Amazon WorkSpaces

管理指南

Amazon WorkSpaces: 管理指南

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

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

什么是 Amazon WorkSpaces?

Amazon WorkSpaces 使您可以为用户预置基于云的虚拟 Microsoft Windows 或 Amazon Linux 桌面（称为 WorkSpaces ）。 WorkSpaces 使您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，Amazon WorkSpaces请参阅。

Features

- 选择您的操作系统（Windows 或 Amazon 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 Bundles 和 the section called “创建自定义映像和服务包” (p. 123)。
- 选择您的协议： PCoIP 或 WorkSpaces Streaming Protocol (WSP)。有关更多信息，请参阅协议Amazon WorkSpaces (p. 8).
- 连接到您的 WorkSpace 并从您上次停止的地方开始。 WorkSpaces 提供持久桌面体验。
- WorkSpaces 提供了按月或按小时对 计费的灵活性WorkSpaces。 有关更多信息，请参阅 WorkSpaces 定价。
- WorkSpaces 使用 Amazon WorkSpaces Application Manager （Amazon WAM）为 Windows 部署和管理应用程序。
- 对于 Windows 桌面，您可以自带许可证和应用程序，或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，或将您的 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无缝访问企业资源。有关更多信息，请参阅目录 (p. 53).
- 使用与 WorkSpaces 管理本地桌面相同的工具来管理 。
- 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。
- 控制允许用户从中访问其 的 IP 地址WorkSpaces。

Architecture

对于 Windows 和 Amazon Linux WorkSpaces，每个 WorkSpace 都与 Virtual Private Cloud （VPC）以及用于存储和管理 WorkSpaces 和 用户信息的目录关联。有关更多信息，请参阅the section called “VPC 要求” (p. 9). 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 Administration Guide.

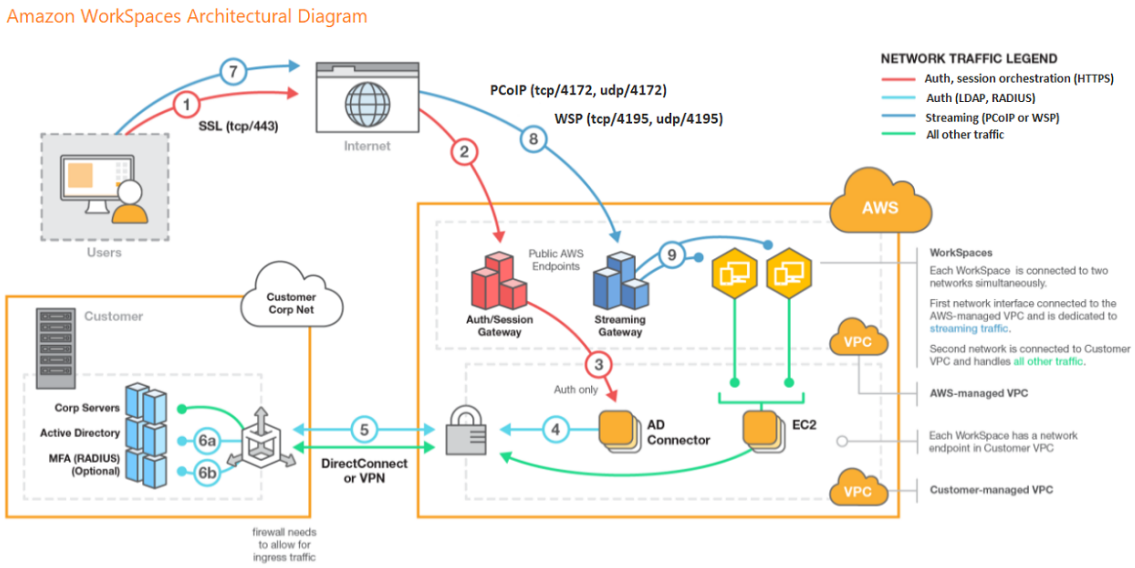
WorkSpaces 使用您的 Simple AD、AD Connector 或 AWS Managed Microsoft AD 目录对用户进行身份验证。用户使用受支持的设备上的WorkSpaces客户端应用程序或 Web 浏览器访问其 WorkSpaces，并使用目录凭证登录。登录信息将发送到身份验证网关，该网关将流量转发到 的 目录WorkSpace。 对用户进行身份验证后，流式传输流量将通过流式传输网关启动。

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 495（WSP）实现到 的像素流式传输WorkSpace，并使用端口 4172 和 495 进行网络运行状况检查。有关更多信息，请参阅用于客户端应用程序的端口 (p. 16).

每个 WorkSpace 具有两个与之关联的弹性网络接口：一个网络接口用于管理和流式处理（eth0另一个是主网络接口（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。这可确保来自 的流量

WorkSpace可以轻松到达 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，请参阅网络接口 (p. 28).

下图演示了 的架构。WorkSpaces.



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

访问您的 WorkSpace

您可以使用受支持设备的 WorkSpaces 客户端应用程序连接到 ，或者对于 Windows WorkSpaces，在受支持的操作系统上使用受支持的 Web 浏览器连接到 。

> **Note**
>
> 您不能使用 Web 浏览器连接到 Amazon 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
- iPads
- Android 设备
- Fire 平板电脑
- 零客户端设备（仅支持 Teradici 零客户端设备） PCoIP.)

在 Windows、 macOS和 Linux 上PCs，您可以使用以下 Web 浏览器连接到 Windows WorkSpaces：

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

有关更多信息，请参阅 WorkSpaces 中的 Amazon WorkSpaces 用户指南 客户端.

Pricing

注册 AWS 后，您便可通过 WorkSpaces 免费套餐优惠开始免费使用 WorkSpaces 有关更多信息，请参阅 WorkSpaces 定价.

使用 WorkSpaces，您可以按实际用量付费。将根据服务包和WorkSpaces您启动的 的数量向您收费。WorkSpaces 的定价包含 Simple AD 和 AD Connector 的使用，但不包含 AWS 托管的 Microsoft AD 的使用。

WorkSpaces 提供 的每月或每小时账单WorkSpaces。 通过按月计费，您可以为无限制使用支付固定费用，这最适合使用其WorkSpaces全部时间的用户。通过按小时计费，您可以按 支付小型固定月费WorkSpace，加上按小时收取的低小时费率，该小时WorkSpace运行 。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，请尝试以下某个教程中介绍的方法：

- 使用 WorkSpaces 快速设置来入门 (p. 4)
- 启动使用 AWS 托管的 Microsoft AD 的 WorkSpace (p. 67)
- 启动使用 Simple AD 的 WorkSpace (p. 69)
- 启动使用 AD Connector 的 WorkSpace (p. 72)
- 启动使用受信任域的 WorkSpace (p. 75)

使用 WorkSpaces 快速设置来入门

在本教程中，您将了解如何预配置基于云的虚拟 Microsoft Windows 或Amazon Linux桌面，称为WorkSpace，通过使用WorkSpaces和AWS Directory Service。

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 (p. 66)。

Note

以下 AWS 区域支持快速设置：

- 美国东部（弗吉尼亚北部）
- 美国西部（俄勒冈）
- 欧洲（爱尔兰）
- 亚太区域（新加坡）
- 亚太区域（悉尼）
- 亚太区域（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。验证支持的区域和选择区域为您的 WorkSpace。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。

在继续操作之前，请查看和理解以下概念也很有帮助：

- 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 服务包。
- 启动 Workspace 时，必须选择要用于捆绑包的协议（PCoIP 或 WorkSpace 流式处理协议 [WSP]）。有关更多信息，请参阅 协议Amazon WorkSpaces (p. 8)。
- 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 (p. 53)。

快速设置功能

快速设置将代表您完成以下任务：

- 创建IAM角色允许WorkSpaces服务创建弹性网络接口并列出WorkSpaces目录。此角色的名称为 `workspaces_DefaultRole`。
- 创建 Virtual Private Cloud (VPC)。如果您想要改为使用现有 VPC，请确保它满足为 配置 VPCWorkSpaces (p. 9)，然后按照使用 WorkSpaces 启动虚拟桌面 (p. 66)。选择与您要使用的活动目录类型对应的教程。
- 设置 Simple AD 目录VPC 中。Simple AD 目录用于存储用户和 WorkSpace 信息。该目录有一个管理员账户并为 Amazon WorkDocs 启用。
- 创建指定用户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 Internet 访问。运行模式为 AlwaysOn。有关更多信息，请参阅 管理 WorkSpace 运行模式 (p. 99)。
- 向指定的用户发送邀请电子邮件。如果您的用户没有收到他们的邀请电子邮件，请参阅发送邀请电子邮件 (p. 79)。

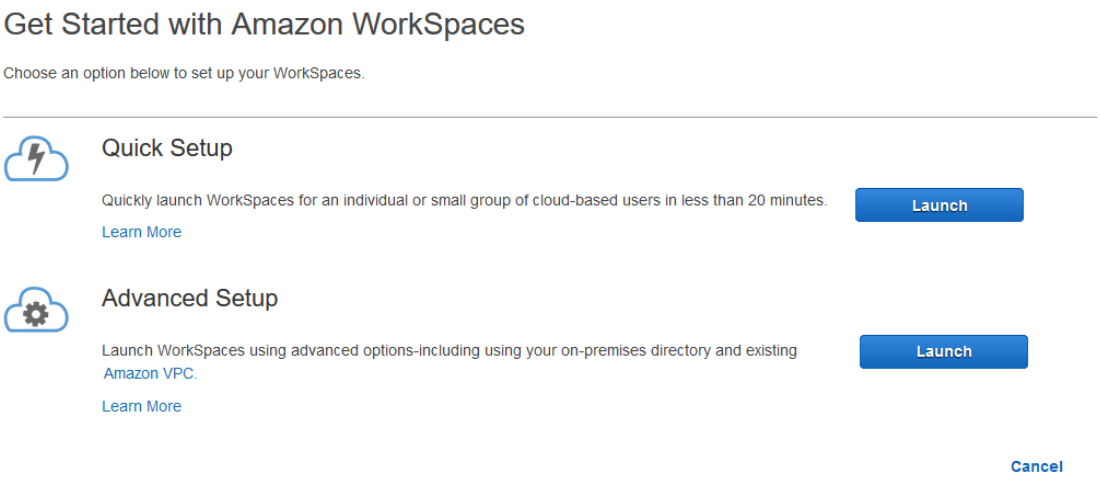
> **Note**
>
> 快速设置创建的第一个用户账户是您的管理员用户账户。您无法从 WorkSpaces 控制台更新此用户账户。请勿与任何其他人分享此管理员账户的信息。如果您想要邀请其他用户使用 WorkSpaces，请为他们创建新的用户账户。

步骤 1: 启动 WorkSpace

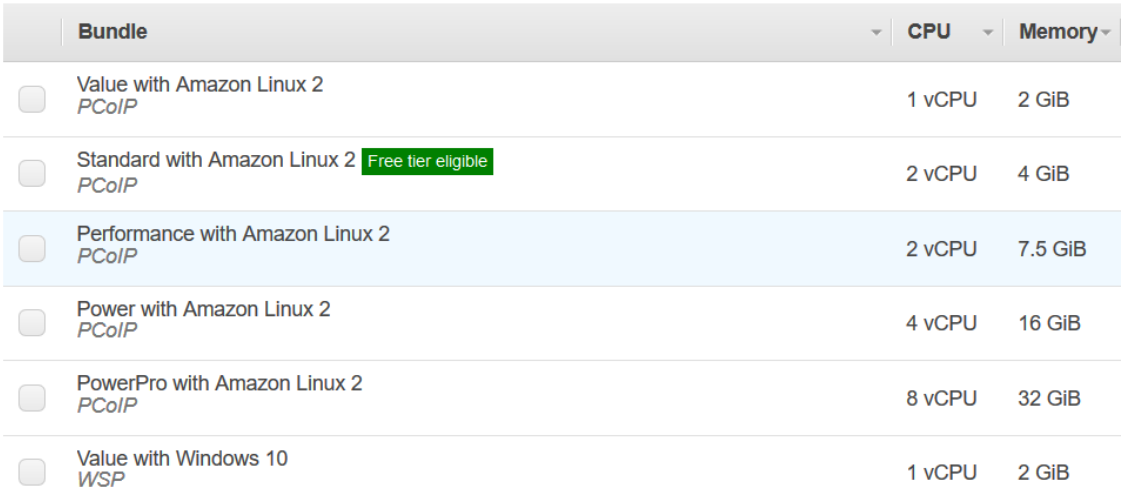
使用 Quick Setup，可以在几分钟内启动您的第一个 WorkSpace。

启动 WorkSpace

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 选择 Get Started Now。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 (p. 4)之一。在这种情况下，请参阅使用 WorkSpaces 启动虚拟桌面 (p. 66)。
3. 在 Get Started with WorkSpaces (开始使用 Amazon WorkSpaces) 页面的 Quick Setup (快速设置) 旁边，选择 Launch (启动)。



4. 适用于bundle中，为具有适当协议（PCoIP 或 WSP）的用户选择一个捆绑包（硬件和软件）。有关 Amazon WorkSpaces 可用的各种公有服务包的更多信息，请参阅 Amazon WorkSpace 服务包。



5. 对于 Enter User Details，填写 Username、First Name、Last Name 和 Email。

   Note

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

6. 选择 Launch WorkSpaces。
7. 在确认页面上，选择 View the WorkSpaces Console。启动 WorkSpace 大约需要 20 分钟时间。要监控进度，请转到左侧导航窗格，然后选择目录。您将看到正在创建的目录，其初始状态为`REQUESTED`然后`CREATING`。

   创建目录并且状态为`ACTIVE`，您可以选择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他们的邀请电子邮件，请参阅发送邀请电子邮件 (p. 79)。

步骤 2: Connect 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)。密码必须混合使用以下字符：小写字母 (a-z)、大写字母 (A-Z)、数字 (0-9) 以及~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/。
2. 审核WorkSpaces客户中的Amazon WorkSpaces 用户指南了解有关每个客户端的要求的更多信息，然后执行以下操作之一：

- 根据系统提示，下载一个客户端应用程序或启动Web 访问。
- 如果您未看到提示且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 访问。

Note

您不能使用 Web 浏览器（Web Access）连接Amazon LinuxWorkSpaces.

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. 当系统提示您登录时，输入用户名和密码，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（如设置多个显示器或使用外围设备）的详细信息，请参阅WorkSpaces客户和外围设备支持中的Amazon WorkSpaces 用户指南。

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 “删除工作区” (p. 122)。

Note

Simple AD向您提供免费与 WorkSpace 一起使用。如果没有 WorkSpaces 与Simple AD目录中连续 30 天，此目录将自动取消注册，以便与Amazon WorkSpaces，并且您将根据AWS Directory Service定价条款。
要删除空目录，请参阅删除您的 WorkSpace 目录 (p. 62)。如果您删除Simple AD目录中，当您想要重新开始使用 WorkSpaces 时，您始终可以创建一个新的目录。

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。您还可以为工作空间和 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 WorkSpace 映像和服务包 (p. 123)
- 管理您的 WorkSpace (p. 83)
- 管理 WorkSpaces 目录 (p. 53)

要创建其他 WorkSpaces，请执行以下操作之一：

- 如果您希望继续使用由快速设置创建的 VPC 和 Simple AD 目录，您可以按照步骤 2: 创建 WorkSpace (p. 71)启动使用 Simple AD 教程的 WorkSpace。
- 如果您需要使用其他目录类型，或者需要使用现有的活动目录，请参阅使用 WorkSpaces 启动虚拟桌面 (p. 66)。

有关使用 WorkSpaces 客户端应用程序（如设置多个显示器或使用外围设备）的详细信息，请参阅WorkSpaces客户和外围设备支持中的Amazon WorkSpaces 用户指南。

WorkSpaces 的网络和访问

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

目录

协议Amazon WorkSpaces

Amazon WorkSpaces支持两种协议：PCoIP 和WorkSpaces Streaming Protocol (WSP)。您选择的协议取决于多个因素，例如用户将访问其 WorkSpace 的设备类型、WorkSpace 上的操作系统、用户将面临的网络条件以及用户是否需要双向视频支持。

何时使用 PCoIP

- 如果您想要使用 iPad、安卓或 Linux 客户端。
- 如果您使用 Tiradici 零客户端设备。
- 如果您需要使用基于 GPU 的捆绑包（图形或 GraphicsPro）。
- 如果您需要将 Linux 捆绑包用于非智能卡使用案例。
- 如果您 WorkSpaces 要在中国 (宁夏) 区域。

何时使用WSP

- 如果您需要更高的损耗/延迟容差来支持最终用户网络条件。例如，您的用户正在跨全局距离访问其 WorkSpace 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。
- 如果您需要会话中的网络摄像头支持功能。

Note

- 一个目录可以混合使用 PCoIP 和WSP其中的 WorkSpaces。
- 用户可以拥有 PCoIP 和WSP只要两个 WorkSpaces 位于不同的目录中，就可以 WorkSpace。同一用户不能拥有 PCoIP 和WSP同一目录中的 WorkSpace。有关为用户创建多个 WorkSpace 的更多信息，请参阅为用户创建多个WorkSpaces (p. 79)。
- 您可以使用 WorkSpaces 迁移功能在两个协议之间迁移 WorkSpace，该功能需要重建 Workspace。有关更多信息，请参阅 迁移 WorkSpace (p. 118)。

为 配置 VPCWorkSpaces

WorkSpaces 在 Virtual Private Cloud （ VPC ） WorkSpaces 中启动 。您的 WorkSpaces 必须能够访问 Internet，以便将更新安装到操作系统并使用 Amazon WorkSpaces Application Manager （ ） Amazon WAM 部署应用程序。

您可以为 创建具有两个私有子网的 WorkSpaces VPC，并在公有子网中创建 NAT 网关。或者，您可以为 创建具有两个公有子网的 WorkSpaces VPC，并将弹性 IP 地址与每个 关联WorkSpace。

Tip

有关各种部署场景的目录和 Virtual Private Cloud （ VPC ） 设计注意事项的详细探讨，请参阅部署最佳实践Amazon WorkSpaces白皮书。

主题

Requirements

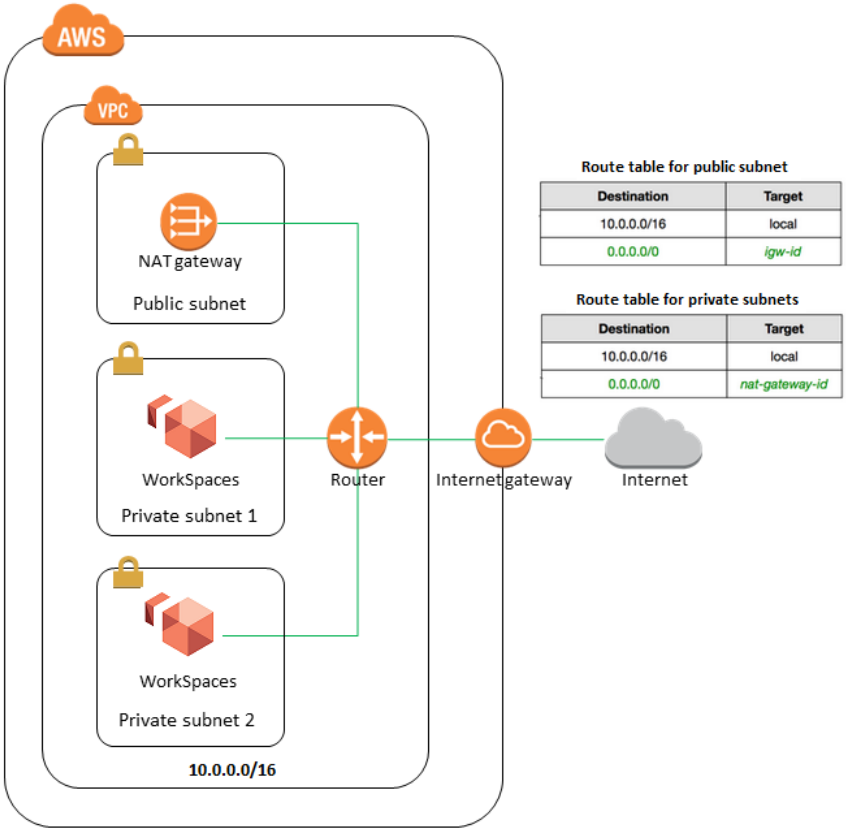
您的 VPC 的子网必须位于您要启动 的区域中的不同可用区中WorkSpaces。 可用区是被设计为可隔离其他可用区中的故障的不同位置。通过启动独立可用区内的实例，您可以保护您的应用程序不受单一位置故障的影响。每个子网都必须完全位于一个可用区之内，不能跨越多个可用区。

Note

Amazon WorkSpaces 在每个受支持区域中的可用区子集中可用。要确定可用于用于 的 VPC 子网的可用区WorkSpaces，请参阅的可用区Amazon WorkSpaces (p. 15)。

配置具有私有子网和 NAT 网关的 VPC

如果您使用 AWS Directory Service 来创建 AWS 托管的 Microsoft AD 或 Simple AD，我们建议您使用一个公有子网和两个私有子网来配置 VPC。配置目录以在私有子网WorkSpaces中启动 。要提供对私有子网 WorkSpaces中 的 Internet 访问，请在公有子网中配置 NAT 网关。



Prerequisites

如果您还不熟悉 VPCs 和子网的使用，我们建议您先阅读 IPv4 中的 VPC 和子网大小调整Amazon VPC 用户指南，然后再执行以下任务。

任务

- 步骤 1：分配弹性 IP 地址 (p. 10)
- 步骤 2：创建 VPC (p. 11)
- 步骤 3：添加第二个私有子网 (p. 12)
- 步骤 4：验证并命名路由表 (p. 12)
- 步骤 5：将您的 WorkSpaces 路由到子网 (p. 13)

> **Note**
>
> 作为配置具有私有子网和 NAT 网关的 VPC 的以下过程的替代方法，您可以按照“入门项目”教程中的步骤操作，该教程详细说明了如何设置 VPC 和 WorkSpaces 目录。该教程还介绍了如何启动 WorkSpaces、创建自定义映像和服务包，以及执行与管理 相关的其他任务WorkSpaces。

步骤 1：分配弹性 IP 地址

为您的 NAT 网关分配弹性 IP 地址，如下所示。请注意，如果您使用其他方法来提供 Internet 访问，则可以跳过此步骤。

分配弹性 IP 地址

1. 打开 Amazon VPC 控制台 https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Elastic （弹性IPs）。
3. 选择 Allocate Elastic IP address (分配弹性 IP 地址).
4. 在 Allocate Elastic IP address （分配弹性 IP 地址）页面上，对于 Public iPv4 address pool （公有地址池），选择 Amazon's pool of IPv4 addresses （Amazon 的地址池）、Public address that you fring to you AWS account （您引入到 AWS 账户IPv4的公有地址） 或 Customer owned pool of addresses （客户拥有IPv4的地址池），然后选择 Allocate （分配）。
5. 记下弹性 IP 地址，然后选择关闭.

步骤 2：创建 VPC

按照如下所示创建具有一个公有子网和两个私有子网的 VPC。

创建 VPC

1. 打开 Amazon VPC 控制台 https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择左上角的 VPC Dashboard （VPC 控制面板）。
3. 选择 Launch VPC Wizard (启动 VPC 向导).
4. 选择 VPC with Public and Private Subnets，然后选择 Select.
5. 按下面所示配置 VPC：
   a. 对于 IPv4 CIDR block （CIDR 块），输入 VPC 的 CIDR 块。我们建议您使用私有（非公共可路由）IP 地址范围（RFC 1918. 中所指定）内的 CIDR 块。例如，`10.0.0.0/16`。 有关更多信息，请参阅 IPv4 中的 的 VPC Amazon VPC 用户指南 和子网大小调整。
   b. 对于 IPv6 CIDR Block （CIDR 块），保留 No CIDR Block （无 IPv6 CIDR 块）。
   c. 对于 VPC name （VPC 名称），输入 VPC 的名称。
6. 按照如下所示配置公有子网：
   a. 对于 IPv4 CIDR block （CIDR 块），输入子网的 CIDR 块。例如，`10.0.0.0/24`。 有关更多信息，请参阅 IPv4 中的 的 VPC Amazon VPC 用户指南 和子网大小调整。
   b. 对于可用区，保留无首选项.
   c. 对于公有子网名称，输入子网的名称（例如，`WorkSpaces Public Subnet`).
7. 按照如下所示配置第一个私有子网：
   a. 对于 Private subnet's IPv4 CIDR （私有子网的 CIDR），输入子网的 CIDR 块。例如，`10.0.1.0/24`。
   b. 要为可用区进行适当的选择，请参阅的可用区Amazon WorkSpaces (p. 15)。
   c. 对于私有子网名称，输入子网的名称（例如，`WorkSpaces Private Subnet 1`).
8. 对于 Elastic IP Allocation ID （弹性 IP 分配 ID），选择您创建的弹性 IP 地址。请注意，如果您使用其他方法来提供 Internet 访问，则可以跳过此步骤。
9. 对于 Service endpoints （服务终端节点），不执行任何操作。
10. 对于启用 DNS 主机名，保留是.
11. 对于硬件租赁，请保留默认值.
12. 选择 Create VPC. 请注意，设置您的 VPC 可能需要几分钟。创建了 VPC 后，选择 OK.

Note

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将IPv6地址分配给在子网中启动的实例，则无法使用 Graphics 捆绑包。（但是，您可以使用GraphicsPro捆绑。）此限制来自不支持 的上一代实例类型的硬件限制IPv6。
要解决此问题，您可以在启动 Graphics 捆绑包之前暂时禁用子网上的IPv6自动分配地址WorkSpaces设置，然后在启动 Graphics 捆绑包后重新启用此设置（如果需要），以便任何其他捆绑包接收所需的 IP 地址。
默认情况下，自动分配IPv6地址设置处于禁用状态。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.
有关使用IPv6地址的更多信息，请参阅 中的您的 VPC Amazon VPC 用户指南中的 IP 寻址。

步骤 3：添加第二个私有子网

在上一步中，您创建了具有一个公有子网和一个私有子网的 VPC。使用以下过程添加第二个私有子网。

添加私有子网

1. 在导航窗格中，选择 Subnets.
2. 选择 Create Subnet.
3. 对于名称标签，输入私有子网的名称（例如，`WorkSpaces Private Subnet 2`).
4. 对于 VPC，选择您创建的 VPC。
5. 要为可用区进行适当的选择，请参阅的可用区Amazon WorkSpaces (p. 15)。确保选择与Step 7 (p. 11)之前选择的可用区不同的可用区。
6. 对于 IPv4 CIDR block （CIDR 块），输入子网的 CIDR 块。例如，`10.0.2.0/24`。
7. 选择 Create （创建）和 Close （关闭）。

步骤 4：验证并命名路由表

您可以验证并命名各个子网的路由表。

验证并命名路由表

1. 在导航窗格中，选择 Subnets （子网），然后选择您创建的公有子网。
   a. 在 Route Table （路由表）选项卡上，选择路由表的 ID（例如rtb-12345678
   b. 选择路由表。在 Name （名称）下，选择编辑图标（铅笔），输入一个名称（例如`workspaces-public-routetable`，），然后选择复选标记以保存名称。
   c. 在 Routes （路由）选项卡上，验证有一个路由用于发送本地流量，另一个路由用于向 VPC 的 Internet 网关发送所有其他流量。例如，您应看到类似于下表中的条目。

目的地	目标
10.0.0.0/16	本地
0.0.0.0/0	igw-12345678

2. 在导航窗格中，选择 Subnets (子网)，然后选择您创建的第一个私有子网（例如 `WorkSpaces Private Subnet 1`).
   a. 在 Route Table 选项卡上，选择路由表的 ID。
   b. 选择路由表。在 Name （名称）下，选择编辑图标（铅笔），然后输入名称（例如`workspaces-private-routetable`，），然后选择复选标记以保存名称。
   c. 在 Routes （路由）选项卡上，确认有一个路由用于发送本地流量，另一个路由用于向 NAT 网关发送所有其他流量。例如，您应看到类似于下表中的条目。

目的地	目标
10.0.0.0/16	本地
0.0.0.0/0	nat-12345678

Note

要为私有子网WorkSpaces中的 提供 Internet 访问，请确保您的 NAT 网关已在公有子网中配置。

3. 在导航窗格中，选择 Subnets (子网)，然后选择您创建的第二个私有子网（例如 `WorkSpaces Private Subnet 2`). 在 Route Table (路由表) 选项卡上，验证路由表是否为私有路由表（例如，`workspaces-private-routetable`). 如果路由表不同，请选择 Edit （编辑），然后选择此路由表。

步骤 5：将您的 WorkSpaces 路由到子网

要将 路由到 WorkSpaces VPC 的子网，请确保在设置WorkSpaces目录的过程中选择 VPC 和子网。

要设置WorkSpaces您的目录，请参阅使用 WorkSpaces 启动虚拟桌面 (p. 66)，并选择适合您要使用的目录类型的教程（AWS 托管的 Microsoft AD、Simple AD、AD Connector，或 AWS 托管的 Microsoft AD 目录与本地域之间的信任关系）。

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。要在公有子网WorkSpaces中提供对 的 Internet 访问，请将 目录配置为自动或手动为每个 分配弹性 IP 地址WorkSpace。

Prerequisites

如果您还不熟悉 VPCs 和子网的使用，我们建议您先阅读 IPv4 中的 VPC 和子网大小调整Amazon VPC 用户指南，然后再执行以下任务。

任务

- 步骤 1：创建 VPC (p. 13)
- 步骤 2：添加第二个公有子网 (p. 14)
- 步骤 3：分配弹性 IP 地址 (p. 14)
- 步骤 4：将您的 WorkSpaces 路由到子网 (p. 15)

步骤 1：创建 VPC

如下所示创建具有一个公有子网的 VPC。

创建 VPC

1. 打开 Amazon VPC 控制台 https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择左上角的 VPC Dashboard （VPC 控制面板）。
3. 选择 Launch VPC Wizard (启动 VPC 向导).
4. 选择带单个公有子网的 VPC，然后选择选择.
5. 对于 IPv4 CIDR block （CIDR 块），输入 VPC 的 CIDR 块。我们建议您使用私有（非公共可路由）IP 地址范围（RFC 1918. 中所指定）内的 CIDR 块。例如，`10.0.0.0/16`。 有关更多信息，请参阅 IPv4 中的 的 VPC Amazon VPC 用户指南 和子网大小调整。

6. 对于 IPv6 CIDR block （CIDR 块），保留 No CIDR Block （无 IPv6 CIDR 块）。
7. 对于 VPC name （VPC 名称），输入 VPC 的名称。
8. 对于 Public subnet's IPv4 CIDR （公有子网的 CIDR），输入子网的 CIDR 块。例如，`10.0.0.0/24`。有关更多信息，请参阅 IPv4 中的 的 VPC Amazon VPC 用户指南 和子网大小调整。
9. 要为可用区进行适当的选择，请参阅的可用区Amazon WorkSpaces (p. 15)。
10. （可选）对于 Subnet name （子网名称），输入子网的名称。
11. 对于 Service endpoints （服务终端节点），不执行任何操作。
12. 对于启用 DNS 主机名，保留是.
13. 对于硬件租赁，请保留默认值.
14. 选择 Create VPC. 创建了 VPC 后，选择 OK.

Note

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将IPv6地址分配给在子网中启动的实例，则无法使用 Graphics 服务包。（但是，您可以使用GraphicsPro捆绑。）此限制来自不支持 的上一代实例类型的硬件限制IPv6。
要解决此问题，您可以在启动 Graphics 捆绑包之前暂时禁用子网上的IPv6自动分配地址WorkSpaces设置，然后在启动 Graphics 捆绑包后重新启用此设置（如果需要），以便任何其他捆绑包接收所需的 IP 地址。
默认情况下，自动分配IPv6地址设置处于禁用状态。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.
有关使用IPv6地址的更多信息，请参阅 中的您的 VPC Amazon VPC 用户指南中的 IP 寻址。

步骤 2：添加第二个公有子网

在上一步中，您创建了具有一个公有子网的 VPC。使用以下过程可添加第二个公有子网，并将其与第一个公有子网的路由表关联，而第一个公有子网具有指向 VPC 的 Internet 网关的路由。

添加公有子网

1. 在导航窗格中，选择 Subnets.
2. 选择 Create Subnet.
3. 对于 Name tag （名称标签），输入子网的名称。
4. 对于 VPC，选择您创建的 VPC。
5. 要为可用区进行适当的选择，请参阅的可用区Amazon WorkSpaces (p. 15)。确保选择与Step 9 (p. 14)之前选择的可用区不同的可用区。
6. 对于 IPv4 CIDR block （CIDR 块），输入子网的 CIDR 块。例如，`10.0.1.0/24`。
7. 选择 Create. 创建子网后，选择关闭.
8. 将新的公有子网与为第一个子网创建的路由表关联：
   a. 在导航窗格中，选择 Subnets.
   b. 选择第一个子网。
   c. 在 Route Table 选项卡上，选择路由表的 ID。
   d. 在子网关联选项卡上，选择编辑子网关联.
   e. 选中第二个子网（您刚创建的公有子网）的复选框，然后选择 Save (保存).

步骤 3：分配弹性 IP 地址

您可以自动或手动将弹性 IP 地址WorkSpaces（静态公有 IP 地址）分配给您的 。要使用自动分配，请参阅配置自动 IP 地址 (p. 55). 要手动分配弹性 IP 地址，请使用以下过程。

Warning

我们建议您不要在 启动WorkSpace后修改 的弹性网络接口。如果您已在目录级别启用弹性 IP 地址自动分配，则在启动WorkSpace时，系统会为您的 分配弹性 IP 地址（来自 Amazon 提供的池）。但是，如果您将您拥有的弹性 IP 地址与 关联WorkSpace，并且稍后取消了该弹性 IP 地址与 的关联WorkSpace，则 将WorkSpace失去其公有 IP 地址，并且不会自动从 Amazon 提供的池中获取新的地址。
要将 Amazon 提供的池中的新公有 IP 地址与 关联WorkSpace，您必须重建 WorkSpace (p. 111)。 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 WorkSpace。

手动将弹性 IP 地址分配给 WorkSpace

有关如何将弹性 IP 地址分配给 的视频教程WorkSpace，请参阅 AWS 知识中心视频如何将弹性 IP 地址与 关联WorkSpace?

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces 。
3. 展开 的行（选择箭头图标WorkSpace），并记下 WorkSpace IP 的值。这是 的主要私有 IP 地址 WorkSpace。
4. 打开 Amazon EC2 控制台 https://console.aws.amazon.com/ec2/。
5. 在导航窗格中，选择 Elastic（弹性IPs）。 如果您没有可用的弹性 IP 地址，请选择 Allocate Elastic IP address（分配弹性 IP 地址），然后选择 Amazon's pool of IPv4 addresses（Amazon 的地址池）或 Customer owned pool of addresses（客户拥有IPv4的地址池），然后选择 Allocate（分配）。记下新的 IP 地址。
6. 在导航窗格中，选择 Network Interfaces.
7. 为您的 选择网络接口WorkSpace。 要查找您的 的网络接口WorkSpace，请在搜索框中输入 WorkSpace IPStep 3 (p. 15) 值（您之前在中记下），然后按 Enter。WorkSpace IP 值与网络接口的 Primary private IPv4 IP 列中的值匹配。请注意，网络接口的 VPC ID 值与您的 WorkSpaces VPC 的 ID 匹配。
8. 依次选择 Actions、Manage IP Addresses. 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.

