问。如果贵公司限制可信设备（也称为托管设备）访问企业数据，则可以限制对具有有效证书的可信设备的 WorkSpaces 访问。

启用此功能后，将 WorkSpaces 使用基于证书的身份验证来确定设备是否可信。如果 WorkSpaces 客户端应用程序无法验证设备是否可信，则会阻止尝试登录或从该设备重新连接。

对于每个目录，您最多可以导入 2 个根证书。如果您导入两个根证书， WorkSpaces 则将它们都提供给客户端，客户端会找到第一个链接到其中一个根证书的有效匹配证书。

支持的客户端

- Android，在 Android 或与 Android 兼容的 Chrome 操作系统上运行
- macOS
- Windows

> **Important**
>
> 以下客户端不支持此功能：
>
> - WorkSpaces 适用于 Linux 或 iPad 的客户端应用程序
> - 第三方客户端，包括但不限于 Teradici PCoIP、RDP 客户端和远程桌面应用程序。

> **Note**
>
> 在为特定客户端启用访问权限时，请确保阻止其他不需要的设备类型的访问。有关如何执行此操作的更多信息，请参阅下面的步骤 3.7。

第 1 步：创建证书

此功能需要两种类型的证书：内部证书颁发机构 (CA) 生成的根证书和一直串联到根证书的客户端证书。

要求

- 根证书必须是 Base64 编码的证书文件 (采用 CRT、CERT 或 PEM 格式)。
- 根证书必须满足以下正则表达式模式，这意味着除最后一行外，每行编码的长度必须正好为 64 个字符：`-{5}BEGIN CERTIFICATE-{5}\u000D?\u000A([A-Za-z0-9/+]{64} \u000D?\u000A)*[A-Za-z0-9/+]{1,64}={0,2}\u000D?\u000A-{5}END CERTIFICATE-{5}(\u000D?\u000A)`。
- 设备证书必须包含公用名。
- 设备证书必须包含以下扩展：`Key Usage: Digital Signature` 和 `Enhanced Key Usage: Client Authentication`。
- 从设备证书到受信任根证书颁发机构的证书链中的所有证书都必须安装在客户端设备上。
- 证书链支持的最大长度为 4。
- WorkSpaces 目前不支持客户端证书的设备吊销机制，例如证书吊销列表 (CRL) 或在线证书状态协议 (OCSP)。
- 使用强加密算法。建议使用带 RSA 的 SHA256、带 ECDSA 的 SHA256、带 ECDSA 的 SHA381 或带 ECDSA 的 SHA512。
- 对于 macOS，如果设备证书位于系统钥匙串中，我们建议您授权 WorkSpaces 客户端应用程序访问这些证书。否则，用户必须在登录或重新连接时，输入密钥链凭证。

第 2 步：为受信任设备部署客户端证书

在用户可信设备上，您必须安装证书捆绑包，其中包含从设备证书到可信根证书颁发机构的证书链中的所有证书。您可以使用首选解决方案将证书安装到一批客户端设备；例如，System Center Configuration Manager (SCCM) 或移动设备管理 (MDM)。请注意，SCCM 和 MDM 可以选择执行安全态势评估，以确定设备是否符合您的公司访问政策。 WorkSpaces

WorkSpaces 客户端应用程序按如下方式搜索证书：

- Android - 转至设置，选择安全和位置、凭证，然后选择从 SD 卡安装。
- 与 Android 兼容的 Chrome 操作系统 - 打开 Android 设置并选择安全和位置、凭证，然后选择从 SD 卡安装。
- macOS - 在密钥链中搜索客户端证书。
- Windows - 在用户和根证书存储中搜索客户端证书。

第 3 步：配置限制

在受信任设备上部署客户端证书后，您可以在目录级别启用受限访问权限。这要求 WorkSpaces 客户端应用程序在允许用户登录设备之前验证设备上的证书 WorkSpace。

配置限制

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择目录。
3. 选择目录，然后选择 Actions、Update Details。
4. 展开 Access Control Options。
5. 在 “针对每种设备类型，指定哪些设备可以访问” 下 WorkSpaces，选择 “可信设备”。
6. 最多导入 2 个根证书。对于每个根证书，请执行以下操作：
   a. 选择 Import（导入）。
   b. 将证书文本复制到表单中。
   c. 选择 Import（导入）。
7. 指定其他类型的设备是否可以访问 WorkSpaces。
   a. 向下滚动到 Other Platforms (其他平台) 部分。默认情况下， WorkSpaces Linux 客户端处于禁用状态，用户可以 WorkSpaces 从 iOS 设备、安卓设备、Web Access、Chromeb ook 和 PCoIP 零客户端设备访问它们。
   b. 选择要启用的设备类型并清除要禁用的设备类型。
   c. 要阻止来自所有选定设备类型的访问，请选择 Block。
8. 选择更新并退出。

将 WorkSpaces 与 SAML 2.0 集成

将 SAML 2.0 与 WorkSpaces 集成以进行桌面会话身份验证，可允许您的用户通过其默认 Web 浏览器使用其现有的 SAML 2.0 身份提供者 (IdP) 凭证和身份验证方法。通过使用 IdP 对 WorkSpaces 用户进行身份验证，您可以采用 IdP 功能（如多因素身份验证和上下文访问策略）来保护 WorkSpaces。

身份验证工作流

以下各节描述了由 WorkSpaces 客户端应用程序、WorkSpaces Web Access 和 SAML 2.0 身份提供者 (IdP) 启动的身份验证工作流：

- 当流由 IdP 启动时。例如，当用户使用 Web 浏览器在 IdP 用户门户中选择应用程序时。
- 当流由 WorkSpaces 客户端启动时。例如，当用户打开客户端应用程序并登录时。
- 当流由 WorkSpaces Web Access 启动时。例如，当用户在浏览器中打开 Web Access 并登录时。

在这些示例中，用户输入 `user@example.com` 以登录 IdP。IdP 已为 WorkSpaces 目录配置了 SAML 2.0 服务提供者应用程序，并且用户已获得使用 WorkSpaces SAML 2.0 应用程序的授权。用户在启用 SAML 2.0 身份验证的目录中为其用户名 `user` 创建 WorkSpace。此外，用户在自己的设备上安装 WorkSpaces 客户端应用程序，或者用户在 Web 浏览器中使用 Web Access。

由身份提供者 (IdP) 启动的客户端应用程序流

IdP 启动的流允许用户在其设备上自动注册 WorkSpaces 客户端应用程序，而无需输入 WorkSpaces 注册码。用户不会使用 IdP 启动的流登录其 WorkSpaces。WorkSpaces 身份验证必须源自客户端应用程序。

1. 用户使用其 Web 浏览器登录 IdP。
2. 登录 IdP 后，用户从 IdP 用户门户中选择 WorkSpaces 应用程序。
3. 系统在浏览器中将用户重定向到此页面，并自动打开 WorkSpaces 客户端应用程序。

4. WorkSpaces 客户端应用程序现已注册，用户可以单击继续登录 WorkSpaces，以继续登录。

身份提供者 (IdP) 启动的 Web Access 流

IdP 启动的 Web Acess 流允许用户通过 Web 浏览器自动注册其 WorkSpaces，而无需输入 WorkSpaces 注册码。用户不会使用 IdP 启动的流登录其 WorkSpaces。WorkSpaces 身份验证必须源自 Web Access。

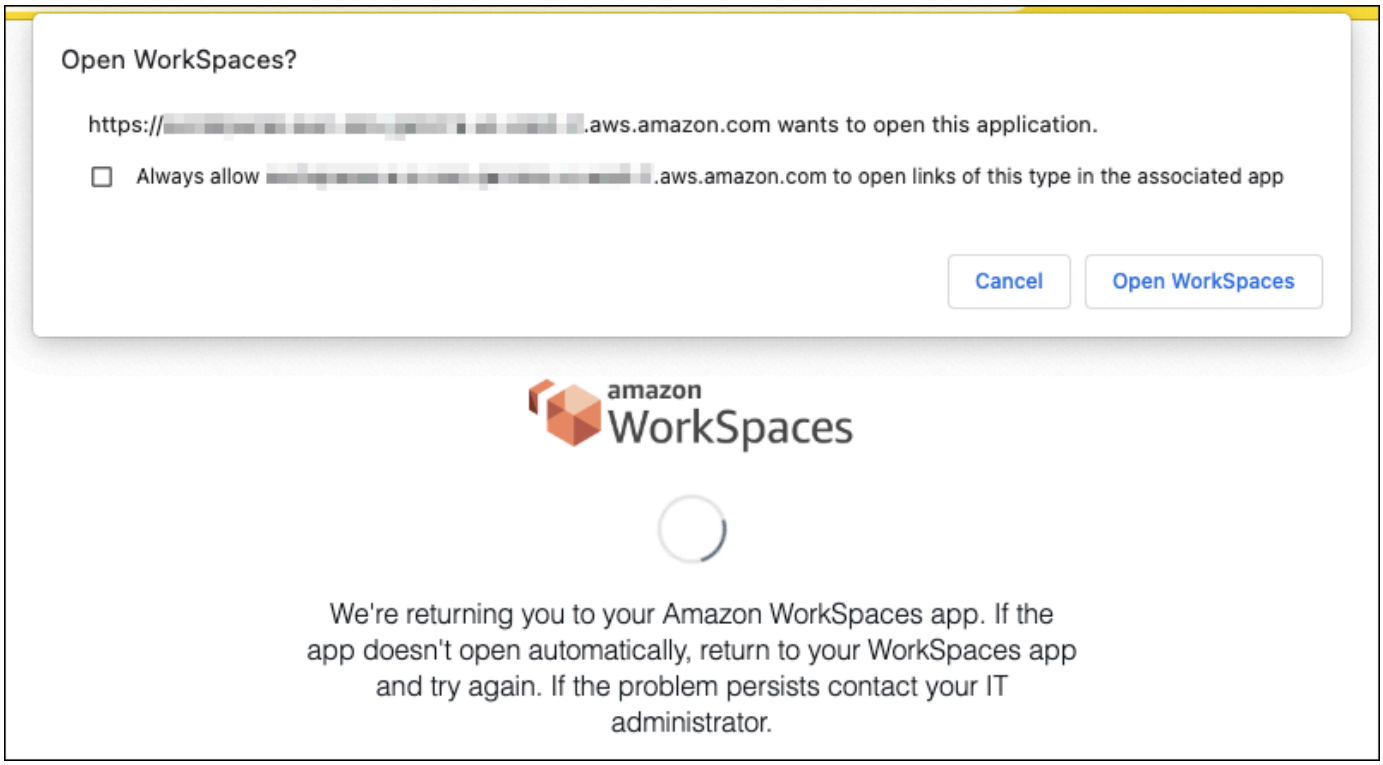
1. 用户使用其 Web 浏览器登录 IdP。
2. 登录 IdP 后，用户从 IdP 用户门户单击 WorkSpaces 应用程序。
3. 系统在浏览器中将用户重定向到此页面。要打开 WorkSpaces，请在浏览器中选择 Amazon WorkSpaces。

4. WorkSpaces 客户端应用程序现已注册，用户可以继续通过 WorkSpaces Web Access 登录。

由 WorkSpaces 客户端启动的流

客户端启动的流允许用户在登录 IdP 后登录其 WorkSpaces。

1. 用户启动 WorkSpaces 客户端应用程序（如果尚未运行），然后单击继续登录 WorkSpaces。
2. 系统会将用户重定向到其默认 Web 浏览器以登录 IdP。如果用户已经在浏览器中登录 IdP，则无需再次登录，可以跳过此步骤。
3. 登录 IdP 后，系统会将用户重定向到弹出窗口。按照提示允许您的 Web 浏览器打开客户端应用程序。



4. 系统将用户重定向到 WorkSpaces 客户端应用程序，以完成其 WorkSpaces 登录。WorkSpaces 用户名根据 IdP SAML 2.0 断言自动填充。使用基于证书的身份验证 (CBA) 时，用户会自动登录。
5. 用户已登录其 WorkSpaces。

由 WorkSpaces Web Access 启动的流

Web Access 启动的流允许用户在登录 IdP 后登录其 WorkSpaces。

1. 用户启动 WorkSpaces Web Access，并选择登录。
2. 在同一个浏览器选项卡中，系统将用户重定向到 IdP 门户。如果用户已经在浏览器中登录 IdP，则无需再次登录，可以跳过此步骤。

3. 登录 IdP 后，系统在浏览器中将用户重定向到此页面，然后用户单击登录 WorkSpaces。
4. 系统将用户重定向到 WorkSpaces 客户端应用程序，以完成其 WorkSpaces 登录。WorkSpaces 用户名根据 IdP SAML 2.0 断言自动填充。使用基于证书的身份验证 (CBA) 时，用户会自动登录。
5. 用户已登录其 WorkSpaces。

设置 SAML 2.0

使用 SAML 2.0 身份提供商 (IdP) 凭据和身份验证方法，通过使用 SAML 2.0 设置联合身份验证，为您的用户启用 WorkSpaces 客户端应用程序注册和登录。 WorkSpaces 要使用 SAML 2.0 设置身份联合验证，请使用 IAM 角色和中继状态 URL 来配置您的 IdP 并启用 AWS。这将授予您的联合用户访问 WorkSpaces 目录的权限。中继状态是用户成功登录后被转发到的 WorkSpaces目录端点 AWS。

内容

要求

- 以下区域提供 SAML 2.0 身份验证：
  - 美国东部（弗吉尼亚州北部）区域
  - 美国西部（俄勒冈州）区域
  - 非洲（开普敦）区域
  - 亚太地区（孟买）区域
  - 亚太地区（首尔）区域
  - 亚太地区（新加坡）区域
  - 亚太地区（悉尼）区域

  - Asia Pacific（Tokyo）Region
  - 加拿大（中部）区域
  - 欧洲地区（法兰克福）区域
  - 欧洲地区（爱尔兰）区域
  - 欧洲地区（伦敦）区域
  - 南美洲（圣保罗）区域
  - 以色列（特拉维夫）区域
  - AWS GovCloud （美国西部）
  - AWS GovCloud （美国东部）
- 要将 SAML 2.0 身份验证与一起使用 WorkSpaces，IdP 必须通过深度链接目标资源或中继状态端点 URL 支持未经请求的 IdP 发起的 SSO。的示例 IdPs 包括 ADFS、Azure AD、Duo 单点登录、Okta 和。 PingFederate PingOne有关更多信息，请参阅 IdP 文档。
- SAML 2.0 身份验证将在使用 Simple AD WorkSpaces 启动时起作用，但不建议这样做，因为 Simple AD 未与 SAML 2.0 集成。 IdPs
- 以下 WorkSpaces 客户端支持 SAML 2.0 身份验证。SAML 2.0 身份验证不支持其他客户端版本。打开 Amazon WorkSpaces 客户端下载以查找最新版本：
  - Windows 客户端应用程序 5.1.0.3029 或更高版本
  - macOS 客户端 5.x 或更高版本
  - 适用于 Ubuntu 22.04 版本 2024.1 或更高版本、Ubuntu 20.04 版本 24.1 或更高版本的 Linux 客户端
  - Web Access

  除非启用了回退，否则其他客户端版本将无法连接到 WorkSpaces 启用 SAML 2.0 身份验证。有关更多信息，请参阅在 WorkSpaces 目录上启用 SAML 2.0 身份验证。

step-by-step 有关将 SAML 2.0 与 WorkSpaces 使用 ADFS、Azure AD、Duo 单点登录、Okta PingFederate 以及 PingOne 企业版集成的说明 OneLogin，请查看 A mazon WorkSpaces SAM L 身份验证实施指南。

先决条件

在配置 SAML 2.0 身份提供商 (IdP) 与目录的连接之前，请完成以下先决条件。 WorkSpaces

1. 配置您的 IdP 以集成与该目录一起使用的 Microsoft 活动目录中的用户身份。 WorkSpaces 对于具有的用户 WorkSpace，Active Directory 用户的 S aM AccountName 和电子邮件属性以及 SAML 声明值必须匹配，用户才能 WorkSpaces 使用 IdP 登录。有关将 Active Directory 与 IdP 集成的更多信息，请参阅您的 IdP 文档。
2. 配置 IdP 以与 建立信任关系 AWS

   - 有关配置 AWS 联合的更多信息，请参阅将第三方 SAML 解决方案提供商与 AWS集成。相关示例包括 IdP 与 AWS IAM 集成以访问 AWS 管理控制台。
   - 使用您的 IdP 生成和下载联合身份验证元数据文档，该文档将您的组织描述为 IdP。此签名 XML 文档用于建立信赖方信任关系。将该文件保存您稍后可通过 IAM 控制台访问的位置。
3. 使用 WorkSpaces 管理控制台 WorkSpaces 为创建或注册目录。有关更多信息，请参阅管理目录 WorkSpaces。以下目录类型支持 WorkSpaces SAML 2.0 身份验证：

   - AD Connector
   - AWS 微软 AD 托管
4. WorkSpace 为可以使用支持的目录类型登录 IdP 的用户创建。您可以使用 WorkSpaces 管理控制台或 WorkSpaces API 创建。 WorkSpace AWS CLI有关更多信息，请参阅使用启动虚拟桌面 WorkSpaces。

步骤 1：在 IAM 中 AWS 创建 SAML 身份提供商

首先，在 IAM 中创建一个 SAML IdP AWS 。此 IdP 使用组织中 IdP 软件生成的元数据文档定义贵组织的 IdP AWS 信任关系。有关更多信息，请参阅创建和管理 SAML 身份提供者（Amazon Web Services 管理控制台）。有关 IdPs 在 AWS GovCloud （美国西部）和 AWS GovCloud （美国东部）使用 SAML 的信息，请参阅 Identity and Access Managem AWS en t。

步骤 2：创建 SAML 2.0 联合身份验证 IAM 角色

接下来创建 SAML 2.0 联合身份验证 IAM 角色。此步骤在 IAM 与您的组织的 IdP 之间建立信任关系，将您的 IdP 作为可信实体进行联合身份验证。

为 SAML IdP 创建 IAM 角色

1. 通过 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 在导航窗格中，选择角色 > 创建角色。
3. 对于 Role type，选择 SAML 2.0 federation。
4. 对于 SAML 提供者，选择您创建的 SAML IdP。

> **Important**
>
> 请勿选择两个 SAML 2.0 访问方法（只允许编程访问或允许编程访问和 Amazon Web Services 管理控制台访问）中的任何一个。

5. 对于 Attribute，选择 SAML:sub_type。
6. 对于值，输入 `persistent`。该值将角色访问权限仅局限于 SAML 用户的流式传输请求，其中包括值为 persistent 的 SAML 主题类型断言。如果 SAML:sub_type 为 persistent，在来自特定用户的所有 SAML 请求中，您的 IdP 会为 NameID 元素发送相同的唯一值。有关 SAML: sub_type 断言的更多信息，请参阅使用基于 SAML 的联合身份验证进行 API 访问的 “在基于 SAML 的联合身份验证中唯一标识用户” 部分。 AWS
7. 检查您的 SAML 2.0 信任信息，确认正确的可信实体和条件，然后选择 Next: Permissions。
8. 在 Attach permissions policies (附加权限策略) 页面上，选择 Next: Tags (下一步：标签)。
9. （可选）为要添加的每个标签输入键和值。有关更多信息，请参阅标记 IAM 用户和角色。
10. 完成此操作后，选择 Next: Review (下一步：审核)。稍后您将为此角色创建并嵌入内联策略。
11. 对于角色名称，输入有助于标识此角色作用的名称。由于多个实体可能引用该角色，因此，角色创建完毕后，您将无法编辑角色名称。
12. （可选）对于角色描述，输入新角色的描述。
13. 检查角色详细信息，然后选择 Create role。
14. 将 sts: TagSession 权限添加到您的新 IAM 角色的信任策略中。有关更多信息，请参阅在 AWS STS中传递会话标签。在新 IAM 角色的详细信息中，选择信任关系选项卡，然后选择编辑信任关系*。当 “编辑信任关系” 策略编辑器打开时，添加 sts: TagSession * 权限，如下所示：

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Principal": {
            "Federated": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:saml-provider/
IDENTITY-PROVIDER"
        },
        "Action": [
            "sts:AssumeRoleWithSAML",
            "sts:TagSession"
        ],
```

```
        "Condition": {
            "StringEquals": {
                "SAML:aud": "https://signin.aws.amazon.com/saml"
            }
        }
    }]
}
```

将 IDENTITY-PROVIDER 替换为在步骤 1 中创建的 SAML IdP 的名称。然后选择更新信任策略。

步骤 3：为 IAM 角色嵌入内联策略

接下来为您创建的角色嵌入内联 IAM 策略。嵌入内联策略时，策略中的权限不能意外分配给错误的主体实体。内联策略为联合用户提供了对 WorkSpaces 目录的访问权限。

> **Important**
>
> 该`workspaces:Stream`操作不支持 AWS 根据源 IP 管理访问权限的 IAM 策略。要管理的 IP 访问控制 WorkSpaces，请使用 IP 访问控制组。此外，在使用 SAML 2.0 身份验证时，如果您的 SAML 2.0 IdP 提供了 IP 访问控制策略，则可以使用 IP 访问控制策略。

1. 在您创建的 IAM 角色的详细信息中，选择权限选项卡，然后向该角色的权限策略添加所需的权限。创建策略向导将启动。
2. 在 Create policy (创建策略) 中，选择 JSON 选项卡。
3. 将以下 JSON 策略复制并粘贴到 JSON 窗口中。然后，通过输入您的 AWS 区域代码、账户 ID 和目录 ID 来修改资源。在以下策略中，`"Action": "workspaces:Stream"`是向您的 WorkSpaces 用户提供在 WorkSpaces 目录中连接到其桌面会话的权限的操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "workspaces:Stream",
            "Resource": "arn:aws:workspaces:REGION-CODE:ACCOUNT-ID-WITHOUT-
HYPHENS:directory/DIRECTORY-ID",
```

```
            "Condition": {
                "StringEquals": {
                    "workspaces:userId": "${saml:sub}"
                }
            }
        }
    ]
}
```

REGION-CODE替换为您的 WorkSpaces目录所在的 AWS 区域。DIRECTORY-ID替换为可在 WorkSpaces 管理控制台中找到的 WorkSpaces 目录 ID。对于 AWS GovCloud （美国西部）或 AWS GovCloud （美国东部）中的资源，请使用以下格式的 ARN：。arn:aws-us-gov:workspaces:REGION-CODE:ACCOUNT-ID-WITHOUT-HYPHENS:directory/DIRECTORY-ID

4. 完成后，选择 Review policy (审核策略)。策略验证程序将报告任何语法错误。

步骤 4：配置 SAML 2.0 身份提供者

接下来，根据您的 SAML 2.0 IdP，您可能需要手动更新您的 IdP，使其成为 AWS 值得信赖的服务提供商，方法是将文件上传saml-metadata.xml到您的 IdP，网址为 https://signin.aws.amazon.com/static/saml-metadata.xml。此步骤会更新您的 IdP 的元数据。对于某些人来说 IdPs，更新可能已经配置好了。如果是这样，请继续下一步。

如果您的 IdP 中尚未配置此更新，请查看您的 IdP 提供的文档，了解有关如何更新元数据的信息。一些提供商为您提供了键入 URL 并由 IdP 获取并安装该文件的选项。另一些提供商则要求您从该 URL 处下载该文件，然后将其作为本地文件提供。

> **Important**
>
> 此时，您还可以授权 IdP 中的用户访问您在 IdP 中配置的 WorkSpaces应用程序。有权访问您的目录 WorkSpaces 应用程序的用户不会自动为他们 WorkSpace 创建一个。同样，为其 WorkSpace 创建的用户也不会自动获得访问该 WorkSpaces 应用程序的权限。要成功连接 WorkSpace 使用 SAML 2.0 身份验证，用户必须获得 IdP 的授权并且必须已 WorkSpace创建。

步骤 5：为 SAML 身份验证响应创建断言

接下来，将您的 IdP 发送到的信息配置 AWS 为身份验证响应中的 SAML 属性。根据您的 IdP，此配置已完成，跳过此步骤，并继续执行步骤 6：配置联合身份验证的中继状态。

如果您的 IdP 中尚未配置此信息，请提供以下内容：

- SAML 主题 NameID – 登录用户的唯一标识符。该值必须与 WorkSpaces 用户名相匹配，通常是 Active Directory 用户的 s aM AccountName 属性。
- SAML 主题类型（值设为 `persistent`）– 将值设为 `persistent` 可确保在来自特定用户的所有 SAML 请求中，您的 IdP 会为 `NameID` 元素发送相同的唯一值。请确保您的 IAM 策略包含一个条件，仅允许将 SAML sub_type 设置为 `persistent` 的 SAML 请求（如步骤 2：创建 SAML 2.0 联合身份验证 IAM 角色中所述）。
- 将 **Name** 属性设置为 **`https://aws.amazon.com/SAML/Attributes/Role`** 的 **Attribute** 元素 - 此元素中包含一个或多个 `AttributeValue` 元素，用于列出您的 IdP 将用户映射到哪个 IAM 角色和 SAML IdP。角色和 IdP 指定为逗号分隔的 ARN 对。预期值的一个示例是 `arn:aws:iam::ACCOUNTNUMBER:role/ROLENAME,arn:aws:iam::ACCOUNTNUMBER:saml-provider/PROVIDERNAME`。
- **AttributeName**属性设置为的元素 **`https://aws.amazon.com/SAML/Attributes/RoleSessionName`** — 此元素包含一个元素，该`AttributeValue`元素为为 SSO 颁发的 AWS 临时证书提供标识符。`AttributeValue` 元素中的值长度必须介于 2 到 64 个字符之间，只能包含字母数字字符、下划线和以下字符：_ . : / = + - @。它不能包含空格。该值通常是电子邮件地址或用户主体名 (UPN)。该值不应包含空格，如用户的显示名称。
- 将 **Name** 属性设置为 **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`** 的 **Attribute** 元素 - 此元素包含一个提供用户电子邮件地址的 `AttributeValue` 元素。该值必须与 WorkSpaces 目录中定义的 WorkSpaces 用户电子邮件地址相匹配。标签值可能包括字母、数字和 _ . : / = + - @ 字符的组合。有关更多信息，请参阅《IAM 用户指南》中的标记 IAM 用户和 AWS STS的规则。
- 将 **Name** 属性设置为 **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:UserPrincipalName`** 的 **Attribute** 元素（可选）- 此元素包含一个为登录用户提供 Active Directory `userPrincipalName` 的 `AttributeValue` 元素。必须采用 `username@domain.com` 格式提供该值。此参数与基于证书的身份验证一起使用，作为最终用户证书中的主题备用名称。有关更多信息，请参阅基于证书的身份验证。
- 将 **Name** 属性设置为 **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:ObjectSid`** 的 **Attribute** 元素（可选）- 此元素包含一个为登录用户提供

Active Directory 安全标识符 (SID) 的 AttributeValue 元素。此参数与基于证书的身份验证一起使用，以启用到 Active Directory 用户的强映射。有关更多信息，请参阅基于证书的身份验证。

- 将 **Name** 属性设置为 **https://aws.amazon.com/SAML/Attributes/PrincipalTag:ClientUserName** 的 **Attribute** 元素（可选）- 此元素包含一个提供备用用户名格式的 AttributeValue 元素。如果您的用例需要用户名格式（例如corp\username、或）username@corp.example.com才能使用 WorkSpaces 客户端登录corp.example.com\username，请使用此属性。标签键和值可以包含字母、数字、空格以及 _ : / . + = @ - 字符的任意组合。有关更多信息，请参阅《IAM 用户指南》中的标记 IAM 用户和 AWS STS的规则。要声明 corp\username 或 corp.example.com\username 格式，请将 SAML 断言中的 \ 替换为 /。
- **AttributeName**属性设置为 https://aws.amazon.com/SAML/Attributes/:Domain 的元素 PrincipalTag（可选）— 此元素包含一个为登录用户提供 Active Directory DNS 完全限定域名 (FQDN) 的元素AttributeValue。当用户的 Active Directory userPrincipalName 包含备用后缀时，此参数用于基于证书的身份验证。必须采用 domain.com 提供该值，包括所有子域名。
- **AttributeName**属性设置为 https://aws.amazon.com/SAML/Attributes/ 的元素 SessionDuration（可选）— 此元素包含一个AttributeValue元素，用于指定在要求重新进行身份验证之前，用户的联合流媒体会话可以保持活动状态的最长时间。默认值为 3600 秒（60 分钟）。有关更多信息，请参阅 SAML SessionDurationAttribute。

> **Note**
>
> 虽然 SessionDuration 是一个可选属性，但建议您将该属性包含在 SAML 响应中。如果您未指定此属性，则会话持续时间将设置为默认值 3600 秒（60 分钟）。 WorkSpaces 桌面会话将在会话持续时间到期后断开连接。

有关如何配置这些元素的更多信息，请参阅《IAM 用户指南》中的为身份验证响应配置 SAML 断言。有关 IdP 的具体配置要求的信息，请参阅 IdP 的文档。

步骤 6：配置您的联合身份验证的中继状态

接下来，使用您的 IdP 将联盟的中继状态配置为指向 WorkSpaces 目录中继状态 URL。成功通过身份验证后 AWS，用户将被定向到 WorkSpaces 目录端点，该终端节点在 SAML 身份验证响应中定义为中继状态。

以下为中继状态 URL 格式：

```
https://relay-state-region-endpoint/sso-idp?registrationCode=registration-code
```

根据您的 WorkSpaces 目录注册码和与您的目录所在区域关联的中继状态端点构建您的中继状态 URL。可以在 WorkSpaces 管理控制台中找到注册码。

或者，如果您使用跨区域重定向 WorkSpaces，则可以将注册代码替换为与主区域和故障转移区域中的目录关联的完全限定域名 (FQDN)。有关更多信息，请参阅 Amazon 的跨区域重定向。 WorkSpaces 使用跨区域重定向和 SAML 2.0 身份验证时，需要使用与每个区域关联的中继状态端点，为 SAML 2.0 身份验证启用主目录和故障转移目录，并使用 IdP 进行独立配置。这将允许用户在登录前注册其 WorkSpaces 客户端应用程序时正确配置 FQDN，并允许用户在故障转移事件期间进行身份验证。

下表列出了可用 WorkSpaces SAML 2.0 身份验证的区域的中继状态端点。

支持 WorkSpaces SAML 2.0 身份验证的区域

区域	中继状态端点
美国东部（弗吉尼亚州北部）区域	• workspaces.euc-sso.us-east-1.aws.amazon.com • (FIPS) workspaces.euc-sso-fips.us-east-1.aws.amazon.com
美国西部（俄勒冈州）区域	• workspaces.euc-sso.us-west-2.aws.amazon.com • (FIPS) workspaces.euc-sso-fips.us-west-2.aws.amazon.com
非洲（开普敦）区域	workspaces.euc-sso.af-south-1.aws.amazon.com
亚太地区（孟买）区域	workspaces.euc-sso.ap-south-1.aws.amazon.com
亚太地区（首尔）区域	workspaces.euc-sso.ap-northeast-2.aws.amazon.com
亚太地区（新加坡）区域	workspaces.euc-sso.ap-southeast-1.aws.amazon.com

区域	中继状态端点
亚太地区（悉尼）区域	workspaces.euc-sso.ap-southeast-2.aws.amazon.com
Asia Pacific（Tokyo）Region	workspaces.euc-sso.ap-northeast-1.aws.amazon.com
加拿大（中部）区域	workspaces.euc-sso.ca-central-1.aws.amazon.com
欧洲地区（法兰克福）区域	workspaces.euc-sso.eu-central-1.aws.amazon.com
欧洲地区（爱尔兰）区域	workspaces.euc-sso.eu-west-1.aws.amazon.com
欧洲地区（伦敦）区域	workspaces.euc-sso.eu-west-2.aws.amazon.com
南美洲（圣保罗）区域	workspaces.euc-sso.sa-east-1.aws.amazon.com
以色列（特拉维夫）区域	workspaces.euc-sso.il-central-1.aws.amazon
AWS GovCloud （美国西部）	• workspaces.euc-sso.us-gov-west-1.amazonaws-us-gov.com • (FIPS) workspaces.euc-sso-fips.us-gov-west-1.amazonaws-us-gov.com **Note** 有关更多信息，请参阅 AWS GovCloud（美国）用户指南 WorkSpaces中的 Amazon。

区域	中继状态端点
AWS GovCloud （美国东部）	• workspaces.euc-sso.us-gov-east-1.amazonaws-us-gov.com • (FIPS) workspaces.euc-sso-fips.us-gov-east-1.amazonaws-us-gov.com **Note** 有关更多信息，请参阅 AWS GovCloud （美国）用户指南 WorkSpaces中的 Amazon。

步骤 7：在您的 WorkSpaces 目录上启用与 SAML 2.0 的集成

您可以使用 WorkSpaces 控制台在 WorkSpaces 目录上启用 SAML 2.0 身份验证。

启用与 SAML 2.0 的集成

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择目录。
3. 选择您的 “目录 ID” WorkSpaces。
4. 在身份验证下，选择编辑。
5. 选择编辑 SAML 2.0 身份提供者。
6. 选中启用 SAML 2.0 身份验证。
7. 对于用户访问 URL 和 IdP 深层链接参数名称，输入适用于您 IdP 和您在步骤 1 中配置的应用程序的值。如果您省略此参数，则 IdP 深度链接参数名称的默认值RelayState为 “”。下表列出了应用程序的各种身份提供者所独有的用户访问 URL 和参数名称。

   要添加到允许列表的域和 IP 地址

身份提供商	参数	用户访问 URL
ADFS	`RelayState`	`https://<host>/adfs/ls/idpinitiateds`

身份提供商	参数	用户访问 URL
		ignon.aspx?RelayState=RPID=<relaying-party-uri>
Azure AD	RelayState	https://myapps.microsoft.com/signin/<app_id>?tenantId=<tenant_id>
Duo Single Sign-On	RelayState	https://<sub-domain>.sso.duosecurity.com/saml2/sp/<app_id>/sso
Okta	RelayState	https://<sub_domain>.okta.com/app/<app_name>/<app_id>/sso/saml
OneLogin	RelayState	https://<sub-domain>.onelogin.com/trust/saml2/http-post/sso/<app-id>
JumpCloud	RelayState	https://sso.jumpcloud.com/saml2/<app-id>
Auth0	RelayState	https://<DefaultTenatName>.us.auth0.com/samlp/<Client_Id>
PingFederate	TargetResource	https://<host>/idp/startSSO.ping?PartnerSpId=<sp_id>

身份提供商	参数	用户访问 URL
PingOne 适用于企业	`TargetResource`	`https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=<app_id>&idpid=<idp_id>`

用户访问 URL 通常由提供者针对未经请求的 IdP 发起的 SSO 定义。用户可以在 Web 浏览器中输入此 URL，以直接与 SAML 应用程序联合。要测试 IdP 的用户访问 URL 和参数值，请选择测试。将测试 URL 复制并粘贴到当前浏览器或其他浏览器的私有窗口，以便在不中断当前 AWS 管理控制台会话的情况下测试 SAML 2.0 登录。当 IDP 启动的流程打开时，您可以注册您的 WorkSpaces 客户端。有关更多信息，请参阅身份提供者 (IdP) 启动的流程。

8. 通过选中或取消选中允许不支持 SAML 2.0 的客户端登录，管理回退设置。启用此设置可继续为用户提供 WorkSpaces 使用不支持 SAML 2.0 的客户端类型或版本的访问权限，或者如果用户需要时间升级到最新的客户端版本。

> **Note**
>
> 此设置允许用户绕过 SAML 2.0 和使用旧版客户端通过目录身份验证进行的登录。

9. 要将 SAML 与 Web 客户端一起使用，请启用 Web Access。有关更多信息，请参阅启用和配置 Amazon WorkSpaces Web Access。

> **Note**
>
> Web Access 不支持带有 SAML 的 PCoIP。

10. 选择保存。您的 WorkSpaces 目录现已启用 SAML 2.0 集成。您可以使用 IDP 启动的流程和客户端应用程序启动的流程来注册 WorkSpaces 客户端应用程序并登录。 WorkSpaces

基于证书的身份验证

您可以使用基于证书的身份验证 WorkSpaces 来移除用户输入 Active Directory 域密码的提示。通过对您的 Active Directory 域使用基于证书的身份验证，您可以：

- 依靠您的 SAML 2.0 身份提供商对用户进行身份验证，并提供 SAML 断言以匹配 Active Directory 中的用户。
- 使用更少的用户提示启用单点登录体验。
- 使用 SAML 2.0 身份提供商启用无密码身份验证流程。

基于证书的身份验证使用您 AWS Private CA AWS 账户中的资源。 AWS Private CA 允许创建私有证书颁发机构 (CA) 层次结构，包括根证书颁发机构和从属 CA。使用 AWS Private CA，您可以创建自己的 CA 层次结构，并使用它颁发证书，用于对内部用户进行身份验证。有关更多信息，请参阅《AWS Private Certificate Authority 用户指南》。

使用基于证书 AWS Private CA 的身份验证时， WorkSpaces 将在会话身份验证期间自动为您的用户请求证书。使用预调配了证书的虚拟智能卡对用户进行 Active Directory 身份验证。

使用最新的 WorkSpaces Web Access、Windows WorkSpaces 和 macOS 客户端应用程序的 Windows WorkSpaces 流媒体协议 (WSP) 捆绑包支持基于证书的身份验证。打开 Amazon WorkSpaces 客户端下载以查找最新版本：

- Windows 客户端 5.5.0 或更高版本
- macOS 客户端 5.6.0 或更高版本

有关使用 Amazon 配置基于证书的身份验证的更多信息 WorkSpaces，请参阅如何为 Amazon 配置基于证书的身份验证 WorkSpaces和 2.0 版基于证书的身份验证在高度监管的环境中的设计注意事项。AppStream WorkSpaces

先决条件

在启用基于证书的身份验证之前，请完成以下步骤。

1. 使用 SAML 2.0 集成配置您的 WorkSpaces 目录，以使用基于证书的身份验证。有关更多信息，请参阅与 SAML 2.0 WorkSpaces 集成。
2. 在 SAML 断言中配置 `userPrincipalName` 属性。有关更多信息，请参阅为 SAML 身份验证响应创建断言。
3. 在 SAML 断言中配置 `ObjectSid` 属性。这为可选项，用于对 Active Directory 用户执行强映射。如果该属性与 SAML_Subject `NameID` 中指定的用户的 Active Directory 安全标识符 (SID) 不匹配，则基于证书的身份验证将失败。有关更多信息，请参阅为 SAML 身份验证响应创建断言。

4. 将 sts: TagSession 权限添加到用于 SAML 2.0 配置的 IAM 角色信任策略（如果尚未存在）。使用基于证书的身份验证时需要此权限。有关更多信息，请参阅创建 SAML 2.0 联合身份验证 IAM 角色。
5. AWS Private CA 如果您的 Active Directory 中没有配置私有证书颁发机构 (CA)，请使用创建私有证书颁发机构 (CA)。 AWS Private CA 必须使用基于证书的身份验证。有关更多信息，请参阅规划 AWS Private CA 部署并按照指南为基于证书的身份验证配置 CA。以下 AWS Private CA 设置是基于证书的身份验证用例中最常见的设置：
   a. CA 类型选项：
      i. 短期证书 CA 使用模式（如果您仅使用 CA 为基于证书的身份验证颁发最终用户证书，则建议使用此模式）
      ii. 带有根 CA 的单级层次结构（或者，在希望与现有 CA 层次结构集成时选择从属 CA）
   b. 密钥算法选项：RSA 2048
   c. 主题可分辨名称选项：使用任何选项组合在 Active Directory 受信任的根证书颁发机构存储中识别此 CA。
   d. 证书吊销选项：CRL 分发

   > **Note**
   >
   > 基于证书的身份验证需要一个可从桌面和域控制器访问的在线 CRL 分发点。这需要对为私有 CA CRL 条目配置的 Amazon S3 存储桶进行未经身份验证的访问权限，或者如果 CloudFront分配阻止公开访问，则该分配将有权访问 S3 存储桶。有关这些选项的更多信息，请参阅计划证书吊销列表 (CRL)。

6. 使用名为 `euc-private-ca` 的键标记您的私有 CA，以指定该 CA 用于 EUC 基于证书的身份验证。该键不需要值。有关更多信息，请参阅管理私有 CA 的标签。
7. 基于证书的身份验证使用虚拟智能卡进行登录。按照 Active Directory 中使用第三方证书颁发机构启用智能卡登录的指导原则，执行以下步骤：
   - 使用域控制器证书配置域控制器，以对智能卡用户进行身份验证。如果您在 Active Directory 中配置了 Active Directory 证书服务企业 CA，则系统会自动使用启用智能卡登录的证书注册域控制器。如果您没有 Active Directory 证书服务，请参阅对第三方 CA 的域控制器证书的要求。您可以使用 AWS Private CA创建域控制器证书。如果这样做，请不要使用为短期证书配置的私有 CA。

     > **Note**
     >
     > 如果您正在使用 AWS Managed Microsoft AD，则可以在 EC2 实例上配置证书服务以满足域控制器证书的要求。有关 AWS Managed Microsoft AD 配置AWS Launch Wizard了

Active Directory 证书服务的部署示例，请参阅。 AWS 私有 CA 可以配置为 Active Directory 证书服务 CA 的从属机构，也可以在使用时将其配置为自己的根 AWS Managed Microsoft AD。
AWS Managed Microsoft AD 和 Active Directory 证书服务的另一项配置任务是创建从控制器 VPC 安全组到运行证书服务的 EC2 实例的出站规则，允许 TCP 端口 135 和 49152-65535 启用证书自动注册。此外，正在运行的 EC2 实例还必须允许域实例（包括域控制器）在这些相同的端口上进行入站访问。有关查找安全组的更多信息， AWS Managed Microsoft AD 请参阅配置您的 VPC 子网和安全组。

- 在 AWS Private CA 控制台上或使用 SDK 或 CLI，选择您的 CA，然后在 CA 证书下导出 CA 私有证书。有关更多信息，请参阅导出私有证书。
- 将 CA 发布到 Active Directory。登录到域控制器或已加入域的计算机。将私有 CA 证书复制到任意 `<path>\<file>`，然后以域管理员身份运行以下命令。或者，您也可以使用组策略和 Microsoft PKI Health Tool (PKIView) 工具发布 CA。有关更多信息，请参阅配置说明。

```
certutil -dspublish -f <path>\<file> RootCA
certutil -dspublish -f  <path>\<file> NTAuthCA
```

确保命令成功完成，然后删除私有证书文件。根据 Active Directory 复制设置，CA 可能需要几分钟才能发布到您的域控制器和桌面实例。

> **Note**
>
> - Active Directory 要求 Active Directory 在 WorkSpaces 台式机加入域时自动将 CA 分发给受信任的根证书颁发机构和企业 nTauth 存储区。
> - Active Directory 域控制器必须处于兼容模式，证书强制执行才能支持基于证书的身份验证。有关更多信息，请参阅 Microsoft Support 文档中的 kb5014754 — Windows 域控制器上基于证书的身份验证更改。如果你使用的是 AWS 托管 Microsoft AD，请参阅配置目录安全设置了解更多信息。

启用基于证书的身份验证

要启用基于证书的身份验证，请完成以下步骤。

1. 打开 WorkSpaces 控制台，网址为https://console.aws.amazon.com/workspaces。
2. 在导航窗格中，选择目录。

3. 选择您的目录 ID WorkSpaces。
4. 在身份验证下，单击编辑。
5. 单击编辑基于证书的身份验证。
6. 选中启用基于证书的身份验证。
7. 确认您的私有 CA ARN 已关联到列表中。私有 CA 应位于同一个 AWS 账户中 AWS 区域，并且必须使用有权出现在列表中的密钥 euc-private-ca 进行标记。
8. 单击 Save Changes（保存更改）。基于证书的身份验证现已启用。
9. 重启你的 Window WorkSpaces s WorkSpaces 直播协议 (WSP) 捆绑包以使更改生效。有关更多信息，请参阅重启 a WorkSpace。
10. 重启后，当用户使用支持的客户端通过 SAML 2.0 进行身份验证时，将不再收到输入域密码的提示。

> **Note**
>
> 启用基于证书的身份验证登录时，即使在目录中启用了多重身份验证 (MFA) WorkSpaces，也不会提示用户进行多重身份验证 (MFA)。使用基于证书的身份验证时，可以通过 SAML 2.0 身份提供商启用 MFA。有关 AWS Directory Service MFA 的更多信息，请参阅多重身份验证 (AD Connector) 或为启用多因素身份验证。 AWS Managed Microsoft AD

管理基于证书的身份验证

CA 证书

在典型配置中，私有 CA 证书的有效期为 10 年。有关更换证书过期的 CA 或重新颁发具有新有效期的 CA 的更多信息，请参阅管理私有 CA 生命周期。

最终用户证书

为 WorkSpaces 基于证书的身份验证 AWS Private CA 而颁发的最终用户证书不需要续订或撤销。这些证书是短暂的。 WorkSpaces每 24 小时自动颁发一次新证书。这些最终用户证书的有效期比典型的 AWS Private CA CRL 发行版短。因此，无需吊销最终用户证书，这些证书也不会出现在 CRL 中。

审核报告

您可以创建审核报告，以列出您的私有 CA 已颁发和吊销的所有证书。有关更多信息，请参阅将审核报告与私有 CA 结合使用。

日志记录和监控

您可以使用AWS CloudTrail来记录对 by 的 API 调 AWS Private CA 用 WorkSpaces。有关更多信息，请参阅使用 CloudTrail。在CloudTrail事件历史记录中GetCertificate，IssueCertificate您可以查看由 WorkSpacesEcmAssumeRoleSession用户名acm-pca.amazonaws.com创建的事件源中的事件名称。每个 EUC 基于证书的身份验证请求都将记录这些事件。

启用跨账户 PCA 共享

当您使用 Private CA 跨账户共享时，您可以向其他账户授予使用集中式 CA 的权限，这样就无需在每个账户中都使用私有 CA。CA 可以通过使用 R es AWS ource Access M anager 来管理权限来生成和颁发证书。私有 CA 跨账户共享可在同一区域内与 WorkSpaces 基于证书的身份验证 (CBA) 一起使用。 AWS

与 CBA 一起使用共享的私有 WorkSpaces CA 资源

1. 在集中 AWS 账户中配置 CBA 的私有 CA。有关更多信息，请参阅 基于证书的身份验证。
2. 按照如何使用 AWS RAM 跨 AWS 账户共享 ACM 私有 CA 中的步骤，与 WorkSpaces 资源使用 CBA 的资源账户共享私有 CA。您无需完成步骤 3 即可创建证书。您可以与个人 AWS 账户共享私有 CA，也可以通过 Organizations AWS 共享。要与个人账户共享，您需要使用资源访问管理器 (RAM) 控制台或 API 接受资源账户中的共享私有 CA。配置共享时，请确认资源账户中私有 CA 的 RAM 资源共享使用AWS RAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority托管权限模板。此模板与 WorkSpaces 服务角色在颁发 CBA 证书时使用的 PCA 模板一致。
3. 共享成功后，您应该能够使用资源账户中的私有 CA 控制台查看共享的私有 CA。
4. 使用 API 或 CLI 在目录属性中将私有 CA ARN 与 CBA 相关联。 WorkSpaces 目前，WorkSpaces 控制台不支持选择共享的私有 CA ARN。CLI 命令示例：

```
aws workspaces modify-certificate-based-auth-properties –resource-id <value> –
certificate-based-auth-properties Status=<value>,CertificateAuthorityArn=<value>
```

使用智能卡进行身份验证

WorkSpaces 基于 WorkSpaces 流媒体协议 (WSP) 的 Windows 和 Linux 套装允许使用通用访问卡 (CAC) 和个人身份验证 (PIV) 智能卡进行身份验证。

Amazon WorkSpaces 支持使用智能卡进行会话前身份验证和会话中身份验证。会话前身份验证是指在用户登录时执行的智能卡身份验证。 WorkSpaces会话中身份验证是指登录后执行的身份验证。

例如，在使用 Web 浏览器和应用程序时，用户可以使用智能卡进行会话中身份验证。他们也可以使用智能卡执行需要管理权限的操作。例如，如果用户拥有其 Linux 的管理权限 WorkSpace，则他们可以在运行`sudo`和`sudo -i`命令时使用智能卡进行身份验证。

内容

要求

- 会话前身份验证需要 Active Directory Connector (AD Connector) 目录。AD Connector 使用基于证书的相互传输层安全行协议身份验证（相互 TLS），通过基于硬件或软件的智能卡证书对 Active Directory 的用户进行身份验证。有关如何配置 AD Connector 和本地目录的更多信息，请参阅目录配置。
- 要在 Windows 或 Linux 上使用智能卡 WorkSpace，用户必须使用亚马逊 WorkSpaces Windows 客户端版本 3.1.1 或更高版本或 mac WorkSpaces OS 客户端 3.1.5 或更高版本。有关在 Windows 和 macOS 客户端上使用智能卡的更多信息，请参阅亚马逊 WorkSpaces 用户指南中的智能卡支持。
- 根 CA 和智能卡证书必须满足某些要求。有关更多信息，请参阅《AWS Directory Service 管理指南》中的在 AD Connector 中启用 mTLS 身份验证以用于智能卡以及 Microsoft 文档中的证书要求。

  除这些要求外，用于向 Amazon 进行智能卡身份验证的用户证书还 WorkSpaces 必须包含以下属性：

  - 证书 userPrincipalName (SAN) 字段中的 AD 用户 subjectAltName (UPN)。建议为用户的默认 UPN 颁发智能卡证书。
  - 客户端身份验证 (1.3.6.1.5.5.7.3.2) 扩展密钥使用 (EKU) 属性。
  - 智能卡登录 (1.3.6.1.4.1.311.20.2.2) EKU 属性。
- 对于会话前身份验证，需要在线证书状态协议 (OCSP) 来检查证书吊销。对于会话中身份验证，建议使用 OCSP，但不是必需的。

限制

- 目前仅支持 WorkSpaces Windows 客户端应用程序版本 3.1.1 或更高版本以及 macOS 客户端应用程序版本 3.1.5 或更高版本进行智能卡身份验证。
- 只有在 64 位版本的 WorkSpaces Windows 上运行时，Windows 客户端应用程序 3.1.1 或更高版本才支持智能卡。
- Ubuntu 目前 WorkSpaces 不支持智能卡身份验证。
- 目前只支持 AD Connector 目录进行智能卡身份验证。
- 会话中身份验证在所有支持 WSP 的区域均可用。以下区域提供会话前身份验证：
  - 亚太地区（悉尼）区域
  - Asia Pacific（Tokyo）Region
  - 欧洲地区（爱尔兰）区域
  - AWS GovCloud （美国东部）区域
  - AWS GovCloud （美国西部）区域
  - 美国东部（弗吉尼亚州北部）区域
  - 美国西部（俄勒冈州）区域
- 对于 Linux 或 Windows 上的会话内身份验证和会话前身份验证 WorkSpaces，目前一次只能使用一张智能卡。
- 对于会话前身份验证，目前不支持在同一目录上同时启用智能卡身份验证和登录身份验证。
- 目前仅支持 CAC 和 PIV 卡。其他类型基于硬件或软件的智能卡也可能起作用，但它们尚未经过与 WSP 配合使用的全面测试。

目录配置

要启用智能卡身份验证，必须按以下方式配置 AD Connector 目录和本地目录。

AD Connector 目录配置

在开始之前，请确保您的 AD Connector 目录已按照《AWS Directory Service 管理指南》内 AD Connector 先决条件中所述进行设置。特别是，请确保您已在防火墙中打开必要的端口。

要完成 AD Connector 目录的配置，请按照《AWS Directory Service 管理指南》内在 AD Connector 中启用 mTLS 身份验证以用于智能卡中的说明进行操作。

> **Note**
>
> 智能卡身份验证需要 Kerberos 约束委托 (KCD) 才能正常运行。KCD 要求 AD Connector 服务帐户的用户名部分与同一用户的 SaM AccountName 相匹配。SaM AccountName 不能超过 20 个字符。

本地目录配置

除了配置 AD Connector 目录外，您还必须确保向本地目录的域控制器颁发的证书设置了“KDC 身份验证”扩展密钥使用 (EKU)。为此，请使用 Active Directory 域服务 (AD DS) 默认 Kerberos 身份验证证书模板。请勿使用域控制器证书模板或域控制器身份验证证书模板，因为这些模板不包含智能卡身份验证所需的设置。

启用适用于 Windows 的智能卡 WorkSpaces

有关如何在 Windows 上启用智能卡身份验证的一般指南，请参阅 Microsoft 文档中使用第三方证书颁发机构启用智能卡登录指南。

检测 Windows 锁屏并断开会话连接

要允许用户在屏幕锁定时解锁启用了智能卡会话前身份验证的 Window WorkSpaces s，可以在用户会话中启用 Windows 锁屏检测。当检测到 Windows 锁屏时， WorkSpace 会话将断开，用户可以使用其智能卡从 WorkSpaces 客户端重新连接。

您可以使用组策略设置，启用在检测到 Windows 锁屏时断开会话连接。有关更多信息，请参阅启用或禁用 WSP 屏幕锁定时断开会话连接。

启用会话内或会话前身份验证

默认情况下，Windows WorkSpaces 不支持使用智能卡进行会话前或会话中身份验证。如果需要，您可以使用组策略设置为 Windows WorkSpaces 启用会话中和会话前身份验证。有关更多信息，请参阅启用或禁用 WSP 的智能卡重定向。

要使用会话前身份验证，除了更新组策略设置外，您还必须通过 AD Connector 目录设置启用会话前身份验证。有关更多信息，请按照《AWS Directory Service 管理指南》内在 AD Connector 中启用 mTLS 身份验证以用于智能卡中的说明进行操作。

允许用户在浏览器中使用智能卡

如果您的用户使用 Chrome 作为浏览器，则无需进行特殊配置即可使用智能卡。

如果您的用户使用 Firefox 作为浏览器，则您可以通过组策略允许您的用户在 Firefox 中使用智能卡。您可以在中使用这些 Firefox 组策略模板。 GitHub

例如，您可以安装适用于 Windows 的 64 位版本的 OpenSC 来支持 PKCS #11，然后使用以下组策略设置，其中 *NAME_OF_DEVICE* 是您要用来标识 PKCS #11 的任何值，例如 OpenSC，其中 *PATH_TO_LIBRARY_FOR_DEVICE* 是 PKCS #11 模块的路径。此路径应指向扩展名为 .DLL 的库，例如 `C:\Program Files\OpenSC Project\OpenSC\pkcs11\onepin-opensc-pkcs11.dll`。

```
Software\Policies\Mozilla\Firefox\SecurityDevices\NAME_OF_DEVICE
 = PATH_TO_LIBRARY_FOR_DEVICE
```

Tip

如果您使用的是 OpenSC，也可以通过运行 `pkcs11-register.exe` 程序，将 OpenSC pkcs11 模块加载到 Firefox 中。要运行此程序，请双击 `C:\Program Files\OpenSC Project\OpenSC\tools\pkcs11-register.exe` 中的文件，或者打开命令提示符窗口并运行以下命令：

```
"C:\Program Files\OpenSC Project\OpenSC\tools\pkcs11-register.exe"
```

要验证 OpenSC pkcs11 模块是否已加载到 Firefox 中，请执行以下操作：

1. 如果 Firefox 已经在运行，请将其关闭。
2. 打开 Firefox。选择右上角的菜单按钮

   ，

   然后选择选项。
3. 在关于: 首选项页面上，在左侧导航窗格中选择隐私与安全。
4. 在证书下，选择安全设备。
5. 在设备管理器对话框中，您应该在左侧导航栏中看到 OpenSC 智能卡框架 (0.21)，当您选择它时，它应该具有以下值：

   模块：`OpenSC smartcard framework (0.21)`

   路径：`C:\Program Files\OpenSC Project\OpenSC\pkcs11\onepin-opensc-pkcs11.dll`

故障排除

有关排查智能卡问题的信息，请参阅 Microsoft 文档中的证书和配置问题。

可能导致问题的一些常见问题：

- 槽与证书的映射不正确。
- 智能卡上有多个可以与用户匹配的证书。证书使用以下标准进行匹配：
  - 证书的根 CA。
  - 证书的 <KU> 和 <EKU> 字段。
  - 证书主题中的 UPN。
- 多个证书的密钥用法中存在 <EKU>msScLogin。

通常，最好只有一个用于智能卡身份验证的证书，该证书映射到智能卡的第一个槽。

用于管理智能卡上的证书和密钥（例如删除或重新映射证书和密钥）的工具可能因制造商而异。有关更多信息，请参阅智能卡制造商提供的文档。

启用适用于 Linux 的智能卡 WorkSpaces

> **Note**
>
> WSP WorkSpaces 上的 Linux 目前存在以下限制：
>
> - 不支持剪贴板、音频输入、视频输入和时区重定向。
> - 不支持多个显示器。
> - 你必须使用 WorkSpaces Windows 客户端应用程序连接到 WSP WorkSpaces 上的 Linux。

要在 Linux 上启用智能卡 WorkSpaces，您需要在 WorkSpace 镜像中包含 PEM 格式的根 CA 证书文件。

获取根 CA 证书

您可以通过以下几种方式获取根 CA 证书：

- 您可以使用由第三方证书颁发机构运营的根 CA 证书。

- 您可以使用 Web 注册网站导出自己的根 CA 证书，该网站为 `http://ip_address/certsrv` 或 `http://fqdn/certsrv`，其中 *ip_address* 和 *fqdn* 分别是根证书 CA 服务器的 IP 地址和完全限定域名 (FQDN)。有关使用 Web 注册网站的更多信息，请参阅 Microsoft 文档中的如何导出根证书颁发机构证书。
- 您可以使用以下步骤，从运行 Active Directory 证书服务 (AD CS) 的根 CA 证书服务器导出根 CA 证书。有关安装 AD CS 的信息，请参阅 Microsoft 文档中的安装证书颁发机构。

  1. 使用管理员账户登录根 CA 服务器。
  2. 在 Windows 的开始菜单中，打开命令提示符窗口（开始 > Windows 系统 > 命令提示符）。
  3. 使用以下命令将根 CA 证书导出到新文件，其中 *rootca*.cer 是新文件的名称：

     ```
     certutil -ca.cert rootca.cer
     ```

     有关运行 certutil 的更多信息，请参阅 Microsoft 文档中的 certutil。
  4. 使用以下 OpenSSL 命令将导出的根 CA 证书从 DER 格式转换为 PEM 格式，其中 *rootca* 是证书的名称。有关 OpenSSL 的更多信息，请访问 www.openssl.org。

     ```
     openssl x509 -inform der -in rootca.cer -out /tmp/rootca.pem
     ```

将您的根 CA 证书添加到您的 Linux WorkSpaces

为了帮助您启用智能卡，我们已将 `enable_smartcard` 脚本添加到我们的 Amazon Linux WSP 捆绑包中。此脚本将执行以下操作：

- 将您的根 CA 证书导入网络安全服务 (NSS) 数据库。
- 安装可插入验证模块 (PAM) 身份验证的 `pam_pkcs11` 模块。
- 执行默认配置，包括在 WorkSpace 置备`pkinit`期间启用。

以下过程说明如何使用`enable_smartcard`脚本将根 CA 证书添加到 Linux WorkSpaces 以及如何为 Linux 启用智能卡 WorkSpaces。

1. 创建一个启用了 WSP 协议 WorkSpace 的新 Linux。在亚马逊 WorkSpaces 控制台 WorkSpace 中启动时，请务必在 “选择捆绑包” 页面上为协议选择 WSP，然后选择一个 Amazon Linux 2 公共捆绑包。
2. 在新版本中 WorkSpace，以 root 身份运行以下命令，其中*pem-path*是 PEM 格式的根 CA 证书文件的路径。

```
/usr/lib/skylight/enable_smartcard --ca-cert pem-path
```

> **Note**
>
> Linux WorkSpaces 假设智能卡上的证书是针对用户的默认用户主体名称 (UPN) 颁发的，例如*sAMAccountName*@*domain*，其中*domain*是完全限定域名 (FQDN)。
> 要使用备用 UPN 后缀，请参阅 `run /usr/lib/skylight/enable_smartcard --help`，了解更多信息。备用 UPN 后缀的映射对每个用户来说都是唯一的。因此，必须对每个用户单独执行映射 WorkSpace。

3. （可选）默认情况下，所有服务都启用在 Linux 上使用智能卡身份验证 WorkSpaces。要将智能卡身份验证仅限于特定服务，必须编辑 `/etc/pam.d/system-auth`。取消 `pam_succeed_if.so` 对应的 `auth` 行的注释，并根据需要编辑服务列表。

   取消 `auth` 行的注释后，要允许服务使用智能卡身份验证，必须将其添加到列表中。要使服务仅使用密码身份验证，必须从列表中将其删除。

4. 对执行任何其他自定义。 WorkSpace例如，您可能希望添加一个系统范围的策略，以允许用户在 Firefox 中使用智能卡。（Chrome 用户必须自己在客户端上启用智能卡。 有关更多信息，请参阅 Amazon WorkSpaces 用户指南中的智能卡支持。）
5. 从@@ 中创建自定义 WorkSpace 映像和捆绑包 WorkSpace。
6. 使用新的自定义捆绑包 WorkSpaces 为用户启动。

允许用户在 Firefox 中使用智能卡

您可以在 Linux WorkSpace 映像中添加 SecurityDevices 策略，让您的用户能够在 Firefox 中使用智能卡。有关向 Firefox 添加系统范围策略的更多信息，请参阅上的 Mozilla 策略模板。 GitHub

1. 在你 WorkSpace 用来创建 WorkSpace 图像的上，创建一个名为`policies.json`的新文件/`usr/lib64/firefox/distribution/`。
2. 在 JSON 文件中，添加以下 SecurityDevices 策略，其中*NAME_OF_DEVICE*是您要用来标识`pkcs`模块的任何值。例如，您可能想使用 "0penSC" 这样的值：

```
{
    "policies": {
        "SecurityDevices": {
            "NAME_OF_DEVICE": "/usr/lib64/opensc-pkcs11.so"
```

```
        }
    }
}
```

故障排除

为了排查问题，建议添加 pkcs11-tools 实用工具。此实用工具允许您执行以下操作：

- 列出每张智能卡。
- 列出每张智能卡上的槽。
- 列出每张智能卡上的证书。

可能导致问题的一些常见问题：

- 槽与证书的映射不正确。
- 智能卡上有多个可以与用户匹配的证书。证书使用以下标准进行匹配：
  - 证书的根 CA。
  - 证书的 <KU> 和 <EKU> 字段。
  - 证书主题中的 UPN。
- 多个证书的密钥用法中存在 <EKU>msScLogin。

通常，最好只有一个用于智能卡身份验证的证书，该证书映射到智能卡的第一个槽。

用于管理智能卡上的证书和密钥（例如删除或重新映射证书和密钥）的工具可能因制造商而异。可用来处理智能卡的其他工具包括：

- opensc-explorer
- opensc-tool
- pkcs11_inspect
- pkcs11_listcerts
- pkcs15-tool

启用调试日志记录

要排查 pam_pkcs11 和 pam-krb5 配置问题，您可以启用调试日志记录。

1. 在 /etc/pam.d/system-auth-ac 文件中，编辑 auth 操作，并将 pam_pksc11.so 的 nodebug 参数更改为 debug。
2. 在 /etc/pam_pkcs11/pam_pkcs11.conf 文件中，将 debug = false; 更改为 debug = true;。debug 选项分别适用于每个映射器模块，因此，您可能需要直接在pam_pkcs11部分下方和相应的映射器部分（默认情况下，这为 mapper generic）下，对其进行更改。
3. 在 /etc/pam.d/system-auth-ac 文件中，编辑 auth 操作，并将 debug 或 debug_sensitive 参数添加到 pam_krb5.so。

启用调试日志记录后，系统会直接在活动终端中打印出 pam_pkcs11 调试消息。来自 pam_krb5 的消息已记录在 /var/log/secure 中。

要检查智能卡证书映射到哪个用户名，请使用以下 pklogin_finder 命令：

```
sudo pklogin_finder debug config_file=/etc/pam_pkcs11/pam_pkcs11.conf
```

系统提示时，输入智能卡 PIN。pklogin_finder 在 stdout 上以 *NETBIOS**username* 的形式输出智能卡证书的用户名。此用户名应与 WorkSpace 用户名匹配。

在 Active Directory 域服务 (AD DS) 中，NetBIOS 域名是 Windows 2000 之前的域名。通常（但并非总是如此），NetBIOS 域名是域名系统 (DNS) 域名的子域。例如，如果 DNS 域名为 example.com，则 NetBIOS 域名通常为 EXAMPLE。如果 DNS 域名为 corp.example.com，则 NetBIOS 域名通常为 CORP。

例如，对于域 corp.example.com 中的用户 mmajor，来自 pklogin_finder 的输出为 CORP\mmajor。

> **Note**
>
> 如果您收到消息 "ERROR:pam_pkcs11.c:504: verify_certificate() failed"，则此消息表示 pam_pkcs11 已在智能卡上找到了符合用户名标准的证书，但该证书未链接到计算机可识别的根 CA 证书。发生这种情况时，pam_pkcs11 会输出上述消息，然后尝试下一个证书。它仅在找到与用户名匹配且链接到可识别的根 CA 证书的证书时，才允许进行身份验证。

要排查 pam_krb5 配置问题，您可以使用以下命令在调试模式下手动调用 kinit：

```
KRB5_TRACE=/dev/stdout kinit -V
```

此命令应成功获取 Kerberos 票证授予票证 (TGT)。如果失败，请尝试在命令中显式添加正确的 Kerberos 主体名称。例如，对于域 `corp.example.com` 中的用户 `mmajor`，使用以下命令：

```
KRB5_TRACE=/dev/stdout kinit -V mmajor
```

如果此命令成功，则问题很可能出在从 WorkSpace 用户名到 Kerberos 主体名称的映射中。检查 `/etc/krb5.conf` 文件中的 `[appdefaults]/pam/mappings` 部分。

如果此命令不成功，但基于密码的 `kinit` 命令成功了，请检查 `/etc/krb5.conf` 文件中的 `pkinit_` 相关配置。例如，如果智能卡包含多个证书，则可能需要对 `pkinit_cert_match` 进行更改。

提供您的 Internet 访问权限 WorkSpace

您 WorkSpaces 必须能够访问互联网，这样才能安装操作系统的更新并部署应用程序。您可以使用以下选项之一来允许您在虚拟私有云 (VPC) WorkSpaces 中访问互联网。

Options

- WorkSpaces 在私有子网中启动您的，并在您的 VPC 的公有子网中配置 NAT 网关。
- WorkSpaces 在公有子网中启动你的，然后自动或手动为你 WorkSpaces分配公有 IP 地址。

有关这些选项的更多信息，请参阅 为以下项配置 VPC WorkSpaces。

使用这些选项中的任何一个，您都必须确保您的安全组 WorkSpaces允许端口 80 (HTTP) 和 443 (HTTPS) 上的出站流量到达所有目的地 (`0.0.0.0/0`)。

Amazon Linux Extras 库

如果您使用的是亚马逊 Linux 存储库，则您的亚马逊 Linux WorkSpaces 必须能够访问互联网，或者必须为此存储库和主 Amazon Linux 存储库配置 VPC 终端节点。有关更多信息，请参阅 Amazon S3 端点中的示例：启用对 Amazon Linux AMI 存储库的访问部分。每个区域中的 Amazon Linux AMI 存储库都是 Amazon S3 存储桶。如果您希望 VPC 中的实例通过端点访问该存储库，请创建端点策略以允许对这些存储桶进行访问。以下策略授予对 Amazon Linux 存储库的访问权限。

```
{
  "Statement": [
    {
        "Sid": "AmazonLinux2AMIRepositoryAccess",
```

```
        "Principal": "*",
        "Action": [
            "s3:GetObject"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::amazonlinux.*.amazonaws.com/*"
        ]
    }
  ]
}
```

您的安全组 WorkSpaces

向注册目录时 WorkSpaces，它会创建两个安全组，一个用于目录控制器，另一个用于目录 WorkSpaces 中。目录控制器的安全组的名称为目录标识符后跟 _controllers（例如，d-12345678e1_controllers）。的安全组的名称由目录标识符组成，后面跟着 _workspacesMembers（例如，d-123456fc 11_workspacesM embers）。 WorkSpaces

> **Warning**
>
> 避免修改、删除或分离 _controllers 和 _work spacesM embers 安全组。修改或删除这些安全组时要小心，因为修改或删除这些安全组后，您将无法重新创建和重新添加它们。相关详情，请参阅适用于 Linux 实例的 Amazon EC2 安全组或适用于 Windows 实例的 Amazon EC2 安全组。

您可以将默认 WorkSpaces 安全组添加到目录中。将新的安全组与 WorkSpaces 目录关联后 WorkSpaces ，您启动的新安全组或重建 WorkSpaces 的现有安全组将拥有新的安全组。您也可以将这个新的默认安全组添加到现有安全组中， WorkSpaces 而无需对其进行重建，如本主题后面所述。

当您将多个安全组与一个 WorkSpaces 目录关联时，每个安全组的规则会被有效地聚合以创建一组规则。建议尽可能精简您的安全组规则。

有关安全组的更多信息，请参阅《Amazon VPC 用户指南》中的您的 VPC 的安全组。

向 WorkSpaces 目录中添加安全组

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。

2. 在导航窗格中，选择目录。
3. 选择目录，然后选择 Actions、Update Details。
4. 展开 Security Group 并选择一个安全组。
5. 选择更新并退出。

要将安全组添加到现有安全组 WorkSpace 而不对其进行重建，请将新的安全组分配给的 elastic network interface (ENI) WorkSpace。

向现有安全组添加安全组 WorkSpace

1. 查找需要更新的每 WorkSpace 个 IP 地址。
    a. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
    b. 展开每个 WorkSpace 并记录其 WorkSpace IP 地址。
2. 找到每个弹性网卡 WorkSpace 并更新其安全组分配。
    a. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
    b. 在网络与安全下，选择网络接口。
    c. 搜索您在步骤 1 中记录的第一个 IP 地址。
    d. 选择与该 IP 地址关联的 ENI，选择操作，然后选择更改安全组。
    e. 选择新安全组，然后选择保存。
    f. 根据需要对其他任何过程重复此过程 WorkSpaces。

适用于您的 WorkSpaces 的 IP 访问控制组

Amazon WorkSpaces 允许您控制可以从哪些 IP 地址访问您的 WorkSpaces。通过使用基于 IP 地址的控制组，您可以定义和管理可信 IP 地址组，并仅允许用户在连接到可信网络时访问其 WorkSpaces。

IP 访问控制组 充当虚拟防火墙，该虚拟防火墙用于控制允许用户从中访问其 WorkSpace 的 IP 地址。要指定 CIDR 地址范围，请向 IP 访问控制组添加规则，然后将该组与您的目录关联。您可以将每个 IP 访问控制组与一个或多个目录关联。您可以为每个区域的每个 AWS 账户创建最多 100 个 IP 访问控制组。不过，您只能将最多 25 个 IP 访问控制组与单个目录关联。

每个目录都与一个默认 IP 访问控制组关联。此默认组包含一条默认规则，以允许用户从任何地方访问其 WorkSpaces。您无法修改目录的默认 IP 访问控制组。如果您没有将 IP 访问控制组与您的目录关联，请使用默认组。如果您将 IP 访问控制组与目录关联，则默认的 IP 访问控制组将断开连接。

要为您的受信任网络指定公有 IP 地址和 IP 地址范围，请向 IP 访问控制组添加规则。如果您的用户通过 NAT 网关或 VPN 访问其 WorkSpace，您必须创建允许从 NAT 网关或 VPN 的公有 IP 地址发出的流量的规则。

> **Note**
>
> - IP 访问控制组不允许为 NAT 使用动态 IP 地址。如果您使用 NAT，请将其配置为使用静态 IP 地址而不是动态 IP 地址。确保 NAT 在 WorkSpace 会话期间通过同一静态 IP 地址路由所有 UDP 流量。
> - IP 访问控制组用于控制用户可将其流式传输会话连接到 WorkSpaces 的 IP 地址。用户仍然可以使用 Amazon WorkSpaces 的公共 API 从任何 IP 地址执行诸如重启、重建、关闭等功能。

您可以将此功能与 Web Access、PCoIP 零客户端及适用于 macOS、iPad、Windows、Chromebook 和 Android 的客户端应用程序结合使用。

创建 IP 访问控制组

可以按以下所述创建 IP 访问控制组。每个 IP 访问控制组可以包含最多 10 个规则。

创建 IP 访问控制组

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 IP Access Controls。
3. 选择 Create IP Group。
4. 在 Create IP Group (创建 IP 组) 对话框中，输入组的名称和描述，然后选择 Create (创建)。
5. 选择所需组，然后选择 Edit。
6. 对于每个 IP 地址，选择 Add Rule。对于 Source (来源)，输入 IP 地址或 IP 地址范围。对于说明，输入说明。添加完规则后，选择 Save。

将 IP 访问控制组与目录关联

您可以将 IP 访问控制组与目录关联，以确保仅从受信任的网络访问 WorkSpace。

如果将没有规则的 IP 访问控制组与目录关联，则会阻止对所有 WorkSpace 的所有访问。

将 IP 访问控制组与目录关联

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择目录。
3. 选择目录，然后选择 Actions、Update Details。
4. 展开 IP Access Control Groups，并选择一个或多个 IP 访问控制组。
5. 选择更新并退出。

复制 IP 访问控制组

您可以使用现有的 IP 访问控制组作为创建新 IP 访问控制组的基础。

从现有的 IP 访问控制组创建一个 IP 访问控制组

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 IP Access Controls。
3. 选择所需组，然后选择 Actions、Copy to New。
4. 在 Copy IP Group (复制 IP 组) 对话框中，输入新组的名称和描述，然后选择 Copy Group (复制组)。
5. (可选) 要修改从原始组中复制的规则，请选择新组，然后选择 Edit。根据需要添加、更新或删除规则。选择 Save（保存）。

删除 IP 访问控制组

您可以随时从 IP 访问控制组中删除规则。如果删除一个用于允许连接到某 WorkSpace 的规则，则用户将与该 WorkSpace 断开连接。

在可以删除 IP 访问控制组之前，必须将其与任何目录解除关联。

删除 IP 访问控制组

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择目录。
3. 对于每个与 IP 访问控制组关联的目录，请选择该目录，然后选择 Actions、Update Details。展开 IP Access Control Groups (IP 访问控制组)，清除 IP 访问控制组的复选框，然后选择 Update and Exit (更新并退出)。

4. 在导航窗格中，选择 IP Access Controls。
5. 选择所需组，然后选择 Actions、Delete IP Group。

为 WorkSpaces 设置 PCoIP 零客户端

PCoIP 零客户端仅与使用 PCoIP 协议的 WorkSpaces 捆绑包兼容。

如果您的零客户端设备的固件为 6.0.0 或更高版本，您的用户就可以直接连接到 WorkSpaces。当您的用户使用零客户端设备直接连接到其 WorkSpaces 时，建议对您的 WorkSpaces 目录使用多重身份验证 (MFA)。有关对目录使用 MFA 的更多信息，请参阅以下文档：

- AWS Managed Microsoft AD -《AWS Directory Service 管理指南》中的为 AWS Managed Microsoft AD 启用多重身份验证。
- AD Connector -《AWS Directory Service 管理指南》中的为 AD Connector 启用多重身份验证以及多重身份验证 (AD Connector)
- 受信任域 -《AWS Directory Service 管理指南》中的为 AWS Managed Microsoft AD 启用多重身份验证
- Simple AD - 多重身份验证对 Simple AD 不可用。

自 2021 年 4 月 13 日起，在 4.6.0 和 6.0.0 之间的零客户端设备固件版本中，不再支持使用 PCoIP Connection Manager。如果您的零客户端固件版本不是 6.0.0 或更高版本，则可以访问以下网址通过 Desktop Access 订阅来获取最新固件：https://www.teradici.com/desktop-access。

Important

- 在 Teradici PCoIP 管理 Web 接口 (AWI) 或 Teradici PCoIP 管理控制台 (MC) 中，请确保启用了网络时间协议 (NTP)。对于 NTP 主机 DNS 名称，请使用 **`pool.ntp.org`**，并将 NTP 主机端口设置为 123。如果未启用 NTP，PCoIP 零客户端用户可能会收到证书失败错误，例如“提供的证书由于时间戳而无效。”
- 从 PCoIP 代理的 20.10.4 版本开始，Amazon WorkSpaces 默认禁用通过 Windows 注册表进行的 USB 重定向。当您的用户使用 PCoIP 零客户端设备连接到其 WorkSpaces 时，此注册表设置会影响 USB 外围设备的行为。有关更多信息，请参阅USB 打印机和其他 USB 外围设备不适用于 PCoIP 零客户端。

有关设置和连接 PCoIP 零客户端设备的信息，请参阅《Amazon WorkSpaces 用户指南》中的 PCoIP 零客户端。有关经批准的 PCoIP 零客户端设备列表，请参阅 Teradici 网站上的 PCoIP 零客户端。

为 Chromebook 设置 Android

版本 2.4.13 是亚马逊 WorkSpaces Chromebook 客户端应用程序的最终版本。由于谷歌正在逐步停止对Chrome应用程序的支持，因此Chro WorkSpaces mebook客户端应用程序将不会有进一步的更新，也不支持其使用。

对于支持安装安卓应用程序的 Chromeb ook，我们建议改用 WorkSpaces 安卓客户端应用程序。

在 2019 年之前发布的某些 Chromebook 必须启用才能安装安卓应用程序，然后用户才能安装亚马逊 WorkSpaces 安卓客户端应用程序。有关更多信息，请参阅支持 Android 应用的 Chrome 操作系统。

要远程管理启用用户的 Chromebook 以安装 Android 应用程序，请参阅在 Chrome 设备上设置 Android。

启用和配置 Amazon WorkSpaces Web Access

大多数 WorkSpaces 捆绑包都支持 Amazon WorkSpaces Web Access。有关支持网络浏览器访问的列表 WorkSpaces ，请参阅 “哪些 Amazon WorkSpaces 捆绑包支持 Web Access？” 客户端访问、Web Access 和用户体验中的“哪些 Amazon WorkSpaces 捆绑包支持 Web Access？”。

> **Note**
>
> - 所有提供 WSP 的区域都支持使用 W WorkSpaces SP 进行 Windows 和 Ubuntu WorkSpaces 的 Web 访问。适用于 Amazon Linux WorkSpaces 的 WSP 仅在 AWS GovCloud （美国西部）提供。
> - 我们强烈建议将 Web Access 与 WSP 配合使用， WorkSpaces 以获得最佳的直播质量和用户体验。以下是将 Web 访问与 PCo WorkSpaces IP 配合使用时的限制：
>   - 亚太地区（孟买） AWS GovCloud (US) Regions、非洲（开普敦）和以色列（特拉维夫）不支持使用 PCoIP 进行网络访问
>   - 只有 Windows 支持使用 PCoIP 进行网络访问 WorkSpaces，亚马逊 Linux 不支持。WorkSpaces
>   - Web Access 不适用于某些使用 PCoIP 协议 WorkSpaces 的 Windows 10。如果你的 PCoIP WorkSpaces 由 Windows Server 2019 或 2022 提供支持，则 Web Access 不可用。

- 您无法使用 Web 浏览器连接到启用 GPU WorkSpaces 的网络。
- 如果你在 VPN 上使用 macOS 并使用 Firefox 网络浏览器，则网络浏览器将不支持使用 Web Access 直播 PCoIP WorkSpaces 。 WorkSpaces 这是由于 Firefox 在实施 WebRTC 协议时存在限制。

Important

从 2020 年 10 月 1 日起，客户将无法再使用亚马逊 WorkSpaces Web Access 客户端连接到 Windows 7 自定义版 WorkSpaces 或 Windows 7 自带许可证 (BYOL) WorkSpaces。

步骤 1：启用对您的 Web 访问权限 WorkSpaces

您可以在目录级别控制对您的 WorkSpaces Web 访问权限。对于 WorkSpaces 包含要允许用户通过 Web Access 客户端访问的每个目录，请执行以下步骤。

启用对您的 Web 访问权限 WorkSpaces

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择目录。
3. 在目录 ID列下，选择要为其启用 Web 访问功能的目录的目录 ID。
4. 在目录详细信息页面上，向下滚动到其他平台部分，然后选择编辑。
5. 选择 Web Access (Web 访问)。
6. 选择保存。

Note

启用 Web Access 后，请 WorkSpace 重新启动以使更改生效。

步骤 2：为 Web 访问配置对端口的入站和出站访问

Amazon WorkSpaces Web Access 要求某些端口具有入站和出站访问权限。有关更多信息，请参阅 用于 Web Access 的端口。

步骤 3：配置组策略和安全策略设置以允许用户登录

Amazon WorkSpaces 依靠特定的登录屏幕配置来使用户能够成功地从 Web Access 客户端登录。

要使 Web Access 用户能够登录他们的 WorkSpaces，必须配置一个组策略设置和三个安全策略设置。如果这些设置配置不正确，则用户在尝试登录时可能会遇到登录时间过长或黑屏的情况 WorkSpaces。要配置这些设置，请使用以下过程。

你可以使用组策略对象 (GPO) 来应用设置来管理 Windows WorkSpaces 或属于你的 Windows WorkSpaces 目录的用户。我们建议您为 WorkSpaces 计算机对象创建一个组织单位，为 WorkSpaces 用户对象创建一个组织单位。

有关使用 Active Directory 管理工具处理 GPO 的信息，请参阅《AWS Directory Service 管理指南》中的安装 Active Directory 管理工具。

使 WorkSpaces 登录代理能够切换用户

在大多数情况下，当用户尝试登录时 WorkSpace，用户名字段会预先填充该用户的名称。但是，如果管理员与建立了 RDP 连接 WorkSpace 以执行维护任务，则用户名字段将改为使用管理员的姓名填充。

要避免此问题，请禁用 Hide entry points for Fast User Switching (隐藏入口点以快速进行用户切换) 组策略设置。禁用此设置后， WorkSpaces 登录代理可以使用 “切换用户” 按钮在用户名字段中填入正确的名称。

1. 打开组策略管理工具 (gpmc.msc)，在您使用的目录的域或域控制器级别导航并选择一个 GPO。WorkSpaces（ 如果您的域中安装了 WorkSpaces 组策略管理模板，则可以将 WorkSpaces GPO 用于您的 WorkSpaces 计算机帐户。 ）
2. 在主菜单中依次选择操作和编辑。
3. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、系统和登录。
4. 打开 Hide entry points for Fast User Switching (隐藏入口点以快速进行用户切换) 设置。
5. 在 Hide entry points for Fast User Switching (隐藏入口点以快速进行用户切换) 对话框中，选择 Disabled (已禁用)，然后选择 OK (确定)。

隐藏上次登录的用户名

默认情况下，显示上次登录的用户列表，而不是 Switch User (切换用户) 按钮。根据的配置 WorkSpace，列表可能不会显示 “其他用户” 图块。出现这种情况时，如果预先填充的用户名不正确，WorkSpaces 登录代理将无法使用正确的名称填充该字段。

要避免此问题，请启用安全策略设置交互式登录: 不显示上次登录) 或交互式登录: 不显示上次用户名（具体取决于您使用的 Windows 版本）。

1. 打开组策略管理工具 (gpmc.msc)，在您使用的目录的域或域控制器级别导航并选择一个 GPO。WorkSpaces（如果您的域中安装了 WorkSpaces 组策略管理模板，则可以将 WorkSpaces GPO 用于您的 WorkSpaces 计算机帐户。）
2. 在主菜单中依次选择操作和编辑。
3. 在组策略管理编辑器中，选择计算机配置、Windows 设置、安全设置、本地策略和安全选项。
4. 打开以下设置之一：
   - 对于 Windows 7 — 交互式登录：不显示上次登录
   - 对于 Windows 10 — 交互式登录：不显示上次的用户名
5. 在设置的 Properties (属性) 对话框中，选择 Enabled (已启用)，然后选择 OK (确定)。

要求在用户可以登录之前按 CTRL+ALT+DEL

对于 WorkSpaces Web Access，你需要要求用户在登录之前按 CTRL+ALT+DEL。要求用户在登录之前按 CTRL+ALT+DEL 可确保用户在输入密码时使用受信任的路径。

1. 打开组策略管理工具 (gpmc.msc)，在您使用的目录的域或域控制器级别导航并选择一个 GPO。WorkSpaces（如果您的域中安装了 WorkSpaces 组策略管理模板，则可以将 WorkSpaces GPO 用于您的 WorkSpaces 计算机帐户。）
2. 在主菜单中依次选择操作和编辑。
3. 在组策略管理编辑器中，选择计算机配置、Windows 设置、安全设置、本地策略和安全选项。
4. 打开交互式登录: 不需要 CTRL+ALT+DEL 设置。
5. 在本地安全设置选项卡上，选择禁用，然后选择确定。

锁定会话时显示域和用户信息

WorkSpaces 登录代理会查找用户的名字和域。配置此设置后，锁定屏幕将显示用户的全名（如果在 Active Directory 中指定）、用户的域名和用户名。

1. 打开组策略管理工具 (gpmc.msc)，在您使用的目录的域或域控制器级别导航并选择一个 GPO。WorkSpaces（如果您的域中安装了 WorkSpaces 组策略管理模板，则可以将 WorkSpaces GPO 用于您的 WorkSpaces 计算机帐户。）
2. 在主菜单中依次选择操作和编辑。

3. 在组策略管理编辑器中，选择计算机配置、Windows 设置、安全设置、本地策略和安全选项。
4. 打开交互式登录: 当会话被锁定时显示用户信息设置。
5. 在本地安全设置选项卡上，选择用户显示名称、域和用户名，然后选择确定。

应用组策略和安全策略设置更改

组策略和安全策略设置的更改将在下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要在之前的过程中应用组策略和安全策略更改，请执行以下操作之一：

- 重启 WorkSpace （在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
- 从管理命令提示符下，输入 gpupdate /force。

设置 Amazon WorkSpaces 以符合 FedRAMP 授权或 DoD SRG 合规性要求

为了遵守联邦风险与授权管理计划 (FedRAMP) 或国防部 (DoD) 云计算安全要求指南 (SRG)，您必须配置 Amazon WorkSpaces 以在目录级别使用联邦信息处理标准 (FIPS) 端点加密技术。您还必须使用具有 FedRAMP 授权或符合 DoD SRG 的美国 AWS 区域。

FedRAMP 授权级别（中或高）或 DoD SRG 影响级别（2、4 或 5）取决于使用 Amazon WorkSpaces 的美国 AWS 区域。有关适用于每个区域的 FedRAMP 授权级别和 DoD SRG 合规性级别，请参阅合规性计划范围内的 AWS 服务。

> **Note**
>
> 除了使用 FIPS 端点加密外，您还可以加密您的 WorkSpaces。有关更多信息，请参阅已加密 WorkSpaces。

要求

- 您必须在具有 FedRAMP 授权或符合 DoD SRG 的美国 AWS 区域中创建 WorkSpaces。
- 必须将 WorkSpaces 目录配置为使用 FIPS 140-2 验证模式进行端点加密。

> **Note**
>
> 要使用 FIPS 140-2 验证模式设置，WorkSpaces 目录必须是新的，或者目录中的所有现有 WorkSpaces 必须使用 FIPS 140-2 验证模式进行端点加密。否则，您将无法使用此设置，因此您创建的 WorkSpaces 也不符合 FedRAMP 或 DoD 的安全要求。

- 用户必须从以下 WorkSpaces 客户端应用程序之一访问其 WorkSpaces：
  - Windows：2.4.3 或更高版本
  - macOS：2.4.3 或更高版本
  - Linux：3.0.0 或更高版本
  - iOS：2.4.1 或更高版本
  - Android：2.4.1 或更高版本
  - Fire Tablet：2.4.1 或更高版本
  - ChromeOS：2.4.1 或更高版本
  - Web Access

使用 FIPS 端点加密

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择目录。
3. 验证您要在其中创建 FedRAMP 授权和符合 DoD SRG 的 WorkSpaces 的目录没有与之关联的任何现有 WorkSpaces。如果存在与该目录关联的 WorkSpaces，并且尚未启用该目录以使用 FIPS 140-2 验证模式，请终止 WorkSpaces 或创建一个新目录。
4. 选择符合上述条件的目录，然后依次选择 Actions (操作) 和Update Details (更新详细信息)。
5. 在 Update Directory Details (更新目录详细信息) 页面上，选择箭头以展开 Access Control Options (访问控制选项) 部分。
6. 对于 Endpoint Encryption (端点加密)，选择 FIPS 140-2 Validated Mode (FIPS 140-2 验证模式) 而不是 TLS Encryption Mode (Standard) (TLS 加密模式（标准）)。
7. 选择更新并退出。
8. 现在，您可以从此目录创建 FedRAMP 授权且符合 DoD SRG 的 WorkSpaces。要访问这些 WorkSpaces，用户必须使用前面要求部分中列出的 WorkSpaces 客户端应用程序之一。

为你的 Linux 启用 SSH 连接 WorkSpaces

如果您或您的用户想要使用命令行连接到您的 Amazon Linux WorkSpaces ，则可以启用 SSH 连接。您可以启用与目录 WorkSpaces 中所有人的 SSH 连接，也可以启用与目录 WorkSpaces 中个人的 SSH 连接。

要启用 SSH 连接，您可以创建新的安全组或更新现有安全组，然后添加规则以允许入站流量用于此目的。安全组用作相关实例的防火墙，可在实例级别控制入站和出站的数据流。在您创建或更新安全组后，您的用户和其他人可以使用 Putty 或其他终端从其设备连接到您的 Amazon Linux。 WorkSpaces 有关更多信息，请参阅the section called “安全组”。

有关视频教程，请参阅如何 WorkSpaces 使用 SSH 连接到我的 Linux Amazon？ 在 AWS 知识中心上。

内容

通过 SSH 连接亚马逊 Linux 的先决条件 WorkSpaces

- 启用入站 SSH 流量 WorkSpace -要添加允许入站 SSH 流量流向一个或多个 Amazon Linux WorkSpaces 的规则，请确保您拥有需要 SSH 连接的设备的公用或私有 IP 地址 WorkSpaces。例如，您可以指定虚拟私有云 (VPC) 之外的设备的公有 IP 地址，或者指定与您位于同一 VPC 中的其他 EC2 实例的私有 IP 地址 WorkSpace。

  如果您计划 WorkSpace 从本地设备连接到，则可以在互联网浏览器中使用搜索短语 “我的 IP 地址是什么” 或使用以下服务：Check IP。
- 连接到 WorkSpace — 启动从设备到 Amazon Linux 的 SSH 连接需要以下信息 WorkSpace。
  - 您连接到的 Active Directory 域的 NetBIOS 名称。
  - 您的 WorkSpace 用户名。
  - 您要连接的的 WorkSpace 的公用或私有 IP 地址。

私有：如果您的 VPC 连接到公司网络并且您可以访问该网络，则可以指定该网络的私有 IP 地址 WorkSpace。

公共：如果您 WorkSpace 有公有 IP 地址，则可以使用 WorkSpaces 控制台查找公有 IP 地址，如以下过程所述。

要查找 WorkSpace 您要连接的 Amazon Linux 的 IP 地址和您的用户名

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 在列表中 WorkSpaces，选择 WorkSpace 要启用 SSH 连接的。
4. 在 “运行模式” 列中，确认 WorkSpace状态为 “可用”。
5. 单击 WorkSpace 名称左侧的箭头以显示行内摘要，并记下以下信息：
   - WorkSpace 知识产权。这是的私有 IP 地址 WorkSpace。

     需要私有 IP 地址才能获取与关联的 elastic network 接口 WorkSpace。需要网络接口才能检索诸如安全组或与之关联的公有 IP 地址之类的信息 WorkSpace。
   - 用户 WorkSpace 名。这是您为连接而指定的用户名 WorkSpace。
6. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
7. 在导航窗格中，选择网络接口。
8. 在搜索框中，键入您在步骤 5 中记下WorkSpace 的 IP。
9. 选择与 WorkSpaceIP 关联的网络接口。
10. 如果您 WorkSpace 有公有 IP 地址，则该地址将显示在 IPv4 公有 IP 列中。记下该地址（如果适用）。

查找您连接到的 Active Directory 域的 NetBIOS 名称

1. 打开 AWS Directory Service 控制台，网址为 https://console.aws.amazon.com/directoryservicev2/。
2. 在目录列表中，单击该目录的目录 ID 链接 WorkSpace。
3. 在 Directory details (目录详细信息) 部分中，记下 Directory NetBIOS name (目录 NetBIOS 名称)。

启用与目录中所有 Amazon Linux WorkSpaces 的 SSH 连接

要启用与目录 WorkSpaces 中所有 Amazon Linux 的 SSH 连接，请执行以下操作。

使用允许入站 SSH 流量流向目录中所有 Amazon Linux WorkSpaces 的规则创建安全组

1. 打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择安全组。
3. 选择创建安全组。
4. 键入安全组的名称（可选）和描述。
5. 对于 VP C，请选择 WorkSpaces 包含要启用 SSH 连接的 VPC。
6. 在 Inbound (入站) 选项卡上，选择 Add Rule (添加规则)，然后执行以下操作：
   - 对于 Type，选择 SSH。
   - 对于 Protocol (协议)，在您选择 SSH 时会自动指定 TCP。
   - 对于 Port Range (端口范围)，在您选择 SSH 时会自动指定 22。
   - 对于 “源”，指定用户将用于连接的计算机的公有 IP 地址的 CIDR 范围。 WorkSpaces例如，公司网络或家庭网络。
   - 对于 Description (描述)（可选），键入规则的描述。
7. 选择 创建。

亚马逊 Linux 中基于密码的身份验证 2 WorkSpaces

2023 年 11 月 10 日之前 WorkSpaces 推出的亚马逊 Linux 2 默认启用 SSH 密码认证。适用于亚马逊 Linux 2，在 11 月 10 日之后 WorkSpaces 推出。默认情况下禁用 SSH 密码身份验证。

在现有 Amazon Linux 2 WorkSpaces 实例中禁用密码身份验证

1. 启动 WorkSpaces 客户端并登录到您的 WorkSpace。
2. 打开终端窗口（应用程序 > 系统工具 > MATE 终端）。
3. 在终端窗口中，运行以下命令。

```
sudo sed -E -i 's|^#?(PasswordAuthentication)\s.*|\1 no|' /etc/ssh/sshd_config
```

在新创建的 Amazon Linux 2 WorkSpaces 实例中启用密码身份验证

1. 启动 WorkSpaces 客户端并登录到您的 WorkSpace。
2. 打开终端窗口（应用程序 > 系统工具 > MATE 终端）。
3. 在终端窗口中，运行以下命令。

```
sudo sed -E -i 's|^#?(PasswordAuthentication)\s.*|\1 yes|' /etc/ssh/sshd_config
```

与 Ubuntu 不同， WorkSpacesAmazon Linux 2 WorkSpaces 默认不在自定义镜像中保留 SSH 密码身份验证设置。如果您想在 Amazon Linux 2 中默认启用通过自定义映像 WorkSpaces 配置的 SSH 密码身份验证，除了启用密码身份验证外，还必须更改`/etc/cloud/cloud.cfg`文件以删除创建自定义映像`ssh_pwauth`时包含的行。要更改 `/etc/cloud/cloud.cfg` 文件，请运行以下命令：

```
sudo sed -i '/^\s*ssh_pwauth:.*$/d' /etc/cloud/cloud.cfg
```

启用与特定亚马逊 Linux 的 SSH 连接 WorkSpace

要启用与特定 Amazon Linux 的 SSH 连接 WorkSpace，请执行以下操作。

向现有安全组添加规则以允许入站 SSH 流量进入特定 Amazon Linux WorkSpace

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，在 Network & Security (网络与安全性) 下，选择 Network Interfaces (网络接口)。
3. 在搜索栏中，键入要启用 SSH 连接 WorkSpace 的的私有 IP 地址。
4. 在 Security groups (安全组) 列中，单击安全组的链接。
5. 在 Inbound (入站) 选项卡上，选择 Edit (编辑)。
6. 选择 Add Rule (添加规则)，然后执行以下操作：
   - 对于 Type，选择 SSH。
   - 对于 Protocol (协议)，在您选择 SSH 时会自动指定 TCP。
   - 对于 Port Range (端口范围)，在您选择 SSH 时会自动指定 22。
   - 对于 Source (源)，选择 My IP (我的 IP) 或 Custom (自定义)，然后用 CIDR 表示法指定单个 IP 地址或 IP 地址范围。例如，如果您的 IPv4 地址为 `203.0.113.25`，请指定 `203.0.113.25/32`，以使用 CIDR 表示法列出此单个 IPv4 地址。如果您的公司要分配同一范围内的地址，请指定整个范围，例如 `203.0.113.0/24`。

- 对于 Description (描述) (可选) ，键入规则的描述。

7. 选择保存。

WorkSpace 使用 Linux 或 Putty 连接到亚马逊 Linux

在您创建或更新安全组并添加所需规则后，您的用户和其他人可以使用 Linux 或 PuTTY 从其设备连接到您的设备。 WorkSpaces

> **Note**
>
> 在完成以下任一过程之前，请确保您具有：
>
> - 您连接到的 Active Directory 域的 NetBIOS 名称。
> - 您用来连接的用户名 WorkSpace。
> - 您要连接的的 WorkSpace 的公用或私有 IP 地址。
>
> 有关如何获取此信息的说明，请参阅本主题前面的 “通过 SSH 连接到 Amazon Linux 的先决条件 WorkSpaces”。

WorkSpace 使用 Linux 连接到亚马逊 Linux

1. 以管理员身份打开命令提示符并输入以下命令。在 *NetBIOS ##*、*###*和 *WorkSpace IP* 中，输入适用的值。

```
ssh "NetBIOS_NAME\Username"@WorkSpaceIP
```

以下是 SSH 命令的示例，其中：

- *NetBIOS_NAME* 为 anycompany
- *Username* 为 janedoe
- *WorkSpace IP* 是 203.0.113.25

```
ssh "anycompany\janedoe"@203.0.113.25
```

2. 出现提示时，输入与 WorkSpaces 客户端进行身份验证时使用的相同密码（您的 Active Directory 密码）。

WorkSpace 使用 PuTTY 连接亚马逊 Linux

1. 打开 PuTTY。
2. 在 PuTTY Configuration (PuTTY 配置) 对话框中，执行以下操作：

   - 对于 Host Name (or IP address) (主机名（或 IP 地址）)，输入以下命令。将这些值替换为您所连接的 Active Directory 域的 NetBIOS 名称 WorkSpace、用于连接的用户名以及要连接的 IP 地址。 WorkSpace

     ```
     NetBIOS_NAME\Username@WorkSpaceIP
     ```

   - 对于端口，输入 **22**。
   - 对于 Connection type (连接类型)，选择 SSH。

   有关 SSH 命令的示例，请参阅上一过程中的步骤 1。
3. 选择打开。
4. 出现提示时，输入与 WorkSpaces 客户端进行身份验证时使用的相同密码（您的 Active Directory 密码）。

所需的配置和服务组件 WorkSpaces

作为 WorkSpace 管理员，您必须了解有关所需配置和服务组件的以下内容。

- the section called “路由表配置”
- the section called “Windows 组件”
- the section called “Linux 组件”
- the section called “Ubuntu 组件”

必需路由表配置

我们建议您不要修改的操作系统级路由表。 WorkSpace该 WorkSpaces 服务需要此表中的预配置路由来监控系统状态和更新系统组件。如果您的组织需要更改路由表，请在应用任何更改之前联系 Su AWS pport 或您的 AWS 客户团队。

Windows 所需的服务组件

在 Windows 上 WorkSpaces，服务组件安装在以下位置。不要删除、更改、阻止或隔离这些对象。如果这样做， WorkSpace 将无法正常运行。

如果上安装了防病毒软件 WorkSpace，请确保它不会干扰安装在以下位置的服务组件。

- `C:\Program Files\Amazon`
- `C:\Program Files\NICE`
- `C:\Program Files\Teradici`
- `C:\Program Files (x86)\Teradici`
- `C:\ProgramData\Amazon`
- `C:\ProgramData\NICE`
- `C:\ProgramData\Teradici`

32 位 PCoIP 代理

自 2021 年 3 月 29 日起，我们将 PCoIP 代理从 32 位更新为 64 位。对于使用 PCoIP 协议的 Windows WorkSpaces ，这意味着 Teradici 文件的位置已从更改为。`C:\Program Files (x86)\Teradici` `C:\Program Files\Teradici`由于我们在常规维护时段内更新了 PCoIP 代理，因此在过渡期间，有些人使用 32 位代理的时间 WorkSpaces 可能比其他人长。

如果您已根据 32 位代理的完整路径配置了防火墙规则、防病毒软件排除项（在客户端和主机端）、组策略对象 (GPO) 设置或 Microsoft 系统中心配置管理器 (SCCM)、Microsoft 端点配置管理器或类似的配置管理工具的设置，则还必须将 64 位代理的完整路径添加到这些设置中。

如果您要筛选任何 32 位 PCoIP 组件的路径，请务必将路径添加到 64 位版本的组件中。由于 WorkSpaces 可能不会同时更新所有路径，因此请不要将 32 位路径替换为 64 位路径，否则其中一些路径 WorkSpaces 可能无法正常工作。例如，如果您的排除项或通信过滤器基于 `C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_server_win32.exe`，则还必须添加 `C:\Program Files\Teradici\PCoIP Agent\bin\pcoip_server.exe`。同样，如果

您的排除项或通信过滤器基于 C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_agent.exe，则还必须添加 C:\Program Files\Teradici\PCoIP Agent\bin\pcoip_agent.exe。

PCoIP 仲裁服务器服务更改 — 请注意，当更新为使用 64 位代理时，PCoIP 仲裁服务 (C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_arbiter_win32.exe) 将被删除。WorkSpaces

PCoIP 零客户端和 USB 设备 — 从 PCoIP 代理的 20.10.4 版本开始， WorkSpaces 亚马逊默认禁用通过 Windows 注册表进行的 USB 重定向。当您的用户使用 PCoIP 零客户端设备连接到 USB 外围设备时，此注册表设置会影响 USB 外围设备的行为。 WorkSpaces有关更多信息，请参阅 USB 打印机和其他 USB 外围设备不适用于 PCoIP 零客户端。

Linux 所需的服务组件

在 Amazon Linux WorkSpaces 上，服务组件安装在以下位置。不要删除、更改、阻止或隔离这些对象。如果这样做， WorkSpace将无法正常运行。

> **Note**
>
> 对其他文件进行更改/etc/pcoip-agent/pcoip-agent.conf可能会 WorkSpaces 导致您停止工作，并且可能需要您重新构建它们。有关修改 /etc/pcoip-agent/pcoip-agent.conf 的信息，请参阅管理你的亚马逊 Linux WorkSpaces。

- /etc/dhcp/dhclient.conf
- /etc/logrotate.d/pcoip-agent
- /etc/logrotate.d/pcoip-server
- /etc/os-release
- /etc/pam.d/pcoip
- /etc/pam.d/pcoip-session
- /etc/pcoip-agent
- /etc/profile.d/system-restart-check.sh
- /etc/X11/default-display-manager
- /etc/yum/pluginconf.d/halt_os_update_check.conf
- /etc/systemd/system/euc-analytic-agent.service

- /lib/systemd/system/pcoip.service
- /lib/systemd/system/pcoip-agent.service
- /lib64/security/pam_self.so
- /usr/bin/pcoip-fne-view-license
- /usr/bin/pcoip-list-licenses
- /usr/bin/pcoip-validate-license
- /usr/bin/euc-analytics-agent
- /usr/lib/firewalld/services/pcoip-agent.xml
- /usr/lib/modules-load.d/usb-vhci.conf
- /usr/lib/pcoip-agent
- /usr/lib/skylight
- /usr/lib/systemd/system/pcoip.service
- /usr/lib/systemd/system/pcoip.service.d/
- /usr/lib/systemd/system/skylight-agent.service
- /usr/lib/tmpfiles.d/pcoip-agent.conf
- /usr/lib/yum-plugins/halt_os_update_check.py
- /usr/sbin/pcoip-agent
- /usr/sbin/pcoip-register-host
- /usr/sbin/pcoip-support-bundler
- /usr/share/doc/pcoip-agent
- /usr/share/pcoip-agent
- /usr/share/selinux/packages/pcoip-agent.pp
- /usr/share/X11
- /var/crash/pcoip-agent
- /var/lib/pcoip-agent
- /var/lib/skylight
- /var/log/pcoip-agent
- /var/log/skylight
- /var/logs/wsp
- /var/log/eucanalytics

Ubuntu 所需的服务组件

在 Ubuntu 上 WorkSpaces，服务组件安装在以下位置。不要删除、更改、阻止或隔离这些对象。如果这样做， WorkSpace将无法正常运行。

- /etc/X11/default-display-manager
- /etc/X11/xorg.conf
- /etc/dcv
- /etc/default/grub.d/zz-hibernation.cfg
- /etc/netplan
- /etc/os-release
- /etc/pam.d/dcv
- /etc/pam.d/dcv-graphical-sso
- /etc/sssd/sssd.conf
- /etc/wsp
- /etc/systemd/system/euc-analytic-agent.service
- /lib64/security/pam_self.so
- /usr/lib/skylight
- /usr/lib/systemd/system/dcvserver.service
- /usr/lib/systemd/system/dcvsessionlauncher.service
- /usr/lib/systemd/system/skylight-agent.service
- /usr/lib/systemd/system/wspdcvhostadapter.service
- /usr/lib/systemd/system/xdcv-console-update.service
- /usr/lib/systemd/system/xdcv-console.path
- /usr/lib/systemd/system/xdcv-console.service
- /usr/share/X11
- /usr/bin/euc-analytics-agent
- /var/lib/skylight
- /var/log/skylight
- /var/log/eucanalytics

管理 WorkSpaces 目录

WorkSpaces 使用目录来存储和管理 WorkSpace 及用户的相关信息。可以使用以下选项之一：

- AD Connector - 使用现有本地部署 Microsoft Active Directory。用户可以使用其本地部署凭证登录 WorkSpace 并从其 WorkSpace 访问本地部署资源。
- AWS Managed Microsoft AD - 创建在 AWS 上托管的 Microsoft Active Directory。
- Simple AD - 创建与 Microsoft Active Directory 兼容的目录，该目录由 Samba 4 提供支持，并在 AWS 上托管。
- Cross trust - 在您的 AWS Managed Microsoft AD 目录与本地域之间创建信任关系。

有关演示如何设置这些目录和启动 WorkSpace 的教程，请参阅使用 WorkSpaces 启动虚拟桌面。

> **Tip**
>
> 要详细了解各种部署场景的目录和虚拟私有云 (VPC) 设计注意事项，请参阅部署 Amazon WorkSpaces 的最佳实践。

创建目录后，您将使用工具 (如 Active Directory 管理工具) 执行大部分目录管理任务。您可以使用 WorkSpaces 控制台执行一些目录管理任务，使用策略组执行其他任务。有关管理用户和组的更多信息，请参阅管理 WorkSpace 用户和为 WorkSpaces 设置 Active Directory 管理工具。

> **Note**
>
> - Amazon WorkSpaces 目前不支持与共享目录一起使用。
> - 如果您将 AWS Managed Microsoft AD 目录配置为多区域复制，则只能注册主区域中的目录以便在 Amazon WorkSpaces 中使用。尝试在复制区域中注册该目录以用于 Amazon WorkSpaces 将失败。复制区域内的 Amazon WorkSpaces 不支持使用 AWS Managed Microsoft AD 进行多区域复制。
> - Simple AD 和 AD Connector 供您免费使用，可用于 WorkSpaces。如果连续 30 天没有一起使用 WorkSpaces 与您的 Simple AD 或 AD Connector 目录，则系统将自动取消注册该目录，无法再将其用于 Amazon WorkSpaces，而且将根据 AWS Directory Service 定价条款向您收取该目录的费用。

要删除空目录，请参阅删除 WorkSpaces 的目录。如果您删除了 Simple AD 或 AD Connector 目录，则当您想重新开始使用 WorkSpaces 时，可以随时创建一个新的目录。

目录

向 WorkSpaces 注册目录

要允许 WorkSpaces 使用现有 AWS Directory Service 目录，必须向 WorkSpaces 注册该目录。注册一个目录后，即可在该目录中启动 WorkSpace。

要求

要注册要在 WorkSpaces 中使用的目录，必须满足以下要求：

- 如果您使用的是 AWS Managed Microsoft AD 或 Simple AD，则您的目录可以位于专用私有子网中，前提是该目录可以访问 WorkSpaces 所在的 VPC。

有关目录和 VPC 设计的更多信息，请参阅部署 Amazon WorkSpaces 的最佳实践白皮书。

> **Note**
>
> Simple AD 和 AD Connector 供您免费使用，可用于 WorkSpaces。如果连续 30 天没有一起使用 WorkSpaces 与您的 Simple AD 或 AD Connector 目录，则系统将自动取消注册该目录，无法再将其用于 Amazon WorkSpaces，而且将根据 AWS Directory Service 定价条款向您收取该目录的费用。
>
> 要删除空目录，请参阅删除 WorkSpaces 的目录。如果您删除了 Simple AD 或 AD Connector 目录，则当您想重新开始使用 WorkSpaces 时，可以随时创建一个新的目录。

注册目录

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择目录。
3. 选择目录。
4. 选择 Actions、Register。

> **Note**
>
> - Amazon WorkSpaces 目前不支持与共享目录一起使用。
> - 如果将 AWS Managed Microsoft AD 目录配置为多区域复制，则只能注册主区域中的目录以便在 Amazon WorkSpaces 中使用。尝试在复制区域中注册该目录以用于 Amazon WorkSpaces 将失败。复制区域内的 Amazon WorkSpaces 不支持使用 AWS Managed Microsoft AD 进行多区域复制。

5. 选择来自不同可用区的 VPC 的两个子网。这些子网将用于启动您的 WorkSpaces。有关更多信息，请参阅Amazon 的可用区域 WorkSpaces。

> **Note**
>
> 如果您不知道要选择哪些子网，请选择无首选项。

6. 对于启用自助服务权限，选择是以使用户能够重建其 WorkSpaces、更改卷大小、计算类型和运行模式。启用操作可能会影响您为 Amazon WorkSpaces 支付的费用。否则，请选择否。
7. 对于启用 Amazon WorkDocs，要注册目录以便用于 Amazon WorkDocs，请选择是，否则，请选择否。

> **Note**
>
> 仅当区域中提供 Amazon WorkDocs 且您不使用 AWS Managed Microsoft AD 时，才显示此选项。如果您使用的是 AWS Managed Microsoft AD，请完成注册目录，然后查看为 AWS Managed Microsoft AD 启用 Amazon WorkDocs。

8. 选择 Register。Registered 最初的值是 `REGISTERING`。注册完成后，该值为 `Yes`。

当不再将目录用于 WorkSpaces 时，可以取消注册该目录。请注意，必须先取消注册目录，然后才能删除它。如果要取消注册并删除目录，则必须首先查找并删除注册到该目录的所有应用程序和服务。有关更多信息，请参阅《AWS Directory Service 管理指南》中的删除您的目录。

取消注册目录

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择目录。
3. 选择目录。
4. 选择 Actions、Deregister。
5. 当系统提示您确认时，选择 Deregister (取消注册)。取消注册完成后，Registered 的值为 No。

更新您的目录详细信息 WorkSpaces

您可以使用 WorkSpaces 控制台完成以下目录管理任务。

任务

- 选择组织单位
- 配置自动公有 IP 地址
- 控制设备访问
- 管理本地管理员权限
- 更新 AD Connector 账户 (AD Connector)
- 多重身份验证 (AD Connector)

选择组织单位

WorkSpace 计算机帐户位于 WorkSpaces 目录的默认组织单位 (OU) 中。最初，计算机账户放在您的目录的“计算机”OU 中，或 AD Connector 连接的目录中。您可以从您的目录或所连接的目录中选择一个不同的 OU，或在单独的目标域中指定一个 OU。请注意，在每个目录中只能选择一个 OU。

选择新的 OU 后，所有 WorkSpaces 创建或重建的计算机帐户都将放置在新选择的 OU 中。

选择组织单位

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择目录。

3. 选择您的目录。
4. 在 “目标域和组织单位” 下，选择 “编辑”。
5. 要查找 OU，可以在 “目标和组织单位” 下开始键入 OU 的全部或部分，然后选择要使用的 OU。
6. （可选）选择 OU 的区分名称，使用自定义 OU 覆盖选定的 OU。
7. 选择保存。
8. （可选）重建现有的 OU WorkSpaces 以更新 OU。有关更多信息，请参见 重建一个 WorkSpace。

配置自动公有 IP 地址

启用自动分配公有 IP 地址后，您启动 WorkSpace 的每个地址都将从亚马逊提供的公有地址池中分配一个公有 IP 地址。公有子网 WorkSpace 中的 A 如果有公有 IP 地址，则可以通过互联网网关访问互联网。 WorkSpaces 在您启用自动分配之前已经存在的公用地址在您重建之前不会收到公用地址。

请注意，如果您位于私有子网中，并且为虚拟私 WorkSpaces 有云 (VPC) 配置了 NAT 网关，或者您位于公有子网中并为其分配了弹性 IP 地址，则无需启用自动分配公 WorkSpaces 有地址。有关更多信息，请参见 为以下项配置 VPC WorkSpaces。

> **Warning**
>
> 如果您将自己拥有的弹性 IP 地址关联到 WorkSpace，然后又将该弹性 IP 地址与解除关联 WorkSpace，则该地址将 WorkSpace 丢失其公有 IP 地址，并且不会自动从亚马逊提供的池中获取新的 IP 地址。要将亚马逊提供的资源池中的新公有 IP 地址与相关联 WorkSpace，您必须重新构建。 WorkSpace如果您不想重建 WorkSpace，则必须将您拥有的另一个弹性 IP 地址与关联起来 WorkSpace。

配置弹性 IP 地址

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择目录。
3. 为你选择目录 WorkSpaces。
4. 选择 Actions、Update Details。
5. 展开 Access to Internet，选择 Enable 或 Disable。
6. 选择更新。

控制设备访问

您可以指定有权访问的设备类型 WorkSpaces。此外，您可以限制对可信设备（也称为受管设备）的访问。 WorkSpaces

要控制设备的访问权限 WorkSpaces

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择目录。
3. 选择您的目录。
4. 在 “访问控制选项” 下，选择 “编辑”。
5. 在 “可信设备” 下，选择 “全部允许”、“可信设备” 或 “全部拒绝”，指定哪些设备类型可以访问 WorkSpaces 。有关更多信息，请参见 限制对可信设备的 WorkSpaces 访问。
6. 选择 Save（保存）。

管理本地管理员权限

您可以指定用户是否是其上的本地管理员 WorkSpaces，这使他们能够在其上安装应用程序和修改设置 WorkSpaces。默认情况下，用户为本地管理员。如果您修改此设置，则更改将应用于您创建 WorkSpaces 的所有新设置以及您重建的所有 WorkSpaces 新设置。

修改本地管理员权限

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择目录。
3. 选择您的目录。
4. 在 “本地管理员设置” 下，选择 “编辑”。
5. 要确保用户是本地管理员，请选择 “启用本地管理员设置”。
6. 选择保存。

更新 AD Connector 账户 (AD Connector)

您可以更新用于读取用户和群组以及将 WorkSpaces 计算机帐户加入您的 AD Connector 目录的 AD Connector 帐户。

更新 AD Connector 账户

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择目录。
3. 选择您的目录，然后选择 “查看详细信息”。
4. 在 AD 连接器帐户下，选择编辑。
5. 输入新账户的登录凭证。
6. 选择保存。

多重身份验证 (AD Connector)

您可以针对 AD Connector 目录启用多重身份验证。有关通过 AWS Directory Service 使用多重身份验证的更多信息，请参阅针对 AD Connector 启用多重身份验证和 AD Connector 先决条件。

> **Note**
>
> - 您的 RADIUS 服务器可以由 AWS 进行托管，也可以位于本地。
> - 用户名必须在 Active Directory 和 RADIUS 服务器之间匹配。

启用多重身份验证

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择目录。
3. 选择您的目录，然后选择 Actions、Update Details。
4. 展开 Multi-Factor Authentication，然后选择 Enable Multi-Factor Authentication。
5. 对于 RADIUS server IP address(es)，键入您的 RADIUS 服务器端点的 IP 地址，以逗号隔开，或键入您的 RADIUS 服务器负载均衡器的 IP 地址。
6. 对于 Port，键入 RADIUS 服务器用来通信的端口。您的本地网络必须允许默认 RADIUS 服务器端口 (1812) 上来自 AD Connector 的入站流量。
7. 对于 Shared secret code 和 Confirm shared secret code，键入您的 RADIUS 服务器的共享密码。
8. 对于 Protocol，为您的 RADIUS 服务器选择协议。

9. 对于 Server timeout，键入等待 RADIUS 服务器作出响应的时间 (以秒为单位)。该值必须在 1 到 50 之间。
10. 对于 Max retries，键入尝试与 RADIUS 服务器通信的最多次数。该值必须在 0 到 10 之间。
11. 选择更新并退出。

当 RADIUS Status 为 Enabled 时，多重验证可用。在设置多因素身份验证时，用户无法登录自己的。WorkSpaces

更新 Amazon WorkSpaces 的 DNS 服务器

如果在启动 WorkSpaces 后需要更新 Active Directory 的 DNS 服务器 IP 地址，则还必须使用新的 DNS 服务器设置更新 WorkSpaces。

您可以通过以下方式使用新的 DNS 设置更新 WorkSpaces：

- 在更新 Active Directory 的 DNS 设置之前，请先更新 WorkSpaces 上的 DNS 设置。
- 更新 Active Directory 的 DNS 设置后，请重建 WorkSpaces。

建议先更新 WorkSpaces 上的 DNS 设置，然后再更新 Active Directory 中的 DNS 设置（如以下过程的步骤 1 中所述）。

如果要改为重建 WorkSpaces，请更新 Active Directory 中的一个 DNS 服务器 IP 地址（步骤 2），然后按照重建一个 WorkSpace中的步骤重建 WorkSpaces。重建 WorkSpaces 后，按照步骤 3 中的说明测试 DNS 服务器更新。完成该步骤后，在 Active Directory 中更新第二台 DNS 服务器的 IP 地址，然后再次重建 WorkSpaces。请务必按照步骤 3 中的说明测试您的第二次 DNS 服务器更新。如最佳实践部分所述，建议逐一更新您的 DNS 服务器 IP 地址。

最佳实践

在您更新 DNS 服务器设置时，建议遵循以下最佳实践：

- 为避免断开连接和无法访问域资源，强烈建议在非高峰时段或计划维护期间执行 DNS 服务器更新。
- 请勿在更改 DNS 服务器设置之前和之后的 15 分钟内启动任何新的 WorkSpaces。
- 更新 DNS 服务器设置时，请一次更改一个 DNS 服务器 IP 地址。在更新第二个 IP 地址之前，请验证第一次更新是否正确。建议执行以下步骤（步骤 1、步骤 2 和步骤 3）两次，一次更新一个 IP 地址。

步骤 1：在您的 WorkSpaces 上更新 DNS 服务器设置

在以下过程中，当前和新的 DNS 服务器 IP 地址的参考值如下所示：

- 当前 DNS IP 地址：*OldIP1*，*OldIP2*
- 新的 DNS IP 地址：*NewIP1*，*NewIP2*

> **Note**
>
> 如果这是您第二次执行此过程，请使用 *OldIP2* 替换 *OldIP1*，使用 *NewIP2* 替换 *NewIP1*。

更新 Windows WorkSpaces 的 DNS 服务器设置

如果您有多个 WorkSpaces，则可以通过在 WorkSpaces 的 Active Directory OU 上应用组策略对象 (GPO) 来将以下注册表更新部署到 WorkSpaces。有关使用 GPO 的更多信息，请参阅管理你的 Windows WorkSpaces。

您可以使用注册表编辑器或使用 Windows PowerShell 进行这些更新。此部分介绍了这些过程。

使用注册表编辑器更新 DNS 注册表设置

1. 在您的 Windows WorkSpace 上，打开 Windows 搜索框并输入 **`registry editor`** 以打开注册表编辑器 (regedit.exe)。
2. 当询问“你要允许此应用对你的设备进行更改吗?”时，选择是。
3. 在注册表编辑器中，导航到以下注册表项：

   HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\SkyLight
4. 打开 DomainJoinDns 注册表项。使用 *NewIP1* 更新 *OldIP1*，然后选择确定。
5. 关闭注册表编辑器。
6. 重启 WorkSpace，或者重新启动服务 SkyLightWorkspaceConfigService。

   > **Note**
   >
   > 重新启动服务 SkyLightWorkspaceConfigService 后，网络适配器最多可能需要 1 分钟才能反映此更改。

7. 继续执行步骤 2，在 Active Directory 中更新 DNS 服务器设置，将 *OldIP1* 替换为 *NewIP1*。

使用 PowerShell 更新 DNS 注册表设置

以下过程使用 PowerShell 命令更新注册表并重新启动服务 SkyLightWorkspaceConfigService。

1. 在您的 Windows WorkSpace 中，打开 Windows 搜索框并输入 **powershell**。选择以管理员身份运行。
2. 当询问“你要允许此应用对你的设备进行更改吗?”时，选择是。
3. 在 PowerShell 窗口中，运行以下命令以检索当前的 DNS 服务器 IP 地址。

```
Get-ItemProperty -Path HKLM:\SOFTWARE\Amazon\SkyLight -Name DomainJoinDNS
```

您应该收到如下所示的输出。

```
DomainJoinDns : OldIP1,OldIP2
PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE
\Amazon\SkyLight
PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE
\Amazon
PSChildName   : SkyLight
PSDrive       : HKLM
PSProvider    : Microsoft.PowerShell.Core\Registry
```

4. 在 PowerShell 窗口中，运行以下命令，将 *OldIP1* 更改为 *NewIP1*。请务必暂时保留 *OldIP2* 原样。

```
Set-ItemProperty -Path HKLM:\SOFTWARE\Amazon\SkyLight -Name DomainJoinDNS -Value
 "NewIP1,OldIP2"
```

5. 运行以下命令以重新启动 SkyLightWorkspaceConfigService 服务。

```
restart-service -Name SkyLightWorkspaceConfigService
```

> **Note**
>
> 重新启动服务 SkyLightWorkspaceConfigService 后，网络适配器最多可能需要 1 分钟才能反映此更改。

6. 继续执行步骤 2，在 Active Directory 中更新 DNS 服务器设置，将 *OldIP1* 替换为 *NewIP1*。

更新 Linux WorkSpaces 的 DNS 服务器设置

如果您有 1 个以上的 Linux WorkSpace，建议您使用配置管理解决方案来分发和实施策略。例如，您可以使用 AWS OpsWorks for Chef Automate、AWS OpsWorks for Puppet Enterprise 或 Ansible。

更新 Linux WorkSpace 上的 DNS 服务器设置

1. 在 Linux WorkSpace 上，打开终端窗口（应用程序 > 系统工具 > MATE 终端）。
2. 使用以下 Linux 命令编辑 `/etc/dhcp/dhclient.conf` 文件。您必须具有根用户权限才能编辑此文件。要成为根用户，可以使用 `sudo -i` 命令，也可以运行所有命令，如 `sudo` 所示。

   ```
   sudo vi /etc/dhcp/dhclient.conf
   ```

   在 `/etc/dhcp/dhclient.conf` 文件中，您将看到以下 `prepend` 命令，其中 *OldIP1* 和 *OldIP2* 是 DNS 服务器的 IP 地址。

   ```
   prepend domain-name-servers OldIP1, OldIP2; # skylight
   ```

3. 将 *OldIP1* 替换为 *OldIP2*，并且暂时保持 *NewIP1* 原样。
4. 将更改保存到 `/etc/dhcp/dhclient.conf`。
5. 重启 WorkSpace。
6. 继续执行步骤 2，在 Active Directory 中更新 DNS 服务器设置，将 *OldIP1* 替换为 *NewIP1*。

步骤 2：更新 Active Directory 的 DNS 服务器设置

在此步骤中，您将更新 Active Directory 的 DNS 服务器设置。如最佳实践部分所述，建议逐一更新您的 DNS 服务器 IP 地址。

要更新 Active Directory 的 DNS 服务器设置，请参阅《AWS Directory Service 管理指南》中的以下文档：

- AD Connector：更新 AD 连接器的 DNS 地址
- AWS Managed Microsoft AD：为本地域配置 DNS 条件转发服务器
- Simple AD：配置 DNS

更新 DNS 服务器设置后，继续执行步骤 3。

步骤 3：测试更新的 DNS 服务器设置

完成步骤 1 和步骤 2 后，使用以下步骤验证更新后的 DNS 服务器设置是否按预期运行。

在以下过程中，当前和新的 DNS 服务器 IP 地址的参考值如下所示：

- 当前 DNS IP 地址：*OldIP1*，*OldIP2*
- 新的 DNS IP 地址：*NewIP1*，*NewIP2*

> **Note**
>
> 如果这是您第二次执行此过程，请使用 *OldIP2* 替换 *OldIP1*，使用 *NewIP2* 替换 *NewIP1*。

测试更新后的 Windows WorkSpaces 的 DNS 服务器设置

1. 关闭 *OldIP1* DNS 服务器。
2. 登录 Windows WorkSpace。
3. 在 Windows 开始菜单上，选择 Windows 系统，然后选择命令提示符。
4. 运行以下命令，其中 *AD_Name* 是您的 Active Directory 的名称（例如，`corp.example.com`）。

   ```
   nslookup AD_Name
   ```

   `nslookup` 命令应返回以下输出。（如果这是您第二次执行此过程，您应看到 *NewIP2* 取代了 *OldIP2*。）

   ```
   Server:  Full_AD_Name
   Address:  NewIP1

   Name:    AD_Name
   Addresses:  OldIP2
             NewIP1
   ```

5. 如果输出与预期不符，或者收到任何错误，请重复步骤 1。
6. 等待一个小时，确认没有报告任何用户问题。验证 *NewIP1* 是否正在获取 DNS 查询并做出答复。

7. 确认第一台 DNS 服务器运行正常后，重复步骤 1 更新第二台 DNS 服务器，这次将 *OldIP2* 替换为 *NewIP2*。然后重复步骤 2 和步骤 3。

测试更新后的 Linux WorkSpaces 的 DNS 服务器设置

1. 关闭 *OldIP1* DNS 服务器。
2. 登录到 Linux WorkSpace。
3. 在 Linux WorkSpace 上，打开终端窗口（应用程序 > 系统工具 > MATE 终端）。
4. DHCP 响应中返回的 DNS 服务器 IP 地址将写入 WorkSpace 上的本地 `/etc/resolv.conf` 文件中。运行以下命令以查看 `/etc/resolv.conf` 文件的内容。

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

您应当看到如下输出。（如果这是您第二次执行此过程，您应看到 *NewIP2* 取代了 *OldIP2*。）

```
; This file is generated by Amazon WorkSpaces
; Modifying it can make your WorkSpace inaccessible until reboot
options timeout:2 attempts:5
; generated by /usr/sbin/dhclient-script
search region.compute.internal
nameserver NewIP1
nameserver OldIP2
nameserver WorkSpaceIP
```

> **Note**
>
> 如果您对 `/etc/resolv.conf` 文件进行手动修改，则当 WorkSpace 重新启动时，这些更改将丢失。

5. 如果输出与预期不符，或者收到任何错误，请重复步骤 1。
6. 实际的 DNS 服务器 IP 地址存储在 `/etc/dhcp/dhclient.conf` 文件中。要查看此文件的内容，请运行以下命令。

```
sudo cat /etc/dhcp/dhclient.conf
```

您应当看到如下输出。（如果这是您第二次执行此过程，您应看到 *NewIP2* 取代了 *OldIP2*。）

```
# This file is generated by Amazon WorkSpaces
# Modifying it can make your WorkSpace inaccessible until rebuild
prepend domain-name-servers NewIP1, OldIP2; # skylight
```

7. 等待一个小时，确认没有报告任何用户问题。验证 *NewIP1* 是否正在获取 DNS 查询并做出答复。
8. 确认第一台 DNS 服务器运行正常后，重复步骤 1 更新第二台 DNS 服务器，这次将 *OldIP2* 替换为 *NewIP2*。然后重复步骤 2 和步骤 3。

删除 WorkSpaces 的目录

如果 WorkSpaces 目录不再被其他 WorkSpaces 或其他应用程序（如 Amazon WorkDocs、Amazon WorkMail 或 Amazon Chime）使用，则您可将其删除。请注意，必须先取消注册目录，然后才能删除它。

> **Note**
>
> Simple AD 和 AD Connector 供您免费使用，可用于 WorkSpaces。如果连续 30 天没有一起使用 WorkSpaces 与您的 Simple AD 或 AD Connector 目录，则系统将自动取消注册该目录，无法再将其用于 Amazon WorkSpaces，而且将根据 AWS Directory Service 定价条款向您收取该目录的费用。
>
> 如果您删除了 Simple AD 或 AD Connector 目录，则当您想重新开始使用 WorkSpaces 时，可以随时创建一个新的目录。

删除目录时会发生什么

删除 Simple AD 或 AWS Directory Service for Microsoft Active Directory 目录时，所有目录数据和快照都会删除，并且无法恢复。删除目录之后，加入到目录的所有 Amazon EC2 实例都保持不变。但是，不能使用目录凭证登录这些实例。需要使用实例的本地 AWS 账户登录这些实例。

删除 AD Connector 目录时，本地目录保持不变。加入到目录的任何 Amazon EC2 实例也保持不变，并保持加入本地目录。仍可以使用目录凭证登录这些实例。

要删除目录

1. 删除目录中的所有 WorkSpace。有关更多信息，请参阅删除 WorkSpace。
2. 查找并删除注册到目录的所有应用程序和服务。有关更多信息，请参阅《AWS Directory Service 管理指南》中的删除您的目录。

3. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。
4. 在导航窗格中，选择目录。
5. 选择目录，然后选择 Actions、Deregister。
6. 当系统提示您确认时，选择 Deregister (取消注册)。
7. 再次选择目录，然后选择 Actions 和 Delete。
8. 当系统提示进行确认时，选择 Delete（删除）。

> **Note**
>
> 删除应用程序分配有时可能需要超出预期的时间。如果您收到以下错误消息，请确保已删除所有应用程序分配，等待 30 到 60 分钟，然后再次尝试删除该目录：
>
> ```
> An Error Has Occurred
> Cannot delete the directory because it still has authorized applications.
> Additional directory details can be viewed at the Directory Service console.
> ```

9. (可选) 删除虚拟私有云(VPC) 中用于您的目录的所有资源后，可以删除 VPC 并释放用于 NAT 网关的弹性 IP 地址。有关更多信息，请参阅《Amazon VPC 用户指南》中的删除您的 VPC 和使用弹性 IP 地址。
10. (可选) 要删除您不再使用的任何自定义捆绑包和映像，请参阅 删除自定义 WorkSpaces 捆绑包或图片。

为 AWS Managed Microsoft AD 启用 Amazon WorkDocs

如果您在 Amazon WorkSpaces 中使用 AWS Managed Microsoft AD，则可以通过 Amazon WorkDocs 控制台或 AWS Directory Service 控制台，为您的目录启用 Amazon WorkDocs。

> **Note**
>
> Amazon WorkDocs 并非在所有提供 Amazon WorkSpaces 的 AWS 区域都可用。有关更多信息，请参阅 Amazon WorkDocs 定价。

通过 Amazon WorkDocs 控制台启用 WorkDocs

1. 打开 Amazon WorkDocs 控制台，网址为：https://console.aws.amazon.com/zocalo/。

2. 选择 Create a New WorkDocs Site (创建新的 WorkDocs 站点)。
3. 在 Standard Setup (标准设置) 中，选择 Launch (启动)。
4. 选择目录并创建您的站点名称。
5. 指定将管理 WorkDocs 站点的用户。您可以使用管理员或在目录中创建的任何用户。

有关更多信息，请参阅《Amazon WorkDocs 管理指南》中的 AWS Managed Microsoft AD 入门。

通过 AWS Directory Service 控制台启用 WorkDocs

1. 打开 AWS Directory Service 控制台，网址为：https://console.aws.amazon.com/directoryservicev2/。
2. 在导航窗格中，选择目录。
3. 在 Directories (目录) 页面上，选择您的目录。
4. 在 Directory details (目录详细信息) 页面上，选择 Application management (应用程序管理) 选项卡。
5. 在 Application access URL (应用程序访问 URL) 部分中，如果尚未向目录分配访问 URL，则会显示 Create (创建) 按钮。输入目录别名，然后选择 Create (创建)。有关更多信息，请参阅《AWS Directory Service 管理指南》中的创建访问 URL。
6. 在 Application access URL (应用程序访问 URL) 部分中，选择 Enable (启用) 以便为 Amazon WorkDocs 启用单点登录。有关更多信息，请参阅《AWS Directory Service 管理指南》中的单点登录。

为 WorkSpaces 设置 Active Directory 管理工具

您将使用目录管理工具 (如 Active Directory 管理工具) 为您的 WorkSpace 目录执行大部分管理任务。不过，您将使用 WorkSpaces 控制台来执行一些与目录相关的任务。有关更多信息，请参阅管理 WorkSpaces 目录。

如果创建拥有 AWS Managed Microsoft AD 或 Simple AD 的目录，且其中包含五个或更多个 WorkSpaces，建议您在 Amazon EC2 实例上进行集中式管理。尽管您可以在 WorkSpace 上安装目录管理工具，但使用 Amazon EC2 实例是一种更可靠的解决方案。

设置 Active Directory 管理工具

1. 启动一个 Amazon EC2 Windows 实例，然后使用以下一个选项，将其加入您的 WorkSpaces 目录：

- 如果您还没有现有 Amazon EC2 Windows 实例，则可以在启动实例时将该实例加入您的目录域。有关更多信息，请参阅《AWS Directory Service 管理指南》中的无缝加入 Windows EC2 实例。
- 如果您已经有一个现有 Amazon EC2 Windows 实例，则可以手动将其加入您的目录。有关更多信息，请参阅《AWS Directory Service 管理指南》中的手动添加 Windows 实例。

2. 在 Amazon EC2 Windows 实例上安装 Active Directory 管理工具。有关更多信息，请参阅《AWS Directory Service 管理指南》中的安装 Active Directory 管理工具。

   > **Note**
   >
   > 安装 Active Directory 管理工具时，请务必同时选择组策略管理来安装组策略管理编辑器 (gpmc.msc) 工具。

   功能安装完成后，Windows 管理工具下的 Windows 开始菜单上将提供 Active Directory 工具。

3. 按照如下步骤以目录管理员身份运行工具：

   a. 在 Windows 开始菜单上，打开 Windows 管理工具。

   b. 按住 Shift 键，右键单击您要使用的工具快捷方式，然后选择以其他用户身份运行。

   c. 输入管理员登录凭证。对于 Simple AD，用户名为 **`Administrator`**，对于 AWS Managed Microsoft AD，管理员为 **`Admin`**。

现在，您可以使用熟悉的 Active Directory 工具执行目录管理任务。例如，您可以使用 Active Directory 用户和计算机工具添加用户、删除用户、将用户提升为目录管理员或重置用户密码。请注意，您必须以有权管理目录中用户的用户身份登录您的 Windows 实例。

将用户提升为目录管理员

> **Note**
>
> 此过程仅适用于使用 Simple AD 创建的目录，而不适用于 AWS 托管 AD。有关使用 AWS 托管 AD 创建的目录，请参阅《AWS Directory Service 管理指南》中的在 AWS Managed Microsoft AD 中管理用户和组。

1. 打开“Active Directory 用户和计算机”工具。

2. 导航到您的域下的用户文件夹并选择要提升的用户。
3. 选择操作、属性。
4. 在 ***username*** 属性对话框中，选择隶属于。
5. 将用户添加到下列组并选择确定。

   - Administrators
   - Domain Admins
   - Enterprise Admins
   - Group Policy Creator Owners
   - Schema Admins

添加或删除用户

您只能在启动 WorkSpace 的过程中从 Amazon WorkSpaces 控制台创建新用户，并且无法通过 Amazon WorkSpaces 控制台删除用户。大多数用户管理任务（包括管理用户组）都必须通过您的目录执行。

> **Important**
>
> 在删除用户之前，必须先删除分配给该用户的 WorkSpace。有关更多信息，请参阅删除 WorkSpace。

用于管理用户和组的过程取决于您使用的目录类型。

- 如果您使用的是 AWS Managed Microsoft AD，请参阅《AWS Directory Service 管理指南》中的在 AWS Managed Microsoft AD 中管理用户和组。
- 如果您使用的是 Simple AD，请参阅《AWS Directory Service 管理指南》中的在 Simple AD 中管理用户和组。
- 如果通过 AD Connector 或信任关系使用 Microsoft Active Directory，则可以使用 Active Directory 模块来管理用户和组。

重置用户密码

在为现有用户重置密码时，不要设置 User must change password at next logon。否则，用户无法连接到其 WorkSpace。相反，应为每个用户分配一个安全的临时密码，然后要求他们在下次登录时从 WorkSpace 内手动更改其密码。

> **Note**
>
> 如果您使用的是 AD Connector，或者您的用户位于 AWS GovCloud（美国西部）区域，则您的用户将无法重置自己的密码。（WorkSpaces 客户端应用程序登录屏幕上的忘记密码？选项将不可用。）

使用 WorkSpaces 启动虚拟桌面

借助 WorkSpaces，您可以为用户预调配基于云的虚拟 Microsoft Windows、Amazon Linux 或 Ubuntu Linux 桌面（称为 WorkSpaces）。

> **Note**
>
> 根据您启动的 WorkSpace 类型（Amazon Linux、Ubuntu 或 Windows），Amazon WorkSpaces 控制台中为 WorkSpace 显示的计算机名称值会有所不同。WorkSpace 的计算机名称可以采用以下一种格式：
>
> - Amazon Linux：A-*xxxxxxxxxxxxx*
> - Ubuntu：U-*xxxxxxxxxxxxx*
> - Windows：IP-C*xxxxxx* 或 WSAMZN-*xxxxxxx* 或 EC2AMAZ-*xxxxxxx*
>
> 对于 Windows WorkSpaces，计算机名称格式由捆绑包类型决定；对于从公共捆绑包或基于公共映像的自定义捆绑包创建的 WorkSpaces，则由创建公共映像的时间决定。
> 从 2020 年 6 月 22 日起，从公共捆绑包中推出的 Windows WorkSpaces 的计算机名称采用 WSAMZN-*xxxxxxx* 格式，而不是 IP-C*xxxxxx* 格式。
> 对于基于公共映像的自定义捆绑包，如果公共映像是在 2020 年 6 月 22 日之前创建的，则计算机名称采用 EC2AMAZ-*xxxxxxx* 格式。如果公共映像是在 2020 年 6 月 22 日当天或之后创建的，则计算机名称采用 WSAMZN-*xxxxxxx* 格式。
> 对于自带许可 (BYOL) 捆绑包，默认情况下，计算机名称使用 DESKTOP-*xxxxxxx* 或 EC2AMAZ-*xxxxxxx* 格式。
> 如果您在自定义或 BYOL 捆绑包中为计算机名称指定了自定义格式，则您的自定义格式将覆盖这些默认格式。要指定自定义格式，请参阅创建自定义 WorkSpaces 镜像和捆绑包。
> 重要提示 - 如果您通过 Windows 系统设置更改 WorkSpace 的计算机名称，则将无法再访问 WorkSpace。

WorkSpaces 使用目录来存储和管理 WorkSpace 及用户的相关信息。您可以执行以下任意操作：

- 创建 Simple AD 目录。
- 创建 AWS Directory Service for Microsoft Active Directory，也称为 AWS 托管的 Microsoft AD。
- 使用 Active Directory Connector 连接到现有 Microsoft Active Directory。
- 在 AWS 托管的 Microsoft AD 目录与本地域之间创建信任关系。

> **Note**
>
> - Amazon WorkSpaces 目前不支持与共享目录一起使用。
> - 如果您将 AWS Managed Microsoft AD 目录配置为多区域复制，则只能注册主区域中的目录以便在 Amazon WorkSpaces 中使用。尝试在复制区域中注册该目录以用于 Amazon WorkSpaces 将失败。复制区域内的 Amazon WorkSpaces 不支持使用 AWS Managed Microsoft AD 进行多区域复制。
> - Simple AD 和 AD Connector 供您免费使用，可用于 WorkSpaces。如果连续 30 天没有一起使用 WorkSpaces 与您的 Simple AD 或 AD Connector 目录，则系统将自动取消注册该目录，无法再将其用于 Amazon WorkSpaces，而且将根据 AWS Directory Service 定价条款向您收取该目录的费用。
>
> 要删除空目录，请参阅删除 WorkSpaces 的目录。如果您删除了 Simple AD 或 AD Connector 目录，则当您想重新开始使用 WorkSpaces 时，可以随时创建一个新的目录。

以下教程将为您介绍如何使用受支持的目录服务选项启动 WorkSpace。

教程

- 启动使用 AWS Managed Microsoft AD 的 WorkSpace
- 启动使用 Simple AD 的 WorkSpace
- 启动使用 AD Connector 的 WorkSpace
- 启动使用受信任域的 WorkSpace

启动使用 AWS Managed Microsoft AD 的 WorkSpace

借助 WorkSpaces，您可以为用户预调配基于云的虚拟 Windows 和 Linux 桌面（称为 WorkSpaces）。

WorkSpaces 使用目录来存储和管理 WorkSpace 及用户的相关信息。对于您的目录，您可以从 Simple AD、AD Connector 或 AWS Directory Service for Microsoft Active Directory（也称为 AWS 托管的 Microsoft AD）中选择。此外，您可以在 AWS 托管的 Microsoft AD 目录与本地域之间建立信任关系。

在本教程中，我们将启动使用 AWS 托管的 Microsoft AD 的 WorkSpace。要了解使用其他选项的教程，请参阅使用 WorkSpaces 启动虚拟桌面。

任务

开始前的准备工作

- WorkSpaces 并非在所有区域均可用。请确认受支持的区域，并为您的 WorkSpaces 选择一个区域。有关受支持区域的更多信息，请参阅按 AWS 区域划分的 WorkSpaces 定价。
- 启动 WorkSpace 时，您必须选择一个 WorkSpace 服务包。服务包是操作系统、存储、计算和软件资源的组合。有关更多信息，请参阅 Amazon WorkSpaces 服务包。
- 使用 AWS Directory Service 创建目录或启动 WorkSpace 时，您必须创建或选择通过 1 个公有子网和 2 个私有子网配置的 Virtual Private Cloud。有关更多信息，请参阅为以下项配置 VPC WorkSpaces。

步骤 1：创建 AWS 托管的 Microsoft AD 目录

首先，创建一个 AWS 托管的 Microsoft AD 目录。AWS Directory Service 会创建 2 个目录服务器，您的 VPC 的每个私有子网中各有一个。请注意，目录最初没有任何用户。您将在下一步启动 WorkSpace 时添加用户。

> **Note**
>
> - Amazon WorkSpaces 目前不支持与共享目录一起使用。
> - 如果您将 AWS Managed Microsoft AD 目录配置为多区域复制，则只能注册主区域中的目录以便在 Amazon WorkSpaces 中使用。尝试在复制区域中注册该目录以用于 Amazon WorkSpaces 将失败。复制区域内的 Amazon WorkSpaces 不支持使用 AWS Managed Microsoft AD 进行多区域复制。

创建 AWS 托管的 Microsoft AD 目录

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。

2. 在导航窗格中，选择目录。
3. 选择 Set up Directory、Create Microsoft AD。
4. 按以下说明配置目录：

   a. 对于组织名称，为您的目录输入一个具有唯一性的组织名称（例如，my-demo-directory）。此名称的字符数不得少于 4 个，仅包含字母数字字符和连字符 (-)，并以连字符以外的其他字符开头或结尾。

   b. 对于目录 DNS，为目录输入一个完全限定名称（例如，workspaces.demo.com）。

   > **Important**
   >
   > 如果您需要在启动 WorkSpaces 后更新 DNS 服务器，请按照更新 Amazon WorkSpaces 的 DNS 服务器中的步骤操作，确保您的 WorkSpaces 得到正确更新。

   c. 对于 NetBIOS 名称，为目录输入一个短名称（例如，workspaces）。

   d. 对于 Admin 密码和确认密码，输入目录管理员账户的密码。有关密码要求的更多信息，请参阅《AWS Directory Service 管理指南》中的创建您的 AWS Managed Microsoft AD 目录。

   e. （可选）对于描述，输入目录的描述。

   f. 对于 VPC，选择您创建的 VPC。

   g. 对于 Subnets，选择两个私有子网 (具有 CIDR 块 `10.0.1.0/24` 和 `10.0.2.0/24`)。

   h. 选择 Next Step。

5. 选择 Create Microsoft AD。
6. 选择完成。目录的初始状态是 `Creating`。目录创建完毕后，状态会变为 `Active`。

步骤 2：创建 WorkSpace

现在，您已经创建了一个 AWS 托管的 Microsoft AD 目录，接下来可以创建 WorkSpace。

创建 WorkSpace

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择 Launch WorkSpaces。
4. 在选择目录页面上，选择您创建的目录，然后选择下一步。WorkSpaces 会注册您的目录。
5. 在 Identify Users 页面上，按照以下步骤向目录添加新用户：

a. 填写 Username、First Name、Last Name 和 Email。使用您有权访问的电子邮件地址。

b. 选择 Create Users。

c. 选择 Next Step。

6. 在 Select Bundle 页面上，选择服务包，然后选择 Next Step。

> **Note**
>
> 查看为每个捆绑包建议的用途和规格，以帮助确保您选择最适合用户的捆绑包。有关每个使用案例的更多信息，请参阅 Amazon WorkSpaces 捆绑包。有关捆绑包规格、推荐用途和定价的更多信息，请参阅 Amazon WorkSpaces 定价。

7. 在 WorkSpaces Configuration 页面上，选择运行模式，然后选择 Next Step。

8. 在 Review & Launch WorkSpaces 页面上，选择 Launch WorkSpaces。WorkSpace 的初始状态是 PENDING。启动完毕后，状态会变为 AVAILABLE，然后系统会向您为用户指定的电子邮件地址发送一封邀请电子邮件。

> **Note**
>
> 如果用户已存在于 Active Directory 中，则不会发送邀请电子邮件。相反，请务必手动向用户发送邀请电子邮件。有关更多信息，请参阅发送邀请电子邮件。

9. （可选）如果区域支持 Amazon WorkDocs，则您可以为目录中的所有用户启用 Amazon WorkDocs。有关更多信息，请参阅为 AWS Managed Microsoft AD 启用 Amazon WorkDocs。有关 Amazon WorkDocs 的更多信息，请参阅《Amazon WorkDocs 管理指南》中的 Amazon WorkDocs Drive。

第 3 步：连接到 WorkSpace

收到邀请电子邮件后，您可以使用所选的客户端连接到您的 WorkSpace。登录后，此客户端会显示 WorkSpace 桌面。

连接到 WorkSpace

1. 打开邀请电子邮件中的链接。根据系统提示，指定密码并激活用户。请记住此密码，因为您会在登录 WorkSpace 时用到它。

> **Note**
>
> 密码区分大小写，且长度必须介于 8 到 64 个字符之间 (含 8 和 64)。密码必须至少包含以下每个类别中的一个字符：小写字母 (a-z)、大写字母 (A-Z)、数字 (0-9) 以及 ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/。

2. 查看《Amazon WorkSpaces 用户指南》中的 WorkSpaces 客户端，详细了解每个客户端的要求，然后执行以下一项操作：

   - 根据系统提示，下载一个客户端应用程序或启动 Web Access。
   - 如果系统未提示您且您尚未安装客户端应用程序，请打开 https://clients.amazonworkspaces.com/ ，并下载一个客户端应用程序或启动 Web Access。

   > **Note**
   >
   > 您不能使用 Web 浏览器 (Web Access) 连接到 Amazon Linux WorkSpaces。

3. 启动客户端，输入邀请电子邮件中的注册代码，然后选择 Register。
4. 当系统提示登录时，输入用户的登录凭证，然后选择登录。
5. (可选) 当系统提示您保存凭证时，选择 Yes。

后续步骤

您可以继续自定义您刚创建的 WorkSpace。例如，您可以安装软件，然后在 WorkSpace 中创建自定义服务包。您还可以对 WorkSpaces 和 WorkSpaces 目录执行各种管理任务。使用完 WorkSpace 后，可以将其删除。有关更多信息，请参阅以下文档。

- 创建自定义 WorkSpaces 镜像和捆绑包
- 管理你的 WorkSpaces
- 管理 WorkSpaces 目录
- 删除 WorkSpace

有关使用 WorkSpaces 客户端应用程序（例如设置多台显示器或使用外围设备）的更多信息，请参阅《Amazon WorkSpaces 用户指南》中的 WorkSpaces 客户端和外围设备支持。

启动使用 Simple AD 的 WorkSpace

借助 WorkSpaces，您可以为用户预调配基于云的虚拟 Microsoft Windows 和 Linux 桌面（称为 WorkSpaces）。

WorkSpaces 使用目录来存储和管理 WorkSpace 及用户的相关信息。对于您的目录，您可以从 Simple AD、AD Connector 或 AWS Directory Service for Microsoft Active Directory（也称为 AWS 托管的 Microsoft AD）中选择。此外，您可以在 AWS 托管的 Microsoft AD 目录与本地域之间建立信任关系。

在本教程中，我们将启动使用 Simple AD 的 WorkSpace。要了解使用其他选项的教程，请参阅使用 WorkSpaces 启动虚拟桌面。

任务

开始前的准备工作

- 并非所有区域都提供 Simple AD。请查看受支持的区域，并为您的 Simple AD 目录选择一个区域。有关 Simple AD 支持的区域的更多信息，请参阅 AWS Directory Service 的区域可用性。
- WorkSpaces 并非在所有区域均可用。请确认受支持的区域，并为您的 WorkSpaces 选择一个区域。有关受支持区域的更多信息，请参阅按 AWS 区域划分的 WorkSpaces 定价。
- 启动 WorkSpace 时，您必须选择一个 WorkSpace 服务包。服务包是操作系统、存储、计算和软件资源的组合。有关更多信息，请参阅 Amazon WorkSpaces 服务包。
- 使用 AWS Directory Service 创建目录或启动 WorkSpace 时，您必须创建或选择通过 1 个公有子网和 2 个私有子网配置的 Virtual Private Cloud。有关更多信息，请参阅为以下项配置 VPC WorkSpaces。

步骤 1：创建 Simple AD 目录

创建一个 Simple AD 目录。AWS Directory Service 会创建 2 个目录服务器，您的 VPC 的每个私有子网中各有一个。请注意，目录最初没有任何用户。在下一步创建 WorkSpace 时，您将添加用户。

> **Note**
>
> Simple AD 供您免费使用，可用于 WorkSpaces。如果连续 30 天没有一起使用 WorkSpaces 与您的 Simple AD 目录，则系统将自动取消注册该目录，无法再将其用于 Amazon WorkSpaces，而且将根据 AWS Directory Service 定价条款向您收取该目录的费用。要删除空目录，请参阅删除 WorkSpaces 的目录。如果您删除了 Simple AD 目录，则当您想重新开始使用 WorkSpaces 时，可以随时创建一个新的目录。

创建 Simple AD 目录

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择目录。
3. 依次选择设置目录、Simple AD 和下一步。
4. 按以下说明配置目录：
   a. 对于组织名称，为您的目录输入一个具有唯一性的组织名称（例如，my-example-directory）。此名称的字符数不得少于 4 个，仅包含字母数字字符和连字符 (-)，并以连字符以外的其他字符开头或结尾。
   b. 对于目录 DNS 名称，输入目录的完全限定名称（例如，example.com）。

      > **Important**
      >
      > 如果您需要在启动 WorkSpaces 后更新 DNS 服务器，请按照更新 Amazon WorkSpaces 的 DNS 服务器中的步骤操作，确保您的 WorkSpaces 得到正确更新。

   c. 对于 NetBIOS 名称，为目录键入一个短名称（例如，example）。
   d. 对于 Admin 密码和确认密码，输入目录管理员账户的密码。有关密码要求的更多信息，请参阅《AWS Directory Service 管理指南》中的如何创建 Microsoft AD 目录。
   e. （可选）对于描述，输入目录的描述。
   f. 对于目录大小，选择小。
   g. 对于 VPC，选择您创建的 VPC。
   h. 对于 Subnets，选择两个私有子网 (具有 CIDR 块 `10.0.1.0/24` 和 `10.0.2.0/24`)。
   i. 选择 Next（下一步）。
5. 选择创建目录。

6. 目录的初始状态是 Requested，然后是 Creating。目录创建完成后（这可能需要几分钟），状态会变为 Active。

在目录创建期间发生的情况

WorkSpaces 将代表您完成以下任务：

- 创建一个 IAM 角色以允许 WorkSpaces 服务创建弹性网络接口并列出您的 WorkSpaces 目录。此角色的名称为 workspaces_DefaultRole。
- 在 VPC 中设置用于存储用户和 WorkSpace 信息的 Simple AD 目录。此目录的管理员账户具有用户名 Administrator 和指定的密码。
- 创建 2 个安全组，一个用于目录控制器，另一个用于目录中的 WorkSpace。

步骤 2：创建 WorkSpace

现在，您可以启动 WorkSpace。

为用户创建 WorkSpace

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择 Launch WorkSpaces。
4. 在 Select a Directory 页面上，执行以下操作：
   a. 对于 Directory，选择您创建的目录。
   b. 对于启用自助服务权限，选择是或否，然后输入描述。
   c. 对于 Enable Amazon WorkDocs，选择 Yes。

      > **Note**
      > 仅当在所选区域提供 Amazon WorkDocs 时，此选项才可用。

   d. 选择 Next Step。WorkSpaces 会注册您的 Simple AD 目录。
5. 在 Identify Users 页面上，按照以下步骤向目录添加新用户：
   a. 填写 Username、First Name、Last Name 和 Email。使用您有权访问的电子邮件地址。
   b. 选择 Create Users。

c. 选择 Next Step。

6. 在 Select Bundle 页面上，选择服务包，然后选择 Next Step。

> **Note**
>
> 查看为每个捆绑包建议的用途和规格，以帮助确保您选择最适合用户的捆绑包。有关每个使用案例的更多信息，请参阅 Amazon WorkSpaces 捆绑包。有关捆绑包规格、推荐用途和定价的更多信息，请参阅 Amazon WorkSpaces 定价。

7. 在 WorkSpaces Configuration 页面上，选择运行模式，然后选择 Next Step。
8. 在 Review & Launch WorkSpaces 页面上，选择 Launch WorkSpaces。WorkSpace 的初始状态是 PENDING。启动完毕后（这最多可能需要 20 分钟），状态会变为 AVAILABLE，然后系统会向您为用户指定的电子邮件地址发送一封邀请电子邮件。

> **Note**
>
> 如果用户已存在于 Active Directory 中，则不会发送邀请电子邮件。相反，请务必手动向用户发送邀请电子邮件。有关更多信息，请参阅发送邀请电子邮件。

第 3 步：连接到 WorkSpace

收到邀请电子邮件后，您可以使用所选的客户端连接到您的 WorkSpace。登录后，此客户端会显示 WorkSpace 桌面。

连接到 WorkSpace

1. 打开邀请电子邮件中的链接。根据系统提示，输入密码并激活用户。请记住此密码，因为您会在登录 WorkSpace 时用到它。

> **Note**
>
> 密码区分大小写，且长度必须介于 8 到 64 个字符之间 (含 8 和 64)。密码必须至少包含以下每个类别中的一个字符：小写字母 (a-z)、大写字母 (A-Z)、数字 (0-9) 以及 ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/。

2. 查看《Amazon WorkSpaces 用户指南》中的 WorkSpaces 客户端，详细了解每个客户端的要求，然后执行以下一项操作：

- 根据系统提示，下载一个客户端应用程序或启动 Web Access。
- 如果系统未提示您且您尚未安装客户端应用程序，请打开 https://clients.amazonworkspaces.com/ ，并下载一个客户端应用程序或启动 Web Access。

> **Note**
>
> 您不能使用 Web 浏览器 (Web Access) 连接到 Amazon Linux WorkSpaces。

3. 启动客户端，输入邀请电子邮件中的注册代码，然后选择 Register。
4. 当系统提示登录时，输入用户的登录凭证，然后选择登录。
5. (可选) 当系统提示您保存凭证时，选择 Yes。

后续步骤

您可以继续自定义您刚创建的 WorkSpace。例如，您可以安装软件，然后在 WorkSpace 中创建自定义服务包。您还可以对 WorkSpaces 和 WorkSpaces 目录执行各种管理任务。使用完 WorkSpace 后，可以将其删除。有关更多信息，请参阅以下文档。

- 创建自定义 WorkSpaces 镜像和捆绑包
- 管理你的 WorkSpaces
- 管理 WorkSpaces 目录
- 删除 WorkSpace

有关使用 WorkSpaces 客户端应用程序（例如设置多台显示器或使用外围设备）的更多信息，请参阅《Amazon WorkSpaces 用户指南》中的 WorkSpaces 客户端和外围设备支持。

启动使用 AD Connector 的 WorkSpace

借助 WorkSpaces，您可以为用户预调配基于云的虚拟 Microsoft Windows 和 Linux 桌面（称为 WorkSpaces）。

WorkSpaces 使用目录来存储和管理 WorkSpace 及用户的相关信息。对于您的目录，您可以从 Simple AD、AD Connector 或 AWS Directory Service for Microsoft Active Directory（也称为 AWS 托管的 Microsoft AD）中选择。此外，您可以在 AWS 托管的 Microsoft AD 目录与本地域之间建立信任关系。

在本教程中，我们将启动使用 AD Connector 的 WorkSpace。要了解使用其他选项的教程，请参阅使用 WorkSpaces 启动虚拟桌面。

任务

开始前的准备工作

- WorkSpaces 并非在所有区域均可用。请确认受支持的区域，并为您的 WorkSpaces 选择一个区域。有关受支持区域的更多信息，请参阅按 AWS 区域划分的 WorkSpaces 定价。
- 启动 WorkSpace 时，您必须选择一个 WorkSpace 服务包。服务包是操作系统、存储、计算和软件资源的组合。有关更多信息，请参阅 Amazon WorkSpaces 服务包。
- 创建具有至少两个私有子网的 Virtual Private Cloud。有关更多信息，请参阅为以下项配置 VPC WorkSpaces。必须通过虚拟专用网络 (VPN) 连接或 AWS Direct Connect 将 VPC 连接到您的本地网络。有关更多信息，请参阅《AWS Directory Service 管理指南》中的 AD Connector 先决条件。
- 从 WorkSpace 提供对互联网的访问。有关更多信息，请参阅提供您的 Internet 访问权限 WorkSpace。

步骤 1：创建 AD Connector

> **Note**
>
> AD Connector 供您免费使用，可用于 WorkSpaces。如果连续 30 天没有一起使用 WorkSpaces 与您的 AD Connector 目录，则系统将自动取消注册该目录，无法再将其用于 Amazon WorkSpaces，而且将根据 AWS Directory Service 定价条款向您收取该目录的费用。要删除空目录，请参阅删除 WorkSpaces 的目录。如果您删除了 AD Connector 目录，则当您想重新开始使用 WorkSpaces 时，可以随时创建一个新的目录。

创建 AD Connector

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择目录。
3. 选择 Set up Directory、Create AD Connector。
4. 对于组织名称，为您的目录输入一个具有唯一性的组织名称（例如，my-example-directory）。此名称的字符数不得少于 4 个，仅包含字母数字字符和连字符 (-)，并以连字符以外的其他字符开头或结尾。
5. 对于已连接的目录 DNS，输入您的本地目录的完全限定名称（例如 example.com）。
6. 对于已连接的目录 NetBIOS 名称，输入您的本地目录的短名（例如 example）。
7. 对于 Connector 账户用户名，输入您的本地目录中的一个用户的用户名。该用户必须有权读取用户和组、创建计算机对象并将其加入到域中。
8. 对于 Connector 账户密码和确认密码，输入本地用户的密码。
9. 对于 DNS 地址，输入您的本地目录中至少一个 DNS 服务器的 IP 地址。

   > **Important**
   >
   > 如果您需要在启动 WorkSpaces 后更新 DNS 服务器 IP 地址，请按照更新 Amazon WorkSpaces 的 DNS 服务器中的步骤操作，确保您的 WorkSpaces 得到正确更新。

10. （可选）对于描述，输入目录的描述。
11. 保持 Size 为 Small。
12. 对于 VPC，选择您的 VPC。
13. 对于 Subnets，选择您的子网。所指定的 DNS 服务器必须能够从每个子网访问。
14. 选择 Next Step。
15. 选择 Create AD Connector。连接目录需要几分钟时间。目录的初始状态是 `Requested`，然后是 `Creating`。目录创建完毕后，状态会变为 `Active`。

步骤 2：创建 WorkSpace

现在，您已准备就绪，可为本地目录中的一个或多个用户启动 WorkSpace。

为现有用户启动 WorkSpace

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。

2. 在导航窗格中，选择 WorkSpaces。
3. 选择 Launch WorkSpaces。
4. 对于 Directory，选择您创建的目录。
5. （可选）如果这是您首次在该目录中启动 WorkSpace，并且 Amazon WorkDocs 在区域中受支持，则您可在该目录中为所有用户启用或禁用 Amazon WorkDocs。有关 Amazon WorkDocs 的更多信息，请参阅《Amazon WorkDocs 管理指南》中的 Amazon WorkDocs Drive。
6. 选择 Next（下一步）。WorkSpaces 会注册您的 AD Connector。
7. 从您的本地目录选择一个或多个现有用户。不要通过 WorkSpaces 控制台向本地目录添加新用户。

   要查找所要选择的用户，可以输入用户的完整或部分名称，然后选择搜索或显示所有用户。请注意，不能选择没有电子邮件地址的用户。

   选择了用户后，选择 Add Selected，然后选择 Next Step。
8. 在 Select Bundle 下，选择要用于 WorkSpace 的默认 WorkSpace 服务包。在 Assign WorkSpace Bundles 下，如果需要，可以为单独的 WorkSpace 选择一个不同的服务包。完成后，选择 Next Step。

   > **Note**
   >
   > 查看为每个捆绑包建议的用途和规格，以帮助确保您选择最适合用户的捆绑包。有关每个使用案例的更多信息，请参阅 Amazon WorkSpaces 捆绑包。有关捆绑包规格、推荐用途和定价的更多信息，请参阅 Amazon WorkSpaces 定价。
9. 为您的 WorkSpace 选择一种运行模式，然后选择 Next Step。有关更多信息，请参阅管理 WorkSpace 运行模式。
10. 选择 Launch WorkSpaces。WorkSpace 的初始状态是 `PENDING`。启动完毕后，状态会变为 `AVAILABLE`。
11. 向每个用户的电子邮件地址发送邀请。（如果使用的是 AD Connector，则不会自动发送这些邀请。）有关更多信息，请参阅发送邀请电子邮件。

第 3 步：连接到 WorkSpace

您可以使用所选的客户端连接到您的 WorkSpace。登录后，此客户端会显示 WorkSpace 桌面。

连接到 WorkSpace

1. 打开邀请电子邮件中的链接。
2. 查看《Amazon WorkSpaces 用户指南》中的 WorkSpaces 客户端，详细了解每个客户端的要求，然后执行以下一项操作：
   - 根据系统提示，下载一个客户端应用程序或启动 Web Access。
   - 如果系统未提示您且您尚未安装客户端应用程序，请打开 https://clients.amazonworkspaces.com/ ，并下载一个客户端应用程序或启动 Web Access。

   > **Note**
   > 您不能使用 Web 浏览器 (Web Access) 连接到 Amazon Linux WorkSpaces。

3. 启动客户端，输入邀请电子邮件中的注册代码，然后选择 Register。
4. 当系统提示登录时，输入用户的登录凭证，然后选择登录。
5. (可选) 当系统提示您保存凭证时，选择 Yes。

> **Note**
> 由于您使用的是 AD Connector，您的用户将无法重置自己的密码。（WorkSpaces 客户端应用程序登录屏幕上的忘记密码？选项将不可用。）有关如何重置用户密码的信息，请参阅为 WorkSpaces 设置 Active Directory 管理工具。

后续步骤

您可以继续自定义您刚创建的 WorkSpace。例如，您可以安装软件，然后在 WorkSpace 中创建自定义服务包。您还可以对 WorkSpaces 和 WorkSpaces 目录执行各种管理任务。使用完 WorkSpace 后，可以将其删除。有关更多信息，请参阅以下文档。

- 创建自定义 WorkSpaces 镜像和捆绑包
- 管理你的 WorkSpaces
- 管理 WorkSpaces 目录
- 删除 WorkSpace

有关使用 WorkSpaces 客户端应用程序（例如设置多台显示器或使用外围设备）的更多信息，请参阅《Amazon WorkSpaces 用户指南》中的 WorkSpaces 客户端和外围设备支持。

启动使用受信任域的 WorkSpace

借助 WorkSpaces，您可以为用户预调配基于云的虚拟 Microsoft Windows、Amazon Linux 或 Ubuntu Linux 桌面（称为 WorkSpaces）。

WorkSpaces 使用目录来存储和管理 WorkSpace 及用户的相关信息。对于您的目录，您可以从 Simple AD、AD Connector 或 AWS Directory Service for Microsoft Active Directory（也称为 AWS 托管的 Microsoft AD）中选择。此外，您可以在 AWS 托管的 Microsoft AD 目录与本地域之间建立信任关系。

在本教程中，我们将启动使用信任关系的 WorkSpace。要了解使用其他选项的教程，请参阅使用 WorkSpaces 启动虚拟桌面。

任务

- 开始前的准备工作
- 步骤 1：建立信任关系
- 步骤 2：创建 WorkSpace
- 第 3 步：连接到 WorkSpace
- 后续步骤

开始前的准备工作

- 当 AWS Managed Microsoft AD 配置有与本地目录的信任关系时，在单独的受信任域中通过 AWS 账户启动 WorkSpaces 的情况下可以使用该 AD。但是，使用 Simple AD 或 AD Connector 的 WorkSpaces 无法为受信任域中的用户启动 WorkSpaces。
- WorkSpaces 并非在所有区域均可用。请确认受支持的区域，并为您的 WorkSpaces 选择一个区域。有关受支持区域的更多信息，请参阅按 AWS 区域划分的 WorkSpaces 定价。
- 启动 WorkSpace 时，您必须选择一个 WorkSpace 服务包。服务包是存储、计算和软件资源的组合。有关更多信息，请参阅 Amazon WorkSpaces 服务包。
- 使用 AWS Directory Service 创建目录或启动 WorkSpace 时，您必须创建或选择通过 1 个公有子网和 2 个私有子网配置的 Virtual Private Cloud。有关更多信息，请参阅为以下项配置 VPC WorkSpaces。

步骤 1：建立信任关系

设置信任关系

1. 在您的虚拟私有云(VPC) 中设置 AWS 托管的 Microsoft AD。有关更多信息，请参阅《AWS Directory Service 管理指南》中的创建您的 AWS Managed Microsoft AD 目录。

   > **Note**
   >
   > - Amazon WorkSpaces 目前不支持与共享目录一起使用。
   > - 如果您将 AWS Managed Microsoft AD 目录配置为多区域复制，则只能注册主区域中的目录以便在 Amazon WorkSpaces 中使用。尝试在复制区域中注册该目录以用于 Amazon WorkSpaces 将失败。复制区域内的 Amazon WorkSpaces 不支持使用 AWS Managed Microsoft AD 进行多区域复制。

2. 在 AWS 托管的 Microsoft AD 与本地域之间创建信任关系。确保该信任关系配置为双向信任。有关更多信息，请参阅《AWS Directory Service 管理指南》中的教程：创建 AWS Managed Microsoft AD 与本地域之间的信任关系。

可以使用单向或双向信任，来管理 WorkSpace 并向 WorkSpace 进行身份验证，以便向本地用户和组预调配 WorkSpaces。有关更多信息，请参阅通过 AWS Directory Service 使用单向信任资源域部署 Amazon WorkSpaces。

> **Note**
>
> Ubuntu WorkSpaces 使用系统安全服务进程守护程序 (SSSD) 进行 Active Directory 集成，SSSD 不支持林信任。改为配置外部信任。建议对 Amazon Linux 和 Ubuntu WorkSpaces 使用双向信任。

步骤 2：创建 WorkSpace

在您的 AWS 托管的 Microsoft AD 与本地 Microsoft Active Directory 域之间创建了信任关系之后，就可以为本地域中的用户预调配 WorkSpace 了。

注意，您必须确保跨域复制 GPO 设置，然后才能将其应用到 WorkSpaces。

为本地受信任域中的用户启动 WorkSpaces

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择 Launch WorkSpaces。
4. 在 Select a Directory 页面上，选择您刚注册的目录，然后选择 Next Step。
5. 在 Identify Users 页面上，执行以下操作：
   a. 对于 Select trust from forest，选择您创建的信任关系。
   b. 从本地部署域中选择用户，然后选择 Add Selected。
   c. 选择 Next Step。
6. 选择要用于 WorkSpace 的服务包，然后选择 Next Step。