步骤 4：将您的 WorkSpaces 路由到子网

要将 路由到 WorkSpaces VPC 的子网，请确保在设置WorkSpaces目录的过程中选择 VPC 和子网。

要设置WorkSpaces您的目录，请参阅使用 WorkSpaces 启动虚拟桌面 (p. 66)，并选择适合您要使用的目录类型的教程（AWS 托管的 Microsoft AD、Simple AD、AD Connector，或 AWS 托管的 Microsoft AD 目录与本地域之间的信任关系）。

的可用区Amazon WorkSpaces

创建一个 Virtual Private Cloud (VPC)，它与Amazon WorkSpaces，则 VPC 的子网必须位于您要启动 WorkSpaces 的区域中的不同可用区域中。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`。为确保资源分配到某个区域的各个可用区，我们将可用区独立映射到每个 AWS 账户的名称。例如，您的 AWS 账户的可用区 `us-east-1a` 可能与另一 AWS 账户的 `us-east-1a` 不在同一位置。

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 us-east-1 区域的 AZ ID，它在每个 AWS 账户中的位置均相同。

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在每个受支持区域的可用区域的子集中可用。下表列出了您可在每个区使用的 AZ ID。要查看您账户中账户中的可用区的 AZ ID 的映射，请参阅您的资源的 AZ ID中的AWS RAM 用户指南。

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

有关可用区和 AZ ID 的更多信息，请参阅区域、可用区和本地区域中的Amazon EC2 用户指南（适用于 Linux 实例）。

WorkSpaces 的 IP 地址和端口要求

要连接到您的 WorkSpace，您的 WorkSpaces 客户端连接的网络必须对各种 AWS 服务（分为不同子集）的 IP 地址范围开放某些端口。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AWS 的 IP 地址范围中的Amazon Web Services 一般参考。

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

用于客户端应用程序的端口

WorkSpaces 客户端应用程序需要以下端口上的出站访问：

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。
- WorkSpace 所在区域中的 `AMAZON` 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 和 4195 (UDP 和 TCP)

这些端口用于流式处理 WorkSpace 桌面和运行状况检查。桌面客户端应用程序不支持对端口 4172 和 4195 流量使用代理服务器；它们需要直接连接到端口 4172 和 4195。这些端口必须对 PCoIP 网关开放，并且WorkSpaces Streaming Protocol (WSP)网关 IP 地址范围和 WorkSpace 所在区域中的运行状况检查服务器。有关更多信息，请参阅Health 检查服务器 (p. 24)、PCoIP 网关服务器 (p. 26)和WSP网关服务器 (p. 28)。

Note

如果防火墙使用有状态筛选，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，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。

用于 Web 访问的端口

WorkSpaces Web Access 需要以下端口的入站和出站访问：

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 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。它必须对 WorkSpace 所在区域中的 `EC2` 子集中的所有 IP 地址范围开放。

端口 443 (UDP 和 TCP)

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

一般情况下，Web 浏览器在较高范围内随机选择一个源端口来用于流式处理流量。WorkSpacesWeb Access 对浏览器选择的端口没有控制权。您必须确保允许流量返回到该端口。

WorkSpaces Web Access 首选 UDP 而非 TCP 用于桌面流，但如果 UDP 不可用，则会回退到 TCP。即使阻止除 53、80 和 443 外的所有 UDP 端口，Web Access 也将使用 TCP 连接在 Chrome 和 Firefox 上运行。

要添加到允许列表的域和 IP 地址

对于WorkSpaces客户端应用程序，以便能够访问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。

要添加到允许列表中的域和 IP 地址

类别	域或 IP 地址
CAPTCHA	https://opfcaptcha-prod.s3.amazonaws.com/
客户端自动更新	• https://d2td7dqidlhjx7.cloudfront.net/ • 在 AWS GovCloud (US-West) 区域中： https://s3.amazonaws.com/workspaces-client-updates/prod/pdt/windows/WorkSpacesAppCast.xml
连接检查	https://connectivity.amazonworkspaces.com/
设备指标（适用于 1.0+ 和 2.0+ WorkSpaces 客户端应用程序）	https://device-metrics-us-2.amazon.com/
客户端指标（适用于 3.0+ WorkSpaces 客户端应用程序）	域: • https://skylight-client-ds.us-east-1.amazonaws.com • https://skylight-client-ds.us-west-2.amazonaws.com • https://skylight-client-ds.ap-south-1.amazonaws.com • https://skylight-client-ds.ap-northeast-2.amazonaws.com • https://skylight-client-ds.ap-southeast-1.amazonaws.com • https://skylight-client-ds.ap-southeast-2.amazonaws.com • https://skylight-client-ds.ap-northeast-1.amazonaws.com • https://skylight-client-ds.ca-central-1.amazonaws.com • https://skylight-client-ds.eu-central-1.amazonaws.com • https://skylight-client-ds.eu-west-1.amazonaws.com • https://skylight-client-ds.eu-west-2.amazonaws.com • https://skylight-client-ds.sa-east-1.amazonaws.com • 在 AWS GovCloud (US-West) 区域中： https://skylight-client-ds.us-gov-west-1.amazonaws.com
动态消息服务（适用于 3.0+ WorkSpaces 客户端应用程序）	域: • https://ws-client-service.us-east-1.amazonaws.com • https://ws-client-service.us-west-2.amazonaws.com

类别	域或 IP 地址
	• https://ws-client-service.ap-south-1.amazonaws.com • https://ws-client-service.ap-northeast-2.amazonaws.com • https://ws-client-service.ap-southeast-1.amazonaws.com • https://ws-client-service.ap-southeast-2.amazonaws.com • https://ws-client-service.ap-northeast-1.amazonaws.com • https://ws-client-service.ca-central-1.amazonaws.com • https://ws-client-service.eu-central-1.amazonaws.com • 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.com

类别	域或 IP 地址
目录设置	在登录 WorkSpace 之前从客户端到客户目录的身份验证： • 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/ 登录页面的 JavaScript 文件： • 美国东部（弗吉尼亚北部）— https://d32i4gd7pg4909.cloudfront.net/ • 美国西部（俄勒冈）— https://d18af777lco7lp.cloudfront.net/ • 亚太地区（孟买）—https://d78hovzzqqtsb.cloudfront.net/ • 亚太区域（首尔）— https://dtyv4uwoh7ynt.cloudfront.net/ • 亚太区域（新加坡）— https://d3qzmd7y07pz0i.cloudfront.net/ • 亚太区域（悉尼）— https://dwcpoxuuza83q.cloudfront.net/ • 亚太区域（东京）— https://d2c2t8mxjhq5z1.cloudfront.net/ • 加拿大 (中部) — https://d2wfbsypmqjmog.cloudfront.net/ • 欧洲（法兰克福）— https://d1whcm49570jjw.cloudfront.net/ • 欧洲（爱尔兰）— https://d3pgffbf39h4k4.cloudfront.net/ • 欧洲（伦敦）— https://d16q6638mh01s7.cloudfront.net/

类别	域或 IP 地址
	• 南美洲（圣保罗）— https://d2lh2qc5bdoq4b.cloudfront.net/ 在 AWS GovCloud (US-West) 区域中： • 客户目录设置： https://s3.amazonaws.com/workspaces-client-properties/prod/pdt/<目录 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/<目录 ID> • 用于设计登录页面的 CSS 文件： https://s3.amazonaws.com/workspaces-clients-css/workspaces_v2.css • 登录页面的 JavaScript 文件： 不适用
Forrester 日志服务	https://fls-na.amazon.com/
运行 Health 检查 (DRP) 服务器	Health 检查服务器 (p. 24)
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	http:// <directory id> .awsapps.com/ (其 <directory id> 中是客户的域) 在 AWS GovCloud (US-West) 区域中： https://login.us-gov-home.awsapps.com/directory/<directory id>/(其中 <directory id> 是客户的域)

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

类别	域或 IP 地址
WorkSpaces API 终端节点	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.us-gov-west-1.amazonaws.com • https://workspaces-fips.us-gov-west-1.amazonaws.com

要添加到 PCoIP 允许列表中的域和 IP 地址

类别	域或 IP 地址
PCoIP 会话网关 (PSG)	PCoIP 网关服务器 (p. 26)
会话代理 (PCM)	域: • https://skylight-cm.us-east-1.amazonaws.com • https://skylight-cm-fips.us-east-1.amazonaws.com • https://skylight-cm.us-west-2.amazonaws.com • https://skylight-cm-fips.us-west-2.amazonaws.com • 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

类别	域或 IP 地址
	• https://skylight-cm.ap-northeast-1.amazonaws.com • https://skylight-cm.ca-central-1.amazonaws.com • https://skylight-cm.eu-central-1.amazonaws.com • 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.us-gov-west-1.amazonaws.com • https://skylight-cm-fips.us-gov-west-1.amazonaws.com
PCoIP 网页访问 TURIP 服务器	服务器： • turn:*.us-east-1.rdn.amazonaws.com • turn:*.us-west-2.rdn.amazonaws.com • Web 访问目前在亚太地区（孟买）区域。 • 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

要添加到允许列表的域和 IP 地址WorkSpaces Streaming Protocol (WSP)

类别	域或 IP 地址
WSP会话网关 (WSG)	WSP网关服务器 (p. 28)
Web 访问 TURN 服务器WSP	服务器： • 此功能不适用于WSP。

Health 检查服务器

这些区域有：WorkSpaces客户端应用程序对端口 4172 和 4195 执行运行状况检查。这些检查验证 TCP 或 UDP 流量是否从 WorkSpaces 服务器流式传输到客户端应用程序。为了成功完成这些检查，您的防火墙策略必须允许发送到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（弗吉尼亚北部）	drp-iad.amazonworkspaces.com	3.209.215.252 3.212.50.30

区域	运行状况检查主机名	IP 地址
		3.225.55.35 3.226.24.234 34.200.29.95 52.200.219.150
美国西部（俄勒冈）	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
亚太区域（首尔）	drp-icn.amazonworkspaces.com	13.124.44.166 13.124.203.105 52.78.44.253 52.79.54.102
亚太区域（新加坡）	drp-sin.amazonworkspaces.com	3.0.212.144 18.138.99.116 18.140.252.123 52.74.175.118
亚太区域（悉尼）	drp-syd.amazonworkspaces.com	3.24.11.127 13.237.232.125
亚太区域（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

区域	运行状况检查主机名	IP 地址
欧洲（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（爱尔兰）	drp-dub.amazonworkspaces.com	18.200.177.86 52.48.86.38 54.76.137.224
欧洲（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
AWS GovCloud (US-West)	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

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。WorkSpaces 会为其 PCoIP 网关服务器使用较小范围的 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。

> **Note**
>
> 我们定期更新我们的 IP 地址范围AWS 的 IP 地址范围 `ip-ranges.json`文件。要获取 WorkSpaces 的最新 IP 地址范围，请在 `ip-ranges.json` 文件中查找符合 `service: "WORKSPACES_GATEWAYS"` 的条目。

区域	公有 IP 地址范围
美国东部（弗吉尼亚北部）	3.217.228.0 - 3.217.231.255

区域	公有 IP 地址范围
	3.235.112.0 - 3.235.119.255 52.23.61.0 - 52.23.62.255
美国西部（俄勒冈）	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
亚太区域（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
亚太区域（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
亚太区域（悉尼）	3.25.43.0 - 3.25.43.255 3.25.44.0 - 3.25.45.255 54.153.254.0 - 54.153.254.255
亚太区域（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（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（爱尔兰）	3.249.28.0 - 3.249.29.255 52.19.124.0 - 52.19.125.255
欧洲（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

区域	公有 IP 地址范围
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
AWS GovCloud (US-West)	52.61.193.0 - 52.61.193.255

WSP网关服务器

Important

从二零零年六月开始,WorkSpaces流式传输桌面会话WSP通过端口 4195 而不是端口 4172 向客户端提供 WorkSpaces。如果要使用WSPWorkSpaces，请确保端口 4195 对流量开放。

WorkSpaces使用一小范围Amazon EC2公有 IPv4 地址，其WSP网关服务器。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（弗吉尼亚北部）	3.227.4.0/22
美国西部（俄勒冈）	34.223.96.0/22
亚太地区（孟买）	65.1.156.0/22
亚太区域（首尔）	3.35.160.0/22
亚太区域（新加坡）	13.212.132.0/22
亚太区域（悉尼）	3.25.248.0/22
亚太区域（东京）	3.114.164.0/22
加拿大 (中部)	3.97.20.0/22
欧洲（法兰克福）	18.192.216.0/22
欧洲（爱尔兰）	3.248.176.0/22
欧洲（伦敦）	18.134.68.0/22
南美洲（圣保罗）	15.228.64.0/22
AWS GovCloud (US-West)	3.32.139.0/24

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 内以及 Internet 上的资源的连接，并用于将 WorkSpace 加入目录。
- 管理网络接口 (eth0) 已连接到安全的 WorkSpaces 管理网络。它用于将 WorkSpace 桌面以交互方式流式传输到 WorkSpaces 客户端，并允许 WorkSpaces 管理 WorkSpace。

WorkSpaces 从多个地址范围中选择管理网络接口的 IP 地址，具体取决于创建 WorkSpace 的区域。目录注册后，WorkSpaces 会测试 VPC CIDR 和您的 VPC 中的路由表，以确定这些地址范围是否会发生冲突。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

请勿修改或删除与 WorkSpace 相连接的任何网络接口。这样做可能会导致 WorkSpace 变得无法访问或导致它无法访问 Internet。例如，如果您在目录级别启用了弹性 IP 地址自动分配 (p. 55)，则会在您的 WorkSpace 启动时为其分配弹性 IP 地址（来自 Amazon 提供的池）。但是，如果您将您拥有的弹性 IP 地址与 WorkSpace 关联，稍后您将该弹性 IP 地址与 WorkSpace 取消关联，则 WorkSpace 将失去其公有 IP 地址，并且不会自动从 Amazon 提供的池中获取新的 IP 地址。要将 Amazon 提供的池中的新公有 IP 地址与 WorkSpace 关联，您必须重建 WorkSpace (p. 111)。如果您不想重建 WorkSpace，必须将您拥有的另一个弹性 IP 地址与 WorkSpace 关联。

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

- 如果使用自带许可 (BYOL) Windows WorkSpaces，则下表中的 IP 地址范围不适用。相反，PCoIP BYOL WorkSpaces 将 54.239.224.0/20 IP 地址范围用于所有 AWS 区域的管理接口流量。对于 WSP BYOL Windows WorkSpaces，54.239.224.0/20 和 10.0.0.0/8 的 IP 地址范围都适用于所有 AWS 区域。（除了您为 BYOL 工作空间的管理流量选择的 /16 CIDR 块之外，还使用这些 IP 地址范围。）
- 如果您使用的是从公共捆绑包创建的 WSP WorkSpaces，除了下表所示的 PCOIP/WSP 范围之外，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（弗吉尼亚北部）	预防和保护儿童基金会/WSP：172.31.0.0/16、192.168.0.0/16 和 198.19.0.0/16 WSP：10.0.0.0/8
美国西部（俄勒冈）	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）	预防和保护儿童基金会/WSP：192.168.0.0/16 WSP：10.0.0.0/8
亚太区域（首尔）	预防和保护儿童基金会/WSP：198.19.0.0/16 WSP：10.0.0.0/8
亚太区域（新加坡）	预防和保护儿童基金会/WSP：198.19.0.0/16 WSP：10.0.0.0/8
亚太区域（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

区域	IP 地址范围
亚太区域（东京）	预防和保护儿童基金会/WSP：198.19.0.0/16 WSP：10.0.0.0/8
加拿大 (中部)	预防和保护儿童基金会/WSP：198.19.0.0/16 WSP：10.0.0.0/8
欧洲（法兰克福）	预防和保护儿童基金会/WSP：198.19.0.0/16 WSP：10.0.0.0/8
欧洲（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（伦敦）	预防和保护儿童基金会/WSP：198.19.0.0/16 WSP：10.0.0.0/8
南美洲（圣保罗）	预防和保护儿童基金会/WSP：198.19.0.0/16 WSP：10.0.0.0/8
AWS GovCloud (US-West)	预防和保护儿童基金会/WSP：198.19.0.0/16 WSP：10.0.0.0/8

管理接口端口

以下端口在所有 WorkSpace 的管理网络接口上都必须处于打开状态：

- 端口 4172 上的入站 TCP。它用于在 PCoIP 协议上建立流式连接。
- 端口 4172 上的入站 UDP。它用于 PCoIP 协议上的流式用户输入。
- 端口 4489 上的入站 TCP。这用于通过 Web 客户端访问。（Web 访问客户端不支持WSP协议。）
- 端口 8200 上的入站 TCP。它用于 PCoIP 协议上的 WorkSpace 管理和配置。
- 端口 8201-8250 上的入站 TCP。这些端口用于建立流式连接和流式用户输入WSP协议。
- 出站 TCP 端口 8443 和 9997。这用于通过 Web 客户端访问。（Web 访问客户端不支持WSP协议。）
- 端口 3478、4172 和 4195 上的出站 UDP。这用于通过 Web 客户端访问。（Web 访问客户端不支持WSP协议。）
- 端口 50002 和 55002 上的出站 UDP。它用于流式处理。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。
- 使用端口 80 通过出站 TCP 发送到 IP 地址 169.254.169.254，用于访问 EC2 元数据服务。分配给您的 WorkSpace 的任何 HTTP 代理中还必须排除 169.254.169.254。
- 端口 1688 上的出站 TCP 发送到 IP 地址 169.254.169.250 和 169.254.169.251，以允许访问 Microsoft KMS 来激活基于公共捆绑的工作区。如果您使用自带许可证 (BYOL) Windows WorkSpaces，则必须允许访问您自己的 KMS 服务器以进行 Windows 激活。
- 端口 1688 上的出站 TCP 发送到 IP 地址 54.239.239.236.220，以允许访问 Microsoft KMS 来激活 BYOL WorkSpaces 的 Office。

  如果您正在通过 WorkSpaces 公用包之一使用 Office，则用于 Office 激活的 Microsoft KMS 的 IP 地址会有所不同。若要确定该 IP 地址，请查找 WorkSpace 管理接口的 IP 地址，然后将最后两个八位字节替

换为64.250。例如对于如果管理接口的 IP 地址是 192.168.3.5，则微软 KMS 办公室激活的 IP 地址是 192.168.64.250。

- 出站 TCP 到 IP 地址 127.0.0.2 的WSP将 WorkSpaces 主机配置为使用代理服务器时的工作空间。

正常情况下，WorkSpaces 服务会为您的 WorkSpace 配置这些端口。如果 WorkSpace 上安装了任何拦截这些端口的安全或防火墙软件，则 WorkSpace 可能无法正常工作，或者可能无法连接。

主接口端口

不论您拥有哪种类型的目录，以下端口在所有 WorkSpace 的主网络接口上都必须打开：

- 对于 Internet 连接，以下端口在出站至所有目的地和从 WorkSpace VPC 入站时必须处于打开状态。如果您希望它们能够访问 Internet，则需要将这些端口手动添加到您的 WorkSpace 的安全组。
  - TCP 80 (HTTP)
  - TCP 443 (HTTPS)
- 要与目录控制器通信，以下端口必须在您的 WorkSpace VPC 与目录控制器之间处于打开状态。在 Simple AD 目录中，通过 AWS Directory Service 创建的安全组会将这些端口配置正确。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 authentication
  - UDP 123 - NTP
  - TCP 135 - RPC
  - UDP 137-138 - Netlogon
  - TCP 139 - Netlogon
  - TCP/UDP 389 - LDAP
  - TCP/UDP 445 - SMB
  - TCP 1024-65535 - Dynamic ports for RPC

  如果 WorkSpace 上安装了任何拦截这些端口的安全或防火墙软件，则 WorkSpace 可能无法正常工作，或者可能无法连接。

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 “哪些 Amazon WorkSpaces 服务包支持 Web 访问？”。in客户端访问、Web 访问和用户体验。

> 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 Internet 连接。我们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 WorkSpaces 的 IP 地址和端口要求 (p. 16)。

- 为了 PCoIP 的最佳性能，从客户端网络到 WorkSpaces 所在区域之间的往返时间 (RTT) 应小于 100ms。如果 RTT 介于 100ms 到 200ms 之间，则用户可以访问 WorkSpace，但性能会受到影响。如果 RTT 介于 200ms 到 375 毫秒之间，则性能会降低。如果 RTT 超过 375 毫秒，则工作空间客户端连接将终止。

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

  要检查 RTT 到各种AWS区域，请使用Amazon WorkSpaces连接 Health 检查。
- 使用网络摄像头WSP，我们建议将上传带宽最小为 1.7 兆位/秒。
- 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 Virtual Private Cloud (VPC) 的 VPN 访问 WorkSpaces。要使用 VPN 访问 WorkSpaces，需要 Internet 连接（通过 VPN 的公有 IP 地址），如 WorkSpaces 的 IP 地址和端口要求 (p. 16)中所述。
- 客户端需要通过 HTTPS 访问由此服务和 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 零客户端设备访问，您必须使用 PCoIP 协议包为 WorkSpaces 使用。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 WorkSpace 设置 PCoIP 零客户端 (p. 44)。
- 对于 3.0 以上客户端，如果您使用单点登录 (SSO)Amazon WorkDocs，您必须按照中的说明进行操作。单点登录中的AWS Directory Service Administration Guide。

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，请执行以下操作之一。

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。

限制对受信任设备的 WorkSpaces 访问

默认情况下，用户可以从连接到 Internet 的任何受支持的设备访问其 WorkSpaces。如果您的公司仅允许受信任设备（也称为托管设备）访问公司数据，则可以使用有效的证书将 WorkSpaces 访问限制为受信任设备。

启用此功能后，WorkSpaces 会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，则会阻止从该设备登录或重新连接的尝试。

对于每个目录，您最多可以导入 2 个根证书。如果您导入 2 个根证书，则 WorkSpaces 会将这 2 个证书都显示给客户端，然后客户端查找一直串联到其中一个根证书的第一个有效匹配的证书。

Important

此功能仅适用于 WorkSpaces Windows 和 macOS 客户端。
此功能不 适用于：

- 适用于 Linux、Android 或 WorkSpaces 的 iPad 客户端应用程序
- Web Access 客户端WorkSpaces
- 任何第三方客户端，包括但不限于：
  - Teradici PCoIP 软件和移动客户端
  - Teradici PCoIP 零客户端
  - RDP 客户端
  - 远程桌面应用程序

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。

Requirements

- 证书必须是 Base64 编码的证书文件 (采用 CRT、CERT 或 PEM 格式)。
- 证书必须包含公用名。
- 证书链支持的最大长度为 4。
- WorkSpaces 当前不支持客户端证书的设备撤销机制，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。我们建议使用带 RSA 的 SHA256、带 ECDSA 的 SHA256、带 ECDSA 的 SHA384 或带 ECDSA 的 SHA512。
- 确保公有密钥上存在“密钥用法：数字签名”，否则即使计算机和 WorkSpaces 控制台上存在公有密钥和私有密钥，设备身份验证也将失败。
- 对于 macOS，如果设备证书位于系统密钥链中，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

您必须在受信任设备上为用户安装客户端证书。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 可以选择执行安全状况评估，以确定设备是否符合访问 WorkSpaces 的公司策略。

在 Windows 上，WorkSpaces 客户端应用程序在用户和根证书存储区中搜索客户端证书。在 macOS 上，WorkSpaces 客户端应用程序在整个密钥链中搜索客户端证书。

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。这需要 WorkSpaces 客户端应用程序在允许用户登录到 WorkSpace之前验证设备上的证书。

配置限制

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Directories.
3. 选择目录，然后选择 Actions、Update Details.
4. 展开 Access Control Options.
5. [Windows] 选择仅允许受信任的 Windows 设备访问 WorkSpaces。
6. [macOS] 选择仅允许受信任的 macOS 设备访问 WorkSpaces。
7. 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.
   b. 将证书文本复制到表单中。
   c. 选择 Import.
8. （可选）指定其他类型的设备是否有权访问 WorkSpaces。
   a. 向下滚动到 Other Platforms （其他平台） 部分。默认情况下，WorkSpaces Web Access 和 Linux 客户端处于禁用状态，用户可以从其 iOS 设备、Android 设备、WorkSpacesChromebook 和 零客户端设备访问其 PCoIP。
   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.
9. 选择 Update and Exit.

使用智能卡进行身份验证

上的 Windows 和 Linux WorkSpacesWorkSpaces Streaming Protocol (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。

Amazon WorkSpaces支持使用智能卡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其 WorkSpaces 时执行的智能卡身份验证。会话内身份验证是指登录后执行的身份验证。

例如，用户可以在使用 Web 浏览器和应用程序时使用智能卡进行会话中身份验证。他们还可以使用智能卡执行需要管理权限的操作。例如，如果用户对其 Linux WorkSpace 具有管理权限，则在运行`sudo`和`sudo -i`命令。

目录

Requirements

- 活动目录连接器（AD Connector）目录是必需的。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 (p. 35)。

- 若要将智能卡与 Windows 或 Linux WorkSpace 一起使用，用户必须使用Amazon WorkSpacesWindows 客户端版本 3.1.1 或更高版本或 WorkSpaces macOS 客户端 3.1.5 或更高版本。有关在 Windows 和 macOS 客户端中使用智能卡的详细信息，请参阅智能卡 Support中的Amazon WorkSpaces 用户指南。
- 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 。为 Amazon WorkSpaces 启用智能卡身份验证中的AWS Directory Service Administration Guide和证书要求在微软文档中。

  除了这些要求之外，用于智能卡身份验证的用户证书Amazon WorkSpaces必须包含以下属性：
  - 证书的 userPrincipalName (SAN) 字段中的 AD 用户主题名称 (UPN)。我们建议为用户的默认 UPN 颁发智能卡证书。
  - 客户端身份验证 (1.3.6.1.5.7.3.2) 扩展密钥用法 (EKU) 属性。
  - 智能卡登录 (1.3.6.1.1.1.311.20.2.2) EKU 属性。
- 对于会话前身份验证，证书吊销检查需要在线证书状态协议 (OCSP)。对于会话中身份验证，建议使用 OCSP，但不是必需的。

Limitations

- 智能卡身份验证当前仅支持 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 3.1.5 或更高版本。
- 仅当客户端在 64 位版本的 Windows 上运行时，WorkSpaces Windows 客户端应用程序 3.1.1 或更高版本支持智能卡。
- 智能卡身份验证当前仅支持 AD Connector 目录。
- 会话前身份验证仅在AWS GovCloud（美国西部）区域目前。会话内身份验证在所有提供的区域中可用WSP支持。
- 对于 Linux 或 Windows WorkSpaces 上的会话中身份验证和会话前身份验证，当前一次只允许使用一个智能卡。
- 对于会话前身份验证，当前不支持在同一目录上启用智能卡身份验证以及用户名和密码身份验证。
- 目前仅支持 CAC 和 PIV 卡。其他类型的智能卡可能也可以工作，但它们尚未经过充分测试是否可以与 WSP。
- 当前不支持在 Windows 或 Linux WorkSpace 会话期间使用智能卡解锁屏幕。要解决 Windows WorkSpace 的此问题，请参阅检测 Windows 锁定屏幕并断开会话连接 (p. 36)。要解决 Linux WorkSpace 的此问题，请参阅在 Linux WorkSpaces 上禁用锁定屏幕 (p. 38)。

目录配置

要启用智能卡身份验证，必须按照以下方式配置 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AD Connector 先决条件中的AWS Directory Service Administration Guide。特别是，请确保已在防火墙中打开必要的端口。

要完成配置 AD Connector 目录，请按照为 Amazon WorkSpaces 启用智能卡身份验证中的AWS Directory Service Administration Guide。

> **Note**
>
> 用于配置会话前智能卡身份验证的 AWS Directory Service API 操作和 Directory Service AWS 命令行界面 (AWS CLI) 命令目前仅在AWS GovCloud（美国西部）区域。

本地目录配置

除了配置 AD Connector 目录之外，还必须确保颁发给您的内部部署目录的域控制器的证书具有 "KDC 身份验证" 扩展密钥用法 (EKU) 设置。若要执行此操作，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的必要设置。

启用 Windows WorkSpaces 的智能卡

有关如何在 Windows 上启用智能卡身份验证的一般指导，请参阅使用第三方证书颁发机构启用智能卡登录的指南在微软文档中。

检测 Windows 锁定屏幕并断开会话连接

若要允许用户在屏幕锁定时解锁为智能卡会话前身份验证启用的 Windows WorkSpace，您可以在用户会话中启用 Windows 锁屏检测。检测到 Windows 锁定屏幕后，WorkSpace 会话将断开连接，并且用户可以使用智能卡从 WorkSpaces 客户端重新连接。

通过使用组策略设置检测到 Windows 锁定屏幕时，可以启用断开会话连接。有关更多信息，请参阅 启用或禁用屏幕锁定上的断开连接会话WSP (p. 94)。

启用会话中或会话前身份验证

默认情况下，Windows WorkSpaces 未启用以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 启用会话中身份验证和会话前身份验证。有关更多信息，请参阅 为的启用或禁用智能卡重定向WSP (p. 94)。

要使用会话前身份验证，除了更新组策略设置外，还必须通过 AD Connector 目录设置启用会话前身份验证，方法是使用EnableClientAuthenticationAPI 操作或enable-client-authenticationCLI 命令。有关更多信息，请参阅 。启用 AD Connector 的智能卡身份验证中的AWS Directory Service Administration Guide。

使用户能够在浏览器中使用智能卡

如果您的用户使用 Chrome 作为其浏览器，则无需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，您可以通过组策略让用户在 Firefox 中使用智能卡。可以使用这些Firefox 组策略模板（位于 GitHub 中）。

例如，您可以安装 64 位版本的OpenSC以支持 PKCS #11，然后使用下面的组策略设置，其中*NAME_OF_DEVICE*是您想要用来标识 PKCS #11 的任何值，例如`OpenSC`，其中*PATH_TO_LIBRARY_FOR_DEVICE*是指向 PKCS #11 模块的路径。此路径应指向具有 .DLL 扩展名的库，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，也可以加载 OpenSSL`pkcs11`模块添加到 Firefox 中，方法是运行`pkcs11-register.exe`计划。要运行此程序，请双击`C:\Program Files\OpenSC Project\OpenSC\tools\pkcs11-register.exe`，或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"
```

验证 OpenSC 是否`pkcs11`模块已加载到 Firefox 中，请执行以下操作：

1. 如果 Firefox 已在运行中，请关闭它。
2. 打开 Firefox。选择菜单按钮，然后选择选项。
3. 在存储库的关于:首选项页面上，在左侧导航窗格中选择隐私和安全。
4. 在Certificates中，选择安全设备。

5. 在设备管理器对话框中，您应该看到OpenSC 智能卡框架 (0.21)，并且当您选择它时，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`

Troubleshooting

有关解决智能卡的信息，请参阅证书和配置问题在微软文档中。

一些可能导致问题的常见问题：

- 插槽到证书的映射不正确。
- 在智能卡上具有多个可与用户匹配的证书。证书将使用以下标准进行匹配：
  - 证书的根 CA。
  - 这些区域有：`<KU>`和`<EKU>`字段。
  - 证书主题中的 UPN。
- 具有多个具有`<EKU>msScLogin`在他们的密钥用法中。

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插槽。

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）的工具可能是制造商特定的。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 WorkSpaces 的智能卡

Note

上的 Linux WorkSpacesWorkSpaces Streaming Protocol (WSP)捆绑包仅在中可用AWS GovCloud（美国西部）区域目前。
上的 Linux WorkSpacesWSP当前具有以下限制：

- 不支持剪贴板、音频输入、视频输入和时区重定向。
- 不支持多台显示器。
- 必须使用 WorkSpaces Windows 客户端应用程序来连接到WSP。

要在 Linux WorkSpaces 上启用智能卡的使用，您需要在 WorkSpace 映像中包含 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操作的根 CA 证书。
- 您可以使用 Web 注册站点导出您自己的根 CA 证书，该站点是`http://`*`ip_address`*`/certsrv`或者`http://`*`fqdn`*`/certsrv`，其中，*`ip_address`*和*`fqdn`*是根证书 CA 服务器的 IP 地址和完全限定域名 (FQDN)。有关如何使用 Web 注册站点的更多信息，请参阅如何导出根证书颁发机构证书在微软文档中。
- 您可以使用以下过程从运行活动目录证书服务 (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，请参阅安装证书颁发机构在微软文档中。

  1. 使用管理员帐户登录到根 CA 服务器。
  2. 从 Windows 中启动菜单中，打开命令提示符窗口 (启动 >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，请参阅证书在微软文档中。

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，请参阅www.openssl.org。

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

将根 CA 证书添加到 Linux WorkSpaces

为了帮助您启用智能卡，我们添加了enable_smartcard脚本添加到我们的Amazon Linux WSP服务包。此脚本将执行以下操作：

- 将您的根 CA 证书导入到网络安全服务 (NSS)数据库。
- 安装pam_pkcs11模块进行可插拔身份验证模块 (PAM) 身份验证。
- 执行默认配置，其中包括启用pkinit在 WorkSpace 设置过程中。

以下步骤将说明如何使用enable_smartcard脚本将根 CA 证书添加到 Linux WorkSpaces，并为 Linux 工作空间启用智能卡。

1. 创建一个新的 Linux WorkSpace，使用WSP协议已启用。WorkSpace 在Amazon WorkSpaces控制台上的选择服务包页面上，请确保选择WSP，然后选择其中一个Amazon Linux 2公共服务包。
2. 在新 WorkSpace 上，以 root 用户身份运行以下命令，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 假定智能卡上的证书是为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)。
> 若要使用备用 UPN 后缀，run /usr/lib/skylight/enable_smartcard --help，了解更多信息。备用 UPN 后缀的映射对于每个用户都是唯一的。因此，必须在每个用户的 WorkSpace 上单独执行该映射。

3. （可选）默认情况下，启用所有服务以便在 Linux WorkSpaces 上使用智能卡身份验证。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。取消的注释auth的行pam_succeed_if.so并根据需要编辑服务列表。

   在auth行未注释，则要允许服务使用智能卡身份验证，您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. （可选）当前不支持使用智能卡解锁屏幕。要在 Linux WorkSpaces 上禁用锁定屏幕，请创建一个名为/usr/share/glib-2.0/schemas/10_screensaver.gschema.override，其中包含以下内容：

```
[org.mate.screensaver]
lock-enabled=false
```

创建此文件后，运行以下命令：

```
sudo glib-compile-schemas /usr/share/glib-2.0/schemas/
```

5. 对 WorkSpace 执行任何其他自定义。例如，您可能希望将系统范围的策略添加到使用户能够在 Firefox 中使用智能卡 (p. 39)。Chrome 用户必须在自己的客户端上启用智能卡。 有关更多信息，请参阅 。智能卡 Support中的Amazon WorkSpaces 用户指南。)
6. 创建自定义 WorkSpace 映像和捆绑 (p. 123) (从 WorkSpace 中) 。
7. 使用新的自定义捆绑包为您的用户启动 WorkSpaces。

使用户能够在 Firefox 中使用智能卡

您可以通过将安全设备策略添加到您的 Linux WorkSpace 映像中，使用户能够在 Firefox 中使用智能卡。有关向 Firefox 添加系统范围内的更多信息，请参阅Mozilla 策略模板 (位于 GitHub 上) 。

1. 在用于创建 WorkSpace 映像的 WorkSpace 上，创建一个名为`policies.jsonin/usr/lib64/firefox/distribution/`。
2. 在 JSON 文件中，添加以下安全设备策略，其中*`NAME_OF_DEVICE`*是您要使用的任何值来标识`pkcs`模块。例如，您可能希望使用诸如`"OpenSC"`：

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

Troubleshooting

为了进行故障排除，我们建议添加`pkcs11-tools`实用工具。此实用程序允许您执行以下操作：

- 列出每个智能卡。
- 列出每个智能卡上的插槽。
- 列出每个智能卡上的证书。

一些可能导致问题的常见问题：

- 插槽到证书的映射不正确。
- 在智能卡上具有多个可与用户匹配的证书。证书将使用以下标准进行匹配：
  - 证书的根 CA。
  - 这些区域有：`<KU>`和`<EKU>`字段。
  - 证书主题中的 UPN。
- 具有多个具有`<EKU>msScLogin`在他们的密钥用法中。

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插槽。

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）的工具可能是制造商特定的。可用于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

排查问题pam_pkcs11和pam-krb5配置，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，然后更改nodebug的参数pam_pksc11.so到debug。
2. 在/etc/pam_pkcs11/pam_pkcs11.conf文件，更改debug = false;到debug = true;。这些区域有：debug选项分别应用于每个映射器模块，因此您可能需要直接在pam_pkcs11部分以及相应的映射器部分（默认情况下，这是mapper generic)。
3. 在/etc/pam.d/system-auth-ac文件中，编辑auth操作并添加debug或debug_sensitive参数设置为pam_krb5.so。

启用调试日志记录后，系统将打印出pam_pkcs11调试消息直接在活动终端中。来自的消息pam_krb5登录/var/log/secure。

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
```

在系统提示时，输入智能卡 PIN。pklogin_finder上的输出stdout智能卡证书上的用户名*NETBIOS**username*。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。NetBIOS 域名通常是域名系统 (DNS) 域名的子域。例如，如果 DNS 域名是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，对于用户mmajor在域中corp.example.com，输出来自pklogin_finder是CORP\mmajor。

> **Note**
>
> 如果您收到消息"ERROR:pam_pkcs11.c:504: verify_certificate() failed"，此消息表示pam_pkcs11在智能卡上找到了与用户名标准相匹配的证书，但该证书没有链接到计算机识别的根 CA 证书。如果发生这种情况,pam_pkcs11输出上面的消息，然后尝试下一个证书。仅当它找到与用户名匹配并链接到已识别的根 CA 证书的证书时，它才允许进行身份验证。

排查问题pam_krb5配置，您可以手动调用kinit在调试模式下，并使用以下命令：

```
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，请尝试将正确的 Kerberos 主体名称显式添加到命令中。例如，对于用户mmajor在域中corp.example.com，请使用此命令：

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

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

如果此命令未成功，但是基于密码的kinit命令成功，请检查pkinit_相关配置/etc/krb5.conf文件。例如，如果智能卡包含多个证书，则可能需要更改pkinit_cert_match。

提供 WorkSpace 的 Internet 访问权限

您的 WorkSpace 必须具有 Internet 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。您可以使用以下选项之一，以允许 Virtual Private Cloud (VPC) 中的 WorkSpace 访问 Internet。

Options

- 在私有子网中启动您的 WorkSpace 并在 VPC 中的公有子网内配置 NAT 网关。
- 在公有子网中启动您的 WorkSpaces 并自动或手动将公有 IP 地址分配到 WorkSpace。

有关这些选项的更多信息，请参阅为 配置 VPCWorkSpaces (p. 9)。

通过上述任一选项，您必须确保 WorkSpace 的安全组允许端口 80 (HTTP) 和 443 (HTTPS) 上的出站流量流向所有目的地 (`0.0.0.0/0`)。

Amazon WAM

如果使用 Amazon WorkSpaces Application Manager (Amazon WAM) 将应用程序部署到您的 WorkSpace，那么 WorkSpace 必须能够访问 Internet。

Amazon Linux Extras 库

如果您使用的是 Amazon Linux 存储库，则 Amazon Linux WorkSpaces 必须能够访问 Internet，否则您必须配置指向此存储库和主 Amazon Linux 存储库的 VPC 终端节点。有关更多信息，请参阅 。例如：允许访问Amazon LinuxAMI 存储库部分Amazon S3 的终端节点。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 中的实例通过终端节点访问该存储库，请创建终端节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/*"
        ]
    }
  ]
}
```

的安全组WorkSpaces

向 WorkSpaces 注册目录时，它会创建两个安全组，一个用于目录控制器，另一个用于目录中的 WorkSpaces。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）。的安全组的名称为目录标识符后跟 WorkSpaces_workspacesMembersworkspacesMembers（例如，d-123456fc11_workspacesMembersworkspacesMembers

> **Warning**
>
> 请勿修改或删除 _controllers 和 _workspacesMembers 安全组。如果您修改或删除这些安全组，您的 WorkSpaces 将无法正常运行，并且您将无法重新创建这些组并将它们重新添加。

您可以将默认 WorkSpaces 安全组添加到目录中。将新安全组与 WorkSpaces 目录关联后，您启动的新 WorkSpaces 或重建的现有 WorkSpaces 将具有新的安全组。您还可以将此新的默认安全组添加到现有 WorkSpaces，而无需重新生成它们 (p. 42)，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，将有效汇总每个安全组的规则以创建一组规则。我们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 https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html 中的您的 VPC 的安全组Amazon VPC 用户指南。

向 WorkSpaces 目录添加安全组

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Directories.
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 Update and Exit.