> **Note**
>
> 查看为每个捆绑包建议的用途和规格，以帮助确保您选择最适合用户的捆绑包。有关每个使用案例的更多信息，请参阅 Amazon WorkSpaces 捆绑包。有关捆绑包规格、推荐用途和定价的更多信息，请参阅 Amazon WorkSpaces 定价。

7. 选择运行模式，选择加密设置，并配置任何标签。完成后，选择 Next Step。
8. 选择 Launch WorkSpaces。注意，WorkSpace 最长可能需要 20 分钟的时间才能变得可用，而且如果启用了加密，最长可能需要 40 分钟的时间。WorkSpace 的初始状态是 PENDING。启动完毕后，状态会变为 AVAILABLE。
9. 向每个用户的电子邮件地址发送邀请。（如果使用的是信任关系，则不会自动发送这些邀请。）有关更多信息，请参阅发送邀请电子邮件。

第 3 步：连接到 WorkSpace

收到邀请电子邮件后，您可以连接到您的 WorkSpace。用户可以用 username、corp\username 或 corp.example.com\username 的形式输入其用户名。

连接到 WorkSpace

1. 打开邀请电子邮件中的链接。根据系统提示，输入密码并激活用户。请记住此密码，因为您会在登录 WorkSpace 时用到它。

> **Note**
>
> 密码区分大小写，且长度必须介于 8 到 64 个字符之间 (含 8 和 64)。密码必须至少包含以下每个类别中的一个字符：小写字母 (a-z)、大写字母 (A-Z)、数字 (0-9) 以及 ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/。

2. 查看《Amazon WorkSpaces 用户指南》中的 WorkSpaces 客户端，详细了解每个客户端的要求，然后执行以下一项操作：

   - 根据系统提示，下载一个客户端应用程序或启动 Web Access。
   - 如果系统未提示您且您尚未安装客户端应用程序，请打开 https://clients.amazonworkspaces.com/ ，并下载一个客户端应用程序或启动 Web Access。

   > **Note**
   >
   > 您不能使用 Web 浏览器 (Web Access) 连接到 Amazon Linux WorkSpaces。

3. 启动客户端，输入邀请电子邮件中的注册代码，然后选择 Register。
4. 当系统提示登录时，输入用户的登录凭证，然后选择登录。
5. (可选) 当系统提示您保存凭证时，选择 Yes。

后续步骤

您可以继续自定义您刚创建的 WorkSpace。例如，您可以安装软件，然后在 WorkSpace 中创建自定义服务包。您还可以对 WorkSpaces 和 WorkSpaces 目录执行各种管理任务。使用完 WorkSpace 后，可以将其删除。有关更多信息，请参阅以下文档。

- 创建自定义 WorkSpaces 镜像和捆绑包
- 管理你的 WorkSpaces
- 管理 WorkSpaces 目录
- 删除 WorkSpace

有关使用 WorkSpaces 客户端应用程序（例如设置多台显示器或使用外围设备）的更多信息，请参阅《Amazon WorkSpaces 用户指南》中的 WorkSpaces 客户端和外围设备支持。

管理 WorkSpace 用户

一个 WorkSpace 只能分配给一个用户，不能在多个用户间共享。默认情况下，每个目录的每个用户只允许使用一个 WorkSpace。

目录

管理 WorkSpace 用户

作为 WorkSpaces 的管理员，您可以执行以下任务来管理 WorkSpace 用户 。

编辑用户信息

您可以使用 WorkSpaces 控制台为 WorkSpace 编辑用户信息。

> **Note**
>
> 仅当您使用 AWS Managed Microsoft AD 或 Simple AD 时该功能才可用。如果通过 AD Connector 或信任关系使用 Microsoft Active Directory，则可以使用 Active Directory 模块来管理用户和组。

要编辑用户信息

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择一个用户，然后依次选择操作、编辑用户。
4. 根据需要，更新名字、姓氏和电子邮件地址。
5. 选择更新。

添加或删除用户

您只能在启动 WorkSpace 的过程中从 Amazon WorkSpaces 控制台创建用户，并且无法通过 Amazon WorkSpaces 控制台删除用户。大多数用户管理任务（包括管理用户组）都必须通过您的目录执行。

添加或删除用户和组

要添加、删除或管理用户和组，您必须通过目录进行此操作。您将使用目录管理工具 (如 Active Directory 管理工具) 为您的 WorkSpace 目录执行大部分管理任务。有关更多信息，请参阅为 WorkSpaces 设置 Active Directory 管理工具。

> **Important**
>
> 在删除用户之前，必须先删除分配给该用户的 WorkSpace。有关更多信息，请参阅删除 WorkSpace。

用于管理用户和组的过程取决于您使用的目录类型。

- 如果您使用的是 AWS Managed Microsoft AD，请参阅《AWS Directory Service 管理指南》中的在 AWS Managed Microsoft AD 中管理用户和组。
- 如果您使用的是 Simple AD，请参阅《AWS Directory Service 管理指南》中的在 Simple AD 中管理用户和组。
- 如果通过 AD Connector 或信任关系使用 Microsoft Active Directory，则可以使用 Active Directory 模块来管理用户和组。

发送邀请电子邮件

您可以根据需要向用户手动发送邀请电子邮件。

> **Note**
>
> 如果使用的是 AD Connector 或受信任域，则不会自动向您的用户发送邀请电子邮件，因此您必须手动发送。如果用户已经位于 Active Directory 中，系统也不会自动发送邀请电子邮件。

要重新发送邀请电子邮件

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。

2. 在导航窗格中，选择 WorkSpaces。
3. 在 WorkSpaces (工作区) 页面上，使用搜索框搜索要向其发送邀请的用户，然后从搜索结果中选择相应的 WorkSpace。一次只能选择一个 WorkSpace。
4. 依次选择操作和邀请用户。
5. 在邀请用户注册 WorkSpace 页面上，选择发送邀请。

为一个用户创建多个 WorkSpaces

默认情况下，您只能为每个目录的每个用户创建一个 WorkSpace。但是，如果需要，您可以为一个用户创建多个 WorkSpace，具体取决于您的目录设置。

- 如果您的 WorkSpaces 只有一个目录，请为该用户创建多个用户名。例如，名为 Mary Major 的用户可以将 mmajor1、mmajor2 等等作为用户名。每个用户名都与同一目录中的不同 WorkSpace 相关联，但是，只要所有 WorkSpaces 都是在同一 AWS 区域的同一个目录中创建的，这些 WorkSpaces 就具有相同的注册码。
- 如果您的 WorkSpaces 有多个目录，请在单独的目录中为用户创建 WorkSpaces。您可以在目录中使用相同的用户名，也可以在目录中使用不同的用户名。WorkSpaces 将具有不同的注册代码。

> **Tip**
>
> 为便于您轻松找到为用户创建的所有 WorkSpaces，请为每个 WorkSpace 使用相同的基本用户名。
> 例如，如果您有一个名为 Mary Major 的用户，其 Active Directory 用户名为 mmajor，请使用诸如 mmajor、mmajor1、mmajor2、mmajor3 之类的用户名或其他变体（例如 mmajor_windows 或 mmajor_linux）为她创建 WorkSpaces。只要所有 WorkSpaces 都具有相同的起始基本用户名 (mmajor)，您就可以在 WorkSpaces 控制台中对用户名进行排序，将该用户的所有 WorkSpaces 分组在一起。

> **Important**
>
> - 用户可以同时拥有 PCoIP 和 WSP WorkSpaces，前提是这两个 WorkSpaces 位于不同的目录中。同一个用户不能在同一个目录中同时拥有 PCoIP 和 WSP WorkSpaces。

- 如果您要设置多个 WorkSpaces 以用于跨区域重定向，则必须在不同 AWS 区域的不同目录中设置 WorkSpaces，且必须在每个目录中使用相同的用户名。有关跨区域重定向的更多信息，请参阅 Amazon 的跨区域重定向 WorkSpaces。

要在 WorkSpaces 之间切换，用户可使用与特定 Workspace 关联的用户名和注册码登录。如果用户使用的是适用于 Windows、macOS 或 Linux 的 WorkSpaces 客户端应用程序 3.0+ 版本，则用户可以在客户端应用程序中转到设置、管理登录信息来为 WorkSpaces 分配不同的名称。

自定义用户如何登录他们的 WorkSpaces

使用统一资源标识符 (URI) 自定义用户的访问权限，从而提供与组织中现有工作流程集成的简化登录体验。 WorkSpaces 例如，您可以自动生成登录 URI，使用用户的注册码来 WorkSpaces 注册用户。因此：

- 用户可以跳过手动注册过程。
- 他们的用户名会自动输入到他们的 WorkSpaces 客户登录页面上。
- 如果在您的组织中使用了多重身份验证 (MFA)，则用户的用户名和 MFA 代码将自动在其客户端登录页上输入。

URI 访问适用于基于区域的注册码（例如 `WSpdx+ABC12D`）和基于完全限定域名 (FQDN) 的注册码（例如 `desktop.example.com`）。有关创建和使用基于 FQDN 的注册码的更多信息，请参阅 Amazon 的跨区域重定向 WorkSpaces。

您可以在以下支持的设备上 WorkSpaces 为客户端应用程序配置 URI 访问权限：

- Windows 计算机
- macOS 计算机
- Ubuntu Linux 18.04、20.04 和 22.04 计算机
- iPad
- Android 设备

要使用 URI 访问他们的 URI WorkSpaces，用户必须首先通过打开 https://clients.amazonworkspaces.com/ us-iso-eastus-isob-east

Windows 和 macOS 电脑上的 Firefox 和 Chrome 浏览器、Ubuntu Linux 18.04、20.04 和 22.04 电脑上的 Firefox 浏览器以及 Windows 电脑上的 Internet Explorer 和 Microsoft Edge 浏览器支持 URI 访问。有关 WorkSpaces 客户的更多信息，请参阅 Amazon WorkSpaces 用户指南中的WorkSpaces 客户。

> **Note**
>
> 在安卓设备上，URI 访问仅适用于 Firefox 浏览器，而不适用于 Google Chrome 浏览器。

要配置对的 URI 访问权限 WorkSpaces，请使用下表中描述的任何 URI 格式。

> **Note**
>
> 如果您的 URI 的数据组件包含以下任一预留字符，建议您在数据组件中使用百分号编码以避免歧义：
>
> `@ : / ? & =`
>
> 例如，如果您有包含其中任一字符的用户名，则应该对 URI 中的这些用户名进行百分号编码。有关更多信息，请参阅统一资源标识符 (URI)：一般语法。

支持的语法	描述
workspaces://	打开 WorkSpaces 客户端应用程序。（注意：Linux 客户端应用程序目前不支持使用 workspaces:// 本身。）
workspaces://@registrationcode	使用用户的 WorkSpaces 注册码注册用户。此外，显示客户端登录页。
workspaces://username@registrationcode	使用用户的 WorkSpaces 注册码注册用户。此外，在客户端登录页上的用户名字段中自动输入用户名。
workspaces://username@registrationcode?MFACode=mfa	使用用户的 WorkSpaces 注册码注册用户。此外，在客户端登录页上的用户名字段中自动输入用户名，在同一页上的 MFA 代码字段中自动输入多重身份验证 (MFA) 代码。

支持的语法	描述
workspaces://@registrationcode?MFACode=mfa	使用用户的 WorkSpaces 注册码注册用户。此外，在客户端登录页上的 MFA code (MFA 代码) 字段中自动输入多重验证 (MFA) 代码。

> **Note**
>
> 如果用户在已经 WorkSpace 从 Windows 客户端连接到 URI 链接时打开 URI 链接，则 WorkSpaces 会打开一个新会话，其原始 WorkSpaces 会话将保持打开状态。如果用户在 WorkSpace 从 macOS、iPad 或 Android 客户端连接到时打开 URI 链接，则不会打开任何新会话；只有他们的原始 WorkSpaces 会话保持打开状态。

为您的用户启用自助 WorkSpace管理功能

在中 WorkSpaces，您可以为用户启用自助服务 WorkSpace 管理功能，让他们能够更好地控制自己的体验。它还可以减少您的 IT 支持人员的工作量 WorkSpaces。启用自助服务功能后，用户可以直接从其 WorkSpaces 客户端执行以下一项或多项任务：

- 将其凭证缓存在其客户端上。这样，他们 WorkSpace 无需重新输入凭据即可重新连接到自己的账户。
- 重启（重启）他们 WorkSpace的。
- 在其上增加根卷和用户卷的大小 WorkSpace。
- 更改它们的计算类型（捆绑包） WorkSpace。
- 切换他们的运行模式 WorkSpace。
- 重建他们 WorkSpace的。

支持的客户端

- Android，在 Android 或与 Android 兼容的 Chrome 操作系统上运行
- Linux
- macOS
- Windows

为您的用户启用自助服务管理功能

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择目录。
3. 选择要启用自助服务管理功能的目录。
4. 向下滚动到自助服务权限，然后选择编辑。根据需要启用或禁用以下选项，以确定用户可以从其客户端执行的 WorkSpace 管理任务：

   - 记住我 - 用户可以通过选择登录屏幕上的记住我或保持登录状态复选框，选择是否在其客户端上缓存其凭证。这些凭证仅缓存到 RAM 中。当用户选择缓存其凭据时，他们 WorkSpaces 无需重新输入凭据即可重新连接到自己的凭据。要控制用户可以缓存其凭证的时长，请参阅 设置 Kerberos 票证的最长使用期限。
   - WorkSpace 从客户端重新启动-用户可以重新启动（重新启动）他们 WorkSpace的。重新启动会断开用户与他们的连接 WorkSpace，将其关闭，然后重新启动。用户数据、操作系统和系统设置不受影响。
   - 增加卷大小 — 用户无需联系 IT 支持人员即可将其根卷和用户卷扩展 WorkSpace 到指定大小。用户可以将根卷（对于 Windows，是 C: 驱动器；对于 Linux，/）的大小增加到 175 GB，将用户卷（对于 Windows，是 D: 驱动器；对于 Linux，/home）的大小增加到 100 GB。 WorkSpace root 和用户卷属于无法更改的设置组。可用组包括：[根 (GB)，用户 (GB)]: [80，10]、[80，50]、[80，100]、[175 至 2000，100 至 2000]。有关更多信息，请参阅 修改 WorkSpace。

     对于新创建的 WorkSpace，用户必须等待 6 小时才能增加这些驱动器的大小。之后，他们在 6 小时内只能执行此操作一次。在增加卷大小时，用户可以在其上执行大多数任务 WorkSpace。他们无法执行的任务是：更改 WorkSpace 计算类型、切换 WorkSpace 运行模式、重启或重建 WorkSpace计算类型。 WorkSpace该过程完成后， WorkSpace 必须重新启动才能使更改生效。此过程可能需要一个小时。

     > **Note**
     >
     > 如果用户增加音量大小 WorkSpace，则会增加他们的账单费率 WorkSpace。

   - 更改计算类型-用户可以在计算类型（捆绑包） WorkSpace 之间切换。对于新创建的捆绑包 WorkSpace，用户必须等待 6 小时才能切换到其他捆绑包。之后，他们在 6 小时内只能切换到较大的服务包一次，或在 30 天内只能切换到较小的服务包一次。当 WorkSpace 计算类型更改进行时，用户将与其断开连接 WorkSpace，他们无法使用或更改 WorkSpace。 WorkSpace 在计算类型更改过程中会自动重新启动。此过程可能需要一个小时。

> **Note**
>
> 如果用户更改其 WorkSpace 计算类型，则会更改其账单费率 WorkSpace。

- 切换运行模式-用户可以在AlwaysOn和AutoStop运行模式 WorkSpace 之间切换。有关更多信息，请参阅 管理 WorkSpace 运行模式。

> **Note**
>
> 如果用户切换其运行模式 WorkSpace，则会更改其账单费率 WorkSpace。

- WorkSpace 从客户端重建-用户可以将 a 的操作系统重建 WorkSpace 到其原始状态。重建 a WorkSpace 时，将根据最新的备份重新创建用户卷（D: 驱动器）。由于备份每 12 小时完成一次，因此，用户数据可能已存在多达 12 小时。对于新创建的 WorkSpace，用户必须等待 12 小时才能重建自己的 WorkSpace。 WorkSpace重建进行时，用户将与其断开连接 WorkSpace，并且他们无法使用或对其进行更改 WorkSpace。此过程可能需要一个小时。
- 诊断日志上传-用户可以直接将 WorkSpaces 客户端日志文件上传 WorkSpaces 到以解决问题，而无需中断客户端的 WorkSpaces 使用。如果您为用户启用诊断日志上传，或者让您的用户自己上传诊断日志，则日志文件 WorkSpaces 将自动发送到。您可以在 WorkSpaces 直播会话之前或期间启用诊断日志上传。

5. 选择保存。

为用户启用 Amazon Connect 音频优化

在 WorkSpaces 管理控制台中，您可以为 WorkSpaces 队列启用 Amazon Connect 联系人控制面板 (CCP) 音频优化，以增强安全性并启用原生音质音频。启用 CCP 音频优化后，CCP 音频将由客户端端点处理，同时 WorkSpaces 用户可以在其 WorkSpaces 内与 CCP 进行交互。

Amazon Connect 联系人控制面板 (CCP) 音频优化适用于：

- WorkSpaces Windows 客户端。
- Amazon Linux 和 Windows WorkSpaces。
- 使用 PCoIP 或 WSP 的 WorkSpaces。

要求

- 您必须使用 Amazon Connect 进行设置。
- 您必须使用 Amazon Connect 流 API 创建一个不含呼叫信令的媒体 CCP，从而构建自定义 CCP。这样，会在本地桌面上使用标准 CCP 处理媒体，并使用没有媒体的 CCP 通过远程连接处理信号发送和呼叫控制。有关 Amazon Connect 流 API 的更多信息，请通过以下网址参见 GitHub 存储库：https://github.com/aws/amazon-connect-streams。您构建的自定义 CCP 是 Amazon Connect 代理将在其 WorkSpaces 内使用的 CCP。
- 您必须在 Amazon Connect 支持的 WorkSpaces 客户端端点上安装 Web 浏览器。要查看支持的浏览器列表，请参阅 Amazon Connect 支持的浏览器。

> **Note**
>
> 如果您的用户使用不受支持的浏览器，则当他们尝试登录 CCP 时，系统会要求他们下载支持的浏览器。

启用 Amazon Connect 音频优化

为用户启用 Amazon Connect 音频优化：

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择目录。
3. 选择目录，然后选择 Actions、Update Details。
4. 展开 Amazon Connect 音频优化。

> **Note**
>
> 在使用 Amazon Connect 进行配置之前，选择更新，以保存之前在管理控制台中进行的所有未保存的更改。

5. 选择配置 Amazon Connect。
6. 输入 Amazon Connect 联系人控制面板 (CCP) 名称。

> **Note**
>
> 用户插件菜单中将使用您为 CCP 提供的名称。选择一个对您的用户有意义的名称。

7. 输入 Amazon Connect 生成的 Amazon Connect 联系人控制面板 URL。有关获取 URL 的更多信息，请参阅提供对联系人控制面板的访问权限。
8. 选择创建 Amazon Connect。

更新目录的 Amazon Connect 音频优化详细信息

更新目录的 Amazon Connect 音频优化详细信息：

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择目录。
3. 选择目录，然后选择 Actions、Update Details。
4. 展开 Amazon Connect 音频优化。

> **Note**
>
> 在使用 Amazon Connect 进行配置之前，选择更新，以保存之前在管理控制台中进行的所有未保存的更改。

5. 选择配置 Amazon Connect。
6. 选择编辑。
7. 选择目录，然后选择 Actions、Update Details。
8. 更新 Amazon Connect 联系人控制面板的名称和 URL。
9. 选择 Save（保存）。

删除目录的 Amazon Connect 音频优化

删除目录的 Amazon Connect 音频优化：

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择目录。

3. 选择目录，然后选择 Actions、Update Details。
4. 展开 Amazon Connect 音频优化。

> **Note**
>
> 在使用 Amazon Connect 进行配置之前，选择更新，以保存之前在管理控制台中进行的所有未保存的更改。

5. 选择配置 Amazon Connect。
6. 选择删除 Amazon Connect。

有关更多信息，请参阅代理培训指南。

启用诊断日志上传

要对 WorkSpaces 客户端问题进行故障排除，请启用自动上传诊断日志。目前，Windows、macOS、Linux 和 Web Access 客户端支持此功能。

> **Note**
>
> WorkSpaces 客户端诊断日志上传功能目前在 AWS GovCloud （美国西部）地区不可用。

诊断日志上传

通过上传诊断日志，您可以将 WorkSpaces 客户端日志文件直接上传 WorkSpaces 到以解决问题，而无需中断客户端的 WorkSpaces 使用。如果您为用户启用诊断日志上传，或者让您的用户自己上传诊断日志，则日志文件 WorkSpaces 将自动发送到。您可以在 WorkSpaces 直播会话之前或期间启用诊断日志上传。

要从托管设备自动上传诊断日志，请安装支持诊断上传的 WorkSpaces客户端。默认情况下，日志上传处于启用状态。您可以通过以下任一方式修改设置：

选项 1：使用 AWS 控制台

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择目录。

3. 选择要启用诊断日志的目录名称。
4. 向下滚动到自助服务权限。
5. 选择 “查看详情”
6. 选择编辑。
7. 选择诊断日志上传。
8. 选择保存。

选项 2：使用 API 调用

您可以编辑目录设置以启用或禁用 WorkSpaces Windows、macOS 和 Linux 客户端，以便使用 API 调用自动上传诊断日志。如果启用，则当客户端出现问题时， WorkSpaces 无需用户交互即可将日志发送到。如需了解更多信息，请参阅 WorkSpaces API 参考。

您也可以让用户选择是否在安装客户端后启用自动诊断日志上传。有关更多信息，请参阅 WorkSpacesWindows 客户端应用程序、WorkSpaces macOS 客户端应用程序和 WorkSpacesLinux 客户端应用程序。

> **Note**
>
> - 诊断日志不包含敏感信息。您可以在目录级别为用户禁用自动诊断日志上传，或者允许您的用户自行禁用这些功能。
> - 要访问诊断日志上传功能，您需要安装以下版本的 WorkSpaces 客户端：
>   - Windows 客户端 5.4.0 或更高版本
>   - macOS 客户端 5.8.0 或更高版本
>   - Ubuntu 22.04 客户端的 2023.1
>   - Ubuntu 20.04 客户端的 2023.1
>   - 您也可以使用 Web Access 客户端访问诊断日志上传功能

管理你的 WorkSpaces

您可以使用 WorkSpaces 控制台管理您 WorkSpaces 的。

要执行目录管理任务，请参见the section called “设置目录管理”。

> **Note**
>
> - 确保在上更新网络依赖驱动程序，例如 ENA、NVMe 和 PV 驱动程序。 WorkSpaces你应该至少每 6 个月这样做一次。有关更多信息，请参阅安装或升级适用于 Windows 实例的弹性网络适配器 (ENA) 驱动程序和在 Windows 实例上升半虚拟化驱动程序。AWS NVMe 驱动程序
> - 确保定期将 ec2Config、ec2Launch 和 ec2Launch V2 代理更新到最新版本。你应该至少每 6 个月这样做一次。有关更多信息，请参阅更新 ec2Config 和 ec2Launch。

内容

- Microsoft 365 自带许可 (BYOL)
- 升级 Windows BYOL WorkSpaces
- 迁移 WorkSpace
- 删除 WorkSpace

管理你的 Windows WorkSpaces

您可以使用组策略对象 (GPO) 来应用设置来管理 Windows WorkSpaces 或属于您的 Windows WorkSpaces 目录的用户。

> **Note**
>
> Linux 实例不遵循组策略。有关管理亚马逊 Linux 的信息 WorkSpaces，请参阅管理你的亚马逊 Linux WorkSpaces。

我们建议您为 WorkSpaces 计算机对象创建一个组织单位，为 WorkSpaces 用户对象创建一个组织单位。

要使用特定于 Amazon 的组策略设置 WorkSpaces，您必须为正在使用的协议安装组策略管理模板，无论是 PCoIP 还是 WorkSpaces 流协议 (WSP)。

> **Warning**
>
> 组策略设置可能会影响您的 WorkSpace 用户体验，如下所示：
>
> - 实现交互式登录消息以显示登录横幅可防止用户访问他们的。 WorkSpacesPC WorkSpaces oIP 目前不支持交互式登录消息组策略设置。WSP 支持登录消息 WorkSpaces，用户在接受登录横幅后必须重新登录。
> - 通过组策略设置禁用可移动存储会导致登录失败，从而导致用户登录到无权访问驱动器 D 的临时用户配置文件。
> - 通过组策略设置将用户从远程桌面用户本地组中移除会阻止这些用户通过 WorkSpaces 客户端应用程序进行身份验证。有关此组策略设置的更多信息，请参阅 Microsoft 文档中的允许通过远程桌面服务登录。
> - 如果您从 “允许本地登录” 安全策略中移除内置用户组，则您的 PCoIP WorkSpaces 用户将无法 WorkSpaces 通过 WorkSpaces 客户端应用程序连接到他们。您的 PCoIP

WorkSpaces 也不会收到 PCoIP 代理软件的更新。PCoIP 代理更新可能包含安全修复和其他修复程序，或者它们可能会为您启用新功能。 WorkSpaces有关使用此安全策略的更多信息，请参阅 Microsoft 文档中的允许本地登录。

- 组策略设置可用于限制驱动器访问。如果将组策略设置配置为限制对驱动器 C 或驱动器 D 的访问，则用户无法访问他们的 WorkSpaces。要防止此问题发生，请确保您的用户可以访问驱动器 C 和驱动器 D。
- WorkSpaces 音频输入功能需要内部的本地登录访问权限。 WorkSpace默认情况下，Windows WorkSpaces 的音频输入功能处于启用状态。但是，如果您的组策略设置限制了用户的本地登录 WorkSpaces，则音频输入将无法在您的上运行。 WorkSpaces如果删除该组策略设置，则下次重新启动后将启用音频输入功能。 WorkSpace有关此组策略设置的更多信息，请参阅 Microsoft 文档中的允许本地登录。

  有关启用或禁用音频输入重定向的更多信息，请参阅启用或禁用 PCoIP 的音频输入重定向或启用或禁用 WSP 的音频输入重定向。
- 使用组策略将 Windows 电源计划设置为 “平衡” 或 “省电模式”，可能会 WorkSpaces 导致您在它们处于闲置状态时进入睡眠状态。我们强烈建议使用组策略将 Windows 电源计划设置为高性能。有关更多信息，请参阅 我的 Windows 闲置时会 WorkSpace 进入睡眠状态。
- 某些组策略设置会在用户从会话断开连接时迫使其注销。用户在其上打开的所有应用程序 WorkSpaces 都将关闭。
- WSP WorkSpaces 目前不支持 “为处于活动状态但处于空闲状态的远程桌面服务会话设置时间限制”。避免在 WSP 会话期间使用它，因为即使有活动且会话未处于闲置状态，也会导致断开连接。

有关使用 Active Directory 管理工具处理 GPO 的信息，请参阅为 WorkSpaces 设置 Active Directory 管理工具。

内容

安装 WorkSpaces 流协议 (WSP) 的组策略管理模板文件

要使用特定于 WorkSpaces 使用 WorkSpaces 流协议 (WSP) 的组策略设置，必须将 WSP 的组策略管理模板`wsp.admx`和`wsp.adml`文件添加到目录的域控制器的 WorkSpaces 中央存储区。有关 `.admx` 和 `.adml` 文件的更多信息，请参阅如何在 Windows 中创建和管理组策略管理模板的中央存储。

以下过程介绍了如何创建中央存储并向其中添加管理模板文件。在目录管理 WorkSpace 或加入目录的 Amazon EC2 实例上执行以下步骤。 WorkSpaces

为 WSP 安装组策略管理模板文件

1. 在正在运行的 Windows WorkSpace 中，复制`C:\Program Files\Amazon\WSP`目录中的`wsp.admx`和`wsp.adml`文件。
2. 在目录管理 WorkSpace 或已加入 WorkSpaces 目录的 Amazon EC2 实例上，打开 Windows 文件资源管理器，然后在地址栏中输入贵组织的完全限定域名 (FQDN)，例如`\\example.com`。
3. 打开 `sysvol` 文件夹。
4. 打开带有 *FQDN* 名称的文件夹。
5. 打开 `Policies` 文件夹。您现在应该位于 `\\`*FQDN*`\sysvol\`*FQDN*`\Policies` 中。
6. 如果该文件尚不存在，请创建一个名为 `PolicyDefinitions` 的文件夹。
7. 打开 `PolicyDefinitions` 文件夹。
8. 将 `wsp.admx` 文件复制到 `\\`*FQDN*`\sysvol\`*FQDN*`\Policies\PolicyDefinitions` 文件夹中。

9. 在 PolicyDefinitions 文件夹中创建名为 en-US 的文件夹。
10. 打开 en-US 文件夹。
11. 将 wsp.adml 文件复制到 *FQDN*\sysvol*FQDN*\Policies\PolicyDefinitions\en-US 文件夹中。

验证管理模板文件是否已正确安装

1. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)。
2. 展开林（林：***FQDN***）。
3. 展开域。
4. 展开您的 FQDN（例如，example.com）。
5. 展开组策略对象。
6. 选择默认域策略，打开上下文（右键单击）菜单，然后选择编辑。

> **Note**
>
> 如果支持的域 WorkSpaces 是 AWS Managed Microsoft AD 目录，则无法使用默认域策略来创建 GPO。相反，您必须在具有委派权限的域容器下创建和链接 GPO。
> 使用创建目录时 AWS Managed Microsoft AD， AWS Directory Service 会在域根目录下创建一个*####*组织单位 (OU)。此 OU 的名称基于您在创建目录时键入的 NetBIOS 名称。如果您未指定 NetBIOS 名称，则此名称将默认为您目录 DNS 名称的第一部分（例如，如果目录 DNS 名称为 corp.example.com，则 NetBIOS 名称将为 corp）。
> 要创建 GPO，请改为选择默认域策略，选择 *yourdomainname* OU（或该组织下的任何 OU），打开上下文（右键单击）菜单，然后选择在此域中创建 GPO，并将其链接到此处。
> 有关 *yourdomainname* OU 的更多信息，请参阅《AWS Directory Service 管理指南》中的创建的内容。

7. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
8. 现在，您可以使用此 WSP 组策略对象来修改使用 WSP WorkSpaces 时特有的组策略设置。

管理 WorkSpaces 流协议 (WSP) 的组策略设置

使用组策略设置来管理使用 WSP WorkSpaces 的 Windows。

配置对 WSP 的打印机支持

默认情况下，WorkSpaces 启用基本远程打印，它提供的打印功能有限，因为它在主机端使用通用打印机驱动程序来确保打印兼容。

Windows 客户端的高级远程打印（不适用于 WSP）让您可以使用打印机的特定功能（如双面打印），但需要在主机端安装匹配的打印机驱动程序。

远程打印实施为虚拟通道。如果虚拟通道被禁用，远程打印无法正常工作。

对于 Windows WorkSpaces，您可以根据需要使用组策略设置来配置打印机支持。

配置打印机支持

1. 确保在 WorkSpaces目录的域控制器的中央存储区中安装了最新的 WSP WorkSpaces 组策略管理模板。
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)。
3. 展开林（林：*FQDN*）。
4. 展开域。
5. 展开您的 FQDN（例如，`example.com`）。
6. 展开组策略对象。
7. 选择默认域策略，打开上下文（右键单击）菜单，然后选择编辑。

   > **Note**
   >
   > 如果支持的域 WorkSpaces 是 AWS Managed Microsoft AD 目录，则无法使用默认域策略来创建 GPO。相反，请选择 *yourdomainname* OU（或该组织下的任何 OU），打开上下文（右键单击）菜单，然后选择在此域中创建 GPO，并将其链接到此处。有关 *yourdomainname* OU 的更多信息，请参阅《AWS Directory Service 管理指南》中的创建的内容。

8. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
9. 打开配置远程打印设置。
10. 在 Configure remote printing (配置远程打印) 对话框中，执行下列操作之一：
    - 要启用本地打印机重定向，请选择启用，然后在打印选项中选择基本。要自动使用客户端计算机的当前默认打印机，请选择将本地默认打印机映射到远程主机。

- 要禁用打印，请选择禁用。

11. 选择 确定。
12. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：

    - 重启 WorkSpace（在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
    - 在管理命令提示符处，输入 **`gpupdate /force`**。

为 WSP 配置剪贴板重定向（复制/粘贴）

默认情况下， WorkSpaces 支持双向（复制/粘贴）剪贴板重定向。对于 Windows WorkSpaces，您可以使用组策略设置来禁用此功能或配置允许剪贴板重定向的方向。

为 Windows 配置剪贴板重定向 WorkSpaces

1. 确保在 WorkSpaces目录的域控制器的中央存储区中安装了最新的 WSP WorkSpaces 组策略管理模板。
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)。
3. 展开林（林：***FQDN***）。
4. 展开域。
5. 展开您的 FQDN（例如，`example.com`）。
6. 展开组策略对象。
7. 选择默认域策略，打开上下文（右键单击）菜单，然后选择编辑。

> **Note**
>
> 如果支持的域 WorkSpaces 是 AWS Managed Microsoft AD 目录，则无法使用默认域策略来创建 GPO。相反，请选择 *`yourdomainname`* OU（或该组织下的任何 OU），打开上下文（右键单击）菜单，然后选择在此域中创建 GPO，并将其链接到此处。有关 *`yourdomainname`* OU 的更多信息，请参阅《AWS Directory Service 管理指南》中的创建的内容。

8. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
9. 打开 Configure clipboard redirection 设置。

10. 在配置剪贴板重定向对话框中，选择启用或禁用。

    启用配置剪贴板重定向后，以下剪贴板重定向选项将变为可用：

    - 选择复制并粘贴，以允许双向剪贴板复制和粘贴重定向。
    - 选择仅复制，以仅允许将数据从服务器剪贴板复制到客户端剪贴板。
    - 选择仅粘贴，以仅允许将数据从客户端剪贴板粘贴到服务器剪贴板。
11. 选择 确定。
12. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：

    - 重启 WorkSpace（在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
    - 在管理命令提示符处，输入 **`gpupdate /force`**。

已知限制

启用剪贴板重定向后 WorkSpace，如果您从 Microsoft Office 应用程序中复制大于 890 KB 的内容，则该应用程序可能会变慢或在长达 5 秒钟内没有响应。

为 WSP 设置会话恢复超时

网络连接中断时，您的活动 WorkSpaces 客户端会话将断开连接。 WorkSpaces 如果网络连接在一定时间内恢复，则适用于 Windows 和 macOS 的客户端应用程序会尝试自动重新连接会话。默认的会话恢复超时时间为 20 分钟（1200 秒），但您可以修改该值 WorkSpaces ，因为该值由您的域的组策略设置控制。

要设置自动会话恢复超时值

1. 确保在 WorkSpaces目录的域控制器的中央存储区中安装了最新的 WSP WorkSpaces 组策略管理模板。
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)。
3. 展开林（林：***FQDN***）。
4. 展开域。
5. 展开您的 FQDN（例如，`example.com`）。
6. 展开组策略对象。

7. 选择默认域策略，打开上下文（右键单击）菜单，然后选择编辑。

> **Note**
>
> 如果支持的域 WorkSpaces 是 AWS Managed Microsoft AD 目录，则无法使用默认域策略来创建 GPO。相反，请选择 *yourdomainname* OU（或该组织下的任何 OU），打开上下文（右键单击）菜单，然后选择在此域中创建 GPO，并将其链接到此处。有关 *yourdomainname* OU 的更多信息，请参阅《AWS Directory Service 管理指南》中的创建的内容。

8. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
9. 打开启用/禁用自动重新连接设置。
10. 在启用/禁用自动重新连接对话框中，选择启用，然后将重新连接超时（秒）设置为所需的超时时间（以秒为单位）
11. 选择 确定。
12. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：

    - 重启 WorkSpace （在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
    - 在管理命令提示符处，输入 **`gpupdate /force`**。

启用或禁用 WSP 的视频输入重定向

默认情况下， WorkSpaces 支持从本地摄像机重定向数据。如果 Windows 需要 WorkSpaces，您可以使用组策略设置来禁用此功能。

在 Windows 上启用或禁用视频输入重定向 WorkSpaces

1. 确保在 WorkSpaces目录的域控制器的中央存储区中安装了最新的 WSP WorkSpaces 组策略管理模板。
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)。
3. 展开林（林：***FQDN***）。
4. 展开域。
5. 展开您的 FQDN（例如，`example.com`）。

6. 展开组策略对象。
7. 选择默认域策略，打开上下文（右键单击）菜单，然后选择编辑。

> **Note**
>
> 如果支持的域 WorkSpaces 是 AWS Managed Microsoft AD 目录，则无法使用默认域策略来创建 GPO。相反，请选择 *yourdomainname* OU（或该组织下的任何 OU），打开上下文（右键单击）菜单，然后选择在此域中创建 GPO，并将其链接到此处。有关 *yourdomainname* OU 的更多信息，请参阅《AWS Directory Service 管理指南》中的创建的内容。

8. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
9. 打开启用/禁用视频输入重定向设置。
10. 在启用/禁用视频输入重定向对话框中，选择启用或禁用。
11. 选择 确定。
12. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：

    - 重启 WorkSpace（在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
    - 在管理命令提示符处，输入 **`gpupdate /force`**。

启用或禁用 WSP 的音频输入重定向

默认情况下， WorkSpaces 支持从本地麦克风重定向数据。如果 Windows 需要 WorkSpaces，您可以使用组策略设置来禁用此功能。

启用或禁用 Windows 的音频输入重定向 WorkSpaces

1. 确保在 WorkSpaces目录的域控制器的中央存储区中安装了最新的 WSP WorkSpaces 组策略管理模板。
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)。
3. 展开林（林：***FQDN***）。
4. 展开域。
5. 展开您的 FQDN（例如，`example.com`）。

6. 展开组策略对象。
7. 选择默认域策略，打开上下文（右键单击）菜单，然后选择编辑。

> **Note**
>
> 如果支持的域 WorkSpaces 是 AWS Managed Microsoft AD 目录，则无法使用默认域策略来创建 GPO。相反，请选择 *yourdomainname* OU（或该组织下的任何 OU），打开上下文（右键单击）菜单，然后选择在此域中创建 GPO，并将其链接到此处。有关 *yourdomainname* OU 的更多信息，请参阅《AWS Directory Service 管理指南》中的创建的内容。

8. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
9. 打开启用/禁用音频输入重定向设置。
10. 在启用/禁用音频输入重定向对话框中，选择启用或禁用。
11. 选择 确定。
12. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：

    - 重启 WorkSpace（在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
    - 在管理命令提示符处，输入 **`gpupdate /force`**。

启用或禁用 WSP 的音频输出重定向

默认情况下， WorkSpaces 会将数据重定向到本地发言人。如果 Windows 需要 WorkSpaces，您可以使用组策略设置来禁用此功能。

启用或禁用 Windows 的音频输出重定向 WorkSpaces

1. 确保最新的 WSP WorkSpaces 组策略管理模板已安装在 WorkSpaces目录的域控制器的中央存储区中。
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)。
3. 展开林（林：***FQDN***）。
4. 展开域。
5. 展开您的 FQDN。例如，`example.com`。

6. 展开组策略对象。
7. 选择默认域策略，打开上下文（右键单击）菜单，然后选择编辑。

> **Note**
>
> 如果支持的域 WorkSpaces 是 AWS Managed Microsoft AD 目录，则无法使用默认域策略来创建 GPO。相反，请选择 *yourdomainname* OU（或该组织下的任何 OU），打开上下文（右键单击）菜单，然后选择在此域中创建 GPO，并将其链接到此处。有关 *yourdomainname* OU 的更多信息，请参阅《AWS Directory Service 管理指南》中的创建的内容。

8. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
9. 打开启用/禁用音频输出重定向设置。
10. 在启用/禁用音频输出重定向对话框中，选择启用或禁用。
11. 选择 确定。
12. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：
    - 重新启动 WorkSpace。在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作 > 重启 WorkSpaces。
    - 在管理命令提示符处，输入 **`gpupdate /force`**。

禁用 WSP 的时区重定向

默认情况下，工作区内的时间设置为镜像用于连接的客户端的时区 WorkSpace。此行为是通过时区重定向控制的。您可能需要关闭时区定向的原因有多种。例如：

- 您的公司希望所有员工在特定时区中工作（即使某些员工在其他时区）。
- 您在 a 中有计划任务 WorkSpace ，这些任务本应在特定时区的特定时间运行。
- 经常出差的用户希望将自己留 WorkSpaces 在一个时区，以保持一致性和个人喜好。

如果 Windows 需要 WorkSpaces，您可以使用组策略设置来禁用此功能。

禁用 Windows 的时区重定向 WorkSpaces

1. 确保在 WorkSpaces目录的域控制器的中央存储区中安装了最新的 WSP WorkSpaces 组策略管理模板。
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)。
3. 展开林（林：*FQDN*）。
4. 展开域。
5. 展开您的 FQDN（例如，`example.com`）。
6. 展开组策略对象。
7. 选择默认域策略，打开上下文（右键单击）菜单，然后选择编辑。

   > **Note**
   >
   > 如果支持的域 WorkSpaces 是 AWS Managed Microsoft AD 目录，则无法使用默认域策略来创建 GPO。相反，请选择 *yourdomainname* OU（或该组织下的任何 OU），打开上下文（右键单击）菜单，然后选择在此域中创建 GPO，并将其链接到此处。有关 *yourdomainname* OU 的更多信息，请参阅《AWS Directory Service 管理指南》中的创建的内容。

8. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
9. 打开启用/禁用时区重定向设置。
10. 在启用/禁用时区重定向对话框中，选择禁用。
11. 选择 确定。
12. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：

    - 重启 WorkSpace （在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
    - 在管理命令提示符处，输入 **`gpupdate /force`**。

13. 将的时区设置 WorkSpaces 为所需的时区。

的时区现在 WorkSpaces 是静态的，不再反映客户端计算机的时区。

配置 WSP 安全设置

对于 WSP，传输中数据使用 TLS 1.2 加密进行加密。默认情况下，允许使用以下所有密码进行加密，客户端和服务器协商使用哪种密码：

- ECDHE-RSA-AES128- GCM-SHA256
- ECDHE-ECDSA-AES128- GCM-SHA256
- ECDHE-RSA-AES256- GCM-SHA384
- ECDHE-ECDSA-AES256- GCM-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA384

对于 Windows WorkSpaces，您可以使用组策略设置来修改 TLS 安全模式以及添加新密码套件或阻止某些密码套件。配置安全设置组策略对话框中提供了这些设置和支持的密码套件的详细说明。

配置 WSP 安全设置

1. 确保在 WorkSpaces目录的域控制器的中央存储区中安装了最新的 WSP WorkSpaces 组策略管理模板。
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)。
3. 展开林（林：***FQDN***）。
4. 展开域。
5. 展开您的 FQDN。例如，`example.com`。
6. 展开组策略对象。
7. 选择默认域策略，打开上下文（右键单击）菜单，然后选择编辑。

> **Note**
>
> 如果支持的域 WorkSpaces 是 AWS Managed Microsoft AD 目录，则无法使用默认域策略来创建 GPO。相反，请选择 *yourdomainname* OU（或该组织下的任何 OU），打开上下文（右键单击）菜单，然后选择在此域中创建 GPO，并将其链接到此处。有关 *yourdomainname* OU 的更多信息，请参阅《AWS Directory Service 管理指南》中的创建的内容。

8. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
9. 打开配置安全设置。
10. 在配置安全设置对话框中，选择启用。添加要允许的密码套件，并删除要屏蔽的密码套件。有关这些设置的更多信息，请参阅配置安全设置对话框中提供的说明。
11. 选择 确定。
12. 组策略设置更改将在的下一次组策略更新之后以及您重新启动 WorkSpace会话之后生效。WorkSpace要应用组策略更改，请执行下列操作之一：
    - 要重启 WorkSpace，请在 Amazon WorkSpaces 控制台中选择 WorkSpace，然后选择操作，重启 WorkSpaces。
    - 在管理命令提示符处，输入 **`gpupdate /force`**。

为 WSP 配置扩展

默认情况下，对 WorkSpaces 扩展的支持处于禁用状态。如果需要，您可以通过以下方式 WorkSpace 将您的配置为使用扩展程序：

- 服务器和客户端 - 为服务器和客户端启用扩展
- 仅限服务器 - 仅为服务器启用扩展
- 仅限客户端 - 仅为客户端启用扩展

对于 Windows WorkSpaces，您可以使用组策略设置来配置扩展程序的使用。

为 WSP 配置扩展

1. 确保最新的 WSP WorkSpaces 组策略管理模板已安装在 WorkSpaces目录的域控制器的中央存储区中。
2. 在目录管理 WorkSpace 或已加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)。
3. 展开林（林：***FQDN***）。
4. 展开域。
5. 展开您的 FQDN。例如，`example.com`
6. 展开组策略对象。
7. 选择默认域策略，打开上下文（右键单击）菜单，然后选择编辑。

> **Note**
>
> 如果支持的域 WorkSpaces 是 AWS Managed Microsoft AD 目录，则无法使用默认域策略来创建 GPO。相反，请选择 *yourdomainname* OU（或该组织下的任何 OU），打开上下文（右键单击）菜单，然后选择在此域中创建 GPO，并将其链接到此处。有关 *yourdomainname* OU 的更多信息，请参阅《AWS Directory Service 管理指南》中的创建的内容。

8. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
9. 打开配置扩展设置。
10. 在配置扩展对话框中，选择启用，然后设置所需的支持选项。选择仅限客户端、服务器和客户端或仅限服务器。
11. 选择 确定。
12. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及您重新启动 WorkSpace会话之后生效。要应用组策略更改，请执行下列操作之一：

    - 重新启动 WorkSpace。在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces。
    - 在管理命令提示符处，输入 **`gpupdate /force`**。

启用或禁用 WSP 的智能卡重定向

默认情况下，Amazon WorkSpaces 不支持使用智能卡进行会话前身份验证或会话中身份验证。会话前身份验证是指在用户登录时执行的智能卡身份验证。 WorkSpaces会话中身份验证是指登录后执行的身份验证。

如果需要，您可以使用组策略设置为 Windows WorkSpaces 启用会话前和会话中身份验证。还必须使用 EnableClientAuthentication API 操作或enable-client-authentication AWS CLI 命令通过 AD Connector 目录设置启用会话前身份验证。有关更多信息，请参阅《AWS Directory Service 管理指南》中的为 AD Connector 启用智能卡身份验证。

> **Note**
>
> 要在 Windows 中使用智能卡 WorkSpaces，需要执行其他步骤。有关更多信息，请参阅 使用智能卡进行身份验证。

启用或禁用 Windows 的智能卡重定向 WorkSpaces

1. 确保在 WorkSpaces目录的域控制器的中央存储区中安装了最新的 WSP WorkSpaces 组策略管理模板。
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)。
3. 展开林（林：*FQDN*）。
4. 展开域。
5. 展开您的 FQDN（例如，`example.com`）。
6. 展开组策略对象。
7. 选择默认域策略，打开上下文（右键单击）菜单，然后选择编辑。

   > **Note**
   >
   > 如果支持的域 WorkSpaces 是 AWS Managed Microsoft AD 目录，则无法使用默认域策略来创建 GPO。相反，请选择 *yourdomainname* OU（或该组织下的任何 OU），打开上下文（右键单击）菜单，然后选择在此域中创建 GPO，并将其链接到此处。有关 *yourdomainname* OU 的更多信息，请参阅《AWS Directory Service 管理指南》中的创建的内容。

8. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
9. 打开启用/禁用智能卡重定向设置。
10. 在启用/禁用智能卡重定向对话框中，选择启用或禁用。
11. 选择 确定。
12. 组策略设置更改将在会 WorkSpace话重新启动后生效。要应用组策略更改，请重启 WorkSpace（在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。

为 WSP 启用或禁用 WebAuthn (FIDO2) 重定向

默认情况下，Amazon WorkSpaces 允许使用 WebAuthn 身份验证器进行会话内身份验证。会话内身份验证是指登录后执行的 WebAuthn 身份验证，并由在会话中运行的 Web 应用程序请求的身份验证。

要求

WebAuthn (FIDO2) WSP 的重定向需要满足以下条件：

- WSP 主机代理版本 2.0.0.1425 或更高版本

- WorkSpaces 客户：
  - Linux Ubuntu 22.04 2023.3 或更高版本
  - Windows 5.19.0 或更高版本
  - Mac 客户端 5.19.0 或更高版本
- WorkSpaces 正在运行 Amazon DCV WebAuthn 重定向扩展程序时安装的 Web 浏览器：
  - 谷歌浏览器 116+
  - 微软 Edge 116+

在 Windows 上启用或禁用 WebAuthn (FIDO2) 重定向 WorkSpaces

如果需要，您可以使用组策略设置启用或禁用对 Windows 身份 WebAuthn 验证器进行会话内身份验证 WorkSpaces 的支持。如果您启用或未配置此设置，则将启用 WebAuthn 重定向，并且用户可以在远程中使用本地身份验证器。 WorkSpace

启用该功能后，会话中来自浏览器的所有 WebAuthn 请求都将重定向到本地客户端。用户可以使用 Windows Hello 或本地连接的安全设备（例如 YubiKey 其他符合 FIDO2 标准的身份验证器）来完成身份验证过程。

在 Windows 上启用或禁用 WebAuthn (FIDO2) 重定向 WorkSpaces

1. 确保在 WorkSpaces目录的域控制器的中央存储区中安装了最新的 WSP WorkSpaces 组策略管理模板。
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)。
3. 展开林（林：*FQDN*）。
4. 展开域。
5. 展开您的 FQDN（例如，`example.com`）。
6. 展开组策略对象。
7. 选择默认域策略，打开上下文（右键单击）菜单，然后选择编辑。

> **Note**
>
> 如果支持的域 WorkSpaces 是 AWS Managed Microsoft AD 目录，则无法使用默认域策略来创建 GPO。相反，请选择 *yourdomainname* OU（或该组织下的任何 OU），打开上下文（右键单击）菜单，然后选择在此域中创建 GPO，并将其链接到此处。有关

yourdomainname OU 的更多信息，请参阅《AWS Directory Service 管理指南》中的创建的内容。

8. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
9. 打开 “启用/禁用 WebAuthn 重定向” 设置。
10. 在 “启用/禁用 WebAuthn 重定向” 对话框中，选择 “启用” 或 “禁用”。
11. 选择 确定。
12. 组策略设置更改将在会 WorkSpace 话重新启动后生效。要应用组策略更改，请转至 Amazon WorkSpaces 控制台并选择，重新启动 WorkSpace。 WorkSpace 然后，选择操作，重新启动 WorkSpaces ）。

安装 Amazon DCV WebAuthn 重定向扩展

启用该功能 WebAuthn 后，用户需要安装 Amazon DCV WebAuthn 重定向扩展才能使用该功能，方法是执行以下任一操作：

- 系统将提示您的用户在其浏览器中启用浏览器扩展程序。

> **Note**
>
> 这是一次性的浏览器提示。当您将 WSP 代理版本更新到 2.0.0.1425 或更高版本时，您的用户将收到通知。如果您的最终用户不需要 WebAuthn 重定向，他们只需从浏览器中删除扩展程序即可。您也可以使用以下 GPO 策略阻止 WebAuthn 重定向扩展安装提示。

- 您可以使用以下 GPO 策略为用户强制安装重定向扩展程序。如果您启用 GPO 策略，则当您的用户启动支持的 Internet 访问权限的浏览器时，扩展程序将自动安装。
- 你的用户可以使用 Microsoft Edge 插件或 Chrome 网上应用店手动安装扩展程序。

使用组策略管理和安装浏览器扩展程序

您可以使用组策略安装 Amazon DCV WebAuthn 重定向扩展，既可以从您的域集中安装加入 Active Directory (AD) 域的会话主机，也可以使用本地组策略编辑器安装每个会话主机。此过程将根据您使用的浏览器而有所不同。

适用于微软 Edge

1. 下载并安装 Microsoft Edge 管理模板。

2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)。
3. 展开林（林：***FQDN***）。
4. 展开域。
5. 展开您的 FQDN（例如，`example.com`）。
6. 展开组策略对象。
7. 选择默认域策略，打开上下文（右键单击）菜单，然后选择编辑。
8. 选择计算机配置、管理模板、Microsoft Edge 和扩展
9. 打开配置分机管理设置并将其设置为启用。
10. 在 “配置分机管理设置” 下，输入以下内容：

```
{"ihejeaahjpbegmaaegiikmlphghlfmeh":
{"installation_mode":"force_installed","update_url":"https://edge.microsoft.com/
extensionwebstorebase/v1/crx"}}
```

11. 选择 确定。
12. 组策略设置更改将在会 WorkSpace 话重新启动后生效。要应用组策略更改，请转至 Amazon WorkSpaces 控制台并选择，重新启动 WorkSpace。 WorkSpace 然后，选择操作，重新启动 WorkSpaces）。

> **Note**
>
> 您可以通过应用以下配置管理设置来阻止扩展程序的安装：
>
> ```
> {"ihejeaahjpbegmaaegiikmlphghlfmeh":
> {"installation_mode":"blocked","update_url":"https://edge.microsoft.com/
> extensionwebstorebase/v1/crx"}}
> ```

适用于谷歌浏览器

1. 下载并安装谷歌浏览器管理模板。如需了解详情，请参阅在托管电脑上设置 Chrome 浏览器政策。
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)。

3. 展开林（林：***FQDN***）。
4. 展开域。
5. 展开您的 FQDN（例如，example.com）。
6. 展开组策略对象。
7. 选择默认域策略，打开上下文（右键单击）菜单，然后选择编辑。
8. 选择 “计算机配置”、“管理模板”、“谷歌浏览器” 和 “扩展程序”
9. 打开配置分机管理设置并将其设置为启用。
10. 在 “配置分机管理设置” 下，输入以下内容：

```
{"mmiioagbgnbojdbcjoddlefhmcocfpmn":
{ "installation_mode":"force_installed","update_url":"https://clients2.google.com/
service/update2/crx"}}
```

11. 选择 确定。
12. 组策略设置更改将在会 WorkSpace 话重新启动后生效。要应用组策略更改，请转至 Amazon WorkSpaces 控制台并选择，重新启动 WorkSpace。 WorkSpace 然后，选择操作，重新启动 WorkSpaces）。

> **Note**
>
> 您可以通过应用以下配置管理设置来阻止扩展程序的安装：
>
> ```
> {"mmiioagbgnbojdbcjoddlefhmcocfpmn":
> { "installation_mode":"blocked","update_url":"https://clients2.google.com/
> service/update2/crx"}}
> ```

启用或禁用 WSP 屏幕锁定时断开会话连接

如果需要，可以在检测到 Windows 锁屏时断开用户的 WorkSpaces 会话。要从 WorkSpaces 客户端重新连接，用户可以使用自己的密码或智能卡进行身份验证，具体取决于为其 WorkSpaces启用了哪种类型的身份验证。

默认情况下，该组策略设置处于禁用状态。如果需要，您可以使用组策略设置启用在检测到 Windows 锁屏时断 WorkSpaces 开会话连接。

> **Note**
>
> - 此组策略设置适用于密码身份验证的会话和智能卡身份验证的会话。
> - 要在 Windows 中使用智能卡 WorkSpaces，需要执行其他步骤。有关更多信息，请参阅 使用智能卡进行身份验证。

启用或禁用 Windows 屏幕锁定时断开连接会话 WorkSpaces

1. 确保在 WorkSpaces目录的域控制器的中央存储区中安装了最新的 WSP WorkSpaces 组策略管理模板。
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)。
3. 展开林（林：***FQDN***）。
4. 展开域。
5. 展开您的 FQDN（例如，`example.com`）。
6. 展开组策略对象。
7. 选择默认域策略，打开上下文（右键单击）菜单，然后选择编辑。

   > **Note**
   >
   > 如果支持的域 WorkSpaces 是 AWS Managed Microsoft AD 目录，则无法使用默认域策略来创建 GPO。相反，请选择 *yourdomainname* OU（或该组织下的任何 OU），打开上下文（右键单击）菜单，然后选择在此域中创建 GPO，并将其链接到此处。有关 *yourdomainname* OU 的更多信息，请参阅《AWS Directory Service 管理指南》中的创建的内容。

8. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
9. 打开启用/禁用屏幕锁定时断开会话连接设置。
10. 在启用/禁用屏幕锁定时断开会话连接对话框中，选择启用或禁用。
11. 选择 确定。
12. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：

- 重启 WorkSpace （ 在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces ）。
- 在管理命令提示符处，输入 **gpupdate /force**。

启用或禁用 WSP 的间接显示驱动程序 (IDD)

默认情况下， WorkSpaces 支持使用间接显示驱动程序 (IDD)。如果 Windows 需要 WorkSpaces，您可以使用组策略设置来禁用此功能。

启用或禁用 Windows 的间接显示驱动程序 (IDD) WorkSpaces

1. 确保在 WorkSpaces 目录的域控制器的中央存储区中安装了最新的 WSP WorkSpaces 组策略管理模板。
2. 在目录管理 WorkSpace 或加入目录的 Amazon Elastic Compute Cloud 实例上，打开组策略管理工具 (gpmc .msc)。 WorkSpaces
3. 扩大森林（ 森林:FQDN ）。
4. 展开域。
5. 展开您的 FQDN（ 例如，`example.com` ）。
6. 展开组策略对象。
7. 选择默认域策略，右键单击菜单打开上下文，然后选择编辑。

> **Note**
>
> 如果支持的域 WorkSpaces 是 AWS 托管 Microsoft AD 目录，则无法使用默认域策略来创建 GPO。而是选择该域名下的`yourdomainname`组织单位 (OU) 或任何 OU，右键单击菜单打开上下文，然后选择在此域中创建 GPO，然后将其链接到此处。有关 `yourdomainname` OU 的更多信息，请参阅《Director y Servic AWS e 管理指南》中的创建内容。

8. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
9. 打开 “启用 AWS 间接显示驱动程序” 设置。
10. 在 “启用 AWS 间接显示驱动程序” 对话框中，选择 “启用” 或 “禁用”。
11. 选择 确定。
12. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：

a. 重新启动 WorkSpace（在 WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重新启动 WorkSpaces）。

b. 在管理命令提示符处，输入 `gpupdate /force`。

配置 WSP 的显示设置

WorkSpaces 允许您配置多种不同的显示设置，包括最大帧速率、最低图像质量、最大图像质量和 YUV 编码。根据所需的图像质量、响应能力和色彩准确度，调整这些设置。

默认情况下，最大帧速率值为 25。最大帧速率值用于指定允许的最大每秒帧数 (fps)。值 0 表示无限制。

默认情况下，最低图像质量值为 30。可以对最低图像质量进行优化，以获得最佳图像响应能力或最佳图像质量。为了获得最佳响应能力，请减少最低质量。要获得最佳质量，请增加最低质量。

- 最佳响应能力的理想值介于 30 和 90 之间。
- 最佳质量的理想值介于 60 和 90 之间。

默认情况下，最大图像质量值为 80。最大图像质量不会影响图像的响应能力或质量，但会设置最大值以限制网络使用量。

默认情况下，图像编码设置为 YUV420。选择启用 YUV444 编码，可启用 YUV444 编码以实现高色彩精度。

对于 Windows WorkSpaces，您可以使用组策略设置来配置最大帧速率、最低图像质量和最大图像质量值。

配置 Windows 的显示设置 WorkSpaces

1. 确保最新的 WSP WorkSpaces 组策略管理模板已安装在 WorkSpaces目录的域控制器的中央存储区中。
2. 在目录管理 WorkSpace 或已加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)。
3. 展开林（林：***FQDN***）。
4. 展开域。
5. 展开您的 FQDN（例如，`example.com`）。

6. 展开组策略对象。
7. 选择默认域策略，打开上下文（右键单击）菜单，然后选择编辑。

> **Note**
>
> 如果支持的域 WorkSpaces 是 AWS Managed Microsoft AD 目录，则无法使用默认域策略来创建 GPO。相反，请选择 *yourdomainname* OU（或该组织下的任何 OU），打开上下文（右键单击）菜单，然后选择在此域中创建 GPO，并将其链接到此处。有关 *yourdomainname* OU 的更多信息，请参阅《AWS Directory Service 管理指南》中的创建的内容。

8. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
9. 打开配置显示设置设置。
10. 在配置显示设置对话框中，选择启用，然后将最大帧速率 (fps)、最低图像质量和最大图像质量值设置为所需的级别。
11. 选择 确定。
12. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及您重新启动 WorkSpace会话之后生效。要应用组策略更改，请执行下列操作之一：

    - 重启 WorkSpace. Amazon WorkSpaces 控制台，选择 WorkSpace，然后选择操作，重启 WorkSpaces
    - 在管理命令提示符处，输入 **`gpupdate /force`**。

为 WSP 的仅 AWS 虚拟显示驱动程序启用或禁用 vSync

默认情况下， WorkSpaces 支持对仅限 AWS 虚拟显示屏的驱动程序使用 vSync 功能。如果 Windows 需要 WorkSpaces，您可以使用组策略设置来禁用此功能。

启用或禁用 Windows 版垂直同步 WorkSpaces

1. 确保最新的 WSP WorkSpaces 组策略管理模板已安装在 WorkSpaces 目录的域控制器的中央存储中。
2. 在目录管理 WorkSpace 或加入目录的 Amazon Elastic Compute Cloud 实例上，打开组策略管理工具 (gpmc .msc)。 WorkSpaces
3. 扩大森林（森林:FQDN）。
4. 展开域。

5. 展开您的 FQDN（例如，`example.com`）。
6. 展开组策略对象。
7. 选择默认域策略，右键单击菜单打开上下文，然后选择编辑。

> **Note**
>
> 如果支持的域 WorkSpaces 是 AWS 托管 Microsoft AD 目录，则无法使用默认域策略来创建 GPO。而是选择该域名下的`yourdomainname`组织单位 (OU) 或任何 OU，右键单击菜单打开上下文，然后选择在此域中创建 GPO，然后将其链接到此处。有关 `yourdomainname` OU 的更多信息，请参阅《Director y S ervic AWS e 管理指南》中的创建内容。

8. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
9. 打开 “仅限 AWS 虚拟显示器驱动程序” 设置的 “启用 vSync” 功能。
10. 在 “仅 AWS 虚拟显示器驱动程序” 对话框的 “启用 vSync” 功能中，选择 “启用” 或 “禁用”。
11. 选择 确定。
12. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行以下操作：

    a. WorkSpace 通过执行以下任一操作重新启动：

       i. 选项 1-在 WorkSpaces 控制台中，选择 WorkSpace 要重新启动的。然后，选择操作，重新启动 WorkSpaces。

       ii. 选项 2-在管理命令提示符下，输入`gpupdate /force`。

    b. 要应用设置 WorkSpace ，请重新连接到。

    c. 再次重启工作区。

配置 WSP 的日志详细程度

默认情况下，WSP 的日志详细级别设置 WorkSpaces 为 Info。您可以将日志级别设置为详细程度级别（从最不详细到最详细），详见此处：

- 错误 - 最不详细
- Warning
- 信息 - 默认

- 调试 - 最详细

对于 Windows WorkSpaces，您可以使用组策略设置来配置日志详细级别。

为 Windows 配置日志详细级别 WorkSpaces

1. 确保最新的 WSP WorkSpaces 组策略管理模板已安装在 WorkSpaces目录的域控制器的中央存储区中。
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)。
3. 展开林（林：*FQDN*）。
4. 展开域。
5. 展开您的 FQDN。例如，`example.com`。
6. 展开组策略对象。
7. 选择默认域策略，打开上下文（右键单击）菜单，然后选择编辑。

   > **Note**
   >
   > 如果支持的域 WorkSpaces 是 AWS Managed Microsoft AD 目录，则无法使用默认域策略来创建 GPO。相反，请选择 *yourdomainname* OU（或该组织下的任何 OU），打开上下文（右键单击）菜单，然后选择在此域中创建 GPO，并将其链接到此处。有关 *yourdomainname* OU 的更多信息，请参阅《AWS Directory Service 管理指南》中的创建的内容。

8. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
9. 打开配置日志详细程度设置。
10. 在配置日志详细程度对话框中，选择启用，然后将日志详细程度级别设置为调试、错误、信息或警告。
11. 选择 确定。
12. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及您重新启动 WorkSpace会话之后生效。要应用组策略更改，请执行下列操作之一：

    - 重新启动 WorkSpace。在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces。
    - 在管理命令提示符处，输入 **`gpupdate /force`**。

为 PCoIP 安装组策略管理模板

要在使用 PCoIP 协议 WorkSpaces 时使用特定于 Amazon 的组策略设置，您必须添加适用于您的 PCoIP 代理版本（32 位或 64 位）的组策略管理模板。 WorkSpaces

> **Note**
>
> 如果您混合使用 32 位和 64 位代理，则可以对 32 位代理使用组策略管理模板，并且您的组策略设置将同时应用于 32 位和 64 位代理。 WorkSpaces 当所有人 WorkSpaces 都在使用 64 位代理时，可以切换到使用 64 位代理的管理模板。

确定 WorkSpaces 您使用的是 32 位代理还是 64 位代理

1. 登录到 a WorkSpace，然后通过选择 “查看”、“发送 Ctrl + Alt + Delete” 或右键单击任务栏并选择 “任务管理器” 来打开任务管理器。
2. 在任务管理器中，转到详细信息选项卡，右键单击列标题，然后选择选择列。
3. 在选择列对话框中，选择平台，然后选择确定。
4. 在详细信息选项卡上，查找 `pcoip_agent.exe`，然后在平台列中检查其值，以确定 PCoIP 代理是 32 位还是 64 位。（您可能会看到 32 位和 64 位 WorkSpaces 组件的混合；这是正常现象。）

为 PCoIP 安装组策略管理模板（32 位）

要使用与 32 位 PCoIP 代理一起使用 PCoIP 协议 WorkSpaces 时特有的组策略设置，必须安装 PCoIP 的组策略管理模板。在目录管理 WorkSpace 或加入目录的 Amazon EC2 实例上执行以下步骤。

有关使用.adm 文件的更多信息，请参阅 Microsoft 文档中的管理组策略管理模板 (.adm) 文件的建议。

为 PCoIP 安装组策略管理模板

1. 在正在运行的 Windows WorkSpace 中，复制`C:\Program Files (x86)\Teradici\PCoIP Agent\configuration`目录中的`pcoip.adm`文件。
2. 在目录管理 WorkSpace 或加入您 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)，然后导航到您的域中包含您的 WorkSpaces 计算机账户的组织单位。
3. 打开计算机账户组织单位对应的上下文 (右键单击) 菜单，然后选择在这个域中创建 GPO 并在此处链接...。
4. 在 “新建 GPO” 对话框中，输入 GPO 的描述性名称，例如WorkSpaces 计算机策略，并将 Source Starter GPO 设置为（无）。选择 确定。

5. 打开新 GPO 的上下文（右键单击）菜单，然后选择 Edit (编辑)。
6. 在组策略管理编辑器中，依次选择计算机配置、策略和管理模板。从主菜单中依次选择操作和添加/删除模板。
7. 在添加/删除模板对话框中，单击添加，选择之前复制的 pcoip.adm 文件，然后依次选择打开和关闭。
8. 关闭组策略管理编辑器。现在，您可以使用此 GPO 修改特定于的组策略设置。 WorkSpaces

验证管理模板文件是否已正确安装

1. 在目录管理 WorkSpace 或已加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)，导航到您的 WorkSpaces 计算机账户并选择相应的 WorkSpaces GPO。在主菜单中依次选择操作和编辑。
2. 在组策略管理编辑器中，依次选择 计算机配置、策略、管理模板、经典管理模板 和 PCoIP Session Variables。
3. 现在，在使用 PCoIP WorkSpaces 时，您可以使用此 PCoIP 会话变量组策略对象来修改亚马逊特有的组策略设置。

> **Note**
>
> 要允许用户覆盖您的设置，请选择可覆盖的管理员设置；否则，请选择不可覆盖的管理员设置。

为 PCoIP 安装组策略管理模板（64 位）

要使用使用 PCoIP 协议 WorkSpaces 时特有的组策略设置，必须将 PCoIP 的组策略管理模板PCoIP.admx和PCoIP.adml文件添加到目录的域控制器的中央存储区。 WorkSpaces有关 .admx 和 .adml 文件的更多信息，请参阅如何在 Windows 中创建和管理组策略管理模板的中央存储。

以下过程介绍了如何创建中央存储并向其中添加管理模板文件。在目录管理 WorkSpace 或加入目录的 Amazon EC2 实例上执行以下步骤。 WorkSpaces

为 PCoIP 安装组策略管理模板文件

1. 在正在运行的 Windows WorkSpace 中，复制C:\Program Files\Teradici\PCoIP Agent\configuration\policyDefinitions目录中的PCoIP.admx和PCoIP.adml文件。PCoIP.adml 文件位于该目录的 en-US 子文件夹中。

2. 在目录管理 WorkSpace 或已加入 WorkSpaces 目录的 Amazon EC2 实例上，打开 Windows 文件资源管理器，然后在地址栏中输入贵组织的完全限定域名 (FQDN)，例如\\example.com。
3. 打开 sysvol 文件夹。
4. 打开带有 *FQDN* 名称的文件夹。
5. 打开 Policies 文件夹。您现在应该位于 *FQDN*\sysvol*FQDN*\Policies 中。
6. 如果该文件尚不存在，请创建一个名为 PolicyDefinitions 的文件夹。
7. 打开 PolicyDefinitions 文件夹。
8. 将 PCoIP.admx 文件复制到 *FQDN*\sysvol*FQDN*\Policies\PolicyDefinitions 文件夹中。
9. 在 PolicyDefinitions 文件夹中创建名为 en-US 的文件夹。
10. 打开 en-US 文件夹。
11. 将 PCoIP.adml 文件复制到 *FQDN*\sysvol*FQDN*\Policies\PolicyDefinitions\en-US 文件夹中。

验证管理模板文件是否已正确安装

1. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)。
2. 展开林（林：***FQDN***）。
3. 展开域。
4. 展开您的 FQDN（例如，example.com）。
5. 展开组策略对象。
6. 选择默认域策略，打开上下文（右键单击）菜单，然后选择编辑。

> **Note**
>
> 如果支持的域 WorkSpaces 是 AWS Managed Microsoft AD 目录，则无法使用默认域策略来创建 GPO。相反，您必须在具有委派权限的域容器下创建和链接 GPO。
> 使用创建目录时 AWS Managed Microsoft AD， AWS Directory Service 会在域根目录下创建一个####组织单位 (OU)。此 OU 的名称基于您在创建目录时键入的 NetBIOS 名称。如果您未指定 NetBIOS 名称，则此名称将默认为您目录 DNS 名称的第一部分（例如，如果目录 DNS 名称为 corp.example.com，则 NetBIOS 名称将为 corp）。

要创建 GPO，请改为选择默认域策略，选择 *yourdomainname* OU（或该组织下的任何 OU），打开上下文（右键单击）菜单，然后选择在此域中创建 GPO，并将其链接到此处。
有关 *yourdomainname* OU 的更多信息，请参阅《AWS Directory Service 管理指南》中的创建的内容。

7. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板和 PCoIP 会话变量。
8. 现在，您可以使用此 PCoIP 会话变量组策略对象来修改使用 PCoIP WorkSpaces 时特有的组策略设置。

> **Note**
>
> 要允许用户覆盖您的设置，请选择可覆盖的管理员设置；否则，请选择不可覆盖的管理员设置。

管理 PCoIP 的组策略设置

使用组策略设置来管理使用 PCo WorkSpaces IP 的 Windows。

配置对 PCoIP 的打印机支持

默认情况下， WorkSpaces 启用基本远程打印，它提供的打印功能有限，因为它在主机端使用通用打印机驱动程序来确保打印兼容。

Windows 客户端的高级远程打印让您可以使用打印机的特定功能（如双面打印），但需要在主机端安装匹配的打印机驱动程序。

远程打印实施为虚拟通道。如果虚拟通道被禁用，远程打印无法正常工作。

对于 Windows WorkSpaces，您可以根据需要使用组策略设置来配置打印机支持。

配置打印机支持

1. 确保已安装最新的 PCoIP WorkSpaces 组策略管理模板（32 位）或 PCoIP（64 位）的WorkSpaces 组策略管理模板（64 位）。
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc) 并导航到 PCoIP 会话变量。
3. 打开配置远程打印设置。

4. 在 Configure remote printing (配置远程打印) 对话框中，执行下列操作之一：
   - 要启用高级远程打印，请选择已启用，然后在选项、Configure remote printing (配置远程打印) 下，选择 Basic and Advanced printing for Windows clients (适用于 Windows 客户端的基本和高级打印)。要自动使用客户端计算机的当前默认打印机，选择 Automatically set default printer (自动设置默认打印机)。
   - 要禁用打印，请选择 Enabled (已启用)，然后在 Options (选项)、Configure remote printing (配置远程打印) 下选择 Printing disabled (已禁用打印)。
5. 选择 确定。
6. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：
   - 重启 WorkSpace （在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces ）。
   - 在管理命令提示符处，输入 **`gpupdate /force`**。

默认情况下，本地打印机自动重定向被禁用。您可以使用组策略设置来启用此功能，以便每次连接到您的本地打印机时都将您的本地打印机设置为默认打印机 WorkSpace。

> **Note**
>
> 本地打印机重定向不适用于亚马逊 Linux WorkSpaces。

启用本地打印机自动重定向

1. 确保已安装最新的 PCoIP WorkSpaces 组策略管理模板（32 位）或 PCoIP（64 位）的WorkSpaces 组策略管理模板（64 位）。
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc) 并导航到 PCoIP 会话变量。
3. 打开配置远程打印设置。
4. 选择启用，然后在选项、配置远程打印下，选择以下一个选项：
   - 适用于 Windows 客户端的基本和高级打印
   - 基本打印
5. 选择自动设置默认打印机，然后选择确定。

6. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：

   - 重启 WorkSpace （在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
   - 在管理命令提示符处，输入 **gpupdate /force**。

启用或禁用 PCoIP 的剪贴板重定向（复制/粘贴）

默认情况下， WorkSpaces 支持剪贴板重定向。如果 Windows 需要 WorkSpaces，您可以使用组策略设置来禁用此功能。

要启用或禁用剪贴板重定向

1. 确保已安装最新的 PCoIP WorkSpaces 组策略管理模板（32 位）或 PCoIP（64 位）的WorkSpaces 组策略管理模板（64 位）。
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc) 并导航到 PCoIP 会话变量。
3. 打开 Configure clipboard redirection 设置。
4. 在配置剪贴板重定向对话框中，选择启用，然后选择以下设置之一以确定允许剪贴板重定向的方向。完成后，选择确定。

   - 双向禁用
   - 仅对客户端（WorkSpace 本地计算机）启用代理
   - 仅启用客户端到代理（本地计算机到 WorkSpace）
   - 双向启用
5. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：

   - 重启 WorkSpace （在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
   - 在管理命令提示符处，输入 **gpupdate /force**。

已知限制

启用剪贴板重定向后 WorkSpace，如果您从 Microsoft Office 应用程序中复制大于 890 KB 的内容，则该应用程序可能会变慢或在长达 5 秒钟内没有响应。

为 PCoIP 设置会话恢复超时

网络连接中断时，您的活动 WorkSpaces 客户端会话将断开连接。 WorkSpaces 如果网络连接在一定时间内恢复，则适用于 Windows 和 macOS 的客户端应用程序会尝试自动重新连接会话。默认的会话恢复超时时间为 20 分钟，但您可以修改该值 WorkSpaces ，因为该值由您的域的组策略设置控制。

要设置自动会话恢复超时值

1. 确保已安装最新的 PCoIP WorkSpaces 组策略管理模板（32 位）或 PCoIP（64 位）的WorkSpaces 组策略管理模板（64 位）。
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc) 并导航到 PCoIP 会话变量。
3. 打开 Configure Session Automatic Reconnection Policy 设置。
4. 在 Configure Session Automatic Reconnection Policy 对话框中，选择 Enabled，将 Configure Session Automatic Reconnection Policy 选项设置为所需的超时 (以分钟为单位)，然后选择 OK。
5. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：

   - 重启 WorkSpace （在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
   - 在管理命令提示符处，输入 **`gpupdate /force`**。

启用或禁用 PCoIP 的音频输入重定向

默认情况下，Amazon WorkSpaces 支持从本地麦克风重定向数据。如果 Windows 需要 WorkSpaces，您可以使用组策略设置来禁用此功能。

> **Note**
>
> 如果您的组策略设置限制了用户的本地登录 WorkSpaces，则音频输入将无法在您的。 WorkSpaces如果删除该组策略设置，则下次重新启动后将启用音频输入功能。 WorkSpace有关此组策略设置的更多信息，请参阅 Microsoft 文档中的允许本地登录。

启用或禁用音频输入重定向

1. 确保已安装最新的 PCoIP WorkSpaces 组策略管理模板（32 位）或 PCoIP（64 位）的WorkSpaces 组策略管理模板（64 位）。

2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc) 并导航到 PCoIP 会话变量。
3. 打开启用/禁用 PCoIP 会话的音频设置。
4. 在启用/禁用 PCoIP 会话的音频对话框中，选择启用或禁用。
5. 选择 确定。
6. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：
   - 重启 WorkSpace （在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
   - 在管理命令提示符处，输入 **`gpupdate /force`**。

禁用 PCoIP 的时区重定向

默认情况下，工作区内的时间设置为镜像用于连接的客户端的时区 WorkSpace。此行为是通过时区重定向控制的。您可能需要关闭时区定向的原因有多种：

- 您的公司希望所有员工在特定时区中工作（即使某些员工在其他时区）。
- 您在 a 中有计划任务 WorkSpace ，这些任务本应在特定时区的特定时间运行。
- 经常出差的用户希望将自己留 WorkSpaces 在一个时区，以保持一致性和个人喜好。

如果 Windows 需要 WorkSpaces，您可以使用组策略设置来禁用此功能。

禁用时区重定向

1. 确保已安装最新的 PCoIP WorkSpaces 组策略管理模板（32 位）或 PCoIP（64 位）的WorkSpaces 组策略管理模板（64 位）。
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc) 并导航到 PCoIP 会话变量。
3. 打开配置时区重定向设置。
4. 在配置时区重定向对话框中，选择禁用。
5. 选择 确定。
6. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：

- 重启 WorkSpace（在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
- 在管理命令提示符处，输入 **gpupdate /force**。

7. 将的时区设置 WorkSpaces 为所需的时区。

的时区现在 WorkSpaces 是静态的，不再反映客户端计算机的时区。

配置 PCoIP 安全设置

对于 PCoIP，传输中数据使用 TLS 1.2 加密和 SigV4 请求签名进行加密。PCoIP 协议使用加密的 UDP 流量和 AES 加密来传输像素。使用端口 4172（TCP 和 UDP）的流式传输连接通过 AES-128 和 AES-256 密码进行加密，但加密默认为 128 位。您可以使用配置 PCoIP 安全设置组策略设置，将此默认值更改为 256 位。

您还可以使用此组策略设置来修改 TLS 安全模式以及屏蔽某些密码套件。配置 PCoIP 安全设置组策略对话框中提供了这些设置和支持的密码套件的详细说明。

配置 PCoIP 安全设置

1. 确保已安装最新的 PCoIP WorkSpaces 组策略管理模板（32 位）或 PCoIP（64 位）的WorkSpaces 组策略管理模板（64 位）。
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc) 并导航到 PCoIP 会话变量。
3. 打开配置 PCoIP 安全设置设置。
4. 在配置 PCoIP 安全设置对话框中，选择启用。要将流式传输流量的默认加密设置为 256 位，请转到 PCoIP 数据加密密码选项，然后选择仅限 AES-256-GCM。
5. （可选）调整 TLS 安全模式设置，然后列出要屏蔽的所有密码套件。有关这些设置的更多信息，请参阅配置 PCoIP 安全设置对话框中提供的说明。
6. 选择 确定。
7. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：

   - 重启 WorkSpace（在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
   - 在管理命令提示符处，输入 **gpupdate /force**。

为 U2F 启用 USB 重定 YubiKey向

> **Note**
>
> 亚马逊 WorkSpaces 目前仅支持 YubiKey U2F 的 USB 重定向。其他类型的 USB 设备可能会被重定向，但它们不受支持，也可能无法正常运行。

为 U2F 启用 USB 重定 YubiKey 向

1. 确保已安装最新的 PCoIP WorkSpaces 组策略管理模板（32 位）或 PCoIP（64 位）的WorkSpaces 组策略管理模板（64 位）。
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc) 并导航到 PCoIP 会话变量。
3. 打开启用/禁用 PCoIP 会话的 USB 设置。
4. 选择启用，然后选择确定。
5. 打开配置 PCoIP USB 允许和不允许的设备规则设置。
6. 选择启用，然后在输入 USB 授权表（最多十条规则）下，配置您的 USB 设备允许列表规则。
   - 授权规则 - 110500407。此值是供应商 ID (VID) 和产品 ID (PID) 的组合。VID/PID 组合的格式为 1xxxxyyyy，其中 xxxx 是十六进制格式的 VID，yyyy 是十六进制格式的 PID。在本例中，1050 是 VID，0407 是 PID。如需了解更多 YubiKey USB 值，请参阅 YubiKey USB ID 值。
7. 在输入 USB 授权表（最多十条规则）下，配置您的 USB 设备屏蔽列表规则。
   - 对于取消授权规则，设置一个空字符串。这意味着仅允许授权列表中的 USB 设备。

   > **Note**
   >
   > 您最多可以定义 10 条 USB 授权规则和最多 10 条 USB 取消授权规则。使用竖线 (|) 字符分隔多个规则。有关授权/取消授权规则的详细信息，请参阅适用于 Windows 的 Teradici PCoIP 标准代理。
8. 选择 确定。
9. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：

- 重启 WorkSpace （在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
- 在管理命令提示符处，输入 **`gpupdate /force`**。

设置生效后，除非通过 USB 设备规则设置配置了限制， WorkSpaces 否则所有支持的 USB 设备都可以重定向到。

设置 Kerberos 票证的最长使用期限

如果您尚未禁用 Windows 的 “记住我” 功能 WorkSpaces，则您的 WorkSpace 用户可以使用其 WorkSpaces 客户端应用程序中的 “记住我” 或 “让我保持登录状态” 复选框来保存其凭据。此功能允许用户在客户端应用程序保持运行 WorkSpaces时轻松连接到他们的。他们的凭证安全地缓存到 Kerberos 票证中，时间可达其最长使用期限。

如果您 WorkSpace 使用 AD Connector 目录，则可以按照微软 Windows 文档中 WorkSpaces 用户票证的最长使用寿命中的步骤通过组策略修改用户的 Kerberos 票证的最大生命周期。

要启用或禁用 Remember Me 功能，请参阅 为您的用户启用自助 WorkSpace管理功能。

配置用于互联网访问的设备代理服务器设置

默认情况下， WorkSpaces 客户端应用程序使用在设备操作系统设置中为 HTTPS（端口 443）流量指定的代理服务器。Amazon WorkSpaces 客户端应用程序使用 HTTPS 端口进行更新、注册和身份验证。

> **Note**
>
> 不支持需要使用登录凭证进行身份验证的代理服务器。

您可以按照 Microsoft 文档中配置设备代理和互联网连接设置中的步骤， WorkSpaces 通过组策略为 Windows 配置设备代理服务器设置。

有关在 WorkSpaces Windows 客户端应用程序中配置代理设置的更多信息，请参阅 Amazon WorkSpaces 用户指南中的代理服务器。

有关在 WorkSpaces macOS 客户端应用程序中配置代理设置的更多信息，请参阅 A mazon WorkSpaces 用户指南中的代理服务器。

有关在 WorkSpaces Web Access 客户端应用程序中配置代理设置的更多信息，请参阅 Amazon WorkSpaces 用户指南中的代理服务器。

代理桌面流量

对于 PCoIP WorkSpaces，桌面客户端应用程序不支持使用代理服务器，也不支持 TLS 解密和检查 UDP 中的端口 4172 流量（用于桌面流量）。它们需要直接连接到端口 4172。

对于 WSP WorkSpaces， WorkSpaces Windows 客户端应用程序（版本 5.1 及更高版本）和 macOS 客户端应用程序（版本 5.4 及更高版本）支持使用 HTTP 代理服务器处理端口 4195 TCP 流量。不支持 TLS 解密和检查。