要将安全组添加到现有 WorkSpace 而不重新生成它，请将新安全组分配给 WorkSpace 的弹性网络接口（ENI）。

向现有 WorkSpace 添加安全组

1. 查找需要更新的每个 WorkSpace 的 IP 地址。
   a. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
   b. 展开每个 WorkSpace 并记录其 WorkSpace IP 地址。
2. 查找每个 WorkSpace 的 ENI 并更新其安全组分配。
   a. 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. 根据需要对任何其他 WorkSpaces 重复此过程。

适用于您的 WorkSpace 的 IP 访问控制组

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。您可以将每个 IP 访问控制组与一个或多个目录关联。每个AWS帐户每个区域最多可创建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。

有一个与每个目录都关联的默认 IP 访问控制组。默认组允许所有流量。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。

您可以将此功能与 Web Access 和适用于 macOS、iPad、Windows、Chromebook 和 Android 的客户端应用程序结合使用。要将此功能与 PCoIP 零客户端结合使用，您无法使用 PCoIP 连接管理器。

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. 通过以下网址打开 WorkSpaces 控制台：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 Description (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. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Directories。
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 Update and Exit。

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. 通过以下网址打开 WorkSpaces 控制台：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. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Directories。
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 WorkSpace 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。当用户使用零客户端设备直接连接到其 WorkSpaces 时，我们建议您对 WorkSpaces 目录使用多重身份验证 (MFA)。有关使用 MFA 与目录的更多信息，请参阅以下文档：

- AWS Managed Microsoft AD — 为启用多重验证AWS Managed Microsoft AD中的AWS Directory Service管理指南
- AD Connector — 为启用多重验证AD Connector中的AWS Directory Service管理指南和多重验证 (AD Connector) (p. 57)
- 受信任的域 — 为启用多重验证AWS Managed Microsoft AD中的AWS Directory Service管理指南
- Simple AD —多重验证对不可用。Simple AD。

自 2021 年 4 月 13 日起，PCoIP Connection Manager 不再支持用于 4.6.0 和 6.0.0 之间的零客户端设备固件版本。如果您的 zero 客户端固件为 6.0.0 或更高版本，则可以通过桌面访问订阅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。”

有关设置和连接 PCoIP 零客户端设备的信息，请参阅 https://docs.aws.amazon.com/workspaces/latest/userguide/amazon-workspaces-pcoip-zero-client.html 中的 Amazon WorkSpaces 用户指南PCoIP 零客户端。有关批准的 PCoIP 零客户端设备的列表，请参阅PCoIP Zero 客户端 ）。

为 Chromebook 设置 Android

Amazon WorkSpaces Chromebook 客户端应用程序的最终版本是 2.4.13 版。由于 Google 正在逐步退出对 Chrome 应用程序的支持，因此，将不会进一步更新 WorkSpaces Chromebook 客户端应用程序，并且不支持使用该应用程序。

对于支持安装 Android 应用程序的 Chromebook，建议您改为使用 WorkSpaces Android 客户端应用程序。

在用户安装 Amazon WorkSpaces Android 客户端应用程序之前，必须启用 2019 年之前推出的某些 Chromebook 以安装 Android 应用。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 访问

大多数 WorkSpaces 服务包支持通过 Chrome 或 Firefox 浏览器进行 Amazon WorkSpaces Web 访问。有关支持 Web 浏览器访问的 WorkSpaces 的列表，请参阅 “哪些Amazon WorkSpaces捆绑包支持 Web 访问？” in客户端访问、Web 访问和用户体验。

Note

- Web 浏览器不能用于连接到 Amazon Linux WorkSpaces。
- Web 访问目前不支持 WorkSpaces 用WorkSpaces Streaming Protocol (WSP)。
- Web 访问当前不提供亚太地区（孟买）区域。

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。

步骤 1: 启用对 WorkSpaces 的 Web 访问

您可以在目录级别控制对 WorkSpaces 的 Web 访问。对于要允许用户通过 Web 访问客户端访问的包含 WorkSpaces 的每个目录，请执行以下步骤。

启用对 WorkSpaces 的 Web 访问

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Directories。
3. 选择相应的目录，然后选择 Actions (操作)、Update Details (更新详细信息)。
4. 展开 Access Control Options，找到 Other Platforms 部分。
5. 选择 Web Access (Web 访问)。
6. 选择 Update and Exit。

步骤 2: 为 Web 访问配置对端口的入站和出站访问

Amazon WorkSpaces Web 访问要求对某些端口进行入站和出站访问。有关更多信息，请参阅 用于 Web 访问的端口 (p. 17)。

步骤 3: 配置组策略和安全策略设置以允许用户登录

Amazon WorkSpaces 依靠特定登录屏幕配置来让用户能够从 Web Access 客户端成功登录。

要使 Web Access 用户能够登录其 WorkSpaces，您必须配置“Group Policy (组策略)”设置和三个“Security Policy (安全策略)”设置。如果未正确配置这些设置，用户可能会在尝试登录其 WorkSpaces 时遇到长时间登录或黑屏。要配置这些设置，请使用以下过程。

您可以使用组策略对象 (GPO) 应用设置来管理 Windows WorkSpaces 或属于 Windows WorkSpaces 目录的用户。我们建议您分别为 WorkSpace 计算机对象和 WorkSpace 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，请参阅安装 Active Directory 管理工具中的AWS Directory Service Administration Guide。

支持 WorkSpaces 登录代理切换用户

在大多数情况下，当某个用户尝试登录 WorkSpace 时，用户名字段将预填充该用户的名称。但是，如果管理员建立了到 WorkSpace 的 RDP 连接来执行维护任务，则用户名字段将改为填充管理员的名称。

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。禁用此设置时，WorkSpaces 登录代理可以使用 Switch User (切换用户) 按钮来使用正确名称填充用户名字段。

1. 打开组策略管理工具 (gpmc.msc)，然后导航到用于 WorkSpaces 的目录的域或域控制器级别的 GPO 并选择该 GPO。（如果您的域中安装了 WorkSpaces 组策略管理模板 (p. 84)，则可以为 WorkSpaces 计算机账户使用 WorkSpaces GPO。）
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 WorkSpace 的配置，该列表可能不会显示 Other User (其他用户) 磁贴。在发生此情况时，如果填充的用户名不正确，WorkSpaces 登录代理将无法使用正确名称填充该字段。

若要避免此问题，请启用安全策略设置交互式登录: 不显示上次登录或者交互式登录: 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)，然后导航到用于 WorkSpaces 的目录的域或域控制器级别的 GPO 并选择该 GPO。（如果您的域中安装了 WorkSpaces 组策略管理模板 (p. 84)，则可以为 WorkSpaces 计算机账户使用 WorkSpaces GPO。）
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，您需要要求用户按 CTRL+ALT+DEL 才能登录。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)，然后导航到用于 WorkSpaces 的目录的域或域控制器级别的 GPO 并选择该 GPO。（如果您的域中安装了 WorkSpaces 组策略管理模板 (p. 84)，则可以为 WorkSpaces 计算机账户使用 WorkSpaces GPO。）
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 登录代理可查找用户的名称和域。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)，然后导航到用于 WorkSpaces 的目录的域或域控制器级别的 GPO 并选择该 GPO。（如果您的域中安装了 WorkSpaces 组策略管理模板 (p. 84)，则可以为 WorkSpaces 计算机账户使用 WorkSpaces GPO。）
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: 锁定会话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更改将在 WorkSpace 的下一次组策略更新后和重新启动 WorkSpace 会话后生效。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，然后依次选择 Actions (操作)、Reboot WorkSpaces (重启 WorkSpace)）。
- 从管理命令提示符下，输入 gpupdate /force。

为 FedRAMP 授权或 DoD SRG 合规性设置 Amazon WorkSpaces

要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) 终端节点加密。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，您还可以对 WorkSpaces 进行加密。有关更多信息，请参阅 加密的 WorkSpace (p. 105)。

Requirements

- 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 验证模式进行终端节点加密。

  > **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 验证模式进行终端节点加密。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

使用 FIPS 终端节点加密

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Directories。

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 (终端节点加密)，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 Update and Exit。
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 (p. 47)部分中列出的 WorkSpaces 客户端应用程序之一。

为您的 Linux WorkSpace 启用 SSH 连接

如果您或您的用户希望使用命令行连接到 Amazon Linux WorkSpaces，则可启用 SSH 连接。您可以启用与目录中的所有 WorkSpace 或目录中的单个 WorkSpace 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。

有关视频教程，请参阅 AWS 知识中心中的如何使用 SSH 连接到我的 Linux Amazon WorkSpaces？。

目录

到 Amazon Linux WorkSpaces 的 SSH 连接的先决条件

- 启用到 WorkSpace 的入站 SSH 流量 — 要添加允许到一个或多个 Amazon Linux WorkSpaces 的入站 SSH 流量的规则，请确保您具有需要与 WorkSpaces 的 SSH 连接的设备的公有或私有 IP 地址。例如，您可以指定 Virtual Private Cloud (VPC) 之外的设备的公有 IP 地址或您的 WorkSpace 所在的 VPC 中的另一个 EC2 实例的私有 IP 地址。

  如果您计划从本地设备连接到 WorkSpace，则可以在 Internet 浏览器中使用搜索短语 “我的 IP 地址”，或使用以下服务：检查 IP。
- 连接到 WorkSpace — 需要以下信息才能发起从设备到 Amazon Linux WorkSpace 的 SSH 连接。
  - 您连接到的 Active Directory 域的 NetBIOS 名称。
  - 您的 WorkSpace 用户名。
  - 要连接到的 WorkSpace 的公有或私有 IP 地址。

    私有：如果您的 VPC 已连接到公司网络并且您有权访问该网络，则可以指定 WorkSpace 的私有 IP 地址。

    公共：如果您的 WorkSpace 具有公有 IP 地址，则可以使用 WorkSpaces 控制台来查找该公有 IP 地址，如以下过程中所述。

查找要连接到的 Amazon Linux WorkSpace 的 IP 地址和您的用户名

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 在 WorkSpaces 的列表中，选择要为其启用 SSH 连接的 WorkSpace。
4. 在 Running mode (运行模式) 列中，确认 WorkSpace 状态为 Available (可用)。
5. 单击 WorkSpace 名称左侧的箭头以显示内联摘要，并记下以下信息：
   - WorkSpace IP。这是 WorkSpace 的私有 IP 地址。

     需要此私有 IP 地址才能获取与 WorkSpace 关联的弹性网络接口。需要网络接口才能检索与 WorkSpace 关联的安全组或公有 IP 地址等信息。
   - WorkSpace Username (用户名)。这是您指定的要连接到 WorkSpace 的用户名。
6. 打开 Amazon EC2 控制台 https://console.aws.amazon.com/ec2/。
7. 在导航窗格中，选择 Network Interfaces。
8. 在搜索框中，键入在步骤 5 中记下的 WorkSpace IP。
9. 选择与 WorkSpace IP 关联的网络接口。
10. 如果您的 WorkSpace 具有公有 IP 地址，则它会显示在 IPv4 Public IP (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. 通过以下网址打开 AWS Directory Service 控制台：https://console.aws.amazon.com/directoryservicev2/。
2. 在目录列表中，单击 WorkSpace 的目录的 Directory ID (目录 ID) 链接。
3. 在 Directory details (目录详细信息) 部分中，记下 Directory NetBIOS name (目录 NetBIOS 名称)。

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

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

创建具有规则的安全组，此规则允许到目录中的所有 Amazon Linux WorkSpaces 的入站 SSH 流量

1. 打开 Amazon EC2 控制台 https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Security Groups。
3. 选择 Create Security Group。
4. 键入安全组的名称（可选）和描述。
5. 对于 VPC，选择包含要为其启用 SSH 连接的 WorkSpaces 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 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. 选择创建。

启用与特定 Amazon Linux WorkSpace 的 SSH 连接

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

将规则添加到现有安全组以允许到特定 Amazon Linux WorkSpace 的入站 SSH 流量

1. 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，键入要为其启用 SSH 连接的 WorkSpace 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 Save。

使用 Linux 或 PuTTY 连接到 Amazon Linux WorkSpace

在创建或更新安全组并添加所需规则后，您的用户及其他人可以使用 Linux 或 PuTTY 从其设备连接到 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。
> - 用于连接到 WorkSpace 的用户名。
> - 要连接到的 WorkSpace 的公有或私有 IP 地址。
>
> 有关如何获取此信息的说明，请参阅本主题前面的“与 Amazon Linux WorkSpaces 的 SSH 连接的先决条件”。

使用 Linux 连接到 Amazon Linux WorkSpace

1. 以管理员身份打开命令提示符并输入以下命令。对于 *NetBIOS name*, *Username*, 和 *WorkSpace IP*下，输入适用的值。

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

以下是 SSH 命令的示例，其中：

- 这些区域有：*NetBIOS_NAME* 是任何公司
- 这些区域有：*Username* 是 janedo
- 这些区域有：*WorkSpace IP* 为 203.0.113.25

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

2. 系统提示时，输入在使用 WorkSpaces 客户端进行身份验证时使用的同一个密码（您的 Active Directory 密码）。

使用 PuTTY 连接到 Amazon Linux WorkSpace

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。将这些值分别替换为要连接到的 Active Directory 域的 NetBIOS 名称、用于连接到 WorkSpace 的用户名和要连接到的 WorkSpace 的 IP 地址。

     ```
     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 Open。
4. 系统提示时，输入在使用 WorkSpaces 客户端进行身份验证时使用的同一个密码（您的 Active Directory 密码）。

WorkSpace 的必需配置和服务组件

作为 WorkSpace 管理员，您必须了解以下有关必需的配置和服务组件的内容。

必需路由表配置

我们建议不要为 WorkSpace 修改操作系统级别的路由表。WorkSpaces 服务要求此表中有预配置路由，用于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 AWS Support 或 AWS 客户团队。

必需服务组件

在 Windows 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。如果您这样做，WorkSpace 将无法正常运行。

如果 WorkSpace 上安装了防病毒软件，请确保它不会干扰以下位置安装的服务组件。

Important

从 2021 年 3 月 29 日开始，我们正在将 PCoIP 代理从 32 位更新为 64 位。对于正在使用 PCoIP 协议的 Windows WorkSpaces，这意味着 Teradici 文件的位置从`C:\Program Files (x86)\Teradici`到`C:\Program Files\Teradici`。这些 PCoIP 代理更新将在我们的常规维

护窗口中波动进行，这意味着您的某些 WorkSpaces 可能正在使用 32 位代理，有些可能在此过渡期间使用 64 位代理。
如果您已配置防火墙规则、防病毒软件排除（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 端点配置管理器或基于完整配置管理器的类似配置管理工具的设置路径指向 32 位代理，还必须将 64 位代理的完整路径添加到这些设置。
由于您的 WorkSpaces 可能并非全部同时升级，因此不要用 64 位路径替换 32 位路径，或者您的某些 WorkSpaces 可能无法正常工作。例如，如果您将排除项或通信过滤器基于`C:\Program Files (x86)\Teradici\PCoIP Agent\bin\pcoip_server_win32.exe`，则必须添加`C:\Program Files\Teradici\PCoIP Agent\bin\pcoip_server.exe`。

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

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。如果您这样做，WorkSpace 将无法正常运行。

- /etc/dhcp/dh客户端.conf
- /etc/os-release
- /etc/pam.d/pcoip
- /etc/pam.d/pcoip-session
- /etc/profile.d/system-restart-check.sh
- /etc/X11/default-display-manager
- /etc/yum/pluginconf.d/halt_os_update_check.conf
- /usr/lib/pcoip-agent
- /usr/lib/skylight
- /usr/lib/system/systemm/pcoip.service
- /usr/lib/system/systemm/pcoip.service d/
- /usr/lib/system/systemm/skylight-agent.service
- /usr/lib/yum-plugins/halt_os_update_check.py
- /var/lib/pcoip-agent
- /var/lib/skylight
- /var/log/pcoip-agent
- /var/log/skylight

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 —创建托管在AWS。
- 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。
- 交叉信任—在AWS Managed Microsoft AD目录和本地域。

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 (p. 66)。

Tip

有关各种部署方案的目录和虚拟私有云 (VPC) 设计注意事项的详细探索，请参阅 部署的最佳实践 Amazon WorkSpaces白皮书。

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 WorkSpaces 用户 (p. 78)和为 WorkSpaces 设置 Active Directory 管理工具 (p. 63)。

Note

- 目前不支持与共享目录结合使用Amazon WorkSpaces。
- 如果您配置AWS用于多区域复制的托管 Microsoft AD 目录，只有主区域中的目录可以注册以便与 Amazon WorkSpaces。尝试注册复制区域中的目录，以便与Amazon WorkSpaces将失败。多区域复制AWS托管微软 AD 不支持与Amazon WorkSpaces在复制的区域内。
- Simple AD和AD Connector可供您免费使用，以便与 WorkSpaces 一起使用。如果没有 WorkSpaces 与Simple AD或者AD Connector目录中连续 30 天，此目录将自动取消注册，以便与 Amazon WorkSpaces，并且您将根据AWS Directory Service定价条款。

  要删除空目录，请参阅删除您的 WorkSpace 目录 (p. 62)。如果您删除Simple AD或者AD Connector目录中，当您想要重新开始使用 WorkSpaces 时，您始终可以创建一个新的目录。

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。

Requirements

注册目录以与WorkSpaces，则必须满足以下要求：

- 要注册以与Amazon WorkSpaces必须存在于您要启动 WorkSpaces 的每个虚拟私有云 (VPC) 子网中。
- 如果您使用的是AD Connector，您的AD Connector必须直接连接到将用于 WorkSpaces 部署的同一 VPC 的子网。
- 如果您使用的是AWS Managed Microsoft AD或者Simple AD，只要目录可以访问 WorkSpaces 所在的 VPC，您的目录就可以位于专用私有子网中。

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

> **Note**
>
> Simple AD和AD Connector可供您免费使用，以便与 WorkSpaces 一起使用。如果没有 WorkSpaces 与Simple AD或者AD Connector目录中连续 30 天，此目录将自动取消注册，以便与 Amazon WorkSpaces，并且您将根据AWS Directory Service定价条款。
> 要删除空目录，请参阅删除您的 WorkSpace 目录 (p. 62)。如果您删除Simple AD或者AD Connector目录中，当您想要重新开始使用 WorkSpaces 时，您始终可以创建一个新的目录。

注册目录

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

   > **Note**
   >
   > - 目前不支持与共享目录结合使用Amazon WorkSpaces。
   > - 如果您的AWS Managed Microsoft AD目录已配置为多区域复制，则只有主区域中的目录可以注册以便与Amazon WorkSpaces。尝试注册复制区域中的目录，以便与 Amazon WorkSpaces将失败。多区域复制AWS Managed Microsoft AD不支持与Amazon WorkSpaces在复制的区域内。
5. 选择来自不同可用区的两个子网。
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支付的费用Amazon WorkSpaces。否则，请选择否。
7. 对于 Enable Amazon WorkDocs，要注册目录以便用于 ，则选择 YesAmazon WorkDocs，否则，选择 No。

   > **Note**
   >
   > 此选项仅在Amazon WorkDocs在区域中可用，并且您不使用AWS Managed Microsoft AD。如果您使用的是AWS Managed Microsoft AD，完成注册目录，然后查看启用Amazon WorkDocsAWS Managed Microsoft AD (p. 63)。
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 。删除目录中的AWS Directory Service Administration Guide。

取消注册目录

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

更新您的 WorkSpace 目录详细信息

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

WorkSpace 计算机账户放在 WorkSpace 目录的默认组织单位 (OU) 中。最初，计算机帐户放在您的目录的“计算机” OU 中，或AD Connector已连接到。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。

在选择一个新的 OU 后，所有创建的或是重建的 WorkSpace 的计算机账户都放在新选定的 OU 中。

要选择组织单位

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Directories。
3. 选择您的目录，然后选择 Actions、Update Details。
4. 展开 Target Domain and Organizational Unit。
5. 要查找一个 OU，可以键入该 OU 的全部或部分名称并选择 Search OU。或者，可以选择 List all OU 以列出所有 OU。
6. 选择 OU 并选择 Update and Exit。
7. (可选) 重建现有的 WorkSpace 以更新 OU。有关更多信息，请参阅 重建 WorkSpace (p. 111)。

要指定目标域和组织单位

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Directories。
3. 选择您的目录，然后选择 Actions、Update Details。
4. 展开 Target Domain and Organizational Unit。
5. 对于 Selected OU，键入目标域和 OU 的完整 LDAP 可分辨名称，然后选择 Update and Exit。例如，**`OU=WorkSpaces_machines,DC=machines,DC=example,DC=com`**。
6. (可选) 重建现有的 WorkSpace 以更新 OU。有关更多信息，请参阅 重建 WorkSpace (p. 111)。

配置自动 IP 地址

启用弹性 IP 地址自动分配后，会从 Amazon 提供的弹性 IP 地址池中为您启动的每个 WorkSpace 分配一个弹性 IP 地址（静态公有 IP 地址）。这些弹性 IP 地址允许公有子网中的 WorkSpace 访问 Internet。在启用自动分配之前已经存在的 WorkSpace 不会收到弹性 IP 地址，直到您重新构建它们。

请注意，如果您的 WorkSpace 处于私有子网中并且您为 Virtual Private Cloud (VPC) 配置了 NAT 网关，或者如果您的 WorkSpace 位于公有子网中并且您手动分配了弹性 IP 地址，则无需启用弹性 IP 地址的自动分配功能。有关更多信息，请参阅 为 配置 VPCWorkSpaces (p. 9)。

Warning

如果您将您拥有的弹性 IP 地址与 WorkSpace 关联，稍后您将该弹性 IP 地址与 WorkSpace 取消关联，则 WorkSpace 将失去其公有 IP 地址，并且不会自动从 Amazon 提供的池中获取新的 IP 地址。要将 Amazon 提供的池中的新公有 IP 地址与 WorkSpace 关联，您必须重建 WorkSpace (p. 111)。如果您不想重建 WorkSpace，必须将您拥有的另一个弹性 IP 地址与 WorkSpace 关联。

配置弹性 IP 地址

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Directories。
3. 选择您的 WorkSpace 目录。
4. 选择 Actions、Update Details。
5. 展开 Access to Internet，选择 Enable 或 Disable。
6. 选择 Update。

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)。

控制设备对 WorkSpace 的访问

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Directories。
3. 选择目录，然后选择 Actions、Update Details。
4. 展开 Access Control Options，找到 Other Platforms 部分。默认情况下，禁用 WorkSpaces Web Access 和 Linux 客户端，用户可以从其 iOS 设备、Android 设备、Chromebook 和 PCoIP 零客户端设备访问其 WorkSpace。
5. 选择要启用的设备类型并清除要禁用的设备类型。要阻止来自所有选定设备类型的访问，请选择 Block。
6. （可选）还可以将访问仅限定于受信任的设备。有关更多信息，请参阅 限制对受信任设备的 WorkSpaces 访问 (p. 33)。
7. 选择 Update and Exit。

管理本地管理员权限

您可以指定用户在其 WorkSpace 上是否为本地管理员，以决定他们能否在其 WorkSpace 上安装应用程序并修改设置。默认情况下，用户为本地管理员。如果修改此设置时，则更改将应用到您创建的所有新的 WorkSpace 以及重建的任何 WorkSpace。

修改本地管理员权限

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Directories。
3. 选择您的目录，然后选择 Actions、Update Details。
4. 展开 Local Administrator Setting。
5. 要确保用户为本地管理员，请选择 Enable。否则，请选择 Disable。
6. 选择 Update and Exit。

更新 AD Connector 账户 (AD Connector)

您可以更新用于读取用户和组以及将 WorkSpaces 计算机账户加入到您的 AD Connector 目录的 AD Connector 账户。

更新 AD Connector 账户

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Directories。
3. 选择您的目录，然后选择 Actions、Update Details。
4. 展开 Update AD Connector Account。
5. 键入新账户的用户名和密码。
6. 选择 Update and Exit。

多重验证 (AD Connector)

您可以为 AD Connector 目录启用多重验证 (MFA)。有关多重验证与AWS Directory Service，请参阅为启用多重验证AD Connector和 AD Connector先决条件。

Note

- 您的 RADIUS 服务器可以由AWS也可以为本地。
- 活动目录和 RADIUS 服务器之间的用户名必须匹配。

启用多重验证

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Directories。
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 服务器终端节点的 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通过默认的 RADIUS 服务器端口 (UDP: 1812) 从传入站流量AD Connector。
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 Update and Exit。

当 RADIUS Status 为 Enabled 时，多重验证可用。在设置多重验证期间，用户无法登录其 WorkSpace。

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 服务器设置来更新 WorkSpaces。

您可以通过下列方式之一，使用新的 DNS 设置更新 WorkSpaces：

- 在更新 Active Directory 的 DNS 设置WorkSpaces之前，更新 上的 DNS 设置。
- 在更新 Active Directory 的 DNS 设置WorkSpaces之后重新生成 。

我们建议在更新 Active Directory 中的 DNS 设置之前，先更新 WorkSpaces 上的 DNS 设置（如以下过程的步骤 1 (p. 58) 中所述）。

如果要改为重建 WorkSpaces，请更新 Active Directory 中的 DNS 服务器 IP 地址之一（步骤 2 (p. 60)），然后按照重建 WorkSpace (p. 111)中的过程来重建 WorkSpaces。 重建 WorkSpaces 后，请按照步骤 3 (p. 60) 中的过程来测试您的 DNS 服务器更新。完成该步骤后，请更新 Active Directory 中第二个 DNS 服务器的 IP 地址，然后再次重新生成 WorkSpaces。请务必按照步骤 3 (p. 60) 中的过程测试您的第二个 DNS 服务器更新。如 最佳实践 (p. 58)部分中所述，我们建议一次更新您的 DNS 服务器 IP 地址。

最佳实践

在更新 DNS 服务器设置时，我们建议使用以下最佳实践：

- 为避免域资源断开连接且无法访问，我们强烈建议在非高峰时间或计划的维护期内执行 DNS 服务器更新。
- 请勿在 15 分钟前和更改 DNS 服务器设置后的 15 分钟内启动任何新的WorkSpaces。
- 在更新 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，验证第一个更新是否正确。我们建议执行以下过程（步骤 1 (p. 58)、步骤 2 (p. 60) 和步骤 3 (p. 60)）两次，一次更新一个 IP 地址。

步骤 1：更新 WorkSpaces 上的 DNS 服务器设置

在以下过程中，当前和新的 DNS 服务器 IP 地址值引用如下：

- 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，请将 *OldIP1* 替换为 *OldIP2*，将 *NewIP1* 替换为 *NewIP2*。

更新 Windows WorkSpaces 的 DNS 服务器设置

如果您有多个 WorkSpaces，则可通过在 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 GPOs 的更多信息，请参阅管理 Windows WorkSpace (p. 83)。

您可以使用注册表编辑器或使用 Windows PowerShell 来进行这些更新。 本节介绍了这两个过程。

使用注册表编辑器更新 DNS 注册表设置

1. 在 Windows WorkSpace 上，打开 Windows 搜索框，然后输入 **`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 *OldIP1* 更新 *NewIP1*，然后选择 OK（确定）。
5. 关闭注册表编辑器。
6. 重启 WorkSpace，或重启服务 SkyLightWorkspaceConfigService。

   Note

   重新启动服务 SkyLightWorkspaceConfigService 后，网络适配器最多可能需要 1 分钟才能反映更改。
7. 继续执行步骤 2 (p. 60)，并更新 Active Directory 中的 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 命令更新您的注册表并重新启动服务 SkyLightWorkspaceConfigService。

1. 在 Windows WorkSpace 上，打开 Windows 搜索框，然后输入 **powershell**。 选择 Run as Administrator（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 DNS 服务器 IP 地址。

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

   您应该会收到以下输出。

```
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，运行以下命令以将 *OldIP1* 更改为 *NewIP1*。 目前，请确保按原样保留 *OldIP2*。

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

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

```
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 分钟才能反映更改。
6. 继续执行步骤 2 (p. 60)，并更新 Active Directory 中的 DNS 服务器设置，将 *OldIP1* 替换为 *NewIP1*。

更新 Linux WorkSpaces 的 DNS 服务器设置

如果您有多个 Linux WorkSpace，我们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 Chef Automate 、AWS for Puppet EnterpriseOpsWorks 或 Ansible。

更新 Linux 上的 DNS 服务器设置 WorkSpace

1. 在 Linux WorkSpace 上，打开终端窗口（Applications（应用程序）> System Tools（系统工具）> MATE Terminal（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。使用 `sudo -i` 命令变为根，或使用 `sudo` 执行所有命令，如下所示。

   ```
   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 *`NewIP1`*，并保持 *`OldIP2`* 不变。
4. 将您的更改保存到 `/etc/dhcp/dhclient.conf`。
5. 重启 WorkSpace。
6. 继续执行步骤 2 (p. 60)，并更新 Active Directory 中的 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 (p. 58)部分中所述，我们建议一次更新您的 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 Administration Guide 中的以下文档：

- AD Connector：更新您的 AD Connector 的 DNS 地址
- AWS 托管的 Microsoft AD：为您的本地域配置 DNS 条件转发服务器
- Simple AD：配置 DNS

更新 DNS 服务器设置后，请继续执行步骤 3 (p. 60)。

步骤 3：测试更新的 DNS 服务器设置

完成步骤 1 (p. 58) 和步骤 2 (p. 60) 后，使用以下过程验证更新的 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 地址值引用如下：

- 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，请将 *`OldIP1`* 替换为 *`OldIP2`*，将 *`NewIP1`* 替换为 *`NewIP2`*。

测试 Windows WorkSpaces 的更新后的 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 Active Directory 的名称（例如，corp.example.com）。