WSP 不支持使用代理来处理通过 UDP 进行的桌面流量。只有 WorkSpaces Windows 和 macOS 桌面客户端应用程序以及 WSP 网络访问支持对 TCP 流量使用代理。

> **Note**
>
> 如果您选择使用代理服务器，则客户端应用程序对 WorkSpaces 服务进行的 API 调用也会被代理。API 调用和桌面流量都应通过同一个代理服务器。

关于使用代理服务器的建议

我们不建议使用代理服务器来处理您的 WorkSpaces 桌面流量。

Amazon WorkSpaces 桌面流量已经过加密，因此代理并不能提高安全性。代理代表网络路径中的额外跳跃，它可能会通过引入延迟来影响流式传输质量。如果代理的大小不合适，无法处理桌面流式传输流量，则代理也可能会降低吞吐量。此外，大多数代理不是为支持长时间运行 WebSocket (TCP) 连接而设计的，可能会影响直播质量和稳定性。

如果您必须使用代理，请将代理服务器尽可能靠近 WorkSpace客户端，最好位于同一网络中，以避免增加网络延迟，因为这可能会对直播质量和响应能力产生负面影响。

启用 Amazon WorkSpaces for Zoom 会议媒体插件支持

使用 Zoom VDI 插件，Zoom 支持基于 WSP 和 PCoIP Windows WorkSpaces 的优化实时通信。直接的客户端通信允许视频通话绕过基于云的虚拟桌面，并在用户内部进行会议时提供类似本地的 Zoom 体验。 WorkSpace

启用 WSP 的 Zoom 会议媒体插件

在安装 Zoom VDI 组件之前，请更新您的 WorkSpaces 配置以支持 Zoom 优化。

先决条件

在使用该插件之前，请确保满足以下要求。

- 带有 Zoom V DI 插件的 Windows WorkSpaces 客户端版本 5.10.0+ 版本 5.17.10+
- 在你的 WorkSpaces — Zoom VDI Meeting 客户端版本 5. 17.10+

开始前的准备工作

1. 启用扩展组策略设置。有关更多信息，请参阅 为 WSP 配置扩展。
2. 禁用 “自动重新连接组策略” 设置。有关更多信息，请参阅 为 WSP 设置会话恢复超时。

安装 Zoom 组件

要启用缩放优化，请在您的 Windows 上安装 Zoom 提供的两个组件 WorkSpaces。有关更多信息，请参阅使用 Zoom 处理亚马逊 Web Services。

1. 在您的中安装 Zoom VDI Meeting 客户端 5.12.6+ 版。 WorkSpace
2. 在安装你的客户端上安装 Zoom VDI 插件（Windows 通用安装程序）5.12.6+ 版 WorkSpace
3. 通过确认您的 VDI 插件状态在 Zoom VDI 客户端中显示为 “已连接”，验证插件是否在优化 Zoom 流量。有关更多信息，请参阅如何确认 Amazon WorkSpaces 优化。

启用 PCoIP 的 Zoom 会议媒体插件

拥有 Active Directory 管理权限的用户可以使用其组策略对象 (GPO) 生成注册表项。这允许用户使用强制更新将注册表项发送到您域 WorkSpaces 中的所有 Windows。或者，具有管理权限的用户也可以在其 WorkSpaces 主机上单独安装注册表项。

先决条件

在使用该插件之前，请确保满足以下要求。

- Windows WorkSpaces 客户端版本 5.4.0+，带有 Zoom VDI 插件版本 5.12.6+。
- 在你的 WorkSpaces — Zoom VDI Meeting 客户端版本 5.12.6+ 中。

在 Windows WorkSpaces 主机上创建注册表项

完成以下过程，在 Windows WorkSpaces 主机上创建注册表项。在 Windows 上使用 Zoom 需要注册表项 WorkSpaces。

1. 以管理员身份打开 Windows 注册表编辑器。
2. 转到 `\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon`。
3. 如果扩展密钥不存在，请右键单击并选择新建 > 密钥，然后将其命名为 Extension。
4. 在新的扩展密钥中，右键单击并选择新建 > DWORD，然后将其命名为 enable。名称必须为小写。
5. 选择新的 DWORD 并将值更改为 1。
6. 重启计算机以完成该过程。
7. 在您的 WorkSpaces 主机上，下载并安装最新的 Zoom VDI 客户端。在您的 WorkSpaces 客户端（5.4 或更高版本）上，下载并安装适用于亚马逊 WorkSpaces的最新 Zoom VDI 客户端插件。有关更多信息，请参阅 Zoom 支持网站 上的 VDI 版本和下载内容。

启动 Zoom 开始视频通话。

故障排除

完成以下操作对 Windows 上的 Zoom 进行故障排除 WorkSpaces。

- 确认注册表项激活并已正确应用。
- 转到 `C:\ProgramData\Amazon\Amazon WorkSpaces Extension`。您应查看 `wse_core_dll`。
- 确保主机和客户端上的版本正确且相同。

如果您仍然遇到困难，请 AWS Support 使用AWS Support 中心联系。

您可以使用以下示例将 GPO 应用为目录管理员。

- wse.adml

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" revision="1.0"
 schemaVersion="1.0" xmlns="http://www.microsoft.com/GroupPolicy/PolicyDefinitions">
```

```
    <!-- 'displayName' and 'description' don't appear anywhere. All Windows native
 GPO template files have them set like this. -->
    <displayName>enter display name here</displayName>
    <description>enter description here</description>

    <resources>
    <stringTable>
        <string id="SUPPORTED_ProductOnly">N/A</string>
        <string id="Amazon">Amazon</string>
        <string id="Amazon_Help">Amazon Group Policies</string>
        <string id="WorkspacesExtension">Workspaces Extension</string>
        <string id="WorkspacesExtension_Help">Workspace Extension Group Policies</
string>

        <!-- Extension Itself -->
        <string id="ToggleExtension">Enable/disable Extension Virtual Channel</
string>
        <string id="ToggleExtension_Help">
Allows two-way Virtual Channel data communication for multiple purposes

By default, Extension is disabled.</string>

    </stringTable>
    </resources>
</policyDefinitionResources>
```

- WSE.admx

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" revision="1.0" schemaVersion="1.0" xmlns="http://
www.microsoft.com/GroupPolicy/PolicyDefinitions">
    <policyNamespaces>
        <target prefix="WorkspacesExtension"
 namespace="Microsoft.Policies.Amazon.WorkspacesExtension" />
    </policyNamespaces>
    <supersededAdm fileName="wse.adm" />
    <resources minRequiredRevision="1.0" />
    <supportedOn>
        <definitions>
            <definition name="SUPPORTED_ProductOnly"
 displayName="$(string.SUPPORTED_ProductOnly)"/>
        </definitions>
    </supportedOn>
```

```
    <categories>
        <category name="Amazon" displayName="$(string.Amazon)"
 explainText="$(string.Amazon_Help)" />
        <category name="WorkspacesExtension"
 displayName="$(string.WorkspacesExtension)"
 explainText="$(string.WorkspacesExtension_Help)">
            <parentCategory ref="Amazon" />
        </category>
    </categories>

    <policies>
        <policy name="ToggleExtension" class="Machine"
 displayName="$(string.ToggleExtension)" explainText="$(string.ToggleExtension_Help)"
 key="Software\Policies\Amazon\Extension" valueName="enable">
            <parentCategory ref="WorkspacesExtension" />
            <supportedOn ref="SUPPORTED_ProductOnly" />
            <enabledValue>
                <decimal value="1" />
            </enabledValue>
            <disabledValue>
                <decimal value="0" />
            </disabledValue>
        </policy>
    </policies>
</policyDefinitions>
```

管理你的亚马逊 Linux WorkSpaces

与 Windows 一样 WorkSpaces，亚马逊 Linux WorkSpaces 也加入了域名，因此你可以使用 Active Directory 用户和群组来：

- 管理你的 Amazon Linux WorkSpaces
- 为用户提供对这些内容 WorkSpaces 的访问权限

由于 Linux 实例不遵循组策略，因此建议您使用配置管理解决方案进行分发和实施策略。例如，您可以使用 AWS OpsWorks for Chef Automate、AWS OpsWorks for Puppet Enterprise 或 Ansible。

> **Note**
>
> 本地打印机重定向不适用于亚马逊 Linux WorkSpaces。

控制亚马逊 Linux 上的 WorkSpaces 流媒体协议 (WSP) 行为 WorkSpaces

WSP 的行为受 `wsp.conf` 文件中的配置设置控制，该文件位于 `/etc/wsp/` 目录中。要部署和实施对策略的更改，请使用支持 Amazon Linux 的配置管理解决方案。任何更改将在代理启动后生效。

> **Note**
>
> - 如果您对`wsp.conf`文件进行了不正确或不支持的更改，则策略更改可能不会应用于您 WorkSpace上新建立的连接。
> - WSP 捆绑包 WorkSpaces 上的 Amazon Linux 目前存在以下限制：
>   - 目前仅在 AWS GovCloud （美国西部）和 AWS GovCloud （美国东部）提供。
>   - 不支持视频输入。
>   - 不支持屏幕锁定时断开会话连接。

下面各部分介绍了如何启用或禁用某些功能。

为 WSP Amazon Linux 配置剪贴板重定向 WorkSpaces

默认情况下， WorkSpaces 支持剪贴板重定向。如果需要，可以使用 WSP 配置文件配置此功能。当您断开连接并重新连接时，此设置就会生效。 WorkSpace

要为 WSP Amazon Linux 配置剪贴板重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `wsp.conf` 文件。

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. ```
   clipboard = X
   ```

   X 的可能值如下：

   `enabled` - 启用双向剪贴板重定向（默认）
   ```

`disabled` - 禁用双向剪贴板重定向

`paste-only` - 剪贴板重定向已启用，但仅允许您从本地客户端设备复制内容并将其粘贴到远程主机桌面

`copy-only` - 剪贴板重定向已启用，但仅允许您从远程主机桌面复制内容并将其粘贴到本地客户端设备

为 WSP Amazon Linux 启用或禁用音频输入重定向 WorkSpaces

默认情况下， WorkSpaces 支持音频输入重定向。如果需要，可以使用 WSP 配置文件禁用此功能。当您断开连接并重新连接到时，此设置就会生效。 WorkSpace

启用或禁用 WSP Amazon Linux 的音频输入重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `wsp.conf` 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 将以下行添加到文件的末尾。

```
audio-in = X
```

X 的可能值如下：

`enabled` - 启用音频输入重定向（默认）

`disabled` - 禁用音频输入重定向

为 WSP Amazon Linux 启用或禁用时区重定向 WorkSpaces

默认情况下，工作区内的时间设置为镜像用于连接的客户端的时区 WorkSpace。此行为是通过时区重定向控制的。您可能需要关闭时区重定向的原因有多种，例如以下原因：

- 您的公司希望所有员工在特定时区中工作（即使某些员工在其他时区）。
- 您在 a 中有计划任务 WorkSpace ，这些任务本应在特定时区的特定时间运行。
- 经常出差的用户希望将自己留 WorkSpaces 在一个时区，以保持一致性和个人喜好。

如果需要，可以使用 WSP 配置文件配置此功能。此设置在断开连接并重新连接到后生效。 WorkSpace

启用或禁用 WSP Amazon Linux 的时区重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `wsp.conf` 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp-agent/wsp.conf
```

2. 将以下行添加到文件的末尾。

```
timezone_redirect= X
```

X 的可能值如下：

启用 - 启用时区重定向（默认）

禁用 - 禁用时区重定向

控制亚马逊 Linux 上的 PCoIP 代理行为 WorkSpaces

PCoIP 代理的行为受 `pcoip-agent.conf` 文件中的配置设置控制，该文件位于 `/etc/pcoip-agent/` 目录中。要部署和实施对策略的更改，请使用支持 Amazon Linux 的配置管理解决方案。任何更改将在代理启动后生效。重新启动代理会结束所有打开的连接并重新启动窗口管理器。要应用任何更改，我们建议重新启动。 WorkSpace

> **Note**
>
> 如果您对`pcoip-agent.conf`文件进行了不正确或不支持的更改，则可能会导致无法运行。 WorkSpace 如果您 WorkSpace 停止工作，则可能需要 WorkSpace 使用 SSH 连接到您的，以还原更改，或者您可能需要重新构建 WorkSpace。

下面各部分介绍了如何启用或禁用某些功能。要查看可用设置的完整列表，请在任何 Amazon Linux 上`man pcoip-agent.conf`从终端运行 WorkSpace。

为 PCoIP Amazon Linux 配置剪贴板重定向 WorkSpaces

默认情况下，WorkSpaces 支持剪贴板重定向。如果需要，可使用 PCoIP 代理 conf 禁用此功能。此设置将在您重新启动时生效 WorkSpace。

要为 PCoIP 配置剪贴板重定向 Amazon Linux WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `pcoip-agent.conf` 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
```

2. 将以下行添加到文件的末尾。

```
pcoip.server_clipboard_state = X
```

X 的可能值如下：

0 - 禁用双向剪贴板重定向

1 - 启用双向剪贴板重定向

2 - 启用剪贴板重定向，但仅限从客户端剪贴到代理（允许复制，但仅限从本地客户端设备粘贴到远程主机桌面）

3 - 启用剪贴板重定向，但仅限从代理剪贴到客户端（允许复制，但仅限从远程主机桌面粘贴到本地客户端设备）

> **Note**
>
> 剪贴板重定向是作为虚拟通道实施的。如果禁用了虚拟通道，则剪贴板重定向将不起作用。要启用虚拟通道，请参阅 Teradici 文档中的 PCoIP 虚拟通道。

为 PCoIP Amazon Linux 启用或禁用音频输入重定向 WorkSpaces

默认情况下，WorkSpaces 支持音频输入重定向。如果需要，可使用 PCoIP 代理 conf 禁用此功能。此设置将在您重新启动时生效 WorkSpace。

启用或禁用 PCoIP Amazon Linux 的音频输入重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 pcoip-agent.conf 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
```

2. 将以下行添加到文件的末尾。

```
pcoip.enable_audio = X
```

X 的可能值如下：

0 - 禁用音频输入重定向

1 - 启用音频输入重定向

启用或禁用 PCoIP Amazon Linux 的时区重定向 WorkSpaces

默认情况下，工作区内的时间设置为镜像用于连接的客户端的时区 WorkSpace。此行为是通过时区重定向控制的。您可能需要关闭时区重定向的原因有多种，例如以下原因：

- 您的公司希望所有员工在特定时区中工作（即使某些员工在其他时区）。
- 您在 a 中有计划任务 WorkSpace ，这些任务本应在特定时区的特定时间运行。
- 经常出差的用户希望将自己留 WorkSpaces 在一个时区，以保持一致性和个人喜好。

如果 Linux 需要 WorkSpaces，你可以使用 PCoIP 代理会议来禁用此功能。此设置将在您重新启动时生效 WorkSpace。

要为 PCoIP 启用或禁用 Amazon Linux 的时区重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 pcoip-agent.conf 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
```

2. 将以下行添加到文件的末尾。

```
pcoip.enable_timezone_redirect= X
```

X 的可能值如下：

0 - 禁用时区重定向

1 - 启用时区重定向

向 Amazon Linux WorkSpaces 管理员授予 SSH 访问权限

默认情况下，只有域管理员组中分配的用户和账户才能使用 SSH 连接到 Amazon Linux WorkSpaces 。

我们建议您在 Active Directory 中为 Amazon Linux WorkSpaces 管理员创建一个专门的管理员组。

为 Linux_WorkSpaces_Admins Active Directory 组的成员启用 sudo 访问权限

1. 使用 `visudo` 编辑 `sudoers` 文件，如下例所示。

```
[example\username@workspace-id ~]$ sudo visudo
```

2. 添加以下行。

```
%example.com\\Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

在您创建专用管理员组之后，请按照以下步骤为组的成员启用登录。

启用 Linux_ WorkSpaces _Admins Active Directory 组成员的登录

1. 使用提升的权限编辑 `/etc/security/access.conf`。

```
[example\username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. 添加以下行。

```
+:(example\Linux_WorkSpaces_Admins):ALL
```

有关启用 SSH 连接的更多信息，请参阅为你的 Linux 启用 SSH 连接 WorkSpaces。

替换亚马逊 Linux 的默认外壳 WorkSpaces

要覆盖 Linux 的默认外壳 WorkSpaces，我们建议您编辑用户的~/.bashrc文件。例如，要使用 Z shell 而不是 Bash shell，请将以下行添加到 /home/*username*/.bashrc。

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
>
> 进行此更改后，必须重新启动 WorkSpace 或注销 WorkSpace （而不仅仅是断开连接），然后重新登录才能使更改生效。

保护自定义存储库免遭未授权访问

要控制对自定义存储库的访问，建议使用 Amazon Virtual Private Cloud (Amazon VPC) 中内置的安全功能，而不使用密码。例如，使用网络访问控制列表 (ACL) 和安全组。有关这些功能的更多信息，请参阅《Amazon VPC 用户指南》中的安全性。

如果必须使用密码来保护存储库，请确保创建您的 yum 存储库定义文件，如 Fedora 文档中的存储库定义文件所示。

使用 Amazon Linux Extras 库存储库

利用 Amazon Linux，您可以使用 Extras 库，在您的实例上安装应用程序和软件更新。有关使用 Extras 库的信息，请参阅《适用于 Linux 实例的 Amazon EC2 用户指南》中的 Extras 库 (Amazon Linux)。

> **Note**
>
> 如果您使用的是亚马逊 Linux 存储库，则您的亚马逊 Linux WorkSpaces 必须能够访问互联网，或者您必须为该存储库和主 Amazon Linux 存储库配置虚拟私有云 (VPC) 终端节点。有关更多信息，请参阅 提供您的 Internet 访问权限 WorkSpace。

在 Linux 上使用智能卡进行身份验证 WorkSpaces

Linux WorkSpaces WorkSpaces 流媒体协议 (WSP) 捆绑包允许使用通用访问卡 (CAC) 和个人身份验证 (PIV) 智能卡进行身份验证。有关更多信息，请参阅 使用智能卡进行身份验证。

配置用于互联网访问的设备代理服务器设置

默认情况下， WorkSpaces 客户端应用程序使用在设备操作系统设置中为 HTTPS（端口 443）流量指定的代理服务器。Amazon WorkSpaces 客户端应用程序使用 HTTPS 端口进行更新、注册和身份验证。

> **Note**
>
> 不支持需要使用登录凭证进行身份验证的代理服务器。

您可以按照 Microsoft 文档中配置设备代理和互联网连接设置中的步骤， WorkSpaces 通过组策略为 Linux 配置设备代理服务器设置。

有关在 WorkSpaces Windows 客户端应用程序中配置代理设置的更多信息，请参阅 Amazon WorkSpaces 用户指南中的代理服务器。

有关在 WorkSpaces macOS 客户端应用程序中配置代理设置的更多信息，请参阅 A mazon WorkSpaces 用户指南中的代理服务器。

有关在 WorkSpaces Web Access 客户端应用程序中配置代理设置的更多信息，请参阅 Amazon WorkSpaces 用户指南中的代理服务器。

代理桌面流量

对于 PCoIP WorkSpaces，桌面客户端应用程序不支持使用代理服务器，也不支持 TLS 解密和检查 UDP 中的端口 4172 流量（用于桌面流量）。它们需要直接连接到端口 4172。

对于 WSP WorkSpaces， WorkSpaces Windows 客户端应用程序（版本 5.1 及更高版本）和 macOS 客户端应用程序（版本 5.4 及更高版本）支持使用 HTTP 代理服务器处理端口 4195 TCP 流量。不支持 TLS 解密和检查。

WSP 不支持使用代理来处理通过 UDP 进行的桌面流量。只有 WorkSpaces Windows 和 macOS 桌面客户端应用程序以及 WSP 网络访问支持对 TCP 流量使用代理。

> **Note**
>
> 如果您选择使用代理服务器，则客户端应用程序对 WorkSpaces 服务进行的 API 调用也会被代理。API 调用和桌面流量都应通过同一个代理服务器。

关于使用代理服务器的建议

我们不建议使用代理服务器来处理您的 WorkSpaces 桌面流量。

Amazon WorkSpaces 桌面流量已经过加密，因此代理并不能提高安全性。代理代表网络路径中的额外跳跃，它可能会通过引入延迟来影响流式传输质量。如果代理的大小不合适，无法处理桌面流式传输流量，则代理也可能会降低吞吐量。此外，大多数代理不是为支持长时间运行 WebSocket (TCP) 连接而设计的，可能会影响直播质量和稳定性。

如果您必须使用代理，请将代理服务器尽可能靠近 WorkSpace 客户端，最好放在同一个网络中，以避免增加网络延迟，因为这可能会对直播质量和响应能力产生负面影响。

管理你的 Ubuntu WorkSpaces

与 Windows 和 Amazon Linux 一样 WorkSpaces，Ubuntu WorkSpaces 已加入域名，因此你可以使用 Active Directory 用户和群组来：

- 管理你的 Ubuntu WorkSpaces
- 为用户提供对这些内容 WorkSpaces 的访问权限

你可以使用 AdSys 通过组策略管理 Ubuntu WorkSpaces 。有关更多信息，请参阅 Ubuntu Active Directory 集成常见问题。您还可以使用其他配置和管理解决方案，例如 Landscape 和 Ansible。

控制 U WorkSpaces buntu 上的流媒体协议 (WSP) 行为 WorkSpaces

WSP 的行为受 `wsp.conf` 文件中的配置设置控制，该文件位于 `/etc/wsp/` 目录中。要部署和实施对策略的更改，请使用支持 Ubuntu 的配置管理解决方案。任何更改将在代理启动后生效。

> **Note**
>
> 如果您对`wsp.conf`策略做出了不正确或不支持的更改，则可能不会应用于与您的 WorkSpace 新建立的连接。

下面各部分介绍了如何启用或禁用某些功能。

为 Ubuntu 启用或禁用剪贴板重定向 WorkSpaces

默认情况下，WorkSpaces 支持剪贴板重定向。如果需要，可以使用 WSP 配置文件禁用此功能。

为 Ubuntu 启用或禁用剪贴板重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 wsp.conf 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 将以下行添加到 [policies] 组的末尾。

```
clipboard = X
```

X 的可能值如下：

启用 - 启用双向剪贴板重定向（默认）

禁用 - 禁用双向剪贴板重定向

仅粘贴 - 剪贴板重定向已启用，但仅允许您从本地客户端设备复制内容并将其粘贴到远程主机桌面

仅复制 - 剪贴板重定向已启用，但仅允许您从远程主机桌面复制内容并将其粘贴到本地客户端设备

启用或禁用 Ubuntu 的音频输入重定向 WorkSpaces

默认情况下，WorkSpaces 支持音频输入重定向。如果需要，可以使用 WSP 配置文件禁用此功能。

启用或禁用 Ubuntu 的音频输入重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 wsp.conf 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 将以下行添加到 [policies] 组的末尾。

```
audio-in = X
```

X 的可能值如下：

启用 - 启用音频输入重定向（默认）

禁用 - 禁用音频输入重定向

为 Ubuntu 启用或禁用视频输入重定向 WorkSpaces

默认情况下， WorkSpaces 支持视频输入重定向。如果需要，可以使用 WSP 配置文件禁用此功能。

启用或禁用 Ubuntu 的视频输入重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `wsp.conf` 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 将以下行添加到 `[policies]` 组的末尾。

```
video-in = X
```

X 的可能值如下：

启用 - 启用视频输入重定向（默认）

禁用 - 禁用视频输入重定向

启用或禁用 Ubuntu 的时区重定向 WorkSpaces

默认情况下，工作区内的时间设置为镜像用于连接的客户端的时区 WorkSpace。此行为是通过时区重定向控制的。您可能需要关闭时区重定向的原因有多种，例如以下原因：

- 您的公司希望所有员工在特定时区中工作（即使某些员工在其他时区）。
- 您在 a 中有计划任务 WorkSpace ，这些任务本应在特定时区的特定时间运行。
- 您的用户经常旅行，并希望将他们留 WorkSpaces 在同一个时区，以保持一致性和个人偏好。

如果需要，可以使用 WSP 配置文件配置此功能。

启用或禁用 Ubuntu 的时区重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `wsp.conf` 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 将以下行添加到 [policies] 组的末尾。

```
timezone-redirection = X
```

X 的可能值如下：

启用 - 启用时区重定向（默认）

禁用 - 禁用时区重定向

启用或禁用 Ubuntu 的打印机重定向 WorkSpaces

默认情况下，WorkSpaces 支持打印机重定向。如果需要，可以使用 WSP 配置文件禁用此功能。

启用或禁用 Ubuntu 的打印机重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 wsp.conf 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 将以下行添加到 [policies] 组的末尾。

```
remote-printing = X
```

X 的可能值如下：

启用 - 启用打印机重定向（默认）

禁用 - 禁用打印机重定向

启用或禁用 WSP 屏幕锁定时断开会话连接

启用屏幕锁定时断开会话，允许您的用户在检测到锁屏时结束 WorkSpaces 会话。要从 WorkSpaces 客户端重新连接，用户可以使用自己的密码或智能卡进行身份验证，具体取决于为其 WorkSpaces启用了哪种类型的身份验证。

默认情况下， WorkSpaces 不支持屏幕锁定时断开会话连接。如果需要，可以使用 WSP 配置文件启用此功能。

启用或禁用 Ubuntu 的屏幕锁定时断开连接会话 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `wsp.conf` 文件。

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. 将以下行添加到 `[policies]` 组的末尾。

   ```
   disconnect-on-lock = X
   ```

   X 的可能值如下：

   启用 - 启用屏幕锁定时断开连接

   禁用 - 禁用屏幕锁定时断开连接（默认）

向 Ubuntu WorkSpaces 管理员授予 SSH 访问权限

默认情况下，只有域管理员组中分配的用户和帐户才能使用 SSH 连接到 Ubuntu WorkSpaces 。要允许其他用户和账户 WorkSpaces 使用 SSH 连接到 Ubuntu，我们建议你在 Active Directory 中为 Ubuntu 管理员创建一个专门的 WorkSpaces 管理员组。

为 **`Linux_WorkSpaces_Admins`** Active Directory 组的成员启用 sudo 访问权限

1. 使用 `visudo` 编辑 `sudoers` 文件，如下例所示。

   ```
   [username@workspace-id ~]$ sudo visudo
   ```

2. 添加以下行。

```
%Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

在您创建专用管理员组之后，请按照以下步骤为组的成员启用登录。

为 **Linux_WorkSpaces_Admins** Active Directory 组的成员启用登录

1. 使用提升的权限编辑 /etc/security/access.conf。

```
[username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. 添加以下行。

```
+:(Linux_WorkSpaces_Admins):ALL
```

使用 Ubunt WorkSpaces u，在为 SSH 连接指定用户名时无需添加域名，而且默认情况下，密码身份验证处于禁用状态。要通过 SSH 进行连接，你需要在 Ubuntu $HOME/.ssh/authorized_keys 上将 SSH 公钥添加/etc/ssh/sshd_configyes到 WorkSpace，或者编辑设置为 PasswordAuthentication 。有关启用 SSH 连接的更多信息，请参阅为您的 Linux 启用 SSH 连接 WorkSpaces。

覆盖 Ubuntu 的默认外壳 WorkSpaces

要覆盖 Ubuntu 的默认外壳 WorkSpaces，我们建议您编辑用户的~/.bashrc文件。例如，要使用 Z shell 而不是 Bash shell，请将以下行添加到 /home/username/.bashrc。

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
>
> 进行此更改后，必须重新启动 WorkSpace 或注销 WorkSpace （而不仅仅是断开连接），然后重新登录才能使更改生效。

配置用于互联网访问的设备代理服务器设置

默认情况下， WorkSpaces 客户端应用程序使用在设备操作系统设置中为 HTTPS（端口 443）流量指定的代理服务器。Amazon WorkSpaces 客户端应用程序使用 HTTPS 端口进行更新、注册和身份验证。

> **Note**
>
> 不支持需要使用登录凭证进行身份验证的代理服务器。

您可以按照 Microsoft 文档中配置设备代理和互联网连接设置中的步骤， WorkSpaces 通过组策略为 Ubuntu 配置设备代理服务器设置。

有关在 WorkSpaces Windows 客户端应用程序中配置代理设置的更多信息，请参阅 Amazon WorkSpaces 用户指南中的代理服务器。

有关在 WorkSpaces macOS 客户端应用程序中配置代理设置的更多信息，请参阅 A mazon WorkSpaces 用户指南中的代理服务器。

有关在 WorkSpaces Web Access 客户端应用程序中配置代理设置的更多信息，请参阅 Amazon WorkSpaces 用户指南中的代理服务器。

代理桌面流量

对于 PCoIP WorkSpaces，桌面客户端应用程序不支持使用代理服务器，也不支持 TLS 解密和检查 UDP 中的端口 4172 流量（用于桌面流量）。它们需要直接连接到端口 4172。

对于 WSP WorkSpaces， WorkSpaces Windows 客户端应用程序（版本 5.1 及更高版本）和 macOS 客户端应用程序（版本 5.4 及更高版本）支持使用 HTTP 代理服务器处理端口 4195 TCP 流量。不支持 TLS 解密和检查。

WSP 不支持使用代理来处理通过 UDP 进行的桌面流量。只有 WorkSpaces Windows 和 macOS 桌面客户端应用程序以及 WSP 网络访问支持对 TCP 流量使用代理。

> **Note**
>
> 如果您选择使用代理服务器，则客户端应用程序对 WorkSpaces 服务进行的 API 调用也会被代理。API 调用和桌面流量都应通过同一个代理服务器。

关于使用代理服务器的建议

我们不建议使用代理服务器来处理您的 WorkSpaces 桌面流量。

Amazon WorkSpaces 桌面流量已经过加密，因此代理并不能提高安全性。代理代表网络路径中的额外跳跃，它可能会通过引入延迟来影响流式传输质量。如果代理的大小不合适，无法处理桌面流式传输流量，则代理也可能会降低吞吐量。此外，大多数代理不是为支持长时间运行 WebSocket (TCP) 连接而设计的，可能会影响直播质量和稳定性。

如果您必须使用代理，请将代理服务器尽可能靠近 WorkSpace 客户端，最好位于同一网络中，以避免增加网络延迟，因为这可能会对直播质量和响应能力产生负面影响。

优化 Amazon WorkSpaces 以实现实时通信

亚马逊 WorkSpaces 提供多种技术来促进统一通信 (UC) 应用程序的部署，例如微软 Teams、Zoom、Webex 等。在当代应用程序环境中，大多数 UC 应用程序都包含各种功能，包括一对一聊天室、协作群聊频道、无缝文件存储和交换、直播活动、网络研讨会、广播、交互式屏幕共享和控制、白板以及离线音频/视频消息传递功能。其中大多数功能都可以 WorkSpaces 作为标准功能无缝使用，无需进行额外的微调或增强。但是，值得注意的是，实时通信元素，尤其是通 one-on-one 话和集体小组会议，是该规则的例外。成功纳入此类功能通常需要在 WorkSpaces 部署过程中集中精力和进行规划。

在计划在 Amazon 上实施 UC 应用程序的实时通信功能时 WorkSpaces，您有三种不同的实时通信 (RTC) 配置模式可供选择。具体选择取决于您打算向用户提供的一个或多个特定应用程序以及您计划使用的客户端设备。

本文档重点介绍如何优化 Amazon 中最常见的 UC 应用程序的用户体验 WorkSpaces。有关特定于 WorkSpaces Core 的优化，请参阅合作伙伴特定的文档。

主题

- RTC 优化指南

媒体优化模式概述

以下是可用的媒体优化选项。

选项 1：媒体优化的实时通信（媒体优化 RTC）

在此模式下，第三方 UC 和 VoIP 应用程序在远程执行 WorkSpace，而其媒体框架则被卸载到支持的客户端进行直接通信。以下 UC 应用程序在 Amazon 上使用这种方法 WorkSpaces：

- Zoom Meetings
- Cisco Webex Meetings

要使媒体优化的 RTC 模式正常运行，UC 应用程序供应商应 WorkSpaces 使用可用的软件开发套件 (SDK) 之一（例如 D CV Extension SDK）开发集成。此模式要求在客户端设备上安装 UC 组件。

有关配置此模式的更多信息，请参阅配置媒体优化的 RTC。

选项 2：会话中优化的实时通信（会话中优化的 RTC）

在此模式下，未更改的 UC 应用程序在上运行 WorkSpace，通过 WorkSpaces 流协议将音频和视频流量传送到客户端设备。来自麦克风的本地音频和来自网络摄像头的视频流被重定向到 WorkSpace，UC 应用程序将在那里使用它们。此模式提供了广泛的应用程序兼容性，并有效地将 UC 应用程序从远程平台传送 WorkSpace到各种客户端平台。您无需将 UC 应用程序组件部署到客户端设备。

有关配置此模式的更多信息，请参阅配置会话中优化 RTC。

选项 3：直接实时通信（直接 RTC）

在此模式下，在中运行的 WorkSpace 应用程序将控制位于用户桌面或客户端操作系统上的物理或虚拟电话机。这样一来，音频流量会直接从用户工作站的物理电话或在客户端设备上运行的虚拟电话传送到远程呼叫对等端。在此模式下运行的应用程序的重要实例包括：

- 针对亚马逊的 Amazon Connect 优化 WorkSpaces
- Genesys Cloud WebRTC Media Helper
- Microsoft Teams SIP Gateway

- Microsoft Teams 台式电话和 Teams 显示屏
- 通过 UC 应用程序的拨入或“拨打我的电话”功能参与音频会议。

有关配置此模式的更多信息，请参阅配置直接 RTC。

使用哪种 RTC 优化模式？

可以同时使用不同的 RTC 优化模式，也可以将其设置为后备模式相互补充。例如，可以考虑为 Cisco Webex 会议启用媒体优化 RTC。此配置可确保用户在 WorkSpace 通过桌面客户端进行访问时体验到优化的通信。但是，在从缺乏 UC 优化组件的共享互联网自助服务亭访问 Webex 的情况下，Webex 将无缝过渡到会话中优化 RTC 模式以保持功能。当用户使用多个 UC 应用程序时，RTC 配置模式可能会根据其独特要求而有所不同。

下表列出了常见的 UC 应用程序功能，并定义了哪种 RTC 配置模式可提供最佳结果。

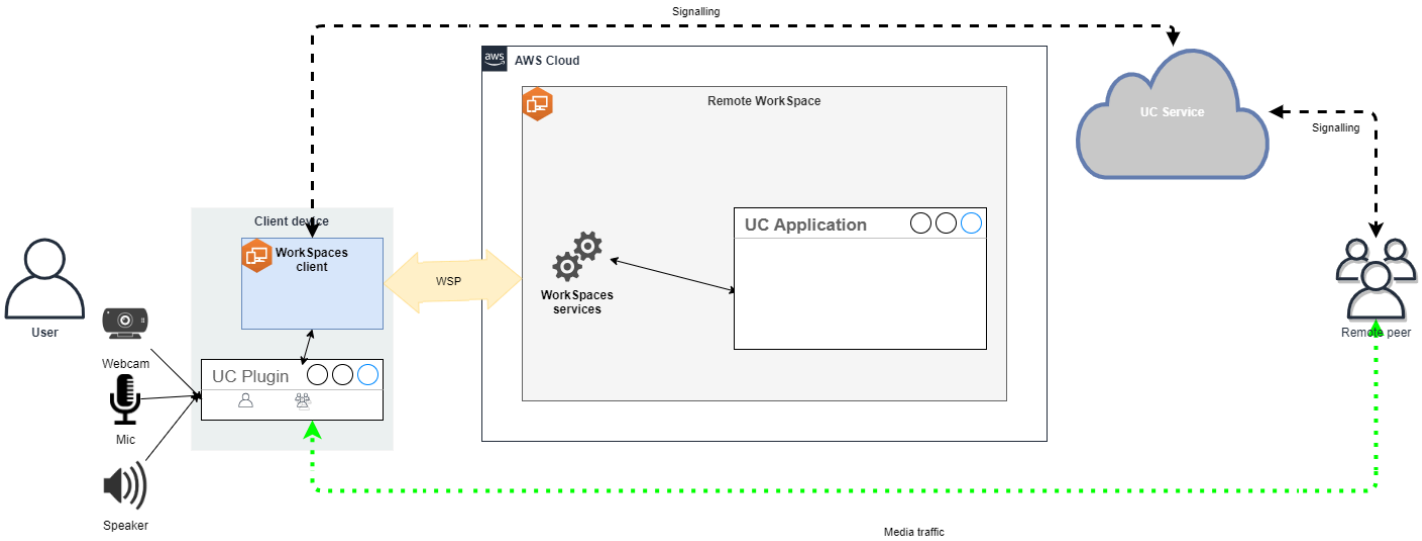
功能	直接 RTC	媒体优化 RTC	会话中优化的 RTC
一对一聊天	不需要 RTC 配置		
群聊室	不需要 RTC 配置		
群组音频会议	最佳	最佳	好
群组视频会议	好	最佳	好
一对一音频通话	最佳	最佳	好
一对一视频通话	好	最佳	好
白板	不需要 RTC 配置		
音频/视频片段/消息传送	不适用	好	最佳
文件共享	不适用	取决于 UC 应用程序	最佳
屏幕共享和控制	不适用	取决于 UC 应用程序	最佳
网络研讨会/广播活动	不适用	好	最佳

RTC 优化指南

配置媒体优化的 RTC

UC 应用程序供应商使用 Amazon 提供的软件开发工具包，使媒体优化的 RTC 模式成为可能。该架构要求 UC 供应商开发特定于 UC 的插件或扩展并将其部署到客户端。

该软件开发工具包含 DCV Extension SDK 和自定义私有版本等公开可用的选项，它在内运行的 UC 应用程序模块 WorkSpace 和客户端的插件之间建立了控制通道。通常，此控制通道会指示客户端扩展发起或加入呼叫。通过客户端扩展建立呼叫后，UC 插件会捕获来自麦克风的音频和来自网络摄像头的视频，然后将其直接传输到 UC 云或呼叫对等端。传入的音频在本地播放，视频叠加在远程客户端 UI 上。控制通道负责传递呼叫的状态。



Amazon WorkSpaces 目前支持以下具有媒体优化 RTC 模式的应用程序：

- Zoom 会议（适用于 PCoIP 和 WSP） WorkSpaces
- 思科 Webex 会议（仅适用于 WS WorkSpaces P）

如果您使用的应用程序不在列表中，建议您与应用程序供应商联系并请求对 WorkSpaces 媒体优化 RTC 的支持。要加快此过程，请鼓励他们联系 aws-av-offloading@amazon .com。

虽然媒体优化的 RTC 模式可增强通话性能并最大限度地减少 WorkSpace资源使用量，但它确实存在某些限制：

- UC 客户端扩展必须安装在客户端设备上。
- UC 客户端扩展需要独立管理和更新。

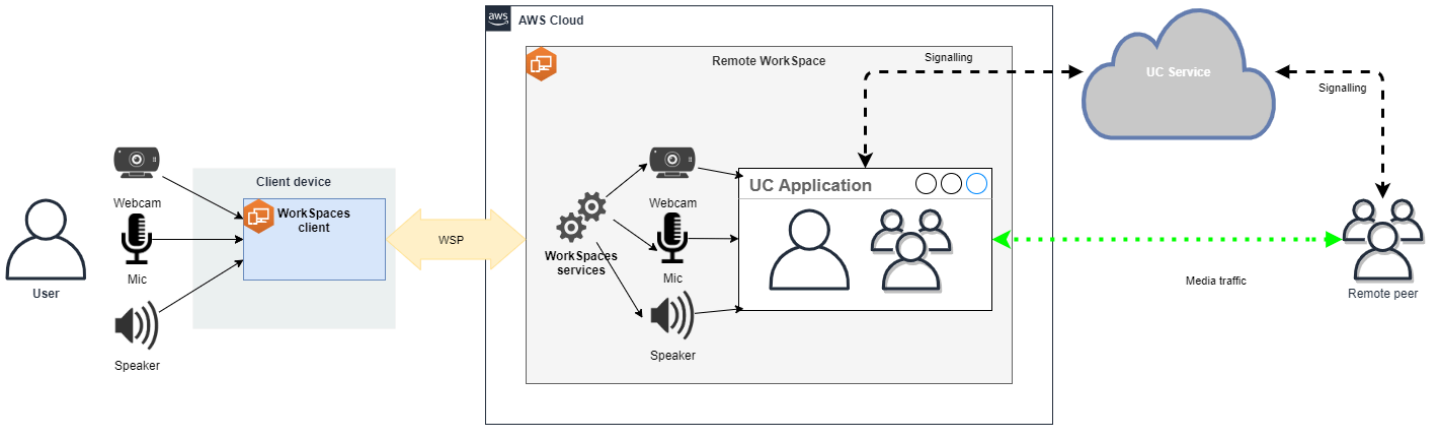
- UC 客户端扩展可能在某些客户端平台上不可用，例如移动平台或 Web 客户端。
- 在此模式下，某些 UC 应用程序功能可能会受到限制；例如，屏幕共享行为可能会有所不同。
- 使用客户端扩展可能不适合自带设备 (BYOD) 或共享自助服务亭等场景。

如果媒体优化的 RTC 模式经过证明不适合您的环境，或者某些用户无法安装客户端扩展，则建议将会话中优化 RTC 模式配置为后备选项。

配置会话中优化 RTC

在会话中优化 RTC 模式下，UC 应用程序 WorkSpace无需任何修改即可在上运行，从而提供类似于本地的体验。应用程序生成的音频和视频流由 WorkSpaces 流协议 (WSP) 捕获并传输到客户端。在客户端，麦克风（在 WSP 和 PCoIP 上 WorkSpaces）和网络摄像头（仅在 WSP 上 WorkSpaces）信号被捕获，重定向回并无缝传递到 UC 应用程序。 WorkSpace

值得注意的是，此选项可确保出色的兼容性，即使使用旧版应用程序也是如此，从而提供连贯的用户体验（无论应用程序的来源如何）。会话中优化也适用于 Web 客户端。



WorkSpaces 流媒体协议 (WSP) 经过精心优化，以增强远程 RTC 模式的性能。优化措施包括：

- 利用基于 UDP 的自适应 QUIC 传输，确保高效的数据传输。
- 建立低延迟音频路径，便于快速音频输入和输出。
- 实施经过语音优化的音频编解码器，以保持音频质量，同时降低 CPU 和网络利用率。
- 网络摄像头重定向，实现网络摄像头功能的集成。
- 配置网络摄像头分辨率以优化性能。
- 集成自适应显示编解码器，以平衡速度和视觉质量。
- 音频抖动校正，保证流畅的音频传输。

这些优化共同有助于在远程 RTC 模式下提供稳定而流畅的体验。

大小调整建议

要有效支持远程 RTC 模式，必须确保 Amazon WorkSpaces 的适当规模。遥控器 WorkSpace 必须满足或超过相应统一通信 (UC) 应用程序的系统要求。下表概述了常用 UC 应用程序用于视频和音频通话时支持的最低配置和推荐 WorkSpaces 配置：

			视频通话		音频通话		
应用程序	RTC 应用程序的 CPU 要求	RTC 应用程序的内存要求	最低支持 WorkSpace	推荐 WorkSpace	最低支持 WorkSpace	推荐 WorkSpace	参考
Microsoft Teams	需要 2 个内核，推荐 4 个内核	4.0 GB 内存	节能（4 个 vCPU，16 GB 内存）	PowerPro（8 个 vCPU，32 GB 内存）	性能（2 个 vCPU，8 GB 内存）	节能（4 个 vCPU，16 GB 内存）	Microsoft Teams 的硬件要求
Zoom	需要 2 个内核，推荐 4 个内核	4.0 GB 内存	节能（4 个 vCPU，16 GB 内存）	PowerPro（8 个 vCPU，32 GB 内存）	性能（2 个 vCPU，8 GB 内存）	节能（4 个 vCPU，16 GB 内存）	Zoom 系统要求：Windows、macOS、Linux
Webex	需要 2 个内核	4.0 GB 内存	节能（4 个 vCPU，16 GB 内存）	PowerPro（8 个 vCPU，32 GB 内存）	性能（2 个 vCPU，8 GB 内存）	节能（4 个 vCPU，16 GB 内存）	Webex 服务的系统要求

值得注意的是，视频会议在视频编码和解码时使用了大量资源。在物理计算机场景中，这些任务会分载到 GPU。在非 GPU 中 WorkSpaces，这些任务在 CPU 上与远程协议编码并行执行。因此，对于经常进行视频流或视频通话的用户，强烈建议选择该 PowerPro配置。

屏幕共享还会消耗大量资源，分辨率越高，资源消耗就会增加。因此，在非 GPU 上 WorkSpaces，屏幕共享通常仅限于较低的帧速率。

通过 WorkSpaces 流媒体协议 (WSP) 利用基于 UDP 的 QUIC 传输

UDP 传输特别适合传输 RTC 应用程序。为了最大限度地提高效率，请确保将您的网络设置为通过 WSP 使用 QUIC 传输。请注意，基于 UDP 的传输仅适用于本机客户端。

配置 UC 应用程序 WorkSpaces

要增强视频处理能力，例如背景模糊、虚拟背景、反应或主持直播活动，选择支持 GPU 的视频对于实现最佳性能 WorkSpace 至关重要。

大多数 UC 应用程序都提供了禁用高级视频处理以降低非 GP WorkSpaces U 上的 CPU 使用率的指导。

有关更多信息，请参阅以下资源。

- Microsoft Teams：虚拟化桌面基础架构中的 Teams
- Zoom Meetings：管理不兼容的 VDI 插件的用户体验
- Webex：适用于虚拟桌面基础架构 (VDI) 的 Webex 应用程序部署指南 - 管理适用于 VDI 的 Webex 应用程序并排除其问题 [Webex 应用程序]
- Google Meet：使用 VDI

启用双向音频和网络摄像头重定向

默认情况下，Amazon WorkSpaces 本质上支持通过视频输入进行音频输入、音频输出和摄像机重定向。但是，如果由于任何特定原因禁用了这些功能，则您可以按照提供的指导重新启用重定向。有关更多信息，请参阅《Amazon 管理指南》中的 “为 WSP 启用或禁用视频输入重定向”。 WorkSpaces连接后，用户需要选择要在会话中使用的摄像头。有关更多信息，用户应参阅《亚马逊 WorkSpaces 用户指南》中的网络摄像头和其他视频设备。

限制网络摄像头的最大分辨率

对于使用 Power 或 PowerPro WorkSpaces 进行视频会议的用户，强烈建议限制重定向网络摄像头的最大分辨率。在这种情况下 PowerPro，建议的最大分辨率为宽 640 像素 x 高 480 像素。就节能而言，建议的最大分辨率为宽 320 像素，高 240 像素。

完成以下步骤，配置网络摄像头的最大分辨率。

1. 打开 Windows 注册表编辑器。
2. 导航到以下注册表路径：

```
HKEY_USERS/S-1-5-18/Software/GSettings/com/nicesoftware/dcv/webcam
```

3. 创建一个名为 `max-resolution` 的字符串值，并将其设置为 `(X,Y)` 格式所需的分辨率，其中 X 表示水平像素数（宽度），Y 表示垂直像素数（高度）。例如，指定 `(640,480)`)，以表示宽度为 640 像素、高度为 480 像素的分辨率。

启用语音优化的音频配置

默认情况下，设置 WorkSpaces 为从 WorkSpaces 客户端传输 7.1 高保真音频，从而确保卓越的音乐播放质量。但是，如果您的主要使用案例涉及音频或视频会议，则将音频编解码器配置文件修改为语音优化设置可以节省 CPU 和网络资源。

完成以下步骤，将音频配置文件设置为语音优化。

1. 打开 Windows 注册表编辑器。
2. 导航到以下注册表路径：

```
HKEY_USERS/S-1-5-18/Software/GSettings/com/nicesoftware/dcv/audio
```

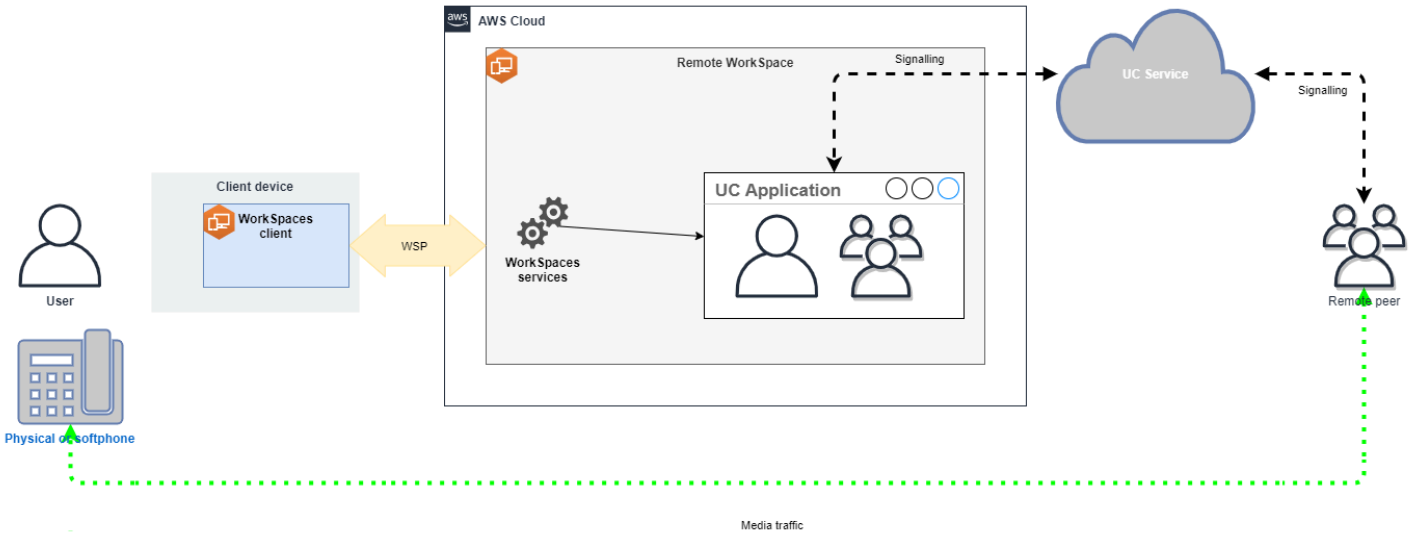
3. 创建名为 `default-profile` 的字符串值，并将其设置为 `voice`。

使用高质量头戴式耳机进行音频和视频通话

为了增强音频体验并防止回声，使用高质量的头戴式耳机至关重要。使用台式机扬声器可能会导致通话的远程端出现回声问题。

配置直接 RTC

直接 RTC 模式的配置取决于特定的统一通信 (UC) 应用程序，不需要对配置进行任何更改。WorkSpaces 以下列表简单编译了针对各种 UC 应用程序的优化。



- Microsoft Teams：
  - 规划 SIP Gateway
  - Microsoft 365 中的音频会议
  - 规划 Teams 语音解决方案
- Zoom Meetings：
  - 启用或禁用长途电话拨入号码
  - 使用桌面电话呼叫控制
  - 桌面电话伴侣模式
- Webex：
  - Webex 应用程序 | 使用桌面电话拨打电话
  - Webex 应用程序 | 支持的通话选项
- BlueJeans:
  - 从台式电话拨入会议
- Genesys：
  - Genesys Cloud WebRTC Media Helper
- Amazon Connect：
  - 针对亚马逊的 Amazon Connect 优化 WorkSpaces
- Google Meet：
  - 在视频会议中针对音频使用电话

管理 WorkSpace 运行模式

WorkSpace 的运行模式 决定其即时可用性和付费方式（按月或按小时）。在创建 WorkSpace 时，可以选择以下运行模式：

- AlwaysOn - 支付固定月费用以无限次使用您的 WorkSpaces。该模式最适合将 WorkSpace 作为主桌面全职使用的用户。
- AutoStop - 按使用 WorkSpace 的小时数付费。在该模式下，您的 WorkSpace 会在指定的断开连接时间后停止运行，而应用程序和数据的状态将会保存。

有关更多信息，请参阅 WorkSpaces 定价。

AutoStop WorkSpaces

要设置自动停止时间，请在 Amazon WorkSpaces 控制台中选择 WorkSpace，依次选择操作、修改运行模式属性，然后设置 AutoStop 时间（小时）。默认情况下，AutoStop 时间（小时）设置为 1 小时，这意味着 WorkSpace 将在 WorkSpace 断开连接一小时后自动停止运行。

在 WorkSpace 断开连接且 AutoStop 时间段到期后，WorkSpace 可能还需要几分钟才能自动停止运行。但是，一旦 AutoStop 时间段到期，计费就会停止，并且不会向您收取额外时间的费用。

如果可能，桌面的状态将会保存到 WorkSpace 的根卷。WorkSpace 会在用户登录时恢复；所有打开的文档和正在运行的程序都会恢复为其已保存的状态。

AutoStop Graphics.g4dn、GraphicsPro.g4dn、Graphics 和 GraphicsPro WorkSpaces 在停止运行时不会保留数据和程序的状态。对于这些 Autostop WorkSpaces，建议您在每次使用完后保存相关内容。

对于自带许可 (BYOL) AutoStop WorkSpaces，大量并发登录可能会显著延长 WorkSpaces 的可用时间。如果您预计会有许多用户同时登录您的 BYOL AutoStop WorkSpaces，请咨询您的客户经理以获取建议。

> **Important**
>
> AutoStop WorkSpaces 仅在 WorkSpaces 断开连接时才会自动停止运行。

只有在以下情况下才会断开 WorkSpace 的连接：

- 用户手动断开与 WorkSpace 的连接或退出 Amazon WorkSpaces 客户端应用程序。
- 客户端设备已关闭。
- 客户端设备和 WorkSpace 之间没有连接的时间超过 20 分钟。

最佳做法是，AutoStop WorkSpace 用户应在每天使用完 WorkSpaces 后，手动断开其连接。要手动断开连接，请在 Linux、macOS 或 Windows WorkSpaces 客户端应用程序的 Amazon WorkSpaces 菜单中，选择断开 WorkSpace 连接或退出 Amazon WorkSpaces。对于 Android 或 iPad，从侧边栏菜单中选择断开连接。

AutoStop WorkSpaces 在以下情况下可能不会自动停止运行：

- 如果客户端设备仅处于锁定状态、睡眠状态或非活动状态（例如，笔记本电脑盖已合上）而不是关闭状态，则表明 WorkSpaces 应用程序可能仍在后台运行。只要 WorkSpaces 应用程序仍在运行，WorkSpace 就可能不会断开连接，因此 WorkSpace 可能就不会自动停止运行。
- 只有当用户使用 WorkSpaces 客户端时，WorkSpaces 才能检测到断开连接。如果用户使用第三方客户端，则 WorkSpaces 可能无法检测到断开连接，因此 WorkSpace 可能不会自动停止运行，计费也可能不会被停用。

修改运行模式

您可以随时切换运行模式。

修改 WorkSpace 的运行模式

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择要修改的 WorkSpace，然后依次选择操作、修改运行模式。
4. 选择新的运行模式 AlwaysOn 或 AutoStop，然后选择保存。

使用 AWS CLI 修改 WorkSpace 的运行模式

使用 modify-workspace-properties 命令。

停止和启动 AutoStop WorkSpace

当您的 AutoStop WorkSpaces 断开连接时，它们会在指定的断开连接时间后自动停止运行，而且按小时计费也会暂停。为了进一步优化成本，您可以手动暂停与 AutoStop WorkSpace 相关联的按小时计

算的费用。WorkSpace 将停止运行，所有应用程序和数据将保存，以供用户下次登录到 WorkSpace 时使用。

当用户重新连接到已停止的 WorkSpace 时，它会恢复到其上次停止时的位置，通常在 90 秒内。

您可以重启可用或处于错误状态的 AutoStop WorkSpaces。

要停止 AutoStop WorkSpace

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择要停止的 WorkSpace，然后依次选择操作、停止 WorkSpaces。
4. 当系统提示您确认时，选择停止 WorkSpace。

要启动 AutoStop WorkSpace

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择要启动的 WorkSpaces，然后依次选择操作、启动 WorkSpaces。
4. 当系统提示您确认时，选择启动 WorkSpace。

要删除与 AutoStop WorkSpace 相关联的固定的基础设施成本，请将 WorkSpace 从您的账户中删除。有关更多信息，请参阅删除 WorkSpace。

使用 AWS CLI 停止和启动 AutoStop WorkSpace

使用 stop-WorkSpaces 和 start-WorkSpaces 命令。

管理应用程序

启动后 WorkSpace，你可以在 WorkSpaces 控制台 WorkSpace 上看到与你关联的所有应用程序包的列表。

要查看与您关联的所有应用程序包的列表 WorkSpace

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 从左侧导航窗格中选择WorkSpaces。

3. 选择 ， WorkSpace 然后选择 “查看详细信息”。
4. 在 “应用程序” 下，找到与此 WorkSpace相关的应用程序列表及其安装状态。

您可以通过以下方式更新您的 WorkSpace 应用程序包：

- 在您的设备上安装应用程序包 WorkSpace
- 从您的应用程序中卸载应用程序包 WorkSpace
- 安装应用程序包并卸载您的应用程序包上的另一组应用程序包 WorkSpace

> **Note**
>
> - 要更新应用程序包，其状态 WorkSpace 必须为`AVAILABLE`或`STOPPED`。
> - 管理应用程序仅适用于 Windows WorkSpaces。
> - 管理应用程序仅适用于通过 AWS订阅的应用程序捆绑包。

管理应用程序支持的捆绑包

“管理应用程序” 允许您在上安装和卸载以下应用程序 WorkSpaces。对于 Microsoft Office 2016 捆绑包和 Microsoft Office 2019，您只能卸载。

- Microsoft Office LTSC Professional Plus 2021
- Microsoft Visio LTSC Professional 2021
- Microsoft Project Professional 2021
- Microsoft Office LTSC Standard 2021
- Microsoft Visio LTSC Standard 2021
- Microsoft Project Standard 2021

下表显示了支持和不支持的应用程序与操作系统组合列表：

	Microsoft Office Professional Plus 2016（32 位）	Microsoft Office Professional Plus 2019（64 位）	Microsoft LTSC Office Professional Plus/ Standard 2021 (64-bit)	Microsoft Project Professional/ Standard 2021（64 位）	Microsoft LTSC Visio Professional/Standard 2021（64 位）
Windows Server 2016	卸载	不支持	不支持	不支持	不支持
Windows Server 2019	不支持	卸载	安装/卸载	安装/卸载	安装/卸载
Windows Server 2022	不支持	卸载	安装/卸载	安装/卸载	安装/卸载
Windows 10	卸载	卸载	安装/卸载	安装/卸载	安装/卸载
Windows 11	卸载	卸载	安装/卸载	安装/卸载	安装/卸载

Important

- 这些应用程序必须遵循相同的版本。例如，您不能将标准应用程序与专业应用程序混合使用。
- 这些应用程序必须遵循相同的版本。例如，您不能将 2019 应用程序与 2021 应用程序混合使用。
- Value、Graphics 和捆绑包不支持微软 Office/Visio/Project 2021 标准版/专业版。GraphicsPro WorkSpaces

- 当你从中卸载适用于 Microsoft Office 2016 的 Plus 应用程序包时，你将无法访问该亚马逊 WorkSpaces 捆绑包中包含的任何趋势科技解决方案。 WorkSpaces如果您想继续在 Amazon 上使用趋势科技解决方案 WorkSpaces，可以在AWS 市场上单独购买。
- 要安装/卸载 Microsoft 365 应用程序，您需要引入自己的工具和安装程序，管理应用程序工作流程无法安装/卸载 Microsoft 365 应用程序。
- 您无法使用通过 “管理应用程序” 安装 WorkSpaces 的应用程序创建的自定义映像，但可以使用 “管理应用程序” 创建用于卸载应用程序包的自定义映像。 WorkSpaces
- 必须启用 DNS 解析才能使用管理应用程序。
- 对于选择加入的区域，例如非洲（开普敦），必须在目录级别启用 WorkSpaces 互联网连接。

要在上更新应用程序包 WorkSpace

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择， WorkSpace 然后选择操作、管理应用程序。
4. 在 “当前应用程序” 下，您将看到已安装在此应用程序上的应用程序包列表 WorkSpace ，在 “选择应用程序” 下，您可以看到可供在此上安装的应用程序包列表。 WorkSpace
5. 要在此 WorkSpace上安装应用程序包，请执行以下操作：
   a. 选择要在此上安装的应用程序包 WorkSpace，然后选择 “关联”。
   b. 重复上一步以安装其他应用程序捆绑包。
   c. 安装应用程序捆绑包时，您将在当前应用程序下看到它们，其状态为 `Pending install deployment`。
6. 要从中卸载应用程序包，请执行以下操作 WorkSpace：
   a. 在选择应用程序下，选择要卸载的应用程序捆绑包，然后选择取消关联。
   b. 重复上一步以卸载其他应用程序捆绑包。
   c. 卸载应用程序捆绑包时，您将在当前应用程序下看到它们，其状态为 `Pending uninstall deployment`。
7. 要恢复捆绑包安装或安装状态，请执行以下一项操作。

- 如果要从 `Pending uninstall deployment` 状态还原捆绑包，请选择要还原的应用程序，然后选择关联。
- 如果要从 `Pending install deployment` 状态还原捆绑包，请选择要还原的应用程序，然后选择取消关联。

8. 在您选择安装或卸载的应用程序捆绑包处于待处理状态后，选择部署应用程序。

> **Important**
>
> 选择 “部署应用程序” 后，最终用户会话将终止，并且在安装或卸载应用程序时 WorkSpaces 将无法访问。

9. 要确认您的操作，请键入确认。选择强制，以安装或卸载处于错误状态的应用程序捆绑包。
10. 监控应用程序捆绑包的进度：

    a. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。

    b. 在导航窗格中，选择 WorkSpaces。您可以在状态下看到状态，包括以下内容。

    - 正在更新 - 应用程序捆绑包更新仍在进行中。
    - 可用/已停止-应用程序包更新已完成 WorkSpace ，并恢复到其原始状态。

    c. 要监视应用程序包的安装或卸载状态，请选择 WorkSpace 并选择查看详细信息。在应用程序下，您可以在状态下看到状态，包括 `Pending install`、`Pending uninstall` 和 `Installed`。

> **Note**
>
> 如果您的用户发现他们通过托管应用程序新安装的应用程序包未激活许可证，则可以手动 WorkSpace 重启。您的用户可以在重启后开始使用这些应用程序。如需其他支持，请联系 AWS Support。

使用 “管理应用程序” 管理 WorkSpaces 修改内容

在上安装或卸载应用程序包后 WorkSpaces，以下操作可能会影响现有配置。

- WorkSpace Re@@ store a WorkSpace-恢复后，会根据运行正常时创建的根卷和用户卷的最新快照，重新创建根卷和用户卷。 WorkSpace 每 12 小时拍摄一次完整 WorkSpace 快照。有关更多信

息，请参阅恢复 WorkSpace。请确保至少等待 12 小时后再恢复使用 WorkSpaces “管理应用程序” 修改过的内容。使用管理应用程序修改 WorkSpaces 过的下一个完整快照恢复之前的完整快照将导致以下结果：

- WorkSpaces 使用 “管理应用程序” 工作流程安装在您的应用程序包上的应用程序包将从您的应用程序中删除， WorkSpaces 但许可证仍会被激活，并且 WorkSpaces 将向您收取这些应用程序的费用。要恢复这些应用程序包， WorkSpaces 您需要再次运行管理应用程序工作流程，卸载应用程序以重新启动，然后重新安装。
- WorkSpaces 使用 “管理应用程序” 工作流程从您的应用程序中删除的应用程序包将重新出现在您 WorkSpaces的。但是，这些应用程序捆绑包将无法正常运行，因为许可证激活缺失。要删除这些应用程序包，请从中手动卸载这些应用程序包。 WorkSpaces

- 重建 a WorkSpace-重建 WorkSpace 会重新创建根卷。有关更多信息，请参阅重新构建 WorkSpace。重建使用 WorkSpaces “管理应用程序” 修改过的内容将导致以下结果：
  - WorkSpaces 使用 “管理应用程序” 工作流程在您上安装的应用程序捆绑包将从您的应用程序中移除并停用。 WorkSpaces为了恢复这些应用程序， WorkSpaces 您需要再次运行 “管理应用程序” 工作流程。
  - WorkSpaces 通过 “管理应用程序” 工作流程从您的 “管理应用程序” 工作流程中删除的应用程序包将安装并激活。 WorkSpaces要从中移除这些应用程序包 WorkSpaces，您需要再次运行管理应用程序工作流程。
- Migr@@ ate a WorkSpace-迁移过程使用目标捆绑包映像中的新根卷和原始 WorkSpace包映像的最后一个可用快照中的用户卷来重新创建。 WorkSpace WorkSpace 使用新 ID 创建了一个新的 WorkSpace ID。有关更多信息，请参阅迁 WorkSpace移使用管理应用程序修改 WorkSpaces 的迁移将导致以下结果：
  - 源中的所有应用程序包都 WorkSpaces 将被移除并停用。新的目标 WorkSpaces 将继承目标 WorkSpaces 包中的应用程序。源 WorkSpaces 应用程序捆绑包将按整月计费，但目标捆绑包中的应用程序捆绑包将按比例计费。

修改 WorkSpace

启动后 WorkSpace，您可以通过三种方式修改其配置：

- 您可以更改其根卷的大小（对于 Windows，为驱动器 C；对于 Linux，为 /）及其用户卷（对于 Windows，为驱动器 D；对于 Linux，为 /home）。
- 您可以更改其计算类型以选择新的捆绑包。
- 如果您 WorkSpace 是使用 PCoIP 捆绑包创建的，则可以使用 AWS CLI 或 Amazon WorkSpaces API 修改直播协议。

要查看 a 的当前修改状态 WorkSpace，请选择箭头以显示有关该修改的更多详细信息 WorkSpace。状态的可能值为正在修改计算、正在修改存储和无。

如果要修改 WorkSpace，则其状态必须为AVAILABLE或STOPPED。您无法同时更改卷大小和计算类型。

更改 a 的卷大小或计算类型 WorkSpace 将更改的账单费率 WorkSpace。

要允许您的用户自行修改卷和计算类型，请参阅为您的用户启用自助 WorkSpace管理功能。

修改卷大小

您可以将根卷和用户卷的大小分别增加到 2000 GB。 WorkSpace WorkSpace root 和用户卷属于无法更改的设置组。可用的组包括：

[根 (GB)、用户 (GB)]
[80, 10]
[80, 50]
[80, 100]
[175 至 2000、100 至 2000]

无论是已加密还是未加密，您都可以扩展根卷和用户卷，并且可以在 6 小时内扩展这两个卷一次。但是，您无法同时增加根卷和用户卷的大小。有关更多信息，请参阅有关增加卷的限制。

> **Note**
>
> 当你扩展一个的卷时 WorkSpace， WorkSpaces 会自动在 Windows 或 Linux 中扩展该卷的分区。该过程完成后，必须重新启动 WorkSpace 才能使更改生效。

为确保数据得以保留，启动后不能减小根卷或用户卷的大小 WorkSpace。相反，请确保在启动时指定这些卷的最小大小 WorkSpace。您可以启动 “超值”、“标准”、“性能”、“Power”，或者 PowerPro WorkSpace 根卷至少为 80 GB，用户卷至少为 10 GB。你可以启动 Graphics.g4dn、GraphicsPro .g4dn、Graphics，或者 GraphicsPro WorkSpace 根卷至少为 100 GB，用户卷至少为 100 GB。

在增加 WorkSpace 磁盘大小的同时，用户可以在其上执行大多数任务 WorkSpace。但是，他们无法更改 WorkSpace 计算类型、切换 WorkSpace 运行模式、重建或重启（重启）计算类型 WorkSpace。WorkSpace

> **Note**
>
> 如果您希望您的用户能够在磁盘大小增加 WorkSpaces 过程中使用他们的，请确保其状态为“ WorkSpaces AVAILABLE而不是”，STOPPED然后再调整其卷的大小 WorkSpaces。如果 WorkSpaces 是STOPPED，则在磁盘大小增加过程中无法启动它们。

在大多数情况下，增加磁盘大小的过程最多可能需要两个小时。但是，如果您要修改大量的卷大小 WorkSpaces，则该过程可能需要更长的时间。如果您有大量 WorkSpaces 需要修改，我们建议您联系以AWS Support寻求帮助。

有关增加卷的限制

- 您只能调整 SSD 卷的大小。
- 启动时 WorkSpace，必须等待 6 小时才能修改其卷的大小。
- 您无法同时增加根卷和用户卷的大小。要增加根卷，您必须先将用户卷更改为 100 GB。进行此更改后，您可以将根卷更新为 175 和 2000 GB 之间的任何值。在将根卷更改为 175 和 2000 GB 之间的任何值后，您可以进一步更新用户卷，以更新为 100 和 2000 GB 之间的任何值。

  > **Note**
  >
  > 如果要增加这两个卷，则必须等待 20-30 分钟让第一个操作完成，然后才能开始第二个操作。

- 除非 WorkSpace 是 graphics.g4dn、 GraphicsPro .g4dn、Graphics 或，否则当用户容量为 100 GB 时 GraphicsPro WorkSpace，根卷不能小于 175 GB。Graphics.g4dn、GraphicsPro .g4dn、Graphics 以及 GraphicsPro WorkSpaces可以将根卷和用户卷都设置为最低 100 GB。
- 如果用户卷是 50 GB，则无法将根卷更新为 80 GB 以外的任何大小。如果根卷是 80 GB，则用户卷只能是 10、50 或 100 GB。

修改的根卷 WorkSpace

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。

2. 在导航窗格中，选择。WorkSpaces
3. 选择 WorkSpace 并选择操作、修改根卷。 。
4. 在根卷大小下，选择卷大小或选择自定义以输入自定义卷大小。
5. 选择保存更改。
6. 磁盘大小增加完成后，必须重新启动才能使更改生效。 WorkSpace为避免数据丢失，请确保用户在重新启动之前保存所有打开的文件 WorkSpace。

修改 a 的用户音量 WorkSpace

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择。WorkSpaces
3. 选择 WorkSpace 并选择操作、修改用户音量。 。
4. 在用户卷大小下，选择卷大小或选择自定义以输入自定义卷大小。
5. 选择保存更改。
6. 磁盘大小增加完成后，必须重新启动才能使更改生效。 WorkSpace为避免数据丢失，请确保用户在重新启动之前保存所有打开的文件 WorkSpace。

要更改 a 的音量大小 WorkSpace

使用带`RootVolumeSizeGib`或属`UserVolumeSizeGib`性的modify-workspace-properties命令。

修改计算类型

您可以在 “标准”、“功耗”、“性能” 和 “ PowerPro 计算” 类型 WorkSpace 之间切换。有关这些计算类型的更多信息，请参阅 Amazon WorkSpaces 捆绑包。

> **Note**
>
> - 你可以将计算类型从 Graphics.g4dn 更改为.g4dn，或者从.g4dn 更改为 graphics GraphicsPro .g4dn。 GraphicsPro您无法将 Graphics.g4dn 和 GraphicsPro .g4dn 的计算类型更改为任何其他值。
> - 2023 年 11 月 30 日之后，不再支持 Graphics 捆绑包。我们建议将你迁移 WorkSpaces 到 Graphics.g4dn 捆绑包。有关更多信息，请参见 迁移 WorkSpace。
> - 您不能将图形的计算类型更改 GraphicsPro 为任何其他值。

当您请求更改计算时，请 WorkSpace 使用新的计算类型 WorkSpaces 重新启动。 WorkSpaces 保留的操作系统、应用程序、数据和存储设置。 WorkSpace

请求较大计算类型的申请每 6 小时可以提一次，而请求较小计算类型的申请每 30 天可以提一次。对于新启动的计算类型 WorkSpace，您必须等待 6 小时才能请求更大的计算类型。

当 WorkSpace 计算类型更改进行时，用户将与其断开连接 WorkSpace，他们无法使用或更改 WorkSpace。 WorkSpace 在计算类型更改过程中会自动重新启动。

> **Important**
>
> 为避免数据丢失，请确保用户在更改 WorkSpace 计算类型之前保存所有打开的文档和其他应用程序文件。

计算类型更改过程可能需要一个小时的时间。

要更改 a 的计算类型 WorkSpace

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择。WorkSpaces
3. 选择 WorkSpace 并选择操作、修改计算类型。
4. 在计算类型下，选择一种计算类型。
5. 选择保存更改。

要更改 a 的计算类型 WorkSpace

使用带`ComputeTypeName`属性的modify-workspace-properties命令。

修改协议

如果您 WorkSpace 是使用 PCoIP 捆绑包创建的，则可以使用 CLI 或 Amazon AP AWS I 修改其直播协议。 WorkSpaces 这样，您就可以在不使用迁移功能 WorkSpace 的情况下使用现有协议进行 WorkSpace 迁移。这还允许您使用 WorkSpaces 流协议 (WSP) 并维护您的根卷，而无需在迁移 WorkSpaces 过程中重新创建现有 PCoIP。

- 如果您的协议是使用 PCoIP 捆绑包创建 WorkSpace 的，则只能修改您的协议。
- 在将协议修改为 WSP 之前，请确保您 WorkSpace 满足 W WorkSpace SP 的以下要求。
  - 您的 WorkSpaces 客户端支持 WSP

- 您的 WorkSpace 部署区域支持 WSP
- WSP 的 IP 地址和端口要求已开放。有关更多信息，请参阅的 IP 地址和端口要求 WorkSpaces。
- 确保您当前的捆绑包在 WSP 中可用。
- 为了获得最佳的视频会议体验，我们建议仅使用 Power 或 PowerPro 捆绑包。

> **Note**
>
> - 我们强烈建议您在开始更改协议 WorkSpaces 之前使用非生产环境进行测试。
> - 如果您将协议从 PCoIP 修改为 WSP，然后将协议修改回 PCoIP，则将无法通过 Web Access 进行连接。 WorkSpaces

要更改 a 的协议 WorkSpace

1. [可选] 重新启动 WorkSpace 并等到其AVAILABLE处于状态后再修改协议。
2. [可选] 使用describe-workspaces命令列出 WorkSpace 属性。确保其处于 AVAILABLE 状态且其当前 Protocol 准确无误。
3. 使用 modify-workspace-properties 命令并将 Protocols 属性从 PCOIP 修改为 WSP，或者反过来。

```
aws workspaces modify-workspace-properties
--workspace-id <value>
--workspace-properties "Protocols=[WSP]"
```

> **Important**
>
> Protocols 属性区分大小写。确保使用 PCOIP 或 WSP。

4. 运行该命令后，最长可能需要 20 分钟 WorkSpace 才能重新启动并完成必要的配置。
5. 再次使用该describe-workspaces命令列出 WorkSpace属性并验证其是否处于AVAILABLE状态以及当前Protocols属性已更改为正确的协议。

> **Note**
>
> - 修改 WorkSpace的协议不会更新控制台中的捆绑包描述。启动捆绑包描述不会更改。

- 如果 20 分钟后 WorkSpace 仍处于UNHEALTHY状态，请在控制台 WorkSpace 中重新启动。

6. 您现在可以连接到您的 WorkSpace.