```
nslookup AD_Name
```

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

```
Server:  Full_AD_Name
Address:  NewIP1

Name:    AD_Name
Addresses:  OldIP2
          NewIP1
```

5. 如果输出不符合您的预期，或者您收到任何错误，请重复步骤 1 (p. 58)。
6. 等待一个小时并确认没有报告任何用户问题。验证 *NewIP1* 正在获取 DNS 查询并使用应答进行响应。
7. 在确认第一个 DNS 服务器正常工作后，请重复步骤 1 (p. 58) 以更新第二个 DNS 服务器，这次请将 *OldIP2* 替换为 *NewIP2*。然后，重复步骤 2 和步骤 3。

测试 Linux WorkSpaces 的更新 DNS 服务器设置

1. 关闭 *OldIP1* DNS 服务器。
2. 登录 Linux WorkSpace。
3. 在 Linux WorkSpace 上，打开终端窗口（Applications（应用程序）> System Tools（系统工具）> MATE Terminal（MATE 终端））。
4. DHCP 响应中返回的 DNS 服务器 IP 地址将写入到 /etc/resolv.conf 上的本地 WorkSpace 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* 代替 *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

如果您手动修改 /etc/resolv.conf 文件，这些更改将在 WorkSpace重新启动时丢失。

5. 如果输出不符合您的预期，或者您收到任何错误，请重复步骤 1 (p. 58)。
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* 代替 *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. 等待一个小时并确认没有报告任何用户问题。验证 *NewIP1* 正在获取 DNS 查询并使用应答进行响应。
8. 在确认第一个 DNS 服务器正常工作后，请重复步骤 1 (p. 58) 以更新第二个 DNS 服务器，这次请将 *OldIP2* 替换为 *NewIP2*。 然后，重复步骤 2 和步骤 3。

删除您的 WorkSpace 目录

如果您的 WorkSpace 目录不再被其他 WorkSpace 或其他应用程序（如 Amazon WorkDocs、Amazon WorkMail 或 Amazon Chime）使用，则可将其删除。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可供您免费使用，以便与 WorkSpaces 一起使用。如果没有 WorkSpaces 与Simple AD或者AD Connector目录中连续 30 天，此目录将自动取消注册，以便与 Amazon WorkSpaces，并且您将根据AWS Directory Service定价条款。
> 如果您删除Simple AD或者AD Connector目录中，当您想要重新开始使用 WorkSpaces 时，您始终可以创建一个新的目录。

删除目录时会发生什么

删除 Simple AD 或 AWS Directory Service for Microsoft Active Directory（企业版）目录时，所有目录数据和快照都会删除，并且无法恢复。删除该目录后，任何Amazon EC2实例保持不变。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用户账户登录这些实例。

删除 AD Connector 目录时，本地目录保持不变。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. 删除目录中的所有工作区。有关更多信息，请参阅 删除工作区 (p. 122)。
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 。删除目录中的AWS Directory Service Administration Guide。
3. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
4. 在导航窗格中，选择 Directories。
5. 选择目录，然后选择 Actions、Deregister。
6. 当系统提示您确认时，选择 Deregister。
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 Virtual Private Cloud (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 。删除 VPC和使用弹性 IP 地址中的Amazon VPC 用户指南。
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 WorkSpace 服务包或映像 (p. 138)。

启用Amazon WorkDocsAWS Managed Microsoft AD

如果您使用的是 AWS Managed Microsoft AD 与Amazon WorkSpaces，您可以启用Amazon WorkDocs为您的目录通过Amazon WorkDocs控制台或AWS Directory Service控制台。

> Note
>
> Amazon WorkDocs并未在所有 AWS 区域提供Amazon WorkSpaces可以使用。有关更多信息，请参阅 Amazon WorkDocs 定价。

通过 Amazon WorkDocs 控制台启用 WorkDocs

1. 从 https://console.aws.amazon.com/zocalo/ 打开 Amazon WorkDocs 控制台。
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 。AWS Managed Microsoft AD 入门中的Amazon WorkDocs 管理指南。

通过 AWS Directory Service 控制台启用 WorkDocs

1. 通过以下网址打开 AWS Directory Service 控制台：https://console.aws.amazon.com/directoryservicev2/。
2. 在导航窗格中，选择 Directories。
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 。创建访问 URL中的AWS Directory Service Administration Guide。
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 。单点登录中的AWS Directory Service Administration Guide。

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 (p. 53)。

如果创建拥有 AWS 托管的 Microsoft AD 或 Simple AD 的目录，其中包含五个或更多个 WorkSpaces，我们建议您在Amazon EC2实例。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Amazon EC2Windows 实例并使用以下选项之一将其加入到 WorkSpaces 目录中：
   - 如果您还没有现有Amazon EC2Windows 实例，您可以在启动实例时将实例加入到目录域。有关更多信息，请参阅 。无缝加入 Windows EC2 实例中的AWS Directory Service Administration Guide。

- 如果您已有Amazon EC2Windows 实例，您可以手动将其加入到目录中。有关更多信息，请参阅 。手动添加 Windows 实例中的AWS Directory Service Administration Guide。

2. 在Amazon EC2Windows 实例。有关更多信息，请参阅 https://docs.aws.amazon.com/directoryservice/latest/admin-guide/install_ad_tools.html 中的AWS Directory Service Administration Guide安装 Active Directory 管理工具。

   Note

   安装活动目录管理工具时，请确保还选择组策略管理以安装组策略管理编辑器 (gpmc.msc) 工具。

   当该功能安装完成后，Active Directory 工具将出现在 Windows 上启动菜单Windows 管理工具。
3. 按照如下步骤以目录管理员身份运行工具：

   a. 在 Windows 上启动菜单中，打开Windows 管理工具。
   b. 按住 Shift 键，右键单击要使用的工具的快捷方式，然后选择以不同用户身份运行。
   c. 键入管理员的用户名和密码。对于 Simple AD，用户名为**`Administrator`**，对于 AWS 托管的 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 Managed AD。有关使用 AWS 托管 AD 创建的目录，请参阅在 AWS 托管的 Microsoft AD 中管理用户和组中的AWS Directory Service Administration Guide。

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，选择成员。
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 删除工作区 (p. 122)。

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 托管的 Microsoft AD，请参阅在 AWS 托管的 Microsoft AD 中管理用户和组中的AWS Directory Service Administration Guide。
- 如果您使用的是 Simple AD，请参阅在 Simple AD 中管理用户和组中的AWS Directory Service Administration Guide。
- 如果通过 AD Connector 或信任关系使用 Microsoft Active Directory，则可以使用 Active Directory 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。（忘记密码？选 WorkSpaces 将不可用。）

使用 WorkSpaces 启动虚拟桌面

借助 WorkSpaces，您可以为用户预置基于云的虚拟 Microsoft Windows 或 Amazon Linux 桌面（称为 WorkSpace）。

Note

这些区域有：Computer Name值中显示的 WorkSpaceAmazon WorkSpaces控制台会有所不同，具体取决于您启动的 WorkSpace 类型（Linux 或 Windows）。WorkSpace Spaces 的计算机名称可以是下列格式之一：

- Linux：A-1*xxxxxxxxxxxx*
- Windows: IP C*xxxxxx* 或西萨姆津-*xxxxxxx* 或东非经济共同体-*xxxxxxx*

对于 Windows WorkSpaces，计算机名称格式由捆绑类型决定，如果是从公共捆绑或基于公共映像的自定义捆绑包创建 WorkSpaces，则取决于创建公用映像的时间。
从 2020 年 6 月 22 日起，从公共捆绑包启动的 Windows WorkSpaces 具有*xxxxxxx* 格式的计算机名称，而不是 IP-C*xxxxxx* 格式的日期和时间。
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，则计算机名称位于 EC2AMAZ-*xxxxxxx* 格式的日期和时间。如果公共映像是在 2020 年 6 月 22 日或之后创建的，则计算机名称位于 WSAMZN-*xxxxxxx* 格式的日期和时间。
对于自带许可 (BYOL) 捆绑，*xxxxxxx* 或欧洲经济共同体代表团-*xxxxxxx* 格式默认用于计算机名称。
如果在自定义或 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值。若要指定自定义格式，请参阅创建自定义 WorkSpace 映像和服务包 (p. 123)。

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

- 目前不支持共享目录用于Amazon WorkSpaces。
- 如果您配置AWS用于多区域复制的托管 Microsoft AD 目录，只有主区域中的目录可以注册以便与 Amazon WorkSpaces。尝试注册复制区域中的目录，以便与Amazon WorkSpaces将失败。多区域复制AWS托管微软 AD 不支持与Amazon WorkSpaces在复制的区域内。
- Simple AD和AD Connector可供您免费使用，以便与 WorkSpaces 一起使用。如果没有任何 WorkSpaces 正在与Simple AD或者AD Connector目录中连续 30 天，此目录将自动取消注册，以便与Amazon WorkSpaces，并且您将根据AWS Directory Service定价条款。

  要删除空目录，请参阅删除您的 WorkSpace 目录 (p. 62)。如果删除Simple AD或者AD Connector目录中，当您想要重新开始使用 WorkSpaces 时，您始终可以创建一个新的目录。

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 托管的 Microsoft AD 的 WorkSpace (p. 67)

启动使用 AWS 托管的 Microsoft AD 的 WorkSpace

借助 WorkSpaces，您可以为用户预置基于云的虚拟 Windows 桌面（称为 WorkSpace）。

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 (p. 66)。

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 WorkSpace 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 配置 VPCWorkSpaces (p. 9)。

步骤 1: 创建AWS托管 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

- 目前不支持共享目录与Amazon WorkSpaces。
- 如果您的AWS已将托管 Microsoft AD 目录配置为多区域复制，只有主区域中的目录可以注册以便与Amazon WorkSpaces。尝试注册复制区域中的目录，以便与Amazon WorkSpaces将失败。多区域复制AWS托管微软 AD 不支持与Amazon WorkSpaces在复制的区域内。

创建 AWS 托管的 Microsoft AD 目录

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Directories。
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 (p. 57)以确保正确更新您的 WorkSpaces。
   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 中的创建您的 AWS Directory Service Administration Guide 托管的 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. 通过以下网址打开 WorkSpaces 控制台：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 (选择目录) 页面上，选择您创建的目录，然后选择 Next Step (下一步)。WorkSpaces 将注册您的目录。
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。
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。
9. （可选）如果Amazon WorkDocs在区域中受支持，则可以启用Amazon WorkDocs目录中的所有用户。有关更多信息，请参阅 启用Amazon WorkDocsAWS Managed Microsoft AD (p. 63)。有关 的更多信息 Amazon WorkDocs，请参阅 Amazon WorkDocsDrive中的Amazon WorkDocs 管理指南。

步骤 3: Connect 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)。密码必须混合使用以下四类字符：小写字母 (a-z)、大写字母 (A-Z)、数字 (0-9) 以及~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/。
2. 审核WorkSpaces客户中的Amazon WorkSpaces 用户指南以了解有关每个客户端的要求的更多信息，然后执行以下操作之一：

   - 根据系统提示，下载一个客户端应用程序或启动 Web Access。
   - 如果您未看到提示且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 LinuxWorkSpaces。
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. 当系统提示您登录时，输入用户的用户名和密码，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。您还可以为工作空间和 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 WorkSpace 映像和服务包 (p. 123)
- 管理您的 WorkSpace (p. 83)
- 管理 WorkSpaces 目录 (p. 53)
- 删除工作区 (p. 122)

有关使用 WorkSpaces 客户端应用程序（如设置多个显示器或使用外围设备）的详细信息，请参阅WorkSpaces客户和外围设备支持中的Amazon WorkSpaces 用户指南。

启动使用 Simple AD 的 WorkSpace

借助 WorkSpaces，您可以为用户预置基于云的虚拟 Microsoft Windows 桌面（称为 WorkSpace）。

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 (p. 66)。

任务

- 开始前的准备工作 (p. 70)
- 步骤 1: 创建 Simple AD 目录 (p. 70)

开始前的准备工作

- Simple AD 并非在所有区域均可用。验证支持的区域和选择区域为您的Simple AD目录。有关支持的区域的更多信息，Simple AD，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 WorkSpace 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 配置 VPCWorkSpaces (p. 9)。

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向您提供免费使用 WorkSpaces。如果没有 WorkSpaces 与Simple AD目录中连续 30 天，此目录将自动取消注册，以便与Amazon WorkSpaces，并且您将根据AWS Directory Service 定价条款。
> 要删除空目录，请参阅删除您的 WorkSpace 目录 (p. 62)。如果您删除Simple AD目录中，当您想要重新开始使用 WorkSpaces 时，您始终可以创建一个新的目录。

创建 Simple AD 目录

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Directories。
3. 选择设置目录、Simple AD, 和下一页。
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. 适用于目录 DNS 名称中，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 (p. 57)以确保正确更新您的 WorkSpaces。

   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 https://docs.aws.amazon.com/directoryservice/latest/admin-guide/create_managed_ad.html 中的 AWS Directory Service Administration Guide如何创建 Microsoft AD 目录。
   e. （可选）对于描述，输入目录的描述。
   f. 适用于目录大小中，选择小型。
   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。

5. 选择创建目录。
6. 目录的初始状态是 `Requested`，然后是 `Creating`。目录创建完毕后（这可能需要几分钟时间），状态会变为`Active`。

目录创建

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. 通过以下网址打开 WorkSpaces 控制台：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. 适用于启用自助服务权限中，选择是或者否并输入说明。
   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. 选择下一步。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。
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（最多可能需要 20 分钟时间），状态会变为`AVAILABLE`并向您为用户指定的电子邮件地址发送一封邀请电子邮件。

步骤 3: Connect 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)。密码必须使用以下每类字符：小写字母 (a-z)、大写字母 (A-Z)、数字 (0-9) 以及~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/。
2. 审核WorkSpaces客户中的Amazon WorkSpaces 用户指南以了解有关每个客户端的要求的更多信息，然后执行以下操作之一：

   - 根据系统提示，下载一个客户端应用程序或启动Web 访问。
   - 如果您未看到提示且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 访问。

   Note

   您不能使用 Web 浏览器（Web Access）连接到Amazon LinuxWorkSpaces。
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. 当系统提示您登录时，输入用户的用户名和密码，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。您还可以为工作空间和 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 WorkSpace 映像和服务包 (p. 123)
- 管理您的 WorkSpace (p. 83)
- 管理 WorkSpaces 目录 (p. 53)
- 删除工作区 (p. 122)

有关使用 WorkSpaces 客户端应用程序（如设置多个显示器或使用外围设备）的详细信息，请参阅WorkSpaces客户和外围设备支持中的Amazon WorkSpaces 用户指南。

启动使用 AD Connector 的 WorkSpace

借助 WorkSpaces，您可以为用户预置基于云的虚拟 Microsoft Windows 桌面（称为 WorkSpace）。

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 (p. 66)。

任务

- 开始前的准备工作 (p. 73)
- 步骤 1: 创建 AD Connector (p. 73)

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 WorkSpace 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 配置 VPCWorkSpaces (p. 9)。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 https://docs.aws.amazon.com/directoryservice/latest/admin-guide/prereq_connector.html 中的 AWS Directory Service Administration GuideAD Connector 先决条件。
- 从 WorkSpace 提供对 Internet 的访问。有关更多信息，请参阅 提供 WorkSpace 的 Internet 访问权限 (p. 40)。

步骤 1: 创建 AD Connector

> Note
>
> AD Connector向您提供免费使用，以便与 WorkSpaces 一起使用。如果没有任何 WorkSpaces 正在与AD Connector目录中连续 30 天，此目录将自动取消注册，以便与Amazon WorkSpaces，并且您将根据AWS Directory Service定价条款。
> 要删除空目录，请参阅删除您的 WorkSpace 目录 (p. 62)。如果您删除AD Connector目录中，当您想要重新开始使用 WorkSpaces 时，您始终可以创建一个新的目录。

创建 AD Connector

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Directories。
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，输入本地用户账户的密码。
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 (p. 57)以确保正确更新您的 WorkSpaces。
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. 通过以下网址打开 WorkSpaces 控制台：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 的更多信息Amazon WorkDocs，请参阅Amazon WorkDocsDrive中的Amazon WorkDocs 管理指南。
6. 选择 Next (下一步)。WorkSpaces 将注册您的 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。
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 (p. 99)。
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 (p. 79)。

步骤 3: Connect 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. 审核WorkSpaces客户中的Amazon WorkSpaces 用户指南，了解有关每个客户端的要求的更多信息，然后执行以下操作之一：

   - 根据系统提示，下载一个客户端应用程序或启动 Web Access。
   - 如果您未看到提示且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 LinuxWorkSpaces。
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. 当系统提示您登录时，输入用户的用户名和密码，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 (p. 63)。

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。您还可以为工作空间和 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 WorkSpace 映像和服务包 (p. 123)
- 管理您的 WorkSpace (p. 83)
- 管理 WorkSpaces 目录 (p. 53)
- 删除工作区 (p. 122)

有关使用 WorkSpaces 客户端应用程序（如设置多个显示器或使用外围设备）的详细信息，请参阅WorkSpaces客户和外围设备支持中的Amazon WorkSpaces 用户指南。

启动使用受信任域的 WorkSpace

借助 WorkSpaces，您可以为用户预置基于云的虚拟 Microsoft Windows 桌面（称为 WorkSpace）。

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 (p. 66)。

任务

- 开始前的准备工作 (p. 75)
- 步骤 1: 建立信任关系 (p. 76)
- 步骤 2: 创建 WorkSpace (p. 76)
- 步骤 3: Connect WorkSpace (p. 76)
- 后续步骤 (p. 77)

开始前的准备工作

- 在单独的受信任域中使用用户帐户启动 WorkSpaces 与AWS将 Microsoft AD 配置为与内部部署目录的信任关系时进行管理。但是，使用简单 AD 或 AD Connector 的工作空间无法为来自受信任域的用户启动工作空间。
- WorkSpaces 并非在所有区域均可用。请确认受支持的区域，并为您的 WorkSpace 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 配置 VPCWorkSpaces (p. 9)。

步骤 1: 建立信任关系

设置信任关系

1. 在您的 Virtual Private Cloud (VPC) 中设置 AWS 托管的 Microsoft AD。有关更多信息，请参阅 AWS 中的创建 AWS Directory Service Administration Guide 托管的 Microsoft AD 目录。

   Note

   - 目前不支持共享目录与Amazon WorkSpaces。
   - 如果您的AWS已将托管 Microsoft AD 目录配置为多区域复制，只有主区域中的目录可以注册以便与Amazon WorkSpaces。尝试注册复制区域中的目录，以便与Amazon WorkSpaces将失败。使用多区域复制AWS托管微软 AD 不支持与Amazon WorkSpaces在复制的区域内。
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 。教程：创建您的AWS托管的微软 AD 和您的内部部署域中的AWS Directory Service Administration Guide。

需要双向信任，以便可以使用本地凭证来管理 WorkSpace，向 WorkSpace 进行身份验证，并且可以向本地用户和组预置 WorkSpace。

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置 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 WorkSpace

1. 通过以下网址打开 WorkSpaces 控制台：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。
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。有关更多信息，请参阅 发送邀请电子邮件 (p. 79)。

步骤 3: Connect 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)。密码必须混合使用以下类字符：小写字母 (a-z)、大写字母 (A-Z)、数字 (0-9) 以及~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/。
2. 审核WorkSpaces客户中的Amazon WorkSpaces 用户指南以了解有关每个客户端的要求的更多信息，然后执行以下操作之一：

   - 根据系统提示，下载一个客户端应用程序或启动 Web Access。
   - 如果您未看到提示且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 LinuxWorkSpaces。
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. 当系统提示您登录时，输入用户的用户名和密码，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。您还可以为工作空间和 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 WorkSpace 映像和服务包 (p. 123)
- 管理您的 WorkSpace (p. 83)
- 管理 WorkSpaces 目录 (p. 53)
- 删除工作区 (p. 122)

有关使用 WorkSpaces 客户端应用程序（如设置多个显示器或使用外围设备）的详细信息，请参阅WorkSpaces客户和外围设备支持中的Amazon WorkSpaces 用户指南。

管理 WorkSpace 用户

每个 WorkSpace 分配给单个用户，无法由多个用户共享。默认情况下，每个目录的每个用户只允许一个 WorkSpace。

目录

管理 WorkSpaces 用户

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

编辑用户信息

您可以使用 WorkSpaces 控制台编辑WorkSpace的用户信息。

> Note
>
> 仅当您使用 AWS 托管的 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. 来管理用户和组。

要编辑用户信息

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择一个用户，然后选择 Actions、Edit User.
4. 根据需要更新 First Name、Last Name 和 Email。
5. 选择 Update.

添加或删除用户

您只能在启动 Amazon WorkSpaces 的过程中从 WorkSpace 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。

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）执行 WorkSpaces 目录的大多数管理任务。有关更多信息，请参阅 为 WorkSpaces 设置 Active Directory 管理工具 (p. 63).

> 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 删除工作区 (p. 122).

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 托管的 Microsoft AD，请参阅 https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_manage_users_groups.html 中的管理 AWS 托管的 Microsoft AD 中的用户和组AWS Directory Service Administration Guide。
- 如果您使用的是 Simple AD，请参阅 中的在 Simple AD 中管理用户和组。AWS Directory Service Administration Guide
- 如果通过 AD Connector 或信任关系使用 Microsoft Active Directory，则可以使用 Active Directory. 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，则欢迎电子邮件不会自动发送给您的用户，因此您必须手动发送。

要重新发送邀请电子邮件

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 在 WorkSpaces 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 Actions (操作) 和 Invite User (邀请用户).
5. 使用您自己的电子邮件应用程序，复制电子邮件正文并将其粘贴到要发送给用户的电子邮件中。如果需要，您可以修改正文。当邀请电子邮件准备就绪之后，将其发送给用户。

为用户创建多个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，请为用户创建多个用户名。例如，名为 Mary Major 的用户可以使用 mmajor1、mmajor2 等作为用户名。每个用户名都与同一目录中的不同WorkSpace关联，但WorkSpaces具有相同的注册代码，只要WorkSpaces都在同一 AWS 区域的同一目录中创建即可。
- 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。将具有不同的注册代码。WorkSpaces

Tip

以便您可以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，其用户名为 Active Directory mmajor，则使用用户名（例如 mmajor、mmajor1、mmajor2、mmajor3）或其他变体（例如 mmajor_windows 或 mmajor_linux）为她创建 WorkSpaces。只要所有 WorkSpaces 的起始基本用户名（主要）相同，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 分组到一起。

Important

- 用户可以同时具有 PCoIP 和 WSP WorkSpace，只要两个 WorkSpaces 位于单独的目录中。同一用户不能在同一目录中具有 PCoIP 和 WSP WorkSpace。
- 如果要设置多个 WorkSpaces 以用于跨区域重定向，则必须在不同的 AWS 区域的不同目录中设置 WorkSpaces，并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，请参阅的跨区域重定向 Amazon WorkSpaces (p. 154)。

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

自定义用户登录其 WorkSpaces的方式

通过使用统一资源标识符（WorkSpacesURIURIs 的访问，以提供与您组织内的现有工作流程集成的简化的登录体验。例如，您可以自动生成登录 URIs，使用用户的 WorkSpaces 注册代码注册用户。因此：

- 用户可以跳过手动注册过程。
- 他们的用户名将自动在其 WorkSpaces 客户端登录页上输入。
- 如果在您的组织中使用了多重验证 (MFA)，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代码（例如 `WSpdx+ABC12D`）和基于完全限定域名（FQDN）的注册代码（例如 `desktop.example.com`）。有关创建和使用基于 FQDN 的注册代码的更多信息，请参阅的跨区域重定向 Amazon WorkSpaces (p. 154)。

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

- Windows 计算机
- macOS 计算机
- Ubuntu Linux 18.04 计算机
- iPads
- Android 设备

要使用 URIs 访问其 WorkSpaces，用户必须先打开 https://clients.amazonworkspaces.com/

在 Windows 和 macOS 计算机上的 Firefox 和 Chrome 浏览器、Ubuntu Linux 18.04 计算机上的 Firefox 浏览器以及 Windows 计算机上的 Internet Explorer 和 Microsoft Edge 浏览器上支持 URI 访问。有关 WorkSpaces 客户端的更多信息，请参阅 中的 WorkSpaces 客户端。Amazon WorkSpaces 用户指南

> **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 WorkSpaces 的 URI 访问，请使用下表中所述的任一 URI 格式。

> **Note**
>
> 如果您的 URI 的数据组件包含以下任一预留字符，我们建议您在数据组件中使用百分号编码以避免歧义：
> `@ : / ? & =`
> 例如，如果您有包含任一这些字符的用户名，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 注册代码注册用户。此外，显示客户端登录页。
workspaces://username@registrationcode	使用用户的 WorkSpaces 注册代码注册用户。此外，在客户端登录页上的 username（用户名）字段中自动输入用户名。

支持的语法	描述
workspaces://username@registrationcode?MFACode=mfa	使用用户的 WorkSpaces 注册代码注册用户。此外，在客户端登录页上的 username （用户名）字段中自动输入用户名，在 Multi-Factor Authentication (MFA) 字段中自动输入 Multi-Factor Authentication （MFA）代码。
workspaces://@registrationcode?MFACode=mfa	使用用户的 WorkSpaces 注册代码注册用户。此外，在客户端登录页上的 Multi-Factor Authentication (MFA) 字段中自动输入多重验证（MFA）代码。

Note

如果用户在从 Windows 客户端连接到 WorkSpace 后打开了一个 URI 链接，新的 WorkSpaces 会话将打开，其原始 WorkSpaces 会话将保持打开状态。如果用户在从 WorkSpace、macOS 或 Android 客户端连接到 iPad时打开了 URI 链接，则不会打开任何新会话；只有其原始 WorkSpaces 会话保持打开状态。

为您的用户启用自助服务 WorkSpace 管理功能

在 WorkSpaces 中，您可以为用户启用自助服务 WorkSpace 管理功能，使他们能够更好地控制其体验。这也可以减少 IT 支持人员的 工作负载。WorkSpaces. 当您启用自助服务功能时，您可以允许用户直接从其适用于 macOS 的 Windows、WorkSpaces 或 Linux 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。这使这些用户能够重新连接到 WorkSpace，而无需重新输入凭证。
- 重启（重启）其 WorkSpace。
- 增加其 WorkSpace 上的根卷和用户卷的大小。
- 更改其 WorkSpace 的计算类型（服务包）。
- 切换其 WorkSpace 的运行模式。
- 重新生成其 WorkSpace。

要为您的用户启用这些功能中的一项或多项功能，请执行以下步骤。

为您的用户启用自助服务管理功能

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Directories.
3. 选择目录，然后选择 Actions、Update Details.
4. 展开 User Self-Service Permissions (用户自助服务权限). 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：

   - Remember me (记住我) — 用户可以通过选择登录屏幕上的 Remember me (记住我) 或 Keep me logged in (保持登录状态) 复选框来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证时，他们可以重新连接到其 WorkSpaces，而无需重新输入其凭证。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 (p. 95).
   - 从客户端重启 WorkSpace 用户可以重启（重启）其 —。WorkSpace 重启将断开用户与 WorkSpace 的连接，关闭它，然后重新启动它。用户数据、操作系统和系统设置不受影响。
   - 增加卷大小 — 用户可以将 WorkSpace 上的根卷和用户卷扩展到指定大小，而无需联系 IT 支持。用户可以将根卷的大小（对于 Windows 为 C: 驱动器；对于 Linux 为 /）增加到 175 GB，将用户卷的大小（对于 Windows 为 D: 驱动器；对于 Linux 为 /home）增加到 100 GB。WorkSpace 根卷和用户卷位于无法更改的集合组中。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 (p. 101).

对于新创建的 WorkSpace，用户必须等待 6 小时，然后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。在增加卷大小的过程中，用户可以在其 WorkSpace 上执行大多数任务。 他们无法执行的任务包括：更改其 WorkSpace 计算类型、切换其 WorkSpace 运行模式、重启其 WorkSpace 或重新生成其 WorkSpace。 该过程完成后，必须重新启动 WorkSpace，更改才能生效。此过程可能需要一个小时。

Note

如果用户增加WorkSpace上的卷大小，这将增加其WorkSpace的账单费率。

- 更改计算类型 用户可以在计算类型（包）之间切换 —。WorkSpace对于新创建的 WorkSpace，用户必须等待 6 小时，然后才能切换到不同的服务包。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。在更改 WorkSpace 计算类型时，用户将与其 WorkSpace 断开连接，他们无法使用或更改 WorkSpace。 在计算类型更改过程中将自动重启。WorkSpace此过程可能需要一个小时。

  Note

  如果用户更改 WorkSpace 计算类型，这将更改其 WorkSpace 的账单费率。

- Switch running mode （切换运行模式） — 用户可以在 WorkSpaceAlwaysOn 和 AutoStop 运行模式之间切换自己的 。有关更多信息，请参阅 管理 WorkSpace 运行模式 (p. 99).

  Note

  如果用户切换其 WorkSpace 的运行模式，这将更改其 WorkSpace 的账单费率。

- 从客户端重建 WorkSpace 用户可将—的操作系统重建到其原始状态。WorkSpace在重建WorkSpace时，将从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，然后才能重新构建 WorkSpace。 当 WorkSpace 重建正在进行时，用户将断开与其 WorkSpace 的连接，并且他们无法使用或更改其 WorkSpace。 此过程可能需要一个小时。

5. 选择 Update (更新) 或 Update and Exit (更新并退出).

管理您的 WorkSpace

可以使用 WorkSpaces 控制台管理您的 WorkSpace。

要执行目录管理任务，请参阅the section called “设置目录管理” (p. 63)。

目录

管理 Windows WorkSpace

您可以使用组策略对象 (GPO) 应用设置来管理 Windows WorkSpaces 或属于 Windows WorkSpaces 目录的用户。

> Note
>
> Linux 实例不遵循组策略。有关管理 Amazon Linux WorkSpaces 的信息，请参阅管理 Amazon Linux WorkSpaces (p. 96)。

我们建议您分别为 WorkSpace 计算机对象和 WorkSpace 用户对象创建一个组织单位。

要使用特定于的组策略设置Amazon WorkSpaces，您必须为您使用的协议或协议安装组策略管理模板（PCoIP 或WorkSpaces Streaming Protocol (WSP)。

> Warning
>
> 组策略设置可以影响工作区用户的体验，如下所示：
>
> - 实施交互式登录消息以显示登录横幅的目的是阻止用户访问其 WorkSpace。 WorkSpaces 目前不支持交互式登录消息的组策略设置。
> - 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。

- 通过组策略设置从远程桌面用户本地组中删除用户会阻止这些用户进行身份验证通过 WorkSpaces 客户端应用程序。有关此组策略设置的更多信息，请参阅。允许通过远程桌面服务登录在微软文档中。
- 组策略设置可用于限制驱动器访问。如果您将组策略设置配置为限制对驱动器 C 或驱动器 D 的访问，则用户无法访问其 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 音频输入功能需要在 WorkSpace 内进行本地登录访问。 默认情况下，为 Windows WorkSpace 启用音频输入功能。但是，如果您的组策略设置限制用户在其 WorkSpace 中的本地登录，则音频输入将无法在您的 WorkSpace 上工作。如果删除该组策略设置，则音频输入功能将在下次重新启动 WorkSpace 后启用。有关此组策略设置的更多信息，请参阅。允许本地登录在微软文档中。

  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 (p. 89)或者启用或禁用音频输入重定向WSP (p. 92)。
- 使用组策略将 Windows 电源计划设置为均衡或者电源节约可能会导致工作空间处于空闲状态时休眠状态。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 WorkSpace 在空闲时进入睡眠状态 (p. 187)。
- 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 WorkSpaces 上打开的任何应用程序都会关闭。

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 (p. 63)。

目录

为 PCoIP 安装组策略管理模板

要在使用 PCoIP 协议时使用特定于 Amazon WorkSpaces 的组策略设置，您必须添加适用于您的 WorkSpaces 的 PCoIP 代理版本（32 位或 64 位）的组策略管理模板。

> Note
>
> 如果混合使用具有 32 位和 64 位代理的 WorkSpaces，则可以对 32 位代理使用组策略管理模板，并且组策略设置将应用于 32 位和 64 位代理。当您的所有 WorkSpaces 都使用 64 位代理时，您可以切换到使用 64 位代理的管理模板。

确定您的 WorkSpaces 是 32 位代理还是 64 位代理

1. 登录到 WorkSpace，然后打开任务管理器，方法是选择查看、发送 Ctrl + Alt + 删除或右键单击任务栏并选择任务管理器。
2. 在任务管理器中，转到详细信息选项卡上，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. 在存储库的详细信息选项卡中，查找`pcoip_agent.exe`，然后在平台列以确定 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；这是正常的。）

为 PCoIP 安装组策略管理模板 (32 位)

要使用特定于的组策略设置WorkSpaces在 32 位 PCoIP 代理中使用 PCoIP 协议时，您必须安装用于 PCoIP 的组策略管理模板。在目录管理 WorkSpace 或加入您的目录的 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。管理组策略管理模板 (.adm) 文件的建议在微软文档中。

为 PCoIP 安装组策略管理模板

1. 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Amazon EC2实例，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 计算机帐户的组织单位。
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 New GPO (新建 GPO) 对话框中，为 GPO 输入一个描述性名称（如 WorkSpaces Machine Policies），并将 Source Starter GPO (源 Starter GPO) 保留为 (无)。选择 OK。
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，您可以使用该 GPO 来修改特定于 WorkSpaces 的组策略设置。

验证管理模板文件是否已正确安装

1. 在目录管理 WorkSpace 或Amazon EC2实例，打开组策略管理工具 (gpmc.msc)，然后导航到 WorkSpaces 计算机帐户的 WorkSpaces GPO 并选择它。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，您可以使用此PCoIP 会话变量组策略对象来修改特定于的组策略设置Amazon WorkSpaces当使用 PCoIP 时。

   Note

   要允许用户覆盖您的设置，请选择 Overridable Administrator Defaults (可覆盖的管理员默认值)；否则，请选择 Not Overridable Administrator Defaults (不可覆盖的管理员默认值)。

为 PCoIP 安装组策略管理模板 (64 位)

要使用特定于的组策略设置WorkSpaces使用 PCoIP 协议时，必须添加组策略管理模板`PCoIP.admx`和`PCoIP.adml`文件到您的 WorkSpace 目录的域控制器的中央存储区。有关 的更多信息`.admx`和`.adml`文件，请参阅如何在 Windows 中创建和管理组策略管理模板的中心存储。

以下过程介绍如何创建中心存储以及如何将管理模板文件添加到它。在目录管理工作区或加入您的 WorkSpaces 目录的 Amazon EC2 实例上执行以下步骤。

为 PCoIP 安装组策略管理模板文件

1. 在运行的 Windows WorkSpace 中，复制PCoIP.admx和PCoIP.adml文件C:\Program Files\Teradici\PCoIP Agent\configuration\policyDefinitions目录。这些区域有：PCoIP.adml文件位于en-US子文件夹。
2. 在目录管理 WorkSpace 或Amazon EC2实例，打开 Windows 文件资源管理器，然后在地址栏中输入组织的完全限定域名 (FQDN)，例如\\example.com。
3. 打开 sysvol 文件夹。
4. 打开文件夹*FQDN*名称。
5. 打开 Policies 文件夹。您现在应该已在*FQDN*\sysvol*FQDN*\Policies。
6. 如果尚不存在，请创建一个名为PolicyDefinitions。
7. 打开 PolicyDefinitions 文件夹。
8. 将复制到PCoIP.admx将复制到*FQDN*\sysvol*FQDN*\Policies\PolicyDefinitionsfolder。
9. 创建一个名为en-US中的PolicyDefinitionsfolder。
10. 打开 en-US 文件夹。
11. 将复制到PCoIP.adml将复制到*FQDN*\sysvol*FQDN*\Policies\PolicyDefinitions\en-USfolder。

验证管理模板文件是否已正确安装

1. 在目录管理 WorkSpace 或Amazon EC2实例，打开组策略管理工具 (gpmc.msc)。
2. 展开目录林 (林：***FQDN***).
3. 扩展域。
4. 扩展您的 FQDN（例如example.com)。
5. 扩展组策略对象。
6. Select默认域策略，打开上下文 (右键单击) 菜单，然后选择编辑。
7. 在组策略管理编辑器中，选择Computer、策略、管理员 Templates, 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特定于的组策略设置WorkSpaces当使用 PCoIP 时。

   Note

   要允许用户覆盖您的设置，请选择可覆盖的管理员默认值；否则，请选择不可覆盖的管理员默认值。

为 PCoIP 配置打印机 Support

默认情况下，WorkSpaces 启用基本远程打印，它提供有限的打印功能，因为它在主机端使用通用打印机驱动程序以确保兼容打印。

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 WorkSpace，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. 请确保您已安装了最新WorkSpacesPCoIP（32 位）的组策略管理模板 (p. 85)或者WorkSpacesPCoIP 的组策略管理模板（64 位） (p. 85)。

2. 在目录管理 WorkSpace 或Amazon EC2实例，打开组策略管理工具 (gpmc.msc) 并导航到PCoIP 会话变量。

   要允许用户覆盖您的设置，请选择 Overridable Administrator Defaults (可覆盖的管理员默认值)；否则，请选择 Not Overridable Administrator Defaults (不可覆盖的管理员默认值)。
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 OK。
6. 组策略设置更改将在 WorkSpace 的下一次组策略更新后和重新启动 WorkSpace 会话后生效。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，然后依次选择 Actions (操作)、Reboot WorkSpaces (重启 WorkSpace)）。
   - 从管理命令提示符下，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启用此功能，以便每次连接到 WorkSpace 时都将本地打印机设置为默认打印机。

Note

本地打印机重定向不适用于Amazon Linux WorkSpace。

启用本地打印机自动重定向

1. 请确保您已安装了最新WorkSpacesPCoIP（32 位）的组策略管理模板 (p. 85)或者WorkSpacesPCoIP 的组策略管理模板（64 位） (p. 85)。
2. 在目录管理 WorkSpace 或Amazon EC2实例，打开组策略管理工具 (gpmc.msc) 并导航到PCoIP 会话变量。

   要允许用户覆盖您的设置，请选择 Overridable Administrator Defaults (可覆盖的管理员默认值)；否则，请选择 Not Overridable Administrator Defaults (不可覆盖的管理员默认值)。
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，请选择下列选项之一：

   - 适用于 Windows 客户端的基本和高级打印
   - 基本打印
5. Select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 WorkSpace 的下一次组策略更新后和重新启动 WorkSpace 会话后生效。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，然后依次选择 Actions (操作)、Reboot WorkSpaces (重启 WorkSpace)）。
   - 从管理命令提示符下，输入 gpupdate /force。

为 PCoIP 启用或禁用剪贴板重定向

默认情况下，WorkSpaces 支持剪贴板重定向。如果 Windows WorkSpace 需要，您可以使用组策略设置禁用此功能。

要启用或禁用剪贴板重定向

1. 请确保您已安装了最新WorkSpacesPCoIP（32 位）的组策略管理模板 (p. 85)或者WorkSpacesPCoIP 的组策略管理模板（64 位） (p. 85)。
2. 在目录管理 WorkSpace 或Amazon EC2实例，打开组策略管理工具 (gpmc.msc) 并导航到PCoIP 会话变量。

   要允许用户覆盖您的设置，请选择 Overridable Administrator Defaults (可覆盖的管理员默认值)；否则，请选择 Not Overridable Administrator Defaults (不可覆盖的管理员默认值)。
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
   - 仅从代理到客户端单向启用（WorkSpace 到本地计算机）
   - 仅从客户端到代理单向启用（本地计算机到 WorkSpace）
   - 双向启用
5. 组策略设置更改将在 WorkSpace 的下一次组策略更新后和重新启动 WorkSpace 会话后生效。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，然后依次选择 Actions (操作)、Reboot WorkSpaces (重启 WorkSpace)）。
   - 从管理命令提示符下，输入 gpupdate /force。

已知限制

在 WorkSpace 上启用剪贴板重定向后，如果您从 Microsoft Office 应用程序复制大于 890 KB 的内容，应用程序可能会变慢或长达 5 秒钟无响应。

为 PCoIP 设置会话恢复超时

在使用 WorkSpaces 客户端应用程序时，网络连接中断会导致活动会话断开连接。这可能会因如下事件导致：合上笔记本电脑的盖子，或无线网连接丢失。如果网络连接在一定时间内恢复，用于 Windows 和 macOS 的 WorkSpaces 客户端应用程序会自动重新连接会话。默认的会话恢复超时为 20 分钟，但您可以为由您的域的组策略设置所控制的 WorkSpace 修改此值。

要设置自动会话恢复超时值

1. 请确保您已安装了最新WorkSpacesPCoIP（32 位）的组策略管理模板 (p. 85)或者WorkSpacesPCoIP 的组策略管理模板（64 位） (p. 85)。
2. 在目录管理 WorkSpace 或Amazon EC2实例，打开组策略管理工具 (gpmc.msc) 并导航到PCoIP 会话变量。

   要允许用户覆盖您的设置，请选择 Overridable Administrator Defaults (可覆盖的管理员默认值)；否则，请选择 Not Overridable Administrator Defaults (不可覆盖的管理员默认值)。
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 WorkSpace 的下一次组策略更新后和重新启动 WorkSpace 会话后生效。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，然后依次选择 Actions (操作)、Reboot WorkSpaces (重启 WorkSpace)）。

- 从管理命令提示符下，输入 gpupdate /force。

启用或禁用 PCoIP 的音频输入重定向

默认值Amazon WorkSpaces支持从本地麦克风重定向数据。如果 Windows WorkSpace 需要，您可以使用组策略设置禁用此功能。

Note

如果您的组策略设置限制用户在其 WorkSpace 中的本地登录，则音频输入将无法在您的 WorkSpace 上工作。如果删除该组策略设置，则音频输入功能将在下次重新启动 WorkSpace 后启用。有关此组策略设置的更多信息，请参阅。允许本地登录在微软文档中。

要启用或禁用音频输入重定向

1. 请确保您已安装了最新WorkSpacesPCoIP（32 位）的组策略管理模板 (p. 85)或者WorkSpacesPCoIP 的组策略管理模板（64 位） (p. 85)。
2. 在目录管理 WorkSpace 或Amazon EC2实例，打开组策略管理工具 (gpmc.msc) 并导航到PCoIP 会话变量。

   要允许用户覆盖您的设置，请选择 Overridable Administrator Defaults (可覆盖的管理员默认值)；否则，请选择 Not Overridable Administrator Defaults (不可覆盖的管理员默认值)。
3. 打开启用/禁用PCoIP 会话中的音频设置。
4. 在启用/禁用PCoIP 会话中的音频对话框中，选择启用或者Disabled。
5. 选择 OK。
6. 组策略设置更改将在 WorkSpace 的下一次组策略更新后和重新启动 WorkSpace 会话后生效。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，然后依次选择 Actions (操作)、Reboot WorkSpaces (重启 WorkSpace)）。
   - 从管理命令提示符下，输入 gpupdate /force。

禁用 PCoIP 的时区重定向

默认情况下，WorkSpace 内的时间设置为镜像用于连接到 WorkSpace 的客户端的时区。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 WorkSpace 中计划的任务要在特定时区内的特定时间运行。
- 频繁出差的用户希望将其 WorkSpace 保持在一个时区中，以保持一致性和个人偏好。

如果 Windows WorkSpace 需要，您可以使用组策略设置禁用此功能。

禁用时区重定向

1. 在目录管理 WorkSpace 或Amazon EC2实例，打开组策略管理工具 (gpmc.msc），然后导航到用于 WorkSpaces 的目录的域或域控制器级别的 GPO 并选择该 GPO。
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、Windows 组件、远程桌面服务、远程桌面会话主机以及设备和资源重定向。
4. 打开 Allow time zone redirection (允许时区重定向) 设置。

5. 在 zone redirection (允许时区重定向) 对话框中，选择禁用， 然后选择确定。
6. 组策略设置更改将在 WorkSpace 的下一次组策略更新后和重新启动 WorkSpace 会话后生效。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，然后依次选择 Actions (操作)、Reboot WorkSpaces (重启 WorkSpace)) 。
   - 从管理命令提示符下，输入 gpupdate /force。
7. 将 WorkSpace 的时区设置为所需的时区。

WorkSpace 的时区现在是静态的，不再镜像客户端计算机的时区。

安装组策略管理模板文件WorkSpaces Streaming Protocol (WSP)

要使用特定于的组策略设置WorkSpaces使用WorkSpaces Streaming Protocol (WSP)时，您必须添加组策略管理模板`wsp.admx`和`wsp.adml`的文件WSP添加到您的 WorkSpace 目录的域控制器的中央存储区。有关的更多信息`.admx`和`.adml`文件，请参阅如何在 Windows 中创建和管理组策略管理模板的中心存储。

以下过程介绍如何创建中心存储以及如何将管理模板文件添加到它。在目录管理工作区或加入您的 WorkSpaces 目录的 Amazon EC2 实例上执行以下步骤。

要安装用于的组策略管理模板文件WSP

1. 在运行的 Windows WorkSpace 中，复制`wsp.admx`和`wsp.adml`文件`C:\Program Files\Amazon\WSP`目录。
2. 在目录管理 WorkSpace 或Amazon EC2实例，打开 Windows 文件资源管理器，然后在地址栏中输入组织的完全限定域名 (FQDN)，例如`\\example.com`。
3. 打开 `sysvol` 文件夹。
4. 打开文件夹*`FQDN`*名称。
5. 打开 `Policies` 文件夹。您现在应该已在`\\`*`FQDN`*`\sysvol\`*`FQDN`*`\Policies`。
6. 如果尚不存在，请创建一个名为`PolicyDefinitions`。
7. 打开 `PolicyDefinitions` 文件夹。
8. 将复制到`wsp.admx`将复制到`\\`*`FQDN`*`\sysvol\`*`FQDN`*`\Policies\PolicyDefinitions`folder。
9. 创建一个名为`en-US`中的`PolicyDefinitions`folder。
10. 打开 `en-US` 文件夹。
11. 将复制到`wsp.adml`将复制到`\\`*`FQDN`*`\sysvol\`*`FQDN`*`\Policies\PolicyDefinitions\en-US`folder。

验证管理模板文件是否已正确安装

1. 在目录管理 WorkSpace 或Amazon EC2实例，打开组策略管理工具 (gpmc.msc)。
2. 展开目录林 (林：***`FQDN`***).
3. 扩展域。
4. 扩展您的 FQDN (例如`example.com`)。
5. 扩展组策略对象。
6. Select默认域策略，打开上下文 (右键单击) 菜单，然后选择编辑。
7. 在组策略管理编辑器中，选择Computer、策略、管理员 Templates、Amazon, 和WSP。
8. 现在，您可以使用此WSP组策略对象来修改特定于的组策略设置WorkSpaces使用WSP。

配置打印机 SupportWSP

默认情况下，WorkSpaces 启用基本远程打印，它提供有限的打印功能，因为它在主机端使用通用打印机驱动程序以确保兼容打印。

针对 Windows 客户端的高级远程打印（不适用于WSP）允许您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 WorkSpace，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. 请确保最近WorkSpaces的组策略管理模板WSP (p. 90)安装在您的 WorkSpaces 目录的域控制器的中央存储区中。
2. 在目录管理 WorkSpace 或Amazon EC2实例，打开组策略管理工具 (gpmc.msc)。
3. 展开目录林 (林：***FQDN***).
4. 扩展域。
5. 扩展您的 FQDN（例如`example.com`)。
6. 扩展组策略对象。
7. Select默认域策略，打开上下文 (右键单击) 菜单，然后选择编辑。
8. 在组策略管理编辑器中，选择Computer、策略、管理员 Templates、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，然后用于打印选项中，选择基本。要自动使用客户端计算机的当前默认打印机，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Disabled。
11. 选择 OK。
12. 组策略设置更改将在 WorkSpace 的下一次组策略更新后和重新启动 WorkSpace 会话后生效。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，然后依次选择 Actions (操作)、Reboot WorkSpaces (重启 WorkSpace)）。
    - 从管理命令提示符下，输入 gpupdate /force。

为的启用或禁用剪贴板重定向WSP

默认值WorkSpaces支持双向（复制/粘贴）剪贴板重定向。如果 Windows WorkSpace 需要，您可以使用组策略设置禁用此功能。

为 Windows WorkSpace 启用或禁用剪贴板重定向

1. 请确保最近WorkSpaces的组策略管理模板WSP (p. 90)安装在您的 WorkSpaces 目录的域控制器的中央存储区中。
2. 在目录管理 WorkSpace 或Amazon EC2实例，打开组策略管理工具 (gpmc.msc)。
3. 展开目录林 (林：***FQDN***).
4. 扩展域。
5. 扩展您的 FQDN（例如`example.com`)。
6. 扩展组策略对象。
7. Select默认域策略，打开上下文 (右键单击) 菜单，然后选择编辑。

8. 在组策略管理编辑器中，选择Computer、策略、管理员 Templates、Amazon, 和WSP。
9. 打开启用/禁用剪贴板重定向设置。
10. 在启用/禁用剪贴板重定向对话框中，选择启用或者Disabled。
11. 选择 OK。
12. 组策略设置更改将在 WorkSpace 的下一次组策略更新后和重新启动 WorkSpace 会话后生效。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，然后依次选择 Actions (操作)、Reboot WorkSpaces (重启 WorkSpace)）。
    - 从管理命令提示符下，输入 gpupdate /force。

已知限制

在 WorkSpace 上启用剪贴板重定向后，如果您从 Microsoft Office 应用程序复制大于 890 KB 的内容，应用程序可能会变慢或长达 5 秒钟无响应。

启用或禁用视频输入重定向WSP

默认值WorkSpaces支持从本地摄像机重定向数据。如果 Windows WorkSpace 需要，您可以使用组策略设置禁用此功能。

为 Windows WorkSpaces 启用或禁用视频重定向

1. 请确保最近WorkSpaces的组策略管理模板WSP (p. 90)安装在您的 WorkSpaces 目录的域控制器的中央存储区中。
2. 在目录管理 WorkSpace 或Amazon EC2实例，打开组策略管理工具 (gpmc.msc)。
3. 展开目录林 (林：***FQDN***).
4. 扩展域。
5. 扩展您的 FQDN（例如`example.com`)。
6. 扩展组策略对象。
7. Select默认域策略，打开上下文 (右键单击) 菜单，然后选择编辑。
8. 在组策略管理编辑器中，选择Computer、策略、管理员 Templates、Amazon, 和WSP。
9. 打开启用/禁用视频重定向设置。
10. 在启用/禁用视频重定向对话框中，选择启用或者Disabled。
11. 选择 OK。
12. 组策略设置更改将在 WorkSpace 的下一次组策略更新后和重新启动 WorkSpace 会话后生效。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，然后依次选择 Actions (操作)、Reboot WorkSpaces (重启 WorkSpace)）。
    - 从管理命令提示符下，输入 gpupdate /force。

启用或禁用音频输入重定向WSP

默认值WorkSpaces支持从本地麦克风重定向数据。如果 Windows WorkSpace 需要，您可以使用组策略设置禁用此功能。

为 Windows WorkSpaces 启用或禁用音频输入重定向

1. 请确保最近WorkSpaces的组策略管理模板WSP (p. 90)安装在您的 WorkSpaces 目录的域控制器的中央存储区中。

2. 在目录管理 WorkSpace 或Amazon EC2实例，打开组策略管理工具 (gpmc.msc)。
3. 展开目录林 (林：***FQDN***).
4. 扩展域。
5. 扩展您的 FQDN（例如`example.com`)。
6. 扩展组策略对象。
7. Select默认域策略，打开上下文 (右键单击) 菜单，然后选择编辑。
8. 在组策略管理编辑器中，选择Computer、策略、管理员 Templates、Amazon, 和WSP。
9. 打开启用/禁用音频进入重定向设置。
10. 在启用/禁用音频进入重定向对话框中，选择启用或者Disabled。
11. 选择 OK。
12. 组策略设置更改将在 WorkSpace 的下一次组策略更新后和重新启动 WorkSpace 会话后生效。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，然后依次选择 Actions (操作)、Reboot WorkSpaces (重启 WorkSpace)）。
    - 从管理命令提示符下，输入 gpupdate /force。

禁用的时区重定向WSP

默认情况下，WorkSpace 内的时间设置为镜像用于连接到 WorkSpace 的客户端的时区。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 WorkSpace 中计划的任务要在特定时区内的特定时间运行。
- 频繁出差的用户希望将其 WorkSpace 保持在一个时区中，以保持一致性和个人偏好。

如果 Windows WorkSpace 需要，您可以使用组策略设置禁用此功能。

禁用 Windows WorkSpaces 的时区重定向

1. 请确保最近WorkSpaces的组策略管理模板WSP (p. 90)安装在您的 WorkSpaces 目录的域控制器的中央存储区中。
2. 在目录管理 WorkSpace 或Amazon EC2实例，打开组策略管理工具 (gpmc.msc)。
3. 展开目录林 (林：***FQDN***).
4. 扩展域。
5. 扩展您的 FQDN（例如`example.com`)。
6. 扩展组策略对象。
7. Select默认域策略，打开上下文 (右键单击) 菜单，然后选择编辑。
8. 在组策略管理编辑器中，选择Computer、策略、管理员 Templates、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Disabled。
11. 选择 OK。
12. 组策略设置更改将在 WorkSpace 的下一次组策略更新后和重新启动 WorkSpace 会话后生效。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，然后依次选择 Actions (操作)、Reboot WorkSpaces (重启 WorkSpace)）。

- 从管理命令提示符下，输入 gpupdate /force。

13. 将 WorkSpace 的时区设置为所需的时区。

WorkSpace 的时区现在是静态的，不再镜像客户端计算机的时区。

为的启用或禁用智能卡重定向WSP

默认值Amazon WorkSpaces未启用，以支持使用智能卡会话前身份验证或者会话中身份验证。会话前身份验证是指在用户登录其 WorkSpaces 时执行的智能卡身份验证。会话内身份验证是指登录后执行的身份验证。

如果需要，可以使用组策略设置为 Windows WorkSpace 启用会话前身份验证和会话中身份验证。还必须通过 AD Connector 目录设置启用会话前身份验证，方法是使用EnableClientAuthenticationAPI 操作或enable-client-authenticationAWS 命令行界面 (AWS CLI) 命令。有关更多信息，请参阅 。启用 AD Connector 的智能卡身份验证中的AWS Directory Service Administration Guide。

Note

若要在 Windows WorkSpaces 中使用智能卡，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 (p. 34)。

为 Windows WorkSpaces 启用或禁用智能卡重定向

1. 请确保最近WorkSpaces的组策略管理模板WSP (p. 90)安装在您的 WorkSpaces 目录的域控制器的中央存储区中。
2. 在目录管理 WorkSpace 或Amazon EC2实例，打开组策略管理工具 (gpmc.msc)。
3. 展开目录林 (林：***FQDN***).
4. 扩展域。
5. 扩展您的 FQDN（例如`example.com`)。
6. 扩展组策略对象。
7. Select默认域策略，打开上下文 (右键单击) 菜单，然后选择编辑。
8. 在组策略管理编辑器中，选择Computer、策略、管理员 Templates、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，选择启用或者Disabled。
11. 选择 OK。
12. 组策略设置更改会在 WorkSpace 会话重启后生效。要应用组策略更改，请重启用 WorkSpace（在Amazon WorkSpaces控制台中，选择 WorkSpace，然后选择操作、重启 WorkSpaces)。

启用或禁用屏幕锁定上的断开连接会话WSP

如果需要，您可以在检测到 Windows 锁定屏幕时断开用户的 WorkSpaces 会话。要从 WorkSpaces 客户端重新连接，用户可以使用其密码或智能卡对自己进行身份验证，具体取决于为其 WorkSpaces 启用了哪种身份验证类型。

默认情况下将禁用此组策略设置。如果需要，您可以使用组策略设置在检测到 Windows WorkSpaces 的 Windows 锁定屏幕时启用断开会话连接。

Note

- 此组策略设置仅在AWS GovCloud（美国西部）区域目前。
- 此组策略设置同时适用于通过密码身份验证的会话和智能卡身份验证的会话。

- 若要在 Windows WorkSpaces 中使用智能卡，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 (p. 34)。

为 Windows WorkSpaces 启用或禁用屏幕锁定的断开连接会话

1. 请确保最近WorkSpaces的组策略管理模板WSP (p. 90)安装在您的 WorkSpaces 目录的域控制器的中央存储区中。
2. 在目录管理 WorkSpace 或Amazon EC2实例，打开组策略管理工具 (gpmc.msc)。
3. 展开目录林 (林：***FQDN***).
4. 扩展域。
5. 扩展您的 FQDN（例如`example.com`)。
6. 扩展组策略对象。
7. Select默认域策略，打开上下文 (右键单击) 菜单，然后选择编辑。
8. 在组策略管理编辑器中，选择Computer、策略、管理员 Templates、Amazon, 和WSP。
9. 打开启用/禁用屏幕锁定上的断开会话设置。
10. 在启用/禁用屏幕锁定上的断开会话对话框中，选择启用或者Disabled。
11. 选择 OK。
12. 组策略设置更改将在 WorkSpace 的下一次组策略更新后和重新启动 WorkSpace 会话后生效。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，然后依次选择 Actions (操作)、Reboot WorkSpaces (重启 WorkSpace)）。
    - 从管理命令提示符下，输入 gpupdate /force。

设置 Kerberos 票证的最长使用期限

如果您尚未禁用请记住我功能，则 WorkSpaces 用户可以使用请记住我或者让我保持登录复选框以保 WorkSpaces 其凭据。此功能允许用户在客户端应用程序保持运行时轻松连接到他们的 WorkSpaces。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。

如果您的 WorkSpace 使用 AD Connector 目录，则可以按照 Microsoft Windows 文档中用户票证的最长使用期限中的步骤，通过组策略来修改 WorkSpaces 用户的 Kerberos 票证的最长使用期限。

要启用或禁用 Remember Me 功能，请参阅 为您的用户启用自助服务 WorkSpace 管理功能 (p. 81)。

配置互联网访问的设备代理服务器设置

默认情况下，WorkSpaces Windows 客户端应用程序使用在 HTTPS（端口 443）通信的设备操作系统设置中指定的代理服务器。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

- 到 WorkSpace 的桌面流式处理连接需要启用端口 4172 和 4195，而且不能通过代理服务器。
- 不支持要求使用用户名和密码进行身份验证的代理服务器。

您可以通过组策略为 Windows WorkSpaces 配置设备代理服务器设置，方法是按照配置设备代理和互联网连接设置在微软文档中。

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。代理服务器中的Amazon WorkSpaces 用户指南。

管理 Amazon Linux WorkSpaces

与 Windows WorkSpace 一样，Amazon Linux WorkSpace 加入了域，因此您可以使用 Active Directory 用户和组来执行以下操作：

- 管理您的 Amazon Linux WorkSpace
- 为用户提供访问这些 WorkSpace 的权限

由于 Linux 实例不遵循组策略，因此我们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，或者Ansible。

Note

上的 Linux WorkSpacesWorkSpaces Streaming Protocol (WSP)捆绑包仅在AWS GovCloud（美国西部）区域目前。
上的 Linux WorkSpacesWSP目前具有以下限制：

- 不支持剪贴板、音频输入、视频输入和时区重定向。
- 不支持多台显示器。
- 您必须使用 WorkSpaces Windows 客户端应用程序连接到WSP。

控制 Amazon Linux WorkSpaces 上的 PCoIP 代理行为

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。

有关可用设置的完整列表，请在任意 Amazon Linux WorkSpace 上从终端运行 `man pcoip-agent.conf`。

Note

本地打印机重定向不适用于 Linux WorkSpace。

为 Amazon Linux WorkSpaces 启用或禁用剪贴板重定向

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 WorkSpace 时生效。

Note

WorkSpaces Linux 客户端应用程序中目前不支持剪贴板重定向WSP。

为 Amazon Linux WorkSpace 启用或禁用剪贴板重定向

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
```