自定义 WorkSpace 品牌

Amazon WorkSpaces 允许您使用 API 使用自己的品牌徽标、IT 支持信息、忘记密码链接和登录消息自定义登录页面的外观，从而为用户创造熟悉的 WorkSpaces 体验。 WorkSpace您的品牌将在用户的 WorkSpace 登录页面中显示给他们，而不是默认的 WorkSpaces 品牌。

支持以下客户端：

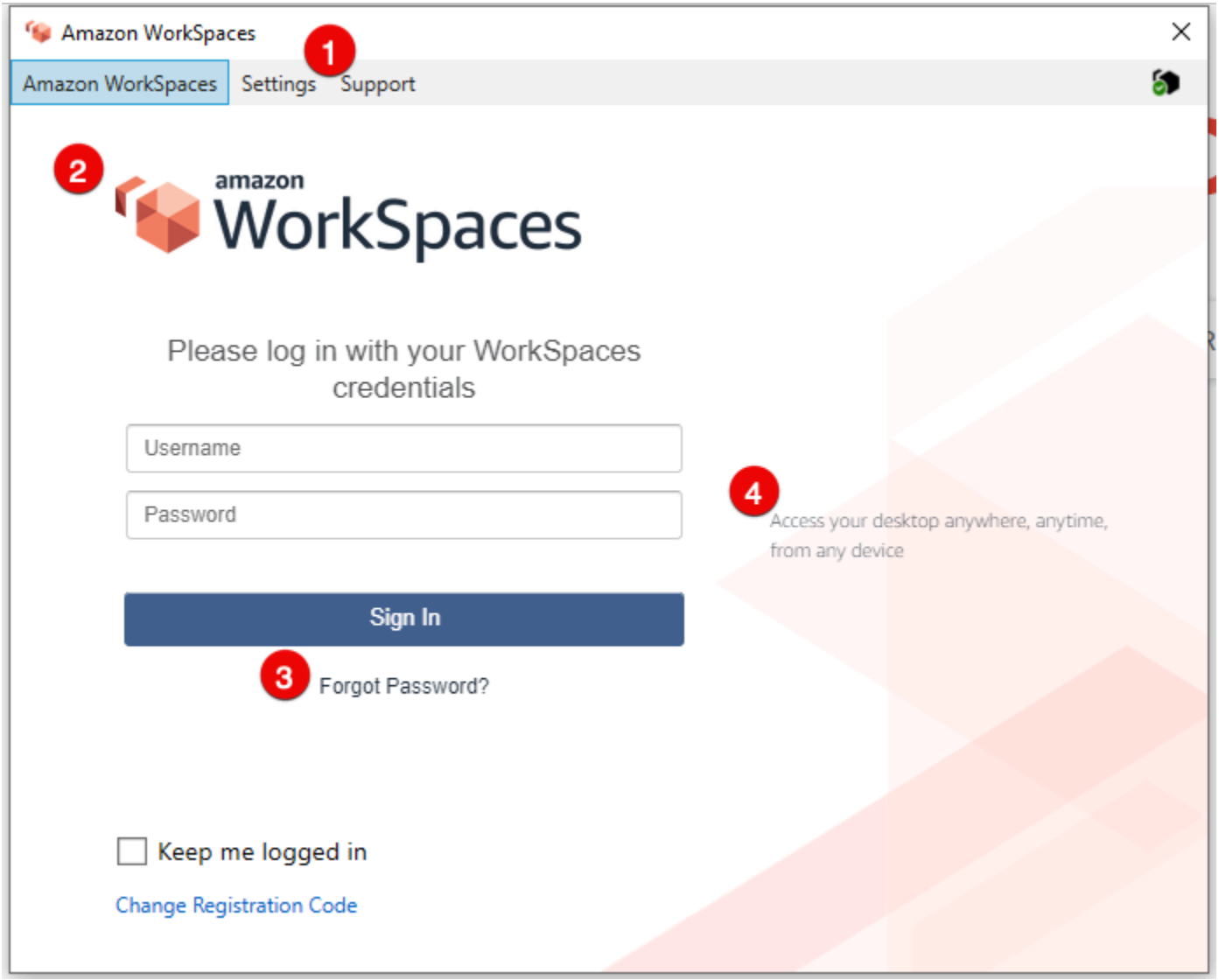
- Windows
- Linux
- Android
- MacOS
- iOS
- Web Access

> **Note**
>
> 要使用中的 ClientBranding API 修改品牌元素AWS GovCloud (US) Region，请使用 WorkSpaces 客户端版本 5.10.0。

导入自定义品牌

要导入您的客户端品牌自定义，请使用包含以下元素的操作 `ImportClientBranding`。有关更多信息，请参阅 ImportClientBranding API 参考。

> **Important**
>
> 客户端品牌属性面向公众。确保您不包含敏感信息。



1. 支持链接
2. 徽标
3. 忘记密码链接
4. 登录消息

自定义品牌元素

品牌元素	描述	要求和建议
支持链接	允许您指定支持电子邮件链接，供用户联系以寻求帮助 WorkSpaces。您可以使用	• 对于每种平台类型，`SupportEmail` 和 `SupportLink` 参数相互排

品牌元素	描述	要求和建议
	SupportEmail 属性或使用 SupportLink 属性提供指向您支持页面的链接。	斥。您可以为每种平台类型指定单个参数，但不能同时指定两者。 • 默认电子邮件地址是 workspaces-feedback@amazon.com 。 • 长度限制：最小长度为 1。最大长度为 200。
徽标	允许您使用 Logo 属性自定义组织的徽标。	• 唯一接受的图像格式是从 .png 文件转换的二进制数据对象。 • 建议的分辨率： • Android：978 x 190 • 台式机：319 x 55 • iOS@2x：110 x 200 • iOS@3x：1650 x 300
忘记密码链接	允许您使用用户忘记密码时可以访问的 ForgotPasswordLink 属性添加网址 WorkSpace。	长度限制：最小长度为 1。最大长度为 200。

品牌元素	描述	要求和建议
登录消息	允许您使用登录屏幕上的 `LoginMessage` 属性自定义消息。	• 长度限制：长度下限为 0。与 HTML 标签和不同的字体大小集成时的最大长度为 2000 个字符。对于没有 HTML 标签的默认情况，建议将登录消息保持在 600 个字符以内。 • 支持的 HTML 标签：`a, b, blockquote, br, cite, code, dd, dl, dt, div, em, i, li, ol, p, pre, q, small, span, strike, strong, sub, sup, u, ul`

以下是供使用的 ImportClientBranding示例代码片段。

AWS CLI 版本 2

> **Warning**
>
> 导入自定义品牌会覆盖您在该平台中使用自定义数据指定的属性。它还会使用默认自定义品牌属性值覆盖您未指定的属性。您必须包含不想覆盖的任何属性的数据。

```
aws workspaces import-client-branding \
--cli-input-json file://~/Downloads/import-input.json \
--region us-west-2
```

导入 JSON 文件应与以下示例代码类似：

```
{
    "ResourceId": "<directory-id>",
    "DeviceTypeOsx": {
```

```
        "Logo":
 "iVBORw0KGgoAAAANSUhEUgAAAAIAAAACCAYAAABytg0kAAAAC0lEQVR42mNgQAcAABIAAeRVjecAAAAASUVORK5CYII="
        "ForgotPasswordLink": "https://amazon.com/",
        "SupportLink": "https://amazon.com/",
        "LoginMessage": {
            "en_US": "Hello!!"
        }
    }
}
```

以下 Java 代码片段示例将徽标图像转换为 base64 编码的字符串：

```
// Read image as BufferImage
BufferedImage bi = ImageIO.read(new File("~/Downloads/logo.png"));

// convert BufferedImage to byte[]
ByteArrayOutputStream baos = new ByteArrayOutputStream();
ImageIO.write(bi, "png", baos);
byte[] bytes = baos.toByteArray();

//convert byte[] to base64 format and print it
String bytesBase64 = Base64.encodeBase64String(bytes);
System.out.println(bytesBase64);
```

以下 Python 代码片段示例将徽标图像转换为 base64 编码的字符串：

```
# Read logo into base64-encoded string
with open("~/Downloads/logo.png", "rb") as image_file:
    f = image_file.read()
    base64_string = base64.b64encode(f)
    print(base64_string)
```

Java

> **Warning**
>
> 导入自定义品牌会覆盖您在该平台中使用自定义数据指定的属性。它还会使用默认自定义品牌属性值覆盖您未指定的属性。您必须包含不想覆盖的任何属性的数据。

```
// Create WS Client
```

```
WorkSpacesClient client = WorkSpacesClient.builder().build();

// Read image as BufferImage
BufferedImage bi = ImageIO.read(new File("~/Downloads/logo.png"));

// convert BufferedImage to byte[]
ByteArrayOutputStream baos = new ByteArrayOutputStream();
ImageIO.write(bi, "png", baos);
byte[] bytes = baos.toByteArray();

// Create import attributes for the plateform
DefaultImportClientBrandingAttributes attributes =
        DefaultImportClientBrandingAttributes.builder()
                .logo(SdkBytes.fromByteArray(bytes))
                .forgotPasswordLink("https://aws.amazon.com/")
                .supportLink("https://aws.amazon.com/")
                .build();

// Create import request
ImportClientBrandingRequest request =
        ImportClientBrandingRequest.builder()
                .resourceId("<directory-id>")
                .deviceTypeOsx(attributes)
                .build();

// Call ImportClientBranding API
ImportClientBrandingResponse response = client.importClientBranding(request);
```

Python

> **Warning**
>
> 导入自定义品牌会覆盖您在该平台中使用自定义数据指定的属性。它还会使用默认自定义品牌属性值覆盖您未指定的属性。您必须包含不想覆盖的任何属性的数据。

```
import boto3

# Read logo into bytearray
with open("~/Downloads/logo.png", "rb") as image_file:
    f = image_file.read()
    bytes = bytearray(f)
```

```
# Create WorkSpaces client
client = boto3.client('workspaces')

# Call import API
response = client.import_client_branding(
    ResourceId='<directory-id>',
    DeviceTypeOsx={
        'Logo': bytes,
        'SupportLink': 'https://aws.amazon.com/',
        'ForgotPasswordLink': 'https://aws.amazon.com/',
        'LoginMessage': {
            'en_US': 'Hello!!'
        }
    }
)
```

PowerShell

```
#Requires -Modules @{ ModuleName="AWS.Tools.WorkSpaces"; ModuleVersion="4.1.56"}

# Specify Image Path
$imagePath = "~/Downloads/logo.png"

# Create Byte Array from image file
$imageByte = ([System.IO.File]::ReadAllBytes($imagePath))

# Call import API
Import-WKSClientBranding -ResourceId <directory-id> `
    -DeviceTypeLinux_LoginMessage @{en_US="Hello!!"} `
    -DeviceTypeLinux_Logo $imageByte `
    -DeviceTypeLinux_ForgotPasswordLink "https://aws.amazon.com/" `
    -DeviceTypeLinux_SupportLink "https://aws.amazon.com/"
```

要预览登录页面，请启动 WorkSpaces 应用程序或 Web 登录页面。

> **Note**
>
> 更改最多可能需要 1 分钟才会显示。

描述自定义品牌

要查看您当前拥有的客户端品牌自定义的详细信息，请使用操作 DescribeCustomBranding。以下是使用的示例脚本 DescribeClientBranding。有关更多信息，请参阅 DescribeClientBranding API 参考。

```
aws workspaces describe-client-branding \
--resource-id <directory-id> \
--region us-west-2
```

删除自定义品牌

要删除您的客户端品牌自定义，请使用操作 DeleteCustomBranding。以下是使用的示例脚本 DeleteClientBranding。有关更多信息，请参阅 DeleteClientBranding API 参考。

```
aws workspaces delete-client-branding \
--resource-id <directory-id> \
--platforms DeviceTypeAndroid DeviceTypeIos \
--region us-west-2
```

> **Note**
>
> 更改最多可能需要 1 分钟才会显示。

标记 WorkSpaces 资源

您可以通过以标签形式为每个资源分配自己的元数据来组织和管理 WorkSpaces 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”。使用标签是管理 AWS 资源和组织数据（包括账单数据）的一种简单却强有力的方式。

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 WorkSpace 添加标签，则直到 8 月 1 日，这些标签才会出现在您的成本分配报告中。有关更多信息，请参阅《AWS Billing 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 资源标签，必须按照《AWS Billing 用户指南》中的激活用户定义的成本分配标签中的说明激活已应用于 WorkSpaces 资源的标签。

尽管标签会在激活 24 小时后显示，但与这些标签关联的值可能需要 4 到 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 资源必须在此期间产生费用。Cost Explorer 仅显示标签激活时及以后的成本数据。目前没有可用的历史数据。

您可以添加标签的资源

- 您可以在创建以下资源时为其添加标签 — WorkSpaces、导入的图像和 IP 访问控制组。
- 您可以为以下类型的现有资源添加标签 — WorkSpaces、注册的目录、自定义捆绑包、图像和 IP 访问控制组。

标签限制

- 每个资源的标签数上限 – 50
- 最大密钥长度 - 127 个 Unicode 字符
- 最大值长度 - 255 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:` 或 `aws:workspaces:` 前缀，因为它们专为 AWS 使用预留。您无法编辑或删除带这些前缀的标签名称或值。

使用控制台（目录、WorkSpaces 或 IP 访问控制组）更新现有资源的标签

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择以下资源类型之一：目录、WorkSpaces 或 IP 访问控制。
3. 选择相应资源以打开其详细信息页面。
4. 执行以下一个或多个操作：
   - 要更新标签，请编辑键和值的值。
   - 要添加标签，请选择 Add Tag，然后编辑 Key 和 Value 的值。
   - 要删除标签，请选择标签旁边的删除图标 (X)。
5. 完成更新标签后，选择 Save (保存)。

使用控制台更新现有资源的标签（图像或捆绑包）

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择以下资源类型之一：捆绑包或图像。
3. 选择相应资源以打开资源详细信息页。
4. 在 Tags（标签）下，选择 Manage tags（管理标签）。
5. 执行以下一个或多个操作：
   - 要更新标签，请编辑键和值的值。
   - 要添加标签，请选择添加新标签，然后编辑键和值的值。
   - 要删除标签，请选择标签旁边的删除。
6. 更新标签后，选择保存更改。

使用 AWS CLI 更新现有资源的标签

使用 create-tags 和 delete-tags 命令

WorkSpace 维护

建议您定期维护 WorkSpaces。WorkSpaces 会为您的 WorkSpaces 安排默认维护时段。在维护时段内，WorkSpace 会根据需要从 Amazon WorkSpaces 安装重要更新并重启。如果有操作系统更新，则也会从 WorkSpace 配置为使用的操作系统更新服务器安装这些更新。维护过程中，您的 WorkSpace 可能无法使用。

默认情况下，您的 Windows WorkSpace 配置为从 Windows 更新接收更新。要为 Windows 配置您自己的自动更新机制，请参阅 Windows Server Update Services (WSUS) 和配置管理器的文档。

要求

您的 WorkSpace 必须具有互联网的访问权限，以便您将更新安装到操作系统以及部署应用程序。有关更多信息，请参阅the section called “互联网访问”。

AlwaysOn WorkSpaces 的维护时段

对于 AlwaysOn WorkSpace，维护时段由操作系统设置决定。默认时段为 WorkSpace 所在时区每个星期日凌晨 00:00 至 04:00 的四小时时段。默认情况下，AlwaysOn WorkSpace 的时区为该 WorkSpace 所在 AWS 区域的时区。但是，如果您从另一个区域连接且时区重定向处于启用状态，然后断开连接，则 WorkSpace 的时区将被更新为您连接时所在区域的时区。

您可以使用组策略禁用 Windows WorkSpaces 的时区重定向。您可以使用 PCoIP 代理配置禁用 Linux WorkSpaces 的时区重定向功能。

对于 Windows WorkSpaces，您可以使用组策略配置维护时段；请参阅配置组策略设置以进行自动更新。您不能为 Linux WorkSpace 配置维护时段。

AutoStop WorkSpaces 的维护时段

AutoStop WorkSpace 每月自动启动一次，以便安装重要更新。维护时段自当月第三个星期一开始，最长为两周，每天 00:00 至 05:00，时区为该 WorkSpace 所在 AWS 区域的时区。可以在维护时段中的任意一天维护 WorkSpace。在此时间段内，仅保留超过 7 天的 WorkSpaces。

在 WorkSpace 进行维护的时间段内，WorkSpace 的状态设置为 `MAINTENANCE`。

尽管您无法修改用于维护 AutoStop WorkSpaces 的时区，但您可以按如下方式禁用 AutoStop WorkSpaces 的维护时段。如果您禁用维护模式，您的 WorkSpace 将不会重启且不会进入 `MAINTENANCE` 状态。

禁用维护模式

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择目录。
3. 选择目录，然后选择 Actions、Update Details。
4. 展开 Maintenance Mode。
5. 要启用自动更新，请选择 Enabled。如果您倾向于手动管理更新，请选择 Disabled。
6. 选择更新和退出。

手动维护

如果您愿意，您可以按照自己的计划维护 WorkSpace。当您执行维护任务时，建议您将 WorkSpace 的状态更改为维护。维护完成后，将 WorkSpace 的状态更改为可用。

当 WorkSpace 处于维护模式下时，会发生以下行为：

- WorkSpace 不会对重启、停止、启动或重建的请求作出响应。
- 用户无法登录到 WorkSpace。
- AutoStop WorkSpace 不会休眠。

使用控制台更改 WorkSpace 的状态

> **Note**
>
> 要更改 WorkSpace 的状态，WorkSpace 必须处于可用状态。当 WorkSpace 未处于可用状态时，修改状态设置不可用。

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择您的 WorkSpace，然后依次选择操作和修改状态。
4. 在修改状态下，选择可用或维护。
5. 选择保存。

使用 AWS CLI 更改 WorkSpace 的状态

使用 modify-workspace-state 命令。

已加密 WorkSpaces

WorkSpaces 已与 AWS Key Management Service (AWS KMS) 集成。这使您能够 WorkSpaces 使用密 AWS KMS 钥对存储卷进行加密。当你启动 a 时 WorkSpace，你可以加密根卷（对于微软 Windows，是 C 盘；Linux，/）和用户卷（对于 Windows，是 D 盘；对于 Linux，/home）。这样做可确保静态存储的数据、卷的磁盘 I/O 及从加密卷创建的快照都会被加密。

> **Note**
>
> 除了加密您的 WorkSpaces，您还可以在某些 AWS 美国地区使用 FIPS 终端节点加密。有关更多信息，请参阅 设置 Amazon WorkSpaces 以符合 FedRAMP 授权或 DoD SRG 合规性要求。

内容

- 使用 WorkSpaces 加密概述 AWS KMS
- WorkSpaces 加密上下文
- 授 WorkSpaces 予代表您使用 KMS 密钥的权限
- 加密 WorkSpace
- 查看已加密 WorkSpaces

先决条件

在开始加密过程之前，您需要一个密 AWS KMS 钥。此 KMS 密钥可以是适用于亚马逊的AWS 托管 KMS 密钥 WorkSpaces （ aws/workspaces ），也可以是对称的客户托管 KMS 密钥。

- AWS 托管 KMS 密钥 — 在您首次 WorkSpace 从 WorkSpaces 控制台启动某个地区的未加密密钥时，Amazon WorkSpaces 会自动在您的账户中创建 AWS 托管 KMS 密钥（ aws/workspaces ）。您可以选择此 AWS 托管 KMS 密钥来加密您的用户和根卷 WorkSpace。有关更多信息，请参阅 使用 WorkSpaces 加密概述 AWS KMS。

  您可以查看此 AWS 托管 KMS 密钥，包括其策略和授权，并可以在 AWS CloudTrail 日志中跟踪其使用情况，但您无法使用或管理此 KMS 密钥。亚马逊 WorkSpaces 创建并管理此 KMS 密钥。只有 Amazon WorkSpaces 可以使用此 KMS 密钥，并且 WorkSpaces 只能使用它来加密您账户中的 WorkSpaces 资源。

  AWS 托管 KMS 密钥（包括 Amazon WorkSpaces 支持的密钥）每三年轮换一次。有关详细信息，请参阅《AWS Key Management Service 开发人员指南》中的轮换 AWS KMS 密钥。
- 客户托管 KMS 密钥 — 或者，您可以选择使用 AWS KMS创建的对称客户托管 KMS 密钥。您可以查看、使用和管理此 KMS 密钥，包括设置其策略。有关创建 KMS 密钥的更多信息，请参阅《AWS Key Management Service 开发人员指南》中的创建密钥。有关使用 AWS KMS API 创建 KMS 密钥的更多信息，请参阅AWS Key Management Service 开发人员指南中的使用密钥。

  除非您决定启用自动密钥轮换，否则客户托管 KMS 密钥不会自动轮换。有关详细信息，请参阅《AWS Key Management Service 开发人员指南》中的轮换 AWS KMS 密钥。

> **Important**
>
> 手动轮换 KMS 密钥时，必须同时启用原始 KMS 密钥和新的 KMS 密钥，这样 AWS KMS 才能解密原始 KMS 密钥加密后的密钥。 WorkSpaces 如果您不想保持原始 KMS 密钥处于启用状态，则必须重新创建 WorkSpaces并使用新的 KMS 密钥对其进行加密。

您必须满足以下要求才能使用密 AWS KMS 钥加密您的 WorkSpaces：

- KMS 密钥必须是对称的。Amazon WorkSpaces 不支持非对称 KMS 密钥。有关区分对称和非对称 KMS 密钥的信息，请参阅《AWS Key Management Service 开发人员指南》中的识别对称和非对称 KMS 密钥。
- KMS 密钥必须已启用。要确定是否启用 KMS 密钥，请参阅《AWS Key Management Service 开发人员指南》中的显示 KMS 密钥详细信息。
- 您必须拥有与 KMS 密钥相关联的正确权限和策略。有关更多信息，请参阅 第 2 部分：使用 IAM 策略向 WorkSpaces 管理员授予额外权限。

限制

- 您无法加密现有的 WorkSpace。启动 WorkSpace 时必须对其进行加密。
- 不支持使用加密 WorkSpace 镜像创建自定义镜像。
- 目前不支持对加密文件 WorkSpace 禁用加密。
- WorkSpaces 在启用根卷加密的情况下启动可能需要长达一个小时才能进行配置。
- 要重新启动或重建加密的 WorkSpace，请先确保 AWS KMS 密钥已启用；否则，密钥 WorkSpace 将无法使用。要确定是否启用 KMS 密钥，请参阅《AWS Key Management Service 开发人员指南》中的显示 KMS 密钥详细信息。

使用 WorkSpaces 加密概述 AWS KMS

使用加密卷创建 WorkSpaces 时， WorkSpaces 使用亚马逊弹性区块存储 (Amazon EBS) Elastic Block Store 来创建和管理这些卷。Amazon EBS 通过行业标准的 AES-256 算法，利用数据密钥加密您的卷。Amazon EBS 和亚马逊都 WorkSpaces 使用您的 KMS 密钥来处理加密卷。有关 EBS 卷加密的更多信息，请参阅 Amazon EC2 用户指南中的亚马逊 EBS 加密。

当您 WorkSpaces 使用加密卷启动时， end-to-end 过程如下所示：

1. 您可以指定用于加密的 KMS 密钥以及用于的用户和目录 WorkSpace。此操作会创建一项授权，该授权仅 WorkSpaces 允许为此使用您的 KMS 密钥 WorkSpace，也就是说，仅允许与指定用户和目录 WorkSpace关联的用户使用 KMS 密钥。
2. WorkSpaces 为创建加密的 EBS 卷 WorkSpace 并指定要使用的 KMS 密钥以及该卷的用户和目录。此操作将创建一项授权，允许 Amazon EBS 仅将您的 KMS 密钥用于该卷 WorkSpace 和卷，也就是说，仅适用于与指定用户和目录 WorkSpace 关联的，并且仅用于指定的卷。

3. Amazon EBS 请求使用您的 KMS 密钥加密的卷数据密钥，并将 WorkSpace 用户的活动目录安全标识符 (SID) 和 AWS Directory Service 目录 ID 以及亚马逊 EBS 卷 ID 指定为加密上下文。
4. AWS KMS 创建新的数据密钥，使用您的 KMS 密钥对其进行加密，然后将加密的数据密钥发送到 Amazon EBS。
5. WorkSpaces 使用 Amazon EBS 将加密卷附加到您的 WorkSpace。Amazon EBS AWS KMS 通过Decrypt请求将加密的数据密钥发送到，并指定 WorkSpace 用户的 SID、目录 ID 和卷 ID，后者用作加密上下文。
6. AWS KMS 使用您的 KMS 密钥解密数据密钥，然后将纯文本数据密钥发送到 Amazon EBS。
7. Amazon EBS 使用纯文本数据密钥加密所有传入和传出加密卷的数据。Amazon EBS 会将纯文本数据密钥保存在内存中，直至卷连接到 WorkSpace。
8. Amazon EBS 将加密的数据密钥（接收于Step 4）与卷元数据一起存储，以备将来重启或重建时使用。 WorkSpace
9. 当您使用删除 WorkSpace （或使用 WorkSpaces API 中的TerminateWorkspaces操作）时，WorkSpaces Amazon EBS 会停用允许他们使用您的 KMS 密钥进行此 WorkSpace操作的授权。 AWS Management Console

WorkSpaces 加密上下文

WorkSpaces 不会将您的 KMS 密钥直接用于加密操作（例如EncryptDecryptGenerateDataKey、、等），这意味着 WorkSpaces 不向包含加密上下文的请求发送请求。 AWS KMS 但是，当 Amazon EBS 请求您的加密卷的加密数据密钥时 WorkSpaces（Step 3在使用 WorkSpaces 加密概述 AWS KMS）以及请求该数据密钥的纯文本副本（Step 5）时，它会在请求中包含加密上下文。

加密上下文提供了额外的身份验证数据 (AAD)， AWS KMS 用于确保数据完整性。加密上下文也会写入您的 AWS CloudTrail 日志文件，这可以帮助您了解使用给定 KMS 密钥的原因。Amazon EBS 会对加密上下文使用以下内容：

- 与 Active Directory 用户关联的安全标识符 (SID) WorkSpace
- 与之关联的 AWS Directory Service 目录的目录 ID WorkSpace
- Amazon EBS 加密卷的卷 ID

以下示例显示了 Amazon EBS 使用的加密上下文的 JSON 表示形式：

```
{
```

```
  "aws:workspaces:sid-directoryid":
 "[S-1-5-21-277731876-1789304096-451871588-1107]@[d-1234abcd01]",
  "aws:ebs:id": "vol-1234abcd"
}
```

授 WorkSpaces 予代表您使用 KMS 密钥的权限

您可以在 WorkSpaces（aws/workspaces）的 AWS 托管 KMS 密钥或客户托管的 KMS 密钥下保护您的 WorkSpace 数据。如果您使用客户托管的 KMS 密钥，则需要授予代表账户 WorkSpaces 管理员使用 KMS 密钥的 WorkSpaces 权限。默认情况下，的 AWS WorkSpaces托管 KMS 密钥具有所需的权限。

要准备您的客户托管的 KMS 密钥以供使用 WorkSpaces，请按以下步骤操作。

1. 将您的 WorkSpaces 管理员添加到 KMS 密钥的密钥策略中的密钥用户列表中
2. 通过 IAM 策略为您的 WorkSpaces 管理员提供更多权限

您的 WorkSpaces 管理员还需要获得使用权限 WorkSpaces。有关这些权限的更多信息，请参阅 对 WorkSpaces 进行身份和访问管理。

第 1 部分：将 WorkSpaces 管理员添加为关键用户

要向 WorkSpaces 管理员授予他们所需的权限，您可以使用 AWS Management Console 或 AWS KMS API。

将 WorkSpaces 管理员添加为 KMS 密钥的密钥用户（控制台）

1. 登录 AWS Management Console 并打开 AWS Key Management Service (AWS KMS) 控制台，网址为 https://console.aws.amazon.com/kms。
2. 要更改 AWS 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。
4. 选择首选客户托管 KMS 密钥的密钥 ID 或别名。
5. 选择 Key policy (密钥策略) 选项卡。在 Key users（密钥用户）下，选择 Add（添加）。
6. 在 IAM 用户和角色列表中，选择与您的 WorkSpaces 管理员对应的用户和角色，然后选择添加。

将 WorkSpaces 管理员添加为 KMS 密钥 (API) 的密钥用户

1. 使用GetKey策略操作获取现有密钥策略，然后将策略文档保存到文件中。

2. 在您的首选文本编辑器中打开策略文档。将与您的 WorkSpaces 管理员对应的 IAM 用户和角色添加到向关键用户授予权限的策略声明中。然后保存文件。
3. 使用PutKey策略操作将密钥策略应用于 KMS 密钥。

第 2 部分：使用 IAM 策略向 WorkSpaces 管理员授予额外权限

如果您选择客户托管的 KMS 密钥用于加密，则必须建立 IAM 策略，允许 Amazon WorkSpaces 代表您的账户中启动加密的 IAM 用户使用 KMS 密钥 WorkSpaces。该用户还需要获得使用Amazon的权限WorkSpaces。有关创建和编辑 IAM 用户策略的更多信息，请参阅《IAM 用户指南》中的管理 IAM 策略和 对 WorkSpaces 进行身份和访问管理。

WorkSpaces 加密需要对 KMS 密钥的有限访问权限。以下是您可以使用的一个示例密钥策略。此策略将可以管理 AWS KMS 密钥的主体与可以使用此密钥的主体分开。在使用此示例密钥策略之前，请将示例账户 ID 和 IAM 用户名替换为您账户中的实际值。

第一条语句与默认 AWS KMS 密钥策略相匹配。它授予您的账户使用 IAM 策略控制对 KMS 密钥的访问的权限。第二和第三条语句分别定义了 AWS 哪些委托人可以管理和使用密钥。第四条语句 AWS KMS 允许与集成的 AWS 服务代表指定的委托人使用密钥。该语句允许 AWS 服务创建和管理授权。该声明使用条件元素，将对 KMS 密钥的授权限制为 AWS 服务代表您账户中的用户进行的授权。

> **Note**
>
> 如果您的 WorkSpaces 管理员使用创建 WorkSpaces 加密卷，则管理员需要列出别名和列出密钥的权限（"kms:ListAliases"和"kms:ListKeys"权限）。 AWS Management Console 如果您的 WorkSpaces 管理员仅使用 Amazon WorkSpaces API（不使用控制台），则可以省略"kms:ListAliases"和"kms:ListKeys"权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:root"},
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
```

```
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:Create*",
        "kms:Describe*",
        "kms:Enable*",
        "kms:List*",
        "kms:Put*",
        "kms:Update*",
        "kms:Revoke*",
        "kms:Disable*",
        "kms:Get*",
        "kms:Delete*"
       ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": "*",
      "Condition": {"Bool": {"kms:GrantIsForAWSResource": "true"}}
    }
  ]
}
```

用于加密的用户或角色的 IAM 策略 WorkSpace 必须包括对客户托管的 KMS 密钥的使用权限以及对的访问 WorkSpaces权限。要向 IAM 用户或角色 WorkSpaces 授予权限，您可以将以下示例策略附加到 IAM 用户或角色。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ds:*",
                "ds:DescribeDirectories",
                "workspaces:*",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:CreateWorkspaces",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaces",
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces"
            ],
            "Resource": "*"
        }
    ]
}
```

用户需要以下 IAM 策略才能使用 AWS KMS。它为用户提供了对 KMS 密钥的只读访问权限以及创建授权的能力。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:Describe*",
                "kms:List*"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

如果您想在策略中指定 KMS 密钥，请使用类似于以下内容的 IAM 策略。将示例 KMS 密钥 ARN 替换为有效值。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kms:CreateGrant",
      "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource": "*"
    }
  ]
}
```

加密 WorkSpace

要加密 WorkSpace

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 选择 Launch WorkSpaces 并完成前三个步骤。
3. 对于 “WorkSpaces 配置” 步骤，请执行以下操作：
   a. 选择要加密的卷：根卷、用户卷或这两种卷。
   b. 对于加密密钥，请选择一个 AWS KMS 密钥，即 Amazon 创建的 AWS 托管 KMS 密钥 WorkSpaces 或您创建的 KMS 密钥。您选择的 KMS 密钥必须是对称的。Amazon WorkSpaces 不支持非对称 KMS 密钥。
   c. 选择下一步。
4. 选择 “启动” WorkSpaces。

查看已加密 WorkSpaces

要从 WorkSpaces 控制台查看哪些 WorkSpaces 和卷已加密，请WorkSpaces从左侧的导航栏中进行选择。“卷加密” 列显示 WorkSpace 每个卷加密是启用还是禁用。要查看哪些特定卷已加密，请展开 WorkSpace 条目以查看 “加密卷” 字段。

重启 a WorkSpace

有时，您可能需要 WorkSpace 手动重启（重新启动）。重新启动会 WorkSpace 断开用户的连接，然后关闭并重新启动用户。 WorkSpace为避免数据丢失，请确保用户在重新启动之前保存所有打开的文档和其他应用程序文件 WorkSpace。用户数据、操作系统和系统设置不受影响。

> **Warning**
>
> 要重新启动加密的 WorkSpace，请先确保AWS KMS密钥已启用；否则，密钥 WorkSpace 将无法使用。要确定是否启用 KMS 密钥，请参阅《AWS Key Management Service 开发人员指南》中的显示 KMS 密钥详细信息。

要重新启动 WorkSpace

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择。WorkSpaces
3. 选择 WorkSpaces 要重新启动的，然后选择操作，重新启动 WorkSpaces。
4. 当系统提示您确认时，选择 “重新启动” WorkSpaces。

要重启，请 WorkSpace 使用 AWS CLI

使用 reboot-workspaces 命令。

批量重启 WorkSpaces

使用 amazon-workspaces-admin-module.

重建一个 WorkSpace

重建时 WorkSpace 会重新创建从中启动的捆绑包的最新映像的根卷、其用户卷及其主 elastic network interface。 WorkSpace 与恢复相比，重建 WorkSpace 会删除更多的数据 WorkSpace，但它只需要您拥有用户卷的快照即可。要恢复 WorkSpace，请参阅还原 WorkSpace。

重建 a WorkSpace 会导致出现以下情况：

- 根卷（对于 Microsoft Windows，驱动器 C；Linux，/）将使用创建 WorkSpace 该捆绑包的最新映像进行刷新。任何已安装的应用程序或在创建后更改的 WorkSpace 系统设置都将丢失。
- 用户卷（对于 Microsoft Windows，为 D 驱动器；对于 Linux，为 /home）是从最新快照中重新创建的。用户卷的当前内容将被覆盖。

  重建时使用的自动快照计划 WorkSpace 每 12 小时一次。无论用户卷的运行状况如何，都会拍摄用户卷的这些快照 WorkSpace。选择 “操作”、“重建/恢复” 时 WorkSpace，将显示最新快照的日期和时间。

  重建时 WorkSpace，还会在重建完成后不久（通常在 30 分钟内）拍摄新的快照。
- 主要弹性网络接口已重新创建。 WorkSpace 接收新的私有 IP 地址。

> **Important**
>
> 2020 年 1 月 14 日之后，通过公共 Windows 7 捆绑包 WorkSpaces 创建的软件将无法再重新构建。你可能需要考虑将 Windows 7 迁移 WorkSpaces 到 Windows 10。有关更多信息，请参阅 迁移 WorkSpace。

WorkSpace 只有满足以下条件才能重新构建：

- 的状态 WorkSpace 必须为`AVAILABLE`、`ERROR`、`UNHEALTHY`或`STOPPED`、或`REBOOTING`。要重建 WorkSpace 处于该`REBOOTING`状态的，必须使用 RebuildWorkspacesAPI 操作或 rebuild- AWS CLI workspaces 命令。
- 用户卷的快照必须存在。

要重建 WorkSpace

> **Warning**
>
> 要重建加密的 WorkSpace，请先确保 AWS KMS 密钥已启用；否则，密钥将 WorkSpace 无法使用。要确定是否启用 KMS 密钥，请参阅《AWS Key Management Service 开发人员指南》中的显示 KMS 密钥详细信息。

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择要重建 WorkSpace ，然后选择 “操作”、“重建”/“恢复” WorkSpace。
4. 在快照下，选择快照的时间戳。
5. 选择 Rebuild (重建)。

要重新构建， WorkSpace 请使用 AWS CLI

使用 rebuild-workspaces 命令。

故障排除

如果您在 Active Directory 中更改AccountName用户的 saM 用户命名属性 WorkSpace 后重新构建，则可能会收到以下错误消息：

```
"ErrorCode": "InvalidUserConfiguration.Workspace"
"ErrorMessage": "The user was either not found or is misconfigured."
```

要解决此问题，要么恢复到原始用户命名属性，然后重新启动重建，要么 WorkSpace 为该用户创建一个新的用户命名属性。

还原 WorkSpace

还原 WorkSpace 将根据在 WorkSpace 运行状况良好时创建的这些卷的最新快照来重新创建根卷和用户卷。与重建 WorkSpace 相比，还原 WorkSpace 时删除的数据要少。但是，它要求您同时拥有根卷和用户卷的快照，而重建 WorkSpace 只需要用户卷的快照。要重建 WorkSpace，请参阅重建一个 WorkSpace。

还原 WorkSpace 将导致以下情况的出现：

- 根卷（对于 Microsoft Windows，为驱动器 C；对于 Linux，为 /）将还原到最新快照中。在创建最新快照之后安装的所有应用程序或更改的系统设置都将丢失。
- 用户卷（对于 Microsoft Windows，为 D 驱动器；对于 Linux，为 /home）是从最新快照中重新创建的。用户卷的当前内容将被覆盖。

拍摄快照时

根卷和用户卷的快照是在以下基础上拍摄的。依次选择操作、重建/还原 WorkSpace 时，将显示最新快照的日期和时间。

- 首次创建 WorkSpace 之后 - 通常，根卷和用户卷的初始快照是在 WorkSpace 创建后不久（通常在 30 分钟内）拍摄的。在某些 AWS 区域，创建 WorkSpace 后可能需要几个小时才能拍摄初始快照。

  如果在拍摄初始快照之前 WorkSpace 运行状况不佳，则无法还原 WorkSpace。在这种情况下，您可以尝试重建 WorkSpace 或联系 AWS Support 寻求帮助。
- 正常使用期间 - 每 12 小时安排一次在还原 WorkSpace 时使用的自动快照。如果 WorkSpace 运行状况良好，则将同时创建根卷和用户卷的快照。如果 WorkSpace 运行状况不佳，则仅针对用户卷创建快照。
- WorkSpace 还原后 - 还原 WorkSpace 时，将在还原完成后不久（通常在 30 分钟内）拍摄新快照。在某些 AWS 区域，还原 WorkSpace 后可能需要几个小时才能拍摄这些快照。

  还原 WorkSpace 后，如果 WorkSpace 在拍摄新快照之前运行状况不佳，则无法再次还原 WorkSpace。在这种情况下，您可以尝试重建 WorkSpace 或联系 AWS Support 寻求帮助。

您只能在满足以下条件时还原 WorkSpace：

- WorkSpace 的状态必须为 `AVAILABLE`、`ERROR`、`UNHEALTHY` 或 `STOPPED`。
- 根卷和用户卷的快照必须存在。

还原 WorkSpace

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择要还原的 WorkSpace，然后依次选择操作、重建/还原 WorkSpace。
4. 在快照下，选择快照的时间戳。
5. 选择 Restore（还原）。

使用 AWS CLI 还原 WorkSpace

使用 restore-workspace 命令。

Microsoft 365 自带许可 (BYOL)

亚马逊 WorkSpaces 允许你自带微软365许可证，前提是这些许可证符合微软的许可要求。这些许可证允许你安装和激活由以下操作系统提供支持的企业软件 WorkSpaces 的 Microsoft 365 应用程序：

- Windows 10（自带许可证）
- Windows 11（自带许可证）
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

要在上使用微软 365 企业版应用程序 WorkSpaces，你必须订阅微软 365 E3/E5、微软 365 A3/A5 或微软 365 商业高级版。

在你的亚马逊上， WorkSpaces 你可以使用你的微软 365 许可证安装和激活微软 365 企业版应用程序，包括以下内容：

- Microsoft Word
- Microsoft Excel
- 微软 PowerPoint
- Microsoft Outlook
- 微软 OneDrive

有关更多信息，请参阅 Microsoft 365 Apps 企业版的完整列表。

你也可以安装微软 365 中未包含的微软应用程序，例如微软 Project、Microsoft Visio 和 Microsoft Power Automate， WorkSpaces 但你需要自带额外的许可证。

你可以在主 WorkSpaces 服务器上安装和使用 Microsoft 365 和其他 Microsoft 应用程序，也可以 WorkSpaces 使用多区域弹性进行故障转移。

内容

- WorkSpaces 使用微软 365 企业版应用程序进行创作

- 迁移现有应用程序 WorkSpaces 以使用适用于企业的微软 365 应用程序
- 在上更新你的 Microsoft 365 企业版应用程序 WorkSpaces

WorkSpaces 使用微软 365 企业版应用程序进行创作

要 WorkSpaces 使用 Microsoft 365 企业版应用程序进行创建，必须创建安装了应用程序的自定义映像，然后使用它来创建自定义软件包。您可以使用该捆绑包来启动 WorkSpaces 已安装应用程序的新版本。 WorkSpaces 不提供企业版 Microsoft 365 应用程序的公共捆绑包。

要 WorkSpaces 使用微软 365 企业版应用程序创建，请执行以下操作：

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 启动 WorkSpace 一个你想用作其他 Microsoft 应用程序的镜像 WorkSpaces。您将在此处安装 Microsoft 应用程序。有关启动的更多信息 WorkSpace，请参阅使用启动虚拟桌面 WorkSpaces。
3. 通过 https://clients.amazonworkspaces.com/ 启动客户端应用程序，输入邀请电子邮件中的注册码，然后选择注册。
4. 当系统提示登录时，输入用户的登录凭证，然后选择登录。
5. 安装和配置 Microsoft 365 Apps 企业版。
6. 从中创建自定义映像 WorkSpace，然后用它来创建自定义捆绑包。有关创建自定义映像和捆绑包的更多信息，请参阅创建自定义 WorkSpaces 映像和捆绑包。
7. WorkSpaces 使用您创建的自定义捆绑包启动。它们安装 WorkSpaces 了微软 365 企业版应用程序。

迁移现有应用程序 WorkSpaces 以使用适用于企业的微软 365 应用程序

如果你 WorkSpaces 没有 Microsoft Office 许可证AWS，你可以在自己的设备上安装和配置适用于企业的 Microsoft 365 应用程序 WorkSpaces。

如果你 WorkSpaces 确实有微软 Office 许可证AWS，则在安装企业版微软 365 应用程序之前，必须先取消注册微软 Office 许可证。

> **Important**
>
> 从你那里卸载 Microsoft Office 应用程序 WorkSpaces 并不会取消许可证的注册。为避免被收取微软 Office 许可证费用，请执行以下任一操作， WorkSpaces 从微软 Office 应用程序中AWS注销你的微软 Office 应用程序：

- 管理应用程序（推荐）— 你可以从你的应用程序中卸载 Microsoft Office 2016 和 2019 WorkSpaces。有关更多信息，请参阅管理应用程序。卸载后，你可以在上安装适用于企业的 Microsoft 365 应用程序 WorkSpaces。
- 迁移 WorkSpace — 您可以将一个 WorkSpace 捆绑包迁移到另一个捆绑包，同时将数据保留在用户卷上。
  - 将你迁移 WorkSpaces 到包含没有 Microsoft Office 订阅的图片的捆绑包。迁移完成后，你可以在自己的设备上安装 Microsoft 365 企业版应用程序 WorkSpaces。
  - 或者，创建已在 WorkSpaces 映像上安装了 Microsoft 365 企业版应用程序的自定义映像和捆绑包，然后将您的映像迁移 WorkSpaces 到这个新的自定义捆绑包。迁移完成后，你的 WorkSpaces 用户就可以开始使用适用于企业的 Microsoft 365 应用程序了。
  - 有关如何迁移的更多信息 WorkSpaces，请参阅迁移 WorkSpace。

在上更新你的 Microsoft 365 企业版应用程序 WorkSpaces

默认情况下，你在微软 Windows 操作系统上 WorkSpaces 运行的配置为接收来自 Windows Update 的更新。但是，Microsoft 365 Apps 企业版的更新无法通过 Windows 更新获得。将更新设置为从 Office CDN 自动运行，或者将 Windows Server Update Services (WSUS) 与 Microsoft Configuration Manager 配合使用，以更新 Microsoft 365 Apps 企业版。有关更多信息，请参阅使用 Microsoft Configuration Manager 管理 Microsoft 365 Apps 的更新。要设置 Microsoft 365 应用程序更新的频率，请指定更新渠道并将其设置为 “当前” 或 “企业月度”，以符合 Microsoft 365 的 WorkSpaces许可政策。

升级 Windows BYOL WorkSpaces

在 Windows 自带许可证 (BYOL) 上 WorkSpaces，你可以使用就地升级过程升级到较新版本的 Windows。为此，请按照本主题中的说明操作。

就地升级过程仅适用于 Windows 10 和 11 BY WorkSpaces OL。

> **Important**
>
> 不要在升级后的版本上运行 Sysprep。 WorkSpace如果这样做，可能会发生阻止 Sysprep 完成的错误。如果您计划运行 Sysprep，请仅在尚未升级的上执行 WorkSpace 此操作。

> **Note**
>
> 你可以使用此过程将 Windows 10 和 11 升级 WorkSpaces 到更新的版本。但是，此过程不能用于将你的 Windows 10 升级 WorkSpaces 到 Windows 11。

内容

先决条件

- 如果您使用组策略或系统中心配置管理器 (SCCM) 推迟或暂停 Windows 10 和 11 升级，请为 Windows 10 和 11 启用操作系统升级。 WorkSpaces
- 如果 WorkSpace 是 AutoStop WorkSpace，则将其更改为就地升级过程 AlwaysOn WorkSpace之前的，这样在应用更新时它就不会自动停止。有关更多信息，请参阅 修改运行模式。如果您希望将 WorkSpace 设置保留为 AutoStop，请在升级进行 AutoStop 时将时间更改为三小时或更长时间。
- 就地升级过程通过制作名为 Default User (`C:\Users\Default`) 的特殊配置文件的副本来重新创建用户配置文件。请勿使用此默认用户配置文件进行自定义。而是建议通过组策略对象 (GPO) 对用户配置文件进行任何自定义。通过 GPO 进行的自定义设置可以很容易地进行修改或回滚，并且不易出错。
- 就地升级过程只能备份和重新创建一个用户配置文件。如果您在驱动器 D 上有多个用户配置文件，请删除除所需配置文件之外的所有用户配置文件。

注意事项

就地升级过程使用两个注册表脚本（`enable-inplace-upgrade.ps1`和`update-pvdrivers.ps1`）对您的注册表脚本进行必要的更改 WorkSpaces ，从而使 Windows 更新进程能够

运行。这些更改涉及在驱动器 C 而不是驱动器 D 上创建（临时）用户配置文件。如果驱动器 D 上已存在用户配置文件，则该原始用户配置文件中的数据保留在驱动器 D 上。

默认情况下，在中 WorkSpaces 创建用户配置文件`D:\Users\%USERNAME%`。`enable-inplace-upgrade.ps1` 脚本会将 Windows 配置为在 `C:\Users\%USERNAME%` 中创建新的用户配置文件，并将用户 Shell 文件夹重定向到 `D:\Users\%USERNAME%`。这个新的用户配置文件是在用户首次登录时创建的。

就地升级后，您可以选择将用户配置文件保留在驱动器 C 上，以允许用户在将来使用 Windows 更新进程升级其计算机。但是，请注意 WorkSpaces ，如果配置文件存储在驱动器 C 上，则无法在不丢失用户配置文件中的所有数据的情况下重建或迁移，除非您自己备份和恢复这些数据。如果您决定将配置文件保留在驱动器 C 上，则可以使用UserShellFoldersRedirection注册表项将用户 shell 文件夹重定向到驱动器 D，如本主题后面所述。

为确保您可以重建或迁移您的 shell， WorkSpaces 并避免用户 shell 文件夹重定向出现任何潜在问题，我们建议您在就地升级后选择将用户配置文件还原到驱动器 D。您可以使用 PostUpgradeRestoreProfileOnD 注册表项来执行此操作，如本主题后面所述。

已知限制条件

- 在 WorkSpace 重建或迁移过程中，用户配置文件位置不会从驱动器 D 更改为驱动器 C。如果您在 Windows 10 或 11 BYOL 上执行就地升级， WorkSpace 然后对其进行重建或迁移，则新版本 WorkSpace 将在驱动器 D 上保存用户配置文件。

  > **Warning**
  >
  > 如果在就地升级后将用户配置文件保留在驱动器 C 上，则在重建或迁移过程中存储在驱动器 C 上的用户配置文件数据将丢失，除非您在重建或迁移之前手动备份用户配置文件数据，并在运行重建或迁移过程后手动还原用户配置文件数据。

- 如果您的默认 BYOL 包包含基于 Windows 10 和 11 早期版本的映像，则必须在重建或迁移后再次执行就 WorkSpace 地升级。

注册表项设置摘要

要启用就地升级过程并指定您要在升级后放置用户配置文件的位置，您必须设置多个注册表项。

注册表路径：HKL M:\Software\Amazon\WorkSpacesConfig\ .ps1 enable-inplace-upgrade

注册表项	Type	值
Enabled (已启用)	DWORD	0 – (默认值) 禁用就地升级 1 – 启用就地升级
PostUpgradeRestoreProfileOnD	DWORD	0 – (默认值) 在就地升级后，不尝试还原用户配置文件路径 1-就地升级后恢复用户配置文件路径 (ProfileImagePath)
UserShellFoldersRedirection	DWORD	0 – 不对用户 Shell 文件夹进行重定向 1 – (默认值) 在用户配置文件在 `C:\Users\%USERNAME%` 上重新生成后，将用户 Shell 文件夹重定向到 `D:\Users\%USERNAME%`
NoReboot	DWORD	0 – (默认值) 允许您控制在修改用户配置文件的注册表后何时重启 1 — 不允许脚本 WorkSpace 在修改用户配置文件的注册表后重新启动

注册表路径：HKL M:\Software\Amazon\WorkSpacesConfig\ up date-pvdrivers.ps1

注册表项	Type	值
Enabled (已启用)	DWORD	0 — (默认) 禁用 AWS PV 驱动程序更新

注册表项	Type	值
		1 — 启用 AWS PV 驱动程序更新

执行就地升级

要在 BYOL 上启用就地升级 Windows WorkSpaces，必须设置某些注册表项，如以下过程所述。您还必须设置某些注册表项，以指示您希望在完成就地升级后在其中放置用户配置文件的驱动器（C 或 D）。

您可以手动进行这些注册表更改。如果您有多个 WorkSpaces 要更新，则可以使用组策略或 SCCM 来推送脚本。 PowerShell 有关示例 PowerShell脚本，请参阅使用 PowerShell 脚本更新您的 WorkSpace 注册表。

执行 Windows 10 和 11 的就地升级

1. 记下你正在更新的 Windows 10 和 11 BYOL WorkSpaces 上当前运行的是哪个版本的 Windows，然后重新启动它们。
2. 更新以下 Windows 系统注册表项，将 Enabled (启用) 的数值数据从 0 更改为 1。这些注册表更改允许就地升级。 WorkSpace

   - HKEY_LOCAL_MACHINE\ SOFTWARE\ 亚马逊\\ .ps1 WorkSpacesConfig enable-inplace-upgrade
   - HKEY_LOCAL_MACHINE\ SOFTWARE\ 亚马逊\\ update-pvdrivers.ps1 WorkSpacesConfig

   > **Note**
   >
   > 如果这些密钥不存在，请重新启动 WorkSpace。重新启动系统时，应该会添加这些键。

   （可选）如果您使用诸如 SCCM 任务序列之类的托管工作流来执行升级，请将以下键值设置为 1 以防止计算机重新启动：

   HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\\ .ps1\ WorkSpacesConfig enable-inplace-upgrade NoReboot

3. 决定您希望在就地升级过程后将用户配置文件放在哪个驱动器上（有关详细信息，请参阅注意事项），并按以下方式设置注册表项：

   - 如果您希望在升级后用户配置文件位于驱动器 C 上，请设置：

     HKEY_LOCAL_MACHINE\ SOFTWARE\ 亚马逊\\ .ps1 WorkSpacesConfig enable-inplace-upgrade

     密钥名称：PostUpgradeRestoreProfileOnD

     键值：0

     密钥名称：UserShellFoldersRedirection

     键值：1

   - 如果您希望在升级后用户配置文件位于驱动器 D 上，请设置：

     HKEY_LOCAL_MACHINE\ SOFTWARE\ 亚马逊\\ .ps1 WorkSpacesConfig enable-inplace-upgrade

     密钥名称：PostUpgradeRestoreProfileOnD

     键值：1

     密钥名称：UserShellFoldersRedirection

     键值：0

4. 将更改保存到注册表后， WorkSpace 再次重新启动以应用更改。

> **Note**
>
> - 重新启动后，登录到会 WorkSpace 创建新的用户配置文件。您可能会在开始菜单中看到占位符图标。此问题在就地升级完成后会自动解决。
> - 等待 10 分钟以确保畅通 WorkSpace 无阻。

（可选）确认将以下密钥值设置为 1，这将解除 WorkSpace 对更新的阻止：

HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\\ .ps1\ 已删除 WorkSpacesConfig enable-inplace-upgrade profileImagePath

5. 执行就地升级。您可以使用任何您喜欢的方法，例如 SCCM、ISO 或 Windows Update (WU)。根据你最初的 Windows 10 和 11 版本以及安装了多少应用程序，此过程可能需要 40 到 120 分钟。

> **Note**
>
> 就地升级过程可能至少需要一个小时。 WorkSpace 实例状态可能显示为升级UNHEALTHY期间。

6. 更新过程结束后，请确认 Windows 版本已更新。

> **Note**
>
> 如果就地升级失败，Windows 会自动回滚以使用你开始升级之前使用的 Windows 10 和 11 版本。有关疑难解答的更多信息，请参阅 Microsoft 文档。

（可选）要确认更新脚本已成功执行，请验证以下键值是否设置为 1：

HKEY_LOCAL_MACHINE\ SOFTWARE\ Amazon\\ .ps1\ WorkSpacesConfig enable-inplace-upgrade scriptExecutionComplete

7. 如果您 WorkSpace 通过将运行模式设置为 AlwaysOn 或更改 AutoStop 时间段来修改运行模式，以便就地升级过程可以不间断地运行，请将运行模式重新设置为原始设置。有关更多信息，请参阅修改运行模式。

如果您尚未将 PostUpgradeRestoreProfileOnD 注册表项设置为 1，则用户配置文件将由 Windows 重新生成并在就地升级`C:\Users\%USERNAME%`后放入，这样将来的 Windows 10 和 11 就地升级就不必再次执行上述步骤。默认情况下，`enable-inplace-upgrade.ps1` 脚本将以下 Shell 文件夹重定向到驱动器 D：

- `D:\Users\%USERNAME%\Downloads`
- `D:\Users\%USERNAME%\Desktop`
- `D:\Users\%USERNAME%\Favorites`
- `D:\Users\%USERNAME%\Music`
- `D:\Users\%USERNAME%\Pictures`

- D:\Users\%USERNAME%\Videos
- D:\Users\%USERNAME%\Documents
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Network Shortcuts
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\SendTo
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
- D:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Templates

如果您将 shell 文件夹重定向到您的其他位置 WorkSpaces，请在就地升级 WorkSpaces 之后对执行必要的操作。

故障排除

如果您在更新过程中遇到任何问题，可以查看以下各项以帮助排除故障：

- Windows 日志，默认情况下位于以下位置：

  C:\Program Files\Amazon\WorkSpacesConfig\Logs\

  C:\Program Files\Amazon\WorkSpacesConfig\Logs\TRANSMITTED

- Windows 事件查看器

  Windows 日志 > 应用程序 > 来源：亚马逊 WorkSpaces

> **Tip**
>
> 在就地升级过程中，如果您看到桌面上的某些图标快捷方式不再起作用，那是因为 WorkSpaces 将驱动器 D 上的所有用户配置文件移至驱动器 C 以准备升级。升级完成后，快捷方式将正常工作。

使用 PowerShell 脚本更新您的 WorkSpace 注册表

您可以使用以下示例 PowerShell 脚本更新您的注册表 WorkSpaces 以启用就地升级。请按照执行就地升级，但使用此脚本更新每个注册表 WorkSpace。

```
# AWS WorkSpaces 1.28.20
# Enable In-Place Update Sample Scripts
# These registry keys and values will enable scripts to run on the next reboot of the
 WorkSpace.

$scriptlist = ("update-pvdrivers.ps1","enable-inplace-upgrade.ps1")
$wsConfigRegistryRoot="HKLM:\Software\Amazon\WorkSpacesConfig"
$Enabled = 1
$script:ErrorActionPreference = "Stop"

foreach ($scriptName in $scriptlist)
{
    $scriptRegKey = "$wsConfigRegistryRoot\$scriptName"

    try
    {
        if (-not(Test-Path $scriptRegKey))
        {
            Write-Host "Registry key not found. Creating registry key '$scriptRegKey'
 with 'Update' enabled."
            New-Item -Path $wsConfigRegistryRoot -Name $scriptName | Out-Null
            New-ItemProperty -Path $scriptRegKey -Name Enabled -PropertyType DWord -
Value $Enabled | Out-Null
            Write-Host "Value created. '$scriptRegKey' Enabled='$((Get-ItemProperty -
Path $scriptRegKey).Enabled)'"
        }
        else
        {
            Write-Host "Registry key is already present with value '$scriptRegKey'
 Enabled='$((Get-ItemProperty -Path $scriptRegKey).Enabled)'"
            if((Get-ItemProperty -Path $scriptRegKey).Enabled -ne $Enabled)
            {
                Set-ItemProperty -Path $scriptRegKey -Name Enabled -Value $Enabled
                Write-Host "Value updated. '$scriptRegKey' Enabled='$((Get-ItemProperty
 -Path $scriptRegKey).Enabled)'"
            }
        }
    }
```

```
    catch
    {
        write-host "Stopping script, the following error was encountered:" `r`n$_ -
ForegroundColor Red
        break
    }
}
```

迁移 WorkSpace

> **Note**
>
> 如果你想取消订阅或卸载 Microsoft Office 版本AWS的许可证 WorkSpace，我们建议你使用管理应用程序。

您可以将 WorkSpace 从一个捆绑包迁移到另一个捆绑包，同时将数据保留在用户卷上。下面是一些示例方案：

- 你可以 WorkSpaces 从 Windows 7 桌面体验迁移到 Windows 10 桌面体验。
- 您可以 WorkSpaces 从 PCoIP 协议迁移到 WorkSpaces 流式传输协议 (WSP)。
- 你可以 WorkSpaces 从 Windows Server 上的 32 位微软 Office 2016 版本的 WorkSpaces 捆绑包迁移到 Windows Server 2019 上的 64 位微软 Office 和支持 Windows Server 2022 的捆绑包。 WorkSpaces
- 您可以 WorkSpaces 从一个公共或自定义捆绑包迁移到另一个捆绑包。例如，你可以从支持 GPU（Graphics.g4dn）迁移。 GraphicsPro.g4dn、Graphics 和 GraphicsPro) 捆绑到不支持 GPU 的捆绑包，反之亦然。
- 你可以 WorkSpaces 从 Windows 10 BYOL 迁移到 Windows 11 BYOL，但不支持从 Windows 11 迁移到 Windows 10。
- Windows 11 不支持经济捆绑包。要将你的 Windows 7 或 10 超值套装迁移 WorkSpaces 到 Windows 11，你需要先将你的超值套装切换 WorkSpaces 到更大的套装产品。
- 在 WorkSpaces 从 Windows 7 迁移到 Windows 11 之前，你需要将其迁移到 Windows 10。在将其迁移到 Windows 11 之前，请 WorkSpace 至少登录一次 Windows 10。不支持从 Windows 7 WorkSpaces 直接迁移到 Windows 11。
- 你可以将使用微软 Office WorkSpaces 的 Windows 迁移AWS到包含微软 365 应用程序的自定义 WorkSpaces 捆绑包。迁移完成后， WorkSpaces 你将取消订阅微软 Office。

- 你可以将使用微软 Office WorkSpaces 的 Windows 迁移AWS到没有 Office 2016/2019 订阅的 WorkSpaces捆绑包中。迁移完成后， WorkSpaces 你将取消订阅微软 Office。

有关 Amazon WorkSpaces 捆绑包的更多信息，请参阅WorkSpace 捆绑包和图片。

迁移过程使用目标捆绑包映像中的新根卷和原始 WorkSpace包上次可用快照中的用户卷来重新创建。WorkSpace 迁移过程中会生成一个新的用户配置文件，以获得更好的兼容性。将重命名旧用户配置文件，然后将旧用户配置文件中的某些文件移动到新用户配置文件。（有关所移动的内容的详细信息，请参阅迁移过程中会发生什么。）

每次迁移过程最多需要一个小时 WorkSpace。启动迁移过程时，会创建一个新的 WorkSpace 迁移过程。如果发生导致无法成功迁移的错误， WorkSpace 则会恢复原始文件并将其恢复到其原始状态，然后终止新的 WorkSpace 迁移。

目录

迁移限制

- 您不能迁移到公有或自定义 Windows 7 桌面体验捆绑包。您也不能迁移到自带许可证 (BYOL) Windows 7 捆绑包。
- 您 WorkSpaces 只能将 BYOL 迁移到其他 BYOL 捆绑包。要将 BYOL WorkSpace 从 PCoIP 迁移到 WSP，必须先使用 WSP 协议创建 BYOL 捆绑包。然后，你可以将你的 PCoIP BYOL 迁移到那个 WSP BYOL WorkSpaces 捆绑包。
- 您无法将从公共或自定义捆绑包中 WorkSpace 创建的分发包迁移到 BYOL 捆绑包。
- Graphics.g4dn、 GraphicsPro .g4dn、Graphics 和 GraphicsPro 捆绑包目前仅适用于 PCoIP 协议，因此 Graphics.g4dn、.g4dn、Graphics，还无法迁移到 WSP。 GraphicsPro GraphicsPro WorkSpaces

- WorkSpaces 目前不支持迁移 Linux。
- 在支持多种语言的AWS区域中，您可以在语言包 WorkSpaces之间迁移。
- 源捆绑包和目标捆绑包必须不同。（但是，在支持多种语言的区域中，只要语言不同，就可以迁移到相同的 Windows 10 捆绑包。）如果您想 WorkSpace 使用相同的捆绑包刷新，请 WorkSpace改为重新构建。
- 您无法 WorkSpaces 跨区域迁移。
- 在某些情况下，如果迁移无法成功完成，您可能不会收到错误消息，并且可能显示迁移过程未启动。如果在尝试迁移一小时后 WorkSpace 捆绑包保持不变，则迁移不成功。请联系 AWS Support 中心以获取帮助。

迁移场景

下表显示了哪些迁移方案可用：

源操作系统	目标操作系统	是否可用？
公有或自定义捆绑包 Windows 7	公有或自定义捆绑包 Windows 10	是
自定义捆绑包 Windows 7	公有捆绑包 Windows 7	否
自定义捆绑包 Windows 7	自定义捆绑包 Windows 7	否
公有捆绑包 Windows 7	自定义捆绑包 Windows 7	否
公有或自定义捆绑包 Windows 10	公有或自定义捆绑包 Windows 7	否
公有或自定义捆绑包 Windows 10	自定义捆绑包 Windows 10	是
Windows 7 BYOL 捆绑包	Windows 7 BYOL 捆绑包	否
Windows 7 BYOL 捆绑包	Windows 10 BYOL 捆绑包	是
Windows 10 BYOL 捆绑包	Windows 7 BYOL 捆绑包	否
Windows 10 BYOL 捆绑包	Windows 10 BYOL 捆绑包	是

源操作系统	目标操作系统	是否可用？
支持 Windows Server 2016 的公有 Windows 10 捆绑包	支持 Windows Server 2019 的公有 Windows 10 捆绑包 	是
支持 Windows Server 2019 的公有 Windows 10 捆绑包 	支持 Windows Server 2016 的公有 Windows 10 捆绑包	是
Windows 10 BYOL 捆绑包	Windows 11 BYOL 捆绑包	是
Windows 11 BYOL 捆绑包	Windows 10 BYOL 捆绑包	否
支持 Windows Server 2016 的自定义 Windows 10 捆绑包	支持 Windows Server 2019 的公有 Windows 10 捆绑包	是
支持 Windows Server 2016 的自定义 Windows 10 捆绑包	支持 Windows Server 2022 的公有 Windows 10 捆绑包	是
支持 Windows Server 2019 的自定义 Windows 10 捆绑包	支持 Windows Server 2022 的公有 Windows 10 捆绑包	是

Note

Web Access 不适用于支持 Windows Server 2019 的公有 Windows 10 捆绑包 PCoIP 分支。

Important

支持 Windows Server 2016 的公有 Windows 10 plus 捆绑包含有 Microsoft Office 2016 和 Trend Micro Worry-Free Business Security Services。支持 Windows Server 2019 的公有 Windows 10 plus 捆绑包仅含有 Microsoft Office 2019，不含 Trend Micro Services。

迁移过程中会发生什么

在迁移过程中，用户卷（驱动器 D）上的数据将保留，但根卷（驱动器 C）上的所有数据都将丢失。这意味着不会保留已安装的应用程序、设置和对注册表的更改。旧用户配置文件文件夹将使用 .NotMigrated 后缀重命名，并创建一个新的用户配置文件。

迁移过程基于原始用户卷的最后一个快照重新创建驱动器 D。在首次启动新文件夹时 WorkSpace，迁移过程会将原始D:\Users\%USERNAME%文件夹移动到名为的文件夹D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated。新的操作系统生成一个新的 D:\Users\%USERNAME%\ 文件夹。

创建新用户配置文件后，以下用户 shell 文件夹中的文件将从旧 .NotMigrated 配置文件移动到新配置文件：

- D:\Users\%USERNAME%\Desktop
- D:\Users\%USERNAME%\Documents
- D:\Users\%USERNAME%\Downloads
- D:\Users\%USERNAME%\Favorites
- D:\Users\%USERNAME%\Music
- D:\Users\%USERNAME%\Pictures
- D:\Users\%USERNAME%\Videos

Important

迁移过程尝试将文件从旧用户配置文件移动到新配置文件。迁移过程中未移动的任何文件将保留在 D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated 文件夹中。如果迁移成功，您可以看到哪些文件被移入 C:\Program Files\Amazon\WorkspacesConfig\Logs\MigrationLogs。您可以手动移动任何未自动移动的文件。
默认情况下，公有捆绑包禁用本地搜索索引。如果您要启用它，则默认设置为搜索 C:\Users 而不是搜索 D:\Users，因此您也需要对其进行调整。如果您已将本地搜索索引专门设置为 D:\Users*username*，而未设置为 D:\Users，则迁移后可能无法对 D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated 文件夹中的任何用户文件使用本地搜索索引。

在迁移过程中，分配给原始标签的所有标签 WorkSpace 都将被保留，并保留 WorkSpace 的运行模式。但是，新用户 WorkSpace 会获得新的 WorkSpace ID、计算机名称和 IP 地址。

最佳实践

在迁移之前 WorkSpace，请执行以下操作：

- 将驱动器 C 上的任何重要数据备份到另一个位置。在迁移过程中，将擦除驱动器 C 上的所有数据。
- 请确保 WorkSpace 正在迁移的已有至少 12 小时的时间，以确保已创建用户卷的快照。在 Amazon WorkSpaces 控制台的 Migrat e WorkSpaces 页面上，您可以看到上次拍摄快照的时间。在迁移过程中，上一个快照之后创建的所有数据将丢失。
- 为避免潜在的数据丢失，请确保您的用户注销其账户， WorkSpaces并且在迁移过程完成后才重新登录。请注意，当它们处于ADMIN_MAINTENANCE模式时 WorkSpaces 无法迁移。
- 确保 WorkSpaces 要迁移的状态为AVAILABLESTOPPED、或ERROR。
- 请确保您有足够的 IP 地址供 WorkSpaces 要迁移的。在迁移期间，将为分配新的 IP 地址 WorkSpaces。
- 如果您使用脚本进行迁移 WorkSpaces，请分批迁移它们，一次不超过 25 WorkSpaces 个。

排查问题

- 如果用户在迁移后报告丢失文件，请检查其用户配置文件是否在迁移过程中未移动。您可以看到哪些文件被移入 C:\Program Files\Amazon\WorkspacesConfig\Logs\MigrationLogs。未移动的文件将位于 D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated 文件夹中。您可以手动移动任何未自动移动的文件。
- 如果您正在使用 API 进行迁移 WorkSpaces ，但迁移未成功，则不会使用该 API 返回的目标 WorkSpace ID，并且仍 WorkSpace将使用原始 WorkSpace ID。
- 如果迁移未成功完成，请检查 Active Directory 以查看它是否相应地被清理了。您可能需要手动删除 WorkSpaces 不再需要的内容。

账单如何受到影响

在迁移发生的当月，您需要为新迁移和原始 WorkSpaces迁移按比例支付费用。例如，如果您在 5 月 10 日将 WorkSpace A 迁移到 WorkSpace B，则将在 5 月 1 日至 5 月 10 日期间支付 WorkSpace A 费用，并在 5 月 11 日至 5 月 30 日期间支付 WorkSpace B 费用。

> **Note**
>
> 如果 WorkSpace 要将 a 迁移到不同的捆绑包类型（例如，从 “性能” 到 “Power”，或 “Value” 到 “标准”），则在迁移过程中，根卷（驱动器 C）和用户卷（驱动器 D）的大小可能会增加。如有必要，根卷增加以匹配新捆绑包的默认根卷大小。但是，如果您已为用户卷指定的大小与原始捆绑包的默认大小不同（更高或更低），则在迁移过程中会保留相同的用户卷大小。否则，迁移过程将使用源 WorkSpace 用户卷大小中较大的容量和新捆绑包的默认用户卷大小。

迁移 WorkSpace

您可以 WorkSpaces 通过亚马逊 WorkSpaces 控制台、AWS CLI或亚马逊 WorkSpaces API 进行迁移。

要迁移 WorkSpace

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择。WorkSpaces
3. 选择您的 WorkSpace ，然后选择操作，迁移 WorkSpaces。
4. 在捆绑包下，选择您要迁移到的捆绑包 WorkSpace 。

   > **Note**
   >
   > 要将 BYOL WorkSpace 从 PCoIP 迁移到 WSP，必须先使用 WSP 协议创建 BYOL 捆绑包。然后，你可以将你的 PCoIP BYOL 迁移到那个 WSP BYOL WorkSpaces 捆绑包。

5. 选择迁移 WorkSpaces。

   Amazon WorkSpaces 控制台中`PENDING`会出现一个状态为的新 WorkSpace 内容。迁移完成后，原始 WorkSpace 迁移将终止，新迁移的状态设置 WorkSpace 为`AVAILABLE`。
6. （可选）要删除您不再需要的任何自定义捆绑包和映像，请参阅删除自定义 WorkSpaces 捆绑包或图片。

要 WorkSpaces 通过迁移AWS CLI，请使用 migrat e-workspace 命令。要 WorkSpaces 通过亚马逊 WorkSpaces API 进行迁移，请参阅MigrateWorkSpace《亚马逊 WorkSpaces API 参考》。

删除 WorkSpace

当不再使用某个 WorkSpace 时，可以将其删除。还可以删除相关资源。

> **Warning**
>
> 删除 WorkSpace 是一项永久性操作，无法撤消。WorkSpace 用户的数据不会保留，而是会销毁。要获取有关备份用户数据的帮助，请联系 AWS Support。

> **Note**
>
> Simple AD 和 AD Connector 供您免费使用，可用于 WorkSpaces。如果连续 30 天没有一起使用 WorkSpaces 与您的 Simple AD 或 AD Connector 目录，则系统将自动取消注册该目录，无法再将其用于 Amazon WorkSpaces，而且将根据 AWS Directory Service 定价条款向您收取该目录的费用。
>
> 要删除空目录，请参阅删除 WorkSpaces 的目录。如果您删除了 Simple AD 或 AD Connector 目录，则当您想重新开始使用 WorkSpaces 时，可以随时创建一个新的目录。

删除 WorkSpace

您可以删除除已暂停之外处于任何状态的 WorkSpace。

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择您的 WorkSpace 并选择删除。
4. 当系统提示进行确认时，选择删除。删除 WorkSpace 大约需要 5 分钟。删除期间，WorkSpace 的状态设置为正在终止。删除完成后，WorkSpace 将从控制台中消失。
5. (可选) 要删除您不再使用的任何自定义捆绑包和映像，请参阅 删除自定义 WorkSpaces 捆绑包或图片。
6. (可选) 删除一个目录下的所有 WorkSpace 后，可删除该目录。有关更多信息，请参阅删除 WorkSpaces 的目录。
7. (可选) 删除虚拟私有云(VPC) 中用于您的目录的所有资源后，可以删除 VPC 并释放用于 NAT 网关的弹性 IP 地址。有关更多信息，请参阅《Amazon VPC 用户指南》中的删除您的 VPC 和使用弹性 IP 地址。

使用 AWS CLI 删除 WorkSpace

使用 terminate-workspaces 命令。

WorkSpace 捆绑包和图片

WorkSpace 捆绑包是操作系统以及存储、计算和软件资源的组合。启动时 WorkSpace，您可以选择满足您需求的捆绑包。可用的默认捆绑包 WorkSpaces 称为公共捆绑包。有关可用的各种公共捆绑包的更多信息 WorkSpaces，请参阅 Amazon WorkSpaces 捆绑包。

如果你已经启动了 Windows 或 Linux WorkSpace 并对其进行了自定义，则可以从中创建自定义镜像 WorkSpace。

自定义映像仅包含的操作系统、软件和设置 WorkSpace。自定义捆绑包是该自定义映像和 WorkSpace 可以从中启动的硬件的组合。

创建自定义映像后，您可以构建一个将自定义映 WorkSpace 像与您选择的底层计算和存储配置相结合的自定义捆绑包。然后，您可以在启动新包时指定此自定义捆绑包， WorkSpaces 以确保新包 WorkSpaces 具有相同的一致配置（硬件和软件）。

如果您需要执行软件更新或在上安装其他软件 WorkSpaces，则可以更新您的自定义软件包并使用它来重建您的 WorkSpaces。

WorkSpaces 支持多种不同的操作系统 (OS)、流媒体协议和捆绑包。下表提供了有关每个操作系统支持的许可、流媒体协议和捆绑包的信息。

操作系统	许可证	流媒体协议	支持的捆绑包	生命周期保单/退休日期
Windows Server 2016	包含	WSP、pCo	价值、标准、性能、功率、显卡（已弃用）、 PowerPro、graphics.g4dn、.g4dn GraphicsPro、.g4dn GraphicsPro	2027年1月12日
Windows Server 2019	包含	WSP、pCo	价值、标准、性能、功率、显卡（已弃用）、 PowerPro、graphics.g4dn、.g4dn GraphicsPro、.g4dn GraphicsPro	2029年1月9日
Windows Server 2022	包含	WSP、pCo	标准、性能、功率、显卡（已弃用） PowerPro、、graphics.g4dn GraphicsPro、.g4dn GraphicsPro	2031年10月14日

操作系统	许可证	流媒体协议	支持的捆绑包	生命周期保单/退休日期
Windows 10	自带许可（BYOL）	WSP、pCo	价值、标准、性能、功率、显卡（已弃用）、 PowerPro、graphics.g4dn、.g4dn GraphicsPro、.g4dn GraphicsPro	在支援中
Windows 11	自带许可（BYOL）	WSP	标准、性能、功率、 PowerPro	在支援中
Amazon Linux 2	包含	WSP、pCo	价值、标准、性能、功率、PowerPro	2025年6月30日
Ubuntu 22.04 LTS	包含	WSP	价值、标准、性能、功率、Graphics.g4d PowerPro n、.g4dn GraphicsPro	2032年6月

Note

- 供应商不再支持的操作系统版本不能保证可以正常运行，也不受支持 AWS 支持。
- 要在 Windows 操作系统上 WorkSpaces 运行，Graphics 捆绑包仅支持 PCoIP 流媒体协议。

内容

捆绑包选项

在选择捆绑包之前，请确保要选择的捆绑包与 WorkSpaces 的协议、操作系统、网络和计算类型兼容。有关协议的更多信息，请参阅 Amazon WorkSpaces 的协议。有关网络的更多信息，请参阅 Amazon WorkSpaces 客户端网络要求。

Note

- 建议 PCoIP WorkSpaces 的最大网络延迟不要超过 250 毫秒。为了获得最佳 PCoIP WorkSpaces 用户体验，建议将网络延迟保持在 100 毫秒以下。当往返时间 (RTT) 超过 375 毫秒时，WorkSpaces 客户端连接将关闭。为了获得最佳 WorkSpaces Streaming Protocol (WSP) 用户体验，建议将 RTT 保持在 250 毫秒以下。如果 RTT 介于 250 毫秒到 400 毫秒之间，则用户可以访问 WorkSpace，但性能将显著降低。
- 建议您通过运行和使用复制用户日常任务的应用程序，在测试环境中测试您要选择的捆绑包的性能。

Important

- 2023 年 11 月 30 日之后，不再支持 Graphics 捆绑包。建议使用 Graphics 捆绑包切换到适用于 WorkSpaces 的 Graphics.g4dn 捆绑包。
- Graphics 和 GraphicsPro 捆绑包目前不在亚太地区（孟买）区域中提供。

以下是 WorkSpaces 提供的捆绑包。有关 WorkSpaces 捆绑包的信息，请参阅 Amazon WorkSpaces 捆绑包。

经济捆绑包

此捆绑包非常适合以下用途：

- 基本的文本编辑和数据输入
- 使用量较少的 Web 浏览
- 即时消息发送

不建议将此捆绑包用于文字处理、音频和视频会议、屏幕共享、软件开发工具、商业智能应用程序和图形应用程序。

标准捆绑包

此捆绑包非常适合以下用途：

- 基本的文本编辑和数据输入
- Web 浏览
- 即时消息发送
- 电子邮件

不建议将此捆绑包用于音频和视频会议、屏幕共享、文字处理、软件开发工具、商业智能应用程序和图形应用程序

性能捆绑包

此捆绑包非常适合以下用途：

- Web 浏览
- 文字处理
- 即时消息发送
- 电子邮件
- 电子表格
- 音频处理
- 课件

不建议将此捆绑包用于视频会议、屏幕共享、软件开发工具、商业智能应用程序和图形应用程序

节能捆绑包

此捆绑包非常适合以下用途：

- Web 浏览
- 文字处理

- 电子邮件
- 即时消息发送
- 电子表格
- 音频处理
- 软件开发（集成式开发环境 (IDE)）
- 中级数据处理入门
- 音频和视频会议

不建议将此捆绑包用于屏幕共享、软件开发工具、商业智能应用程序和图形应用程序。

PowerPro 捆绑包

此捆绑包非常适合以下用途：

- Web 浏览
- 文字处理
- 电子邮件
- 即时消息发送
- 电子表格
- 音频处理
- 软件开发（集成式开发环境 (IDE)）
- 数据仓库
- 商业智能应用程序
- 音频和视频会议

不建议将此捆绑包用于机器学习模型训练和图形应用程序

GraphicsPro 捆绑包

该捆绑包为您的 WorkSpaces 提供基本图形性能以及高水平 CPU 性能和内存。它非常适合以下用途：

- Web 浏览
- 文字处理

- 电子邮件
- 即时消息发送
- 电子表格
- 音频会议
- 软件开发（集成式开发环境 (IDE)）
- 数据仓库
- 商业智能应用程序
- 图形设计
- 图像处理

不建议将此捆绑包用于音频和视频会议、3D 渲染和照片级逼真设计

Graphics.g4dn 捆绑包

该捆绑包为您的 WorkSpaces 提供高水平图形性能以及中等水平 CPU 性能和内存，非常适合以下用途：

- Web 浏览
- 文字处理
- 电子邮件
- 电子表格
- 即时消息发送
- 音频会议
- 软件开发（集成式开发环境 (IDE)）
- 中级数据处理入门
- 数据仓库
- 商业智能应用程序
- 图形设计
- CAD/CAM（计算机辅助设计/计算机辅助制造）

不建议将此捆绑包用于音频和视频会议、3D 渲染、照片级逼真设计和机器学习模型训练

GraphicsPro.g4dn

GraphicsPro.g4dn 捆绑包

该捆绑包为您的 WorkSpaces 提供高水平图形性能、CPU 性能和内存，非常适合以下用途：

- Web 浏览
- 文字处理
- 电子邮件
- 电子表格
- 即时消息发送
- 音频会议
- 软件开发（集成式开发环境 (IDE)）
- 中级数据处理入门
- 数据仓库
- 商业智能应用程序
- 图形设计
- CAD/CAM（计算机辅助设计/计算机辅助制造）
- 视频转码
- 3D 渲染
- 照片级逼真设计
- 游戏流
- ML（机器学习）模型训练和 ML 推理

不建议将此捆绑包用于音频和视频会议。

创建自定义 WorkSpaces 镜像和捆绑包

如果你已经启动了 Windows 或 Linux WorkSpace 并对其进行了自定义，则可以从中创建自定义映像和自定义捆绑包。 WorkSpace

自定义映像仅包含的操作系统、软件和设置 WorkSpace。自定义捆绑包是该自定义映像和 WorkSpace 可以从中启动的硬件的组合。

> **Note**
>
> 请确保在删除捆绑包后至少等待 2 小时，然后再创建同名的新捆绑包。

创建自定义映像后，您可以构建一个自定义服务包，该服务包将自定义映像与您选择的基础计算和存储配置相结合。然后，您可以在启动新包时指定此自定义捆绑包， WorkSpaces 以确保新包 WorkSpaces 具有相同的一致配置（硬件和软件）。

通过为每个服务包选择不同的计算和存储选项，您可以使用相同的自定义映像来创建各种自定义服务包。

> **Important**
>
> - 如果你打算从 Windows 10 创建映像 WorkSpace，请注意，已从 Windows 10 的一个版本升级到较新版本的 Windows 10（Windows 功能/版本升级）的 Windows 10 系统不支持创建映像。但是， WorkSpaces 映像创建过程支持 Windows 累积更新或安全更新。
> - 2020 年 1 月 14 日之后，无法从公有 Windows 7 捆绑包创建映像。你可能需要考虑将你的 Windows 7 迁移 WorkSpaces 到 Windows 10。有关更多信息，请参阅 迁移 WorkSpace。
> - 2023 年 11 月 30 日之后，不再支持 Graphics 捆绑包。我们建议将你迁移 WorkSpaces 到 Graphics.g4dn 捆绑包。有关更多信息，请参阅 迁移 WorkSpace。
> - 亚太地区（孟买）地区目前不提供显卡和 GraphicsPro 捆绑包。
> - 自定义捆绑包存储量不能小于图像存储量。

自定义捆绑包的成本与这些捆绑包创建自的公用捆绑包的成本相同。有关定价的更多信息，请参阅 Amazon WorkSpaces 定价。

内容

- Windows WorkSpaces 自定义镜像中包含的内容
- Linux WorkSpace 自定义镜像中包含的内容

创建 Windows 自定义映像的要求

> **Note**
>
> Windows 目前将 1 GB 定义为 1,073,741,824 字节。客户需要确保 C 盘上有超过 12,884,901,888 字节（或 12 GiB）的可用空间，并且用户配置文件小于 10,737,418,240 字节（或 10 GiB）才能创建 a 的映像。 WorkSpace

- 的状态 WorkSpace 必须为 “可用”，其修改状态必须为 “无”。
- WorkSpaces 图像上的所有应用程序和用户配置文件都必须与 Microsoft Sysprep 兼容。
- 所有要包括在映像中的应用程序都必须安装在 C 驱动器上。
- 对于 Windows 7 WorkSpaces，其总大小（文件和数据）必须小于 10 GB。
- 对于 Windows 7 WorkSpaces，C驱动器必须有至少 12 GB 的可用空间。
- 在上运行的所有应用程序服务都 WorkSpace 必须使用本地系统帐户而不是域用户凭据。例如，不能有使用域用户凭证运行的 Microsoft SQL Server Express 安装。
- WorkSpace 不得加密。目前不支持通过加密 WorkSpace 设备创建映像。
- 映像中要求具有以下组件。如果没有这些组件 WorkSpaces ，您从映像中启动的将无法正常运行。有关更多信息，请参阅 the section called “必需配置”。
  - Windows PowerShell 版本 3.0 或更高版本
  - 远程桌面服务
  - AWS 光伏驱动器
  - Windows 远程管理 (WinRM)
  - Teradici PCoIP 代理和驱动程序
  - STXHD 代理和驱动程序
  - AWS 和 WorkSpaces 证书
  - Skylight 代理

创建 Linux 自定义映像的要求

- 的状态 WorkSpace 必须为 “可用”，其修改状态必须为 “无”。
- 所有将包括在映像中的应用程序都必须安装在用户卷（ /home 目录）之外。
- 根卷 (/) 的使用率必须低于 97%。
- WorkSpace 不得加密。目前不支持通过加密 WorkSpace 设备创建映像。
- 映像中要求具有以下组件。如果没有这些组件 WorkSpaces ，你从镜像中启动的将无法正常运行：
  - Cloud-init
  - Teradici PCoIP 或 WSP 代理和驱动程序
  - Skylight 代理

最佳实践

在从创建图像之前 WorkSpace，请执行以下操作：

- 使用未连接到您的生产环境的单独 VPC。
- 在私有子网 WorkSpace 中部署，并使用 NAT 实例处理出站流量。
- 使用小的 Simple AD 目录。
- 使用源的最小卷大小 WorkSpace，然后在创建自定义捆绑包时根据需要调整音量大小。
- 在上安装所有操作系统更新（Windows 功能/版本更新除外）和所有应用程序更新。 WorkSpace有关更多信息，请参阅本主题开始处的重要提示。
- 从中删除不应 WorkSpace 包含在捆绑包中的缓存数据（例如，浏览器历史记录、缓存文件和浏览器 Cookie）。
- 从中删除不应 WorkSpace 包含在捆绑包中的配置设置（例如，电子邮件配置文件）。
- 使用 DHCP 切换到动态 IP 地址设置。
- 确保您没有超过某个地区允许的 WorkSpace 图片配额。默认情况下，每个区域允许您使用 40 WorkSpace 张图片。如果您已达到此配额，创建映像的新尝试将失败。要申请增加配额，请使用WorkSpaces 限制表单。
- 确保您不是在尝试使用加密镜像创建镜像 WorkSpace。目前不支持通过加密 WorkSpace 设备创建映像。
- 如果您正在上运行任何防病毒软件 WorkSpace，请在尝试创建映像时将其禁用。
- 如果您启用了防火墙 WorkSpace，请确保防火墙没有阻塞任何必要的端口。有关更多信息，请参阅的 IP 地址和端口要求 WorkSpaces。

- 对于 Windows WorkSpaces，请勿在创建映像之前配置任何组策略对象 (GPO)。
- 对于 Windows WorkSpaces，在创建映像之前不要自定义默认用户配置文件 (`C:\Users\Default`)。建议通过 GPO 对用户配置文件进行任何自定义并在创建映像后应用它们。GPO 可以很容易地进行修改或回滚，所以与对默认用户配置文件进行的自定义设置相比更不易出错。
- 对于 Linux WorkSpaces，另请参阅 “为亚马逊 WorkSpaces 提供 Linux 映像做好准备的最佳实践” 白皮书。
- 如果您想在启用了 WorkSpaces 流媒体协议 (WSP) 的 Linux WorkSpaces 上使用智能卡，使用智能卡进行身份验证请参阅，了解在创建映像 WorkSpace 之前必须对 Linux 进行的自定义。
- 确保在上更新网络依赖驱动程序，例如 ENA、NVMe 和 PV 驱动程序。 WorkSpaces你应该至少每 6 个月这样做一次。有关更多信息，请参阅安装或升级适用于 Windows 实例的弹性网络适配器 (ENA) 驱动程序和在 Windows 实例上升半虚拟化驱动程序。AWS NVMe 驱动程序
- 确保定期将 ec2Config、ec2Launch 和 ec2Launch V2 代理更新到最新版本。你应该至少每 6 个月这样做一次。有关更多信息，请参阅更新 ec2Config 和 ec2Launch。

（可选）步骤 1：为映像指定自定义计算机名称格式

对于从您的自定义或自带许可证 (BYOL) 映像 WorkSpaces 启动的，您可以为计算机名称格式指定自定义前缀，而不是使用默认的计算机名称格式。要指定自定义前缀，请按照与您的映像类型相对应的步骤进行操作。

为自定义映像指定自定义计算机名称格式

> **Note**
>
> 默认情况下，Windows 10 的计算机名称格式为 `DESKTOP-XXXXX`，Windows 11 WorkSpaces 的计算机名称格式 WorkSpaces 为`WORKSPA-XXXXX`。

1. 在你 WorkSpace 用来创建自定义图像的上，`C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xml`在记事本或其他文本编辑器中打开。有关使用 `Unattend.xml` 文件的更多信息，请参阅 Microsoft 文档中的应答文件 (unattend.xml)。

   > **Note**
   >
   > 要通过您的 Windows 文件资源管理器访问 C: 驱动器 WorkSpace，请在地址栏**`C:\`**中输入。

2. 在 <settings pass="specialize"> 部分中，确保将 <ComputerName> 设置为星号 (*)。如果将 <ComputerName> 设置为任何其他值，则您的自定义计算机名称设置将被忽略。有关该<ComputerName>设置的更多信息，请参阅 Microsoft 文档 ComputerName中的。
3. 在 <settings pass="specialize"> 部分中，将 <RegisteredOrganization> 和 <RegisteredOwner> 设置为您的首选值。

   在 Sysprep 期间，您为 <RegisteredOwner> 和 <RegisteredOrganization> 指定的值将连接在一起，组合字符串的前 7 个字符用于创建计算机名称。例如，如果您为 for <RegisteredOrganization> 和 **EC2** for 指定 **Amazon.com**<RegisteredOwner>，则通过自定义分发包 WorkSpaces 创建的计算机名称将以 EC2AMAZ-*xxxxxxx* 开头。

   > **Note**
   >
   > Sysprep 会忽略 <settings pass="oobeSystem"> 部分中的 <RegisteredOrganization> 和 <RegisteredOwner> 值。

4. 保存对 Unattend.xml 文件的更改。

为 BYOL 映像指定自定义计算机名称格式

1. 如果您使用的是 Windows 10，请在记事本或其他文本编辑器中打开 C:\Program Files \Amazon\Ec2ConfigService\Sysprep2008.xml。如果您使用的是 Windows 11，请打开 C:\ProgramData\Amazon\EC2Launch\sysprep\OOBE_unattend.xml。
2. 在 <settings pass="specialize"> 部分中，取消注释 <ComputerName>*</ ComputerName>，并确保将 <ComputerName> 设置为星号 (*)。如果将 <ComputerName> 设置为任何其他值，则您的自定义计算机名称设置将被忽略。有关该<ComputerName>设置的更多信息，请参阅 Microsoft 文档 ComputerName中的。
3. 在 <settings pass="specialize"> 部分中，将 <RegisteredOrganization> 和 <RegisteredOwner> 设置为您的首选值。

   在 Sysprep 期间，您为 <RegisteredOwner> 和 <RegisteredOrganization> 指定的值将连接在一起，组合字符串的前 7 个字符用于创建计算机名称。例如，如果您为 for <RegisteredOrganization> 和 **EC2** for 指定 **Amazon.com**<RegisteredOwner>，则通过自定义分发包 WorkSpaces 创建的计算机名称将以 EC2AMAZ-*xxxxxxx* 开头。

> **Note**
>
> Sysprep 会忽略 `<settings pass="oobeSystem">` 部分中的 `<RegisteredOrganization>` 和 `<RegisteredOwner>` 值。

4. 如果您使用的是 Windows 10，请将您的更改保存到 `Sysprep2008.xml` 文件。如果您使用的是 Windows 11，请将您的更改保存到 `OOBE_unattend.xml`

步骤 2：运行映像检查程序

> **Note**
>
> 图像检查器仅适用于 Window WorkSpaces s。如果您要从 Linux 中创建映像 WorkSpace，请跳至步骤 3：创建自定义映像和自定义捆绑包。

要确认您的 Windows 是否 WorkSpace 满足创建映像的要求，我们建议您运行图像检查器。Image Checker 会对要 WorkSpace 用来创建图像的进行一系列测试，并就如何解决发现的任何问题提供指导。

> **Important**
>
> - WorkSpace 必须通过 Image Checker 运行的所有测试，然后才能使用它来创建图像。
> - 在运行映像检查器之前，请验证您的 WorkSpace设备上是否安装了最新的 Windows 安全和累积更新。

要获取映像检查程序，请执行以下操作之一：

- 重启你的 WorkSpace. 系统会在重新启动期间自动下载映像检查程序并将其安装在 `C:\Program Files\Amazon\ImageChecker.exe` 中。
- 从 https://tools.amazonworkspaces.com/ ImageChecker .zip https://tools.amazonworkspaces.awsapps.cn/ ImageChecker .zip 下载 Amaz `ImageChecker.exe`将此文件复制到 `C:\Program Files\Amazon\`。

运行映像检查程序

1. 打开 C:\Program Files\Amazon\ImageChecker.exe文件。
2. 在 “Amazon WorkSpaces 图像检查器” 对话框中，选择 “运行”。
3. 每个测试完成后，您都可以查看测试的状态。

   对于状态为 FAILED (失败) 的任何测试，请选择 Info (信息) 以显示有关如何解决导致失败的问题的信息。有关如何解决这些问题的更多信息，请参阅解决映像检查程序检测到的问题的提示。

   如果任何测试显示了状态 WARNING (警告)，请选择 Fix All Warnings (修复所有警告) 按钮。

   该工具在映像检查程序所在的同一目录中生成输出日志文件。默认情况下，此文件位于 C:\Program Files\Amazon\ImageChecker_*yyyyMMddhhmmss*.log 中。

   > **Tip**
   >
   > 请勿删除此日志文件。如果出现问题，此日志文件可能有助于进行故障排除。

4. 如果适用，请解决任何导致测试失败和警告的问题，然后重复运行图像检查器的过程，直到WorkSpace通过所有测试。在创建映像之前，必须先解决所有失败和警告。
5. WorkSpace 通过所有测试后，您会看到一条验证成功消息。您现在已准备好创建自定义服务包。

解决映像检查程序检测到的问题的提示

除了咨询以下提示以解决映像检查程序检测到的问题之外，请务必查看映像检查程序日志文件：C:\Program Files\Amazon\ImageChecker_*yyyyMMddhhmmss*.log。

PowerShell 必须安装 3.0 或更高版本

安装最新版本的微软 Windows PowerShell。

> **Important**
>
> 的 PowerShell 执行策略 WorkSpace 必须设置为允许RemoteSigned脚本。要检查执行策略，请运行 Get-ExecutionPolicy PowerShell 命令。如果执行策略未设置为 “不受限制” 或 RemoteSigned，请运行 Set-ExecutionPolicy — ExecutionPolicy RemoteSigned 命令来更改执行策略的值。该RemoteSigned设置允许在 Amazon 上执行脚本 WorkSpaces，这是创建图像所必需的。

只可存在 C 和 D 驱动器

用于映像的 a WorkSpace 上只能存在C和D驱动器。删除所有其他驱动器，包括虚拟驱动器。

无法检测到由于 Windows 更新而挂起的重启

- 在重启 Windows 以完成安装安全更新或累积更新之前，无法运行创建映像过程。重启 Windows 以应用这些更新，并确保不需要安装任何其他挂起的 Windows 安全更新或累积更新。
- 已从一个版本的 Windows 10 升级到更高版本（Windows 功能/版本升级）的 Windows 10 的 Windows 10 系统不支持映像创建。但是， WorkSpaces 映像创建过程支持 Windows 累积更新或安全更新。

Sysprep 文件必须存在且不能为空

如果 Sysprep 文件出现问题，请联系 AWS Support 中心，以修复您的 EC2Config 或 EC2Launch。

用户配置文件大小必须小于 10 GB

对于 Windows 7 WorkSpaces，用户配置文件 (`D:\Users\`*`username`*) 的总容量必须小于 10 GB。根据需要删除文件以减小用户配置文件的大小。

驱动器 C 必须有足够的可用空间

对于 Windows 7 WorkSpaces，驱动器上必须有至少 12 GB 的可用空间C。根据需要删除文件以释放 C 驱动器上的空间。对于 Windows 10 WorkSpaces，如果您收到一条FAILED消息并且磁盘空间超过2GB，请忽略。

无法在域账户下运行任何服务

要运行 “创建映像” 进程， WorkSpace 不能在域帐户下运行任何服务。所有服务必须在本地账户下运行。

在本地账户下运行服务

1. 打开 `C:\Program Files\Amazon\ImageChecker_`*`yyyyMMddhhmmss`*`.log` 并查找在域账户下运行的服务列表。
2. 在 Windows 搜索框中，输入 **`services.msc`** 以打开 Windows 服务管理器。
3. 在 Log On As (登录身份) 下，查找在域账户下运行的服务。（以本地系统、本地服务或网络服务身份运行的服务不会干扰映像创建。）
4. 选择在域账户下运行的服务，然后选择操作)、属性。

5. 打开 Log On (登录) 选项卡。在 Log on as (登录身份)下，选择 Local System account (本地系统账户)。
6. 选择 确定。

WorkSpace 必须配置为使用 DHCP

必须将上的所有网络适配器配置 WorkSpace 为使用 DHCP 而不是静态 IP 地址。

将所有网络适配器设置为使用 DHCP

1. 在 Windows 搜索框中，输入 **`control panel`** 以打开控制面板。
2. 选择网络和 Internet。
3. 选择网络和共享中心。
4. 选择更改适配器设置，然后选择适配器。
5. 选择更改此连接的设置。
6. 在网络选项卡上，选择互联网协议版本 4 (TCP/IPv4)，然后选择属性。
7. 在互联网协议版本 4 (TCP/IPv4) 属性对话框中，选择自动获取 IP 地址。
8. 选择 确定。
9. 对上的所有网络适配器重复此过程 WorkSpace。

必须启用远程桌面服务

创建映像过程需要启用远程桌面服务。

启用远程桌面服务

1. 在 Windows 搜索框中，输入 **`services.msc`** 以打开 Windows 服务管理器。
2. 在名称列中，找到远程桌面服务。
3. 选择远程桌面服务，然后选择操作、属性。
4. 在常规选项卡上，对于启动类型，选择手动或自动。
5. 选择 确定。

用户配置文件必须存在

你 WorkSpace 用来创建图像的必须有用户个人资料 (`D:\Users\`*`username`*)。如果此测试失败，请联系 AWS Support 中心寻求帮助。

必须正确配置环境变量路径

本地计算机的环境变量路径缺少 System32 和 Windows PowerShell 的条目。要创建映像，需要这些条目。

配置环境变量路径

1. 在 Windows 搜索框中，输入 **environment variables**，然后选择编辑系统环境变量。
2. 在系统属性对话框中，打开高级选项卡，然后选择环境变量。
3. 在环境变量对话框的系统变量下，选择路径条目，然后选择编辑。
4. 选择新建，然后添加以下路径：

   ```
   C:\Windows\System32
   ```
5. 再次选择新建，然后添加以下路径：

   ```
   C:\Windows\System32\WindowsPowerShell\v1.0\
   ```
6. 选择 确定。
7. 重新启动 WorkSpace。

> **Tip**
>
> 项目在环境变量路径中显示的顺序至关重要。要确定正确的顺序，您可能需要将您的环境变量路径 WorkSpace 与来自新创建 WorkSpace 或新 Windows 实例的环境变量路径进行比较。

必须启用 Windows 模块安装程序

创建映像过程要求启用 Windows 模块安装程序服务。

启用 Windows 模块安装程序服务

1. 在 Windows 搜索框中，输入 **services.msc** 以打开 Windows 服务管理器。
2. 在名称列中，找到 Windows 模块安装程序。
3. 选择 Windows 模块安装程序，然后选择操作、属性。
4. 在常规选项卡上，对于启动类型，选择手动或自动。
5. 选择 确定。

必须禁用 Amazon SSM 代理

创建映像过程要求禁用 Amazon SSM 代理服务。

禁用 Amazon SSM 代理服务

1. 在 Windows 搜索框中，输入 **`services.msc`** 以打开 Windows 服务管理器。
2. 在名称列中，找到 Amazon SSM 代理。
3. 选择 Amazon SSM 代理，然后选择操作、属性。
4. 在常规选项卡上，对于启动类型，选择已禁用。
5. 选择 确定。

必须启用 SSL3 和 TLS 1.2 版本

要为 Windows 配置 SSL/TLS，请参阅 Microsoft Windows 文档中的如何启用 TLS 1.2。

上只能存在一个用户配置文件 WorkSpace

上只能有一个用于创建图像 WorkSpace 的 WorkSpaces 用户个人资料 (`D:\Users\`*`username`*)。删除所有不属于目标用户的用户个人资料 WorkSpace。

要使图像创建起作用，上面 WorkSpace 只能有三个用户配置文件：

- WorkSpace(`D:\Users\`*`username`*) 的目标用户的用户个人资料
- 默认用户配置文件（也称为默认配置文件）
- 管理员用户配置文件

如果有其他用户配置文件，则可以通过 Windows 控制面板中的高级系统属性将其删除。

删除用户配置文件

1. 要访问高级系统属性，请执行以下操作之一：
   - 按 Windows 键 + 暂停中断，然后在控制面板 > 系统和安全 > 系统对话框的左侧窗格中，选择高级系统设置。
   - 在 Windows 搜索框中，输入 **`control panel`**。在“控制面板”中，选择系统和安全，然后选择“系统”，随后在控制面板 > 系统和安全 > 系统对话框的左侧窗格中，选择高级系统设置。
2. 在系统属性对话框的高级选项卡上，选择用户配置文件下的设置。

3. 如果除了管理员配置文件、默认配置文件和目标 WorkSpaces用户的配置文件之外还列出了任何配置文件，请选择该其他配置文件并选择删除。
4. 当询问您是否要删除此配置文件时，请选择是。
5. 如有必要，请重复步骤 3 和 4，删除不属于该的任何其他配置文件 WorkSpace。
6. 选择确定两次并关闭控制面板。
7. 重新启动 WorkSpace。

没有 AppX 程序包可以处于暂存状态

一个或多个 AppX 程序包处于暂存状态。这可能导致在映像创建过程中出现 Sysprep 错误。

删除所有暂存的 AppX 程序包

1. 在 Windows 搜索框中，输入 **powershell**。选择以管理员身份运行。
2. 当询问“你要允许此应用对你的设备进行更改吗?”时，选择是。
3. 在 Windows PowerShell 窗口中，输入以下命令以列出所有暂存的 AppX 软件包，然后在每个命令后按 Enter。