如果可能的值 *x* 是：

0 — 双向禁用

1 — 双向启用

2—启用仅客户端到代理（仅允许从本地客户端设备复制和粘贴到远程主机桌面）

3—已启用代理仅到客户端（仅允许从远程主机桌面复制和粘贴到本地客户端设备）

Note

剪贴板重定向实施为虚拟通道。如果虚拟通道被禁用，剪贴板重定向无法正常工作。要启用虚拟通道，请参阅PCoIP 虚拟通道（TeskSpace 文档中）。

启用或禁用音频输入重定向Amazon LinuxWorkSpaces

默认值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 WorkSpace 时生效。

Note

Linux WorkSpace 目前不支持音频输入重定向WSP。

若要启用或禁用音频输入重定向Amazon LinuxWorkSpaces

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
```

如果可能的值 *x* 是：

0—Disabled

1—启用

为启用或禁用时区重定向Amazon LinuxWorkSpaces

默认情况下，WorkSpace 内的时间设置为镜像用于连接到 WorkSpace 的客户端的时区。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 WorkSpace 中计划的任务要在特定时区内的特定时间运行。
- 频繁出差的用户希望将其 WorkSpace 保持在一个时区中，以保持一致性和个人偏好。

如果 Linux WorkSpaces 需要，您可以使用 PCoIP 代理 conf 禁用此功能。此设置将在您重新启动 WorkSpace 时生效。

Note

Linux WorkSpace 目前不支持使用WSP。

若要启用或禁用Amazon LinuxWorkSpaces

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
```

如果可能的值 *X* 是：

0—Disabled

1—启用

将 SSH 访问权限授给 Amazon Linux WorkSpaces 管理员

默认情况下，只有指定的用户和域管理员组中的账户可以使用 SSH 连接到 Amazon Linux WorkSpaces。

我们建议您为 Active Directory 中的 Amazon Linux WorkSpaces 管理员创建专用的管理员组。

为 Linux_WorkSpace_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。

为 Linux_WorkSpace_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`。

```
[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，请参阅为您的 Linux WorkSpace 启用 SSH 连接 (p. 48)。

覆盖 Amazon Linux WorkSpace 的默认 Shell

要覆盖 Linux WorkSpace 的默认 Shell，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，您必须重新启动 WorkSpace 或注销 Workspace（而不仅仅是断开连接），然后重新登录以使更改生效。

保护自定义资料库免遭未授权访问

要控制对自定义存储库的访问，我们建议使用 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，请参阅安全性中的Amazon VPC 用户指南。

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 库来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 Amazon Linux 用户指南（适用于 Linux 实例） 中的 Extras 库 (Amazon EC2)。

Note

如果您使用的是 Amazon Linux 存储库，则 Amazon Linux WorkSpace 必须能够访问 Internet，否则您必须配置指向此存储库和主 Amazon Linux 存储库的 Virtual Private Cloud (VPC) 终端节点。有关更多信息，请参阅 提供 WorkSpace 的 Internet 访问权限 (p. 40)。

在 Linux WorkSpaces 上使用智能卡进行身份验证

上的 Linux WorkSpacesWorkSpaces Streaming Protocol (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 (p. 34)。

管理 WorkSpace 运行模式

这些区域有：运行模式决定其即时可用性和付费方式（按月或按小时计算）。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 WorkSpace。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。

  要设置自动停止时间，请在Amazon WorkSpaces控制台中，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 将在断开 WorkSpace 连接 1 小时后自动停止。

  Note

  在断开 WorkSpace 连接并且 AutoStop 时间段过期后，可能需要额外几分钟才能自动停止 WorkSpace。但是，一旦 AutoStop 时间段到期，开单就会停止，并且不会向您收取该额外时间的费用。

  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。

Note

AutoStop GraphicsPro WorkSpaces 不会保留数据和程序停止时的状态。对于 GraphicsPro WorkSpaces 间，我们建议您在每次使用完工作时保存您的工作。

Important

仅当 WorkSpaces 断开连接时，AutoStop WorkSpaces 才会自动停止。 仅在以下情况下断开 WorkSpace：

- 如果用户手动断开与 WorkSpace 的连接或退出Amazon WorkSpaces客户端应用程序。
- 如果客户端设备已关闭。
- 如果客户端设备与 WorkSpace 之间没有连接超过 20 分钟。

作为最佳做法，AutoStop Workspace 用户在每天使用完 WorkSpace 时，应手动断开与其 WorkSpaces 的连接。要手动断开连接，请选择WorkSpace 断开连接或者退出 Amazon WorkSpaces来自 的Amazon WorkSpaces菜单中的 对于安卓或 iPad，请选择Disconnect从侧边栏菜单中。

在以下情况下，AutoStop WorkSpaces 可能不会自动停止：

- 如果客户端设备仅锁定、睡眠或其他非活动（例如，笔记本电脑盖已关闭）而不是关闭，则 WorkSpaces 应用程序可能仍在后台运行。只要 WorkSpace 应用程序仍在运行，WorkSpaces 可能不会断开连接，因此 WorkSpace 可能不会自动停止。
- WorkSpaces仅当用户使用WorkSpaces客户端。如果用户使用的是第三方客户端，WorkSpaces可能无法检测到断开连接，因此 WorkSpaces 可能不会自动停止，计费也可能不会暂停。

有关更多信息，请参阅 WorkSpaces 定价。

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. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择要修改的 WorkSpace，然后选择 Actions (操作)、Modify Running Mode Properties (修改运行模式属性)。
4. 选择新的运行模式 (AlwaysOn 或 AutoStop)，然后选择 Modify。

停止和启动 AutoStop WorkSpace

当您的 AutoStop WorkSpace 断开连接时，它们会在指定的断开时间后自动停止，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 关联的按小时计算的费用。WorkSpace 将停止，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（重启）可用或处于错误状态的 AutoStop WorkSpace。

要停止 AutoStop WorkSpace

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择要停止的 WorkSpace，然后选择 Actions (操作)、Stop WorkSpaces (停止 WorkSpace)。

4. 当系统提示您确认时，选择 Stop。

要启动 AutoStop WorkSpace

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择要启动的 WorkSpace，然后选择 Actions、Start WorkSpaces。
4. 当系统提示您确认时，选择 Start。

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 删除工作区 (p. 122)。

修改 WorkSpace

启动 WorkSpace 后，您可以通过两种方式修改其配置：

- 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。

WorkSpace 的当前修改状态显示在State设置WorkSpaces控制台。状态的可能值为正在修改计算、正在修改存储和无。

如果您希望修改工作区，其状态必须为 `AVAILABLE` 或 `STOPPED`。修改卷大小时，不能同时更改计算类型，反之亦然。

更改工作区的卷大小或计算类型时，将更改工作区的账单费率。

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服务 WorkSpace 管理功能 (p. 81)。

更改卷大小

您可以增加 WorkSpace 的根卷和用户卷的大小，每个卷最多 2000 GB。WorkSpace 根卷和用户卷包含无法更改的集合组。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 (p. 102)。

> **Note**
>
> 展开工作区的卷时，WorkSpaces 会自动在 Windows 或 Linux 中扩展卷的分区。完成该过程后，必须重新启动工作区才能使更改生效。

要确保您的数据得以保留，在启动 WorkSpace 后，您不能减小根卷或用户卷的大小。而是确保在启动 WorkSpace 时为这些卷指定最小大小。您可以启动最低根卷容量为 80 GB、最低用户卷容量为 10 GB 的 Value、Standard、Performance、Power 或 PowerPro WorkSpace。您可以启动最低根卷容量为 100 GB、最低用户卷容量为 100 GB 的 Graphics 或 GraphicsPro WorkSpace。

在增加工作区磁盘大小的过程中，用户可以在其工作区上执行大多数任务。但是，用户无法更改其 WorkSpace 计算类型、切换 WorkSpace 运行模式、重建 WorkSpace 或重启（重启）WorkSpace。

Note

如果希望用户能够在磁盘大小增加过程中使用其 WorkSpaces Space，请确保 WorkSpaces 的状态为`AVAILABLE`而不是`STOPPED`，然后再调整 WorkSpaces 的卷大小。如果 WorkSpaces 是`STOPPED`，则无法在磁盘大小增加过程中启动它们。

在大多数情况下，增加磁盘大小过程可能需要一个小时。但是，如果要修改大量 WorkSpaces 的卷大小，则该过程可能需要更长的时间。如果您需要修改大量的 WorkSpaces，我们建议您联系 Support 部门寻求帮助。

有关增加卷的限制

- 您只能调整 SSD 卷的大小。
- 启动 WorkSpace 时，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 或 GraphicsPro WorkSpace，否则，当用户卷为 100 GB 时，根卷不能小于 175 GB。Graphics 或 GraphicsPro WorkSpace 可以将根卷和用户卷都设置为 100 GB 的最小值。
- 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。

更改 WorkSpace 的卷大小

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择 WorkSpace，然后依次选择 Actions 和 Modify WorkSpace。
4. 要增加根卷或用户卷的大小，请选择 Modify Volume Sizes (修改卷大小)，然后输入新值。
5. 选择修改。
6. 完成增加磁盘大小后，您必须重启 WorkSpace (p. 111)以使更改生效。为避免数据丢失，请确保用户在重启 WorkSpace 之前，保存所有打开的文件。

更改捆绑包类型

您可以在 Value、Standard、Performance、Power 和 PowerPro 捆绑包之间切换 WorkSpace。有关这些捆绑包类型的详细信息，请参阅。Amazon WorkSpaces捆绑。

Note

您不能更改图形和图形 SPro WorkSpaces 的计算类型。

当您请求更改服务包时，WorkSpaces 将使用新服务包重新启动 WorkSpace。WorkSpaces 将保留 WorkSpace 的操作系统、应用程序、数据和存储设置。

您可以在 1 小时内申请更大服务包一次，而请求较小服务包的申请每 30 天可以提一次。对于新启动的 WorkSpace，您必须等待 1 个小时之后才能请求更大的捆绑包。

在更改 WorkSpace 计算类型的过程中，用户将断开与其 WorkSpace 的连接，他们无法使用或更改 WorkSpace。在计算类型更改过程中，工作区将自动重新启动。

> **Important**
>
> 为避免数据丢失，请确保用户先保存任意打开的文档和其他应用程序文件，然后再更改工作区计算类型。

计算类型更改过程可能需要一个小时的时间。

更改 WorkSpace 的捆绑包类型

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择 WorkSpace，然后依次选择 Actions 和 Modify WorkSpace。
4. 要更改捆绑包，请选择 Change Compute Type，然后选择新的捆绑包类型。
5. 选择修改。

标记 WorkSpace 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 WorkSpace 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 资源和整理数据（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 日向现有工作区添加标签，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 https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/cost-alloc-tags.html 中的AWS Billing and Cost Management 用户指南使用成本分配标签。

> **Note**
>
> 要在成本资源管理器中查看 WorkSpaces 资源标签，您必须按照激活用户定义的成本分配标签中的AWS Billing and Cost Management 用户指南。
> 尽管标签在激活后 24 小时显示，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，若要在成本资源管理器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 — WorkSpace、导入的图像和 IP 访问控制组。
- 您可以向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

- 每个资源的最大标签数 — 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。

- 请勿使用 “aws:” 或 “aw: 工作区:” 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。

使用控制台更新现有资源的标签

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择以下任一资源类型：目录、WorkSpaces、捆绑、映像，或者IP 访问控制。
3. 选择资源，然后选择 Actions (操作)、Manage Tags (管理标签)。
4. 执行以下一个或多个操作：
   - 要更新标签，请编辑 Key 和 Value 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 AWS CLI 更新现有资源的标签

使用 create-tags 和 delete-tags 命令

WorkSpace 维护

我们建议您定期维护 WorkSpace。WorkSpaces 会为您的 WorkSpace 安排默认的维护时段。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。

Note

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。

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 (p. 89)。您可以禁用 Linux WorkSpaces 的时区重定向 (p. 97)通过使用 PCoIP 代理协议。

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 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 的维护窗口。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。

要禁用维护模式

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Directories。
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 Update and Exit。

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，我们建议您将 WorkSpace 的状态更改为 ADMIN_MAINTENANCE。维护完成后，将 WorkSpace 的状态更改为 AVAILABLE。

当 WorkSpace 处于 ADMIN_MAINTENANCE 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。
- 用户无法登录到工作区。
- AutoStop WorkSpace 不会休眠。

要使用控制台更改 WorkSpace 的状态

> Note
>
> 要更改工作区的状态，工作区必须具有状态 AVAILABLE。这些区域有：修改状态设置不可用，当 WorkSpace 的状态为STOPPED。

1. 通过以下网址打开 WorkSpaces 控制台：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 Actions 和 Modify WorkSpace。
4. 选择 Modify State。对于 Intended State，选择 ADMIN_MAINTENANCE 或 AVAILABLE。
5. 选择修改。

要使用 AWS CLI 更改 WorkSpace 的状态

使用 modify-workspace-state 命令。

加密的 WorkSpace

WorkSpaces 与 AWS Key Management Service (AWS KMS) 集成。这使您能够使用客户主密钥 (CMK) 来加密 WorkSpace 的存储卷。在您启动 WorkSpace 时，可以加密根卷（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 ）。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 之外，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 为 FedRAMP 授权或 DoD SRG 合规性设置 Amazon WorkSpaces (p. 47)。

主题

Prerequisites

在开始加密过程之前，您需要一个 AWS KMS CMK。此 CMK 可以是AWS 托管 CMKAmazon WorkSpaces (aws/workspaces) 或对称客户托管 CMK。

- AWS 托管 CMK –第一次启动未加密的 WorkSpace 时从WorkSpaces控制台，Amazon WorkSpaces 自动创建 AWS 托管 CMK (aws/workspaces) 在您的账户中。您可以选择该 AWS 托管 CMK 来加密您的 WorkSpace 的用户卷和根卷。有关详细信息，请参阅 使用 AWS KMS 的 WorkSpaces 加密概述 (p. 107)。

  您可以查看此 AWS 托管 CMK (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 CMK。Amazon WorkSpaces 创建和管理此 CMK。仅限Amazon WorkSpaces 可以使用此 CMK，WorkSpaces 只能使用它来加密您的帐户中的 WorkSpace 资源。

  AWS 托管 CMK (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。轮换客户主密钥中的AWS Key Management Service Developer Guide。
- 客户托管 CMK –或者，您可以选择您使用创建的对称客户托管 CMKAWS KMS。您可以查看、使用和管理此 CMK，包括设置其策略。有关创建 CMK 的详细信息，请参阅创建密钥中的AWS Key Management Service Developer Guide。有关使用AWS KMSAPI，请参阅使用密钥中的AWS Key Management Service Developer Guide。

  除非您决定启用自动密钥轮换，否则客户管理的 CMK 不会自动轮换。有关详细信息，请参阅。轮换客户主密钥中的AWS Key Management Service Developer Guide。

  Important

  当您旋转 CMK 时，必须同时保持原始 CMK 和新 CMK 的启用状态，以便AWS KMS可以解密原始 CMK 加密的 WorkSpaces。如果您不想保持启用原始 CMK，则必须重新创建 WorkSpaces 并使用新的 CMK 对它们进行加密。

您必须满足以下要求才能使用 AWS KMS CMK 加密您的 WorkSpace：

- CMK 必须是对称的。 Amazon WorkSpaces不支持非对称 CMK。有关区分对称 CMK 和非对称 CMK 的信息，请参阅识别对称 CMK 和非对称 CMK中的AWS Key Management Service Developer Guide。
- 必须启用 CMK。 要确定是否已启用 CMK，请参阅显示 CMK 详细信息中的AWS Key Management Service Developer Guide。
- 您必须拥有与 CMK 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 WorkSpace 管理员授予其他权限 (p. 108)。

Limits

- 您无法加密现有的工作区。您必须在启动工作区时对其加密。

- 不支持从加密的 WorkSpace 中创建自定义映像。
- 目前不支持禁用已加密 WorkSpace 的加密。
- 对于在启动时启用了根卷加密的 WorkSpace，可能需要多达一个小时的时间才能完成配置。
- 要重启或重建已加密的 WorkSpace，请先确保 AWS KMS CMK 已启用；否则 WorkSpace 将变得不可用。要确定是否已启用 CMK，请参阅显示 CMK 详细信息中的AWS Key Management Service Developer Guide。

使用 AWS KMS 的 WorkSpaces 加密概述

当您创建使用加密卷的 WorkSpace 时，WorkSpaces 将使用 Amazon Elastic Block Store (Amazon EBS) 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。亚马逊 EBS 和 Amazon WorkSpaces 都使用您的 CMK 来处理加密的卷。有关 EBS 卷加密的详细信息，请参阅Amazon EBS加密中的Amazon EC2 用户指南（适用于 Windows 实例）。

当您启动使用加密卷的 WorkSpace 时，端到端过程的工作方式如下所示：

1. 您指定用于加密的 CMK，以及 WorkSpace 的用户和目录。该操作创建一个授权，允许 WorkSpaces 将您的 CMK 仅用于此 WorkSpace—即仅用于与指定用户和目录相关联的 WorkSpace。
2. WorkSpaces为 WorkSpace 创建加密的 EBS 卷，并指定要使用的 CMK，以及该卷的用户和目录。此操作将创建一个允许Amazon EBS将您的 CMK 仅用于此 WorkSpace 和卷—即仅用于与指定用户和目录相关联的 WorkSpace，以及指定的卷。
3. Amazon EBS请求使用您的 CMK 加密的卷数据密钥，并指定 WorkSpace 用户的活动目录安全标识符 (SID) 和AWS Directory Service目录 ID 以及Amazon EBS卷 ID 作为加密上下文 (p. 107)。
4. AWS KMS 创建新的数据密钥，使用您的 CMK 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将加密的数据密钥发送给AWS KMS使用 `Decrypt`请求，并指定 WorkSpace 用户的 SID、目录 ID 和卷 ID（用作加密上下文）。
6. AWS KMS 使用您的 CMK 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。只要卷附加在 WorkSpace 上，Amazon EBS 就会将纯文本数据密钥保存在内存中。
8. Amazon EBS 将加密的数据密钥（在Step 4 (p. 107) 中收到）与卷元数据存储在一起，以供将来重启或重建 WorkSpace 时使用。
9. 当您使用 AWS 管理控制台删除 WorkSpace (或使用 API 中的 `TerminateWorkspaces`WorkSpaces 操作) 时，WorkSpaces 和 Amazon EBS 将停用允许它们针对该 WorkSpace 使用 CMK 的授权。

WorkSpaces 加密上下文

WorkSpaces不会直接使用您的 CMK 进行加密操作（例如`Encrypt`、`Decrypt`、`GenerateDataKey`等），这意味着WorkSpaces不会将请求发送到AWS KMS，其中包括加密上下文。但是，当 Amazon EBS 为 WorkSpaces 的加密卷请求加密的数据密钥（使用 AWS KMS 的 WorkSpaces 加密概述 (p. 107)中的Step 3 (p. 107)），以及请求该数据密钥的纯文本副本 (Step 5 (p. 107)) 时，将在请求中提供加密上下文。

加密上下文提供其他已经过身份验证的数据(AAD) 认为AWS KMS用于确保数据完整性。加密上下文也将写入AWS CloudTrail日志文件，这可以帮助您了解为什么要使用给定的 CMK。Amazon EBS会对加密上下文使用以下内容：

- 与 WorkSpace 关联的活动目录用户的安全标识符 (SID)
- 与 WorkSpace 关联的 AWS Directory Service 目录的目录 ID

- 这些区域有：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"
}
```

给予WorkSpaces代表您使用 CMK 的权限

您 WorkSpace 以在AWS托管 CMKWorkSpaces(aws/workspaces) 或客户托管 CMK。如果您使用客户托管 CMK，则需要为 WorkSpaces 提供代表您账户中的 WorkSpaces 管理员使用 CMK 的权限。默认情况下，适用于 WorkSpaces 的 AWS 托管 CMK 具有必需权限。

要准备您的客户托管 CMK 以便与 WorkSpaces 结合使用，请使用以下过程。

1. 将您的 WorkSpaces 管理员添加到 CMK 密钥策略中的密钥用户列表 (p. 108)
2. 为 WorkSpaces 管理员提供额外权限，并使用IAM策略 (p. 108)

WorkSpaces 管理员还需拥有使用WorkSpaces。有关这些权限的更多信息，请转到适用于 WorkSpaces 的 Identity and Access Management (p. 165)。

第 1 部分：向 CMK 的密钥用户添加 WorkSpaces 管理员

要为 WorkSpaces 管理员提供其所需的权限，您可以使用 AWS 管理控制台或 AWS KMS API。

添加 WorkSpaces 管理员作为 CMK 的密钥用户 (控制台)

1. 登录 AWS 管理控制台并通过以下网址打开 AWS Key Management Service (AWS KMS) 控制台：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 Customer managed keys (客户托管密钥)。
4. 选择首选客户托管 CMK 的密钥 ID 或别名。
5. 选择 Key policy (密钥策略) 选项卡。UNDER关键用户中，选择Add。
6. 在列表中IAM用户和角色，请选择与您的 WorkSpace 管理员对应的用户和角色，然后选择Add。

添加 WorkSpaces 管理员作为 CMK (API) 的密钥用户

1. 使用 GetKeyPolicy 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。添加IAM用户和角色，与您的 WorkSpace 管理员对应向关键用户授予权限。然后保存文件。
3. 使用 PutKeyPolicy 操作将密钥策略应用于 CMK。

第 2 部分：使用 IAM 策略向 WorkSpace 管理员授予其他权限

如果您选择用于加密的客户托管 CMK，则必须建立允许Amazon WorkSpaces代表您账户中启动加密 WorkSpaces 的 IAM 用户使用 CMK。该用户还需要使用 Amazon WorkSpaces 的权限。有关创建和编辑 IAM 用户策略的更多信息，请参阅管理 IAM 策略中的IAM 用户指南和适用于 WorkSpaces 的 Identity and Access Management (p. 165)。

WorkSpaces 加密需要对 CMK 拥有有限访问权限。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 CMK 的委托人与可以使用它的委托人分开。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。

第一个语句与默认 AWS KMS 密钥策略匹配。它授予您的账户使用 IAM 策略控制对 CMK 的访问的权限。第二个和第三个语句分别定义哪些 AWS 委托人可以管理和使用密钥。第四个语句允许与 AWS KMS 集成的 AWS 服务代表指定委托人使用密钥。该语句允许 AWS Services 创建和管理授权。该语句使用一个条件元素，该元素将对 CMK 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 AWS 管理控制台创建使用加密卷的 WorkSpaces，则管理员需拥有列出别名和密钥的权限（`"kms:ListAliases"`和`"kms:ListKeys"`权限）。如果您的 WorkSpaces 管理员仅使用 Amazon WorkSpace API（而不是控制台），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 WorkSpace 的用户或角色的 IAM 策略必须包含对于客户托管 CMK 的使用权限以及对 WorkSpace 的访问权限。要授予 IAM 用户或角色对 WorkSpace 的权限，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 CMK 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": "*"
        }
    ]
}
```

如果要在策略中指定 CMK，请使用类似于以下内容的 IAM 策略。将示例 CMK ARN 替换为有效 ARN。

```
{
  "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

加密 WorkSpace

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 选择 Launch WorkSpaces 并完成前三步。
3. 对于 WorkSpaces Configuration 步骤，执行以下操作：
   a. 选择要加密的卷：Root Volume、用户卷，或两种卷。
   b. 对于 Encryption Key (加密密钥)，选择一个 AWS KMS CMK，即由 Amazon WorkSpaces 创建的 AWS 托管 CMK 或您创建的 CMK。您选择的 CMK 必须是对称的。Amazon WorkSpaces 不支持非对称 CMK。
   c. 选择 Next Step。
4. 选择 Launch WorkSpaces。

查看加密的 WorkSpace

要从 WorkSpaces 控制台上查看哪些 WorkSpace 和卷已加密，请在左侧导航栏中选择 WorkSpace。Volume Encryption 列显示每个 WorkSpace 的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 Encrypted Volumes 字段。

重启 WorkSpace

有时，您可能需要手动重启（重新启动）WorkSpace。重启 WorkSpace 将会断开用户的连接，然后执行 WorkSpace 的关闭和重启操作。为避免数据丢失，请确保用户在重启 WorkSpace 之前，保存所有打开的文档和其他应用程序文件。用户数据、操作系统和系统设置不受影响。

> Warning
>
> 要重启已加密的 WorkSpace，请先确保 AWS KMS CMK 已启用；否则 WorkSpace 将变得不可用。要确定是否已启用 CMK，请参阅显示 CMK 详细信息中的AWS Key Management Service Developer Guide。

要重启 WorkSpace

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择要重启的 WorkSpace，然后选择 Actions、Reboot WorkSpaces。
4. 当系统提示您确认时，选择 Reboot WorkSpaces。

重建 WorkSpace

如果需要，您可以重建 WorkSpace。这将重新创建根卷、用户卷和主 elastic network interface。

重建 WorkSpace 将导致以下情况的出现：

- 将会使用从中创建 WorkSpace 的捆绑包的最新映像来刷新根卷（对于 Microsoft Windows，为 C；对于 Linux，为/）。在创建 WorkSpace 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。

  每 12 小时安排一次在重建 WorkSpace 时使用的自动快照。无论 WorkSpace 的运行状况如何，都会拍摄用户卷的这些快照。在选择操作、重建/恢复WorkSpace，则会显示最近快照的日期和时间。
- 主要弹性网络接口已重新创建。WorkSpace 会收到一个新的私有 IP 地址。

Important

在 2020 年 1 月 14 日之后，无法再重建从公有 Windows 7 捆绑包创建的 WorkSpaces。您可能需要考虑将您的 Windows 7 WorkSpaces 迁移到 Windows 10。有关更多信息，请参阅 迁移 WorkSpace (p. 118)。

仅在满足以下条件时，才可以重建 WorkSpace：

- WorkSpace 的状态必须为`AVAILABLE`、`ERROR`、`UNHEALTHY`、`STOPPED`，或者`REBOOTING`。WorkSpace 在`REBOOTING`状态下，您必须使用重建工作空间API 操作或修复工作区AWS 命令行界面 (CLI) 命令。
- 用户卷的快照必须存在。

要重建 WorkSpace

Warning

要重建已加密的 WorkSpace，请先确保 AWS KMS CMK 已启用；否则 WorkSpace 将变得不可用。要确定是否已启用 CMK，请参阅显示 CMK 详细信息中的AWS Key Management Service Developer Guide。

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择要重建的 WorkSpace，然后选择 Actions (操作)、Rebuild / Restore WorkSpace (重建 / 还原 WorkSpace)。
4. 选择重建 WorkSpace选项。
5. 选择重建/恢复WorkSpace。

Note

如果在 Active Directory 中更改用户的 sAMAccountName 用户命名属性后重建 WorkSpace，您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，请还原到原始用户命名属性，然后重新发起重建，或为该用户创建新的 WorkSpace。

还原 WorkSpace

如果需要，您可以将 WorkSpace 还原到其最后一个已知的运行状况良好状态。这将根据在 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。

还原 WorkSpace 将导致以下情况的出现：

- 根卷（对于 Microsoft Windows，为 C 驱动器；对于 Linux，为/）将恢复到最新快照。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基于以下基础进行的。在选择操作、重建/恢复WorkSpace，则会显示最近快照的日期和时间。

- 首次创建 WorkSpace 后 —通常，根卷和用户卷的初始快照将在创建 WorkSpace 后很快拍摄（通常在 30 分钟内）。在某些 AWS 区域中，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 (p. 111)或联系 AWS Support 寻求帮助。
- 在定期使用期间 —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，则不会创建这些快照。
- 恢复 WorkSpace 后 —恢复 WorWorkSpace 时，在恢复完成后很快（通常在 30 分钟内）就会生成新快照。在某些 AWS 区域中，恢复 WorkSpace 后可能需要几个小时才能拍摄这些快照。

  恢复 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 (p. 111)或联系 AWS Support 寻求帮助。

仅在满足以下条件时，才可以还原 WorkSpace：

- WorkSpace 的状态必须为`AVAILABLE`、`ERROR`、`UNHEALTHY`，或者`STOPPED`。
- 根卷和用户卷的快照必须存在。

还原 WorkSpace

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择要还原的 WorkSpace，然后选择 Actions (操作)、Rebuild / Restore WorkSpace (重建 / 还原 WorkSpace)。
4. 选择恢复 WorkSpace选项。
5. 选择重建/恢复WorkSpace。

升级 Windows 10 BYOL WorkSpace

在您的 Windows 10 自带许可 (BYOL) WorkSpaces 上，可以使用就地升级过程升级到 Windows 10 的较新版本。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 BYOL WorkSpaces。

> **Important**
>
> 不要在升级过的 WorkSpace 上运行 Sysprep。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，请仅在没有升级过的 WorkSpace 上进行。

目录

Prerequisites

- 如果您通过使用组策略或 System Center Configuration Manager (SCCM) 推迟或暂停 Windows 10 升级，请对您的 Windows 10 WorkSpaces 启用操作系统升级。
- 如果 WorkSpace 是 AutoStop WorkSpace，请在就地升级过程之前将其更改为 AlwaysOn WorkSpace，以便它不会在应用更新时自动停止。有关更多信息，请参阅 修改运行模式 (p. 100)。如果您希望将 WorkSpace 保留设置为 AutoStop，请在升级过程中将 AutoStop 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配置文件。

重要注意事项

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 WorkSpace 进行必要的更改，以使 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，WorkSpace 会在 `D:\Users\%USERNAME%` 中创建用户配置文件。`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。但请注意，无法在不丢失用户配置文件中所有数据的情况下重建或迁移在驱动器 C 上存储配置文件的 WorkSpace，除非您自行备份和还原这些数据。如果您决定在驱动器 C 上保留配置文件，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。

为了确保您可以重建或迁移 WorkSpace 并避免出现与用户 Shell 文件夹重定向相关的任何潜在问题，我们建议您选择在就地升级后将用户配置文件还原到驱动器 D。您可以通过使用 PostUpgradeRestoreProfileOnD 注册表项执行此操作，如本主题后面所述。

已知限制条件

- 在 WorkSpace 重建或迁移期间，不会发生用户配置文件位置从驱动器 D 更改到驱动器 C 的过程。如果您在 Windows 10 BYOL WorkSpace 上执行就地升级，然后重建或迁移它，则新的 WorkSpace 将会在 D 驱动器上拥有用户配置文件。

  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 捆绑包包含基于 Windows 10 早期版本的映像，则必须在重建或迁移 WorkSpace 后再次执行就地升级。

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\enable-inplace-升级.ps1

注册表项	类型	值
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 – 在就地升级后，还原用户配置文件路径 (ProfileImagePath)
UserShellFoldersRedirection	DWORD	0 – 不启用用户 Shell 文件夹的重定向 1 – (默认值) 在用户配置文件在 `C:\Users\%USERNAME%` 上重新生成后，启用将用户 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 –修改用户配置文件的注册表后，不允许脚本重启 WorkSpace

注册表路径：HKL M:\Software\Amazon\WorkSpacesConfig\update-pvdrivers.ps1

注册表项	类型	值
启用	DWORD	0 – (默认值) 禁用 AWS PV 驱动程序更新 1 – 启用 AWS PV 驱动程序更新

执行就地升级的步骤

要在 BYOL WorkSpace 上启用就地 Windows 升级，您必须设置某些注册表项，如下面的过程所述。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。如果要更新多个 WorkSpace，则可以使用组策略或 SCCM 推送 PowerShell 脚本。有关 PowerShell 脚本的示例，请参阅使用 PowerShell 脚本更新您的 WorkSpace 注册表 (p. 118)。

执行 Windows 10 就地升级

1. 记下要更新的 Windows 10 BYOL WorkSpace 上当前运行的 Windows 版本，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。这些注册表更改会启用 WorkSpace 的就地升级。

- HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\WorkSpacesConfig\enable-inplace-upgrade.ps1
- HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\WorkSpaceConfig\update-pvdrivers.ps1

Note

如果这些键不存在，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\WorkSpacesConfig\enable-inplace-upgrade.ps1\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，请参阅重要注意事项 (p. 114)），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\Amazon\WorkSpacesConfig\enable-inplace-upgrade.ps1

     键名称：PostUpgradeRestoreProfileOnD

     键值：0

     键名称：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\Amazon\WorkSpacesConfig\enable-inplace-upgrade.ps1

     键名称：PostUpgradeRestoreProfileOnD

     键值：1

     键名称：UserShellFoldersRedirection

     键值：0

4. 保存注册表更改后，再次重新启动 WorkSpace 以便应用更改。

   Note

   重新启动后，登录到 WorkSpace 会创建一个新的用户配置文件。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。

   （可选）确认以下键值设置为 1，这将取消阻止 WorkSpace 进行更新：

   HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\WorkSpacesConfig\enable-inplace-upgrade.ps1\profileImagePathDeleted

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)。根据您的原始 Windows 10 版本和安装的应用程序数量，此过程可能需要 40-120 分钟。
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 会自动回滚以使用开始升级之前已安装的 Windows 10 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\WorkSpacesConfig\enable-inplace-upgrade.ps1\scriptExecutionComplete

7. 如果您通过将 WorkSpace 的运行模式设置为 AlwaysOn 或通过更改 AutoStop 时间段来设置它，以便就地升级过程可以不中断地运行，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 (p. 100)。

如果您尚未将 PostUpgradeRestoreProfileOnD 注册表项设置为 1，则在就地升级后 Windows 将重新生成用户配置文件并将其放在 `C:\Users\%USERNAME%` 中，这样，您就不必在将来进行 Windows 10 就地更新时再次执行上述步骤。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`

如果将 shell 文件夹重定向到 WorkSpaces 上的其他位置，请在就地升级后对 WorkSpaces 执行必要的操作。

Troubleshooting

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：Amazon WorkSpaces

  Tip

  在就地升级过程中，如果您发现桌面上的某些图标快捷方式不再有效，那是因为 WorkSpaces 会将位于驱动器 D 上的任何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 脚本来更新 WorkSpaces 上的注册表以启用就地升级。按照执行就地升级的步骤 (p. 115)，但使用此脚本更新每个 WorkSpace 上的注册表。

```
# AWS WorkSpaces 1.28.20
# Enable In-Place Update Sample Scripts
# These registry keys and values will enable scripts to execute 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

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，或从 PCoIP 协议迁移到 WorkSpaces Streaming Protocol (WSP)。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。例如，您可以从启用 GPU（图形和 GraphicSpro）的捆绑包迁移到非启用 GPU 的捆绑包，反之亦然。有关 Amazon WorkSpaces 捆绑包的更多信息，请参阅WorkSpace 服务包和映像 (p. 123)。

迁移过程通过使用目标捆绑包映像中的新根卷和原始 WorkSpace 的上一个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 (p. 120)。）

对于每个 WorkSpace，迁移过程最多需要一个小时。启动迁移过程时，将创建一个新的 WorkSpace。如果发生错误阻止成功迁移，将恢复原始 WorkSpace 并返回到其原始状态，并终止新的 WorkSpace。

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。
- 您只能将 BYOL WorkSpaces 迁移到其他 BYOL 捆绑包。
- 无法将从公有或自定义捆绑包创建的 WorkSpace 迁移到 BYOL 捆绑包。
- 目前不支持迁移 Linux WorkSpaces。
- 在支持多种语言的 AWS 区域中，您可以在语言包之间迁移 WorkSpaces。
- 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。）如果要使用相同的捆绑包刷新 WorkSpace，请改为重新构建 WorkSpace (p. 111)。
- 您不能跨区域迁移 WorkSpace。
- 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，则迁移失败。请联系 AWS Support Center 以获取帮助。

可用的迁移方案

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
自定义捆绑包 Windows 10	公有捆绑包 Windows 10	否

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 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

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。在新的 WorkSpace 首次启动期间，迁移过程会将原始 `D:\Users\%USERNAME%` 文件夹移动到名为 `D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated` 的文件夹。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。

分配给原始 WorkSpace 的任何标签都会在迁移过程中进行转移，并保留 WorkSpace 的运行模式。但是，新的 WorkSpace 将获得新的 WorkSpace ID、计算机名称和 IP 地址。

最佳实践

在迁移 WorkSpace 之前，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。
- 请确保正在迁移的 WorkSpace 至少已有 12 小时，以确保已创建用户卷的快照。在存储库的迁移 WorkSpaces页面中的Amazon WorkSpaces控制台中，您可以看到最后一个快照的时间。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 WorkSpaces，并在迁移过程完成后才重新登录。请注意，WorkSpaces 处于 `ADMIN_MAINTENANCE` 模式时无法迁移。

- 请确保要迁移的 WorkSpaces 的状态为 AVAILABLE、STOPPED 或 ERROR。
- 请确保您有足够的 IP 地址用于要迁移的 WorkSpaces。迁移期间，将为 WorkSpaces 分配新的 IP 地址。
- 如果您正在使用脚本迁移 WorkSpaces，请以一次不超过 25 个 WorkSpaces 的批次迁移它们。

Troubleshooting

- 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。
- 如果您使用 API 迁移 WorkSpaces，但迁移未获成功，则不会使用 API 返回的目标 WorkSpace ID，并且 WorkSpace 仍将具有原始 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不再需要的 WorkSpaces。

账单如何受到影响

在执行迁移的月份，将按比例对新 WorkSpaces 和原始 WorkSpaces 收取费用。例如，如果您在 5 月 10 日将工作区 A 迁移到工作区 B，则将向您收取 5 月 1 日至 5 月 10 日期间工作区 A 的费用，以及 5 月 11 日至 5 月 30 日期间工作区 B 的费用。

> **Note**
>
> 如果要将 WorkSpace 迁移到不同的捆绑包类型（例如，从性能到节能，或从高价值到标准），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值，并为新捆绑包使用默认的用户卷大小。

迁移 WorkSpace

您可以通过 Amazon WorkSpaces 控制台、AWS 命令行界面 (CLI) 或 Amazon WorkSpaces API 迁移 WorkSpace。

迁移 WorkSpace

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择 WorkSpace，然后依次选择 Actions (操作) 和 Migrate WorkSpaces (迁移 WorkSpaces)。
4. 在 Select Target Bundle (选择目标捆绑包) 下，选择要将 WorkSpace 迁移到的捆绑包。
5. 在 Assign WorkSpace Bundle (分配 WorkSpace 捆绑包) 下，为每个 WorkSpace 用户选择目标捆绑包。

   > **Warning**
   >
   > 对于每个 WorkSpace，请记下列出的快照时间。在所列快照时间之后对用户卷所做的任何更改都将在迁移过程中丢弃。
6. 选择 Migrate WorkSpaces (迁移 WorkSpaces)。

   Amazon WorkSpaces 控制台中将显示一个状态为 PENDING 的新 WorkSpace。迁移完成后，原始 WorkSpace 将终止，并将新 WorkSpace 的状态设置为 AVAILABLE。
7. （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 WorkSpace 服务包或映像 (p. 138)。

要通过 AWS CLI 迁移 WorkSpace，请使用 migrate-workspace 命令。要 WorkSpaces 过Amazon WorkSpacesAPI，请参阅MigrateWorkSpace中的Amazon WorkSpaces API 参考。

删除工作区

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

删除工作区是一项永久性操作，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可供您免费使用，以便与 WorkSpaces 一起使用。如果没有任何 WorkSpaces 正在与Simple AD或者AD Connector目录中连续 30 天，此目录将自动取消注册，以便与Amazon WorkSpaces，并且您将根据AWS Directory Service定价条款。
要删除空目录，请参阅删除您的 WorkSpace 目录 (p. 62)。如果删除Simple AD或者AD Connector目录中，当您想要重新开始使用 WorkSpaces 时，您始终可以创建一个新的目录。

删除 WorkSpace

您可以 WorkSpace 除处于`SUSPENDED`。

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择 WorkSpace，然后选择 Actions、Remove WorkSpaces。
4. 当系统提示您确认时，选择 Remove WorkSpaces。删除 WorkSpace 大约需要 5 分钟时间。删除过程中，WorkSpace 的状态设置为`TERMINATING`。删除完毕后，状态会很简单地设置为`TERMINATED`之前，WorkSpace 从控制台消失。
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 WorkSpace 服务包或映像 (p. 138)。
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 删除您的 WorkSpace 目录 (p. 62)。
7. (可选) 删除 Virtual Private Cloud (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 。删除 VPC和使用弹性 IP 地址中的Amazon VPC 用户指南。

WorkSpace 服务包和映像

WorkSpace 服务包 是操作系统、存储、计算和软件资源的组合。当您启动 WorkSpace 时，选择符合您需求的服务包。WorkSpace 可用的默认服务包称为公有服务包。有关 WorkSpaces 可用的各种公有服务包的更多信息，请参阅 Amazon WorkSpace 服务包。

如果您已启动 Windows 或 Amazon Linux WorkSpace 并对其进行了自定义，则可以从该 WorkSpace 创建自定义映像。

自定义映像 只包含操作系统、软件和 WorkSpace 设置。自定义服务包 是自定义映像和 WorkSpace 启动所依赖的硬件的集合。

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 WorkSpace 映像与您选择的基础计算和存储配置相结合。然后，您可以在启动新的 WorkSpace 时指定此自定义服务包，以确保新的 WorkSpace 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 WorkSpace 上安装其他软件，可以更新您的自定义服务包并使用它来重建您的 WorkSpace。

目录

创建自定义 WorkSpace 映像和服务包

如果您已启动 Windows 或 Amazon Linux WorkSpace 并对其进行了自定义，则可以从该 WorkSpace 创建自定义服务包和自定义映像。

自定义映像 只包含操作系统、软件和 WorkSpace 设置。自定义服务包 是自定义映像和 WorkSpace 启动所依赖的硬件的集合。

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，您可以在启动新的 WorkSpace 时指定此自定义服务包，以确保新的 WorkSpace 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

- 如果您打算从 Windows 10 WorkSpace 创建映像，请注意，已经从一个版本的 Windows 10 升级到了较新的 Windows 10 版本（Windows 功能/版本升级）的 Windows 10 系统不支持映像创建。但是，Windows 累积更新或安全更新由 WorkSpaces 映像创建过程支持。
- 2020 年 1 月 14 日之后，无法从公有 Windows 7 捆绑包创建映像。您可能需要考虑将您的 Windows 7 WorkSpaces 迁移到 Windows 10。有关更多信息，请参阅 迁移 WorkSpace (p. 118)。
- Graphics 和 GraphicSPro 服务包当前不可用于亚太地区（孟买）区域。

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。

目录

创建 Windows 自定义映像的要求

- 工作区的状态必须为可用，其修改状态必须为无。
- WorkSpace 映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 盘上。
- 用户配置文件必须存在且位于 `D:\Users\username`，其总大小（文件和数据）必须小于 10GB。
- C 驱动器必须至少有 12 GB 的可用空间。
- 所有运行在 WorkSpace 上的应用程序服务必须使用本地系统账户，而不是域用户凭证。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。目前不支持从加密的 WorkSpace 创建映像。
- 映像中要求具有以下组件。如果没有这些组件，从映像启动的 WorkSpace 将无法正常工作：
  - Windows PowerShell 3.0 或更高版本
  - 远程桌面服务
  - AWS PV 驱动程序
  - 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 Amazon Linux 自定义映像的要求

- 工作区的状态必须为可用，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。目前不支持从加密的 WorkSpace 创建映像。
- 映像中要求具有以下组件。如果没有这些组件，从映像启动的 WorkSpace 将无法正常工作：
  - Cloud-init
  - Teradici PCoIP 代理和驱动程序
  - Skylight 代理

最佳实践

从 WorkSpace 创建映像前，请执行以下操作：

- 使用未连接到您的生产环境的单独 VPC。
- 在私有子网中部署 WorkSpace，并将 NAT 实例用于出站流量。
- 使用小的 Simple AD 目录。
- 为源 WorkSpace 使用最小卷大小，然后在创建自定义服务包时根据需要调整卷大小。
- 在工作区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。有关更多信息，请参阅本主题开始处的重要提示 (p. 123)。
- 删除 WorkSpace 中不应该包含在服务包中的缓存数据 (例如，浏览器历史记录、缓存文件和浏览器 Cookie)。
- 删除 WorkSpace 中不应该包括在服务包中的配置设置（例如，电子邮件配置文件）。
- 使用 DHCP 切换到动态 IP 地址设置。
- 确保您没有超过区域中允许的 WorkSpace 映像数量的配额。默认情况下，每个区域允许您具有 40 个 WorkSpace 映像。如果您已达到此配额，创建映像的新尝试将失败。要请求增加配额，请使用 WorkSpaces 限制表单。
- 请确保您没有尝试从加密的 WorkSpace 创建映像。目前不支持从加密的 WorkSpace 创建映像。
- 如果 WorkSpace 上正在运行任何防病毒软件，请在尝试创建映像时禁用该软件。
- 如果在 WorkSpace 上启用了防火墙，请确保防火墙未阻止任何必要的端口。有关更多信息，请参阅WorkSpaces 的 IP 地址和端口要求 (p. 16)。
- 对于 Windows WorkSpace，请勿在创建映像之前配置任何组策略对象 (GPO)。
- 对于 Windows WorkSpace，在创建映像之前，请勿自定义默认用户配置文件 (`C:\Users\Default`)。我们建议通过 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 Linux 映像准备 Amazon WorkSpaces 的最佳实践白皮书。
- 如果您想在 Linux WorkSpaces 中使用智能卡WorkSpaces Streaming Protocol (WSP)已启用，请参阅使用智能卡进行身份验证 (p. 34)，以获取在创建映像之前必须对 Linux WorkSpace 进行的自定义。

（可选）步骤 1：为映像指定自定义计算机名格式

对于从自定义或自带许可证 (BYOL) 映像启动的 WorkSpaces，您可以为计算机名称格式指定自定义前缀，而不是使用默认计算机名格式 (p. 66)。要指定自定义前缀，请按照映像类型的相应步骤操作。

为自定义图像指定自定义计算机名称格式

1. 在用于创建自定义映像的 WorkSpace 上，打开`C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xml`在记事本或其他文本编辑器中。有关使用`Unattend.xml`文件，请参阅应答文件 (unattend.xml)在微软文档中。

   Note

   要从 WorkSpace 上的 Windows 文件资源管理器访问 C: 驱动器，请输入**`C:\`**地址栏中。

2. 请在 `<settings pass="specialize">` 部分执行以下操作：

   a. 确保`<ComputerName>`设置为星号（`*`）。如果`<ComputerName>`设置为任何其他值，则将忽略您的自定义计算机名称设置。有关的更多信息`<ComputerName>`设置，请参阅计算机名在微软文档中。

   b. （可选）设置`<RegisteredOrganization>`设置为您首选的组织名称。

3. 在`<settings pass="oobeSystem">`部分，设置`<RegisteredOrganization>`和`<RegisteredOwner>`设置为您首选的值。

   在 Sysprep 期间，您为`<RegisteredOwner>`和`<RegisteredOrganization>`连接在一起，并使用组合字符串的前 7 个字符来创建计算机名称。例如，如果指定**`Amazon.com`**对于 来说为`<RegisteredOrganization>`和**`EC2`**对于 来说为`<RegisteredOwner>`，则从您的自定义捆绑包创建的 WorkSpaces 的计算机名称将以 EC2AMAZ-*xxxxxxx*.

4. 保存对 Unattend.xml 文件的更改。

为 BYOL 图像指定自定义计算机名称格式

1. Open C:\Program Files\Amazon\Ec2ConfigService\Sysprep2008.xml在记事本或其他文本编辑器中。
2. 在<settings pass="specialize">部分，取消注释<ComputerName>*</ComputerName>，并确保<ComputerName>设置为星号 (*)。如果<ComputerName>设置为任何其他值，则将忽略您的自定义计算机名称设置。有关的更多信息<ComputerName>设置，请参阅计算机名在微软文档中。
3. 在<settings pass="specialize">部分，设置<RegisteredOrganization>和<RegisteredOwner>设置为您首选的值。

   在 Sysprep 期间，您为<RegisteredOwner>和<RegisteredOrganization>连接在一起，并使用组合字符串的前 7 个字符来创建计算机名称。例如，如果指定**Amazon.com**对于 来说为<RegisteredOrganization>和**EC2**对于 来说为<RegisteredOwner>，则从您的自定义捆绑包创建的 WorkSpaces 的计算机名称将以 EC2AMAZ-*xxxxxxx*.

   Note

   这些区域有：<RegisteredOrganization>和<RegisteredOwner>中的值<settings pass="oobeSystem">部分将被 Sysprep 忽略。
4. 保存对 Sysprep2008.xml 文件的更改。

步骤 2: 运行映像检查程序

Note

映像检查程序仅适用于 Windows WorkSpace。如果要从 Linux WorkSpace 创建映像，请跳至步骤 3: 创建自定义映像和自定义服务包 (p. 132)。

要确认 Windows WorkSpace 满足映像创建的要求，我们建议运行映像检查程序。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。

Important

- WorkSpace 必须先通过映像检查程序运行的所有测试，然后才能用于创建映像。
- 在运行映像检查程序之前，请验证是否在 WorkSpace 上安装了最新的 Windows 安全更新和累积更新。
- 图像检查器不检查 Windows 10 WorkSpaces 的用户配置文件大小。如果您有 Windows 10 WorkSpace，请确保用户配置文件大小小于 10 GB。

要获取映像检查程序，请执行以下操作之一：

- 重启 WorkSpace (p. 111)。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。
- 下载Amazon WorkSpaces映像检查程序从https://tools.amazonworkspaces.com/ImageChecker.zip 并解压缩ImageChecker.exe文件。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 Image Checker (Amazon WorkSpaces 映像检查程序) 对话框中，选择 Run (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 (p. 127)。

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. 适当时，请解决导致测试失败和警告的任何问题，然后重复运行映像检查程序的过程，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. 如果您的 WorkSpace 通过了所有测试，您将看到 Validation Successful (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`。

必须安装 PowerShell 3.0 或更高版本

安装最新版本的 Microsoft Windows PowerShell。

Important

必须将 WorkSpace 的 PowerShell 执行策略设置为允许 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 Unrestricted 或 RemoteSigned，请运行 Set-ExecutionPolicy –ExecutionPolicy RemoteSigned 命令以更改执行策略的值。RemoteSigned 设置允许在 Amazon WorkSpaces 上执行脚本，这是创建映像所需的。

只可存在 C 和 D 驱动器

只有 `C` 和 `D` 驱动器可以存在于用于创建映像的 WorkSpace 上。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，Windows 累积更新或安全更新由 WorkSpaces 映像创建过程支持。

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 Center以修复您的 EC2Config 或 EC2Launch。

用户配置文件大小必须小于 10 GB

用户配置文件 (`D:\Users\username`) 的总大小必须小于 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

驱动器 `C` 上必须至少有 12 GB 的可用空间。根据需要删除文件以释放 `C` 驱动器上的空间。

无法在域账户下运行任何服务

要运行创建映像过程，WorkSpace 上的任何服务都不能在域账户下运行。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 OK。

必须安装 Amazon WorkSpaces Application Manager (Amazon WAM)

如果您已使用 Amazon WAM 将应用程序分配给用户，则必须在 WorkSpace 上设置 Amazon WAM 安装程序。完成后，Amazon WAM 快捷方式将显示在您的 WorkSpace 桌面上。

必须将 WorkSpace 配置为使用 DHCP

必须将 WorkSpace 上的所有网络适配器配置为使用 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 Internet 协议版本 4 (TCP/IPv4)，然后选择属性。
7. 在 Internet 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 OK。
9. 对 WorkSpace 上的所有网络适配器重复此过程。

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 OK。

用户配置文件必须存在

用于创建映像的 WorkSpace 必须具有用户配置文件(`D:\Users\username`)。如果此测试失败，请联系 AWS Support Center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与 System32 和 Windows PowerShell 对应的条目。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 OK。
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 WorkSpace 的环境变量路径与新创建的 WorkSpace 或新 Windows 实例中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 OK。

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 OK。

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。

WorkSpace 上只能存在一个用户配置文件

WorkSpace 上只能有一个用于创建映像的 WorkSpace 用户配置文件 (`D:\Users\`*`username`*) 。删除不属于 WorkSpace 的预期用户的任何用户配置文件。

为了能够创建映像，您的 WorkSpace 上只能有三个用户配置文件：

- WorkSpace 的预期用户的用户配置文件(`D:\Users\username`)
- 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：
   - 按窗口键 + 暂停休息，然后选择。高级系统设置的左侧窗格中的控制面板 >系统和安全性 >系统对话框中。
   - 在 Windows 搜索框中，输入 **`control panel`**。在控制面板中，选择系统和安全性，然后选择 System (系统)，然后选择高级系统设置的左侧窗格中的控制面板 >系统和安全性 >系统对话框中。
2. 在系统属性对话框中的高级选项卡上，选择。设置根据用户资料。
3. 如果除了管理员配置文件、默认配置文件和预期 WorkSpace 用户的配置文件以外列出了任何配置文件，请选择该额外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 和步骤 4 以删除不属于 WorkSpace 的任何其他配置文件。
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 程序包，然后在每个程序包之后按 Enter 键。

```
$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，请使用尚未进行 Windows 功能/版本升级的 WorkSpace 。

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。

其他故障排查技巧

如果 WorkSpace 通过了映像检查程序运行的所有测试，但仍然无法从 WorkSpace 创建映像，请检查以下问题：

- 请确保 WorkSpace 未分配给 Domain Guests (域来宾) 组中的用户。要检查是否存在任何域账户，请运行以下 PowerShell 命令。

  ```
  Get-WmiObject -Class Win32_Service | Where-Object { $_.StartName -like "*
  $env:USERDOMAIN*" }
  ```

- 仅适用于 Windows 7 WorkSpaces：如果在映像创建过程中复制用户配置文件时出现问题，请检查以下问题：
  - 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 WorkSpace 移到具有阻止继承且未应用 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 OK。

步骤 3: 创建自定义映像和自定义服务包

验证 WorkSpace 映像后，可以继续执行创建自定义映像和自定义服务包的过程。

创建自定义映像和自定义服务包

1. 如果您仍然连接着 WorkSpace，请在 WorkSpace 中选择Amazon WorkSpaces和Disconnect。
2. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
3. 在导航窗格中，选择 WorkSpaces。
4. 选择 WorkSpace，然后选择 Actions、Create Image。
5. 将显示一条消息，提示您在继续操作之前重新启动 WorkSpace。重新启动 WorkSpace 会更新Amazon WorkSpaces软件添加到最新版本。

   请 WorkSpace 闭消息并按照重启 WorkSpace (p. 111)。完成此操作后，重复Step 4 (p. 132)这个过程，但这次选择下一页当显示重启消息时。要创建映像，WorkSpace 的状态必须为 Available (可用)，其修改状态必须为 None (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。在创建映像的过程中，WorkSpace 的状态为 Suspended (暂停)，并且 WorkSpace 不可用。
7. 在导航窗格中，选择 Images。当 WorkSpace 的状态变为Available（这最多需要 45 分钟）。
8. 选择映像，然后选择 Actions、Create Bundle。

   Note

   要以编程方式创建捆绑包，请使用CreateWorkspaceBundleAPI 操作。有关更多信息，请参阅 。创建工作空间捆绑中的Amazon WorkSpaces API 参考。
9. 输入服务包的名称和描述，然后执行以下操作：

   - 对于 Bundle Type (服务包类型)，选择从该自定义服务包启动 WorkSpaces 时要使用的硬件。
   - 对于Root Volume Size (根卷大小)，保留默认值或者输入等于或大于当前大小的新值。然后，在用户卷大小中输入一个值。

     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 和 GraphicPro WorkSpace：根：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

     要确保您的数据得以保留，在启动 WorkSpace 后，您不能减小根卷或用户卷的大小。而是确保在启动 WorkSpace 时为这些卷指定最小大小。您可以启动最低根卷容量为 80 GB、最低用户卷容量为 10 GB 的 Value、Standard、Performance、Power 或 PowerPro WorkSpace。您可以启动最低根卷容量为 100 GB、最低用户卷容量为 100 GB 的 Graphics 或 GraphicsPro WorkSpace。
10. 选择创建服务包。
11. 要确认您的捆绑包已创建，请选择捆绑并验证是否列出了捆绑包。

Windows WorkSpace 自定义映像中包含的内容

从 Windows 7 或 10 WorkSpace 创建映像时，将包括 C 驱动器的全部内容。

对于 Windows 10 WorkSpace，`D:\Users\`*`username`* 中的用户配置文件不包括在自定义映像中。

对于 Windows 7 WorkSpace，还将包含 `D:\Users\username` 中用户配置文件的全部内容，不过以下内容除外：

- 联系人
- 下载
- 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 internet 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\

Amazon Linux WorkSpace 自定义映像包含的内容

从 Amazon Linux WorkSpace 创建映像时，将删除用户卷 (/home) 中的整个内容。删除内容中包括根卷 (/) 的内容，但以下文件夹和密钥除外：

- /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
- /etc/security/access.conf
- /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

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 WorkSpace 服务包

您可以更新现有的自定义 WorkSpace 服务包，方法是修改基于服务包的 WorkSpace，从 WorkSpace 创建映像，然后用新映像更新服务包。然后，您可以使用更新的服务包启动新的 WorkSpace。

> **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。

使用控制台更新服务包

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服务包的映像相同的基本软件包（Plus 或 Standard），然后进行更改。
2. 如果您还连接着 WorkSpace，请断开。
3. 通过以下网址打开 WorkSpaces 控制台：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。
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。
7. 在导航窗格中，选择 Bundles。
8. 选择服务包，然后选择 Actions、Update Bundle。

9. 对于 Update WorkSpace Bundle，选择创建的映像并选择 Update Bundle。
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 WorkSpace (p. 111)。

以编程方式更新服务包

要以编程方式更新服务包，请使用UpdateWorkspaceBundleAPI 操作。有关更多信息，请参阅 。更新工作空间包中的Amazon WorkSpaces API 参考。

复制自定义 WorkSpace 映像

您可在内部或跨部复制自定义 WorkSpaces 映像AWS区域。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。

> **Note**
>
> 在中国 (宁夏) 区域，您只能在同一区域内复制镜像。
> 在AWS GovCloud（美国西部） 区域，要向其他 AWS 区域复制映像，请联系 AWS Support。

您还可以复制已与您共享的镜像AWSaccount. 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 (p. 136)。

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Amazon WorkSpaces 配额 (p. 193)。

用于复制映像的 IAM 权限

如果您使用 IAM 用户复制映像，则用户必须具有`workspaces:DescribeWorkspaceImages`和`workspaces:CopyWorkspaceImage`。

以下示例策略允许用户将指定映像复制映像到指定的区域中的指定账户。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:DescribeWorkspaceImages",
        "workspaces:CopyWorkspaceImage"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:123456789012:workspaceimage/wsi-a1bcd2efg"
      ]
    }
  ]
}
```

> **Important**
>
> 如果您正在为不拥有映像的账户创建用于复制共享映像的 IAM 策略，则无法在 ARN 中指定账户 ID。而是必须使用*作为账户 ID，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"
      ]
    }
  ]
}
```

只有当该帐户拥有要复制的映像时，才能在 ARN 中指定帐户 ID。

有关使用 IAM 的更多信息，请参阅适用于 WorkSpaces 的 Identity and Access Management (p. 165)。

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，请使用 CopyWorkspaceImage API 操作或 AWS 命令行界面 (CLI) 中的 copy-workspace-image 命令。有关更多信息，请参阅 。CopyWorkspaceImage中的Amazon WorkSpaces API 参考或请参阅复制工作空间映像中的AWS CLI Command Reference。

> Important
>
> 在复制共享映像之前，请确保验证共享映像是否已从正确的AWSaccount. 要确定图像是否已共享并查看AWS拥有映像的账户 ID，请使用说明工作空间图像和说明工作空间图像权限API 操作或描述工作区图像和描述-工作空间映像权限的命令AWSCLI。

使用控制台复制映像

1. 通过以下网址打开 WorkSpaces 控制台：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 Actions、Copy Image。
4. 为复制的映像提供名称、描述和区域信息，然后选择 Copy Image。

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 WorkSpace 映像 (p. 135)。

> Note
>
> 在中国 (宁夏) 区域，您只能在同一区域内复制镜像。
> 在AWS GovCloud（美国西部） 区域，要向其他 AWS 区域复制映像，请联系 AWS Support。

共享映像不会产生额外的费用。但是，在镜像数量配额AWS适用区域。在收件人复制映像之前，共享映像不会计入收件人帐户的配额。有关 Amazon WorkSpaces 配额的更多信息，请参阅Amazon WorkSpaces 配额 (p. 193)。

要删除映像，必须先取消映像共享，然后才能删除映像。

共享自带许可映像

您只能与共享自带许可 (BYOL) 映像AWS为 BYOL 启用的帐户。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**
>
> 共享 BYOL 图像AWS帐户目前不受支持AWS GovCloud (US-West)区域。若要在AWS GovCloud (US-West)区域，联系AWSSupport。

与您共享的图像

如果与您共享图像，您可以复制它们。然后，您可以使用您的共享映像副本创建用于启动新 WorkSpaces 的服务包。

> **Important**
>
> 在复制共享映像之前，请确保验证共享映像是否已从正确的AWSaccount. 要以编程方式确定图像是否已共享，请使用说明工作空间图像和说明工作空间图像权限API 操作或描述工作区图像和描述-工作空间映像权限的命令AWS命令行界面 (CLI)。

为已与您共享的映像显示的创建日期是最初创建映像的日期，而不是与您共享映像的日期。

如果已与您共享图像，您将无法进一步与其他帐户共享该图像。

共享图像

1. 通过以下网址打开 WorkSpaces 控制台：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、查看详细信息。
4. 在图片详细信息页面上，在共享账户部分，选择。添加账户。
5. 在存储库的添加账户页面，在添加要共享的帐户中，输入要与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. 选择共享图片。

   > **Note**
   >
   > 要使用共享映像，收件人帐户必须首先复制映像 (p. 135)。然后，收件人账户可以使用其共享映像副本创建用于启动新 WorkSpaces 的服务包。

停止共享映像

1. 通过以下网址打开 WorkSpaces 控制台：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、查看详细信息。
4. 在图片详细信息页面上，在共享账户部分中，选择AWS帐户停止共享，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**
   >
   > 如果要在取消共享后删除该图像，则必须首先从共享该图像的所有帐户中取消共享。

停止映像共享后，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图像

要以编程方式共享或取消共享图像，请使用更新工作空间图像权限API 操作或更新工作空间映像权限AWS 命令行界面 (CLI) 命令。要确定图像是否已共享，请使用说明工作空间图像权限API 操作或描述-工作空间映像权限CLI 命令。

删除自定义 WorkSpace 服务包或映像

如果需要，您可以删除未使用的自定义服务包。如果删除正在被 WorkSpace 使用的某个服务包，则该服务包将被放在删除队列中，然后在基于该服务包的所有 WorkSpace 被删除后删除。

使用控制台删除服务包

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Bundles。
3. 选择服务包，然后选择 Actions、Delete Bundle。
4. 当系统提示您确认时，选择 Delete Bundle。

以编程方式删除服务包

要以编程方式删除服务包，请使用DeleteWorkspaceBundleAPI 操作。有关更多信息，请参阅 。删除工作空间包中的Amazon WorkSpaces API 参考。

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。

> Note
>
> 要删除映像，您必须首先删除与该映像关联的所有服务包，如果与其他账户共享该映像，则取消共享。此外，映像不能处于 `PENDING` 或 `VALIDATING` 状态。

使用控制台删除镜像

1. 通过以下网址打开 WorkSpaces 控制台：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 Actions、Delete Image。
4. 当系统提示您确认时，选择 Delete Image。

以编程方式删除镜像

要以编程方式删除镜像，请使用DeleteWorkspaceImageAPI 操作。有关更多信息，请参阅 。删除工作空间图像中的Amazon WorkSpaces API 参考。

自带 Windows 桌面许可证

如果您与 Microsoft 签订的许可协议允许使用此类映像，则可以为工作区使用 Windows 10 企业版或 Windows 10 专业版桌面许可证。为此，您必须自带许可 (BYOL) 并提供满足以下要求的 Windows 10 许可证。有关在上使用 Microsoft 软件的更多信息AWS，请参阅Amazon Web Services。

要遵守微软许可条款，AWS在 AWS 云中专供您使用的硬件上运行 BYOL WorkSpaces。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 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，Windows 累积更新或安全更新由 WorkSpaces 映像创建过程支持。

要开始使用，请打开 WorkSpaces 控制台，然后选择 Account Settings (账户设置) 为您的账户启用 BYOL。

目录

Requirements

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。
- 如果您要使用未启用 GPU 的捆绑包（Graphics 和 GraphicSPro 以外的捆绑包），请验证您至少使用 200 个WorkSpaces每个区域。这 200 个 WorkSpace 可以是 AlwaysOn 和 AutoStop WorkSpace 的任意组合。每个区域至少使用 200 个 WorkSpaces 是运行您的WorkSpaces在专用硬件上。在专用硬件上运行您的 WorkSpaces 需要符合 Microsoft 许可要求。专用硬件在 AWS 端预配置，因此您的 VPC 可以保持默认租赁状态。

  如果您计划使用启用 GPU（Graphics 和 GraphicsPro）的捆绑包，请验证您在专用硬件上每个月在一个区域中是否至少会运行 4 个 AlwaysOn 或 20 个 AutoStop 支持 GPU 的 WorkSpace。

  Note

  启用 GPU 的捆绑包当前在亚太地区（孟买）区域。
- WorkSpaces 可以在 /16 IP 地址范围内使用管理接口。管理接口连接到一个用于交互式流式传输的安全 WorkSpaces 管理网络。这样可允许 WorkSpaces 管理您的 WorkSpace。有关更多信息，请参阅 网络接口 (p. 28)。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

  - 在采用 WorkSpaces 服务时，可用的管理接口 IP 地址范围经常会发生变化。要确定当前可用的范围，请运行 list-available-management-cidr-ranges AWS Command Line Interface (AWS CLI) 命令。
  - 除了您选择的 /16 CIDR 块之外，54.239.224.0/20 IP 地址范围还用于所有 AWS 区域的管理接口流量。
- 请确保您已打开必要的管理界面端口为微软 Windows 和微软办公室 KMS 激活 BYOL WorkSpaces。有关更多信息，请参阅 管理接口端口 (p. 30)。
- 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 (p. 140)。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。我们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。
  - 在共享映像之前，您必须创建具有本地管理员访问权限的 WorkSpaces_BYOL 账户。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。如果您还打算为 BYOL 映像订阅 Microsoft Office，VM 必须位于最大大小为 70 GB 且可用空间至少为 20 GB 的单个卷上。
  - VM 必须运行 Windows PowerShell 版本 4 或更高版本。
- 在本主题后面的步骤 2 (p. 143) 中运行 BYOL 检查程序 PowerShell 脚本之前，请确保您已安装最新的 Microsoft Windows 补丁。

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 1809（2018 年 10 月更新）
- Windows 10 版本 1903（2019 年 5 月更新）
- Windows 10 版本 1909（2019 年 11 月更新）
- 视窗 10 版本 (二零零年五月更新)
- 视窗 10 版本二零零年十月更新

所有受支持的操作系统版本都支持您使用 WorkSpaces 时所在 AWS 区域中可用的所有计算类型。不再受 Microsoft 支持的 Windows 版本不能保证正常工作，也不受 AWS Support 支持。

将微软办公室添加到您的 BYOL 映像

在 BYOL 映像摄入过程中，如果您使用的是 Windows 10，您可以选择通过 AWS 订阅微软办公室专业版 2016 年（32 位）或 2019 年（64 位）。如果选择此选项，Office 将预安装在您的 BYOL 映像中，并包含在您从此映像启动的任何 WorkSpaces 中。

如果您选择通过 AWS 订阅 Office，将收取额外费用。有关更多信息，请参阅 WorkSpaces 定价。

Important

- 如果您正在用于创建 BYOL 映像的虚拟机上已安装 Microsoft Office，则如果要通过 AWS 订阅 Office，则必须将其从虚拟机中卸载。
- 如果您计划通过 AWS 订阅 Office，请确保您的 VM 至少有 20 GB 的可用磁盘空间。

如果您选择订阅 Office，则 BYOL 映像摄入过程至少需要 3 小时。

有关在 BYOL 接收过程中订阅 Office 的详细信息，请参阅步骤 5：使用创建 BYOL 映像WorkSpaces控制台 (p. 145)。

Office 语言设置

我们选择用于 Office 订阅的语言，基于AWS您正在执行 BYOL 图像摄取的区域。例如，如果您正在亚太区域（东京），则您的 Office 订阅使用日语作为其语言。

默认情况下，我们会在您的 WorkSpaces 上安装许多常用 Office 语言包。如果未安装所需的语言包，则可以从 Microsoft 下载其他语言包。有关更多信息，请参阅 。办公语言配件包在微软文档中。

您可以通过几种方法更改 Office 的语言：

选项 1：允许单个用户自定义其 Office 语言设置

个人用户可以调整其 WorkSpaces 上的 Office 语言设置。有关更多信息，请参阅 。在 Office 中添加编辑或创作语言或设置语言首选项在微软文档中。

选项 2：使用 GPO 管理模板 (.admx/.adml) 为您的所有 WorkSpaces 用户强制实施默认 Office 语言设置

您可以使用组策略对象 (GPO) 设置为 WorkSpaces 用户强制实施默认 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 设置 Office 语言的更多信息，请参阅。自定义 Office 的语言设置和设置在微软文档中。办公室 2016 年和办公室 2019 使用相同的 GPO 设置（标有 Office 2016）。

若要使用 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 (p. 63)。

在您可以配置 Office 2016 或 Office 2019 策略设置之前，必须下载管理模板文件 (.admx/.adml)Microsoft 下载中心。下载管理模板文件后，必须添加`office16.admx`和`office16.adml`文件添加到您的 WorkSpaces 目录的域控制器的中央存储区。（`office16.admx`和`office16.adml`文件同时适用于办公室 2016 和办公室 2019。）有关使用`.admx`和`.adml`文件，请参阅如何在 Windows 中创建和管理组策略管理模板的中心存储在微软文档中。

以下过程介绍如何创建 Central Store 以及如何将管理模板文件添加到它中。在目录管理工作区或加入您的 WorkSpaces 目录的 Amazon EC2 实例上执行以下步骤。

为 Office 安装组策略管理模板文件

1. 下载管理模板文件 (.admx/.adml)Microsoft 下载中心。
2. 在目录管理 WorkSpace 或Amazon EC2实例，打开 Windows 文件资源管理器，然后在地址栏中输入组织的完全限定域名 (FQDN)，例如`\\example.com`。
3. 打开 `SYSVOL` 文件夹。
4. 打开文件夹*`FQDN`*名称。
5. 打开 `Policies` 文件夹。您现在应该位于`\\`*`FQDN`*`\SYSVOL\`*`FQDN`*`\Policies`。
6. 如果它尚不存在，请创建一个名为`PolicyDefinitions`。
7. 打开 `PolicyDefinitions` 文件夹。
8. 将复制`office16.admx`将文件放到`\\`*`FQDN`*`\SYSVOL\`*`FQDN`*`\Policies\PolicyDefinitionsfolder`。
9. 创建名为的文件夹`en-US`中的`PolicyDefinitionsfolder`。
10. 打开 `en-US` 文件夹。
11. 将复制`office16.adml`将文件放到`\\`*`FQDN`*`\SYSVOL\`*`FQDN`*`\Policies\PolicyDefinitions\en-USfolder`。

为 Office 配置 GPO 语言设置的步骤

1. 在您的目录管理 WorkSpace 或Amazon EC2实例加入您的 WorkSpaces 目录的组策略管理工具 (gpmc.msc)。

2. 展开林 (林：***FQDN***).
3. 扩展域。
4. 扩展您的 FQDN（例如`example.com`)。
5. 选择 FQDN，打开上下文菜单（右键单击）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 GPO，打开上下文菜单（右键单击），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、从本地计算机检索的管理模板策略定义（ADMX 文件）、Microsoft Office, 和语言首选项。

   Note

   办公室 2016 年和办公室 2019 使用相同的 GPO 设置（标有 Office 2016）。如果您没有看到从本地计算机检索的管理模板策略定义（ADMX 文件）UNTER用户配置、策略，`office16.admx`和`office16.adml`文件未正确安装在您的域控制器上。
9. UNTER语言首选项中，指定所需的语言以用于以下设置的语言。请务必将每个设置设置为启用，然后在选项中，选择所需的语言。选择确定以保存每个设置。

   - 显示语言 >显示的帮助
   - 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 WorkSpace 的下一次组策略更新后和重新启动 WorkSpace 会话后生效。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，然后依次选择 Actions (操作)、Reboot WorkSpaces (重启 WorkSpace)）。
    - 从管理命令提示符下，输入 gpupdate /force。

选项 3：更新工 WorkSpaces 间上的 Office 语言注册表设置

若要通过注册表设置 Office 语言设置，请更新以下注册表设置：

- HKEY_ 当前用户\ 软件\ 微软\ 办公\ 16.0\ 常见\ 语言资源
- HKEY_ 当前 _ 用户\ 软件\ 微软\ 办公\ 16.0\ 常见\ 语言资源\ 帮助计划

对于这些设置，请添加具有相应 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，因此必须将Base选项设置为小数。有关 Office LCID 的列表，请参阅语言标识符和 OptionState ID 值在 Office 2016在微软文档中。

您可以通过 GPO 设置或登录脚本将这些注册表设置应用到您的 WorkSpaces。

有关使用 Office 的语言设置的更多信息，请参阅。自定义 Office 的语言设置和设置在微软文档中。

将办公室添加到现有 BYOL WorkSpaces

您还可以将 Office 订阅添加到您现有的 BYOL WorkSpaces。创建安装 Office 的 BYOL 捆绑包后，您可以使用 WorkSpaces 迁移功能将现有的 BYOL 工作空间迁移到订阅到 Office 的 BYOL 捆绑包。有关更多信息，请参阅 迁移 WorkSpace (p. 118)。

在微软 Office 版本之间迁移

若要从办公室 2016 年迁移到办公室 2019 或从办公室 2019 迁移到办公室 2016，您必须创建一个 BYOL 捆绑包，您要迁移到的 Office 版本。然后，您可以使用 WorkSpaces 迁移功能将订阅到 Office 的现有 BYOL 工作空间迁移到您想要迁移到的 Office 版本的 BYOL 捆绑包。

例如，若要从办公室 2016 迁移到办公室 2019，请创建订阅 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 工作空间迁移到订阅 Office 2019 的 BYOL 捆绑包。

有关迁移过程的更多信息，请参阅。迁移 WorkSpace (p. 118)。

从 Office 取消订阅

若要取消订阅 Office，您必须创建一个未订阅到 Office 的 BYOL 捆绑包。然后使用 WorkSpaces 迁移功能将您现有的 BYOL 工作空间迁移到未订阅到 Office 的 BYOL 捆绑包。有关更多信息，请参阅 迁移 WorkSpace (p. 118)。

Office 更新

如果您已通过 AWS 订阅 Office，Office 更新将作为常规 Windows 更新的一部分包括在内。为了保持所有安全修补程序和更新的最新状态，我们建议您定期更新 BYOL 基础映像。

步骤 1: 使用您的账户启用 BYOLWorkSpaces控制台

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 WorkSpaces 管理网络。它用于将 WorkSpace 桌面以交互方式流式传输到 WorkSpaces 客户端，并允许 WorkSpaces 管理 WorkSpace。

> Note
>
> 此过程中为账户启用 BYOL 的步骤只需在每个区域为每个账户执行一次。

使用 WorkSpaces 控制台为账户启用 BYOL

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Account Settings (账户设置)。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。
3. 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)。

   WorkSpaces 将在您指定的范围内搜索可用的 IP 地址范围并将其显示为 IPv4 无类别域间路由 (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，请在继续操作之前联系您的 AWS 客户经理或销售代表，或联系 AWS Support Center。
4. 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。当 WorkSpaces 为您的账户启用 BYOL 时，请继续执行下一步。

步骤 2: 在 Windows VM 上运行 BYOL 检查程序 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。要执行此操作，请执行以下步骤来下载并运行 WorkSpaces BYOL 检查程序 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 检查程序脚本 .zip 文件下载到您的 `Downloads` 文件夹。
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 Start 按钮，右键单击 Windows PowerShell，然后选择 Run as administrator (以管理员身份运行)。如果用户账户控制提示您选择是否希望 PowerShell 更改您的设备，请选择 Yes (是)。
2. 在 PowerShell 命令提示符处，转至 BYOL 检查程序脚本所在的目录。例如，如果脚本位于`Downloads\BYOL`目录中，输入下面的命令并按Enter：

   ```
   cd C:\Users\username\Downloads\BYOL
   ```
3. 输入以下命令以在计算机上更新 PowerShell 执行策略。这样做将允许 BYOL 检查程序脚本运行：

   ```
   Set-ExecutionPolicy Unrestricted
   ```
4. 当系统提示您确认是否要更改 PowerShell 执行策略时，请输入 A 以便为所有项指定“Yes (是)”。
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 Image Validation (Amazon WorkSpaces 映像验证) 对话框中，选择 Begin Tests (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 (p. 144) 和 Step 8 (p. 144)，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 Run Sysprep (运行 Sysprep)。如果 Sysprep 成功，您在 Step 12 (p. 144) 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 (p. 144) 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 删除 AppX 程序包。