```
$workSpaceUserName = $env:username
```

```
$allAppxPackages = Get-AppxPackage -AllUsers
```

```
$packages = $allAppxPackages |    Where-Object { `
                                 (($_.PackageUserInformation -like "*S-1-5-18*" -
and !($_.PackageUserInformation -like "*$workSpaceUserName*")) -and `
                                 ($_.PackageUserInformation -like "*Staged*" -or
 $_.PackageUserInformation -like "*Installed*")) -or `
                                 ((!($_.PackageUserInformation -like "*S-1-5-18*") -
and $_.PackageUserInformation -like "*$workSpaceUserName*") -and `
                                 $_.PackageUserInformation -like "*Staged*")
                                 }
```

4. 输入以下命令以删除所有暂存的 AppX 程序包，然后按 Enter 键。

```
$packages | Remove-AppxPackage -ErrorAction SilentlyContinue
```

5. 再次运行映像检查程序。如果此测试仍然失败，请输入以下命令以删除所有 AppX 程序包，然后在每个程序包之后按 Enter 键。

```
Get-AppxProvisionedPackage -Online | Remove-AppxProvisionedPackage -Online -
ErrorAction SilentlyContinue
```

```
Get-AppxPackage -AllUsers | Remove-AppxPackage -ErrorAction SilentlyContinue
```

Windows 必须尚未从以前的版本升级

已从一个版本的 Windows 10 升级到更高版本（Windows 功能/版本升级）的 Windows 10 的 Windows 系统不支持映像创建。

要创建映像，请使用 WorkSpace 尚未升级 Windows 功能/版本的。

Windows 重置计数不得为 0

重置功能允许您延长 Windows 试用版的激活期。创建映像过程要求重置计数为 0 以外的值。

检查 Windows 重置计数

1. 在 Windows 开始菜单上，选择 Windows 系统，然后选择命令提示符。
2. 在命令提示符窗口中，键入以下命令，然后按 Enter。

   ```
   cscript C:\Windows\System32\slmgr.vbs /dlv
   ```

要将重置计数重置为非 0 的值，请参阅 Microsoft Windows 文档中的 Sysprep（通用化）Windows 安装。

其他故障排查提示

如果您 WorkSpace 通过了 Image Checker 运行的所有测试，但仍然无法从中创建图像 WorkSpace，请检查是否存在以下问题：

- 确保 WorkSpace 未将分配给域访客群组中的用户。要检查是否有任何域帐户，请运行以下 PowerShell命令。

  ```
  Get-WmiObject -Class Win32_Service | Where-Object { $_.StartName -like "*
  $env:USERDOMAIN*" }
  ```

- WorkSpaces 仅适用于 Windows 7：如果在创建映像期间复制用户配置文件时出现问题，请检查是否存在以下问题：

- 长的配置文件路径可能会导致映像创建错误。请确保用户配置文件中所有文件夹的路径少于 261 个字符。
- 确保将配置文件的文件夹的完全权限授予系统和所有应用程序包。
- 如果用户配置文件中的任何文件被进程锁定或在映像创建过程中正在使用，则复制配置文件时可能会失败。

- 当 EC2Config 服务或 EC2Launch 脚本在 Windows 实例配置期间请求 RDP 证书指纹时，某些组策略对象 (GPO) 会限制对 RDP 证书指纹的访问。在尝试创建映像之前，请将其移 WorkSpace 至继承受阻且未应用 GPO 的新组织单位 (OU)。
- 请确保 Windows 远程管理 (WinRM) 服务配置为自动启动。执行以下操作：
  1. 在 Windows 搜索框中，输入 **`services.msc`** 以打开 Windows 服务管理器。
  2. 在名称列中，找到 Windows 远程管理(WS-Management)。
  3. 选择 Windows 远程管理(WS-Management)，然后选择操作、属性。
  4. 在常规选项卡上，对于启动类型，选择自动。
  5. 选择 确定。

步骤 3：创建自定义映像和自定义捆绑包

验证 WorkSpace 图片后，您可以继续创建自定义图像和自定义捆绑包。

创建自定义映像和自定义服务包

1. 如果您仍处于连接状态 WorkSpace，请在 WorkSpaces 客户端应用程序中选择 Amazon WorkSpaces 并断开连接，从而断开连接。
2. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
3. 在导航窗格中，选择 WorkSpaces。
4. 选择打开 WorkSpace 其详细信息页面，然后选择创建图像。如果的状态为 “ WorkSpace 已停止”，则必须先启动它（选择 “操作”，“开始” WorkSpaces），然后才能选择 “操作”、“创建映像”。

   > **Note**
   >
   > 要以编程方式创建图像，请使用 CreateWorkspaceImage API 操作。有关更多信息，请参阅 Amazon WorkSpaces API 参考 CreateWorkspaceImage中的。

5. 屏幕上会显示一条消息，提示您在继续操作 WorkSpace之前重新启动（重新启动）。重新启动后，您的 Amazon WorkSpaces 软件会 WorkSpace 更新到最新版本。

关闭消息并 WorkSpace 按照中的步骤进行操作，重新启动您的重启 a WorkSpace。完成后，重复执行此过程中的Step 4，但这次在显示重启消息时，选择下一步。要创建映像，其状态 WorkSpace 必须为 “可用”，其修改状态必须为 “无”。

6. 输入映像名称和有助于您识别映像的描述，然后选择 创建映像。在创建映像时，的状态 WorkSpace 为已暂停且 WorkSpace 不可用。

> **Note**
>
> 输入图片描述时，请确保不要使用特殊字符 “-”，否则会出现错误。

7. 在导航窗格中，选择 Images。当状态 WorkSpace 更改为 “可用”（这最多可能需要 45 分钟）时，映像就完成了。
8. 选择映像，然后选择操作、创建捆绑包。

> **Note**
>
> 要以编程方式创建捆绑包，请使用 CreateWorkspaceBundle API 操作。有关更多信息，请参阅 Amazon WorkSpaces API 参考 CreateWorkspaceBundle中的。

9. 输入服务包的名称和描述，然后执行以下操作：

   - 对于 Bundle 硬件类型，请选择 WorkSpaces 从此自定义捆绑包启动时要使用的硬件。
   - 在存储设置中，选择根卷和用户卷大小的默认组合之一，或者选择自定义，然后为根卷大小和用户卷大小输入值（最多 2000 GB）。

     根卷（对于 Microsoft Windows，为 C 驱动器；对于 Linux，为 /）和用户卷（对于 Windows，为 D 驱动器；对于 Linux，为 /home）的默认可用大小组合如下所示：

     - 根：80 GB，用户：10 GB、50 GB 或 100 GB
     - 根：175 GB，用户：100 GB
     - 仅适用于 Graphics.g4dn、 GraphicsPro .g4dn、Graphics， GraphicsPro WorkSpaces 仅限：root：100 GB，用户：100 GB

     此外，您可以将根卷和用户卷分别扩展到最大 2000 GB。

> **Note**
>
> 为确保数据得以保留，启动后不能减小根卷或用户卷的大小 WorkSpace。相反，请务必在启动时指定这些卷的最小大小 WorkSpace。您可以启动 “超值”、“标准”、“性能”、“Power”，或者 PowerPro WorkSpace 根卷至少为 80 GB，用户卷至少为 10 GB。你可以启动 Graphics.g4dn、 GraphicsPro .g4dn、Graphics，或者 GraphicsPro WorkSpace 根卷至少为 100 GB，用户卷至少为 100 GB。

10. 选择创建捆绑包。
11. 要确认您的捆绑包是否已创建，请选择捆绑包，并检查该捆绑包已列出。

Windows WorkSpaces 自定义镜像中包含的内容

当你从 Windows 7、Windows 10 或 Windows 11 创建映像时 WorkSpace，C驱动器的全部内容都包含在内。

对于 Windows 10 或 11 WorkSpaces，中的用户配置文件`D:\Users\`*`username`*不包含在自定义映像中。

对于 Windows 7 WorkSpaces，中`D:\Users\`*`username`*包含用户配置文件的所有内容，但以下内容除外：

- 联系人
- Downloads
- 音乐
- 图片
- 已保存的游戏
- 视频
- 播客
- 虚拟机
- 虚拟机
- 跟踪
- appdata\local\temp
- appdata\roaming\apple computer\mobilesync\

- appdata\roaming\apple computer\logs\
- appdata\roaming\apple computer\itunes\iphone software updates\
- appdata\roaming\macromedia\flash player\macromedia.com\support\flashplayer\sys\
- appdata\roaming\macromedia\flash player\#sharedobjects\
- appdata\roaming\adobe\flash player\assetcache\
- appdata\roaming\microsoft\windows\recent\
- appdata\roaming\microsoft\office\recent\
- appdata\roaming\microsoft office\live meeting
- appdata\roaming\microsoft shared\livemeeting shared\
- appdata\roaming\mozilla\firefox\crash reports\
- appdata\roaming\mcafee\common framework\
- appdata\local\microsoft\feeds cache
- appdata\local\microsoft\windows\temporary互联网files\
- appdata\local\microsoft\windows\history\
- appdata\local\microsoft\internet explorer\domstore\
- appdata\local\microsoft\internet explorer\imagestore\
- appdata\locallow\microsoft\internet explorer\iconcache\
- appdata\locallow\microsoft\internet explorer\domstore\
- appdata\locallow\microsoft\internet explorer\imagestore\
- appdata\local\microsoft\internet explorer\recovery\
- appdata\local\mozilla\firefox\profiles\

Linux WorkSpace 自定义镜像中包含的内容

当您从 Amazon Linux 上创建映像时 WorkSpace，用户卷 (/home) 的全部内容都将被删除。删除内容中包括根卷 (/) 的内容，但以下适用文件夹和密钥除外：

- /tmp
- /var/spool/mail
- /var/tmp
- /var/lib/dhcp

- /var/lib/cloud
- /var/cache
- /var/backups
- /etc/sudoers.d
- /etc/udev/rules.d/70-persistent-net.rules
- /etc/network/interfaces.d/50-cloud-init.cfg
- /var/log/amazon/ssm
- /var/log/pcoip-agent
- /var/log/skylight
- /var/lock/.skylight.domain-join.lock
- /var/lib/skylight/domain-join-status
- /var/lib/skylight/configuration-data
- /var/lib/skylight/config-data.json
- /home
- /etc/default/grub.d/zz-hibernation.cfg
- /etc/netplan/zz-workspaces-domain.yaml
- /etc/netplan/yy-workspaces-base.yaml
- /var/lib/ /users AccountsService

在创建自定义映像期间将销毁以下密钥：

- /etc/ssh/ssh_host_*_key
- /etc/ssh/ssh_host_*_key.pub
- /var/lib/skylight/tls.*
- /var/lib/skylight/private.key
- /var/lib/skylight/public.key

更新自定义 WorkSpaces 捆绑包

您可以更新现有的自定义 WorkSpaces 捆绑包，方法是修改基于服务包的 WorkSpaces，从 WorkSpaces 创建映像，然后用新映像更新捆绑包。然后，您可以使用更新的捆绑包启动新的 WorkSpaces。

> **Important**
>
> 当您更新现有 WorkSpaces 所基于的捆绑包时，不会自动更新现有 WorkSpaces。要更新基于您已更新的捆绑包的现有 WorkSpaces，您必须重建 WorkSpaces 或删除并重新创建它们。

使用控制台更新捆绑包

1. 连接到基于该服务包的 WorkSpace 并进行所需的更改。例如，您可以应用最新的操作系统和应用程序修补程序并安装其他应用程序。

   或者，您可以创建一个新的 WorkSpace，它具有与用于创建该捆绑包的映像相同的基本软件包（Plus 或 Standard），然后进行更改。
2. 如果您仍连接到 WorkSpace，请通过在 WorkSpaces 客户端应用程序中选择 Amazon WorkSpaces 和断开连接，来断开连接。
3. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
4. 在导航窗格中，选择 WorkSpaces。
5. 选择 WorkSpace，然后选择 Actions、Create Image。如果 WorkSpace 的状态为 STOPPED，则必须先启动它（选择操作，启动 WorkSpaces），然后才能选择操作、创建映像。
6. 输入映像名称和描述，然后选择创建映像。在创建映像期间 WorkSpace 不可用。有关映像创建过程的详细信息，请参阅创建自定义 WorkSpaces 镜像和捆绑包。
7. 在导航窗格中，选择 Bundles。
8. 选择相应捆绑包以打开其详细信息页面，然后在源映像下选择编辑。
9. 在更新源映像页面上，选择所创建的映像并选择更新捆绑包。
10. 根据需要，更新任何基于该捆绑包的现有 WorkSpaces，方法是重建 WorkSpaces 或删除并重新创建它们。有关更多信息，请参阅重建一个 WorkSpace。

以编程方式更新捆绑包

要以编程方式更新捆绑包，请使用 UpdateWorkspaceBundle API 操作。有关此操作的更多信息，请参阅《Amazon WorkSpaces API 参考》中的 UpdateWorkspaceBundle。

复制自定义 WorkSpaces 映像

您可以在 AWS 区域内或跨此类区域复制自定义 WorkSpace 映像。复制映像将导致创建完全相同的映像（具有其自己的唯一标识符）。

只要另一个区域已启用自带许可 (BYOL)，您就可以将 BYOL 映像复制到目标区域。确保为所有相关账户和区域启用 BYOL。

> **Note**
>
> 在中国（宁夏）区域，您只能复制同一区域内的映像。
> 在 AWS GovCloud (US) Region中，要将映像复制到其他 AWS 区域或从此类区域复制映像，请联系 AWS Support。
> 在选择加入区域中，要将映像复制到其他区域，请联系 AWS Support。有关选择加入区域的更多信息，请参阅可用区域。

您也可以复制已由其他 AWS 账户与您共享的映像。有关共享映像的更多信息，请参阅共享或取消共享自定义 WorkSpaces 映像。

在区域内或跨区域复制映像不收取额外费用。但需遵循目标区域中的映像数量配额。有关 Amazon WorkSpaces 配额的更多信息，请参阅 亚马逊 WorkSpaces 配额。

用于复制映像的 IAM 权限

如果您使用 IAM 用户复制映像，则该用户必须具有 `workspaces:DescribeWorkspaceImages` 和 `workspaces:CopyWorkspaceImage` 权限。

以下示例策略允许用户将指定的映像复制到指定区域的指定账户中。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeWorkspaceImages",
        "workspaces:CopyWorkspaceImage"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:123456789012:workspaceimage/wsi-a1bcd2efg"
      ]
    }
  ]
}
```

Important

如果您正在创建 IAM 策略，用于为不拥有共享映像的账户复制此类映像，则无法在 ARN 中指定账户 ID。您必须改用账户 ID 的 *，如以下示例策略所示。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeWorkspaceImages",
        "workspaces:CopyWorkspaceImage"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:*:workspaceimage/wsi-a1bcd2efg"
      ]
    }
  ]
}
```

只有当账户拥有要复制的映像时，您才能在 ARN 中指定该账户 ID。

有关使用 IAM 的更多信息，请参阅 对 WorkSpaces 进行身份和访问管理。

批量复制映像

您可以使用控制台逐个复制映像。要批量复制映像，请在 AWS Command Line Interface (AWS CLI) 中使用 CopyWorkspaceImage API 操作或 copy-workspace-image 命令。有关更多信息，请参阅《Amazon WorkSpaces API 参考》中的 CopyWorkspaceImage 或《AWS CLI 命令参考》中的 copy-workspace-image。

Important

在复制共享映像之前，请务必确认该映像是从正确的 AWS 账户共享的。要确定映像是否已共享并查看拥有映像的 AWS 账户 ID，请在 AWS CLI 中使用 DescribeWorkSpaceImages 和 DescribeWorkspaceImagePermissions API 操作或 describe-workspace-images 和 describe-workspace-image-permissions 命令。

使用控制台复制映像

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Images。
3. 选择映像，然后选择操作、复制映像。
4. 对于选择目标，选择要复制映像的 AWS 区域。
5. 对于副本名称，输入复制映像的新名称，对于描述，输入复制映像的描述。
6. （可选）在标签下，为复制的映像输入标签。有关更多信息，请参阅标记 WorkSpaces 资源。
7. 选择复制映像。

共享或取消共享自定义 WorkSpaces 映像

您可以在同一 AWS 区域内的 AWS 账户间共享自定义 WorkSpaces 映像。共享映像后，收件人账户可以根据需要将映像复制到其他 AWS 区域。有关复制映像的更多信息，请参阅复制自定义 WorkSpaces 映像。

> **Note**
>
> 在中国（宁夏）区域，您只能复制同一区域内的映像。
> 在 AWS GovCloud (US) Region中，要将映像复制到其他 AWS 区域或从此类区域复制映像，请联系 AWS Support。

共享映像不会产生额外的费用。但需遵循 AWS 区域中的映像数量配额。在收件人复制共享映像之前，该映像不会计入收件人账户的配额。有关 Amazon WorkSpaces 配额的更多信息，请参阅 亚马逊 WorkSpaces 配额。

要删除共享映像，您必须首先取消共享映像，然后才能将其删除。

共享自带许可映像

您只能与启用 BYOL 的 AWS 账户共享自带许可 (BYOL) 映像。您想要与其共享 BYOL 映像的 AWS 账户也必须是您组织的一部分（在同一付款人账户下）。

> **Note**
>
> 目前，AWS GovCloud（美国西部）和 AWS GovCloud（美国东部）区域不支持跨 AWS 账户共享 BYOL 映像。要在 AWS GovCloud（美国西部）和 AWS GovCloud（美国东部）区域跨账户共享 BYOL 映像，请联系 AWS Support。

与您共享的映像

如果与您共享映像，则您可以复制此类映像。然后，您可以使用共享映像的副本创建用于启动新 WorkSpaces 的捆绑包。

> **Important**
>
> 在复制共享映像之前，请务必确认该映像是从正确的 AWS 账户共享的。要以编程方式确定映像是否已共享，请在 AWS 命令行界面 (CLI) 中使用 DescribeWorkSpaceImages 和 DescribeWorkspaceImagePermissions API 操作或 describe-workspace-images 和 describe-workspace-image-permissions 命令。

为与您共享的映像显示的创建日期是该映像最初的创建日期，而不是与您共享映像的日期。

如果映像已与您共享，则您无法与其他账户进一步共享该映像。

共享映像

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Images。
3. 选择映像以打开其详细信息页面。
4. 在映像详细信息页面的共享账户部分，选择添加账户。
5. 在添加账户页面的添加要与之共享的账户下，输入要与之共享映像的账户的账户 ID。

   > **Important**
   >
   > 在共享映像之前，请确认您正在共享到正确的 AWS 账户 ID。

6. 选择共享映像。

> **Note**
>
> 要使用共享映像，收件人账户必须先复制该映像。然后，收件人账户可以使用共享映像的副本创建用于启动新 WorkSpaces 的捆绑包。

停止共享映像

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Images。
3. 选择映像以打开其详细信息页面。
4. 在映像详细信息页面的共享账户部分，选择要停止共享的 AWS 账户，然后选择取消共享。
5. 当系统提示您确认取消共享映像时，选择取消共享。

> **Note**
>
> 如果要在取消共享映像后将其删除，则必须先取消与其共享的所有账户的共享。

如果您停止共享映像，则收件人账户将无法再复制映像。但是，收件人账户中已存在的共享映像的任何副本都将保留在该账户中，并且可以从这些副本启动新的 WorkSpaces。

以编程方式共享或取消共享映像

要以编程方式共享或取消共享映像，请使用 UpdateWorkspaceImagePermission API 操作或 update-workspace-image-permission AWS Command Line Interface (AWS CLI) 命令。要确定映像是否已共享，请使用 DescribeWorkspaceImagePermissions API 操作或 describe-workspace-image-permissions CLI 命令。

删除自定义 WorkSpaces 捆绑包或图片

您可以根据需要，删除未使用的自定义捆绑包或自定义映像。

删除捆绑包

要删除捆绑包，必须先删除所有基于 WorkSpaces 该捆绑包的捆绑包。

使用控制台删除捆绑包

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Bundles。
3. 选择捆绑包，然后选择删除。
4. 当系统提示进行确认时，选择 Delete（删除）。

以编程方式删除捆绑包

要以编程方式删除捆绑包，请使用 DeleteWorkspaceBundle API 操作。有关更多信息，请参阅 Amazon WorkSpaces API 参考 DeleteWorkspaceBundle中的。

> **Note**
>
> 请确保在删除捆绑包后至少等待 2 小时，然后再创建同名的新捆绑包。

删除映像

在删除自定义服务包后，可以删除用于创建或更新该服务包的映像。

要删除映像，您必须先删除与该映像关联的所有捆绑包，或者必须更新这些捆绑包以使用其他源映像。如果映像与其他账户共享，则还必须取消共享。此外，映像不能处于待处理或正在验证状态。

使用控制台删除映像

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Images。
3. 选择映像，然后选择删除。
4. 当系统提示进行确认时，选择 Delete（删除）。

以编程方式删除映像

要以编程方式删除映像，请使用 DeleteWorkspaceImage API 操作。有关更多信息，请参阅 Amazon WorkSpaces API 参考 DeleteWorkspaceImage中的。

自带 Windows 桌面许可证

如果你与微软签订的许可协议允许，你可以将你的 Windows 10 或 11 桌面带到自己的 WorkSpaces。为此，您必须启用自带许可 (BYOL) 并提供满足以下要求的 Windows 10 或 11 许可证。有关在上使用微软软件的更多信息 AWS，请参阅亚马逊 Web Services 和 Microsoft。

为了遵守 Microsoft 许可条款，请在 AWS 云端专为你设计的硬件 WorkSpaces上 AWS 运行 BYOL。通过提供您自己的许可证，您可以为用户提供一致的体验。有关更多信息，请参阅WorkSpaces 定价。

> **Important**
>
> 已从一个版本的 Windows 10 或 11 升级到较新版本的 Windows 10 或 11（Windows 功能/版本升级）的 Windows 10 或 11 系统不支持创建映像。但是， WorkSpaces 映像创建过程支持 Windows 累积更新或安全更新。

内容

要求

在开始之前，请验证以下几点：

- 您的 Microsoft 许可协议是否允许 Windows 在虚拟托管环境中运行。
- 如果您要使用不支持 GPU 的捆绑包（除了 Graphics.g4dn、.g4dn、Graphics 和 GraphicsPro之外的捆绑包 GraphicsPro），请确认每个区域至少要使用 100 个。 WorkSpaces 这 100 WorkSpaces 可以是 AlwaysOn 和的任意组合 AutoStop WorkSpaces。要在专用硬件 WorkSpaces 上运行，则要求 WorkSpaces 每个区域至少使用 100 个。为了符合 Microsoft 的许可要求，你必须在专用硬件 WorkSpaces 上运行。专用硬件在 AWS 侧面配置，因此您的 VPC 可以保持默认租期。

  如果您计划使用支持 GPU 的捆绑包（Graphics.g4dn、 GraphicsPro .g4dn、Graphics 和 GraphicsPro），请确认在专用硬件上每月在一个区域中至少运行 4 AlwaysOn 或 20 个 GPU 支持。AutoStop WorkSpaces

  > **Note**
  >
  > - 目前只能为 PCoIP 协议创建 Graphics GraphicsPro .g4dn、.g4dn、Graphics 和 GraphicsPro 捆绑包。
  > - 2023 年 11 月 30 日之后，不再支持 Graphics 捆绑包。我们建议将你迁移 WorkSpaces 到 Graphics.g4dn 捆绑包。有关更多信息，请参阅 迁移 WorkSpace。
  > - 亚太地区（孟买）地区目前不提供显卡和 GraphicsPro 捆绑包。
  > - Graphics.g4dn、 GraphicsPro .g4dn、Graphics 和 GraphicsPro 捆绑包目前不在非洲（开普敦）地区上市。
  > - 要 WorkSpaces 在非洲（开普敦）地区跑步，你需要 WorkSpaces 在非洲（开普敦）地区跑至少400分。
  > - 只能针对 WSP 协议创建 Windows 11 捆绑包。
  > - Graphics.g4dn 和 GraphicsPro .g4dn 捆绑包目前不适用于 Windows 11。
  > - Windows 11 不支持显卡和 GraphicsPro 捆绑包。
  > - 服务捆绑包不适用于 Windows 11。有关迁移现有超值包的更多信息， WorkSpaces 请参阅迁移 WorkSpace。
  > - 为了获得最佳的视频会议体验，我们建议使用 Power 或 PowerPro 套装
  > - Windows 11 需要统一可扩展固件接口 (UEFI) 启动模式才能运行。确保将可选`--boot-mode`参数指定为 UEFI，以便成功导入虚拟机。

- WorkSpaces 可以使用 /16 IP 地址范围内的管理接口。管理接口连接到用于交互式流媒体的安全 WorkSpaces 管理网络。这样可以 WorkSpaces 管理你的 WorkSpaces. 有关更多信息，请参阅 网络接口。您必须至少从以下 IP 地址范围之一保留 /16 子网掩码用于此目的：
  - 10.0.0.0/8

- 100.64.0.0/10
- 172.16.0.0/12
- 192.168.0.0/16
- 198.18.0.0/15

> **Note**
>
> - 在您采用该 WorkSpaces 服务时，可用的管理接口 IP 地址范围经常发生变化。要确定当前有哪些范围可用，请运行 list-available-management-cidr-ranges AWS Command Line Interface (AWS CLI) 命令。
> - 除了您选择的 /16 CIDR 块外，54.239.224.0/20 IP 地址范围还用于所有区域的管理接口流量。 AWS

- 确保你已打开微软 Windows 和微软 Office KMS 激活 BYOL WorkSpaces 所需的管理接口端口。有关更多信息，请参阅 管理接口端口。
- 您有一台运行受支持的 64 位版 Windows 的虚拟机 (VM)。有关受支持版本的列表，请参阅本主题中的下一节 支持 BYOL 的 Windows 版本。VM 还必须满足以下要求：
  - Windows 操作系统必须对密钥管理服务器激活。
  - Windows 操作系统必须将 English (United States) (英语 (美国)) 作为主要语言。
  - 无法在 VM 上安装 Windows 附带的软件之外的软件。您可以在稍后创建自定义映像时添加其他软件（如防病毒解决方案）。
  - 在创建映像之前，请勿自定义默认用户配置文件 (`C:\Users\Default`) 或进行其他自定义设置。所有自定义都应在映像创建后进行。建议通过组策略对象 (GPO) 对用户配置文件进行任何自定义，并在创建映像后应用它们。这是因为通过 GPO 进行的自定义设置可以很容易地进行修改或回滚，并且与对默认用户配置文件进行的自定义设置相比更不易出错。
  - 在共享镜像之前，您必须创建一个具有本地管理员访问权限的 WorkSpaces_BYOL 帐户。稍后可能需要此账户的密码，因此请记下它。
  - VM 必须位于最大大小为 70 GB 且可用空间至少为 10 GB 的单个卷上。如果您还计划为 BYOL 映像订阅 Microsoft Office，则虚拟机必须位于单个卷上，且其最大大小为 70 GB，可用空间至少为 20 GB。根卷所在的 DISK 不能超过 70 GB。
  - 您的虚拟机必须运行 Windows PowerShell 版本 4 或更高版本。
- 在步骤 3：在 Windows 虚拟机上运行 BYOL Checker PowerShell 脚本中运行 BYOL 检查程序脚本之前，请确保您已安装最新的 Microsoft Windows 补丁。

> **Note**
>
> - 对于 BYOL 来说 AutoStop WorkSpaces，大量的并发登录可能会显著延长可用 WorkSpaces 时间。如果您预计会有许多用户同时登录您的 BYOL AutoStop WorkSpaces ，请咨询您的客户经理以获取建议。
> - 导入过程不支持加密 AMI。确保您禁用用于创建具有 EBS 加密的 EC2 AMI 的实例。可以在配置最终 WorkSpaces 版本后启用加密。

支持 BYOL 的 Windows 版本

您的 VM 必须运行以下 Windows 版本之一：

- Windows 10 版本 21H2（2021 年 12 月更新）
- Windows 10 版本 22H2（2022 年 11 月更新）
- Windows 10 Enterprise LTSC 2019 (1809)
- Windows 10 Enterprise LTSC 2021 (21H2)
- Windows 11 Enterprise 23H2（2023 年 10 月发布）
- Windows 11 Enterprise 22H2（2022 年 10 月发布）

所有支持的操作系统版本都支持您使用的 AWS 区域中可用的所有计算类型 WorkSpaces。微软不再支持的 Windows 版本不能保证能正常运行，Support 也不支持这些版本。 AWS

> **Note**
>
> 目前，BYOL 不支持 Windows 10 N 和 Windows 11 N 版本。

将 Microsoft Office 添加到 BYOL 映像中

在 BYOL 图像摄取过程中，如果你使用的是 Windows 10，则可以选择通过订阅微软 Office Professional 2016（32 位）或 2019（64 位）。 AWS如果您使用的是 Windows 11，则您可以订阅 Microsoft Office Professional 2019（64 位）。如果你选择这两个选项中的任何一个，Microsoft Office 将预先安装在你的 BYOL 映像中，并包含在你从 WorkSpaces 该映像启动的任何映像中。

如果您选择通过订阅 Office AWS，则需要支付额外费用。有关更多信息，请参阅WorkSpaces 定价。

Important

- 如果用于创建 BYOL 映像的虚拟机上已经安装了 Microsoft Office，那么如果要通过 AWS订阅 Office，则必须将其从虚拟机中卸载。
- 如果您计划通过订阅 Office AWS，请确保您的虚拟机至少有 20 GB 的可用磁盘空间。
- 在映像导入期间，您可以订阅 Office 2016 或 2019，但不能订阅 Office 2021。对于 Office 2021 和其他应用程序，例如 Microsoft Visio 2021 和 Microsoft Project 2021，请参阅管理应用程序。
- 要在亚马逊上同时使用基于浏览器的应用程序和桌面应用程序的 Microsoft 365 许可证 WorkSpaces，请在 BYOL 图像摄取过程完成后，在 BYOL 映像上安装 Microsoft 365 应用程序。

Note

Graphics.g4dn 和 GraphicsPro .g4dn BYOL 图片仅支持 Office 2019，不支持 Office 2016。

如果您选择订阅 Office，则 BYOL 映像摄取过程至少需要 3 个小时。

有关在 BYOL 摄取过程中订阅 Office 的详细信息，请参阅步骤 6：使用控制台创建 BYOL 映像 WorkSpaces 。

Office 语言设置

我们会根据你执行 BYOL 图像摄取所在的 AWS 地区来选择 Office 订阅所使用的语言。例如，如果您在亚太地区（东京）区域执行 BYOL 映像摄取，则您的 Office 订阅将使用日语作为其语言。

默认情况下，我们会在您的计算机上安装许多常用的 Office 语言包 WorkSpaces。如果未安装您想要的语言包，则您可以从 Microsoft 下载其他语言包。有关更多信息，请参阅 Microsoft 文档中的 Office 语言配件包。

要更改 Office 的语言，可以从以下几个选项中选择：

选项 1：允许个人用户自定义 Office 语言设置

个人用户可以调整自己的 Office 语言设置 WorkSpaces。有关更多信息，请参阅 Microsoft 文档中的在 Office 中添加一种编辑/共同创作语言或设置语言首选项。

选项 2：使用 GPO 管理模板 (.admx/.adml) 为所有用户强制执行默认 Office 语言设置 WorkSpaces

您可以使用组策略对象 (GPO) 设置为您的 WorkSpaces 用户强制执行默认 Office 语言设置。

> **Note**
>
> 您的 WorkSpaces 用户将无法覆盖通过 GPO 强制执行的语言设置。

有关使用 GPO 为 Office 设置语言的更多信息，请参阅 Microsoft 文档中的自定义 Office 的语言安装和设置。Office 2016 和 Office 2019 使用相同的 GPO 设置（标有 Office 2016）。

要使用 GPO，您必须安装 Active Directory 管理工具。有关使用 Active Directory 管理工具处理 GPO 的信息，请参阅为 WorkSpaces 设置 Active Directory 管理工具。

在配置 Office 2016 或 Office 2019 策略设置之前，您必须从 Microsoft 下载中心下载 Office 的管理模板文件 (.admx/.adml)。下载管理模板文件后，必须将`office16.admx`和`office16.adml`文件添加到 WorkSpaces 目录的域控制器的中央存储区。（`office16.admx` 和 `office16.adml` 文件同时适用于 Office 2016 和 Office 2019。）有关使用 `.admx` 和 `.adml` 文件的更多信息，请参阅 Microsoft 文档中的如何在 Windows 中创建和管理组策略管理模板的中央存储。

以下过程介绍了如何创建中央存储并向其中添加管理模板文件。在目录管理 WorkSpace 或加入目录的 Amazon EC2 实例上执行以下步骤。 WorkSpaces

为 Office 安装组策略管理模板文件

1. 从 Microsoft 下载中心下载 Office 的管理模板文件 (.admx/.adml)。
2. 在目录管理 WorkSpace 或已加入 WorkSpaces 目录的 Amazon EC2 实例上，打开 Windows 文件资源管理器，然后在地址栏中输入贵组织的完全限定域名 (FQDN)，例如`\\example.com`。
3. 打开 `SYSVOL` 文件夹。
4. 打开带有 *`FQDN`* 名称的文件夹。
5. 打开 `Policies` 文件夹。您现在应该位于 `\\`*`FQDN`*`\SYSVOL\`*`FQDN`*`\Policies` 中。
6. 如果该文件尚不存在，请创建一个名为 `PolicyDefinitions` 的文件夹。
7. 打开 `PolicyDefinitions` 文件夹。
8. 将 `office16.admx` 文件复制到 `\\`*`FQDN`*`\SYSVOL\`*`FQDN`*`\Policies\PolicyDefinitions` 文件夹中。
9. 在 `PolicyDefinitions` 文件夹中创建名为 `en-US` 的文件夹。
10. 打开 `en-US` 文件夹。

11. 将 `office16.adml` 文件复制到 `\\FQDN\SYSVOL\FQDN\Policies\PolicyDefinitions\en-US` 文件夹中。

配置 Office 的 GPO 语言设置

1. 在您的目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)。
2. 展开林（林：***FQDN***）。
3. 展开域。
4. 展开您的 FQDN（例如，`example.com`）。
5. 选择您的 FQDN，打开上下文（右键单击）菜单或打开操作菜单，然后选择在此域中创建 GPO，并将其链接到此处。
6. 为您的 GPO 命名（例如，**`Office`**）。
7. 选择您的 GPO，打开上下文（右键单击）菜单或打开操作菜单，然后选择编辑。
8. 在组策略管理编辑器中，选择用户配置、策略、从本地计算机检索到的管理模板策略定义（ADMX 文件）、Microsoft Office 2016 和语言首选项。

   > **Note**
   >
   > Office 2016 和 Office 2019 使用相同的 GPO 设置（标有 Office 2016）。如果您在用户配置、策略下看不到从本地计算机检索到的管理模板策略定义（ADMX 文件），则表明 `office16.admx` 和 `office16.adml` 文件未正确安装在您的域控制器上。

9. 在语言首选项下，为以下设置指定所需的语言。请务必将每项设置设置为启用，然后在选项下选择所需的语言。选择确定，保存每项设置。

   - 显示语言 > 显示帮助
   - 显示语言 > 显示菜单和对话框
   - 编辑语言 > 主要编辑语言

10. 完成后关闭组策略管理工具。
11. 组策略设置更改将在下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：

    - 重启 WorkSpace （在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。

- 从管理命令提示符下，输入 gpupdate /force。

选项 3：更新你的 Office 语言注册表设置 WorkSpaces

要通过注册表设置 Office 语言设置，请更新以下注册表设置：

- HKEY_CURRENT_USER\ SOFTWARE\ 微软\ Office\ 16.0\ Common\ uiLanguage LanguageResources
- HKEY_CURRENT_USER\ SOFTWARE\ 微软\ Office\ 16.0\ Common\ LanguageResources HelpLanguage

对于这些设置，请添加带有相应的 Office 区域设置 ID (LCID) 的 DWORD 键值。例如，英语（美国）的 LCID 为 1033。由于 LCID 是十进制值，因此，您必须将 DWORD 值的基本选项设置为十进制。有关 Office LCID 的列表，请参阅微软文档中的 Office 2016 中的语言标识符和 OptionState ID 值。

您可以 WorkSpaces 通过 GPO 设置或登录脚本将这些注册表设置应用于您的。

有关使用 Office 语言设置的更多信息，请参阅 Microsoft 文档中的自定义 Office 的语言安装和设置。

将 Office 添加到你现有的 BYOL WorkSpaces

您还可以通过执行以下操作将对 Office 的订阅添加到现有 BYOL WorkSpaces 中。

- 管理应用程序（推荐）-你可以在现有 WorkSpaces应用程序上安装和配置微软 Office、Microsoft Visio 或 Microsoft Project 2021。有关更多信息，请参阅管理应用程序。
- 迁移 WorkSpace-安装了 Office 的 BYOL 捆绑包后，您可以使用 WorkSpaces 迁移功能将现有 BYOL WorkSpaces 迁移到已订阅 Office 的 BYOL 捆绑包。有关更多信息，请参阅 迁移 WorkSpace。

> **Note**
>
> 管理应用程序选项可用于向你 WorkSpaces安装微软 Office 2021 和其他应用程序，例如微软 Visio 2021 和微软 Project 2021。要在你上安装微软 Office 2016 或 2019 WorkSpaces，请使用迁移 WorkSpace。

在 Microsoft Office 版本之间迁移

要从一个 Microsoft Office 版本迁移到另一个版本，您可通过以下选项实现：

- 管理应用程序（推荐）— 你可以卸载原始 Office 版本，在现有 WorkSpaces版本上安装 Office 2021 和其他应用程序，例如微软 Visio 2021 和微软 Project 2021。例如，要从 Microsoft Office 2019 迁移到 Microsoft Office 2021，请使用管理应用程序工作流，卸载 Microsoft Office 2019 并安装 Microsoft Office 2021。有关更多信息，请参阅管理应用程序。
- 迁移 WorkSpace — 要从微软 Office 2016 迁移到微软 Office 2019 或从微软 Office 2019 迁移到微软 Office 2016，你必须创建一个订阅了你要迁移到的 Office 版本的 BYOL 包。然后，使用 WorkSpaces 迁移功能将订阅 Office 的现有 BYOL WorkSpaces 迁移到已订阅要迁移到的 Office 版本的 BYOL 捆绑包。例如，要从微软 Office 2016 迁移到微软 Office 2019，请创建订阅微软 Office 2019 的 BYOL 捆绑包。然后使用 WorkSpaces 迁移功能将订阅 Office 2016 的现有 BYOL WorkSpaces 迁移到订阅 Office 2019 的 BYOL 捆绑包。有关更多信息，请参阅迁移 WorkSpace。

你可以使用这些选项将订阅微软 O WorkSpaces ffice 的应用程序迁移 AWS 到微软 365 应用程序。但是，管理应用程序仅限于从你 WorkSpace卸载 Microsoft Office。你必须自带工具和安装程序才能在自己上安装 Microsoft 365 应用程序。 WorkSpaces

> **Note**
>
> 使用管理应用程序，你可以安装或卸载微软 Office、Microsoft Visio 或 MicrosoftProject 2021。 WorkSpaces对于微软 Office 2016 或 2019 版本，你只能将其从你的版本中删除 WorkSpaces。要在你的电脑上安装微软 Office 2016 或 2019 WorkSpaces，请迁移 a WorkSpace。

有关迁移过程的更多信息，请参阅迁移 WorkSpace。

取消订阅 Office

要取消订阅 Office，您可通过以下选项实现。

- 管理应用程序（推荐）-你可以从中卸载 Microsoft Office 和其他应用程序，例如微软 Visio 和 Microsoft Project。 WorkSpaces有关更多信息，请参阅管理应用程序。
- 迁移 WorkSpace-您可以创建未订阅 Office 的 BYOL 捆绑包。然后使用 WorkSpaces 迁移功能将现有的 BYOL 迁移 WorkSpaces 到未订阅 Office 的 BYOL 捆绑包。有关更多信息，请参阅 迁移 WorkSpace。

Office 更新

如果你通过订阅了 Office AWS，Office 更新将作为常规 Windows 更新的一部分包括在内。为了及时了解所有安全补丁和更新，建议您定期更新 BYOL 基础映像。

第 1 步：使用亚马逊 WorkSpaces 控制台检查您的账户是否有资格获得 BYOL

在为账户启用 BYOL 之前，您必须通过验证流程，才能确认您是否有资格获得 BYOL。在您完成此过程之前，“启用 BYOL” 选项将无法在您的 Amazon WorkSpaces 控制台中使用。

> **Note**
>
> 验证过程至少需要一个工作日。如果要将现有 AWS 账户的 CIDR 范围和 BYOL 配置应用于其他账户，则可以将它们关联在一起以使用相同的底层硬件。要关联您的 AWS 账户，您无需提交支持请求。您可以使用 API（例如 CreateAccountLinkInvitations和）AcceptAccountLinkInvitation来关联您的 AWS 账户。有关更多信息，请参阅 关联 BYOL 账户。

使用亚马逊 WorkSpaces 控制台查看您的账户是否有资格获得 BYOL

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 “账户设置”，然后在 “自带许可证 (BYOL)” 下，选择 “查看 WorkSpaces BYOL 设置”。如果您的账户当前不符合 BYOL 的条件，将有一条消息提供后续步骤的指导。要开始使用，请联系您的 AWS 客户经理或销售代表，或者联系AWS Support 中心。您的联系人将验证您是否有资格获得 BYOL。

   要确定您是否有资格获得 BYOL，您的联系人需要您提供某些信息。例如，可能会要求您回答以下问题。

   - 您是否已查看并接受前面列出的 BYOL 要求？
   - 在哪些 AWS 区域，您需要为账户启用 BYOL？
   - 您计划在每个 AWS 区域部署多少 BYOL WorkSpaces ？
   - 您的过渡计划是什么？
   - 您是 WorkSpaces 从经销商那里购买吗？
   - BYOL 需要什么捆绑包类型？

- 您的组织是否在同一地区启用了 BYOL 的任何其他 AWS 账户？ 如果是，您是否要关联这些账户，以便它们使用相同的底层硬件？

  如果账户已关联，则会将这些账户中 WorkSpaces 部署的总数汇总在一起，以确定您是否有资格获得 BYOL。如果这两个问题的答案均为是，则可以将您的账户关联在一起。您可以使用 API（例如 CreateAccountLinkInvitations和）AcceptAccountLinkInvitation来关联您的 AWS 账户。如果您想关联其他启用 BYOL 的账户，但想要使用不同的 BYOL 设置（CIDR 范围和图像），请与 Supp AWS ort 联系，为新账户启用 BYOL。

3. 确认您的 BYOL 资格后，您可以继续执行下一步，即在亚马逊 WorkSpaces 控制台中为您的账户启用 BYOL。

第 2 步：使用亚马逊控制台为您的账户启用 BYOL 的 BYOL WorkSpaces

要为您的账户启用 BYOL，必须指定一个管理网络接口。此接口已连接到安全的 Amazon WorkSpaces 管理网络。它用于将 WorkSpace 桌面交互式传输到亚马逊 WorkSpaces 客户，并 WorkSpaces允许亚马逊管理 WorkSpace。

> **Note**
>
> 此过程中为账户启用 BYOL 的步骤只需在每个区域执行一次。

使用亚马逊 WorkSpaces 控制台为您的账户启用 BYOL

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 “账户设置”，然后在 “自带许可证 (BYOL)” 下，选择 “查看 WorkSpaces BYOL 设置”。
3. 在账户设置页面的自带许可 (BYOL) 下，选择启用 BYOL。

   如果您没有看到启用 BYOL 选项，则表示您的账户目前没有资格获得 BYOL。有关更多信息，请参阅 第 1 步：使用亚马逊 WorkSpaces 控制台检查您的账户是否有资格获得 BYOL。
4. 在 Bring Your Own License (BYOL) (自带许可 (BYOL)) 下的 Management network interface IP address range (管理网络接口 IP 地址范围) 区域中，选择 IP 地址范围，然后选择 Display available CIDR blocks (显示可用的 CIDR 块)。

   Amazon 在您指定的范围内 WorkSpaces 搜索并显示可用的 IP 地址范围，即 IPv4 无类域间路由 (CIDR) 块。如果您需要特定 IP 地址范围，可以编辑搜索范围。

> **Important**
>
> 指定 IP 地址范围后，您不能对其进行修改。请务必指定与您内部网络使用的范围不冲突的 IP 地址范围。如果您对指定哪个范围有任何疑问，请联系您的 AWS 客户经理或销售代表，或者在继续操作之前联系AWS Support 中心。

5. 从结果列表中选择所需的 CIDR 块，然后选择 Enable BYOL (启用 BYOL)。

   此过程可能耗时数小时。在为您的账户启 WorkSpaces 用 BYOL 时，请继续执行下一步。

步骤 3：在 Windows 虚拟机上运行 BYOL Checker PowerShell 脚本

为您的账户启用 BYOL 后，您必须确认您的 VM 满足 BYOL 的要求。为此，请执行以下步骤下载并运行 WorkSpaces BYOL Checker PowerShell 脚本。该脚本将对您计划用于创建映像的 VM 执行一系列测试。

> **Important**
>
> VM 必须先通过所有测试，然后您才能将其用于 BYOL。

下载 BYOL 检查程序脚本

在下载并运行 BYOL 检查程序脚本之前，请验证是否在 VM 上安装了最新的 Windows 安全更新。此脚本在运行时会禁用 Windows 更新服务。

1. 从 https://tools.amazonworkspaces.com/BYOLChecker.zip 将 BYOL Checker 脚本.zip 文件下载到你的文件夹。`Downloads`
2. 在 `Downloads` 文件夹中，创建一个 `BYOL` 文件夹。
3. 从 `BYOLChecker.zip` 中提取文件并将其复制到 `Downloads\BYOL` 文件夹。
4. 删除 `Downloads\BYOLChecker.zip` 文件夹，以便仅保留提取的文件。

执行以下步骤以运行 BYOL 检查程序脚本。

运行 BYOL 检查程序脚本

1. 在 Windows 桌面上，打开 Windows PowerShell。选择 Windows 开始按钮，右键单击 Windows PowerShell，然后选择以管理员身份运行。如果用户帐户控制提示您选择是否 PowerShell 要对设备进行更改，请选择 “是”。
2. 在 PowerShell 命令提示符处，切换到 BYOL Checker 脚本所在的目录。例如，如果脚本位于 Downloads\BYOL 目录中，请输入以下命令并按 Enter：

   ```
   cd C:\Users\username\Downloads\BYOL
   ```

3. 输入以下命令以更新计算机上的 PowerShell 执行策略。这样做将允许 BYOL 检查程序脚本运行：

   ```
   Set-ExecutionPolicy AllSigned
   ```

4. 当系统提示您确认是否更改 PowerShell 执行策略时，请输入A以指定 Yes to All。
5. 输入以下命令以运行 BYOL 检查程序脚本：

   ```
   .\BYOLChecker.ps1
   ```

6. 如果有安全通知出现，请按 R 键以运行一次。
7. 在 “WorkSpaces 图像验证” 对话框中，选择 “开始测试”。
8. 每个测试完成后，您都可以查看测试的状态。对于状态为 FAILED (失败) 的任何测试，请选择 Info (信息) 以显示有关如何解决导致失败的问题的信息。如果任何测试显示了状态 WARNING (警告)，请选择 Fix All Warnings (修复所有警告) 按钮。
9. 适当时，请解决导致测试故障和警告的任何问题，然后重复 Step 7 和 Step 8，直到 VM 通过所有测试。您在导出 VM 之前必须解决所有故障和警告。
10. BYOL 脚本检查程序将生成两个日志文件：`BYOLPrevalidationlog`*`YYYY-MM-DD_HHmmss`*`.txt` 和 `ImageInfo.text`。这两个文件位于 BYOL 检查程序脚本文件所在的目录中。

    > **Tip**
    >
    > 请勿删除这些文件。出现问题时，它们可能有助于解决问题。

11. 如果您的 VM 通过了所有测试，您将收到 Validation Successful (验证成功) 消息。检查该工具中显示的 VM 区域设置。要更新区域设置，请遵循 Microsoft 文档中的这些说明，然后再次运行 BYOL 检查程序脚本。
12. 关闭 VM 并创建它的快照。

13. 再次启动虚拟机。选择运行 Sysprep。如果 Sysprep 成功，则您在 Step 12 之后导出的 VM 可以导入到 Amazon Elastic Compute Cloud (Amazon EC2) 中。否则，请查看 Sysprep 日志，回滚到 Step 12 中拍摄的快照，解决报告的问题，拍摄新的快照，然后再次运行 BYOL 检查程序脚本。

    Sysprep 失败的最常见原因是未针对所有用户卸载现代 AppX 程序包。使用 Remove-AppxPackage PowerShell cmdlet 移除 AppX 软件包。
14. 成功创建镜像后，您可以删除 WorkSpaces_BYOL 账户。

错误消息和错误修复列表

BYOL 导入需要 Powershell 4.0 或更高版本。不支持已安装 PowerShell 的版本。

PowerShell 必须安装 4.0 或更高版本。欲了解更多信息，请参阅微软 Windows PowerShell。

BYOL 导入不支持安装了处于活动状态的 Microsoft Office 的系统。

导入前必须卸载 Microsoft Office。有关更多信息，请参阅从 PC 上卸载 Office。

BYOL 导入要求系统没有 PCoIP 代理。

卸载 PCoIP 代理。有关卸载 PCoIP 代理的信息，请参阅卸载适用于 Mac 的 Teradici PCoIP 软件客户端

BYOL 导入需要禁用 Windows 更新。

按照以下步骤禁用 Windows 更新：

1. 按 Windows 键 + R。 键入 `services.msc`，然后按 Enter。
2. 右键单击 Windows 更新，然后选择属性。
3. 在常规选项卡下，将启动类型设置为禁用。
4. 选择停止。
5. 单击应用，然后选择确定。
6. 重新启动您的计算机。

BYOL 导入需要启用自动挂载。

您必须启用自动挂载。以管理员身份在 PowerShell 中运行以下命令：

```
C:\> diskpart
DISKPART> automount enable
```

已启用自动挂载新卷。

BYOL 导入需要启用 WorkSpaces _BYOL 帐户

WorkSpaces必须启用 _BYOL 帐户。有关更多信息，请参阅使用亚马逊 WorkSpaces 控制台为您的账户启用 BYOL 的 BYOL。

BYOL 导入要求网络接口使用 DHCP 自动分配 IP 地址。网络接口当前使用静态 IP 地址。

必须更改网络接口才能使用 DHCP。有关更多信息，请参阅更改 TCP/IP 设置。

BYOL 导入需要本地磁盘上超过 20 GB 的空间。

本地磁盘必须有足够的空间，并且需要您腾出 20 GB 或更多空间。

BYOL 导入要求系统具有 1 个本地驱动器。还有其他本地驱动器、可移动驱动器或网络驱动器。

用于导入图像的 a WorkSpace 上只能有 C 和 D 驱动器。删除所有其他驱动器，包括虚拟驱动器。

BYOL 导入需要 Windows 10 或 Windows 11。

使用 Windows 10 或 Windows 11 操作系统。

BYOL 导入需要未加入 AD 域的系统。

必须取消系统与 AD 域的连接。有关更多信息，请参阅 Azure Active Directory 设备管理常见问题。

BYOL 导入需要未加入 Azure 域的系统。

必须取消系统与 Azure 域的连接。有关更多信息，请参阅 Azure Active Directory 设备管理常见问题。

BYOL 导入需要禁用 Windows 公共防火墙。

必须禁用公共防火墙配置文件。有关更多信息，请参阅打开或关闭 Microsoft Defender 防火墙。

BYOL 导入要求系统没有 VMware 工具。

必须卸载 VMware 工具。有关更多信息，请参阅在 VMware Fusion 中卸载和手动安装 VMware 工具 (1014522)。

BYOL 导入要求本地磁盘容量小于 80 GB。

磁盘必须小于 80 GB。减小磁盘大小。

BYOL 导入需要本地驱动器上的分区少于 2 个。此外，所有 Windows 10 分区都必须采用 MBR 分区，所有 Windows 11 分区都必须采用 GPT 分区。

对于 Windows 10，卷必须采用 MBR 分区，对于 Windows 11，卷必须采用 GPT 分区。有关更多信息，请参阅管理磁盘。

BYOL 导入需要完成所有需要重启的待处理更新。

安装所有更新并重启操作系统。

BYOL 导入要求将其禁 AutoLogon 用。

要禁用 AutoLogon 注册表，请执行以下操作：

1. 按 Windows 键 + R，然后在命令提示符处键入 `Regedit.exe`。
2. 向下滚动到 `HKEY_LOCAL_Machine\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon`
3. 为 `DontDisplayLastUserName` 添加一个值。
4. 对于类型，输入 `REG_SZ`。
5. 对于值，请输入 `0`。

> **Note**
>
> - 值 `DontDisplayLastUserName` 决定登录对话框是否显示上次登录 PC 的用户的用户名。
> - 默认情况下，该值不存在。如果存在，则必须将其设置为，`0`否则的值`DefaultUser`将被擦除并 AutoLogon 失败。

BYOL 导入需要启用 **`RealTimeIsUniversal`**。

RealTimeUniversal 必须启用注册表项。有关更多信息，请参阅为 Windows Server 2008 和更高版本配置时间设置。

BYOL 导入要求系统具有一个可启动分区。

可启动分区的数量不得超过一个。

移除其他分区

1. 按 Windows 徽标 + R 键，打开运行框。输入 `msconfig`，并按键盘上的 Enter 键，打开“系统配置”窗口。
2. 从窗口中选择启动选项卡，然后检查要使用的操作系统是否设置为当前操作系统；默认操作系统。如果未设置，请从窗口中选择所需的操作系统，然后在同一窗口中选择设置为默认值。
3. 要删除其他分区，请选择该分区，然后选择删除、应用、确定。

如果错误仍然出现，请从安装光盘或修复光盘启动计算机，然后按照以下步骤操作。

1. 跳过初始语言屏幕，然后在主安装屏幕上选择修复计算机。
2. 在选择选项屏幕上，选择问题排查。
3. 在高级选项屏幕上，选择命令提示符。
4. 在命令提示符处输入 `bootrec.exe /fixmbr`，然后按 Enter。

BYOL 导入需要 64 位系统。

必须使用 64 位操作系统映像。有关更多信息，请参阅 BYOL 支持的 Windows 版本。

BYOL 导入需要使用尚未重置的系统。

映像重置计数不得为 0。重置功能允许您延长 Windows 试用版的激活期。创建映像过程要求重置计数为 0 以外的值。

检查 Windows 重置计数

1. 在 Windows“开始”菜单上，选择 Windows 系统，然后选择命令提示符。
2. 在命令提示符处输入 `cscript C:\Windows\System32\slmgr.vbs /dlv`，然后按 Enter。
3. 将重置计数重置为 0 以外的值。有关更多信息，请参阅 Sysprep（概化）Windows 安装。

BYOL 导入需要使用尚未就地升级的系统。该系统已就地升级。

Windows 必须尚未从以前的版本升级。

BYOL 导入要求系统上未安装防病毒软件。

必须卸载防病毒软件。运行 BYOLChecker 以获取要卸载的防病毒软件的详细信息。

BYOL 导入要求 Windows 10 系统使用旧版启动模式。

Windows 10 BootMode 必须使用旧版 BIOS。有关更多信息，请参阅启动模式。

步骤 4：将 VM 从虚拟化环境中导出

要为 BYOL 创建映像，您必须先将 VM 从虚拟化环境中导出。VM 必须位于最大大小为 70 GB 且可用空间至少为 10 GB 的单个卷上。有关更多信息，请参阅《VM Import/Export 用户指南》中的虚拟化环境文档以及从虚拟化环境中导出虚拟机。

Windows 11 为统一可扩展固件接口 (UEFI)、可信平台模块 (TPM) 2.0 和安全启动支持设定了新的硬件要求。VM Import/Export 是 Windows 11 导入所独有的，它使用 Microsoft 密钥和 NitrotPM 自动启用 UEFI 安全启动。有关更多信息，请参阅使用虚拟机导入/导出将 Windows 11 映像 AWS 带到。

步骤 5：将 VM 作为映像导入 Amazon EC2

在导出 VM 后，请查看从 VM 导入 Windows 操作系统的要求。根据需要执行操作。有关更多信息，请参阅 VM Import/Export 要求。

> **Note**
>
> 不支持导入带有加密磁盘的 VM。如果您已为 Amazon Elastic Block Store (Amazon EBS) 卷选择了默认加密，则必须在导入 VM 之前取消选择该选项。

将 VM 作为 Amazon 系统映像 (AMI) 导入 Amazon EC2。使用以下方法之一：

- 通过 AWS CLI使用 import-image 命令。有关更多信息，请参阅《AWS CLI 命令参考》中的 import-image。
- 使用 ImportImage API 操作。有关更多信息，请参阅 Amazon EC2 API 参考ImportImage中的。

有关更多信息，请参阅《VM Import/Export 用户指南》 中的将 VM 作为映像导入。

步骤 6：使用控制台创建 BYOL 映像 WorkSpaces

执行以下步骤创建 WorkSpaces BYOL 映像。

> **Note**
>
> 要执行此过程，请确认您拥有 AWS Identity and Access Management (IAM) 权限：
>
> - 打电话 WorkSpaces **`ImportWorkspaceImage`**。
> - 对要用于创建 BYOL 映像的 Amazon EC2 映像调用 Amazon EC2 **`DescribeImages`**。
> - 对要用于创建 BYOL 映像的 Amazon EC2 映像调用 Amazon EC2 **`ModifyImageAttribute`**。确保对 Amazon EC2 映像的启动权限不受限制。在整个 BYOL 映像创建过程中，映像必须可共享。
>
> 有关特定于 BYOL 的 IAM 策略示例 WorkSpaces，请参阅对 WorkSpaces 进行身份和访问管理。有关使用 IAM 权限的更多信息，请参阅《IAM 用户指南》中的更改 IAM 用户的权限。要根据您的图片创建 Graphics.g4dn、 GraphicsPro .g4dn、Graphics 或 GraphicsPro 捆绑包，请联系AWS Support 中心将您的账户添加到允许列表中。在您的账户被列入允许列表后，您可以使用 AWS CLI import-workspace-image命令收录 Graphics.g4dn、.g4dn、Graphics 或图像 GraphicsPro。 GraphicsPro 有关更多信息，请参阅《AWS CLI 命令参考》中的 import-workspace-image。

从 Windows VM 创建映像

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Images。
3. 选择创建 BYOL 映像。
4. 在创建 BYOL 映像页面上，执行以下操作：
   - 对于 AMI ID，请选择 EC2 控制台链接，然后选择您按照上一节 (步骤 5：将 VM 作为映像导入 Amazon EC2) 中所述导入的 Amazon EC2 映像。映像名称必须以 `ami-` 开头并后跟 AMI 的标识符（例如，`ami-1234567e`）。
   - 对于映像名称，请输入映像的唯一名称。
   - 对于描述，请输入一个描述以帮助您快速识别映像。
   - 对于实例类型，根据要用于图像的协议（PCoIP 或流媒体协议 (WSP GraphicsPro)），选择相应的捆绑包类型（常规、Graphics.g4dn、Graphics 或）。 WorkSpaces 如果要创建.g4d GraphicsPro n 捆绑包，请选择 Graphics.g4dn。对于不支持 GPU 的捆绑包（除了 Graphics.g4dn、.g4dn、Graphics 或之外的捆绑包），请选择常规。 GraphicsPro GraphicsPro

> **Note**
>
> - 目前只能为 PCoIP 协议创建 Graphics GraphicsPro .g4dn、.g4dn、Graphics 和 GraphicsPro 图像。
> - 只能针对 WSP 协议创建 Windows 11 映像。
> - Graphics.g4dn 和 GraphicsPro .g4dn 捆绑包目前不适用于 Windows 11。
> - Windows 11 不支持图形和 GraphicsPro 图像。

- （可选）对于所选应用程序，选择要订阅的 Microsoft Office 版本。有关更多信息，请参阅 将 Microsoft Office 添加到 BYOL 映像中。
- （可选）对于标签，选择添加新标签，将标签与此映像相关联。有关更多信息，请参阅 标记 WorkSpaces 资源。

5. 选择创建 BYOL 映像。

   创建映像时，控制台映像页面上的映像状态将显示为待处理。BYOL 摄取过程至少需要 90 分钟。如果您还订阅了 Office，则预计该过程至少需要 3 个小时。

   如果映像验证不成功，控制台将显示一条错误代码。当映像创建完成时，状态将更改为 Available (可用)。

步骤 7：从 BYOL 映像创建自定义捆绑包

创建 BYOL 映像后，您可以使用该映像创建一个自定义捆绑包。有关信息，请参阅 创建自定义 WorkSpaces 镜像和捆绑包。

第 8 步：注册专用目录 WorkSpaces

要将 BYOL 映像用于 WorkSpaces，必须为此目的注册一个目录。

要为其注册目录 WorkSpaces

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择目录。
3. 选择目录，然后依次选择 Actions (操作) 和 Register (注册)。
4. 在 “注册目录” 对话框中，对于 “启用专用” WorkSpaces，选择 “是”。
5. 选择 Register。

如果您已经注册了未在专用硬件上运行的 AWS Managed Microsoft AD 目录或 AD Connector 目录，则可以为此目的设置一个新 AWS Managed Microsoft AD 目录或 AD Connector 目录。 WorkSpaces 您也可以取消注册该目录，然后将其重新注册为专用目录。 WorkSpaces为此，请执行以下步骤。

> **Note**
>
> 只有在没有与该目录关联的情况下 WorkSpaces ，您才能执行此过程。

取消注册目录并将其重新注册为专用目录 WorkSpaces

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 终止现有 WorkSpaces的。
3. 在导航窗格中，选择目录。
4. 选择目录，然后选择 Actions、Deregister。
5. 当系统提示您确认时，选择 Deregister (取消注册)。
6. 再次选择目录，然后依次选择 Actions (操作) 和 Register (注册)。
7. 在 “注册目录” 对话框中，对于 “启用专用” WorkSpaces，选择 “是”。
8. 选择 Register。

第 9 步：启动你的 BYOL WorkSpaces

注册专用目录后 WorkSpaces，可以在此目录 WorkSpaces 中启动 BYOL。有关如何启动的信息 WorkSpaces，请参阅使用 WorkSpaces 启动虚拟桌面。

关联 BYOL 账户

您可以使用 BYOL 链接来关联账户和共享 BYOL 配置。BYOL 配置包括您的帐户使用的 CIDR 范围以及您使用 Windows 许可证创建 WorkSpaces 的映像。所有关联的账户共享相同的底层硬件基础架构。

启用 BYOL 关联的账户是底层硬件基础设施的主要所有者，称为源账户。源帐户管理对底层硬件基础架构的访问权限。目标账户是指与来源账户关联的账户。

> **Important**
>
> BYOL 账户关联的 API 目前在中 AWS GovCloud (US) Region不可用。

> **Note**
>
> 您要关联的 AWS 账户必须是您的组织的一部分，并且属于同一个付款人账户。您只能关联同一区域内的账户。

关联来源账户和目标账户

1. 使用 CreateAccountLinkInvitationAPI 将邀请链接从您的来源账户发送到目标账户。
2. 使用 AcceptAccountLinkInvitationAPI 接受来自目标账户的待处理链接。
3. 使用 GetAccountLink或链接 API 验证ListAccount链接是否已建立。

监控你的 WorkSpaces

您可以使用以下功能来监视您的 WorkSpaces.

CloudWatch 指标

亚马逊向亚马逊 WorkSpaces 发布 CloudWatch 有关您的数据点 WorkSpaces。 CloudWatch 允许您以一组有序的时间序列数据（称为指标）的形式检索有关这些数据点的统计信息。您可以使用这些指标来验证您的表现 WorkSpaces 是否符合预期。有关更多信息，请参见 监控您的 WorkSpaces 使用 CloudWatch 指标。

CloudWatch 活动

当用户登录您的网站时，亚马逊 WorkSpaces 可以向亚马逊活动提交 CloudWatch 事件 WorkSpace。这使您能够在事件发生时进行响应。有关更多信息，请参见 监控您的 Amazon WorkSpaces 使用情况 EventBridge。

CloudTrail 日志

AWS CloudTrail 提供用户、角色或 AWS 服务在 WorkSpaces 中执行的操作记录。使用收集的信息 CloudTrail，您可以确定向哪个请求发出 WorkSpaces、发出请求的 IP 地址、谁发出了请求、何时发出请求以及其他详细信息。有关更多信息，请参阅使用记录 WorkSpaces API 调用 CloudTrail。AWS CloudTrail记录智能卡用户的成功和失败登录事件。有关更多信息，请参见 了解智能卡用户的 AWS 登录事件。

CloudWatch 互联网监视器

借助 Amazon CloudWatch Internet Monitor，您可以了解互联网问题如何影响托管的应用程序与最终用户之间的性能AWS和可用性。您还可以使用 CloudWatch 互联网监视器来：

- 为一个或多个 WorkSpace 目录创建监视器。
- 监控互联网性能。
- 针对最终用户的城市网络（包括其位置）和 ASN（通常是互联网服务提供商 (ISP)）及其 WorkSpace 区域之间的问题获取警报。

网络监测仪使用 AWS 从其全球网络足迹中捕获的连接数据来计算面向互联网流量的性能和可用性基准。网络监测仪目前无法为个人最终用户提供互联网性能，但可以在城市和 ISP 级别提供此类性能。

使用 CloudWatch 自动仪表板监控您的 WorkSpaces 健康状况

WorkSpaces 您可以使用 CloudWatch 自动仪表板进行监控，该仪表板收集原始数据并将其处理为可读的近乎实时的指标。这些指标会保留 15 个月，用于访问历史信息并监控 Web 应用程序或服务的性能。还可以设置特定阈值监视警报，在达到对应阈值时发送通知或采取行动。有关更多信息，请参阅 Amazon CloudWatch 用户指南。

当您使用您的AWS帐户进行配置时， CloudWatch 控制面板会自动创建 WorkSpaces。控制面板允许您监控各个区域的 WorkSpaces 指标，例如其运行状况和绩效。您也可以将控制板用于以下目的：

- 识别运行状况不佳的 WorkSpace 实例。
- 识别 WorkSpace 实例不健康的运行模式、协议和操作系统。
- 查看一段时间内的关键资源利用率。
- 识别异常以帮助进行故障排除。

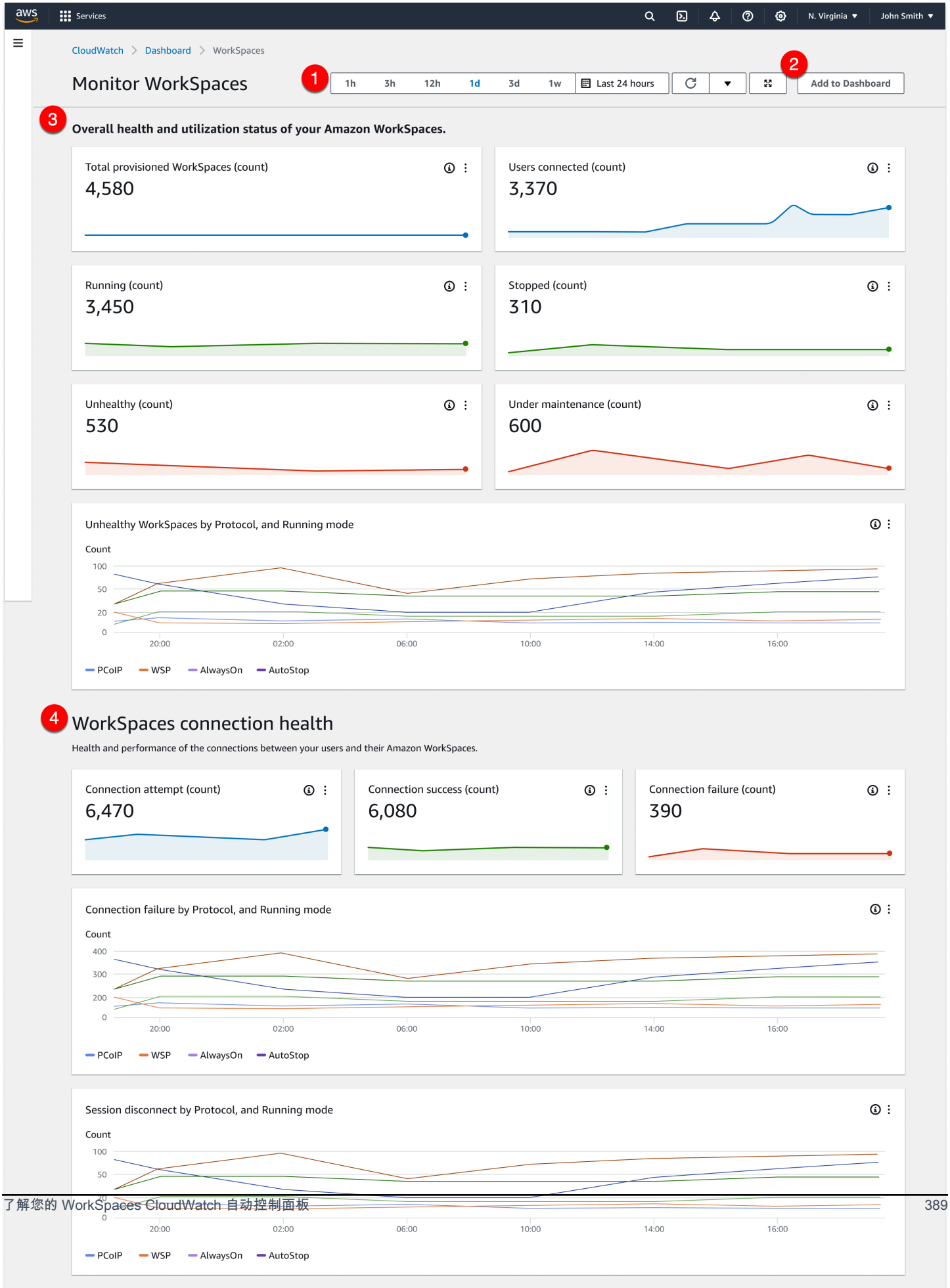
WorkSpaces CloudWatch 所有AWS商业区域均提供自动控制面板。

使用 WorkSpaces CloudWatch 自动控制面板

1. 打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，选择控制面板。
3. 选择 “自动仪表板” 选项卡。
4. 选择WorkSpaces。

了解您的 WorkSpaces CloudWatch 自动控制面板

CloudWatch 自动控制面板允许您深入了解 WorkSpaces 资源的性能，并帮助您识别性能问题。


aws
Services
N. Virginia
John Smith
CloudWatch > Dashboard > WorkSpaces
Monitor WorkSpaces
1
1h 3h 12h 1d 3d 1w
Last 24 hours
2
Add to Dashboard
3
Overall health and utilization status of your Amazon WorkSpaces.
Total provisioned WorkSpaces (count)
4,580
Users connected (count)
3,370
Running (count)
3,450
Stopped (count)
310
Unhealthy (count)
530
Under maintenance (count)
600
Unhealthy WorkSpaces by Protocol, and Running mode
Count
100
50
20
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop
4
WorkSpaces connection health
Health and performance of the connections between your users and their Amazon WorkSpaces.
Connection attempt (count)
6,470
Connection success (count)
6,080
Connection failure (count)
390
Connection failure by Protocol, and Running mode
Count
400
300
200
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop
Session disconnect by Protocol, and Running mode
Count
100
50
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop

仪表板包含以下功能：

1. 使用时间和日期范围控件查看历史数据。
2. 向自定义仪表板添加 CloudWatch 自定义仪表板视图。
3. WorkSpaces 通过执行以下操作来监控您的整体运行状况和利用率状态：
    a. 查看已配置的总数 WorkSpaces、连接的用户数、运行状况不佳和运行良好的实例数。WorkSpace
    b. 查看不健康状况 WorkSpaces 及其不同的变量，例如协议和计算模式。
    c. 将鼠标悬停在折线图上，可以查看一段时间内特定协议和运行模式下运行正常或不健康的 WorkSpace 实例数量。
    d. 选择省略号菜单，然后选择在指标中查看，以在时间尺度图表上查看指标。
4. 查看您的连接指标及其不同的变量，例如任何给定时间 WorkSpaces 环境中的连接尝试次数、成功连接次数和连接失败次数。
5. 查看影响用户体验的 InSession 延迟，例如往返时间 (RTT)，以确定连接运行状况和数据包丢失以监控网络运行状况。
6. 查看主机性能和资源利用率，以识别和解决潜在的性能问题。

监控您的 WorkSpaces 使用 CloudWatch 指标

WorkSpaces 和 Amazon CloudWatch 已整合，因此您可以收集和分析绩效指标。您可以使用 CloudWatch 控制台、 CloudWatch 命令行界面或使用 CloudWatch API 以编程方式监控这些指标。CloudWatch 还允许您在达到指标的指定阈值时设置警报。

有关使用 CloudWatch 和警报的更多信息，请参阅 Amazon CloudWatch 用户指南。

先决条件

要获取 CloudWatch 指标，请`us-east-1`在该区域的`AMAZON`子集上启用端口 443 的访问权限。有关更多信息，请参阅 的 IP 地址和端口要求 WorkSpaces。

内容

- WorkSpaces 指标
- WorkSpaces 指标的维度
- 监控示例

WorkSpaces 指标

AWS/WorkSpaces 命名空间包括以下指标。

指标	描述	尺寸	统计数据	单位
Available [1]	其中的数字返回 WorkSpaces 了健康状态。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	计数
Unhealthy [1]	其中的数字返回 WorkSpaces 了不健康的状态。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	计数
ConnectionAttempt [2]	连接尝试次数。	DirectoryId WorkspaceId RunningMode Protocol ComputeType	Average、Sum、Maximum、Minimum、Data Samples	计数

指标	描述	尺寸	统计数据	单位
		BundleId UserName		
ConnectionSuccess [2]	成功连接的数量。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	计数
ConnectionFailure [2]	失败连接的数量。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	计数

指标	描述	尺寸	统计数据	单位
SessionLaunchTime [2、6]	启动 WorkSpaces 会话所需的时间。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	秒（时间）
InSessionLatency [2、6]	WorkSpaces 客户端与之间的往返时间 WorkSpace。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	毫秒（时间）
SessionDisconnect [2、6]	已关闭的连接数，包括用户启动的和失败的连接。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	计数

指标	描述	尺寸	统计数据	单位
UserConnected [3]	WorkSpaces 已连接用户的数量。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	计数
Stopped	其中的数量 WorkSpaces 已停止。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	计数
Maintenance [4]	其数量 WorkSpaces 正在维护中。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	Average、Sum、Maximum、Minimum、Data Samples	计数

指标	描述	尺寸	统计数据	单位
TrustedDeviceValidationAttempt [5、6]	设备身份验证签名验证尝试次数。	DirectoryId	Average、Sum、Maximum、Minimum、Data Samples	计数
TrustedDeviceValidationSuccess [5、6]	成功的设备身份验证签名验证次数。	DirectoryId	Average、Sum、Maximum、Minimum、Data Samples	计数
TrustedDeviceValidationFailure [5、6]	失败的设备身份验证签名验证次数。	DirectoryId	Average、Sum、Maximum、Minimum、Data Samples	计数
TrustedDeviceCertificateDaysBeforeExpiration [6]	与该目录关联的根证书过期前所剩的天数。	CertificateId	Average、Sum、Maximum、Minimum、Data Samples	计数
CPUUsage	已使用的 CPU 资源的百分比。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均值、最大值、最小值	百分比

指标	描述	尺寸	统计数据	单位
MemoryUsage	已用计算机内存的百分比。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均值、最大值、最小值	百分比
RootVolumeDiskUsage	已使用的根磁盘容量的百分比。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均值、最大值、最小值	百分比
UserVolumeDiskUsage	已使用的用户磁盘容量的百分比。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均值、最大值、最小值	百分比

指标	描述	尺寸	统计数据	单位
UDPPacketLossRate [7]	在客户端和网关之间丢弃的数据包的百分比。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均值、最大值、最小值、数据样本	百分比
UpTime	自上次重启以来的时间 WorkSpace。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName	平均值、最大值、最小值、数据样本	秒

[1] WorkSpaces 定期向 a 发送状态请求 WorkSpace。A WorkSpace Available 在响应这些请求以及未能响应这些请求Unhealthy时被标记。这些指标是按粒度WorkSpace 级别提供的，也可以汇总组织 WorkSpaces 中的所有指标。

[2] WorkSpaces 记录了与每个连接的指标 WorkSpace。这些指标是在用户成功通过客户端进行身份验证，然后 WorkSpaces 客户端启动会话后发出的。这些指标按粒度WorkSpace 级别提供，也可以在目录 WorkSpaces 中汇总所有指标。

[3] WorkSpaces 定期向 a 发送连接状态请求 WorkSpace。当用户正在主动使用他们的会话时，他们被报告为已连接。该指标按粒度WorkSpace 级别提供，也针对组织 WorkSpaces 中的所有人进行汇总。

[4] 此指标适用于配置 WorkSpaces 了 AutoStop 运行模式的指标。如果您启用了维护功能 WorkSpaces，则此指标会捕获当前处于维护状态的 WorkSpaces 数量。该指标按粒度提供，它描述了何时 WorkSpace 进入维护状态以及何时被移除。WorkSpace

[5] 如果目录启用了可信设备功能，Amazon 将 WorkSpaces 使用基于证书的身份验证来确定设备是否可信。当用户尝试访问其设备时 WorkSpaces，系统会发出这些指标以指示可信设备身份验证成功或失败。这些指标在每个目录的粒度级别上可用，并且仅适用于亚马逊 WorkSpaces Windows 和 macOS 客户端应用程序。

[6] 在 WorkSpaces Web 访问上不可用。

[7] 该指标衡量平均丢包率。

- 在 PCoIP 上：测量来自客户端的网关平均丢包率。
- 在 WSP 上：测量从客户端到网关的平均丢包率。

WorkSpaces 指标的维度

要筛选指标数据，请使用以下维度。

维度	描述
DirectoryId	将指标数据筛选到 WorkSpaces 指定目录中的。目录 ID 的形式为 d-XXXXXXXXXX 。
WorkspaceId	将指标数据筛选为指定值 WorkSpace。WorkSpace 身份证的形式是ws-XXXXXXXXXX 。
CertificateId	将指标数据筛选到与该目录关联的指定根证书。证书 ID 的形式为 wsc-XXXXXXXXX 。
RunningMode	WorkSpaces 按运行模式筛选指标数据。运行模式的形式为 AutoStop 或 AlwaysOn。
BundleId	WorkSpaces 按协议筛选指标数据。捆绑包的形式是wsb-XXXXXXXXX 。
ComputeType	WorkSpaces 按计算类型筛选指标数据。

维度	描述
Protocol	WorkSpaces 按协议类型筛选指标数据。
UserName	WorkSpaces 按用户名筛选指标数据。

监控示例

以下示例演示了如何使用 AWS CLI 来响应 CloudWatch 警报并确定目录 WorkSpaces 中哪个出现了连接故障。

回应 CloudWatch 警报

1. 使用 describe-alarms 命令确定警报适用于哪个目录。