14. 成功创建映像后，您可以删除 WorkSpaces_BYOL 账户。

步骤 3: 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，请参阅您的虚拟化环境的文档和将您的 VM 从其虚拟化环境导出中的VM Import/Export 用户指南。

步骤 4: 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。如果您选择了默认加密Amazon Elastic Block Store(Amazon EBS)卷，则必须先取消选择该选项，然后才能导入虚拟机。

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 。导入映像中的AWS CLI Command Reference。
- 使用 ImportImage API 操作。有关更多信息，请参阅 。ImportImage中的Amazon EC2 API Reference。

有关更多信息，请参阅 。将 VM 作为映像导入中的VM Import/Export 用户指南。

步骤 5：使用创建 BYOL 映像WorkSpaces控制台

执行以下步骤以创建 WorkSpaces BYOL 映像。

> Note
>
> 要执行此过程，请验证您具有 AWS Identity and Access Management (IAM) 权限以：
>
> - CallWorkSpaces **`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`**。确保启动许可Amazon EC2图片不受限制。在整个 BYOL 映像创建过程中，映像必须可以共享。
>
> 例如IAM策略的详细信 WorkSpaces，请参阅适用于 WorkSpaces 的 Identity and Access Management (p. 165)。有关使用IAM权限，请参阅更改的权限IAMUser中的IAM 用户指南。
> 要从映像创建 Graphics 或 GraphicsPro 捆绑包，请联系 AWS Support Center 以将您的账户添加到允许列表。当您的账户位于允许列表之后，就可以使用 AWS CLI import-workspace-image 命令来提取 Graphics 或 GraphicsPro 映像。有关更多信息，请参阅 。导入工作空间映像中的AWS CLI Command Reference。

从 Windows VM 创建映像

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Images。
3. 依次选择 Actions (操作) 和 Create BYOL Image (创建 BYOL 映像)。
4. 在 Create BYOL Image (创建 BYOL 映像) 对话框中，执行以下操作：

- 适用于AMI ID，单击EC2 控制台链接，然后选择Amazon EC2您根据上一节所述导入的映像 (步骤 4: 将 VM 作为映像导入Amazon EC2 (p. 145))。映像名称必须以 `ami-` 开头并后跟 AMI 的标识符（例如，`ami-1234567e`）。
- 对于 BYOL image name (BYOL 映像名称)，请输入映像的唯一名称。
- 对于 Image description (映像描述)，请输入一个描述以帮助您快速识别映像。
- 适用于摄取过程，选择适当的捆绑类型（定期、图形，或者GraphicsPro），具体取决于要为映像使用的协议（PCoIP 或 WorkSpaces 流式处理协议 (WSP)）。对于未启用 GPU 的捆绑包（Graphics 或 GraphicSpro 以外的捆绑包），请选择 Regular (常规)。
- （可选）应用程序中，选择您要订阅的 Microsoft Office 版本。有关更多信息，请参阅 将微软办公室添加到您的 BYOL 映像 (p. 140)。

5. 选择创建。

   创建映像时，控制台的映像注册表中的映像状态将显示为 Pending (待处理)。BYOL 摄入过程至少需要 90 分钟。如果您也订阅了 Office，则预计此过程至少需要 3 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 6：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 WorkSpace 映像和服务包 (p. 123)。

步骤 7：为专用 WorkSpaces 注册目录

要对 WorkSpaces 使用 BYOL 映像，您必须专门注册一个目录。为此，请执行以下步骤。

为专用 WorkSpaces 注册目录

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 Directories。
3. 选择目录，然后依次选择 Actions (操作) 和 Register (注册)。
4. 在 Register directory (注册目录) 对话框中，对于 Enable Dedicated WorkSpaces (启用专用 WorkSpaces)，选择 Yes (是)。
5. 选择 Register。

如果您已注册AWS Managed Microsoft AD目录或AD Connector目录，则可以在专用硬件上运行的 WorkSpaces 目录中设置一个新的AWS Managed Microsoft AD目录或 AD Connector 目录。您也可以取消注册该目录，然后将其注册为专用 WorkSpaces 的目录。为此，请执行以下步骤。

Note

仅当没有该目录关联的 WorkSpaces 时，您才能执行此过程。

为专用 WorkSpaces 取消注册并重新注册目录

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 终止现有 WorkSpaces。
3. 在导航窗格中，选择 Directories。
4. 选择目录，然后选择 Actions、Deregister。
5. 当系统提示您确认时，选择 Deregister。

6. 再次选择目录，然后依次选择 Actions (操作) 和 Register (注册)。
7. 在 Register directory (注册目录) 对话框中，对于 Enable Dedicated WorkSpaces (启用专用 WorkSpaces)，选择 Yes (是)。
8. 选择 Register。

步骤 8：启动 BYOL WorkSpaces

为专用 WorkSpaces 注册目录后，您可以在此目录中启动 BYOL WorkSpaces。有关如何启动 WorkSpaces 的信息，请参阅使用 WorkSpaces 启动虚拟桌面 (p. 66)。

监控您的 WorkSpaces

您可以使用以下功能监控您的 WorkSpaces。

CloudWatch 指标

Amazon WorkSpaces 将数据点发布到有关您的 WorkSpaces 的 Amazon CloudWatch。利用 CloudWatch，您可以按一组有序的时间序列数据（称为指标）来检索关于这些数据点的统计数据。您可使用这些指标来验证您的 WorkSpaces 是否按预期运行。有关更多信息，请参阅 使用 CloudWatch 指标监控您的 WorkSpaces (p. 148)。

CloudWatch Events

Amazon WorkSpaces 可以在用户登录您的 WorkSpace 时将事件提交到 Amazon CloudWatch Events。这使您能够在事件发生时进行响应。有关更多信息，请参阅 使用 CloudWatch Events 监控您的 WorkSpaces (p. 151)。

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。通过使用 CloudTrail 收集的信息，您可以确定向 WorkSpaces 发出了什么请求、发出请求的 IP 地址、何人发出的请求、请求的发出时间以及其他详细信息。有关更多信息，请参阅使用 CloudTrail 记录 WorkSpaces API 调用。

使用 CloudWatch 指标监控您的 WorkSpaces

WorkSpaces 和 Amazon CloudWatch 均为集成式，因此您可收集并分析性能指标。您可以使用 CloudWatch 控制台、CloudWatch 命令行界面或者以编程方式使用 CloudWatch API 来监控这些指标。您还可以使用 CloudWatch 设置警报，让系统在达到某指标的指定阈值时提醒您。

有关更多使用 CloudWatch 和警报的信息，参阅 Amazon CloudWatch 用户指南。

Prerequisites

要获取CloudWatch指标，请在`AMAZON`子集，限定为`us-east-1` 区域。有关更多信息，请参阅 WorkSpaces 的 IP 地址和端口要求 (p. 16)。

目录

WorkSpaces 指标

`AWS/WorkSpaces` 命名空间包括以下指标。

指标	描述	Dimensions	可用统计数据	单位
`Available`[1]	返回正常运行状态的 WorkSpaces 的数量。	`DirectoryId` `WorkspaceId`	Average、Sum、Maximum、Minimum、Data Samples	计数
`Unhealthy`[1]	返回不正常运行状态的 WorkSpaces 的数量。	`DirectoryId` `WorkspaceId`	Average、Sum、Maximum、Minimum、Data Samples	计数

指标	描述	Dimensions	可用统计数据	单位
ConnectionAttempt[2,5]	连接尝试次数。	DirectoryId WorkspaceId	Average、Sum、Maximum、Minimum、Data Samples	计数
ConnectionSuccess[2,5]	成功连接的数量。	DirectoryId WorkspaceId	Average、Sum、Maximum、Minimum、Data Samples	计数
ConnectionFailure[2,5]	失败连接的数量。	DirectoryId WorkspaceId	Average、Sum、Maximum、Minimum、Data Samples	计数
SessionLaunchTime[2]	发起 WorkSpaces 会话所用的时间量。	DirectoryId WorkspaceId	Average、Sum、Maximum、Minimum、Data Samples	秒（时间）
InSessionLatency[2]	WorkSpaces 客户端和 WorkSpace 之间的往返操作时间。	DirectoryId WorkspaceId	Average、Sum、Maximum、Minimum、Data Samples	毫秒（时间）
SessionDisconnect[2]	已关闭的连接数，包括用户启动的和失败的连接。	DirectoryId WorkspaceId	Average、Sum、Maximum、Minimum、Data Samples	计数
UserConnected[3]	用户已连接的 WorkSpaces 数量。	DirectoryId WorkspaceId	Average、Sum、Maximum、Minimum、Data Samples	计数
Stopped	已停止的 WorkSpaces 的数量。	DirectoryId WorkspaceId	Average、Sum、Maximum、Minimum、Data Samples	计数
Maintenance[4]	正在维护的 WorkSpaces 的数量。	DirectoryId WorkspaceId	Average、Sum、Maximum、Minimum、Data Samples	计数
TrustedDeviceValidationAttempt[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[6]	成功的设备身份验证签名验证的数量。	DirectoryId	Average、Sum、Maximum、Minimum、Data Samples	计数
TrustedDeviceValidationFailure[6]	设备身份验证签名验证失败的数量。	DirectoryId	Average、Sum、Maximum、Minimum、Data Samples	计数
TrustedDeviceCertificateDaysToExpiration	与目录关联的根证书过期之前的剩余天数。	CertificateId	Average、Sum、Maximum、Minimum、Data Samples	计数

[1] WorkSpaces 定期向 WorkSpace 发送状态请求。响应这些请求的 WorkSpace 标记为 `Available`，不响应这些请求的 WorkSpace 标记为 `Unhealthy`。这些指标以 WorkSpace 为粒度提供，并且对一个组织内的所有 WorkSpaces 进行汇总。

[2] WorkSpaces 记录针对每个 WorkSpace 进行的连接的指标。在用户成功通过 WorkSpaces 客户端进行身份验证并且客户端启动会话后，会发出这些指标。这些指标以 WorkSpace 为粒度提供，并且对一个目录内的所有 WorkSpaces 进行汇总。

[3] WorkSpaces 定期向 WorkSpace 发送连接状态请求。当用户正在主动使用他们的会话时，他们被报告为已连接。此指标以 WorkSpace 为粒度提供，并且对一个组织内的所有 WorkSpaces 进行汇总。

[4] 此指标适用于以 AutoStop 运行模式配置的 WorkSpaces。如果您已为您的 WorkSpaces 启用了维护，则此指标捕获当前正在维护的 WorkSpaces 数量。此指标以 WorkSpace 为粒度提供，描述 WorkSpace 何时进入维护，以及何时删除。

[5]此度量目前仅针对 PCoIP WorkSpaces 发出。

[6]如果为目录启用了受信任设备功能，则Amazon 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 WorkSpaces 时，会发出这些指标，以指示成功或失败的受信任设备身份验证。这些指标以粒度为级别提供，并且仅适用于Amazon WorkSpacesWindows 和 macOS 客户端应用。

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`	筛选指标数据，限定为指定目录中的 WorkSpaces。目录 ID 的形式为 `d-xxxxxxxxxx`。
`WorkspaceId`	筛选指标数据，限定为指定的 WorkSpace。WorkSpace ID 的形式为`ws-xxxxxxxxxx`。
`CertificateId`	筛选指标数据，限定为与目录关联的指定根证书。证书 ID 的形式为`wsc-xxxxxxxxx`。

监控示例

以下示例展示了如何使用 AWS CLI 响应 CloudWatch 警报，以及如何确定目录中的哪些 WorkSpace 遇到了连接故障。

响应 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 describe-workspaces 命令获取指定目录中的 WorkSpace 列表。

```
aws workspaces describe-workspaces --directory-id directory_id

{
  "Workspaces": [
    {
      ...
      "WorkspaceId": "workspace1_id",
      ...
    },
    {
      ...
      "WorkspaceId": "workspace2_id",
      ...
    },
    {
      ...
      "WorkspaceId": "workspace3_id",
      ...
    }
  ]
}
```

3. 使用 CloudWatchget-metric-statistics 命令获取目录中每个 WorkSpace 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"
}
```

使用 CloudWatch Events 监控您的 WorkSpaces

您可以使用 Amazon CloudWatch Events 中的事件查看、搜索、下载、存档、分析和响应对您的 WorkSpace 的成功登录。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供日后参考，分析日志以查找模式，并根据这些模式采取措施。

- 使用 WAN IP 地址确定用户登录的位置，然后使用策略允许用户仅访问 WorkSpace 中符合在 CloudWatch 事件类型 `WorkSpaces Access` 中找到的访问条件的文件或数据。
- 分析几乎实时提供的登录数据，并使用 AWS Lambda 执行自动化操作。
- 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。

有关事件的更多信息，请参阅 Amazon CloudWatch Events 用户指南。

WorkSpaces 事件

WorkSpaces 客户端应用程序在用户成功登录 WorkSpace 时将 WorkSpaces Access 事件发送到 CloudWatch Events。所有 WorkSpaces 客户端都发送这些事件。

Note

- 尽最大努力发出事件。
- 当前不会为 WorkSpaces 发出事件，使用WorkSpaces Streaming Protocol (WSP)。

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": "2018-07-01T17:53:06Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "clientIpAddress": "192.0.2.3",
        "actionType": "successfulLogin",
        "workspacesClientProductName": "WorkSpaces Desktop client",
        "loginTime": "2018-07-01T17:52:51.595Z",
        "clientPlatform": "Windows",
        "directoryId": "domain/d-123456789",
        "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
- `WorkSpaces Web Client` — Web Access 客户端

- Teradici PCoIP Zero Client, Teradici PCoIP Desktop Client, or Dell Wyse PCoIP Client — 零客户端

loginTime

登录 WorkSpace 的时间。

clientPlatform

- Android
- Chrome
- iOS
- Linux
- OSX
- Windows
- Teradici PCoIP Zero Client and Tera2
- Web

directoryId

WorkSpace 的目录的标识符。您必须在目录标识符前加上domain/。例如，"domain/d-123456789"。

workspaceId

WorkSpace 的标识符。

创建一个规则来处理 WorkSpaces 事件

使用以下过程创建一个 CloudWatch Events 规则来处理 WorkSpaces 事件。

创建一个规则来处理 WorkSpaces 事件

1. 通过以下网址打开 CloudWatch 控制台：https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，选择 Events。
3. 选择 Create rule (创建规则)。
4. 对于 Event Source，执行以下操作：
   a. 选择 Event Pattern (事件模式) 和 Build event pattern to match events by service (生成事件模式以按服务匹配事件) (默认值) 。
   b. 对于 Service Name (服务名称)，选择 WorkSpaces。
   c. 对于 Event Type (事件类型)，选择 WorkSpaces Access (WorkSpaces 访问)。
5. 对于 Targets (目标)，选择 Add target (添加目标)，然后选择当检测到 WorkSpaces 事件时要执行的服务。提供此服务所需的任何信息。
6. 选择 Configure details。对于 Rule definition (规则定义)，输入名称和描述。
7. 选择 Create rule (创建规则)。

业务持续性 Amazon WorkSpaces

Amazon WorkSpaces 构建于 AWS 全球基础设施,其组织成 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弹性。有关更多信息，请参阅 中的弹性Amazon WorkSpaces (p. 173)。

Amazon WorkSpaces 还提供跨区域重定向功能,该功能可与您的域名系统(DNS)路由策略一起使用,以便在主要工作区不可用时将您的工作区用户重定向到其他工作区。例如,通过使用DNS故障转移路由策略,您可以将用户连接到指定故障转移区域中的WorkSpaces,因为他们无法访问主区域中的WorkSpaces。

您可以使用跨区域重定向来实现区域弹性和高可用性。您还可以将其用于其他目的,如流量分布或在维护期间提供备用工作空间。如果您使用 Amazon Route 53 对于DNS配置,您可以利用监控的运行状况检查 Amazon CloudWatch 警报。

内容

的跨区域重定向 Amazon WorkSpaces

利用 中的跨区域重定向功能Amazon WorkSpaces，您可以使用完全限定域名 （FQDN） 作为 的注册代码WorkSpaces。 跨区域重定向将与您的域名系统 （DNS） 路由策略一起使用，以在用户的主节点WorkSpaces不可用WorkSpaces时将WorkSpaces用户重定向到备用节点。例如，通过使用 DNS 故障转移路由策略，您可以在用户无法访问WorkSpaces您指定的故障转移AWS区域中的用户时将其连接到WorkSpaces主区域中的这些用户。

您可以使用跨区域重定向以及 DNS 故障转移路由策略来实现区域弹性和高可用性。您还可以将此功能用于其他目的，例如流量分配或在WorkSpaces维护期间提供备用功能。如果您使用 Amazon Route 53 Route 53 进行 DNS 配置，则可以利用监控 Amazon 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 区域中的用户设置 。您还必须创建称为连接别名的基于 FQDN 的特殊注册代码。这些连接别名替换您的WorkSpaces用户的特定于区域的注册代码。（特定于区域的注册代码保持有效；但是，要使跨区域重定向正常工作，您的用户必须改用 FQDN 作为其注册代码。）

要创建连接别名，请指定一个连接字符串，即 FQDN，例如 `www.example.com` 或 `desktop.example.com`。 要将此域用于跨区域重定向，您必须向域注册商注册此域并为域配置 DNS 服务。

创建连接别名后，您可以将它们与不同区域中的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。如果主区域中发生中断，您的 DNS 故障转移路由策略会将WorkSpaces用户重定向到WorkSpaces您在故障转移区域中为他们设置的 。

要指定您的主区域和故障转移区域，您可以在配置 DNS 故障转移路由策略时定义区域优先级（主要或辅助）。

目录

Prerequisites

- 您必须拥有并注册要用作连接别名中的 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 中的使用 注册域名Amazon Route 53 开发人员指南。

  Important

  您必须拥有所有必要的权限才能使用与 结合使用的任何域名Amazon WorkSpaces。您同意域名不会违反或侵犯任何第三方的合法权利，也不会违反适用的法律。

  域名的总长度不能超过 255 个字符。有关域名的更多信息，请参阅 中的 DNS Amazon Route 53 开发人员指南域名格式。

  跨区域重定向适用于私有 DNS 区域中的公有域名和域名。如果您使用的是私有 DNS 区域，则必须提供到包含 的 Virtual Private Cloud （ VPC ） 的虚拟专用网络 （ VPN ） 连接WorkSpaces。 如果您的WorkSpaces用户尝试从公共 Internet 使用私有 WorkSpaces FQDN，则客户端应用程序将返回以下错误消息：

  ```
  "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。跨区域重定向将与您的 DNS 路由策略结合使用，以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，为您的用户创建 。确保在每个WorkSpaces区域的每个目录中使用相同的用户名。为了保持 Active Directory 用户数据的同步，我们建议使用 AD Connector 指向您已WorkSpaces为用户设置的每个区域中的同一 Active Directory。有关创建 的更多信息WorkSpaces，请参阅启动 WorkSpaces (p. 66)。

  Important

  如果您为多区域复制配置AWS了 托管的 Microsoft AD 目录，则只能注册主区域中的 目录以用于 Amazon WorkSpaces。尝试在复制的区域中注册目录以便与 结合使用Amazon WorkSpaces将失败。不支持使用 AWS 托管 Microsoft AD 的多区域复制在复制Amazon WorkSpaces的区域内用于 。

  完成设置跨区域重定向后，您必须确保您的WorkSpaces用户对其`WSpdx+ABC12D`主要区域使用基于 FQDN 的注册代码，而不是基于区域的注册代码（例如 ）。为此，您必须使用中的过程向他们发送包含 FQDN 连接字符串的电子邮件步骤 5：将连接字符串发送给WorkSpaces您的用户 (p. 160)。

  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，则每当您启动新的 时， 都会使用基于区域的注册代码WorkSpaces自动向用户发送邀请电子邮件 WorkSpace。 这意味着，当您WorkSpaces为故障转移区域中的用户设置 时，您的用户还会自动收到这些故障转移 的电子邮件WorkSpaces。 您需要指示用户使用基于区域的注册代码忽略电子邮件。

Limitations

- 跨区域重定向不会自动检查与主区域的连接是否失败，然后将您的 WorkSpaces 故障转移到另一个区域。换句话说，不会进行自动故障转移。

  要实施自动故障转移方案，您必须将其他机制与跨区域重定向结合使用。例如，您可以使用故障Amazon Route 53转移 DNS 路由策略，该策略与监控主区域中Route 53的 警报的CloudWatch运行状况检查配对。如果触发主区域中的 CloudWatch 警报，则 DNS 故障转移路由策略会将WorkSpaces您的用户重定向到WorkSpaces您在故障转移区域中为他们设置的 。
- 当您使用跨区域重定向时，不同WorkSpaces区域中的 之间不会保留用户数据。要确保用户可以从不同区域访问其文件，我们建议您Amazon WorkDocs为WorkSpaces用户设置 （ 如果您的主区域和故障转移区域中支持 Amazon WorkDocs ）。有关 的更多信息Amazon WorkDocs，请参阅 中的 Amazon WorkDocs Amazon WorkDocs 管理指南Drive。有关Amazon WorkDocs为您的WorkSpace用户启用 的更多信息，请参阅向 WorkSpaces 注册目录 (p. 53)和启用Amazon WorkDocsAWS Managed Microsoft AD (p. 63)。有关WorkSpaces用户如何在其 Amazon WorkDocs 上设置 的信息WorkSpaces，请参阅 WorkDocs 中的将 Amazon WorkSpaces 用户指南与 集成。
- 仅 Linux、 macOS和 Windows WorkSpaces 客户端应用程序的版本 3.0.9 或更高版本支持跨区域重定向。
- 跨区域重定向适用于所有提供 Amazon WorkSpaces的 AWS 区域，但AWS GovCloud （ 美国西部 ） 区域和除外中国 (宁夏) 区域。

步骤 1：创建连接别名

使用相同的AWS账户，在要设置跨区域重定向的每个主区域和故障转移区域中创建连接别名。

创建连接别名

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在 控制台的右上角，选择 的主要AWS区域WorkSpaces。
3. 在导航窗格中，选择 Account Settings (账户设置).
4. 在 Cross-Region redirection （ 跨区域重定向 ） 下，选择 Create connection alias （ 创建连接别名 ）。
5. 对于 Connection string （ 连接字符串 ），输入 FQDN，例如 `www.example.com` 或 `desktop.example.com`。 连接字符串最多可包含 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AWS您的账户关联。您不能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该账户的所有实例。连接字符串全局为您的账户预留。
6. （ 可选 ）在 Tags （ 标签 ） 下，指定要与连接别名关联的任何标签。
7. 选择 Create connection alias （ 创建连接别名 ）。
8. 重复这些步骤，但在 中Step 2 (p. 156)，请务必为 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. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在 控制台的右上角，选择要与另一个AWS账户共享连接别名AWS的区域。
3. 在导航窗格中，选择 Account Settings (账户设置).
4. 在 Cross-Region redirection associations （跨区域重定向关联） 下，选择连接字符串，然后选择 Actions （操作）、Share/unshare connection alias （共享/取消共享连接别名）。

   您还可以从连接别名的详细信息页面共享别名。为此，请在 Shared account （共享账户） 下，选择 Share connection alias （共享连接别名）。
5. 在 Share/unshare connection alias （共享/取消共享连接别名） 页面上的 Share with an account （与某个账户共享） 下，输入您要与此AWS区域中的共享连接别名AWS的账户 ID。
6. 选择 Share.

步骤 3：将连接别名与每个区域中的目录关联

将同一连接别名与两个或更多区域中的WorkSpaces目录关联将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，如果您的主区域是 美国西部（俄勒冈）区域，则可以将 中的 WorkSpaces 目录美国西部（俄勒冈）区域与 中的 WorkSpaces 目录配对美国东部（弗吉尼亚北部）地区。如果主区域中发生中断，则跨区域重定向将与您在 上部署的 DNS 故障转移路由策略和任何运行状况检查结合使用美国西部（俄勒冈）区域，以将用户重定向到WorkSpaces您在 中为他们设置的 美国东部（弗吉尼亚北部）地区。有关跨区域重定向体验的更多信息，请参阅跨区域重定向过程中会发生什么 (p. 161)。

Note

如果您的WorkSpaces用户与故障转移区域相距较远（例如，几千英里远），则他们的WorkSpaces体验可能比平常不太响应。要检查从您的位置到各个 AWS 区域的往返时间（RTT），请使用 Amazon WorkSpaces 连接运行状况检查。

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. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在 控制台的右上角，选择 的主要AWS区域WorkSpaces。
3. 在导航窗格中，选择 Account Settings (账户设置).
4. 在 Cross-Region redirection associations （跨区域重定向关联） 下，选择连接字符串，然后选择 Actions （操作）、Associate/disassociate （关联/取消关联）。

   您还可以从连接别名的详细信息页面将连接别名与目录关联。为此，请在 Associated directory 下，选择 Associate directory。
5. 在 Associate/disassociate 页面上的 Associate to a directory 下，选择要在此AWS区域中将连接别名与关联的目录。

   Note

   如果您为多区域复制配置AWS了 托管的 Microsoft AD 目录，则只有主区域中的 目录可与 一起使用Amazon WorkSpaces。尝试在复制的区域中使用 目录Amazon WorkSpaces将失败。不支持使用 AWS 托管 Microsoft AD 的多区域复制在复制Amazon WorkSpaces的区域内用于 。

6. 选择 Associate.
7. 重复这些步骤，但在 中Step 2 (p. 157)，请务必为 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。请确保将相同的连接别名与每个故障转移区域中的目录关联。

步骤 4：配置 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。如果您还没有首选的 DNS 服务提供商，则可以使用 Amazon Route 53。有关更多信息，请参阅 中的将 Amazon Route 53 Route 53 配置为您的 DNS Amazon Route 53 开发人员指南服务。

为您的域配置 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 运行状况检查确定您的用户是否可以连接到特定WorkSpaces区域中的 。如果您的用户无法连接，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 中的https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html选择路由策略Amazon Route 53 开发人员指南。有关 Amazon Route 53 运行状况检查的更多信息，请参阅 中的 Amazon Route 53如何检查资源的运行状况Amazon Route 53 开发人员指南。

在设置 DNS 路由策略时，您需要连接别名与主区域中的 目录之间的关联的连接标识符WorkSpaces。您还需要连接别名与故障转移区域中的 WorkSpaces 目录之间的关联的连接标识符。

> Note
>
> 连接标识符与连接别名 ID 不同。连接别名 ID 以 开头`wsca-`。

查找连接别名关联的连接标识符

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在 控制台的右上角，选择 的主要 AWS 区域WorkSpaces。
3. 在导航窗格中，选择 Account Settings (账户设置).
4. 在 Cross-Region redirection associations （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. 在连接别名的详细信息页面上的 Associated directory （关联目录） 下，记下为 Connection identifier （连接标识符） 显示的值。
6. 重复这些步骤，但在 中Step 2 (p. 158)，请务必为 选择故障转移区域WorkSpaces。 如果您有多个故障转移区域，请重复这些步骤以查找每个故障转移区域的连接标识符。

示例：使用 Route 53 53 设置 DNS 故障转移路由策略

以下示例为您的域设置公有托管区域。但是，您可以设置公有或私有托管区域。有关设置托管区域的更多信息，请参阅 中的https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zones-working-with.html使用托管区域Amazon Route 53 开发人员指南。

此示例还使用故障转移路由策略。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 中的https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html选择路由策略Amazon Route 53 开发人员指南。

在 Route Route 53 中设置故障转移路由策略时，需要对主区域进行运行状况检查。有关在 Route 53 53 中创建运行状况检查的更多信息，请参阅 中的创建 Amazon Amazon Route 53 53 运行状况检查以及配置 DNS 故障转移和Amazon Route 53 开发人员指南创建、更新和删除运行状况检查。

如果要将 Amazon CloudWatch 警报与 Route Route 53 运行状况检查结合使用，您还需要设置 CloudWatch 警报来监控主区域中的资源。有关 的更多信息CloudWatch，请参阅 中的什么是 Amazon CloudWatch Amazon CloudWatch 用户指南?。有关 Route 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 中的 Route 53 53 如何确定监控 CloudWatch 警报的运行状况检查的状态和监控 CloudWatch Amazon Route 53 开发人员指南警报。

要在 Route 53 53 中设置 DNS 故障转移路由策略，您首先需要为域创建一个托管区域。

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，选择托管区域，然后选择创建托管区域。
3. 在 Created hosted zone （已创建托管区域）页面上，在 `example.com`Domain name （域名）下输入您的域名（例如 ）。
4. 在 Type （类型）下，选择 Public hosted zone （公有托管区域）。
5. 选择 Create hosted zone （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 Health checks （运行状况检查），然后选择 Create health check （创建运行状况检查）。
3. 在 Configure health check （配置运行状况检查）页面上，输入运行状况检查的名称。
4. 对于 What to monitor （要监控的内容），选择 Endpoint （终端节点）、Status of other health checks （已计算的运行状况检查）或 State of alarm 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 Next （下一步）。
6. 在 Get notification when health check fails （在运行状况检查失败时收到通知）页面上，对于 Create alarm （创建警报），选择 Yes （是）或 No （否）。
7. 选择 Create health check （创建运行状况检查）。

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.
3. 在 Hosted zones （托管区域）页面上，选择您的域名。
4. 在域名的详细信息页面上，选择 Create record （创建记录）。
5. 在 Choose routing policy （选择路由策略）页面上，选择 Failover （故障转移），然后选择 Next （下一步）。
6. 在 Configure records （配置记录）页面上的 Basic configuration （基本配置）下，对于 Record name （记录名称），输入您的子域名。例如，如果您的 FQDN 为 `desktop.example.com`，请输入 **`desktop`**。

   Note

   如果要使用根域，请将 Record name （记录名称）留空。但是，我们建议使用子域，例如 `desktop` 或 `workspaces`，除非您已专门设置该域以用于 WorkSpaces。
7. 对于 Record type （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 Failover records to add to （要添加到的故障转移记录）下 ***`your_domain_name`***，选择 Define failover record （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：为主要区域设置故障转移记录

1. 在 Define failover record （定义故障转移记录）对话框中，对于 Value/route traffic to （值/路由流量），根据记录类型选择 IP 地址或其他值。

2. 此时会打开一个框，以便您输入示例文本条目。输入主区域的连接别名关联的连接标识符。
3. 对于 Failover record type （故障转移记录类型），选择 Primary （主节点）。
4. 对于 Health check （运行状况检查），选择您为主区域创建的运行状况检查。
5. 对于 Record ID （记录 ID），输入描述以标识此记录。
6. 选择 Define failover record （定义故障转移记录）。您的新故障转移记录将显示在要添加到 的故障转移记录下 ***your_domain_name***.

示例：为故障转移区域设置故障转移记录

1. 在 Failover records to add to （要添加到的故障转移记录） 下 ***your_domain_name***，选择 Define failover record （定义故障转移记录）。
2. 在 Define failover record （定义故障转移记录） 对话框中，对于 Value/route traffic to （值/路由流量），根据记录类型选择 IP 地址或其他值。
3. 此时会打开一个框，以便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 Failover record type （故障转移记录类型），选择 Secondary （辅助）。
5. （可选）对于 Health check （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 Record ID （记录 ID），输入描述以标识此记录。
7. 选择 Define failover record （定义故障转移记录）。您的新故障转移记录将显示在要添加到 的故障转移记录下 ***your_domain_name***.

如果您为主区域设置的运行状况检查失败，则 DNS 故障转移路由策略会将WorkSpaces您的用户重定向到故障转移区域。Route 53 53 继续监控主区域的运行状况检查，当主区域的运行状况检查不再失败时 Route 53 53 会自动将WorkSpaces用户重定向回主区域中WorkSpaces的 。

有关创建 DNS 记录的更多信息，请参阅 中的使用 Amazon Route 53 Route 53 https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-creating.html 控制台Amazon Route 53 开发人员指南创建记录。有关配置 DNS TXT 记录的更多信息，请参阅 中的 TXT Amazon Route 53 开发人员指南记录类型。

步骤 5：将连接字符串发送给WorkSpaces您的用户

要确保在中断期间根据需要WorkSpaces重定向您的用户，您必须将连接字符串 （FQDN） 发送给用户。如果您已`WSpdx+ABC12D`向用户发布基于区域的注册代码（例如，WorkSpaces），这些代码将保持有效。但是，要使跨区域重定向正常工作，您的WorkSpaces用户在WorkSpacesWorkSpaces客户端应用程序中注册时必须使用连接字符串作为注册代码。

> **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，则每当您启动新的 时， 都会使用基于区域的注册代码（例如WorkSpaces， ）`WSpdx+ABC12D`自动向用户发送邀请电子邮件WorkSpace。 即使您已设置跨区域重定向，自动为 发送的邀请电子邮件WorkSpaces也会包含此基于区域的注册代码，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代码，您必须使用以下过程向这些用户发送另一封连接字符串电子邮件。

将连接字符串发送给WorkSpaces用户

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在 控制台的右上角，选择 的主要AWS区域WorkSpaces。
3. 在导航窗格中，选择 WorkSpaces 。
4. 在 WorkSpaces 页面上，使用搜索框搜索要向其发送邀请的用户，然后从WorkSpace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 Invite Users to their （邀请用户加入其 ） WorkSpaces 页面上，您将看到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目录关联，请从 Connection alias string （连接别名字符串 ） 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发送给用户的电子邮件中。在您的电子邮件应用程序中，您可以根据需要修改文本。准备好邀请电子邮件后，将其发送给您的用户。

跨区域重定向过程中会发生什么

如果出现中断，您的WorkSpaces用户将与主区域中WorkSpaces的断开。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，系统会提示用户再次登录。如果用户使用 FQDN 作为其注册代码，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WorkSpaces您在故障转移区域中为他们设置的 。

> Note
>
> 在某些情况下，用户可能无法在再次登录时重新连接。如果发生此行为，则它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目录的关联。

如果您已与其他账户共享连接别名，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目录的关联。

取消连接别名与目录的关联

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在控制台的右上角，选择要取消关联的连接别名所在的AWS区域。
3. 在导航窗格中，选择 Account Settings (账户设置).
4. 在 Cross-Region redirection associations （跨区域重定向关联 ） 下，选择连接字符串，然后选择 Actions （操作 ）、Associate/disassociate （关联/取消关联 ）。

   您还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 Associated directory 下，选择 Disassociate。
5. 在 Associate/disassociate 页面上，选择 Disassociate。
6. 在要求您确认取消关联的对话框中，选择 Disassociate （ 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别名。如果您取消与某个账户的连接别名共享，则该账户将无法再将该连接别名与目录关联。

取消共享连接别名

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在 控制台的右上角，选择要取消共享的连接别名所在的AWS区域。
3. 在导航窗格中，选择 Account Settings (账户设置).

4. 在 Cross-Region redirection associations （跨区域重定向关联） 下，选择连接字符串，然后选择 Actions （操作）、Share/unshare connection alias （共享/取消共享连接别名）。

   您还可以从连接别名详细信息页面取消共享连接别名。为此，请在 Shared account （共享账户） 下，选择 Unshare （取消共享）。
5. 在 Share/unshare connection alias （共享/取消共享连接别名） 页面上，选择 Unshare （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 Unshare （取消共享）。

删除连接别名

只有在连接别名归您的账户所有并且未与目录关联时，您才能删除连接别名。

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该目录的关联，然后才能删除连接别名。

> Important
>
> 创建连接字符串后，它始终与您的 AWS 账户关联。您不能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该账户的所有实例。连接字符串全局为您的账户预留。
>
> Warning
>
> 如果您不再使用 FQDN 作为WorkSpaces用户的注册代码，则必须采取某些预防措施来防止潜在的安全问题。 有关更多信息，请参阅停止使用跨区域重定向时的安全注意事项 (p. 163).

删除连接别名

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在 控制台的右上角，选择包含要删除的连接别名AWS的区域。
3. 在导航窗格中，选择 Account Settings (账户设置).
4. 在 Cross-Region redirection associations （跨区域重定向关联） 下，选择连接字符串，然后选择 Delete （删除）。

   您还可以从连接别名详细信息页面删除连接别名。为此，请选择页面右上角的 Delete （删除）。

   > Note
   >
   > 如果 Delete （删除） 按钮处于禁用状态，请确保您是别名的所有者，并确保别名未与目录关联。
5. 在要求您确认删除的对话框中，选择 Delete （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，则该用户必须具有 `workspaces:AssociateConnectionAlias` 和 的权限`workspaces:DisassociateConnectionAlias`。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:AssociateConnectionAlias",
        "workspaces:DisassociateConnectionAlias"
      ],
```

```
      "Resource": [
          "arn:aws:workspaces:us-east-1:123456789012:connectionalias/wsca-a1bcd2efg"
      ]
    }
  ]
}
```

Important

如果要创建 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。相反，您必须使用 * 作为账户 ID，如以下示例策略中所示。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:AssociateConnectionAlias",
        "workspaces:DisassociateConnectionAlias"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:*:connectionalias/wsca-a1bcd2efg"
      ]
    }
  ]
}
```

仅当 ARN 中的账户拥有要关联或取消关联的连接别名时，才能在该 ARN 中指定账户 ID。

有关使用 IAM 的更多信息，请参阅适用于 WorkSpaces 的 Identity and Access Management (p. 165)。

停止使用跨区域重定向时的安全注意事项

如果您不再使用 FQDN 作为WorkSpaces用户的注册代码，则必须采取以下预防措施来防止潜在的安全问题：

- 请确保为您的WorkSpaces用户发布其`WSpdx+ABC12D`目录的特定于区域的注册代码（例如 WorkSpaces，），并指示他们停止使用 FQDN 作为注册代码。
- 如果您仍拥有此域，请务必更新您的 DNS TXT 记录以删除此域，使其不会在网络钓鱼攻击中被利用。如果您从 DNS TXT 记录中删除此域，并且您的WorkSpaces用户尝试使用 FQDN 作为其注册代码，则其连接尝试将无害地失败。
- 如果您不再拥有此域，您的WorkSpaces用户必须使用其特定于区域的注册代码。如果它们继续尝试使用 FQDN 作为注册代码，则其连接尝试可能会重定向到恶意站点。

中的安全性Amazon WorkSpaces

AWS 的云安全性的优先级最高。作为 AWS 客户，您将从专为满足大多数安全敏感型组织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。责任共担模型责任共担模型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。

该文档帮助您了解如何在使用 时应用责任共担模型。WorkSpaces. 其中说明如何配置 WorkSpaces 以实现您的安全性和合规性目标。您还将了解如何使用其他 AWS 服务来帮助您监控和保护 WorkSpaces 资源。

目录

中的数据保护Amazon WorkSpaces

AWS 责任共担模式适用于 Amazon WorkSpaces 中的数据保护。如该模式中所述，AWS 负责保护运行所有 AWS 云的全球基础设施。您负责维护对托管在此基础设施上的内容的控制。此内容包括您所使用的 AWS 服务的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。 有关欧洲数据保护的信息，请参阅 AWS 安全性博客 上的 AWS 责任共担模式和 GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户凭证并使用 AWS Identity and Access Management (IAM) 设置单独的用户账户。这仅向每个用户授予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您的数据：

- 对每个账户使用 Multi-Factor Authentication (MFA)。
- 使用 SSL/TLS 与 AWS 资源进行通信。建议使用 TLS 1.2 或更高版本。
- 使用 AWS CloudTrail 设置 API 和用户活动日志记录。
- 使用 AWS 加密解决方案以及 AWS 服务中的所有默认安全控制。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的个人数据。
- 如果在通过命令行界面或 API 访问 AWS 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 终端节点。有关可用的 FIPS 终端节点的更多信息，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敏感的可识别信息（例如您客户的账号）放入自由格式字段（例如 Name (名称) 字段）。这包括使用控制台、API、AWS CLI 或 AWS 开发工具包处理 WorkSpaces 或其他 AWS 服务时。您输入到 WorkSpaces 或其他服务中的任何数据都可能被选取以包含在诊断日志中。当您向外部服务器提供 URL 时，请勿在 URL 中包含凭证信息来验证您对该服务器的请求。

有关 WorkSpaces 和 FIPS 终端节点加密的更多信息，请参阅为 FedRAMP 授权或 DoD SRG 合规性设置 Amazon WorkSpaces (p. 47)。

静态加密

您可以使用 WorkSpaces 中的客户主密钥（CMK）加密 AWS Key Management Service 的存储卷。有关更多信息，请参阅 加密的 WorkSpace (p. 105).

当您创建使用加密卷的 WorkSpaces 时，WorkSpaces 将使用 Amazon Elastic Block Store（Amazon EBS）创建和管理这些卷。EBS 使用行业标准的 AES-256 算法通过数据密钥加密您的卷。有关更多信息，请参阅 https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html 中的 Amazon EBS 加密Amazon EC2 用户指南（适用于 Windows 实例）。

传输中加密

对于 PCoIP，传输中的数据使用 TLS 1.2 加密和 SigV4 请求签名进行加密。协议使用加密 UDP 流量和 AES 加密来传输像素。PCoIP

对于 WorkSpaces Streaming Protocol (WSP)，传输中的数据的流式处理和控制是使用 DTLS 1.2 加密（针对 UDP 流量）和 TLS 1.2 加密（针对 TCP 流量）通过 AES-256 密码加密的。

适用于 WorkSpaces 的 Identity and Access Management

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 策略以明确向他们授予权限，并将该策略附加到需要这些权限的 IAM 用户或组。有关 的更多信息IAM策略，请参阅策略和权限中的IAM 用户指南指南。

WorkSpaces 还创建了一个 IAM 角色来允许 WorkSpaces 服务访问所需资源。

> Note
>
> Amazon WorkSpaces 不支持将 IAM 凭证预置到工作区中（例如使用实例配置文件）。

有关 IAM 的更多信息，请参阅 Identity and Access Management (IAM) 和 IAM 用户指南。您可以在 IAM 权限策略中使用的 WorkSpace 特定资源、操作和条件上下文键Amazon WorkSpaces 的操作、资源和条件键中的IAM 用户指南。

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 测试策略是允许还是拒绝对 AWS 的特定请求。

Example ：1 全部执行WorkSpacestasks

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。

注意，尽管在使用 API 和命令行工具时 WorkSpaces 完全支持 `Action` 和 `Resource` 元素，但您必须将它们都设置为“*”才能成功使用 WorkSpaces 控制台。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
```

```
        "ds:*",
        "iam:PassRole",
        "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: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": "*"
    }
  ]
}
```

Example 2: 执行 WorkSpace 特定任务

以下策略语句将为 IAM 用户授予执行 WorkSpace 特定任务的权限，比如启动和删除 WorkSpace。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: 全部执行WorkSpacesBYOL WorkSpaces 的任务

以下策略语句向IAM用户执行所有WorkSpaces任务，包括Amazon EC2创建自带许可 (BYOL) WorkSpace 所需的任务。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:PassRole",
        "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": "*"
    }
  ]
}
```

创建 workspaces_DefaultRole 角色

您必须先创建 WorkSpaces_Defaultrole 角色（如果此角色不存在），然后才能使用 API 注册目录。

创建 workspaces_DefaultRole 角色

1. 登录 AWS 管理控制台 并通过以下网址打开 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. 选择创建角色。
4. 在 Select type of trusted entity (选择受信任实体的类型) 下，选择其他 AWS 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. 选择后续：权限。
8. 在 Attach permissions policies (附加权限策略) 页面上，选择 AWS 托管策略 AmazonWorkSpacesServiceAccess 和 AmazonWorkSpacesSelfServiceAccess。
9. UNDER设置权限边界，我们建议您不要使用权限边界，因为可能会与附加到 WorkSpace _DefaultRole 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. 选择后续：Tags。
11. 在 Add tags (optional) (添加标签(可选)) 页面上，根据需要添加标签。
12. 选择后续：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. 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。

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)。控制对的访问WorkSpaces资源，通过允许或拒绝使用 API 操作的权限，可以使用`Action`元素IAM策略声明。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 图像所在的区域（例如，`us-east-1`)。

account_id

的 IDAWS帐户，不包含连字符（例如，`123456789012`)。

bundle_identifier

WorkSpace 图像的 ID (例如，`wsi-a1bcd2efg`)。

以下是`Resource`元素，用于标识某个特定的图像。

```
"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服务包。

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）。

连接别名 _ 标识符

连接别名的 ID (例如，wsca-12345a67b8)。

以下是Resource元素，用于标识某个特定连接别名。

```
"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
- 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 Support 对共享资源的账户级限制的 API 操作

对于以下 API 操作，当资源不属于账户所有时，您无法在资源 ARN 中指定账户 ID：

- AssociateConnectionAlias
- CopyWorkspaceImage
- DisassociateConnectionAlias

对于这些 API 操作，只有当资源 ARN 拥有要执行操作的资源时，您才能在该资源 ARN 中指定账户 ID。如果帐户不拥有资源，则必须指定*作为账户 ID，如以下示例中所示。

```
"arn:aws:workspaces:region:*:resource_type/resource_identifier"
```

的合规性验证Amazon WorkSpaces

作为多个 Amazon WorkSpaces 合规性计划的一部分，第三方审计员将评估 AWS 的安全性和合规性。其中包括 SOC、PCI、FedRAMP、HIPAA 等。

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 下载第三方审计报告。AWS Artifact. 有关更多信息，请参阅在 AWS Artifact 中下载报告.

有关 WorkSpaces 和 FedRAMP 的更多信息，请参阅为 FedRAMP 授权或 DoD SRG 合规性设置 Amazon WorkSpaces (p. 47)。

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

- 安全性与合规性快速入门指南 – 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。
- 《设计符合 HIPAA 安全性和合规性要求的架构》白皮书 – 此白皮书介绍公司如何使用 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。

- 中的AWS Config Developer Guide使用规则评估资源；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 Config
- 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。

中的弹性Amazon WorkSpaces

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，这是一项功能，可用于您的域名系统（DNS）故障转移路由策略，以便在您的 WorkSpaces 用户主 WorkSpaces 不可用时将其重定向到其他 AWS 区域中的替代 WorkSpaces。有关更多信息，请参阅 的跨区域重定向 Amazon WorkSpaces (p. 154).

中的基础设施安全性Amazon WorkSpaces

作为一项托管服务，Amazon WorkSpaces 由 AWS：安全流程概述Amazon Web Services白皮书中所述的全球网络安全程序提供保护。

您可以使用 AWS 发布的 API 调用通过网络访问 WorkSpaces 客户端必须支持传输层安全性 (TLS) 1.0 或更高版本。建议使用 TLS 1.2 或更高版本。客户端还必须支持具有完全向前保密 (PFS) 的密码套件，例如 Ephemeral Diffie-Hellman (DHE) 或 Elliptic Curve Ephemeral Diffie-Hellman (ECDHE)。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 WorkSpaces。有关更多信息，请参阅 为 配置 VPCWorkSpaces (p. 9).

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 (p. 42).

您可以使用有效的证书将 WorkSpace 访问限制为受信任的设备。有关更多信息，请参阅 限制对受信任设备的 WorkSpaces 访问 (p. 33).

物理主机上的隔离

同一物理主机上的不同 WorkSpaces 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，管理程序将清理分配给它的内存（设置为零），然后再将内存分配给新的WorkSpace。

企业用户授权

借助 WorkSpaces，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 (p. 53).

要进一步控制对 WorkSpaces 的访问，请使用多重验证。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 接口终端节点发出 Amazon WorkSpaces API 请求

您可以通过 Virtual Private Cloud （ VPC ） 中的Amazon WorkSpaces接口终端节点直接连接到 API 终端节点，而不是通过 Internet 连接。当您使用 VPC 接口终端节点时，您的 VPC 与 Amazon WorkSpaces API 终端节点之间的通信完全在 AWS 网络内安全进行。

> Note
>
> 此功能只能用于连接到 WorkSpaces API 终端节点。要使用 WorkSpaces 客户端连接到 WorkSpaces，需要 Internet 连接，如WorkSpaces 的 IP 地址和端口要求 (p. 16)中所述。

API 终端节点支持 Amazon WorkSpacesAmazon Virtual Private Cloud （ Amazon Virtual Private Cloud AWS Amazon VPC 提供支持 ）。PrivateLink 每个 VPC 终端节点都由您的 VPC 子网中一个或多个具有私有 IP 地址的网络接口（ 也称为弹性网络接口或 ENIs ）表示。

VPC 接口终端节点将您的 VPC 直接连接到 Amazon WorkSpaces API 终端节点，而无需 Internet 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 终端节点进行通信。

您可以通过 AWS 控制台或 Amazon WorkSpaces (AWS Command Line Interface) 命令创建接口终端节点来连接到 AWS CLI 有关说明，请参阅创建接口终端节点.

在创建 VPC 终端节点后，您可以使用以下示例 CLI 命令，这些命令使用 `endpoint-url` 参数指定连接到 Amazon WorkSpaces API 终端节点的接口终端节点：

```
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 终端节点启用专用 DNS 主机名，您不需要指定终端节点 URL。CLI 和 Amazon WorkSpaces 开发工具包默认使用的 Amazon WorkSpaces API DNS 主机名 （ https://api.workspaces.) Region.amazonaws.com ） 解析为您的 VPC 终端节点。

API 终端节点支持 Amazon WorkSpacesAmazon VPC 和 Amazon WorkSpaces 在其中均可用的所有 AWS 区域中的 VPC 终端节点。 支持调用 VPC 内其所有Amazon WorkSpaces公有 APIs。

要了解有关 AWS PrivateLink 的更多信息，请参阅 AWS PrivateLink 文档。有关 VPC 终端节点的价格，请参阅 VPC 定价. 要了解有关 VPC 和终端节点的更多信息，请参阅 Amazon VPC.

要查看按区域列出的 Amazon WorkSpaces API 终端节点的列表，请参阅 API 终端节点 WorkSpaces。 (p. 23)

> 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 创建 VPC 终端节点策略Amazon WorkSpaces

您可以为 Amazon VPC 的 Amazon WorkSpaces 终端节点创建一个策略，在该策略中指定以下内容：

- 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 用户指南 中的使用 VPC 终端节点控制对服务的访问Amazon VPC。

Note

联邦信息处理标准 (FIPS) Amazon WorkSpaces 终端节点不支持 VPC 终端节点策略。

以下示例 VPC 终端节点策略指定有权访问 VPC 接口终端节点的所有用户都可以调用名为 Amazon WorkSpaces 的 `ws-f9abcdefg`. 托管终端节点。

```
{
     "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 Amazon WorkSpaces 之外的 `ws-f9abcdefg`. 托管终端节点。
- 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，请参阅适用于 WorkSpaces 的 Identity and Access Management (p. 165)，以了解有关使用基于身份的策略控制对 Amazon WorkSpaces API 终端节点的访问的信息。

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 Amazon Virtual Private Network (VPN) 或 AWS Direct Connect. 将您的专用网络连接到 VPC。有关 Amazon VPN 的信息，请参阅 https://docs.aws.amazon.com/vpc/latest/userguide/vpn-connections.html 用户指南 中的 Amazon Virtual Private CloudVPN 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WorkSpaces上的操作系统和应用程序。 您可以将 WorkSpaces 配置为在常规维护时段内由 WorkSpaces 进行更新，也可以自行更新。有关更多信息，请参阅 WorkSpace 维护 (p. 104).

对于 WorkSpaces 上的应用程序，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的建议进行操作。

Amazon WAM

Amazon WorkSpaces Application Manager（Amazon WAM）提供了一种快速、灵活且安全的方法，可为您的 Windows WorkSpaces 部署和管理应用程序。 有关更多信息，请参阅 Amazon WAM Administration Guide。

排查 WorkSpaces 问题

以下信息可帮助您排除与 WorkSpace 相关的问题。

启用高级日志记录

为了帮助解决用户可能遇到的问题，您可以在任何 Amazon WorkSpaces 客户端上启用高级日志记录。在禁用高级日志记录之前，将为每个后续客户端会话启用高级日志记录。

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+ 客户端，这些高级日志记录文件会自动上传到 AWS 中的数据库。

Note

要让 AWS 审查由高级日志记录生成的日志文件，以及接收您的 WorkSpaces 客户端的技术支持问题，请联系 AWS Support。有关更多信息，请参阅 AWS 支持中心。

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 Amazon WorkSpaces 客户端。
2. 打开命令提示符应用程序。
3. 使用 `-l3` 标志启动 WorkSpaces 客户端。

```
c:

cd "C:\Program Files (x86)\Amazon Web Services, Inc\Amazon WorkSpaces"

workspaces.exe -l3
```

Note

如果为一个用户而不是所有用户安装了 WorkSpaces，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 Amazon WorkSpaces 客户端。

2. 打开终端。
3. 运行以下命令。

```
open -a workspaces --args -l3
```

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 Amazon 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 Save。

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

以下信息可帮助您排查与 WorkSpace 相关的特定问题。

问题

我无法创建 Amazon Linux WorkSpace，因为用户名中存在无效字符

对于 Amazon Linux WorkSpace，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。对于用户名中的所有字符，Windows WorkSpaces 支持 @ 和 - 符号。

我更改了 Amazon Linux WorkSpace 的 shell，现在我无法预配置 PCoIP 会话

要覆盖 Linux WorkSpaces 的默认 shell，请参阅 覆盖 Amazon Linux WorkSpace 的默认 Shell (p. 98)。

我的Amazon LinuxWorkSpaces 无法启动

自 2020 年 7 月 20 日起，亚马逊 Linux WorkSpaces 将使用新的许可证证书。这些新证书仅与 PCoIP 代理版本的 2.14.1.1、2.14.7 和 2.14.9 兼容。

如果您使用的是 PCoIP 代理不受支持的版本，则必须将其升级到最新版本 (2.14.9)，该版本具有与新证书兼容的最新修补程序和性能改进。如果您未在 7 月 20 日之前进行这些升级，则 Linux WorkSpaces 的会话预配将失败，并且您的最终用户将无法连接到其 WorkSpaces。

升级到最新版本

1. 通过以下网址打开 WorkSpaces 控制台：https://console.aws.amazon.com/workspaces/。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择您的 Linux WorkSpace，然后通过选择操作、重新启动 WorkSpaces。如果 WorkSpace 状态为`STOPPED`，您必须选择操作、启动 WorkSpaces，然后等到其状态为`AVAILABLE`，然后才能重新启动它。
4. 在您的 WorkSpace 重新启动并且其状态为`AVAILABLE`，建议您将 WorkSpace 的状态更改为`ADMIN_MAINTENANCE`当您执行此升级时。当您完成后，将 WorkSpace 的状态更改为`AVAILABLE`。有关 的更多信息`ADMIN_MAINTENANCE`模式，请参阅手动维护。

   将 WorkSpace 的状态更改为`ADMIN_MAINTENANCE`中，执行以下操作：

   a. 选择 WorkSpace，然后依次选择 Actions 和 Modify WorkSpace。
   b. 选择 Modify State。
   c. 适用于目标状态，选择管理维护。
   d. 选择修改。
5. 通过 SSH Connect 到 Linux WorkSpace。有关更多信息，请参阅 为您的 Linux WorkSpace 启用 SSH 连接 (p. 48)。
6. 要更新 PCoIP 代理，请运行以下命令：

   ```
   sudo yum --enablerepo=pcoip-stable install pcoip-agent-standard-2.14.9
   ```
7. 要验证代理版本并确认更新是否成功，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-2.14.9-27877.el7.x86_64
   ```
8. 断开与 WorkSpace 的连接，然后再次重新启动。
9. 如果将 WorkSpace 的状态设置为`ADMIN_MAINTENANCE`inStep 4 (p. 180)，重复此过程Step 4 (p. 180)并将设置为 Intended State 到`AVAILABLE`。

如果您的 Linux WorkSpace 在升级 PCoIP 代理后仍然无法启动，请联系 AWS Support。

经常无法在我连接的目录中启动 WorkSpace

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 WorkSpace 失败，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 Subnet Actions (子网操作) 和 Modify auto-assign IP settings (修改自动分配 IP 设置)。如果此设置启用，则无法使用性能或图形服务包启动 WorkSpace。解决办法是，在启动实例时，禁用此设置并手动指定 IPv6 地址。

当我尝试注册一个目录时，注册失败，并使目录处于错误状态

如果您尝试注册AWS已为多区域复制配置的托管 Microsoft AD 目录。虽然主区域中的目录可以成功注册，以便与Amazon WorkSpaces，尝试在复制的区域中注册该目录失败。使用多区域复制AWS托管微软 AD 不支持与Amazon WorkSpaces在复制的区域内。

我的用户无法连接到 Windows WorkSpace，系统显示了一个交互式登录横幅

如果实施了交互式登录消息以显示登录横幅，则会阻止用户访问其 Windows WorkSpace。WorkSpaces 目前不支持交互式登录消息的组策略设置。将 WorkSpace 移动到未应用 Interactive logon: Message text for users attempting to log on 组策略的组织单位 (OU)。

我的用户无法连接到 Windows WorkSpace

我的用户在尝试连接到他们的 Windows WorkSpaces 时收到以下错误：

```
"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 WorkSpace 以自动重新安装它。
- 您可能还会在Amazon WorkSpaces客户端长时间延迟后，如果WorkSpaces 安全组 (p. 41)已修改以限制出站流量。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。验证您的安全组是否允许 WorkSpace 通过主网络接口与所有必需端口 (p. 16)上的目录控制器进行通信。

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，它会阻止用户访问其 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：从网络访问此计算机

  设置：*Domain name*\ 域计算机

  获胜 GPO：允许文件访问
- 正确的策略：

  策略：从网络访问此计算机

  设置：*Domain name*\ 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。

我的用户在尝试从 WorkSpaces Web Access 登录 WorkSpaces 时遇到问题

Amazon WorkSpaces 依靠特定登录屏幕配置来让用户能够从 Web Access 客户端成功登录。

要使 Web Access 用户能够登录其 WorkSpaces，您必须配置“Group Policy (组策略)”设置和三个“Security Policy (安全策略)”设置。如果未正确配置这些设置，用户可能会在尝试登录其 WorkSpaces 时遇到长时间登录或黑屏。要配置这些设置，请参阅 启用和配置 Amazon WorkSpaces Web 访问 (p. 44)。

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。

Amazon WorkSpaces 客户端显示一个灰色的“正在加载...”屏幕一段时间，然后返回登录屏幕。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)。当未满足网络先决条件 (p. 16)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（通常是在 2.0+ 客户端登录屏幕右下角的红色三角形或网络图标在 3.0 + 客户端的右上角）。

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。

如果网络检查获得通过，则 WorkSpace 的网络配置可能存在问题。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。使用远程桌面协议 (RDP) 客户端 Connect 到 WorkSpace以验证 WorkSpace 是否满足必要的端口要求 (p. 16)。

我的用户收到消息 “WorkSpace 状态：不正常。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。

如果您刚刚重启或启动了 WorkSpace，请等待几分钟，然后重试。

如果 WorkSpace 已经运行了一段时间，而您仍然看到此错误，请使用 RDP 进行连接以验证 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。

我的用户收到消息“此设备未获授权，无法访问 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 IP 访问控制组 (p. 42)，但客户端 IP 地址未列入白名单。

检查您的目录上的设置。确认用户所连接的公有 IP 地址允许访问 WorkSpace。

我的用户收到消息 “没有网络。网络连接丢失。请检查您的网络连接或联系您的管理员寻求帮助。” 尝试连接到 WSP WorkSpace 时

如果发生此错误，并且您的用户没有连接问题，请确保网络防火墙上的端口 4195 处于打开状态。对 WorkSpaces 用WorkSpaces Streaming Protocol (WSP)，则用于流式传输客户端会话的端口从 4172 更改为 4195。

我的用户在使用 WorkSpaces 客户端时遇到了网络错误提示，但他们能够在其设备上使用其他网络支持的应用程序

WorkSpaces 客户端应用程序的运行依赖于对 AWS 云中资源的访问，需要可提供至少 1 Mbps 下载带宽的连接。如果设备是间歇性地连接到网络，WorkSpaces 客户端应用程序就可能报告网络问题。

从 2018 年 5 月开始，WorkSpaces 强制使用 Amazon Trust Services 颁发的数字证书。在 WorkSpaces 支持的操作系统上，Amazon Trust Services 已经是受信任的根 CA。如果操作系统的根 CA 列表不是最新的，则设备无法连接到 WorkSpaces，客户端会发出网络错误提示。

识别由于证书失败造成的连接问题

- PCoIP zero 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 Internet 红色警告三角形。

解决证书故障

- Windows 客户端应用程序 (p. 184)
- PCoIP Zero 客户端 (p. 184)
- 其他客户端应用程序 (p. 185)

Windows 客户端应用程序

使用以下解决方案之一处理证书故障。

解决方案 1：更新客户端应用程序

从 Amazon WorkSpaces Client Downloads 下载并安装最新 Windows 客户端应用程序。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 File (文件)、Add/Remove Snap-in (添加/删除管理单元)、Certificates (证书)、Add (添加)。
5. 在 Certificates snap-in (证书管理单元) 页面上，选择 Computer account (计算机账户)，然后选择 Next (下一步)。保留默认值 Local computer (本地计算机)。选择 Finish。选择 OK。
6. 展开 Certificates (Local Computer) (证书 (本地计算机))，然后选择 Trusted Root Certification Authorities (受信任的根证书颁发机构)。依次选择 Action (操作)、All Tasks (所有任务) 和 Import (导入)。
7. 按照向导的说明，导入下载的证书。
8. 退出并重启 WorkSpace 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 Zero 客户端

要直接连接到使用固件版本 6.0 或更高版本的 WorkSpace，请下载并安装由 Amazon Trust Services 发布的证书。

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 操作系统：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。”

当出现注册服务故障时，您的 WorkSpace 用户可能会在连接 Health 检查页: “您的设备无法连接到 WorkSpaces 注册服务。您无法向 WorkSpaces 注册设备。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会出现此错误。通常，这是在删除 WorkSpace 目录时出现。要纠正此错误，请确保注册代码有效并与 AWS 云中一个正在运行的目录相对应。

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 WorkSpace 设置 PCoIP 零客户端 (p. 44)。

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，系统将设置 SkipThisVersion 注册表项，并且在发布客户端的新版本时不再提示他们更新其客户端。要更新到最新版本，您可以编辑注册表，如将 WorkSpaces Windows 客户端应用程序更新到更新版本中的Amazon WorkSpaces 用户指南。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，系统将设置 `SUSkippedVersion` 首选项，并且在发布客户端的新版本时不再提示他们更新其客户端。要更新到最新版本，您可以按照将 WorkSpaces 的 macOS 客户端应用程序更新到更新版本中的Amazon WorkSpaces 用户指南。

我的用户无法在其 Chromebook 上安装 Android 客户端应用程序

Amazon WorkSpaces Chromebook 客户端应用程序的最终版本是 2.4.13 版。由于 Google 正在逐步退出对 Chrome 应用程序的支持，因此，将不会进一步更新 WorkSpaces Chromebook 客户端应用程序，并且不支持使用该应用程序。

对于支持安装 Android 应用程序的 Chromebook，建议您改为使用 WorkSpaces Android 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 (p. 44)。

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 或可信域创建的 WorkSpaces 的欢迎或密码重置电子邮件。

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 (p. 79)。

要重置用户密码，请参阅为 WorkSpaces 设置 Active Directory 管理工具 (p. 63)。

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 或可信域，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。）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 (p. 63)。

当我尝试在 Windows WorkSpace 上安装应用程序时，我收到消息“系统管理员已设置策略以阻止此安装”

您可以通过修改 Windows 安装程序组策略设置来解决此问题。若要将此策略部署到目录中的多个 WorkSpace，请将此设置应用于从加入域的 EC2 实例链接到 WorkSpace 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详细信息，请参阅安装 Active Directory 管理工具中的AWS Directory Service Administration Guide。

以下过程说明如何为 WorkSpaces 组策略对象配置 Windows 安装程序设置。

1. 确保您的域中安装了最新的 WorkSpaces 组策略管理模板 (p. 84)。
2. 在您的 Windows WorkSpace 客户端上打开组策略管理工具，导航并选择您的 WorkSpace 计算机账户的 WorkSpace 组策略对象。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 OK。
7. 要应用组策略更改，请执行下列操作之一：
   - 重启 WorkSpace（在 WorkSpaces 控制台中，选择WorkSpace，然后依次选择 Actions (操作)、Reboot WorkSpaces (重启 WorkSpace)）。
   - 从管理命令提示符下，输入 gpupdate /force。

我的目录中的 WorkSpaces 均无法连接到 Internet

默认情况下，WorkSpaces 无法与 Internet 通信。您必须显式提供 Internet 访问。有关更多信息，请参阅 提供 WorkSpace 的 Internet 访问权限 (p. 40)。

我的 WorkSpace 已失去对 Internet 的访问权限

如果您的 WorkSpace 已失去对 Internet 的访问权限，并且您无法使用 RDP 连接到 WorkSpace，则此问题可能是由于 WorkSpace 的公有 IP 地址丢失而导致的。如果您在目录级别启用了弹性 IP 地址自动分配 (p. 55)，则会在您的 WorkSpace 启动时为其分配弹性 IP 地址（来自 Amazon 提供的池）。但是，如果您将您拥有的弹性 IP 地址与 WorkSpace 关联，稍后您将该弹性 IP 地址与 WorkSpace 取消关联，则 WorkSpace 将失去其公有 IP 地址，并且不会自动从 Amazon 提供的池中获取新的 IP 地址。

要将 Amazon 提供的池中的新公有 IP 地址与 WorkSpace 关联，您必须重建 WorkSpace (p. 111)。如果您不想重建 WorkSpace，必须将您拥有的另一个弹性 IP 地址与 WorkSpace 关联。

我们建议您不要在 WorkSpace 启动后修改其弹性网络接口。将弹性 IP 地址分配给 WorkSpace 后，WorkSpace 会保留相同的公有 IP 地址（除非重建 WorkSpace ，在这种情况下，它会获得新的公有 IP 地址）。

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 WorkSpace 在空闲时进入睡眠状态

要解决此问题，请连接到 WorkSpace 并通过使用以下过程将电源计划更改为 High performance (高性能)：

1. 在 WorkSpace 中，打开控制面板，然后选择Hardware (硬件)或选择硬件和声音（名称可能会有所不同，具体取决于您的 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。
   - 如果选择高性能禁用电源计划，请选择更改当前不可用的设置，然后选择高性能电源计划。
   - 如果高性能计划不可见，请选择显示其他计划以显示它，或者选择创建电源计划在左侧导航窗格中，选择高性能，为电源计划提供一个名称，然后选择下一页。
4. 在存储库的更改计划的设置：高性能页面上，确保关闭显示和 (如果可用)将计算机置于睡眠状态设置为从来没有。
5. 如果您对高绩效计划做了任何改动，请选择保存更改。（或选择创建如果您正在创建一个新的计划）。

如果上述步骤无法解决该问题，请执行以下操作：

1. 在 WorkSpace 中，打开控制面板，然后选择Hardware (硬件)或选择硬件和声音（名称可能会有所不同，具体取决于您的 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)。

我的一个 WorkSpaces 显示UNHEALTHY

WorkSpaces 服务会向 WorkSpace 定期发送状态请求。当 WorkSpace 无法响应这些请求时，它将标记为 UNHEALTHY。导致此问题的常见原因包括：

- WorkSpace 上的某个应用程序阻塞了网络端口，这阻止 WorkSpace 响应状态请求。
- CPU 使用率高，阻止了 WorkSpace 及时响应状态请求。
- WorkSpace 的计算机名称已发生更改。这会阻止 WorkSpaces 与 WorkSpace 之间建立安全通道。

您可以尝试使用以下方法来纠正这种状况：

- 从 WorkSpaces 控制台重启 WorkSpace。
- 使用以下过程连接到不正常状态的 WorkSpace (此方法仅限于故障排除目的)：

  1. 连接到与不正常状态的 WorkSpace 同处一个目录下的运行正常的 WorkSpace。
  2. 从运行正常的 WorkSpace 中，通过远程桌面协议 (RDP) 使用不正常状态 WorkSpace 的 IP 地址连接到该不正常状态的 WorkSpace。根据问题的严重程度，您或许无法连接到不正常状态的 WorkSpace。
  3. 在运行状况不正常的 WorkSpace 上，确认满足最低端口 (p. 16)要求。

- 确保 SkyLightWorkSpacesConfigService 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：不正常。我们无法将您连接到您的 WorkSpace。请过几分钟再试。” (p. 183)。
- 从 WorkSpaces 控制台重建 WorkSpace。重建 WorkSpace 可能会导致数据丢失，因此该选项应只在所有其他尝试纠正此问题的措施都不成功的情况下使用。

我的 WorkSpace 意外崩溃或重启

如果您的 WorkSpace 反复崩溃或重启，并且您的错误日志或崩溃转储指向与 `spacedeskHookKmode.sys` 或 `spacedeskHookUmode.dll` 有关的问题，或者如果您收到以下错误消息，则可能需要禁用对 WorkSpace 的 Web 访问：

```
The kernel power manager has initiated a shutdown transition.
Shutdown reason: Kernel API
```

```
The computer has rebooted from a bugcheck.
```

Note

- 仅当您不允许用户使用 Web 访问时，才应禁用 Web 访问。
- Web 访问仅适用于 PCoIP WorkSpaces。Web 访问不可用于WorkSpaces Streaming Protocol (WSP)WorkSpaces。

要禁用对 WorkSpace 的 Web 访问，必须设置组策略并修改两个注册表设置。有关使用 Active Directory 管理工具处理组策略对象的信息，请参阅安装 Active Directory 管理工具中的AWS Directory Service Administration Guide。

步骤 1: 设置组策略以在目录级别禁用 Web 访问

您必须从 PCoIP WorkSpace 而不是域控制器进行这些更改，因为 STXHD 托管应用程序服务必须存在。

1. 编辑 WorkSpaces 使用的安全组以允许 RDP 连接。有关更多信息，请参阅 。如何使用 RDP 连接到 WorkSpace？。
2. 使用 RDP 连接到 WorkSpace。请确保您使用的是具有域权限的用户帐户来创建和修改 GPO。如果您正在为 WorkSpace 目录使用 Simple AD，则用户名为`Administrator`。如果您使用的是 Microsoft AD，则管理员用户名为`Admin`。
3. 安装活动目录管理工具 (RSAT) 以获取组策略管理编辑器工具。要安装这些工具，请参阅安装 Active Directory 管理工具中的AWS Directory Service Administration Guide。

   您还可以通过以管理员身份运行以下 Windows PowerShell 命令来安装这些工具：

   ```
   Install-WindowsFeature -Name GPMC,RSAT-AD-PowerShell,RSAT-AD-AdminCenter,RSAT-ADDS-
   Tools,RSAT-DNS-Server
   ```
4. 打开组策略管理编辑器 (gpmc.msc)，并在目录的域控制器级别找到组策略对象 (GPO) 策略。

   Note

   如果支持 WorkSpaces 的域是 AWS 托管的 Microsoft 活动目录，则必须在具有委派权限的域容器下创建并链接 GPO。有关更多信息，请参阅 。创建的内容中的AWS Directory Service Administration Guide。
5. 选择 Action (操作) 和 Edit (编辑)。

6. 导航到以下设置：

   计算机配置\ 策略\ Windows 设置\ 安全设置\ 系统服务\ STxHD 托管应用程序服务
7. 在 STXHD Hosted Application Service Properties (STXHD 托管应用程序服务属性) 对话框的 Security Policy Setting (安全策略设置) 选项卡上，选中 Define this policy setting (定义此策略设置) 复选框。
8. 在 Select Service Startup Mode (选择服务启动模式) 下，选择 Disabled (已禁用)。
9. 选择 OK。
10. 在完成注册表编辑（步骤 2）之前，阻止计算机重新启动。

步骤 2: 编辑注册表以禁用 Web 访问

我们建议您通过 GPO 推送这些注册表更改。

1. 将以下注册表项值设置为 1（已启用）：

   KeyPath = HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\WorkSpacesConfig\update-webaccess.ps1

   KeyName = RebootCount

   KeyType = DWORD

   KeyValue = 1
2. 将以下注册表项值设置为 4（已禁用）：

   KeyPath = HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\spacedeskHookKmode

   KeyName = Start

   KeyType = DWORD

   KeyValue = 4
3. 重启计算机。

同一用户名具有多个工作区，但用户只能登录到其中一个工作区

如果在 Active Directory (AD) 中删除用户而不先删除其工作区，然后将该用户添加回 Active Directory 并为该用户创建新的工作区，则同一个用户名现在将在同一目录中具有两个工作区。但是，如果用户尝试连接到其原始工作区，则将收到以下错误：

```
"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仅返回新的工作区，即使这两个工作区仍然存在。（您可以通过搜索工作区 ID 而不是用户名来查找原始工作区。）

如果在不首先删除用户的工作区的情况下重命名 Active Directory 中的用户，也会发生此行为。如果之后您将其用户名更改回原始用户名并为用户创建新的工作区，则同一用户名将在目录中有两个工作区。

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。在搜索用户名时，Amazon WorkSpaces 控制台使用 SID 搜索 Active Directory 中的匹配项。当客户端连接到工作区时，Amazon WorkSpaces 客户端还使用 SID 来标识用户。

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。如果您能够还原原始用户对象，请确保用户可以连接到其原始工作区。如果可以，您可以在手动备份并将任何用户数据从新工作区传输到原始工作区之后删除新的工作区 (p. 122)（如果需要）。
- 如果无法还原原始用户对象，请删除用户的原始工作区 (p. 122)。用户应该能够连接到并使用其新的工作区。请确保手动备份并将所有用户数据从原始工作区传输到新工作区。

  Warning

  删除工作区是一项永久性操作，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。

我在将 Docker 与 Amazon WorkSpaces 结合使用时遇到问题

Windows WorkSpaces

在 Windows WorkSpaces 上不支持嵌套虚拟化（包括使用 Docker）。有关更多信息，请参阅 。Docker 文档。

Linux WorkSpaces

要在 Linux 工作空间上使用 Docker，请确保 Docker 使用的 CIDR 块不会与与 WorkSpaces 关联的两个弹性网络接口 (ENI) 中使用的 CIDR 块重叠。如果在 Linux WorkSpaces 上使用 Docker 时遇到问题，请与 Docker 联系以获得帮助。

我的一些 API 调用收到了 ThrottlingException 错误

WorkSpaces API 调用的默认速率是一个恒定速率，为每秒两次 API 调用；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。
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。

秒	发送的请求数	允许的 Net 请求数	详细信息
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。

Amazon WorkSpaces 配额

以下是的配额（也称为限制）WorkSpaces为您的AWSaccount. 要请求增加配额，请使用 WorkSpaces 限制表单。

资源	默认值	描述	可调整
WorkSpaces	1	此账户中的 WorkSpaces 的最大数量。	是
Graphics WorkSpaces	0	此账户中的图形 WorkSpaces 的最大数量。	是
图形 Spaces WorkSpaces WorkSpace	0	此账户中的当前区域中的此账户中的图形 SWorkSpaces 的最大数目。	是
映像	40	此账户中的图像在当前区域中的最大数量。	是
Bundles (捆绑	50	此账户中的捆绑的最大数量。此配额仅适用于自定义的捆绑，而不适用于公共捆绑。	否
连接别名	20	此账户中的当前区域中的此账户中的连接别名的最大数目。	否
IP 访问控制组	100	此账户中的 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	此账户中的当前区域中的此账户中每个 IP 访问控制组的规则的最大数目。	否
每个目录的 IP 访问控制组数	25	此账户中的当前区域中的此账户中每个目录的 IP 访问控制组的最大数目。	否

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 Administration Guide 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。

update-history-change	update-history-description	update-history-date
Amazon WorkSpaces网络摄像头支持	Amazon WorkSpaces现在支持实时音频视频 (AV)，方法是将本地网络摄像头视频输入无缝重定向到 Windows WorkSpaces 桌面，使用WorkSpaces Streaming Protocol (WSP)。	April 5, 2021
Amazon WorkSpaces智能卡支持与 WorkSpaces macOS 客户端应用程序	现在，您可以使用Amazon WorkSpacesmacOS 客户端应用程序，具有通用访问卡 (CAC) 和个人身份验证 (PIV) 智能卡。智能卡支持可在 WorkSpaces 使用 WorkSpaces Streaming Protocol (WSP)。	April 5, 2021
Amazon WorkSpaces捆绑管理 API	Amazon WorkSpaces捆绑管理 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。	March 15, 2021
在亚太地区（孟买）中发布了 Amazon WorkSpaces	在 亚太地区（孟买）区域 中提供了 Amazon WorkSpaces。	March 8, 2021
智能卡	Amazon WorkSpaces现在支持 Windows 和 Linux WorkSpaces 上的会话前（登录）和会话中智能卡身份验证AWS GovCloud（美国西部）区域。	December 1, 2020
WorkSpaces Streaming Protocol (WSP)	这些区域有：WorkSpaces Streaming Protocol (WSP)现在可用于包含许可证（Windows 服务器 2016）和 BYOL 基于 Windows 10 的 WorkSpaces 上的所有捆绑包类型，除了图形和图形之 GraphicsPro。WSP也适用于 Linux WorkSpacesAWS GovCloud（美国西部）区域。	December 1, 2020
共享自定义映像	现在，您可以在 AWS 账户间共享自定义 WorkSpaces 映像。共享映像后，收件人账户可以复制映像，并将其用于创建用于启动新 WorkSpaces 的捆绑包。	October 1, 2020
跨区域重定向	现在，您可以使用跨区域重定向功能，此功能与域名系统 (DNS) 路	September 10, 2020

	由策略配合使用，以便在用户的主 WorkSpaces 不可用时将用户重定向到备用 WorkSpaces。	
订阅微软办公室 2016 年或 2019 年 BYOL WorkSpaces	您现在可以订阅微软办公室专业 2016 年或 2019 年AWSon 自带许可 (BYOL) WorkSpaces。	September 3, 2020
中国 (宁夏) 中的 BYOL 自动化	您可以使用自带许可 (BYOL) 自动化来简化对 中国 (宁夏) 中您的 WorkSpace 使用 Windows 10 桌面许可的过程。	April 2, 2020
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。	March 30, 2020
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。	January 9, 2020
适用于 Amazon WorkSpaces API 的 PrivateLink 集成	您可以通过 Virtual Private Cloud (VPC) 中的接口终端节点直接连接到 Amazon WorkSpaces API 终端节点，而不是通过 Internet 进行连接。当您使用 VPC 接口终端节点时，您的 VPC 与 Amazon WorkSpaces API 终端节点之间的通信完全在 AWS 网络内安全进行。	November 25, 2019
Amazon WorkSpaces 的 Linux 客户端	用户现在可以使用 Linux 客户端访问其 WorkSpace。	November 25, 2019
在中国 (宁夏)中发布了 Amazon WorkSpaces	在 中国 (宁夏) 区域 中提供了 Amazon WorkSpaces。	November 13, 2019
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。	September 18, 2019
FIPS 终端节点加密	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) 终端节点加密。	September 12, 2019

复制 WorkSpace 映像	您可以在同一区域内或跨区域复制映像。	June 27, 2019
适用于用户的自助服务 WorkSpace 管理功能	您可以为用户启用自助服务 WorkSpace 管理功能，使他们能够更好地控制其体验。	November 19, 2018
BYOL 自动化	您可以使用自带许可 (BYOL) 自动化来简化对您的 WorkSpace 使用 Windows 7 和 Windows 10 桌面许可的过程。	November 16, 2018
PowerPro 和 GraphicsPro 服务包	PowerPro 和 GraphicsPro 服务包现在可用于 WorkSpaces。	October 18, 2018
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。	September 17, 2018
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。	August 24, 2018
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。	July 31, 2018
Amazon Linux WorkSpaces	您可以为用户预置 Amazon Linux WorkSpaces。	June 26, 2018
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。	April 30, 2018
就地 升级	您可以将 Windows 10 BYOL WorkSpace 升级为 Windows 10 的较新版本。	March 9, 2018

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。

变更	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置 WorkSpace。	2017 年 2 月 9 日

变更	描述	日期
Windows Server 2016 服务包	WorkSpaces 提供了包含 Windows 10 桌面体验并由 Windows Server 2016 提供支持的服务包。	2016 年 11 月 29 日
Web 访问	您可以使用 WorkSpaces Web Access 从 Web 浏览器访问您的 Windows WorkSpace。	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 BYOLChromebook 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。	2015 年 10 月 1 日
CloudWatch 监控	添加了有关 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 在中发布了 亚太区域（新加坡）	WorkSpaces 在亚太区域（新加坡）区域中可用。	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 的 PCoIP 零客户端设备。	2014 年 10 月 15 日
WorkSpaces 在中发布了 亚太区域（东京）	WorkSpaces 在亚太区域（东京）区域中可用。	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

变更	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 在中发布了 亚太区域（悉尼）	WorkSpaces 在亚太区域（悉尼）区域中可用。	2014 年 5 月 15 日
WorkSpaces 在中发布了 欧洲（爱尔兰）	WorkSpaces 在欧洲（爱尔兰）区域中可用。	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。