```
aws cloudwatch describe-alarms --state-value "ALARM"

{
  "MetricAlarms": [
    {
      ...
      "Dimensions": [
        {
          "Name": "DirectoryId",
          "Value": "directory_id"
        }
      ],
      ...
    }
  ]
}
```

2. 使用 desc ribe- WorkSpaces workspaces 命令获取指定目录中的列表。

```
aws workspaces describe-workspaces --directory-id directory_id

{
  "Workspaces": [
    {
      ...
      "WorkspaceId": "workspace1_id",
```

```
      ...
    },
    {
      ...
      "WorkspaceId": "workspace2_id",
      ...
    },
    {
      ...
      "WorkspaceId": "workspace3_id",
      ...
    }
  ]
}
```

3. 使用 g CloudWatch et-metric -statistics 命令获取目录 WorkSpace 中每个指标的指标。

```
aws cloudwatch get-metric-statistics \
--namespace AWS/WorkSpaces \
--metric-name ConnectionFailure \
--start-time 2015-04-27T00:00:00Z \
--end-time 2015-04-28T00:00:00Z \
--period 3600 \
--statistics Sum \
--dimensions "Name=WorkspaceId,Value=workspace_id"

{
  "Datapoints" : [
    {
      "Timestamp": "2015-04-27T00:18:00Z",
      "Sum": 1.0,
      "Unit": "Count"
    },
    {
      "Timestamp": "2014-04-27T01:18:00Z",
      "Sum": 0.0,
      "Unit": "Count"
    }
  ],
  "Label" : "ConnectionFailure"
}
```

监控您的 Amazon WorkSpaces 使用情况 EventBridge

您可以使用来自 Amazon 的事件 WorkSpaces 来查看、搜索、下载、存档、分析和响应您的 WorkSpaces成功登录。例如，您可以将事件用于以下目的：

- 将 WorkSpaces 登录事件存储或存档为日志，以备将来参考，分析日志以寻找模式，然后根据这些模式采取行动。
- 使用 WAN IP 地址确定用户从何处登录，然后使用策略仅允许用户访问 WorkSpaces 符合事件类型中找到的访问标准的文件或数据`WorkSpaces Access`。
- 使用分析登录数据并执行自动操作 AWS Lambda。
- 使用策略控制阻止未经授权的 IP 地址访问文件和应用程序。
- 找出用于连接的 WorkSpaces 客户端版本 WorkSpaces。

A WorkSpaces mazon 会尽力发布这些事件。近乎实时 EventBridge 地向其发送事件。使用 EventBridge，您可以创建触发程序化操作以响应事件的规则。例如，您可以配置规则，以调用 SNS 主题发送电子邮件通知，或者调用 Lambda 函数执行某些操作。有关更多信息，请参阅 Amazon EventBridge 用户指南。

WorkSpaces 访问事件

WorkSpaces 当用户成功登录到时，客户端应用程序会发送`WorkSpaces Access`事件 WorkSpace。所有 WorkSpaces 客户端都发送这些事件。

WorkSpaces 使用 WorkSpaces 流协议 (WSP) 而发出的事件需要 WorkSpaces 客户端应用程序版本 4.0.1 或更高版本。

事件表示为 JSON 对象。以下是 `WorkSpaces Access` 事件的示例数据。

```
{
    "version": "0",
    "id": "64ca0eda-9751-dc55-c41a-1bd50b4fc9b7",
    "detail-type": "WorkSpaces Access",
    "source": "aws.workspaces",
    "account": "123456789012",
    "time": "2023-04-05T16:13:59Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
```

```
        "clientIpAddress": "192.0.2.3",
        "actionType": "successfulLogin",
        "workspacesClientProductName": "WorkSpacesWebClient",
        "loginTime": "2023-04-05T16:13:37.603Z",
        "clientPlatform": "Windows",
        "directoryId": "domain/d-123456789",
        "clientVersion": "5.7.0.3472",
        "workspaceId": "ws-xyskdga"
    }
}
```

特定于事件的字段

`clientIpAddress`

客户端应用程序的 WAN IP 地址。对于 PCoIP 零客户端，这是 Teradici 身份验证客户端的 IP 地址。

`actionType`

此值始终为 `successfulLogin`。

`workspacesClientProductName`

以下值区分大小写。

- `WorkSpaces Desktop client` - Windows、macOS 和 Linux 客户端
- `Amazon WorkSpaces Mobile client` - iOS 客户端
- `WorkSpaces Mobile Client` - Android 客户端
- `WorkSpaces Chrome Client` - Chromebook 客户端
- `WorkSpacesWebClient` - Web Access 客户端
- `AmazonWorkSpacesThinClient`— Amazon WorkSpaces 瘦客户机设备
- `Teradici PCoIP Zero Client, Teradici PCoIP Desktop Client, or Dell Wyse PCoIP Client` - 零客户端

`loginTime`

用户登录的时间 WorkSpace。

`clientPlatform`

- `Android`
- `Chrome`

- iOS
- Linux
- OSX
- Windows
- Teradici PCoIP Zero Client and Tera2
- Web

directoryId

的目录标识符 WorkSpace。必须在目录标识符前面加上 domain/。例如，"domain/d-123456789"。

clientVersion

用于连接的客户端版本 WorkSpaces。

workspaceId

WorkSpace 的标识符。

创建用于处理 WorkSpaces 事件的规则

使用以下步骤创建用于处理 WorkSpaces 事件的规则。

先决条件

要接收电子邮件通知，请创建 Amazon Simple Notification Service 主题。

1. 通过 https://console.aws.amazon.com/sns/v3/home 打开 Amazon SNS 控制台。
2. 在导航窗格中，选择 Topics（主题）。
3. 选择创建主题。
4. 对于类型，选择标准。
5. 对于 Name（名称），请为主题输入一个名称。
6. 选择创建主题。
7. 选择创建订阅。
8. 对于协议，选择电子邮件。
9. 对于 Endpoint（端点），请输入接收通知的电子邮件地址。
10. 选择创建订阅。

11. 您将收到电子邮件消息，其主题行为：AWS Notification - Subscription Confirmation。请按照说明确认订阅。

创建用于处理 WorkSpaces 事件的规则

1. 打开亚马逊 EventBridge 控制台，网址为 https://console.aws.amazon.com/events/。
2. 选择创建规则。
3. 对于 Name（名称），请为规则输入一个名称。
4. 对于规则类型，选择具有事件模式的规则。
5. 选择下一步。
6. 对于 Event pattern（事件模式），执行以下操作：
   a. 对于事件源，选择 AWS 服务。
   b. 对于 AWS 服务，选择WorkSpaces。
   c. 对于事件类型，选择WorkSpaces访问权限。
   d. 默认情况下，我们会就每个事件发送通知。如果愿意，您可以创建一种事件模式来筛选特定客户端或 WorkSpaces 的事件。
7. 选择下一步。
8. 按以下操作指定目标：
   a. 对于 Target types（目标类型），选择 AWS 服务。
   b. 对于 Select a target（选择一个目标），选择 SNS topic（SNS 主题）。
   c. 对于主题，选择您为通知创建的 SNS 主题。
9. 选择下一步。
10. （可选）向规则添加标签。
11. 选择下一步。
12. 选择创建规则。

了解智能卡用户的 AWS 登录事件

AWS CloudTrail 会记录智能卡用户的成功和失败登录事件。这包括每次提示用户解决特定凭证问题或因素时捕获的登录事件，以及该特定凭证验证请求的状态。用户只有在完成所有必需的凭证质疑后才能登录，这会导致系统记录 `UserAuthentication` 事件日志。

下表记录了每个登录的 CloudTrail 事件名称及其目的。

事件名称	事件目的
CredentialChallenge	通知 AWS 登录已请求用户解决特定的凭证质疑，并指定所需的 CredentialType 凭证（例如 SMARTCARD）。
CredentialVerification	通知用户已尝试解决特定 CredentialChallenge 请求，并指定该凭证是成功还是失败。
UserAuthentication	通知用户受到质疑的所有身份验证要求均已成功完成，并且用户已成功登录。当用户未能成功完成所需的凭证质疑时，不会记录 UserAuthentication 事件日志。

下表记录了特定登录 CloudTrail 事件中包含的其他有用事件数据字段。

事件名称	事件目的	登录事件适用性	示例值
AuthWorkflowID	关联整个登录序列中发出的所有事件。对于每位用户登录，AWS 登录可发出多个事件。	CredentialChallenge，CredentialVerification，UserAuthentication	“AuthWorkflowID”：“9de74b32-8362-4a01-a524-de21df59fd83”
CredentialType	通知用户已尝试解决特定 CredentialChallenge 请求，并指定该凭证是成功还是失败。	CredentialChallenge，CredentialVerification，UserAuthentication	“CredentialType”：“SMARTCARD”（目前可能的值：SMARTCARD）
LoginTo	通知用户受到质疑的所有身份验证要求均已成功完成，并且用户已成功登录。当用户未能成功完成所需的凭证质疑时，不会记录 UserAuthe	UserAuthentication	“LoginTo”：“https://skylight.local”

事件名称	事件目的	登录事件适用性	示例值
	ntication 事件日志。		

AWS 登录场景的示例事件

以下示例显示了适用于不同登录场景的 CloudTrail 事件的预期序列。

目录

使用智能卡进行身份验证时成功登录

以下事件序列捕获了成功登录智能卡的示例。

CredentialChallenge


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:29Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialChallenge",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
```

```
        "CredentialType": "SMARTCARD"
    },
    "requestID": "65551a6d-654a-4be8-90b5-bbfef7187d3a",
    "eventID": "fb603838-f119-4304-9fdc-c0f947a82116",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialChallenge": "Success"
    }
}
```

Successful CredentialVerification

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialVerification",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "81869203-1404-4bf2-a1a4-3d30aa08d8d5",
    "eventID": "84c0a2ff-413f-4d0f-9108-f72c90a41b6c",
    "readOnly": false,
```

```
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialVerification": "Success"
    }
}
```

Successful UserAuthentication

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "UserAuthentication",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "LoginTo": "https://skylight.local",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "81869203-1404-4bf2-a1a4-3d30aa08d8d5",
    "eventID": "acc0dba8-8e8b-414b-a52d-6b7cd51d38f6",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
```

```
    "serviceEventDetails": {
        UserAuthentication": "Success"
    }
}
```

仅使用智能卡进行身份验证时登录失败

以下事件序列捕获了登录智能卡失败的示例。

CredentialChallenge

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:06Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialChallenge",
    "awaRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "73dfd26b-f812-4bd2-82e9-0b2abb358cdb",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "73eb499d-91a8-4c18-9c5d-281fd45ab50a",
    "eventID": "f30a50ec-71cf-415a-a5ab-e287edc800da",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
```

```
    "serviceEventDetails": {
        CredentialChallenge": "Success"
    }
}
```

Failed CredentialVerification

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:13Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialVerification",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "73dfd26b-f812-4bd2-82e9-0b2abb358cdb",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "051ca316-0b0d-4d38-940b-5fe5794fda03",
    "eventID": "4e6fbfc7-0479-48da-b7dc-e875155a8177",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialVerification": "Failure"
    }
}
```

Amazon 的业务连续性 WorkSpaces

WorkSpaces Amazon 建立AWS在全球基础设施之上，该基础设施分为AWS区域和可用区。这些区域和可用区在物理隔离和数据冗余方面提供了故障恢复能力。有关更多信息，请参见 Amazon WorkSpaces 中的故障恢复能力。

Amazon WorkSpaces 还提供跨区域重定向，该功能可与您的域名系统 (DNS) 路由策略配合使用，以便在主域名系统 (DNS) 路由策略 WorkSpaces 不可用 WorkSpaces 时将您的 WorkSpaces 用户重定向到替代方案。例如，通过使用 DNS 故障转移路由策略，当用户无法访问主区域 WorkSpaces 中的用户时，您可以将他们连接到您指定的故障转移区域。 WorkSpaces

您可以使用跨区域重定向来实现区域故障恢复能力和高可用性。您也可以将其用于其他目的，例如流量分配或 WorkSpaces 在维护期间提供替代方案。如果您使用 Amazon Route 53 进行 DNS 配置，则可以利用监控亚马逊 CloudWatch 警报的运行状况检查。

Amazon M WorkSpaces ulti-Region Resilition 在辅助 WorkSpace 区域提供自动化的冗余虚拟桌面基础架构，并简化了在主区域因中断而无法访问时将用户重定向到辅助区域的流程。

您可以将 WorkSpaces 多区域弹性与跨区域重定向结合使用，在辅助区域部署冗余的虚拟桌面基础架构，并设计跨 WorkSpace 区域故障转移策略，为中断事件做好准备。您也可以将此解决方案用于其他目的，例如流量分配或 WorkSpaces 在维护期间提供替代方案。如果您使用 Route 53 进行 DNS 配置，则可以利用监控 CloudWatch 警报的运行状况检查。

内容

Amazon 的跨区域重定向 WorkSpaces

借助 Amazon 的跨区域重定向功能 WorkSpaces，您可以使用完全限定的域名 (FQDN) 作为您的注册码。 WorkSpaces跨区域重定向与您的域名系统 (DNS) 路由策略配合使用，可在主域名系统 (DNS) 路由策略 WorkSpaces 不可用 WorkSpaces 时将您的 WorkSpaces 用户重定向到替代方案。例如，通过使用 DNS 故障转移路由策略，当用户无法访问主AWS区域 WorkSpaces 中的用户时，您可以将他们连接到您指定的故障转移区域。 WorkSpaces

您可以使用跨区域重定向和 DNS 故障转移路由策略，实现区域灾难恢复能力和高可用性。您也可以将此功能用于其他目的，例如流量分配或 WorkSpaces 在维护期间提供替代方案。如果您使用 Amazon Route 53 进行 DNS 配置，则可以利用监控亚马逊 CloudWatch 警报的运行状况检查。

要使用此功能，您必须 WorkSpaces 为两个（或更多）AWS区域的用户进行设置。您还必须创建称为连接别名 的基于 FQDN 的特殊注册码。这些连接别名会替换您的用户特定于区域的注册码。WorkSpaces （特定于区域的注册码仍然有效；但是，要使跨区域重定向运行，您的用户必须改用 FQDN 作为注册码。）

要创建连接别名，您需指定一个连接字符串，该字符串是您的 FQDN，如 `www.example.com` 或 `desktop.example.com`。要使用此域进行跨区域重定向，您必须向域注册商注册它并为您的域配置 DNS 服务。

创建连接别名后，将其与不同区域的 WorkSpaces 目录关联以创建关联对。每个关联对都有一个主区域和一个或多个故障转移区域。如果主区域发生中断，则您的 DNS 故障转移路由策略会将您的 WorkSpaces 用户重定向到您在故障转移区域中为他们设置的路由策略。 WorkSpaces

要指定您的主区域和故障转移区域，您需在配置 DNS 故障转移路由策略时，定义区域优先级（主区域或辅助区域）。

内容

先决条件

- 您必须拥有并注册要在连接别名中用作 FQDN 的域。如果您尚未使用其他域注册商，则可以使用 Amazon Route 53 注册您的域。有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的使用 Amazon Route 53 注册域名。

  > **Important**
  >
  > 您必须拥有所有必要的权限才能使用与Amazon一起使用的任何域名 WorkSpaces。您同意，该域名不会违反或侵犯任何第三方的合法权利，也不会以其他方式违反适用法律。

  域名总长度不能超过 255 个字符。有关域名的更多信息，请参阅《Amazon Route 53 开发人员指南》中的 DNS 域名格式。

  跨区域重定向既适用于公有域名，也适用于私有 DNS 区域中的域名。如果您使用的是私有 DNS 区域，则必须提供虚拟专用网络 (VPN) 与包含您的虚拟私有云 (VPC) 的连接 WorkSpaces。如果您的 WorkSpaces 用户尝试使用来自公共互联网的私有 FQDN，则 WorkSpaces 客户端应用程序会返回以下错误消息：

  ```
  "We're unable to register the WorkSpace because of a DNS server issue. Contact your administrator for help."
  ```

- 您必须设置 DNS 服务并配置必要的 DNS 路由策略。跨区域重定向与您的 DNS 路由策略配合使用，可根据需要重定向您的 WorkSpaces 用户。
- 在要设置跨区域重定向的每个主区域和故障转移区域中， WorkSpaces 为用户创建。确保在每个区域的每个 WorkSpaces 目录中使用相同的用户名。为了保持您的 Active Directory 用户数据同步，我们建议您使用 AD Connector 指向您 WorkSpaces 为用户设置的每个区域中的同一个活动目录。有关创建的更多信息 WorkSpaces，请参阅启动 WorkSpaces。

  > **Important**
  >
  > 如果您将AWS托管 Microsoft AD 目录配置为多区域复制，则只能注册主区域中的目录以供亚马逊 WorkSpaces使用。尝试在复制区域中注册该目录以供在 Amazon 上使用 WorkSpaces 将失败。在复制的区域 WorkSpaces 内，亚马逊不支持使用AWS托管 Microsoft AD 进行多区域复制。

完成跨区域重定向的设置后，必须确保您的 WorkSpaces 用户使用的是基于 FQDN 的注册码，而不是其主区域的基于区域的注册码（例如）。`WSpdx+ABC12D`为此，您必须按照步骤 5：向您的 WorkSpaces 用户发送连接字符串中的步骤操作，向他们发送一封包含 FQDN 连接字符串的电子邮件。

> **Note**
>
> 如果您在 WorkSpaces 控制台中创建用户而不是在 Active Directory 中创建用户，则每当您启动新用户时，都会 WorkSpaces 自动向您的用户发送一封包含基于区域的注册码的邀请电子邮件。 WorkSpace这意味着，当您在故障转移区域中 WorkSpaces 为用户进行设置时，您的用户还将自动收到有关这些故障转移的电子邮件 WorkSpaces。您需要指示您的用户忽略含有基于区域的注册码的电子邮件。

限制

- 跨区域重定向不会自动检查与主区域的连接是否失败，然后会使您无法转移 WorkSpaces 到另一个区域。换句话说，自动故障转移不会发生。

  要实施自动故障转移场景，您必须将其他机制与跨区域重定向结合使用。例如，您可以将 Amazon Route 53 故障转移 DNS 路由策略与监控主要区域 CloudWatch 警报的 Route 53 运行状况检查配对。如果触发了主区域的 CloudWatch 警报，则您的 DNS 故障转移路由策略会将您的 WorkSpaces 用户重定向到您在故障转移区域中为他们设置的策略。 WorkSpaces
- 当您使用跨区域重定向时，用户数据不会 WorkSpaces 在不同区域之间保存。为了确保用户可以从不同的区域访问他们的文件，如果您的主区域和故障转移区域支持亚马逊 WorkDocs ，我们建议您 WorkDocs 为 WorkSpaces 用户设置亚马逊。有关亚马逊的更多信息 WorkDocs，请参阅《亚马逊 WorkDocs 管理指南》中的 Amazon WorkDocs Driv e。有关为 WorkSpace 用户启用 Amazon WorkDocs 的更多信息，请参阅向 WorkSpaces 注册目录和为 AWS Managed Microsoft AD 启用 Amazon WorkDocs。有关 WorkSpaces 用户如何在其 WorkDocs 上设置亚马逊的信息 WorkSpaces，请参阅《亚马逊 WorkSpaces 用户指南》 WorkDocs中的与集成。
- 只有版本 3.0.9 或更高版本的 Linux、macOS 和 Windows 客户端应用程序支持跨区域重定向。WorkSpaces 您也可以将跨区域重定向与 Web Access 配合使用。
- 跨区域重定向在所有可用 Amazon 的AWS区域中 WorkSpaces 都可用，但除了 AWS GovCloud (US) Region s 和中国（宁夏）区域。

步骤 1：创建连接别名

使用相同的 AWS 账户，在您要设置跨区域重定向的每个主区域和故障转移区域中创建连接别名。

创建连接别名

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在控制台的右上角，为您的选择主要AWS区域。 WorkSpaces
3. 在导航窗格中，选择 Account Settings (账户设置)。
4. 在跨区域重定向下，选择创建连接别名。
5. 对于连接字符串，输入 FQDN，例如 `www.example.com` 或 `desktop.example.com`。连接字符串最大长度为 255 个字符。它只能包含字母（A-Z 和 a-z）、数字（0-9）和以下字符：.-

   > **Important**
   >
   > 创建连接字符串后，它始终与您的 AWS 账户关联。您无法使用其他账户重新创建相同的连接字符串，即使您从原始账户中删除了连接字符串的所有实例也是如此。连接字符串针对您的账户进行了全局保留。

6. （可选）在标签下，指定要与连接别名关联的任意标签。
7. 选择创建连接别名。
8. 重复这些步骤，但是在中Step 2，请务必为您的选择故障转移区域 WorkSpaces。如果您有多个故障转移区域，请对每个故障转移区域重复这些步骤。请务必使用相同的 AWS 账户，在每个故障转移区域中创建连接别名。

（可选）步骤 2：与其他账户共享连接别名

您可以与同一 AWS 区域中的另一个 AWS 账户共享连接别名。与另一个账户共享连接别名将向该账户授予权限，以便仅将该别名与该账户在同一区域中拥有的目录关联或取消关联。只有拥有连接别名的账户才能删除该别名。

> **Note**
>
> 对于每个 AWS 区域，只能将一个目录与连接别名关联。如果您与其他 AWS 账户共享连接别名，则只有一个账户（您的账户或共享账户）可以将别名与该区域中的目录关联。

与其他 AWS 账户共享连接别名

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在控制台的右上角，选择要与其他 AWS 账户共享连接别名的 AWS 区域。
3. 在导航窗格中，选择 Account Settings (账户设置)。
4. 在跨区域重定向关联下，选择连接字符串，然后选择操作、共享/取消共享连接别名。

   您也可以从详细信息页面共享连接别名的别名。为此，请在共享账户下，选择共享连接别名。
5. 在共享/取消共享连接别名页面的与账户共享下，输入您要在此 AWS 区域中与之共享连接别名的 AWS 账户 ID。
6. 选择共享。

步骤 3：将连接别名与每个区域的目录相关联

将相同的连接别名与两个或更多区域中的 WorkSpaces 目录相关联可在目录之间创建关联对。每个关联对都有一个主区域和一个或多个故障转移区域。

例如，如果您的主要区域是美国西部（俄勒冈）区域，则可以将美国西部（俄勒冈）地区的 WorkSpaces 目录与美国东部（弗吉尼亚北部）地区的目录配对。 WorkSpaces 如果主区域发生中断，则跨区域重定向将与您的 DNS 故障转移路由策略以及您在美国西部（俄勒冈）区域实施的任何运行状况检查结合使用，以将您的用户重定向到 WorkSpaces 您在美国东部（弗吉尼亚北部）区域为他们设置的区域。有关跨区域重定向体验的更多信息，请参阅跨区域重定向期间会发生什么。

> **Note**
>
> 如果您的 WorkSpaces 用户距离故障转移区域很远（例如，数千英里之外），则他们的 WorkSpaces 体验可能比平时响应不佳。要查看从您所在地前往各个AWS地区的往返时间 (RTT)，请使用 A mazon Connection Healt WorkSpaces h Check。

将连接别名与目录关联

对于每个 AWS 区域，只能将连接别名与一个目录关联。如果您已与其他 AWS 账户共享连接别名，则只有一个账户（您的账户或共享账户）可以将别名与该区域中的目录关联。

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在控制台的右上角，为您的选择主要AWS区域。 WorkSpaces

3. 在导航窗格中，选择 Account Settings (账户设置)。
4. 在跨区域重定向关联下，选择连接字符串，然后选择操作、关联/取消关联。

   您也可以将连接别名与连接别名详细信息页面上的目录相关联。为此，请在关联的目录下，选择关联目录。
5. 在关联/取消关联页面的关联到目录下，选择要在该 AWS 区域中关联连接别名的目录。

   > **Note**
   >
   > 如果您将AWS托管 Microsoft AD 目录配置为多区域复制，则只有主区域中的目录可以与 Amazon WorkSpaces 一起使用。尝试在 Amazon 的复制区域中使用该目录 WorkSpaces 将失败。在复制的区域 WorkSpaces 内，亚马逊不支持使用AWS托管 Microsoft AD 进行多区域复制。
6. 选择关联。
7. 重复这些步骤，但是在中Step 2，请务必为您的选择故障转移区域 WorkSpaces。如果您有多个故障转移区域，请对每个故障转移区域重复这些步骤。请务必将相同的连接别名与每个故障转移区域中的目录相关联。

步骤 4：配置您的 DNS 服务并设置 DNS 路由策略

创建连接别名和连接别名关联对后，您可以为连接字符串中使用的域配置 DNS 服务。为此，您可以使用任何 DNS 服务提供商。如果您还没有首选 DNS 服务提供商，则可使用 Amazon Route 53。有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的将 Amazon Route 53 配置为 DNS 服务。

为域配置 DNS 服务后，您必须设置要用于跨区域重定向的 DNS 路由策略。例如，您可以使用 Amazon Route 53 运行状况检查来确定您的用户是否可以在特定区域连接到他们 WorkSpaces 。如果您的用户无法连接，则您可以使用 DNS 故障转移策略将 DNS 流量从一个区域路由到另一个区域。

有关选择 DNS 路由策略的更多信息，请参阅《Amazon Route 53 开发人员指南》中的选择路由策略。有关 Amazon Route 53 运行状况检查的更多信息，请参阅《Amazon Route 53 开发人员指南》中的 Amazon Route 53 如何检查资源的运行状况。

在设置 DNS 路由策略时，您需要连接别名与主区域中的 WorkSpaces 目录之间的关联的连接标识符。您还需要一个或多个故障转移区域中连接别名和 WorkSpaces 目录之间关联的连接标识符。

> **Note**
>
> 连接标识符与连接别名 ID 不同。连接别名 ID 以 `wsca-` 开头。

查找连接别名关联的连接标识符

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在控制台的右上角，为您的选择主要AWS区域。 WorkSpaces
3. 在导航窗格中，选择 Account Settings (账户设置)。
4. 在跨区域重定向关联下，选择连接字符串文本 (FQDN)，以查看连接别名详细信息页面。
5. 在连接别名详细信息页面的关联的目录下，记下为连接标识符显示的值。
6. 重复这些步骤，但是在中Step 2，请务必为您的选择故障转移区域 WorkSpaces。如果您有多个故障转移区域，请重复这些步骤，查找每个故障转移区域的连接标识符。

示例：使用 Route 53 设置 DNS 故障转移路由策略

以下示例为您所在域设置了公有托管区。但是，您可以设置公有或私有托管区。有关设置托管区的更多信息，请参阅《Amazon Route 53 开发人员指南》中的使用托管区。

此示例还使用了故障转移路由策略。您可以将其他路由策略类型用于跨区域重定向策略。有关选择 DNS 路由策略的更多信息，请参阅《Amazon Route 53 开发人员指南》中的选择路由策略。

在 Route 53 中设置故障转移路由策略时，需要针对主区域进行运行状况检查。有关在 Route 53 中创建运行状况检查的更多信息，请参阅《Amazon Route 53 开发人员指南》中的创建 Amazon Route 53 运行状况检查和配置 DNS 故障转移以及创建、更新和删除运行状况检查。

如果您想在 Route 53 运行状况检查中使用 Amazon CloudWatch 警报，则还需要设置 CloudWatch 警报来监控主区域中的资源。有关的更多信息 CloudWatch，请参阅 Amazon 是什么 CloudWatch？ 在《亚马逊 CloudWatch 用户指南》中。有关 Route 53 如何在其运行状况检查中使用 CloudWatch 警报的更多信息，请参阅《Amazon Route 53 开发者指南》中的 Route 53 如何确定监控 CloudWatch 警报的运行状况检查的状态和监控警 CloudWatch 报。

要在 Route 53 中设置 DNS 故障转移路由策略，您首先需要为您的域创建一个托管区。

1. 通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择托管区，然后选择创建托管区。
3. 在已创建的托管区页面上，在域名下输入您的域名（例如 `example.com`）。

4. 在类型下，选择公有托管区。
5. 选择创建托管区域。

然后为您的主区域创建运行状况检查。

1. 通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择运行状况检查，然后选择创建运行状况检查。
3. 在配置运行状况检查页面上，输入运行状况检查的名称。
4. 在 “要监控的内容” 中，选择 “终端节点”、“其他运行状况检查的状态（计算的运行状况检查）” 或 “CloudWatch 警报状态”。
5. 根据您在上一步中选择的内容，配置您的运行状况检查，然后选择下一步。
6. 在在运行状况检查失败时收到通知页面上，对于创建警报，选择是或否。
7. 选择创建运行状况检查。

在创建运行状况检查后，您可以创建 DNS 故障转移记录。

1. 通过以下网址打开 Route 53 控制台：https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域）。
3. 在托管区页面上，选择您的域名。
4. 在域名的详细信息页面上，选择创建记录。
5. 在选择路由策略页面上，选择故障转移，然后选择下一步。
6. 在配置记录页面的基本配置下，对于记录名称，输入您的子域名。例如，如果您的 FQDN 是 `desktop.example.com`，请输入 **`desktop`**。

   > **Note**
   >
   > 如果要使用根域，请将记录名称留空。但是，我们建议您使用子域名，例如`desktop`或`workspaces`，除非您已将该域名设置为仅用于您 WorkSpaces的。

7. 对于记录类型，选择 TXT - 用于验证电子邮件发件人和应用程序特定的值。
8. 将 TTL 秒设置保留为默认值。
9. 在要添加到 ***`your_domain_name`*** 的故障转移记录下，选择定义故障转移记录。

现在，您需要为主区域和故障转移区域设置故障转移记录。

示例：为您的主区域设置故障转移记录

1. 在定义故障转移记录对话框中，对于值/流量路由至，选择 IP 地址或其他值（具体取决于记录类型）。
2. 这时，将打开一个框供您输入示例文本条目。输入您主区域的连接别名关联的连接标识符。
3. 对于故障转移记录类型，选择主。
4. 在运行状况检查中，选择您为主区域创建的运行状况检查。
5. 对于记录 ID，输入描述以识别此记录。
6. 选择定义故障转移记录。新故障转移记录将显示在要添加到 ***your_domain_name*** 的故障转移记录下方。

示例：为您的故障转移区域设置故障转移记录

1. 在要添加到 ***your_domain_name*** 的故障转移记录下，选择定义故障转移记录。
2. 在定义故障转移记录对话框中，对于值/流量路由至，选择 IP 地址或其他值（具体取决于记录类型）。
3. 这时，将打开一个框供您输入示例文本条目。输入故障转移区域的连接别名关联的连接标识符。
4. 对于故障转移记录类型，选择辅助。
5. （可选）对于运行状况检查，输入您为故障转移区域创建的运行状况检查。
6. 对于记录 ID，输入描述以识别此记录。
7. 选择定义故障转移记录。新故障转移记录将显示在要添加到 ***your_domain_name*** 的故障转移记录下方。

如果您为主区域设置的运行状况检查失败，则您的 DNS 故障转移路由策略会将您的 WorkSpaces 用户重定向到您的故障转移区域。Route 53 继续监控您的主要区域的运行状况检查，当您的主区域的运行状况检查不再失败时，Route 53 会自动将您的 WorkSpaces 用户重定向回主区域 WorkSpaces 中的用户。

有关创建 DNS 记录的更多信息，请参阅《Amazon Route 53 开发人员指南》中的使用 Amazon Route 53 控制台创建记录。有关配置 DNS TXT 记录的更多信息，请参阅《Amazon Route 53 开发人员指南》中的 TXT 记录类型。

步骤 5：向您的 WorkSpaces 用户发送连接字符串

要确保在中断期间根据需要重定向用户，您必须 WorkSpaces 将连接字符串 (FQDN) 发送给您的用户。如果您已经向 WorkSpaces 用户发布了基于区域的注册码（例如WSpdx+ABC12D），则这些代码仍然有效。但是，要使跨区域重定向起作用，您的 WorkSpaces 用户在 WorkSpaces 客户端应用程序 WorkSpaces 中注册时必须使用连接字符串作为注册码。

> **Important**
>
> 如果您在 WorkSpaces 控制台中创建用户而不是在 Active Directory 中创建用户，则每当您启动新用户时，都会 WorkSpaces 自动向您的用户发送一封包含基于区域的注册码（例如WSpdx+ABC12D）的邀请电子邮件。 WorkSpace即使您已经设置了跨区域重定向，自动发送的新版邀请电子邮件也 WorkSpaces 包含此基于区域的注册码，而不是您的连接字符串。
> 要确保您的 WorkSpaces 用户使用的是连接字符串而不是基于区域的注册码，您必须按照以下步骤向他们发送另一封包含连接字符串的电子邮件。

向您的 WorkSpaces 用户发送连接字符串

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在控制台的右上角，为您的选择主要AWS区域。 WorkSpaces
3. 在导航窗格中，选择。WorkSpaces
4. 在该WorkSpaces页面上，使用搜索框搜索要向其发送邀请的用户，然后 WorkSpace 从搜索结果中选择相应的用户。 WorkSpace 一次只能选择一个。
5. 依次选择 Actions (操作) 和 Invite User (邀请用户)。
6. 在邀请用户加入他们的 WorkSpaces页面上，您将看到一个要发送给用户的电子邮件模板。
7. （可选）如果有多个连接别名与您的 WorkSpaces 目录相关联，请从 Connection 别名字符串列表中选择您希望用户使用的连接字符串。电子邮件模板将更新以显示您选择的字符串。
8. 使用您自己的电子邮件应用程序，复制电子邮件模板文本，并将其粘贴到要发送给用户的电子邮件中。在电子邮件应用程序中，您可以根据需要修改文本。当邀请电子邮件准备就绪之后，将其发送给用户。

跨区域重定向架构图

下图描述了跨区域重定向的部署过程。

> **Note**
>
> 跨区域重定向只能促进跨区域故障转移和回退。它不利于 WorkSpaces 在辅助区域中创建和维护，也不允许跨区域数据复制。 WorkSpaces 在主区域和次要区域中，都应分开管理。

启动跨区域重定向

发生中断时，您可以手动更新 DNS 记录，也可以使用基于运行状况检查的自动路由策略，从而确定故障转移区域。我们建议遵循使用 Amazon Route 53 创建灾难恢复机制中概述的灾难恢复机制。

跨区域重定向期间会发生什么

在区域故障转移期间，您的 WorkSpaces 用户将与主区域 WorkSpaces 的用户断开连接。当他们尝试重新连接时，会收到以下错误消息：

```
We can't connect to your WorkSpace. Check your network connection, and then try again.
```

然后，系统会提示您的用户重新登录。如果他们使用 FQDN 作为注册码，则当他们再次登录时，您的 DNS 故障转移路由策略会将他们重定向到您在故障转移区域中为他们设置的路由策略。 WorkSpaces

> **Note**
>
> 在某些情况下，用户在再次登录时可能无法重新连接。如果出现这种情况，他们必须关闭并重新启动 WorkSpaces 客户端应用程序，然后尝试再次登录。

取消连接别名与目录的关联

只有拥有目录的账户才能取消连接别名与该目录的关联。

如果您已与另一个账户共享连接别名，并且该账户已将连接别名与该账户拥有的目录关联，则必须使用该账户，取消连接别名与该目录的关联。

取消连接别名与目录的关联

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在控制台的右上角，选择包含您要取消关联的连接别名的 AWS 区域。

3. 在导航窗格中，选择 Account Settings (账户设置)。
4. 在跨区域重定向关联下，选择连接字符串，然后选择操作、关联/取消关联。

   您也可以取消连接别名与连接别名详细信息页面的关联。为此，请在关联的目录下，选择取消关联。
5. 在关联/取消关联页面上，选择取消关联。
6. 在要求您确认取消关联的对话框中，选择取消关联。

取消共享连接别名

只有连接别名的所有者才能取消共享该别名。如果您取消与某个账户共享连接别名，则该账户将无法再将该连接别名与目录相关联。

取消共享连接别名

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在控制台的右上角，选择包含您要取消共享的连接别名的 AWS 区域。
3. 在导航窗格中，选择 Account Settings (账户设置)。
4. 在跨区域重定向关联下，选择连接字符串，然后选择操作、共享/取消共享连接别名。

   您也可以取消连接别名与连接别名详细信息页面的共享。为此，请在共享账户下选择取消共享。
5. 在共享/取消共享连接别名页面上，选择取消共享。
6. 在要求您确认取消共享连接别名的对话框中，选择取消共享。

删除连接别名

只有当连接别名归您的账户所有且未与目录关联时，您才能删除该别名。

如果您已与另一个账户共享连接别名，并且该账户已将连接别名与该账户拥有的目录关联，则该账户必须先取消连接别名与目录的关联，然后您才能删除该别名。

> **Important**
>
> 创建连接字符串后，它始终与您的 AWS 账户关联。您无法使用其他账户重新创建相同的连接字符串，即使您从原始账户中删除了连接字符串的所有实例也是如此。连接字符串针对您的账户进行了全局保留。

> **Warning**
>
> 如果您不再使用 FQDN 作为 WorkSpaces 用户的注册码，则必须采取某些预防措施来防止出现潜在的安全问题。有关更多信息，请参见 停止使用跨区域重定向后的安全注意事项。

删除连接别名

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在控制台的右上角，选择包含您要删除的连接别名的 AWS 区域。
3. 在导航窗格中，选择 Account Settings (账户设置)。
4. 在跨区域重定向关联下，选择连接字符串，然后选择删除。

   您也可以从连接别名详细信息页面删除连接别名。为此，请在页面右上角，选择删除。

   > **Note**
   >
   > 如果禁用删除按钮，请确保您是别名的所有者，并确保该别名未与目录关联。

5. 在要求您确认删除的对话框中，选择删除。

用于关联和取消关联连接别名的 IAM 权限

如果您使用 IAM 用户关联或取消关联连接别名，则该用户必须拥有 `workspaces:AssociateConnectionAlias` 和 `workspaces:DisassociateConnectionAlias` 的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:AssociateConnectionAlias",
        "workspaces:DisassociateConnectionAlias"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:123456789012:connectionalias/wsca-a1bcd2efg"
      ]
```

```
    }
  ]
}
```

Important

如果您正在创建 IAM 策略来关联或取消关联不拥有连接别名的账户的连接别名，则无法在 ARN 中指定账户 ID。您必须改用账户 ID 的 *，如以下示例策略所示。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:AssociateConnectionAlias",
        "workspaces:DisassociateConnectionAlias"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:*:connectionalias/wsca-a1bcd2efg"
      ]
    }
  ]
}
```

只有当账户拥有要关联或取消关联的连接别名时，您才能在 ARN 中指定该账户 ID。

有关使用 IAM 的更多信息，请参阅 对 WorkSpaces 进行身份和访问管理。

停止使用跨区域重定向后的安全注意事项

如果您不再使用 FQDN 作为 WorkSpaces 用户的注册码，则必须采取以下预防措施来防止出现潜在的安全问题：

- 请务必向 WorkSpaces 用户发放其 WorkSpaces 目录中特定于区域的注册码（例如`WSpdx+ABC12D`），并指示他们停止使用 FQDN 作为注册码。
- 如果您仍然拥有该域，请务必更新您的 DNS TXT 记录以删除该域，这样它就不会在网络钓鱼攻击中遭到利用。如果您从 DNS TXT 记录中删除此域名，而您的 WorkSpaces 用户尝试使用 FQDN 作为注册码，则他们的连接尝试将无害地失败。

- 如果您不再拥有该域名，则您的 WorkSpaces 用户必须使用其区域特定的注册码。如果他们继续尝试使用 FQDN 作为注册码，则系统可能会将其连接尝试重定向到恶意站点。

Amazon 的多区域弹性 WorkSpaces

Amazon WorkSpaces 多区域弹性 (MRR) 使您能够在主区域因中断性事件而无法访问时将用户重定向到辅助 WorkSpaces 区域，而无需您的用户在登录到备用区域时切换注册码。 WorkSpaces待机 WorkSpaces 是 Amazon WorkSpaces 多区域弹性的一项功能，可简化备用部署的创建和管理。在辅助区域设置用户目录后，在主区域中选择要 WorkSpace 为其创建备用目录的用户目录。 WorkSpace 系统会自动将主 WorkSpace 捆绑包映像镜像到次要区域。然后，它会在您的辅助区域自动配置新的备用 WorkSpace 副本

Amazon WorkSpaces 多区域弹性建立在跨区域重定向的基础上，利用 DNS 运行状况检查和故障转移功能。它允许您使用完全限定的域名 (FQDN) 作为 WorkSpaces 注册码。当您的用户登录时 WorkSpaces，您可以根据您的 FQDN 域名系统 (DNS) 策略将他们重定向到支持的 WorkSpaces 区域。如果您使用 Amazon Route 53，我们建议您在为其设计跨区域重定向策略时使用运行状况检查来监控亚马逊 CloudWatch 警报。 WorkSpaces有关更多信息，请参阅 Amazon Route 53 开发人员指南中的创建 Amazon Route 53 运行状况检查和配置 DNS 故障转移。

数据复制是备用模式的一项附加功能 WorkSpaces ，可将数据从主区域单向复制到辅助区域。启用数据复制后，系统和用户卷的 EBS 快照每 12 小时拍摄一次。多区域弹性会定期检查是否有新的快照。找到快照后，它会启动到辅助区域的副本。当副本到达辅助区域时，它们被用来更新辅助区域 WorkSpace。

内容

先决条件

- 在创建备用 WorkSpaces 服务器之前，您必须为主区域中的用户创建 WorkSpaces。有关创建的更多信息 WorkSpaces，请参阅使用 WorkSpaces 启动虚拟桌面。
- 要在待机状态下启用数据复制 WorkSpaces，您应该将自我管理的 Active Directory 或 AWS 托管 Microsoft AD 配置为复制到备用区域。有关更多信息，请参阅创建您的 AWS 托管 Microsoft AD 目录和添加复制区域。
- 确保在主 WorkSpaces服务器上更新网络依赖驱动程序，例如 ENA、NVMe 和 PV 驱动程序。你应该至少每 6 个月这样做一次。有关更多信息，请参阅安装或升级适用于 Windows 实例的弹性网络适配器 (ENA) 驱动程序和在 Windows 实例上升半虚拟化驱动程序。AWS NVMe 驱动程序
- 确保定期将 ec2Config、ec2Launch 和 ec2Launch V2 代理更新到最新版本。你应该至少每 6 个月这样做一次。有关更多信息，请参阅更新 ec2Config 和 ec2Launch。
- 为确保正确的数据复制，请确保主区域和辅助区域中的活动目录与 FQDN、OU 和用户 SID 同步。
- 备用服务器的默认配额（限制）WorkSpaces 为 0。在创建备用副本之前，您需要申请增加服务配额 WorkSpace。有关更多信息，请参阅 亚马逊 WorkSpaces 配额。
- 确保使用客户管理的密钥对主密钥和备用密钥进行加密 WorkSpaces。您可以使用单区域密钥或多区域密钥来加密您的主密钥和备用 WorkSpaces密钥。

限制

- 待机模式 WorkSpaces 仅复制主卷的捆绑映像， WorkSpaces 但不会从主卷复制系统卷（驱动器 C）或用户卷（驱动器 D） WorkSpaces。要将系统卷（驱动器 C）或用户卷（驱动器 D）从主卷复制 WorkSpaces 到备用卷 WorkSpaces，必须启用数据复制。
- 您不能直接修改、重建、恢复或迁移备用实例 WorkSpace。
- 跨区域重定向的故障转移由您的 DNS 设置控制。要实施自动故障转移场景，您必须将其他机制与跨区域重定向结合使用。例如，您可以将 Amazon Route 53 故障转移 DNS 路由策略与监控主区域 CloudWatch 警报的 Route 53 运行状况检查配对。如果在主区域中调用 CloudWatch 警报，则您的 DNS 故障转移路由策略会将您的 WorkSpaces 用户重定向到您在故障转移区域中为他们设置的策略。 WorkSpaces
- 数据复制只有一种方式，即将数据从主区域复制到辅助区域。在待机 WorkSpaces 故障转移期间，您可以在 12 到 24 小时之间访问数据和应用程序。中断后，手动备份您在辅助服务器上创建的所有数据 WorkSpace 并注销。我们建议将您的工作保存到外部驱动器（例如网络驱动器），以便您可以从主驱动器访问数据 WorkSpace。
- 数据复制不支持 S AWS imple AD。

- 在备用模式下启用数据复制时 WorkSpaces，将每 12 小时拍摄一次主卷 WorkSpaces （包括根卷和系统卷）的 EBS 快照。特定数据卷的初始快照为已满，后续快照为增量快照。因此，给定对象的第一次复制 WorkSpace 将比后续复制花费更长的时间。快照是按内部计划启动的 WorkSpaces ，您无法控制时间。
- 如果主域 WorkSpace 和备用域使用同一个域 WorkSpace 加入，我们建议您只 WorkSpace 在给定的时间点连接到主域 WorkSpace 或备用域控制器，以免失去与域控制器的连接。
- 如果您将您的配置 AWS Managed Microsoft AD 为多区域复制，则只能注册主区域中的目录以供使用 WorkSpaces。如果您尝试在复制区域中注册该目录以供使用 WorkSpaces，则该目录将失败。AWS Managed Microsoft AD 不支持在复制的区域 WorkSpaces 内使用多区域复制。
- 如果您已经设置了跨区域重定向，并在不使用备用区域的情况下 WorkSpaces 在主区域和次要区域中创建了跨区域重定向 WorkSpaces，则无法将辅助区域 WorkSpace 中的现有重定向直接转换为备用 WorkSpace 区域。相反，您需要关闭辅助区域 WorkSpace 中的，在主区域中选择要 WorkSpace 为其创建备用副本的区域，然后使用备用创建备 WorkSpaces 用副本 WorkSpace。 WorkSpace
- 中断后，手动备份您在辅助服务器上创建的所有数据 WorkSpace 并注销。我们建议将您的工作保存到外部驱动器（例如网络驱动器），以便您可以从主驱动器访问数据 WorkSpace。
- WorkSpaces 多区域弹性目前在以下区域可用：
  - 美国东部（弗吉尼亚州北部）区域
  - 美国西部（俄勒冈州）区域
  - 欧洲地区（法兰克福）区域
  - 欧洲地区（爱尔兰）区域
- WorkSpaces 只有版本 3.0.9 或更高版本的 Linux、macOS 和 Windows 客户端应用程序支持多区域弹性。 WorkSpaces 您也可以将多区域韧性与 Web Access 结合使用。
- WorkSpaces 多区域弹性支持 Windows 和自带许可证 (BYOL)。 WorkSpaces它不支持亚马逊 Linux、Ubuntu 或支持 GPU WorkSpaces （例如 Graphics WorkSpaces、Graphics.g4dn 或.g4d GraphicsPro n）。 GraphicsPro
- 故障转移或故障恢复完成后，请等待 15 到 30 分钟，然后再连接到您的 WorkSpace。

配置您的多区域弹性备用模式 WorkSpace

配置您的多区域弹性备用副本 WorkSpace

1. 在您的主要和次要区域中设置用户目录。确保在每个区域的每个 WorkSpaces 目录中使用相同的用户名。

为了保持您的 Active Directory 用户数据同步，我们建议您使用 AD Connector 指向您 WorkSpaces 为用户设置的每个区域中的同一个活动目录。有关创建目录的更多信息，请参阅向注册目录 WorkSpaces。

> **Important**
>
> 如果您将 AWS Managed Microsoft AD 目录配置为多区域复制，则只能注册主区域中的目录以供使用 WorkSpaces。尝试在复制的区域中注册该目录以供使用 WorkSpaces 将失败。 AWS Managed Microsoft AD 不支持在复制的区域 WorkSpaces 内使用多区域复制。

2. WorkSpaces 为主区域的用户创建。有关创建的更多信息 WorkSpaces，请参阅启动 WorkSpaces。
3. WorkSpace 在辅助区域创建备用副本。有关创建备用副本的更多信息 WorkSpace，请参阅创建备用实例 WorkSpace。
4. 创建连接字符串 (FQDN)，并将其与主区域和次要区域中的用户目录相关联。

   您必须在账户中启用跨区域重定向，因为备用数据库建立在跨区域重 WorkSpaces 定向的基础上。按照 Amazon 跨区域重定向说明中的步骤 1-3 进行操作。 WorkSpaces
5. 配置 DNS 服务并设置 DNS 路由策略。

   您必须设置 DNS 服务并配置必要的 DNS 路由策略。跨区域重定向与您的 DNS 路由策略配合使用，可根据需要重定向您的 WorkSpaces 用户。
6. 设置完跨区域重定向后，您必须向用户发送一封包含 FQDN 连接字符串的电子邮件。有关更多信息，请参阅步骤 5：向您的 WorkSpaces 用户发送连接字符串。确保您的 WorkSpaces 用户使用的是基于 FQDN 的注册码，而不是其主要区域的基于区域的注册码（例如 wspdx+abc12d）。

> **Important**
>
> - 如果您在 WorkSpaces 控制台中创建用户而不是在 Active Directory 中创建用户，则每当您启动新用户时，都会 WorkSpaces 自动向您的用户发送一封包含基于区域的注册码的邀请电子邮件。 WorkSpace这意味着，当你 WorkSpaces 为次要区域的用户进行设置时，你的用户也将自动收到这些辅助区域的电子邮件 WorkSpaces。您需要指示您的用户忽略含有基于区域的注册码的电子邮件。
> - 区域特定的注册码仍然有效；但是，要使跨区域重定向起作用，您的用户必须改用 FQDN 作为注册码。

创建备用副本 WorkSpace

在创建备用副本之前 WorkSpace，请确保已完成先决条件，包括在主区域和次要区域中创建用户目录、在主区域 WorkSpaces 为用户进行配置、在账户中配置跨区域重定向以及通过服务配额请求提高待机 WorkSpaces 限制。

创建备用副本 WorkSpace

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在控制台的右上角，为您的选择主要 AWS 区域。 WorkSpaces
3. 在导航窗格中，选择 WorkSpaces。
4. 选择 WorkSpace 要为其创建备用副 WorkSpace 本的。
5. 选择 “操作”，然后选择 “创建待机” WorkSpace。
6. 选择要在其中创建备用副本的次要区域 WorkSpace，然后选择 “下一步”。
7. 选择辅助区域中的用户目录，然后选择下一步。
8. （可选）添加加密密钥、启用数据加密并管理标签。

   - 要添加加密密钥，请在输入加密密钥下方输入该密钥。
   - 要启用数据复制，请选择启用数据复制。然后，选中该复选框以确认您已授权每月额外收费。
   - 要添加新标签，请选择添加新标签。

   然后选择下一步。

   > **Note**
   >
   > - 如果原始文件已加密， WorkSpace 则会预填充此字段。但是，您可以选择将其替换为自己的加密密钥。
   > - 更新数据复制状态需要几分钟。
   > - 使用主数据库的快照成功更新备用数据库 WorkSpace 后 WorkSpace，您可以在恢复快照下找到快照的时间戳。

9. 查看待机模式的设置， WorkSpaces 然后选择 “创建”。

> **Note**
>
> - 要查看您的待机信息 WorkSpaces，请前往主要 WorkSpace 详情页面。
> - 备用磁盘 WorkSpace 仅复制主卷的捆绑映像， WorkSpace 但不会从主卷复制系统卷（驱动器 C）或用户卷（驱动器 D） WorkSpaces。默认情况下，数据复制处于关闭状态。要将系统卷（驱动器 C）或用户卷（驱动器 D）从主卷复制 WorkSpaces 到备用卷 WorkSpaces，必须启用数据复制。

管理待机模式 WorkSpace

您不能直接修改、重建、恢复或迁移备用实例 WorkSpace。

为备用服务器启用数据复制 WorkSpace

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 前往您的主要区域，选择主 WorkSpace ID。
3. 向下滚动到 “待机 WorkSpace ” 部分，然后选择 “编辑待机” WorkSpace。
4. 选择 “启用数据复制”。然后，选中该复选框以确认您已授权每月额外收费。然后，选择保存。

> **Note**
>
> - 待机模式 WorkSpaces 无法休眠。如果您停止待机模式 WorkSpace，它不会保留您未保存的工作。我们建议用户在退出待机状态 WorkSpaces之前务必保存所做的工作。
> - 要在待机状态下启用数据复制 WorkSpaces，您应该将自我管理的 Active Directory 或 AWS 托管 Microsoft AD 配置为复制到备用区域。要设置您的目录，请按照 “使用亚马逊 WorkSpaces 和 AWS 目录服务构建业务连续性演练” 部分的步骤 1 至 3 或参阅在亚马逊使用多区域 AWS 托管 Active D irectory。 WorkSpaces只有 AWS 托管 Microsoft AD 的企业版支持多区域复制。
> - 更新数据复制状态需要几分钟。
> - 使用主数据库的快照成功更新备用数据库 WorkSpace 后 WorkSpace，您可以在恢复快照下找到快照的时间戳。

删除备用副本 WorkSpace

您可以像终止常规备用 WorkSpace 服务器一样终止备用副本 WorkSpace。

删除备用副本 WorkSpace

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在控制台的右上角，为您的选择主要 AWS 区域。 WorkSpaces
3. 在导航窗格中，选择 WorkSpaces。
4. 选择待机模式 WorkSpace 并选择 “删除”。删除备用数据库大约需要 5 分钟 WorkSpace。在删除过程中，备用服务器的状态 WorkSpace 将设置为 “正在终止”。删除完成后，备用数据库将从控制台 WorkSpace 消失。

> **Note**
>
> 删除备用数据库 WorkSpace 是一项永久性操作，无法撤消。备用 WorkSpace 用户的数据不会保留，因此会被销毁。如需有关备份用户数据的帮助，请联系 Supp AWS ort。

备用单向数据复制 WorkSpaces

在多区域弹性中启用数据复制允许您将数据从主区域复制到辅助区域。在稳定状态下，多区域弹性 WorkSpaces 每 12 小时捕获一次主系统的快照（C 盘）和数据（D 盘）的快照。这些快照将传输到辅助区域并用于更新备用区域 WorkSpaces。默认情况下，待机状态的数据复制处于禁用状态 WorkSpaces。

为备用数据库启用数据复制后 WorkSpaces，特定数据卷的初始快照即已完成，而后续快照为增量快照。因此，给定对象的第一次复制 WorkSpace 将比后续复制花费更长的时间。快照是在预先确定的时间间隔内 WorkSpaces 触发的，用户无法控制时间。

在故障转移期间，当用户被重定向到辅助区域时，他们可以访问其备 WorkSpaces 用区域，其中包含保存 12 到 24 小时的数据和应用程序。当用户使用备用模式时 WorkSpaces，多区域弹性不会强迫他们退出备用数据库 WorkSpaces 或使用主区域的快照更新备 WorkSpaces 用副本。

中断后，用户在注销备用服务器 WorkSpaces 之前，应手动备份他们在辅助设备上创建的所有数据 WorkSpaces。当他们再次登录时，他们将被定向到主区域及其主区域 WorkSpaces。

计划预留 Amazon EC2 容量以备恢复

默认情况下，亚马逊多区域弹性 (MRR) 依赖于 Amazon EC2 按需池。如果特定的 Amazon EC2 实例类型无法支持您的恢复，MRR 将自动尝试重复扩展实例，直到找到可用的实例类型，但在极端情况下，实例可能并不总是可用。要提高最关键实例类型的可用性，请联系 Supp WorkSpaces ort AWS ，我们将协助您进行容量规划。

Amazon WorkSpaces 中的安全性

AWS 十分重视云安全性。作为 AWS 客户，您将从专为满足大多数安全敏感型企业的要求而打造的数据中心和网络架构中受益。

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

- 云的安全性 – AWS 负责保护在 AWS 云中运行 AWS 服务的基础设施。AWS 还向您提供可安全使用的服务。作为AWS合规性计划的一部分，第三方审计人员将定期测试和验证安全性的有效性。要了解适用于 WorkSpaces 的合规性计划，请参阅合规性计划范围内的 AWS 服务。
- 云中的安全性 - 您的责任由您使用的AWS服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

此文档将帮助您了解如何在使用 WorkSpaces 时应用责任共担模式。它说明了如何配置 WorkSpaces 以实现您的安全性和合规性目标。您还会了解如何使用其他 AWS 服务来帮助您监控和保护 WorkSpaces 资源。

目录

Amazon 的数据保护 WorkSpaces

分 AWS 担责任模式适用于亚马逊的数据保护 WorkSpaces。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架构上的内容的控制。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。我们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。
- 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）。这包括您使用控制台、API WorkSpaces 或 SDK 或以其他 AWS 服务 方式使用控制台 AWS CLI、API 或 AWS SDK 的情况。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。

有关 WorkSpaces 和 FIPS 端点加密的更多信息，请参阅设置 Amazon WorkSpaces 以符合 FedRAMP 授权或 DoD SRG 合规性要求。

静态加密

你可以 WorkSpaces 使用来自的密 AWS KMS 钥为你的存储卷加密 AWS Key Management Service。有关更多信息，请参阅 已加密 WorkSpaces。

使用加密卷创建 WorkSpaces 时， WorkSpaces 使用亚马逊弹性区块存储 (Amazon EBS) Elastic Block Store 来创建和管理这些卷。EBS 通过行业标准的 AES-256 算法，利用数据密钥加密您的卷。有关更多信息，请参阅《亚马逊 EC2 用户指南》中的 Amazon EBS 加密。

传输中加密

对于 PCoIP，传输中数据使用 TLS 1.2 加密和 SigV4 请求签名进行加密。PCoIP 协议使用带有 AES 加密的加密的 UDP 流量来传输像素。通过端口 4172（TCP 和 UDP）的流连接使用 AES-128 和 AES-256 密码进行加密，但加密默认为 128 位。您可以通过使用适用于 Windows WorkSpaces 的 “配

置 PCoIP 安全设置组策略” 设置或修改 Amazon Linux 文件中的 PCoIP 安全设置来将此默认值更改为 256 位。`pcoip-agent.conf` WorkSpaces

要了解有关 Amazon 组策略管理的更多信息 WorkSpaces，请参阅配置 PCoIP 安全设置中的管理你的 Windows WorkSpaces。要详细了解如何修改 `pcoip-agent.conf` 文件，请参阅 Teradici 文档中的控制亚马逊 Linux 上的 PCoIP 代理行为 WorkSpaces和 PCoIP 安全设置。

对于 WorkSpaces 流协议 (WSP)，传输中的流和控制数据使用 DTLS 1.2 加密 UDP 流量进行加密，使用 AES-256 密码对 TCP 流量进行 TLS 1.2 加密。

对 WorkSpaces 进行身份和访问管理

默认情况下，IAM 用户无权管理 WorkSpaces 资源和操作。要允许 IAM 用户管理 WorkSpaces 资源，您必须创建一个 IAM 策略以向他们显式授予权限，然后将此策略附加到需要这些权限的 IAM 用户或组。

要提供访问权限，请为您的用户、组或角色添加权限：

- AWS IAM Identity Center 中的用户和组：

  创建权限集合。按照《AWS IAM Identity Center 用户指南》中 创建权限集 的说明进行操作。
- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中为第三方身份提供商创建角色（联合身份验证）的说明进行操作。
- IAM 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

有关 IAM 策略的更多信息，请参阅《IAM 用户指南》中的策略和权限。

WorkSpaces 还会创建一个 IAM 角色 `workspaces_DefaultRole`，该角色允许 WorkSpaces 服务访问所需的资源。

有关 IAM 的更多信息，请参阅身份和访问管理 (IAM) 和 IAM 用户指南。您可以在《IAM 用户指南》中的 有关 Amazon WorkSpaces 的操作、资源和条件键中，找到可在 IAM 权限策略中使用的 WorkSpaces 特定资源、操作和条件上下文键。

有关可帮助您创建 IAM 策略的工具，请参阅 AWS 策略生成器。您还可以使用 IAM Policy Simulator 来测试策略是允许还是拒绝对 AWS 的特定请求。

> **Note**
>
> Amazon WorkSpaces 不支持将 IAM 凭证预调配到 WorkSpace 中（例如使用实例配置文件）。

目录

策略示例

以下示例显示了您可用于控制 IAM 用户对 Amazon WorkSpaces 的权限的策略语句。

Example 1：执行所有 WorkSpaces 任务

以下策略语句将授予 IAM 用户执行所有 WorkSpaces 任务的权限，包括创建和管理目录。它还授予运行快速设置过程的权限。

尽管 Amazon WorkSpaces 在使用 API 和命令行工具时完全支持 `Action` 和 `Resource` 元素，但要使用AWS Management Console中的 Amazon WorkSpaces，IAM 用户必须拥有使用以下操作和资源的权限：

- 操作：`workspaces:*" 和 "ds:*"`
- 资源：`"Resource": "*"`

以下策略示例演示了如何允许 IAM 用户使用AWS Management Console中的 Amazon WorkSpaces。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:CreatePolicy",
        "iam:AttachRolePolicy",
        "iam:ListRoles",
        "kms:ListAliases",
        "kms:ListKeys",
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:CreateNetworkInterface",
        "ec2:CreateInternetGateway",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "workdocs:RegisterDirectory",
        "workdocs:DeregisterDirectory",
        "workdocs:AddUserToGroup"
      ],
      "Resource": "*"
    },
    {
      "Sid": "iamPassRole",
      "Effect": "Allow",
```

```
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "workspaces.amazonaws.com"
        }
      }
    }
  ]
}
```

Example 2：执行 WorkSpace 特定任务

以下策略语句将授予 IAM 用户执行 WorkSpace 特定任务的权限，比如启动和删除 WorkSpaces。在策略语句中，`ds:*` 操作授予广泛的权限，这包括对账户中所有目录服务对象的完整控制权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:PutRolePolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

要同时授予用户在 WorkSpaces 中为用户启用 Amazon WorkDocs 的权限，请添加下例所示的 `workdocs` 操作。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "workdocs:AddUserToGroup"
```

```
      ],
      "Resource": "*"
    }
  ]
}
```

要同时授予用户使用“启动 WorkSpace 向导”的权限，请添加下例所示的 kms 操作。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "workdocs:AddUserToGroup",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource": "*"
    }
  ]
}
```

Example 3：为 BYOL WorkSpaces 执行所有 WorkSpaces 任务

以下策略语句授予 IAM 用户执行所有 WorkSpaces 任务（包括创建自带许可 (BYOL) WorkSpaces 所需的 Amazon EC2 任务）的权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "kms:ListAliases",
        "kms:ListKeys",
```

```
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:CreateNetworkInterface",
        "ec2:CreateInternetGateway",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeImages",
        "ec2:ModifyImageAttribute",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "workdocs:RegisterDirectory",
        "workdocs:DeregisterDirectory",
        "workdocs:AddUserToGroup"
      ],
      "Resource": "*"
    },
    {
      "Sid": "iamPassRole",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "workspaces.amazonaws.com"
        }
      }
    }
  ]
```

```
}
```

在 IAM 策略中指定 WorkSpaces 资源

要在策略语句的 Resource 元素中指定 WorkSpaces 资源，请使用资源的 Amazon 资源名称 (ARN)。通过允许或拒绝授予使用在 IAM 策略语句的 Action 元素中指定的 API 操作的权限，您可以控制对 WorkSpaces 资源的访问。WorkSpaces 为 WorkSpaces、捆绑包、IP 组和目录定义 ARN。

WorkSpace ARN

WorkSpace ARN 具有以下示例中显示的语法。

```
arn:aws:workspaces:region:account_id:workspace/workspace_identifier
```

区域

WorkSpace 所在的区域（例如，us-east-1）。

account_id

AWS 账户的 ID，不含连字符（例如，123456789012）。

workspace_identifier

WorkSpace 的 ID (例如，ws-a1bcd2efg)。

以下是用于标识某个特定 WorkSpace 的策略语句的 Resource 元素的格式。

```
"Resource": "arn:aws:workspaces:region:account_id:workspace/workspace_identifier"
```

您可以使用 * 通配符来指定属于特定区域中特定账户的所有 WorkSpaces。

映像 ARN

WorkSpace 映像 ARN 具有以下示例中显示的语法。

```
arn:aws:workspaces:region:account_id:workspaceimage/image_identifier
```

区域

WorkSpace 映像所在的区域（例如，us-east-1）。

account_id

AWS 账户的 ID，不含连字符（例如，123456789012）。

bundle_identifier

WorkSpace 映像的 ID (例如，wsi-a1bcd2efg)。

以下是用于标识某个特定映像的策略语句的 Resource 元素的格式。

```
"Resource": "arn:aws:workspaces:region:account_id:workspaceimage/image_identifier"
```

您可以使用 * 通配符来指定属于特定区域中特定账户的所有映像。

服务包 ARN

服务包 ARN 具有以下示例中显示的语法。

```
arn:aws:workspaces:region:account_id:workspacebundle/bundle_identifier
```

区域

WorkSpace 所在的区域（例如，us-east-1）。

account_id

AWS 账户的 ID，不含连字符（例如，123456789012）。

bundle_identifier

WorkSpace 服务包的 ID (例如，wsb-a1bcd2efg)。

以下是用于标识某个特定服务包的策略语句的 Resource 元素的格式。

```
"Resource": "arn:aws:workspaces:region:account_id:workspacebundle/bundle_identifier"
```

您可以使用 * 通配符来指定属于特定区域中特定账户的所有捆绑包。

IP 组 ARN

IP 组 ARN 具有以下示例中显示的语法。

```
arn:aws:workspaces:region:account_id:workspaceipgroup/ipgroup_identifier
```

区域

WorkSpace 所在的区域（例如，us-east-1）。

account_id

AWS 账户的 ID，不含连字符（例如，123456789012）。

ipgroup_identifier

IP 组的 ID（例如 wsipg-a1bcd2efg）。

以下是用于标识某个特定 IP 组的策略语句的 Resource 元素的格式。

```
"Resource": "arn:aws:workspaces:region:account_id:workspaceipgroup/ipgroup_identifier"
```

您可以使用 * 通配符来指定属于特定区域中特定账户的所有 IP 组。

目录 ARN

目录 ARN 具有以下示例中显示的语法。

```
arn:aws:workspaces:region:account_id:directory/directory_identifier
```

区域

WorkSpace 所在的区域（例如，us-east-1）。

account_id

AWS 账户的 ID，不含连字符（例如，123456789012）。

directory_identifier

目录的 ID（例如 d-12345a67b8）。

以下是用于标识某个特定目录的策略语句的 Resource 元素的格式。

```
"Resource": "arn:aws:workspaces:region:account_id:directory/directory_identifier"
```

您可以使用 * 通配符来指定属于特定区域中特定账户的所有目录。

连接别名 ARN

连接别名 ARN 具有以下示例中显示的语法。

```
arn:aws:workspaces:region:account_id:connectionalias/connectionalias_identifier
```

区域

连接别名所在的区域（例如，us-east-1）。

account_id

AWS 账户的 ID，不含连字符（例如，123456789012）。

connectionalias_identifier

连接别名的 ID（例如，wsca-12345a67b8）。

以下是用于标识某个特定连接别名的策略语句的 Resource 元素的格式。

```
"Resource":
 "arn:aws:workspaces:region:account_id:connectionalias/connectionalias_identifier"
```

您可以使用 * 通配符来指定属于特定区域中特定账户的所有连接别名。

不支持资源级权限的 API 操作

您不能使用以下 API 操作指定资源 ARN：

- AssociateIpGroups
- CreateIpGroup
- CreateTags
- DeleteTags
- DeleteWorkspaceImage
- DescribeAccount
- DescribeAccountModifications
- DescribeIpGroups
- DescribeTags
- DescribeWorkspaceDirectories

- DescribeWorkspaceImages
- DescribeWorkspaces
- DescribeWorkspacesConnectionStatus
- DisassociateIpGroups
- ImportWorkspaceImage
- ListAvailableManagementCidrRanges
- ModifyAccount

对于不支持资源级权限的 API 操作，必须指定以下示例中显示的资源语句。

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

不支持对共享资源进行账号级限制的 API 操作

对于以下 API 操作，当资源不归账户所有时，您无法在资源 ARN 中指定账户 ID：

- AssociateConnectionAlias
- CopyWorkspaceImage
- DisassociateConnectionAlias

对于这些 API 操作，只有当该账户拥有要处理的资源时，您才能在资源 ARN 中指定账户 ID。当账户不拥有资源时，您必须为账户 ID 指定 *，如以下示例中所示。

```
"arn:aws:workspaces:region:*:resource_type/resource_identifier"
```

创建 workspaces_DefaultRole 角色

在使用 API 注册目录之前，必须验证名为 workspaces_DefaultRole 的角色是否存在。此角色由快速设置功能创建，或者如果您使用AWS Management Console启动 WorkSpace，则它会向 Amazon WorkSpaces 授予代表您访问特定 AWS 资源的权限。如果此角色不存在，您可以使用以下程序创建它。

创建 workspaces_DefaultRole 角色

1. 登录AWS Management Console，然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。

2. 在左侧的导航窗格中，选择角色。
3. 选择 Create role（创建角色）。
4. 在 Select type of trusted entity（选择受信任实体的类型）下，选择 Another AWS 账户（其它亚马逊云科技账户）。
5. 对于账户 ID，请输入没有连字符或空格的账户 ID。
6. 对于选项，请勿指定多重验证 (MFA)。
7. 选择Next: Permissions（下一步: 权限）。
8. 在附加权限策略页面上，选择 AWS 托管策略 AmazonWorkSpacesServiceAccess 和 AmazonWorkSpacesSelfServiceAccess。
9. 在设置权限边界下，建议您不要使用权限边界，因为可能会与附加到此角色的策略发生冲突。此类冲突可能会阻止角色的某些必要权限。
10. 请选择下一步：标签。
11. 在 Add tags (optional) (添加标签(可选)) 页面上，根据需要添加标签。
12. 选择 Next: Review（下一步: 审核）。
13. 在审核页面上，对于角色名称，输入 **workspaces_DefaultRole**。
14. （可选）对于角色描述，请输入描述。
15. 请选择 Create Role(创建角色)。
16. 在 workspaces_DefaultRole 角色的摘要页面上，选择信任关系选项卡。
17. 在信任关系选项卡上，选择编辑信任关系。
18. 在编辑信任关系页面上，将现有策略语句替换为以下语句。

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

19. 选择 Update Trust Policy（更新信任策略）。

创建 AmazonWorkSpacesPCAAccess 服务角色

在用户使用基于证书的身份验证方式登录之前，您必须先验证名为 AmazonWorkSpacesPCAAccess 的角色是否存在。此角色是在您使用AWS Management Console对目录进行基于证书的身份验证时创建的，它授予 Amazon WorkSpaces 代表您访问 AWS Private CA 资源的权限。如果由于您未使用控制台管理基于证书的身份验证而导致此角色不存在，则您可以使用以下步骤创建此角色。

使用 AWS CLI 创建 AmazonWorkSpacesPCAAccess 服务角色

1. 使用以下文本创建名为 AmazonWorkSpacesPCAAccess.json 的 JSON 文件。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "prod.euc.ecm.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

2. 根据需要调整 AmazonWorkSpacesPCAAccess.json 路径并运行以下 AWS CLI 命令来创建服务角色，同时附加 AmazonWorkspacesPCAAccess 托管策略。

```
aws iam create-role --path /service-role/ --role-name AmazonWorkSpacesPCAAccess --
assume-role-policy-document file://AmazonWorkSpacesPCAAccess.json
```

```
aws iam attach-role-policy –role-name AmazonWorkSpacesPCAAccess –policy-arn
 arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess
```

WorkSpaces 的 AWS 托管策略

要向用户、组和角色添加权限，与自己编写策略相比，使用 AWS 托管策略更简单。创建仅为团队提供所需权限的 IAM 客户托管策略需要时间和专业知识。要快速入门，请使用 AWS 托管策略。这些策略涵盖常见使用案例，可在您的 AWS 账户中使用。有关 AWS 托管策略的更多信息，请参阅 IAM 用户指南中的 AWS 托管策略。

AWS 服务负责维护和更新 AWS 托管策略。您无法更改 AWS 托管策略中的权限。服务可能偶尔会向 AWS 托管策略添加额外权限以支持新功能。此类更新会影响附加策略的所有身份（用户、组和角色）。当启动新特征或新操作可用时，服务最有可能会更新 AWS 托管策略。服务不会从 AWS 托管策略中删除权限，因此策略更新不会破坏您的现有权限。

此外，AWS 还支持跨多种服务的工作职能的托管策略。例如，ReadOnlyAccess AWS 托管策略提供对所有 AWS 服务和资源的只读访问权限。当服务启动新特征时，AWS 会为新操作和资源添加只读权限。有关工作职能策略的列表和说明，请参阅 IAM 用户指南中的适用于工作职能的 AWS 托管策略。

AWS 托管策略：AmazonWorkSpacesAdmin

此策略提供访问 Amazon WorkSpaces 管理操作的权限。它提供以下权限：

- workspaces - 允许访问针对 WorkSpaces 资源执行管理操作。
- kms - 允许访问列出和描述 KMS 密钥以及列出别名。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListAliases",
                "kms:ListKeys",
                "workspaces:CreateTags",
                "workspaces:CreateWorkspaces",
                "workspaces:CreateWorkspaceImage",
                "workspaces:DeleteTags",
                "workspaces:DescribeTags",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaces",
                "workspaces:DescribeWorkspacesConnectionStatus",
                "workspaces:ModifyCertificateBasedAuthProperties",
                "workspaces:ModifyWorkspaceProperties",
                "workspaces:ModifySamlProperties",
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces",
                "workspaces:RestoreWorkspaces",
                "workspaces:StartWorkspaces",
```

```
                "workspaces:StopWorkspaces",
                "workspaces:TerminateWorkspaces"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS 托管策略：AmazonWorkspacesPCAAccess

此托管策略提供对 AWS 账户中 AWS Certifice Manager Private Certificate Authority (Private CA) 资源的访问权限，以进行基于证书的身份验证。它包含在 AmazonWorkSpacesPCAAccess 角色中，它提供以下权限：

- `acm-pca` - 允许访问 AWS Private CA 以管理基于证书的身份验证。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "acm-pca:IssueCertificate",
        "acm-pca:GetCertificate",
        "acm-pca:DescribeCertificateAuthority"
      ],
      "Resource": "arn:*:acm-pca:*:*:*",
      "Condition": {
        "StringLike": {
          "aws:ResourceTag/euc-private-ca": "*"
        }
      }
    }
  ]
}
```

AWS 托管策略：AmazonWorkSpacesSelfServiceAccess

该策略提供对 Amazon WorkSpaces 服务的访问权限，以执行由用户发起的 WorkSpaces 自助操作。它包含在 `workspaces_DefaultRole` 角色中，它提供以下权限：

- `workspaces` - 允许访问适用于用户的自助服务 WorkSpaces 管理功能。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces",
                "workspaces:ModifyWorkspaceProperties"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS 托管策略：AmazonWorkSpacesServiceAccess

此策略为客户账户提供对 Amazon WorkSpaces 服务的访问权限，以启动 WorkSpace。它包含在 `workspaces_DefaultRole` 角色中，它提供以下权限：

- `ec2` - 允许访问管理与 WorkSpace 关联的 Amazon EC2 资源，例如网络接口。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

WorkSpaces AWS 托管策略更新

查看有关 WorkSpaces 的 AWS 托管策略更新的详细信息（从该服务开始跟踪这些更改开始）。

更改	说明	日期
the section called “AmazonWorkSpacesAdmin” - 更新的策略	WorkSpaces 在 Amazon WorkSpacesAdmin 托管策略中添加了 `workspaces:RestoreWorkspace` 操作，以授予管理员恢复 WorkSpaces 的权限。	2023 年 6 月 25 日
the section called “AmazonWorkspacesPCAAccess” - 添加了新策略	WorkSpaces 添加了一个新的托管策略，以授予管理 AWS Private CA 的 `acm-pca` 权限，从而管理基于证书的身份验证。	2022 年 11 月 18 日
WorkSpaces 已开启跟踪更改	WorkSpaces 开始为其 WorkSpaces 托管策略跟踪更改。	2021 年 3 月 1 日

Amazon WorkSpaces 的合规性验证

作为多项 AWS 合规性计划的一部分，第三方审计员将评估 Amazon WorkSpaces 的安全性和合规性。其中包括 SOC、PCI、FedRAMP、HIPAA 及其它。

有关特定合规性计划范围内的 AWS 服务列表，请参阅合规性计划范围内的 AWS 服务。有关常规信息，请参阅AWS合规性计划。

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

有关 WorkSpaces 和 FedRAMP 文件的更多信息，请参阅设置 Amazon WorkSpaces 以符合 FedRAMP 授权或 DoD SRG 合规性要求。

您使用 WorkSpaces 的合规性责任取决于您数据的敏感度、您公司的合规性目标以及适用的法律法规。AWS 提供以下资源来帮助满足合规性：

- 安全性与合规性 Quick Start 指南 - 这些部署指南讨论了架构注意事项，并提供了在 AWS 上部署基于安全性和合规性的基准环境的步骤。
- Amazon Web Services 上的 HIPAA 安全性和合规性架构设计– 此白皮书介绍了公司如何使用 AWS 创建符合 HIPAA 标准的应用程序。
- AWS合规性资源 – 此业务手册和指南集合可能适用于您的行业和位置。
- 《AWS Config 开发人员指南》中的使用规则评估资源 – AWS Config；评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- AWS Security Hub – 此AWS服务提供了AWS中安全状态的全面视图，可帮助您检查是否符合安全行业标准和最佳实践。

Amazon WorkSpaces 中的故障恢复能力

AWS全球基础设施围绕AWS区域和可用区构建。区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作在可用区之间无中断地自动实现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。

Amazon WorkSpaces 还提供跨区域重定向，该功能可与域名系统 (DNS) 故障转移路由策略配合使用，以便在 WorkSpaces 用户的主 WorkSpaces 不可用时将其重定向到其他 AWS 区域的备用 WorkSpaces。有关更多信息，请参阅Amazon 的跨区域重定向 WorkSpaces。

Amazon WorkSpaces 中的基础设施安全性

作为一项托管式服务，Amazon WorkSpaces 受 AWS 全球网络安全保护。有关 AWS 安全服务以及 AWS 如何保护基础架构的信息，请参阅 AWS 云安全。要按照基础设施安全最佳实践设计您的 AWS 环境，请参阅《安全性支柱 AWS Well-Architected Framework》中的 基础设施保护。

您可以使用 AWS 发布的 API 调用通过网络访问 WorkSpaces。客户端必须支持以下内容：

- 传输层安全性协议（TLS） 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密 (PFS) 的密码套件，例如 DHE（Ephemeral Diffie-Hellman）或 ECDHE（Elliptic Curve Ephemeral Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service (AWS STS) 生成临时安全凭证来对请求进行签名。

网络隔离

Virtual Private Cloud (VPC) 是 AWS 云内您自己的逻辑隔离区域中的虚拟网络。您可以在 VPC 的私有子网中部署您的 WorkSpaces。有关更多信息，请参阅为以下项配置 VPC WorkSpaces。

要仅允许来自特定地址范围（例如，来自您的企业网络）的流量，请更新 VPC 的安全组或使用 IP 访问控制组。

您可以使用有效证书将 WorkSpace 访问限制为受信任的设备。有关更多信息，请参阅限制对可信设备的 WorkSpaces 访问。

物理主机上的隔离

同一物理主机上的不同 WorkSpace 通过管理程序彼此隔离。这就好像它们位于单独的物理主机上。删除 WorkSpace 后，管理程序会在分配给新 WorkSpace 之前清理分配给它的内存（设置为零）。

企业用户授权

借助 WorkSpaces，可通过 AWS Directory Service 管理目录。您可以为用户创建独立的托管目录。或者与现有 Active Directory 环境集成，这样用户就能使用他们当前的凭证无缝访问企业资源。有关更多信息，请参阅管理 WorkSpaces 目录。

要进一步控制对 WorkSpaces 的访问，请使用多重身份验证。有关更多信息，请参阅如何为 AWS 服务启用多重身份验证。

通过 VPC 接口端点发出 Amazon WorkSpaces API 请求

您可以通过虚拟私有云 (VPC) 中的接口端点直接连接到 Amazon WorkSpaces API 端点，而不是通过互联网进行连接。当您使用 VPC 接口端点时，您的 VPC 与 Amazon WorkSpaces API 端点之间的通信完全在 AWS 网络内安全进行。

> **Note**
>
> 此功能仅可用于连接到 WorkSpaces API 端点。要使用 WorkSpaces 客户端连接到 WorkSpaces，需要互联网连接，如 的 IP 地址和端口要求 WorkSpaces中所述。

Amazon WorkSpaces API 端点支持由 AWS PrivateLink 提供支持的 Amazon Virtual Private Cloud (Amazon VPC) 接口端点。每个 VPC 端点都由一个或多个在 VPC 子网中具有私有 IP 地址的网络接口（也称为弹性网络接口或 ENI）表示。

VPC 接口端点将您的 VPC 直接连接到 Amazon WorkSpaces API 端点，而无需互联网网关、NAT 设备、VPN 连接或 AWS Direct Connect 连接。VPC 中的实例不需要公有 IP 地址便可与 Amazon WorkSpaces API 端点进行通信。

您可以创建接口端点以使用 AWS Management Console或 AWS Command Line Interface (AWS CLI) 命令连接到 Amazon WorkSpaces。有关说明，请参阅创建接口端点。

在创建 VPC 端点后，您可以使用以下示例 CLI 命令，这些命令通过 `endpoint-url` 参数指定连接到 Amazon WorkSpaces API 端点的接口端点：

```
aws workspaces copy-workspace-image --endpoint-
url VPC_Endpoint_ID.workspaces.Region.vpce.amazonaws.com

aws workspaces delete-workspace-image --endpoint-
url VPC_Endpoint_ID.api.workspaces.Region.vpce.amazonaws.com

aws workspaces describe-workspace-bundles --endpoint-
url VPC_Endpoint_ID.workspaces.Region.vpce.amazonaws.com  \
   --endpoint-name Endpoint_Name \
   --body "Endpoint_Body" \
   --content-type "Content_Type" \
       Output_File
```

如果为 VPC 端点启用专用 DNS 主机名，您不需要指定端点 URL。CLI 和 Amazon WorkSpaces 开发工具包在默认情况下使用的 Amazon WorkSpaces API DNS 主机名 (https://api.workspaces.*Region*.amazonaws.com) 解析为您的 VPC 端点。

Amazon WorkSpaces API 端点支持同时提供 Amazon VPC 和 Amazon WorkSpaces 的所有 AWS 区域中的 VPC 端点。Amazon WorkSpaces 支持调用您 VPC 中的所有公有 API。

要详细了解 AWS PrivateLink，请参阅 AWS PrivateLink 文档。有关 VPC 端点的价格，请参阅 VPC 定价。要了解有关 VPC 和端点的更多信息，请参阅 Amazon VPC。

要查看按区域划分的 Amazon WorkSpaces API 端点的列表，请参阅 WorkSpaces API 端点。

> **Note**
>
> 联邦信息处理标准 (FIPS) Amazon WorkSpaces API 端点不支持带有 AWS PrivateLink 的 Amazon WorkSpaces API 端点。

为 Amazon WorkSpaces 创建 VPC 端点策略

您可以为 Amazon WorkSpaces 的 Amazon VPC 端点创建一个策略，用于指定以下内容：

- 可执行操作的委托人。
- 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《Amazon VPC 用户指南》中的使用 VPC 端点控制对服务的访问。

> **Note**
>
> 联邦信息处理标准 (FIPS) Amazon WorkSpaces 端点不支持 VPC 端点策略。

以下示例 VPC 端点策略指定有权访问 VPC 接口端点的所有用户都可以调用名为 `ws-f9abcdefg` 的 Amazon WorkSpaces 托管端点。

```
{
     "Statement": [
         {
             "Action": "workspaces:*",
             "Effect": "Allow",
             "Resource": "arn:aws:workspaces:us-west-2:1234567891011:workspace/ws-
f9abcdefg",
             "Principal": "*"
         }
     ]
}
```

在本例中，拒绝以下操作：

- 调用除 `ws-f9abcdefg` 之外的 Amazon WorkSpaces 托管端点。
- 对指定资源以外的任何资源执行操作（WorkSpace ID：`ws-f9abcdefg`）。

> **Note**
>
> 在本例中，用户仍然可以从 VPC 外部调用其他 Amazon WorkSpaces API 操作。要将 API 调用限制为 VPC 内的资源，请参阅 对 WorkSpaces 进行身份和访问管理，以了解有关使用基于身份的策略控制对 Amazon WorkSpaces API 端点的访问的信息。

将您的专用网络连接到 VPC

要通过您的 VPC 调用 Amazon WorkSpaces API，您必须从位于 VPC 中的实例进行连接，或者使用 AWS Virtual Private Network (AWS VPN) 或 AWS Direct Connect 将您的专用网络连接到 VPC。相关信息，请参阅《Amazon虚拟私有云用户指南》中的 VPN 连接。有关 AWS Direct Connect 的信息，请参阅《AWS Direct Connect 用户指南》中的创建连接。

中的更新管理 WorkSpaces

我们建议您定期修补、更新和保护您的操作系统和应用程序 WorkSpaces。您可以将您的配置 WorkSpaces 为在定期维护 WorkSpaces 时段内进行更新，也可以自己进行更新。有关更多信息，请参见 WorkSpace 维护。

对于您的应用程序 WorkSpaces，您可以使用提供的任何自动更新服务，也可以按照应用程序供应商提供的安装更新建议进行操作。

WorkSpaces 问题疑难解答

以下信息可以帮助您解决您的问题 WorkSpaces。

启用高级日志记录

为了帮助解决您的用户可能遇到的问题，您可以在任何 Amazon WorkSpaces 客户端上启用高级登录。

高级日志记录将生成包含诊断信息和调试级别详细信息（包括详细的性能数据）的日志文件。对于 1.0+ 和 2.0+ 的客户端，这些高级日志文件会自动上传到中的数据库。 AWS

> **Note**
>
> 要 AWS 查看高级日志文件并获得有关 WorkSpaces 客户问题的技术支持，请联系 AWS Support。有关更多信息，请参阅 AWS Support 中心。

为 Web Access 启用高级日志记录

为 Web Access 启用高级日志记录

1. 打开您的亚马逊 WorkSpaces 网络访问客户端。
2. 在 WorkSpaces 登录页面的顶部，选择诊断日志。
3. 在弹出对话框中，确保已启用诊断日志记录。
4. 对于日志级别，请选择高级日志记录。

在 Google Chrome、Microsoft Edge 和 Firefox 中访问日志文件

1. 打开浏览器上的上下文（右键单击）菜单或按键盘上的 Ctrl + Shift + I（或者对于 Mac，按 command + option + I），打开开发人员工具面板。
2. 在开发人员工具面板中，选择控制台选项卡以查找日志文件。

在 Safari 中访问日志文件

1. 依次选择 Safari、设置。
2. 在设置窗口中，选择高级选项卡。

3. 在菜单栏中选择“显示开发”菜单。
4. 从菜单栏的开发选项卡中，选择开发 > 显示 Web 检查器。
5. 在 Safari Web 检查器面板中，选择控制台选项卡以查找日志文件。

为 4.0+ 客户端启用高级日志记录

Windows 客户端日志存储在以下位置：

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs
```

为 Windows 客户端启用高级日志记录

1. 关闭亚马逊 WorkSpaces 客户端。
2. 打开命令提示符应用程序。
3. 启动带有`-l3`标志的 WorkSpaces 客户端。

```
c:

cd "C:\Program Files\Amazon Web Services, Inc\Amazon WorkSpaces"

workspaces.exe -l3
```

> **Note**
>
> 如果 WorkSpaces 是为一个用户而不是所有用户安装的，请使用以下命令：
>
> ```
> c:
> cd "%LocalAppData%\Programs\Amazon Web Services, Inc\Amazon
> WorkSpaces"
> workspaces.exe -l3
> ```

macOS 客户端日志存储在以下位置：

```
~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/
logs
```

为 macOS 客户端启用高级日志记录

1. 关闭亚马逊 WorkSpaces 客户端。

2. 打开终端。
3. 运行以下命令。

```
open -a workspaces --args -l3
```

为 Android 客户端启用高级日志记录

1. 关闭亚马逊 WorkSpaces 客户端。
2. 打开 Android 客户端菜单。
3. 选择支持。
4. 选择日志记录设置。
5. 选择启用高级日志记录。

要在启用高级日志记录后检索 Android 客户端的日志，请执行以下操作：

- 选择提取日志，将压缩后的日志保存在本地。

Linux 客户端日志存储在以下位置：

```
~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs
```

为 Linux 客户端启用高级日志记录

1. 关闭亚马逊 WorkSpaces 客户端。
2. 打开终端。
3. 运行以下命令。

```
/opt/workspacesclient/workspacesclient -l3
```

为 3.0 客户端启用高级日志记录

Windows 客户端日志存储在以下位置：

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs
```

为 Windows 客户端启用高级日志记录

1. 关闭亚马逊 WorkSpaces 客户端。

2. 打开命令提示符应用程序。
3. 启动带有-l3标志的 WorkSpaces 客户端。

```
c:

cd "C:\Program Files (x86)\Amazon Web Services, Inc\Amazon WorkSpaces"

workspaces.exe -l3
```

> **Note**
>
> 如果 WorkSpaces 是为一个用户而不是所有用户安装的，请使用以下命令：
>
> ```
> c:
> cd "%LocalAppData%\Programs\Amazon Web Services, Inc\Amazon
> WorkSpaces"
> workspaces.exe -l3
> ```

macOS 客户端日志存储在以下位置：

```
~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/
logs
```

为 macOS 客户端启用高级日志记录

1. 关闭亚马逊 WorkSpaces 客户端。
2. 打开终端。
3. 运行以下命令。

```
open -a workspaces --args -l3
```

为 Android 客户端启用高级日志记录

1. 关闭亚马逊 WorkSpaces 客户端。
2. 打开 Android 客户端菜单。
3. 选择支持。
4. 选择日志记录设置。
5. 选择启用高级日志记录。

要在启用高级日志记录后检索 Android 客户端的日志，请执行以下操作：

- 选择提取日志，将压缩后的日志保存在本地。

Linux 客户端日志存储在以下位置：

```
~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs
```

为 Linux 客户端启用高级日志记录

1. 关闭亚马逊 WorkSpaces 客户端。
2. 打开终端。
3. 运行以下命令。

   ```
   /opt/workspacesclient/workspacesclient -l3
   ```

为 1.0+ 和 2.0+ 客户端启用高级日志记录

1. 打开 WorkSpaces 客户端。
2. 选择客户端应用程序右上角的齿轮图标。
3. 选择 Advanced Settings (高级设置)。
4. 选中 Enable Advanced Logging (启用高级日志记录) 复选框。
5. 选择保存。

Windows 客户端日志存储在以下位置：

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\1.0\Logs
```

macOS 客户端日志存储在以下位置：

```
~/Library/Logs/Amazon Web Services/Amazon WorkSpaces/1.0
```

排查特定问题

以下信息可以帮助您解决与您的特定问题有关的问题 WorkSpaces。

问题

- 我无法创建 Amazon Linux， WorkSpace 因为用户名中有无效字符
- 我为我的 Amazon Linux WorkSpace 换了外壳现在我无法配置 PCoIP 会话
- 我的 Amazon Linux WorkSpaces 无法启动
- WorkSpaces 在我连接的目录中启动经常失败
- 启动 WorkSpaces 失败并出现内部错误
- 当我尝试注册目录时，注册失败并使该目录处于 ERROR 状态
- 我的用户无法使用交互式登录横 WorkSpace 幅连接到 Windows
- 我的用户无法连接到 Windows WorkSpace
- 我的用户在尝试 WorkSpaces 从 WorkSpaces Web Access 登录时遇到了问题
- 在返回登录屏幕之前，Amazon WorkSpaces 客户端会显示灰色的 “正在加载...” 屏幕一段时间。不显示其他错误消息。
- 我的用户收到消息 “WorkSpace 状态：不健康。我们无法将您连接到您的 WorkSpace。请过几分钟再试。”
- 我的用户会收到消息 “此设备无权访问 WorkSpace. 请联系您的管理员寻求帮助。”
- 我的用户在尝试连接到 WSP WorkSpace 时收到消息 “无网络。网络连接中断。请检查网络连接 尝试连接到 WSP 时 WorkSpace
- WorkSpaces 客户端给我的用户带来了网络错误，但他们可以在自己的设备上使用其他支持网络的应用程序
- 我的 WorkSpace 用户看到以下错误消息：“设备无法连接到注册服务。请检查网络设置。”
- 我的 PCoIP 零客户端用户收到错误“提供的证书由于时间戳而无效”
- USB 打印机和其他 USB 外围设备不适用于 PCoIP 零客户端
- 我的用户跳过了更新其 Windows 或 macOS 客户端应用程序的过程，并且没有收到安装最新版本的提示
- 我的用户无法在其 Chromebook 上安装 Android 客户端应用程序
- 我的用户没有收到邀请电子邮件或密码重置电子邮件
- 我的用户在客户端登录屏幕上看不到“忘记密码？”选项
- 当我尝试在 Windows 上安装应用程序时，我收到 “系统管理员已设置策略来阻止此安装” 的消息 WorkSpace
- 我的目录 WorkSpaces 中没有可以连接到互联网
- 我的 WorkSpace 已经失去了互联网接入
- 当我尝试连接我的本地目录时收到一条“DNS unavailable”错误

我无法创建 Amazon Linux， WorkSpace 因为用户名中有无效字符

对于亚马逊 Linux WorkSpaces，用户名：

- 最多可包含 20 个字符
- 可以包含能够以 UTF-8 表示的字母、空格和数字
- 可包含以下特殊字符：_ .-#
- 不能以短划线符号 (-) 作为用户名的开头第一个字符

> **Note**
>
> 这些限制不适用于 Windows WorkSpaces。Windows WorkSpaces 支持对用户名中的所有字符使用 @ 和-符号。

我为我的 Amazon Linux WorkSpace 换了外壳现在我无法配置 PCoIP 会话

要覆盖 Linux 的默认外壳 WorkSpaces，请参见替换亚马逊 Linux 的默认外壳 WorkSpaces。

我的 Amazon Linux WorkSpaces 无法启动

从 2020 年 7 月 20 日起，亚马逊 Linux WorkSpaces 将使用新的许可证书。这些新证书仅与 PCoIP 代理的 2.14.1.1、2.14.7、2.14.9 和 20.10.6 或更高版本兼容。

如果您使用的 PCoIP 代理版本不受支持，则必须将其升级到最新版本 (20.10.6)，该版本包含与新证书兼容的最新修复和性能改进。如果您不在 7 月 20 日之前进行这些升级，则您的 Linux WorkSpaces 会话配置将失败，您的最终用户将无法连接到他们的 WorkSpaces。

将您的 PCoIP 代理升级到最新版本

1. 打开 WorkSpaces 控制台，网址为 https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择你的 Linux WorkSpace，然后选择 “操作”、“重启” 来重启它 WorkSpaces。如果 WorkSpace 状态为`STOPPED`，则必须选择 “操作”、“ WorkSpaces先启动”，然后等到其状态变为`AVAILABLE`后才能重新启动它。
4. WorkSpace 在您重新启动且其状态为`AVAILABLE`，我们建议您在执行此升级`ADMIN_MAINTENANCE`时 WorkSpace 将的状态更改为。完成后，将的状态更改 WorkSpace 为`AVAILABLE`。有关 `ADMIN_MAINTENANCE` 模式的更多信息，请参阅手动维护。

   要将 a 的状态更改 WorkSpace 为`ADMIN_MAINTENANCE`，请执行以下操作：

a. 选择， WorkSpace 然后选择 “操作”、“修改” WorkSpace。
b. 选择 Modify State。
c. 对于预期状态，请选择 ADMIN_MAINTENANCE。
d. 选择 Modify(修改)。

5. WorkSpace 通过 SSH 连接到你的 Linux。有关更多信息，请参阅 为你的 Linux 启用 SSH 连接 WorkSpaces。
6. 要更新 PCoIP 代理，请运行以下命令：

```
sudo yum --enablerepo=pcoip-stable install pcoip-agent-standard-20.10.6
```

7. 要验证代理版本并确认更新成功，请运行以下命令：

```
rpm -q pcoip-agent-standard
```

验证命令应产生以下结果：

```
pcoip-agent-standard-20.10.6-1.el7.x86_64
```

8. 断开与的连接 WorkSpace ，然后重新启动它。
9. 如果您将的状态设置为Step 4，请重复Step 4并将 “预期状态” 设置为AVAILABLE。 WorkSpace ADMIN_MAINTENANCE

如果您的 Linux 在升级 PCoIP 代理后 WorkSpace 仍然无法启动，请联系 Supp AWS ort。

WorkSpaces 在我连接的目录中启动经常失败

验证是否可从您连接到目录时所指定的每个子网访问本地目录中的两个 DNS 服务器或域控制器。您可以通过在每个子网中启动一个 Amazon EC2 实例并将该实例加入您的目录中，然后使用两个 DNS 服务器的 IP 地址来验证此连接。

启动 WorkSpaces 失败并出现内部错误

检查您的子网是否配置为自动将 IPv6 地址分配给在子网中启动的实例。要检查此设置，请打开 Amazon VPC 控制台，选择子网，然后依次选择子网操作、修改自动分配 IP 设置。如果启用此设置，则无法 WorkSpaces 使用 “性能” 或 “显卡” 捆绑包启动。解决办法是，在启动实例时，禁用此设置并手动指定 IPv6 地址。

当我尝试注册目录时，注册失败并使该目录处于 ERROR 状态

如果您尝试注册已配置为用于多区域复制的 AWS 托管 Microsoft AD 目录，则可能会出现此问题。尽管可以成功注册主区域中的目录以供使用 Amazon WorkSpaces，但尝试在复制区域中注册该目录会失败。在复制的区域 WorkSpaces 内，亚马逊不支持使用 AWS 托管 Microsoft AD 进行多区域复制。

我的用户无法使用交互式登录横 WorkSpace 幅连接到 Windows

如果使用交互式登录消息来显示登录横幅，则会阻止用户访问他们的 Windows。 WorkSpacesPC WorkSpaces oIP 目前不支持交互式登录消息组策略设置。将移 WorkSpaces 至未应用Interactive logon: Message text for users attempting to log on组策略的组织单位 (OU)。WSP 支持登录消息 WorkSpaces，用户在接受登录横幅后必须重新登录。

我的用户无法连接到 Windows WorkSpace

我的用户在尝试连接自己的 Windows 时收到以下错误 WorkSpaces：

```
"An error occurred while launching your WorkSpace. Please try again."
```

当 WorkSpace 无法使用 PCoIP 加载 Windows 桌面时，通常会发生此错误。请检查以下事项：

- 如果 Windows 的 PCoIP 标准代理服务未运行，则会显示此消息。使用 RDP 进行连接，以验证服务是否正在运行，是否设置为自动启动，以及是否可以通过管理界面 (eth0) 进行通信。
- 如果卸载了 PCoIP 代理，请通过 Amazon WorkSpaces 控制台重启以自动重新安装。 WorkSpace
- 如果修改WorkSpaces安全组以限制出站流量，则在长时间延迟之后，您也可能会在 Amazon WorkSpaces 客户端上收到此错误。限制出站流量会阻止 Windows 与您的目录控制器通信而导致无法进行登录。确认您的安全组 WorkSpaces 允许您通过主网络接口在所有必需的端口上与目录控制器通信。

此错误的另一个原因与用户权限分配组策略有关。如果以下组策略配置不正确，则会阻止用户访问他们的 Windows WorkSpaces：

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment (计算机配置\Windows 设置\安全设置\本地策略\用户权限分配)

- 不正确的策略：

策略：Access this computer from the network (从网络访问此计算机)

设置：##\域计算机

获胜 GPO：允许文件访问

- 正确的策略：

策略：Access this computer from the network (从网络访问此计算机)

设置：##\域用户

获胜 GPO：允许文件访问

> **Note**
>
> 此策略设置应该应用于 Domain Users (域用户) 而不是 Domain Computers (域计算机)。

有关更多信息，请参阅 Microsoft Windows 文档中的从网络访问此计算机 - 安全策略设置和配置安全策略设置。

我的用户在尝试 WorkSpaces 从 WorkSpaces Web Access 登录时遇到了问题

Amazon WorkSpaces 依靠特定的登录屏幕配置来使用户能够成功地从 Web Access 客户端登录。

要使 Web Access 用户能够登录他们的 WorkSpaces，必须配置一个组策略设置和三个安全策略设置。如果这些设置配置不正确，则用户在尝试登录时可能会遇到登录时间过长或黑屏的情况 WorkSpaces。要配置这些设置，请参阅 启用和配置 Amazon WorkSpaces Web Access。

> **Important**
>
> 从 2020 年 10 月 1 日起，客户将无法再使用亚马逊 WorkSpaces Web Access 客户端连接到 Windows 7 自定义版 WorkSpaces 或 Windows 7 自带许可证 (BYOL) WorkSpaces。

在返回登录屏幕之前，Amazon WorkSpaces 客户端会显示灰色的 “正在加载...” 屏幕一段时间。不显示其他错误消息。

此行为通常表示 WorkSpaces 客户端可以通过端口 443 进行身份验证，但无法通过端口 4172 (PCoIP) 或端口 4195 (WSP) 建立流媒体连接。当未满足网络先决条件时，可能会发生此情况。客户端的问题通常导致客户端的网络检查失败。要查看哪些运行状况检查失败，请选择网络检查图标（通常是 2.0+ 客户端登录屏幕右下角带有感叹号的红色三角形，或 3.0+ 客户端右上角的网络图标 ）。

> **Note**
>
> 此问题的最常见原因是客户端防火墙或代理阻止通过端口 4172 或 4195（TCP 和 UDP）进行访问。如果此运行状况检查失败，请检查您的本地防火墙设置。

如果网络检查通过，则的网络配置可能存在问题 WorkSpace。例如，Windows 防火墙规则可能会阻止管理界面上的端口 UDP 4172 或 4195。 WorkSpace 使用远程桌面协议 (RDP) 客户端连接到，以验证是否 WorkSpace 满足必要的端口要求。

我的用户收到消息 “WorkSpace 状态：不健康。我们无法将您连接到您的 WorkSpace。请过几分钟再试。”

此错误通常表示 SkyLightWorkSpacesConfigService 服务未响应运行状况检查。

如果您刚刚重新启动或启动 WorkSpace，请等待几分钟，然后重试。

如果 WorkSpace 已经运行了一段时间，但您仍然看到此错误，请使用 RDP 进行连接以验证该 SkyLightWorkSpacesConfigService 服务：

- 正在运行。
- 设置为自动启动。
- 可以通过管理界面 (eth0) 进行通信。
- 未被任何第三方防病毒软件阻止。

我的用户会收到消息 “此设备无权访问 WorkSpace. 请联系您的管理员寻求帮助。”

此错误表示已在 WorkSpace 目录上配置了 IP 访问控制组，但客户端 IP 地址未列入许可名单。

检查您的目录上的设置。确认用户连接的公有 IP 地址允许访问 WorkSpace。

我的用户在尝试连接到 WSP WorkSpace 时收到消息 “无网络。网络连接中断。请检查网络连接 尝试连接到 WSP 时 WorkSpace

如果出现此错误并且您的用户没有连接问题，请确保网络防火墙上已打开端口 4195。为了 WorkSpaces 使用 WorkSpaces 流式传输协议 (WSP)，用于流式传输客户端会话的端口已从 4172 更改为 4195。

WorkSpaces 客户端给我的用户带来了网络错误，但他们可以在自己的设备上使用其他支持网络的应用程序

WorkSpaces 客户端应用程序依赖于对 AWS云端资源的访问，并且需要至少提供 1 Mbps 下载带宽的连接。如果设备间歇性地连接到网络，则 WorkSpaces 客户端应用程序可能会报告网络问题。

WorkSpaces 自 2018 年 5 月起，强制使用亚马逊信任服务颁发的数字证书。在支持的操作系统上，Amazon Trust Services 已经是值得信赖的根 CA WorkSpaces。如果操作系统的根 CA 列表不是最新的，则设备无法连接， WorkSpaces 并且客户端会出现网络错误。

识别由于证书失败造成的连接问题

- PCoIP 零客户端 - 将显示以下错误消息。

```
Failed to connect. The server provided a certificate that is invalid. See below for
 details:
- The supplied certificate is invalid due to timestamp
- The supplied certificate is not rooted in the devices local certificate store
```

- 其他客户端 - 运行状况检查失败，出现互联网红色警告三角形。

解决证书问题

- Windows 客户端应用程序
- PCoIP 零客户端
- 其他客户端应用程序

Windows 客户端应用程序

使用以下解决方案之一处理证书问题。

解决方案 1：更新客户端应用程序

https://clients.amazonworkspaces.awsapps.cn/ 在安装过程中，客户端应用程序确保由 Amazon Trust Services 发布了您的操作系统信任证书。

解决方案 2：将 Amazon Trust Services 添加到本地根 CA 列表

1. 打开 https://www.amazontrust.com/repository/。
2. 下载 DER 格式的 Starfield 证书 (2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92)。
3. 打开 Microsoft 管理控制台。（从命令提示符中，运行 mmc。）
4. 依次选择文件、添加/删除管理单元、证书和添加。
5. 在证书管理单元页面上，选择计算机账户，然后选择下一步。保留默认值本地计算机。选择结束。选择 确定。
6. 展开证书 (本地计算机)，然后选择受信任的根证书颁发机构。依次选择操作、所有任务和导入。
7. 按照向导的说明，导入下载的证书。
8. 退出并重新启动 WorkSpaces 客户端应用程序。

解决方案 3：使用组策略部署 Amazon Trust Services 作为可信 CA

对于使用组策略的域，将 Starfield 证书添加到信任根 CA。有关更多信息，请参阅使用策略来分配证书。

PCoIP 零客户端

要直接连接 WorkSpace 使用固件版本 6.0 或更高版本，请下载并安装亚马逊信任服务颁发的证书。

添加 Amazon Trust Services 作为可信根 CA

1. 打开 https://certs.secureserver.net/repository/。
2. 在 Starfield Certificate Chain (Starfield 证书链) 中下载具有指纹 14 65 FA 20 53 97 B8 76 FA A6 F0 A9 95 8E 55 90 E4 0F CC 7F AA 4F B7 C2 C8 67 75 21 FB 5F B6 58 的证书。
3. 上传证书至 zero 客户端。有关更多信息，请参阅 Teradici 文档中的上传证书。

其他客户端应用程序

从 Amazon Trust Services 添加 Starfield 证书 (2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92)。有关如何添加根 CA 的更多信息，请参阅以下文档：

- Android：添加和删除证书
- Chrome OS：管理 Chrome 设备上的客户端证书
- macOS 和 iOS：在测试设备上安装 CA 根证书

我的 WorkSpace 用户看到以下错误消息："设备无法连接到注册服务。请检查网络设置。"

当注册服务出现故障时，您的 WorkSpace 用户可能会在 Connection Healt h Check 页面上看到以下错误消息："您的设备无法连接到 WorkSpaces 注册服务。您将无法使用注册您的设备 WorkSpaces。请检查网络设置。"

当 WorkSpaces 客户端应用程序无法访问注册服务时，就会发生此错误。通常，当 WorkSpaces 目录被删除时，就会发生这种情况。要解决此错误，请确保注册码有效且与 AWS 云端的运行目录相对应。

我的 PCoIP 零客户端用户收到错误"提供的证书由于时间戳而无效"

如果在 Teradici 中未启用网络时间协议 (NTP)，则 PCoIP 零客户端用户可能会收到证书失败错误。要设置 NTP，请参阅为 WorkSpaces 设置 PCoIP 零客户端。

USB 打印机和其他 USB 外围设备不适用于 PCoIP 零客户端

从 PCoIP 代理的 20.10.4 版本开始，亚马逊默认 WorkSpaces 禁用通过 Windows 注册表进行的 USB 重定向。当您的用户使用 PCoIP 零客户端设备连接到 USB 外围设备时，此注册表设置会影响 USB 外围设备的行为。 WorkSpaces

WorkSpaces 如果您使用的是 20.10.4 或更高版本的 PCoIP 代理，则在启用 USB 重定向之前，USB 外围设备将无法与 PCoIP 零客户端设备配合使用。

> **Note**
>
> 如果您使用的是 32 位虚拟打印机驱动程序，则还必须将这些驱动程序更新到 64 位版本。

为 PCoIP 零客户端设备启用 USB 重定向

我们建议您 WorkSpaces 通过组策略将这些注册表更改推送到您的注册表中。有关更多信息，请参阅 Teradici 文档中的配置代理和可配置的设置。

1. 将以下注册表项值设置为 1（已启用）：

   KeyPath = HKEY_LOCAL_MACHINE\ SOFTWARE\ Policies\ Teradici\ pcoip\ pcoip _admin

   KeyName = pcoip.enable_usb

   KeyType = DWORD

   KeyValue = 1
2. 将以下注册表项值设置为 1（已启用）：

   KeyPath = HKEY_LOCAL_MACHINE\ SOFTWARE\ Policies\ Teradici\ pcoip_admin_defaults\ p

   KeyName = pcoip.enable_usb

   KeyType = DWORD

   KeyValue = 1
3. 如果您尚未这样做，请注销 WorkSpace，然后重新登录。您的 USB 设备现在应该可以运行了。

我的用户跳过了更新其 Windows 或 macOS 客户端应用程序的过程，并且没有收到安装最新版本的提示

当用户跳过对 Amazon WorkSpaces Windows 客户端应用程序的更新时，会设置SkipThis版本注册表项，并且在新版本的客户端发布时不再提示他们更新客户端。要更新到最新版本，您可以按照《亚马逊 WorkSpaces 用户指南》中将 WorkSpaces Windows 客户端应用程序更新到新版本中所述编辑注册表。您也可以运行以下 PowerShell 命令：

```
Remove-ItemProperty -Path "HKCU:\Software\Amazon Web Services. LLC\Amazon WorkSpaces
\WinSparkle" -Name "SkipThisVersion"
```

当用户跳过对 Amazon WorkSpaces macOS 客户端应用程序的更新时，会设置`SUSkippedVersion`首选项，并且在新版本的客户端发布时不再提示他们更新客户端。要更新到最

新版本，您可以按照《亚马逊 WorkSpaces 用户指南》中将 WorkSpaces macOS 客户端应用程序更新到新版本中所述重置此首选项。

我的用户无法在其 Chromebook 上安装 Android 客户端应用程序

版本 2.4.13 是亚马逊 WorkSpaces Chromebook 客户端应用程序的最终版本。由于谷歌正在逐步停止对Chrome应用程序的支持，因此Chro WorkSpaces mebook客户端应用程序将不会有进一步的更新，也不支持其使用。

对于支持安装安卓应用程序的 Chromeb ook，我们建议改用 WorkSpaces 安卓客户端应用程序。

在某些情况下，您可能需要启用用户的 Chromebook 以安装 Android 应用程序。有关更多信息，请参阅 为 Chromebook 设置 Android。

我的用户没有收到邀请电子邮件或密码重置电子邮件

用户不会自动收到使用 AD Connector WorkSpaces 或可信域创建的欢迎电子邮件或密码重置电子邮件。如果用户已经位于 Active Directory 中，系统也不会自动发送邀请电子邮件。

要手动向这些用户发送欢迎电子邮件，请参阅 发送邀请电子邮件。

要重置用户密码，请参阅为 WorkSpaces 设置 Active Directory 管理工具。

我的用户在客户端登录屏幕上看不到“忘记密码？”选项

如果您使用的是 AD Connector 或受信任域，则您的用户将无法重置自己的密码。（忘记密码？WorkSpaces 客户端应用程序登录屏幕上的选项将不可用。）有关如何重置用户密码的信息，请参阅为 WorkSpaces 设置 Active Directory 管理工具。

当我尝试在 Windows 上安装应用程序时，我收到 “系统管理员已设置策略来阻止此安装” 的消息 WorkSpace

您可以通过修改 Windows 安装程序组策略设置来解决此问题。要将此策略部署到目录 WorkSpaces 中的多个，请将此设置应用于从已加入域的 EC2 实例链接到 WorkSpaces 组织单位 (OU) 的组策略对象。如果您使用 AD Connector，则可以从域控制器进行这些更改。有关使用 Active Directory 管理工具处理组策略对象的更多信息，请参阅《AWS Directory Service 管理指南》中的安装 Active Directory 管理工具。

以下过程说明如何为 WorkSpaces 组策略对象配置 Windows Installer 设置。

1. 确保您的域中安装了最新的WorkSpaces 组策略管理模板。

2. 在 Windows WorkSpace 客户端上打开组策略管理工具，导航到 WorkSpaces 计算机帐户的 WorkSpaces 组策略对象并将其选中。从主菜单中，依次选择 Action (操作) 和 Edit (编辑)。
3. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、经典管理模板、Windows 组件、Windows 安装程序。
4. 打开 Turn Off Windows Installer (关闭 Windows 安装程序) 设置。
5. 在 Turn Off Windows Installer (关闭 Windows 安装程序) 对话框中，将 Not Configured (未配置) 更改为 Enabled (已启用)，然后将 Disable Windows Installer (禁用 Windows 安装程序) 设置为 Never (从不)。
6. 选择 确定。
7. 要应用组策略更改，请执行下列操作之一：
   - 重新启动 WorkSpace （ 在 WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重新启动 WorkSpaces ）。
   - 从管理命令提示符下，输入 gpupdate /force。

我的目录 WorkSpaces 中没有可以连接到互联网

WorkSpaces 默认情况下无法与互联网通信。您必须显式提供互联网访问。有关更多信息，请参阅 提供您的 Internet 访问权限 WorkSpace。

我的 WorkSpace 已经失去了互联网接入

如果您无法访问互联网，并且无法使用 RDP 连接到互联网，则此问题可能是由于的公有 IP 地址丢失所致。 WorkSpace WorkSpace WorkSpace如果您在目录级别启用了弹性 IP 地址的自动分配，则会在启动弹性 IP 地址（来自亚马逊提供的地址池） WorkSpace 时分配给您。但是，如果您将自己拥有的弹性 IP 地址关联到 WorkSpace，然后又将该弹性 IP 地址与解除关联 WorkSpace，则该弹性 IP 地址将 WorkSpace 丢失其公有 IP 地址，并且不会自动从亚马逊提供的池中获取新的 IP 地址。

要将亚马逊提供的资源池中的新公有 IP 地址与相关联 WorkSpace，您必须重新构建。 WorkSpace如果您不想重建 WorkSpace，则必须将您拥有的另一个弹性 IP 地址与关联起来 WorkSpace。

我们建议您不要在启动 WorkSpace后修改的 elastic network 接口。 WorkSpace 将弹性 IP 地址分配给后 WorkSpace， WorkSpace 会保留相同的公有 IP 地址（除非重建，在这种情况下，它将获得新的公有 IP 地址）。 WorkSpace

当我尝试连接我的本地目录时收到一条“DNS unavailable”错误

在连接您的本地目录时，您收到类似于以下内容的错误消息。

```
DNS unavailable (TCP port 53) for IP: dns-ip-address
```

AD Connector 必须能够通过 TCP 和 UDP 经由端口 53 与您的本地 DNS 服务器通信。验证您的安全组和本地防火墙是否允许经由此端口进行 TCP 和 UDP 通信。

在尝试连接到我的本地目录时，我收到一条“Connectivity issues detected”错误

在连接您的本地目录时，您收到类似于以下内容的错误消息。

```
Connectivity issues detected: LDAP unavailable (TCP port 389) for IP: ip-address
Kerberos/authentication unavailable (TCP port 88) for IP: ip-address
Please ensure that the listed ports are available and retry the operation.
```

AD Connector 必须能够通过 TCP 和 UDP 经由以下端口与您的本地域控制器通信。验证您的安全组和本地防火墙是否允许经由这些端口进行 TCP 和 UDP 通信：

- 88 (Kerberos)
- 389 (LDAP)

在尝试连接到我的本地目录时，我收到一条“SRV record”错误

在连接您的本地目录时，您收到类似于以下一项或多项内容的错误消息。

```
SRV record for LDAP does not exist for IP: dns-ip-address

SRV record for Kerberos does not exist for IP: dns-ip-address
```

在连接您的目录时，AD Connector 需要获取 `_ldap._tcp.`*dns-domain-name* 和 `_kerberos._tcp.`*dns-domain-name* SRV 记录。如果服务无法从您在连接到目录时所指定的 DNS 服务器上获取这些记录，则您会收到此错误。请确保您的 DNS 服务器包含这些 SRV 记录。有关更多信息，请参阅 Microsoft TechNet 上的 SRV 资源记录。

我的 Windows 闲置时会 WorkSpace 进入睡眠状态

要解决此问题，请使用以下步骤连接到 WorkSpace 并将电源计划更改为“高性能”：

1. 从中 WorkSpace打开“控制面板”，然后选择“硬件”或“硬件和声音”（名称可能会有所不同，具体取决于你的 Windows 版本）。

2. 在 Power Options (电源选项) 下，选择 Choose a power plan (选择电源计划)。
3. 在选择或自定义电源计划窗格中，选择高性能电源计划，然后选择更改计划设置。
   - 如果高性能电源计划选项被禁用，请选择更改当前不可用的设置，然后选择高性能电源计划。
   - 如果看不到高性能计划，请选择显示其他计划右侧的箭头以显示它，或者在左侧导航栏中选择创建电源计划，选择高性能，为电源计划命名，然后选择下一步。
4. 在更改计划的设置: 高性能页面上，确保将关闭显示屏和（如果可用）将计算机置于睡眠状态设置为从不。
5. 如果您对高性能计划进行了任何更改，请选择保存更改（或选择创建，如果要创建新计划的话）。

如果上述步骤无法解决该问题，请执行以下操作：

1. 从中 WorkSpace打开 “控制面板”，然后选择 “硬件” 或 “硬件和声音”（名称可能会有所不同，具体取决于你的 Windows 版本）。
2. 在 Power Options (电源选项) 下，选择 Choose a power plan (选择电源计划)。
3. 在 Choose or customize a power plan (选择或自定义电源计划) 窗格中，选择 High performance (高性能) 电源计划右侧的 Change plan settings (更改计划设置) 链接，然后选择 Change advanced power settings (更改高级电源设置) 链接。
4. 在 Power Options (高级选项) 对话框中的设置列表中，选择 Hard disk (硬盘) 左侧的加号以显示相关设置。
5. 验证 Plugged in (已插入) 的 Turn off hard disk after (在多长时间后关闭硬盘) 值是否大于 On battery (使用电池) 的值（默认值为 20 分钟）。
6. 选择 PCI Express 左侧的加号，然后为 Link State Power Management (链路状态电源管理) 执行相同的操作。
7. 验证 Link State Power Management (链路状态电源管理) 设置是否为 Off (关闭)。
8. 选择 OK (确定)（如果您更改了任何设置，则选择 Apply (应用)）以关闭对话框。
9. 在 Change settings for the plan (更改计划的设置) 窗格中，如果您更改了任何设置，请选择 Save changes (保存更改)。

我的其中 WorkSpaces 一个状态为 **UNHEALTHY**

该 WorkSpaces 服务会定期向 a 发送状态请求 WorkSpace。A WorkSpace 在无法响应这些请求UNHEALTHY时会被标记。导致此问题的常见原因包括：

- 上的应用程序 WorkSpace 正在阻塞网络端口，这使无法响应状态请求。 WorkSpace

- CPU 使用率过高导致无法及时响应状态请求。 WorkSpace
- 的计算机名称 WorkSpace 已更改。这可以防止在 WorkSpaces 和之间建立安全通道 WorkSpace。

您可以尝试使用以下方法来纠正这种状况：

- WorkSpace 从 WorkSpaces 控制台重新启动。
- WorkSpace 使用以下步骤连接到运行状况不佳的服务器，该步骤应仅用于故障排除：

  1. Connect 连接到与运行状况不佳 WorkSpace者位于同一目录 WorkSpace 中的操作服务器。
  2. 从操作开始 WorkSpace，使用远程桌面协议 (RDP)， WorkSpace 使用不健康用户的 IP 地址连接到运行状况不佳的服务器。 WorkSpace根据问题的严重程度，您可能无法连接到不健康的服务器 WorkSpace。
  3. 如果运行状况不 WorkSpace佳，请确认满足最低端口要求。

- 确保 SkyLightWorkSpacesConfigService 服务可以响应运行状况检查。要排查此问题，请参阅我的用户收到消息 “WorkSpace 状态：不健康。我们无法将您连接到您的 WorkSpace。请过几分钟再试。”。
- WorkSpace 从 WorkSpaces 控制台重建。由于重建 WorkSpace 可能会导致数据丢失，因此只有在所有其他更正问题的尝试均未成功的情况下，才应使用此选项。

我的 WorkSpace 意外崩溃或重启

如果您的 PCoIP WorkSpace 配置反复崩溃或重新启动，并且错误日志或崩溃转储指向`spacedeskHookKmode.sys`或有问题`spacedeskHookUmode.dll`，或者如果您收到以下错误消息，则可能需要禁用 Web 访问权限： WorkSpace

```
The kernel power manager has initiated a shutdown transition.
Shutdown reason: Kernel API
```

```
The computer has rebooted from a bugcheck.
```

> **Note**
>
> - 这些故障排除步骤不适用于为 WorkSpaces WorkSpaces 流协议 (WSP) 配置的步骤。它们仅适用于为 WorkSpaces PCoIP 配置的。

- 仅当您不允许用户使用 Web 访问时，才应禁用 Web 访问。

要禁用对的 Web 访问 WorkSpace，必须禁用 WorkSpaces 目录中的 Web 访问并重新启动 WorkSpace。

同一个用户名有多个用户名 WorkSpace，但用户只能登录其中一个 WorkSpaces

如果您在 Active Directory (AD) 中删除用户而不先将其删除， WorkSpace 然后将该用户添加回 Active Directory WorkSpace 并为该用户创建一个新用户，那么同一个用户名现在将在同一个目录 WorkSpaces 中包含两个用户名。但是，如果用户尝试连接到其原始设备 WorkSpace，他们将收到以下错误：

```
"Unrecognized user. No WorkSpace found under your username. Contact your administrator
 to request one."
```

此外，在 Amazon WorkSpaces 控制台中搜索用户名时只会返回新的用户名 WorkSpace，尽管两者 WorkSpaces 仍然存在。（您可以 WorkSpace 通过搜索 WorkSpace ID 而不是用户名来找到原件。）

如果您在 Active Directory 中重命名用户而不先将其删除，也会发生这种情况 WorkSpace。如果您随后将他们的用户名改回原来的用户名 WorkSpace 并为该用户创建一个新的用户名，则同一个用户名将在目录 WorkSpaces 中包含两个用户名。

出现此问题的原因是 Active Directory 使用用户的安全标识符 (SID)（而不是用户名）以唯一标识用户。当删除某个用户并在 Active Directory 中重新创建此用户时，即使用户的用户名保持不变，也会为该用户分配一个新的 SID。在搜索用户名的过程中，Amazon WorkSpaces 控制台使用 SID 在 Active Directory 中搜索匹配项。当用户连接时，Amazon WorkSpaces 客户端还使用 SID 来识别用户 WorkSpaces。

要解决此问题，请执行下列操作之一：

- 如果由于在 Active Directory 中删除了用户并在其中重新创建了该用户而发生了此问题，并且在 Active Directory 中启用了回收站功能，则您可能能够还原原始的已删除的用户对象。如果您能够恢复原始用户对象，请确保该用户可以连接到其原始对象 WorkSpace。如果可以，您可以在手动备份并将任何用户数据从新数据传输 WorkSpace 到原始数据 WorkSpace（如果需要）WorkSpace后删除新数据。

- 如果您无法恢复原始用户对象，请删除该用户的原始对象 WorkSpace。用户应该能够连接并使用他们的新 WorkSpace 版本。请务必手动备份所有用户数据，并将所有用户数据从原始数据传输 WorkSpace 到新数据 WorkSpace。

> **Warning**
>
> 删除 WorkSpace 是一项永久性操作，无法撤消。 WorkSpace 用户的数据不会保留，因此会被销毁。要获取有关备份用户数据的帮助，请联系 AWS Support。

我在亚马逊上使用 Docker 时遇到了问题 WorkSpaces

窗户 WorkSpaces

Windows WorkSpaces 不支持嵌套虚拟化（包括使用 Docker）。有关更多信息，请参阅 Docker 文档。

Linu WorkSpaces

要在 Linux 上使用 Docker WorkSpaces，请确保 Docker 使用的 CIDR 块不与与之关联的两个弹性网络接口 (ENI) 中使用的 CIDR 块重叠。 WorkSpace如果你在 Linux 上使用 Docker 时遇到问题 WorkSpaces，请联系 Docker 寻求帮助。

我的一些 API 调用收到了 ThrottlingException 错误

WorkSpaces API 调用的默认允许速率为每秒两次 API 调用的恒定速率，允许的最大 “突发” 速率为每秒五次 API 调用。下表显示了适用于 API 请求的突发速率限制。

秒	发送的请求数	允许的 Net 请求数	详细信息
1	0	5	第一秒（第 1 秒）内允许发出五个请求，最高突发速率为每秒五次调用。
2	2	5	由于在第 1 秒中发出的调用未超过两次，所以五次调用的完整突发容量仍然可用。
3	5	5	由于在第 2 秒中发出的调用只有两次，所以五次调用的完整突发容量仍然可用。

秒	发送的请求数	允许的 Net 请求数	详细信息
4	2	2	因为在第 3 秒中使用了完整突发容量，所以只有每秒两次调用这一恒定速率可用。
5	3	2	由于没有剩余的突发容量，此时仅允许进行两次调用。这意味着剩余三次 API 调用的其中一次会受到限制。在短暂的延迟后，受到限制的调用将发出响应。
6	0	1	由于第 5 秒中的某次调用在第 6 秒中进行了重试，因此，根据每秒两次调用的恒定速率限制，第 6 秒中仅剩余一次额外调用的容量。
7	0	3	现在，队列中不再有任何受限制的 API 调用，速率限制继续增加，直至达到五次调用的突发速率限制。
8	0	5	由于在第 7 秒内没有发出调用，因此允许发送最大数量的请求。
9	0	5	即使在第 8 秒没有发出任何调用，速率限制也不会增加到五次以上。

当我 WorkSpace 让它在后台运行时，我的连接一直处于断开状态

对于 Mac 用户，请查看 Power Nap 功能是否已开启。如果它处于开启状态，请将其关闭。要关闭 Power Nap，请打开终端并运行以下命令：

```
defaults write com.amazon.workspaces NSAppSleepDisabled -bool YES
```

SAML 2.0 联合身份验证不起作用。我的用户无权直播其 WorkSpaces 桌面。

出现此问题的原因可能是为 SAML 2.0 联合身份验证 IAM 角色嵌入的内联策略不包含从目录 Amazon 资源名称 (ARN) 进行流式传输的权限。IAM 角色由正在访问 WorkSpaces 目录的联合用户担任。编辑角色权限以包含目录 ARN，并确保用户在目录 WorkSpace 中有。有关更多信息，请参阅 SAML 2.0 身份验证和使用 S AML 2.0 联合进行故障排除。 AWS

我的用户每 60 分钟就会断开一次 WorkSpaces 会话连接。

如果您已将 SAML 2.0 身份验证配置为 WorkSpaces，则可能需要配置 IdP 在身份验证响应中作为 SAML 属性 AWS 传递的信息，具体取决于您的身份提供商 (IdP)。这包括配置 Attribute (属性) 元素，并将 SessionDuration 属性设置为 https://aws.amazon.com/SAML/Attributes/SessionDuration。

SessionDuration 指定用户的联合流会话在需要重新进行身份验证之前可保持活动状态的最长时间。虽然 SessionDuration 是可选属性，但建议您将它包含在 SAML 身份验证响应中。如果您未指定此属性，则会话持续时间将默认为 60 分钟。

要解决此问题，请配置 IdP 以在 SAML 身份验证响应中包含 SessionDuration 值，并根据需要设置该值。有关更多信息，请参阅步骤 5：为 SAML 身份验证响应创建断言。

我的用户在使用 SAML 2.0 身份提供商 (IdP) 启动的流程进行联合时会收到重定向 URI 错误，或者我的用户在联合到 IdP 后每次尝试从 WorkSpaces 客户端登录时，都会启动客户端应用程序的另一个实例。

出现此错误的原因是中继状态 URL 无效。确保您的 IdP 联合设置中的中继状态正确，并且在目录属性中为 IdP 联合身份验证正确配置了用户访问 URL 和中继状态参数名称。 WorkSpaces 如果它们有效但问题仍然存在，请联系 Su AWS pport。有关更多信息，请参阅设置 SAML。

我的用户在联合到 IdP 后尝试登录 WorkSpaces 客户端应用程序时，他们会收到一条消息：“出了点问题：启动你的应用程序时出错 WorkSpace”。

查看适用于联合身份验证的 SAML 2.0 断言。SAML 主题名称标识值必须与用户名匹配 WorkSpaces ，并且通常与 Active Director y 用户的 AccountName saM 属性相同。此外，属性设置为的PrincipalTag:Email属性元素https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email必须与 WorkSpaces 目录中定义的 WorkSpaces 用户的电子邮件地址相匹配。有关更多信息，请参阅设置 SAML。

我的用户在联合到 IdP 后尝试登录 WorkSpaces 客户端应用程序时会收到“无法验证标签” 的消息。

查看联合身份验证的 SAML 2.0 断言中的 PrincipalTag 属性值，例如 https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email。标签值可能包括字符 _ . : / = + - @、字母、数字和空格的组合。有关更多信息，请参阅 IAM 中的标签规则和。 AWS STS

我的用户会收到消息“客户端和服务器无法通信，因为它们没有共同的算法”。

如果您未启用 TLS 1.2，则可能会出现此问题。

我的麦克风或网络摄像头无法在 Windows 上运行 WorkSpaces。

打开“开始”菜单，查看您的隐私设置

- 开始 > 设置 > 隐私 > 相机
- 开始 > 设置 > 隐私 > 麦克风

如果它们已关闭，请将其打开。

或者， WorkSpaces 管理员可以根据需要创建组策略对象 (GPO) 来启用麦克风和/或网络摄像头。

我的用户无法使用基于证书的身份验证登录，当他们连接到桌面会话时，系统会在 WorkSpaces 客户端或 Windows 登录屏幕上提示他们输入密码。

会话基于证书的身份验证失败。如果问题仍然存在，则基于证书的身份验证失败可能是由以下问题之一导致的：

- 不支持 WorkSpaces 或客户端。使用最新 WorkSpaces 的 Windows 客户端应用程序的 Windows WorkSpaces WorkSpaces 流媒体协议 (WSP) 捆绑包支持基于证书的身份验证。
- 在 WorkSpaces 目录上启用基于证书的身份验证后，需要重新启动。 WorkSpaces
- WorkSpaces 无法与 AWS Private CA证书通信或 AWS Private CA 未颁发证书。检查 AWS CloudTrail 以确定是否已颁发证书。有关更多信息，请参阅 管理基于证书的身份验证。
- 域控制器没有用于智能卡登录的域控制器证书，或者该证书已过期。有关更多信息，请参阅先决条件中的步骤 7，“使用域控制器证书配置域控制器以对智能卡用户进行身份验证”。
- 该证书不可信。有关更多信息，请参阅先决条件中的步骤 7，“将 CA 发布到 Active Directory”。`certutil -viewstore -enterprise NTAuth`在域控制器上运行以确认 CA 已发布。
- 缓存中有一个证书，但是该用户的属性已更改，从而使该证书失效。在证书 AWS Support 到期（24 小时）之前，请联系以清除缓存。有关更多信息，请参阅 AWS Support 中心。
- `UserPrincipalNameSAML` 属性的格式格式不正确或无法解析为用户的实际域。userPrincipalName 有关更多信息，请参阅先决条件中的步骤 1。

- 您的 SAML 断言中的（可选）`ObjectSid` 属性与 SAML_Subject `NameID` 中指定的用户的 Active Directory 安全标识符 (SID) 不匹配。确认您的 SAML 联合身份验证中的属性映射是正确的，并且您的 SAML 身份提供者正在同步 Active Directory 用户的 SID 属性。
- 有些组策略设置会修改智能卡登录的默认 Active Directory 设置，或者在从智能卡读卡器中移除智能卡时执行操作。除了上面列出的错误之外，这些设置还可能会导致其他意外行为。基于证书的身份验证向实例操作系统提供虚拟智能卡，并在登录完成后将其删除。检查智能卡的主组策略设置以及其他智能卡组策略设置和注册表项，包括智能卡删除行为。
- 私有 CA 的 CRL 分发点不在线，也无法从 WorkSpaces 或域控制器访问。有关更多信息，请参阅先决条件中的步骤 5。
- 要检查域或林中是否存在过时的 CA，请在 CA `PKIVIEW.msc` 上运行以进行验证。如果存在陈旧的 CA，请使用 `PKIVIEW.msc` mmc 手动将其删除。
- 要检查 Active Directory 复制是否正常工作以及域中是否没有陈旧的域控制器，请运行`repadmin /replsum`。

其他故障排除步骤包括查看 WorkSpaces 实例 Windows 事件日志。要检查登录失败的常见事件是 Windows 安全日志中的事件 4625：登录账户失败。

如果问题仍然存在，请与联系 AWS Support。有关更多信息，请参阅 AWS Support 中心。

我正在尝试做一些需要 Windows 安装介质但 WorkSpaces 不提供安装介质的事情。

如果您使用的是 AWS提供的公共捆绑包，则可以在需要时使用 Amazon EC2 提供的 Windows 服务器操作系统安装媒体 EBS 快照。

根据这些快照创建 EBS 卷，将其附加到 Amazon EC2，然后根据需要将文件传输到文件 WorkSpace 所在的位置。如果你在 BYOL 上使用 Windows 10 WorkSpaces 并且需要安装媒体，则需要准备自己的安装媒体。有关更多信息，请参阅使用安装介质添加 Windows 组件。由于您无法将 EBS 卷直接连接到 WorkSpace，因此您需要将其连接到 Amazon EC2 实例并复制文件。

我想 WorkSpaces 使用在不支持的 WorkSpaces 地区创建的现有 AWS 托管目录启动。

要 WorkSpaces 使用当前不支持的地区的目录启动 Amazon WorkSpaces，请按照以下步骤操作。

> **Note**
>
> 如果您在运行 AWS Command Line Interface 命令时收到错误，请确保您使用的是最新 AWS CLI 版本。有关更多信息，请参阅确认您运行的是最新版 AWS CLI。

步骤 1：创建与您账户中另一个 VPC 的虚拟私有云 (VPC) 对等连接

1. 创建与不同区域内的 VPC 之间的 VPC 对等连接。有关更多信息，请参阅在同一账户和不同区域中使用 VPC 创建。
2. 接受 VPC 对等连接。有关更多信息，请参阅接受 VPC 对等连接。
3. 激活 VPC 对等连接后，您可以使用 Amazon VPC 控制台 AWS CLI、或 API 查看您的 VPC 对等连接。

步骤 2：更新两个区域中 VPC 对等连接的路由表

更新您的路由表以开启通过 IPv4 或 IPv6 与对等 VPC 的通信。有关更多信息，请参阅为 VPC 对等连接更新路由表。

第 3 步：创建 AD Connector 并注册亚马逊 WorkSpaces

1. 要查看 AD Connector 先决条件，请参阅 AD Connector 先决条件。
2. 通过 AD Connector 连接现有目录。有关更多信息，请参阅创建 AD Connector。
3. 当 AD Connector 状态更改为活动时，打开 AWS Directory Service 控制台，然后为您的目录 ID 选择超链接。
4. 对于 AWS 应用程序和服务，请选择 Amazon WorkSpaces 以开启对该目录的 WorkSpaces 访问权限。
5. 向注册目录 WorkSpaces。有关更多信息，请参阅向注册目录 WorkSpaces。

我想在 Amazon Linux 2 上更新 Firefox。

步骤 1：检查自动更新是否已启用

要验证是否已启用自动更新，请在上运行命令`systemctl status *os-update-mgmt.timer | grep enabled`。 WorkSpace在输出中，应该有两行显示有 `enabled` 字样。

步骤 2：启动更新

Firefox 通常会在维护时段内自动更新 Amazon Linux 2 WorkSpaces 以及系统中的所有其他软件包。但是，这取决于 WorkSpaces 您使用的类型。

- 因为 AlwaysOn WorkSpaces，每周维护时段为星期日 00:00 到 04h00，所在时区为。 WorkSpace
- 对于 AutoStop WorkSpaces. 从每月的第三个星期一开始，在长达两周的时间内，维护窗口的开放时间为每天大约 00:00 到 05h00，与该地区的时区相同。 AWS WorkSpace

有关维护时段的更多信息，请参阅 WorkSpace 维护。

您也可以通过重启 WorkSpace并在 15 分钟后重新连接来启动即时更新周期。您也可以通过输入 `sudo yum update` 来启动更新。要启动仅适用于 Firefox 的更新，请输入 `sudo yum install firefox`。

如果您无法配置对 Amazon Linux 2 存储库的访问权，并且更喜欢使用 Mozilla 构建的二进制文件安装 Firefox，请参阅 Mozilla 支持页面上的从 Mozilla 版本安装 Firefox。建议完全卸载 RPM 打包版本的 Firefox，以确保您不会错误地运行过时的版本。您可以通过运行命令 `sudo yum remove firefox` 将其卸载。

您也可以通过在另一台计算机上运行命令 `yumdownloader firefox`，从 Amazon Linux 2 存储库下载所需的 RPM 软件包。然后，将存储库侧加载到 WorkSpaces，在那里你可以使用类似`sudo yum install firefox-102.11.0-2.amzn2.0.1.x86_64.rpm`的标准YUM命令来安装它们。

> **Note**
>
> 确切的文件名将根据软件包版本而变化。

步骤 3：验证 Firefox 存储库是否已使用

亚马逊 Linux Extras 会自动为亚马逊 Linux 2 WorkSpaces 提供 Firefox 更新。2023 年 7 月 31 日之后 WorkSpaces 创建的亚马逊 Linux 2 已经激活 Firefox Extra 存储库。要验证您是否 WorkSpace 正在使用 Firefox Extra 存储库，请运行以下命令。

```
yum repolist | grep amzn2extra-firefox
```

如果使用了 Firefox Extra 存储库，则命令输出应类似于 `amzn2extra-firefox/2/x86_64 Amazon Extras repo for firefox 10`。如果未使用 Firefox Extra 存储库，则它将为空。如果未使用 Firefox Extra 存储库，您可以尝试使用以下命令手动启用它：

```
sudo amazon-linux-extras install firefox
```

如果 Firefox Extra 存储库激活仍然失败，请检查您的互联网访问并确保您的 VPC 端点未配置。要继续 WorkSpaces 通过 YUM 存储库接收 Amazon Linux 2 的 Firefox 更新，请确保 WorkSpaces 您能够访问亚马逊 Linux 2 存储库。有关在不访问互联网的情况下访问 Amazon Linux 2 存储库的更多信息，请参阅这篇知识中心文章。

我的用户可以使用 WorkSpaces 客户端重置密码，而忽略上配置的细粒度密码策略 (FFGP) 设置。 AWS Managed Microsoft AD

如果您的用户的 WorkSpaces 客户端与关联 AWS Managed Microsoft AD，则他们必须使用默认的复杂性设置重置密码。

默认复杂度密码区分大小写，长度必须介于 8 到 64 个字符（含）之间。它必须包含以下每个类别中的至少一个字符：

- 小写字符 (a-z)
- 大写字符 (A-Z)
- 数字 (0-9)
- 非字母数字字符 (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

确保密码中不包含不可打印的 unicode 字符，例如空格、回车符、换行符和空字符。

如果您的组织要求您强制执行 FFGP WorkSpaces，请联系您的 Active Directory 管理员，直接从 Active Directory（而非 WorkSpaces 客户端）重置用户的密码。

我的用户在尝试使用 Web Access 访问 Windows WorkSpace /Linux 时收到错误消息 WorkSpace “此操作系统/平台无权访问你的”

您的用户尝试使用的操作系统版本与 WorkSpaces Web Access 不兼容。确保在 WorkSpace 目录的“其他平台” 设置下启用 Web Access。有关启用您 WorkSpace的 Web 访问权限的更多信息，请参阅启用和配置 Amazon WorkSpaces Web Access。

Amazon WorkSpaces 客户端应用程序生命周期终止策略

Amazon WorkSpaces 生命周期终止 (EOL) 策略适用于不再获得支持且不再经过与新版本的兼容性测试的 WorkSpaces 的特定主要版本（及其所有次要版本）。

WorkSpaces 客户端版本的生命周期分为三个阶段：一般支持、技术指导和生命周期终止 (EOL)。一般支持阶段从 WorkSpaces 客户端首次公开发布之日开始，持续一段固定的时间。在一般支持阶段，WorkSpaces 支持团队为解决配置问题提供全面支持。缺陷解决方案和功能请求是针对 WorkSpaces 客户端的该主要版本和相关次要版本实施的。

从一般支持阶段结束到生命周期终止日期，均提供技术指导。在技术指导阶段，您只能获得有关受支持配置的支持和指导。仅针对最新版本的 WorkSpaces 客户端实施缺陷解决方案和功能请求。不对较旧的版本实施它们。在技术指导阶段，如果需要修复，AWS 将安排在即将进行的公开版本发行中进行修复，并且您可以选择升级到最新的 WorkSpaces 版本以获得与修复相关的支持。

当一般支持和技术指导阶段都已结束时，主要版本的生命周期将终止。在生命周期终止后，不再提供进一步的支持或维护。AWS 将停止测试兼容性问题。要获得持续支持，您必须升级到最新版本的 WorkSpaces 客户端。

有关特定版本支持的更多信息，请参阅此表。

Windows 客户端	一般支持	技术指导	EOL
2.x	2018	2023 年 3 月 31 日	2023 年 8 月 31 日

Linux 客户端	一般支持	技术指导	EOL
4.x for Ubuntu 18.04	2021 年 8 月 12 日	2023 年 3 月 31 日	2023 年 8 月 31 日
3.x for Ubuntu 18.04	2019 年 11 月 25 日	2023 年 3 月 31 日	2023 年 8 月 31 日

macOS 客户端	一般支持	技术指导	EOL
2.x	2019	2023 年 3 月 31 日	2023 年 8 月 31 日
1.x	2018	2023 年 3 月 31 日	2023 年 8 月 31 日

iPad 客户端	一般支持	技术指导	EOL
1.x	2018	2023 年 3 月 31 日	2023 年 8 月 31 日

Android 客户端	一般支持	技术指导	EOL
2.x	2019	2023 年 3 月 31 日	2023 年 8 月 31 日
1.x	2018	2023 年 3 月 31 日	2023 年 8 月 31 日

Web access	一般支持		
Google Chrome	当前版本以及两个最新的主要版本		
Firefox	当前版本以及两个最新的主要版本		
Microsoft Edge	当前版本以及两个最新的主要版本		

不支持的客户端

不支持以下 WorkSpaces 客户端。

操作系统	客户端版本	一般支持	技术指导	EOL	备注
Windows	5.11	2023 年 7 月 3 日	2023 年 10 月 1 日	2023 年 10 月 1 日	由于质量问题，不受支持
Windows	5.10	2023 年 6 月 19 日	2023 年 10 月 1 日	2023 年 10 月 1 日	由于质量问题，不受支持
Windows	5.9	2023 年 5 月 9 日	2023 年 10 月 1 日	2023 年 10 月 1 日	由于质量问题，不受支持

EOL 常见问题解答

我使用的 WorkSpaces 客户端版本已到达其生命周期终止日期。我应该怎么做才能升级到受支持的版本？

转至 WorkSpaces 客户端下载页面，下载并安装完全受支持的 WorkSpaces 版本。

我能否在受支持的 WorkSpace 上使用已到达生命周期终止日期的 WorkSpaces 客户端版本？

强烈建议将客户端升级到最新版本，因为之前的解决方案和功能不再适用于已到达生命周期终止日期的客户端版本。如果您使用的客户端版本已到达生命周期终止日期，请联系 AWS 支持团队以获取更多信息。

我使用的 WorkSpaces 客户端版本已到达其生命周期终止日期。我还能报告相关问题吗？

您必须先升级到受支持的版本，然后尝试重现该问题。如果问题在受支持的版本中仍然存在，请向 AWS 支持团队提交支持案例。

我在已到达其生命周期终止日的操作系统上使用受支持的 WorkSpaces 客户端版本。我还能报告相关问题吗？

对于已到达生命周期终止日的操作系统，将不再提供技术援助和软件更新，AWS 也不再为使用已到达其生命周期终止日的操作系统的 WorkSpaces 客户端提供支持。应使用受支持的操作系统来确保您的 WorkSpaces 客户端获得相应支持。

亚马逊 WorkSpaces 配额

Amazon WorkSpaces 提供不同资源，您可以在给定区域的账户中使用这些资源，包括图像 WorkSpaces、捆绑包、目录、连接别名和 IP 控制组。在您创建 Amazon Web Services 账户时，我们会根据您创建的资源的数量设置默认配额（也称为限额）。

以下是您AWS账户 WorkSpaces 的默认配额。您可以使用服务配额控制台查看默认配额和应用的配额，或者请求增加配额来调整配额。

在某些不提供服务配额功能的区域，您必须提交支持案例才能请求提高限额。有关更多信息，请参阅《服务配额用户指南》中的查看服务配额和申请增加配额。

资源	默认值	描述	可调整
WorkSpaces	1	当前区域 WorkSpaces 中该账户的最大数量。	是
图形 WorkSpaces	0	当前区域 WorkSpaces 中此账户中图片的最大数量。 **Note** 2023 年 11 月 30 日之后，不再支持 Graphics 捆绑包。我们建议将你迁移 WorkSpaces 到 Graphics.g4dn 捆绑包。有关更多信息，请参见 迁移 WorkSpace。	是

资源	默认值	描述	可调整
Graphics.g4dn WorkSpaces	0	当前区域中此账户中最大的 Graphics.g4dn WorkSpaces 数量。	是
GraphicsPro WorkSpaces	0	当前区域 GraphicsPro WorkSpaces 中该账户的最大数量。	是
GraphicsPro.g4dn WorkSpaces	0	当前区域 WorkSpaces 中此账户中 GraphicsPro .g4dn 的最大数量。	是
待机 WorkSpaces	0	当前区域 WorkSpaces 中该账户的最大数量。	是
捆绑包	50	当前区域中此账户中的捆绑包的最大数目。此配额仅适用于自定义捆绑包，而不适用于公有捆绑包。	否
连接别名	20	当前区域中此账户中的连接别名的最大数目。	否
目录	50	当前地区该账户 WorkSpaces 中可注册并向 Amazon 使用的最大目录数。	否
映像	40	当前区域中此账户中的映像的最大数目。	是
IP 访问控制组	100	当前区域中此账户中的 IP 访问控制组的最大数目。	否

资源	默认值	描述	可调整
每个目录的 IP 访问控制组数	25	当前区域的此账户中，每个 IP 访问控制组的最大数目。	否
每个 IP 访问控制组的规则数	10	当前区域的此账户中，每个 IP 访问控制组的最大规则数。	否

API 节流

允许的速率为每秒两次调用。有关更多信息，请参阅节流列外。

WorkSpaces 流媒体协议 (WSP) 主机代理版本

WorkSpaces 流协议 (WSP) 主机代理是在您的 WorkSpace内部运行的主机代理。它将你的像素流式传输 WorkSpace 到客户端应用程序，并包括会话中的功能，例如双向音频和视频以及打印。有关 WorkSpaces 流媒体协议 (WSP) 的更多信息，请参阅 Amazon WorkSpaces 协议。

建议将您的主机代理软件更新为最新版本。您可以手动重启 WorkSpaces 以更新 WSP 主机代理。WSP Host Agent 还会在常规 WorkSpaces 默认维护时段内自动更新。有关维护时段的更多信息，请参阅WorkSpace 维护。其中一些功能需要最新的 WorkSpaces 客户端版本。有关最新客户端版本的更多信息，请参阅WorkSpaces 客户端。

下表描述了 WSP 主机代理的每个版本中的更改。

发布版本	Date	更改
• Windows WorkSpaces -2.1.0.1554	2024年5月15日	• 添加了对空闲断开连接超时的支持。 • 添加了新的组策略设置以配置空闲断开连接超时。 • 修复 WorkSpaces 了用户修改显示设置时断开连接并显示白屏的问题。 • 缺陷修复和性能改进。
• Ubunt WorkSpaces u-2.1.0.1342	2024 年 2 月 29 日	• 将首选网络摄像头分辨率更改为介于 480x360 和 640x480 之间。 • 缺陷修复和性能改进。
• Windows WorkSpaces -2.0.0.1425	2024年2月22日	• 增加了对在远程谷歌浏览器或 Microsoft Edge 浏览器中运行的网络应用程序发出的会话中 WebAuthn 重定向请求的支持。此功能会添加一次性浏览器提示，要求用户启用 DCV WebAuthn 重定向扩展。只有 Windows WorkSpace

发布版本	Date	更改
		s 和 WorkSpaces 本机客户端支持它。 • 修复了登录时有时会出现白色或冻结屏幕的问题。 • 缺陷修复和性能改进。
• Windows WorkSpaces -2.0.0.1304	2024 年 1 月 11 日	• 修复了与登录期间可能出现直播冻结相关的错误。 • 修复了一个与日志相关的错误。
• Windows WorkSpaces -2.0.0.1288	2023 年 11 月 16 日	• 在 Windows 10+ 上增加了对间接显示驱动程序 (IDD) 的支持，该驱动程序可降低 CPU 消耗并提高流媒体性能。 • 添加了新的组策略设置以启用或禁用 IDD 驱动程序。 • 修复了与剪贴板图像透明度相关的错误。 • 修复了保留 Windows 缩放系数的错误。 • 缺陷修复和性能改进。
• Windows WorkSpaces -2.0.0.1164	2023 年 10 月 13 日	• 在虚拟显示驱动程序中添加了对 vSync 的支持。 • 添加了新的组策略设置以启用或禁用 vSync。 • 改善了重新连接和可靠性问题。 • 缺陷修复和性能改进。

发布版本	Date	更改
• 亚马逊 Linux WorkSpaces -2.0.0.1086 • Ubunt WorkSpaces u-2.1.0.1086	2023 年 8 月 18 日	• 添加了启用或禁用时区重定向的新设置。 • 延长了登录超时时间并添加了配置选项。 • 改进了网关，可在中断后更快地重新连接。 • 缺陷修复和性能改进。
• 亚马逊 Linux WorkSpaces -2.0.0.907	2023 年 6 月 30 日	• 增加了对 DCV Extension SDK 的支持，以启用特定于 ISV 的集成功能。 • 更改了断开连接行为，以便通过注销终止用户的会话。 • 增加了对时区重定向的支持。 • 延长了登录超时时间并添加了配置选项。 • 修复了一些升级问题。 • 缺陷修复和性能改进。
• Windows WorkSpaces -2.0.0.829	2023 年 6 月 8 日	• 更改了断开连接的行为，以便通过注销终止用户的会话。 • 修复了与 A/V 同步和日语键盘相关的错误。 • 提高了 WSP 安装程序的可靠性。
• Ubunt WorkSpaces u-2.1.0.829	2023 年 5 月 16 日	• 更改了断开连接的行为，以便通过注销终止用户的会话。 • 增加了对 DCV Extension SDK 的支持，以启用特定于 ISV 的集成功能。 • 增加了对时区重定向的支持。 • 修复了一些升级问题。

发布版本	Date	更改
• Windows WorkSpaces -2.0.0.799	2023 年 5 月 8 日	• 通过若干可提高图像质量和性能的优化功能，增强了基于 UDP 的 QUIC 传输能力。 • 增加了对 DCV Extension SDK 的支持，以启用特定于 ISV 的集成功能。 • 添加了新的组策略设置以启用或禁用 Extension SDK。 • 改进了韩语、日语和德语键盘布局。 • 修复了与会话冻结问题、硬件加速、打印机重定向、日志详细程度和 target-fps 组策略设置相关的错误。

Note

- 有关如何检查主机代理版本的信息，请参阅最新版本的 WSP 支持哪些客户端和主机操作系统？。
- 有关如何更新主机代理版本的信息，请参阅如果我已有 WSP WorkSpace，如何更新？ 。
- 有关 WSP macOS 客户端版本发行说明，请参阅《用户指南》中 WorkSpaces macOS 客户端应用程序部分的发行说明。 WorkSpaces
- 有关 WSP Windows 客户端版本发行说明，请参阅《 WorkSpaces 用户指南》中 WorkSpaces Windows 客户端应用程序部分的发行说明。

WSP 支持的 SDK 扩展

Amazon WorkSpaces Streaming Protocol (WSP) 使用 NICE DCV 技术构建，支持对各种工作负载和使用案例的 WorkSpaces 实例进行高性能远程访问。借助 NICE DCV Extension SDK，开发人员可以为最终用户自定义 WSP WorkSpaces 体验，包括：

- 为自定义硬件支持提供便利。
- 提高第三方应用程序在远程会话中的可用性。例如，为 VoIP 应用程序添加本地音频终端，或为会议应用程序添加本地视频播放
- 为屏幕阅读器等辅助功能软件提供有关远程会话和远程运行的应用程序的信息。
- 允许安全软件分析本地端点的安全状况，以允许有条件的访问策略。
- 通过已建立的远程会话执行任意数据传输。

要开始使用 NICE DCV 扩展 SDK，请参阅 NICE DCV 扩展 SDK 文档。您可以在 NICE DCV 扩展 SDK Github 存储库中找到该 SDK 本身。此外，该 SDK 的集成示例可在 NICE DCV 扩展 SDK 示例 Github 存储库中找到。

WorkSpaces 支持以下内容。

- 流式传输协议 - WorkSpaces Streaming Protocol (WSP)
- WorkSpaces Windows 客户端 - Windows：5.9.0.4110 及更高版本。

> **Note**
>
> WorkSpaces Android、iOS 客户端、Web Access 不支持 NICE DCV 扩展 SDK。

- 支持的 WorkSpaces - Windows、Linux 和 Ubuntu 服务器

有关 WorkSpaces 的文档历史记录

下表说明了 2018 年 1 月 1 日之后对 WorkSpaces 服务和 Amazon WorkSpaces 管理指南的重要更改。我们还经常更新文档来处理您发送给我们的反馈意见。

如需有关这些更新的通知，您可以订阅 WorkSpaces RSS 源。

变更	说明	日期
AmazonWorkSpacesAdmin 托管策略更新	WorkSpaces 在 AmazonWorkSpacesAdmin 托管策略中添加了 workspaces:RestoreWorkspace 操作，以授予管理员恢复 WorkSpaces 的权限。	2023 年 7 月 17 日
WSP 支持的 SDK 扩展	借助 NICE DCV Extension SDK，开发人员可以为最终用户自定义 WSP WorkSpaces 体验。	2023 年 5 月 25 日
WorkSpaces Streaming Protocol (WSP) 主机代理版本	有关 WorkSpaces Streaming Protocol (WSP) 的版本信息。	2023 年 5 月 8 日
Amazon WorkSpaces 已在 AWS GovCloud（美国东部）地区推出	Amazon WorkSpaces 已在 AWS GovCloud（美国东部）地区推出。	2023 年 5 月 3 日
Amazon WorkSpaces 网络摄像头支持	Amazon WorkSpaces 现在支持实时音频-视频 (AV)，该功能使用 WorkSpaces Streaming Protocol (WSP) 将本地网络摄像头视频输入无缝重定向到 Windows WorkSpaces 桌面。	2021 年 4 月 5 日
通过 WorkSpaces macOS 客户端应用程序支持 Amazon WorkSpaces 智能卡	现在，您可以使用带有通用访问卡 (CAC) 和个人身份验证 (PIV) 智能卡的 Amazon WorkSpaces macOS 客户端	2021 年 4 月 5 日

	应用程序。使用 WorkSpaces Streaming Protocol (WSP) 的 WorkSpaces 支持智能卡。	
Amazon WorkSpaces 捆绑包管理 API	Amazon WorkSpaces 捆绑包管理 API 现已推出。这些 API 操作支持 WorkSpaces 捆绑包的创建、删除和映像关联操作。	2021 年 3 月 15 日
Amazon WorkSpaces 在亚太地区（孟买）推出	Amazon WorkSpaces 现已在亚太地区（孟买）区域提供。	2021 年 3 月 8 日
WorkSpaces Streaming Protocol (WSP)	WorkSpaces Streaming Protocol (WSP) 现已适用于除 Graphics 和 GraphicsPro 之外的所有捆绑包类型中基于许可证（Windows Server 2016）和 BYOL Windows 10 的 WorkSpaces。WSP 还支持在 AWS GovCloud（美国西部）区域提供 Linux WorkSpaces。	2020 年 12 月 1 日
智能卡	Amazon WorkSpaces 现在支持在 AWS GovCloud（美国西部）地区的 Windows 和 Linux WorkSpaces 上进行会话前（登录）和会话中智能卡身份验证。	2020 年 12 月 1 日
共享自定义映像	您现在可以跨 AWS 账户共享自定义 WorkSpaces 映像。共享映像后，收件人账户可以复制该映像，然后用它来创建用于启动新 WorkSpaces 的捆绑包。	2020 年 10 月 1 日

跨区域重定向	现在，您可以使用可与域名系统 (DNS) 路由策略配合使用的跨区域重定向功能，以便在用户的主 WorkSpaces 不可用时将其重定向到备用 WorkSpaces。	2020 年 9 月 10 日
订阅适用于 BYOL WorkSpaces 的 Microsoft Office 2016 或 2019	您现在可以在 Bring Your Own Windows License (BYOL) WorkSpaces 上订阅由 AWS 提供的 Microsoft Office Professional 2016 或 2019。	2020 年 9 月 3 日
BYOL Automation 在中国（宁夏）地区推出	在中国（宁夏）地区，您可以使用自带许可 (BYOL) 自动化功能简化对 WorkSpaces 使用 Windows 10 桌面许可的过程。	2020 年 4 月 2 日
映像检查程序	映像检查程序工具可帮助您确定 Windows WorkSpace 是否满足映像创建的要求。映像检查程序对要用于创建映像的 WorkSpace 执行一系列测试，并提供有关如何解决它发现的任何问题的指导。	2020 年 3 月 30 日
迁移 WorkSpaces	通过 Amazon WorkSpaces 迁移功能，您可以将 WorkSpace 从一个捆绑包迁移到另一个捆绑包，同时将数据保留在用户卷上。您可以使用此功能将 WorkSpaces 从 Windows 7 桌面体验迁移到 Windows 10 桌面体验。您还可以使用此功能将 WorkSpaces 从一个公有或自定义捆绑包迁移到另一个相应的捆绑包。	2020 年 1 月 9 日

对 Amazon WorkSpaces API 进行 PrivateLink 集成	您可以通过虚拟私有云 (VPC) 中的接口端点直接连接到 Amazon WorkSpaces API 端点，而不是通过互联网进行连接。当您使用 VPC 接口端点时，您的 VPC 与 Amazon WorkSpaces API 端点之间的通信完全在 AWS 网络内安全进行。	2019 年 11 月 25 日
适用于 Amazon WorkSpaces 的 Linux 客户端	用户现在可以使用 Linux 客户端访问其 WorkSpace。	2019 年 11 月 25 日
Amazon WorkSpaces 已在中国（宁夏）地区推出	Amazon WorkSpaces 现已在中国（宁夏）地区提供。	2019 年 11 月 13 日
将 WorkSpaces 恢复到上次已知的正常运行状态	您可以使用还原功能将 WorkSpace 回滚到其上次已知的正常运行状态。	2019 年 9 月 18 日
FIPS 端点加密	为了遵守联邦风险与授权管理计划 (FedRAMP) 或国防部 (DoD) 云计算安全要求指南 (SRG)，您可以配置 Amazon WorkSpaces 以在目录级别使用联邦信息处理标准 (FIPS) 端点加密技术。	2019 年 9 月 12 日
复制 WorkSpace 映像	您可以在同一区域内或跨区域复制映像。	2019 年 6 月 27 日
面向用户的自助式 WorkSpace 管理功能	您可以为用户启用自助式 WorkSpace 管理功能，使他们能够更好地控制其体验。	2018 年 11 月 19 日

BYOL Automation	您可以使用自带许可 (BYOL) 自动化功能来简化对您的 WorkSpace 使用 Windows 7 和 Windows 10 桌面许可的过程。	2018 年 11 月 16 日
PowerPro 和 GraphicsPro 捆绑包	PowerPro 和 GraphicsPro 捆绑包现在可用于 WorkSpaces。	2018 年 10 月 18 日
监控成功的 WorkSpace 登录	您可以使用 Amazon CloudWatch Events 中的事件监控并响应成功的 WorkSpace 登录。	2018 年 9 月 17 日
适用于 Windows 10 WorkSpaces 的 Web Access	用户现在可以使用 Web Access 客户端来访问运行 Windows 10 桌面体验的 WorkSpace。	2018 年 8 月 24 日
URI 登录	您可以使用统一资源标识符 (URI) 为用户对其 WorkSpace 的访问权限。	2018 年 7 月 31 日
Amazon Linux WorkSpaces	您可以为用户预调配 Amazon Linux WorkSpaces。	2018 年 6 月 26 日
IP 访问控制组	您可以控制用户可以从中访问其 WorkSpace 的 IP 地址。	2018 年 30 月 4 日
就地升级	您可以将 Windows 10 BYOL WorkSpace 升级为 Windows 10 的较新版本。	2018 年 3 月 9 日

早期更新

下表说明了 2018 年 1 月 1 日之前 Amazon WorkSpaces 服务及其文档集的重要补充部分。

更改	描述	日期
灵活的计算选项	您可以让 WorkSpaces 在经济、标准、高效和高级服务包之间切换	2017 年 12 月 22 日
可配置存储	您可以在启动 WorkSpace 后配置其根卷和用户卷的大小，还可以在稍后增加这些卷的大小。	2017 年 12 月 22 日
控制设备访问	您可以指定有权访问 WorkSpace 的设备类型。此外，您可以将 WorkSpace 的访问权限限定在受信任设备 (也称为托管设备)。	2017 年 6 月 19 日
林间信任	您可以在 AWS 托管的 Microsoft AD 与本地 Microsoft Active Directory 域之间创建信任关系，然后为本地域中的用户预调配 WorkSpace。	2017 年 2 月 9 日
Windows Server 2016 捆绑包	WorkSpaces 提供了包含 Windows 10 桌面体验并由 Windows Server 2016 提供支持的捆绑包。	2016 年 11 月 29 日
Web Access	您可以使用 WorkSpaces Web Access 从 Web 浏览器访问您的 Windows WorkSpaces。	2016 年 11 月 18 日
按小时计费的 WorkSpace	您可以将 WorkSpace 配置为按小时为用户计费。	2016 年 8 月 18 日
Windows 10 BYOL	您可以将 Windows 10 桌面许可证提供给 WorkSpaces (BYOL)。	2016 年 7 月 21 日
标记支持	您可以使用标签来管理和跟踪您的 WorkSpace。	2016 年 5 月 17 日
已保存的注册	每次输入新的注册代码时，WorkSpaces 客户端都会将其保存。这使您能够在不同目录或区域中的 WorkSpace 之间轻松切换。	2016 年 1 月 28 日
Windows 7 BYOL、Chromebook 客户端、WorkSpace 加密	您可以将 Windows 7 桌面许可证提供给 WorkSpaces (BYOL)、使用 Chromebook 客户端以及使用 WorkSpace 加密技术。	2015 年 10 月 1 日

更改	描述	日期
CloudWatch 监控	增加了有关 CloudWatch 监控的信息。	2015 年 4 月 28 日
会话自动重新连接	添加了有关 WorkSpaces 桌面客户端应用程序中会话自动重新连接功能的信息。	2015 年 3 月 31 日
公有 IP 地址	您可以自动向 WorkSpaces 分配公有 IP 地址。	2015 年 1 月 23 日
WorkSpaces 已在亚太地区（新加坡）推出	WorkSpaces 现已在亚太地区（新加坡）区域提供。	2015 年 1 月 15 日
增加了经济服务包、标准服务包更新、增加了 Office 2013	提供了经济服务包，升级了标准服务包硬件，并且在 Plus 软件包中提供了 Microsoft Office 2013。	2014 年 11 月 6 日
映像和服务包支持	您可以从自定义的 WorkSpace 创建映像，再从该映像创建自定义 WorkSpace 服务包。	2014 年 10 月 28 日
PCoIP 零客户端支持	您可以访问 WorkSpaces PCoIP 零客户端设备。	2014 年 10 月 15 日
WorkSpaces 已在亚太地区（东京）推出	WorkSpaces 现已在亚太地区（东京）区域推出。	2014 年 8 月 26 日
本地打印机支持	您可以为 WorkSpaces 启用本地打印机支持。	2014 年 8 月 26 日
多重身份验证	您可以在连接的目录中使用多重验证。	2014 年 8 月 11 日
默认 OU 支持和目标域支持	您可以选择默认的组织部门 (OU)（您的 WorkSpace 计算机账户位于其中）和单独的域（在其中创建了您的 WorkSpace 计算机帐户）。	2014 年 7 月 7 日

更改	描述	日期
添加安全组	您可以向 WorkSpaces 添加安全组。	2014 年 7 月 7 日
WorkSpaces 已在亚太地区（悉尼）推出	WorkSpaces 现已在亚太地区（悉尼）区域推出。	2014 年 5 月 15 日
WorkSpaces 已在欧洲地区（爱尔兰）推出	WorkSpaces 现已在欧洲地区（爱尔兰）区域提供。	2014 年 5 月 5 日
公开测试版	WorkSpaces 公开测试版已推出。	2014 年 3 月 25 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。