亚马逊云科技

管理指南

Amazon WorkSpaces

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon WorkSpaces: 管理指南

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Amazon Web Services 文档中描述的 Amazon Web Services 服务或功能可能因区域而异。要查看适用于中国区域的差异，请参阅 中国的 Amazon Web Services 服务入门 (PDF)。

Table of Contents

什么是 WorkSpaces？ ... 1
使用客户端应用程序进行连接 ... 3
自带 Windows 桌面许可证 ... 4
使用自带 Windows 桌面许可证 WorkSpaces ... 4
关于上传和创建 BYOL 映像的视频 ... 15
在 WorkSpaces 中关联 BYOL 账户 ... 15
常见错误消息及其解决方案 ... 16
Sysprep 错误消息和错误修复列表 ... 22
使用和管理 WorkSpaces 个人 ... 23
WorkSpaces 个人版选项 ... 24
开始使用 WorkSpaces 个人版 ... 24
创建 WorkSpace ... 33
连接到 WorkSpace ... 35
后续步骤 ... 36
网络协议和访问权限 ... 36
适用于 Amazon 的协议 WorkSpaces ... 37
VPC 要求 ... 38
Amazon Global Accelerator（AGA） ... 43
WorkSpaces 的可用区 ... 45
IP 地址和端口要求 ... 47
网络要求 ... 65
受信任设备 ... 67
SAML 2.0 集成 ... 70
Microsoft Entra ID 访问 ... 91
智能卡身份验证 ... 92
互联网访问 ... 108
安全组 ... 109
IP 访问控制组 ... 110
PCoIP 零客户端 ... 113
为 Linux 启用 SSH 连接 WorkSpaces ... 114
必需配置和服务组件 ... 120
管理 WorkSpaces 目录 ... 126
注册现有 Amazon Directory Service 目录 ... 127
选择组织单位 ... 129

配置自动公有 IP 地址 130
控制设备访问 130
管理本地管理员权限 131
更新 AD Connector 账户 (AD Connector) 131
多重身份验证 (AD Connector) 132
创建一个目录 133
更新 WorkSpaces 的 DNS 服务器 154
删除目录 162
设置目录管理 164
管理用户 167
管理用户 167
为一个用户创建多个 WorkSpaces 169
自定义用户登录其 WorkSpaces 的方式 170
启用自助式 WorkSpace 管理功能 172
启用 Amazon Connect 音频优化 174
启用诊断日志上传 177
管理 WorkSpaces 个人版 178
管理窗口 WorkSpaces 179
管理你的亚马逊 Linux 2 WorkSpaces 228
管理你的 Ubuntu WorkSpaces 237
管理你的洛基 Linux WorkSpaces 244
管理你的红帽企业 Linux WorkSpaces 249
优化以进行实时通信 255
管理运行模式 266
管理应用程序 268
修改 WorkSpace 274
自定义品牌 281
标记资源 288
维护 290
已加密 WorkSpaces 292
重启 WorkSpace 301
重建 WorkSpace 302
还原 WorkSpace 304
升级 Windows BYOL WorkSpaces 305
迁移 WorkSpace 314
删除 WorkSpace 321

捆绑包和映像 322
捆绑包选项 324
创建自定义映像和捆绑包 330
更新自定义捆绑包 349
复制自定义映像 350
共享或取消共享自定义映像 353
删除自定义捆绑包或映像 355
监控 WorkSpaces 个人版 356
使用 CloudWatch 自动控制面板进行监控 357
使用 CloudWatch 指标进行监控 360
使用 Amazon EventBridge 进行监控 374
了解智能卡用户的 Amazon 登录事件 377
创建自定义 CloudWatch 仪表板 384
业务连续性 390
跨区域重定向 391
多区域韧性 405
问题排查 412
启用高级日志记录 413
排查特定问题 417
发行说明 442
使用和管理 WorkSpaces Pools 449
受支持的区域和可用区 449
管理目录 452
配置 SAML 2.0 和创建池目录 452
更新目录详细信息 469
删除 WorkSpaces 池目录 473
网络和访问 473
Internet 访问 474
VPC 要求 475
Amazon S3 VPC 端点 487
连接到您的 VPC 488
用户连接 490
创建 WorkSpaces Pools 493
管理 WorkSpaces Pools 495
运行模式 496
捆绑包 497

修改池 ... 497
删除池 ... 498
WorkSpaces Pools 的自动扩缩 ... 499
使用 Active Directory ... 509
Active Directory 域 ... 510
开始前的准备工作 ... 511
基于证书的身份验证 ... 513
管理 ... 519
更多信息 ... 525
捆绑包和映像 ... 526
捆绑包选项 ... 527
创建自定义映像和捆绑包 ... 531
管理自定义映像和捆绑包 ... 543
使用会话脚本管理体验 ... 545
监控 WorkSpaces Pools ... 554
WorkSpaces Pools 指标和维度 ... 554
管理永久存储 ... 556
管理主文件夹 ... 557
为用户启用应用程序设置持久性 ... 563
应用程序设置持久性如何工作 ... 563
启用应用程序设置持久性 ... 565
管理用户应用程序设置的 VHD ... 567
排查通知代码问题 ... 572
安全性 ... 576
数据保护 ... 576
静态加密 ... 577
传输中加密 ... 577
Identity and access management ... 578
策略示例 ... 579
在 IAM 策略中指定 WorkSpaces 资源 ... 586
创建工作空间_ 角色 DefaultRole ... 592
创建 AmazonWorkSpacesPCAAccess 服务角色 ... 593
Amazon的托管策略 WorkSpaces ... 594
对流媒体实例的访问权限 WorkSpaces 和脚本 ... 602
Amazon WorkSpaces 控制台操作权限参考 ... 607
合规性验证 ... 613

恢复能力 614
基础结构安全性 614
网络隔离 615
物理主机上的隔离 615
企业用户授权 615
创建接口 VPC 端点并进行流式传输 615
通过 VPC WorkSpaces 接口终端节点发出 Amazon API 请求 619
为 Amazon WorkSpaces 创建 VPC 端点策略 620
将您的专用网络连接到 VPC 621
更新管理 622
限额 623
WorkSpaces 客户生命周期结束 630
不受支持的客户端版本 632
EOL FAQs 635
我使用的 WorkSpaces 客户端版本已达到 EOL。我应该怎么做才能升级到受支持的版本？ .. 635
我能否使用已达到 EOL 且支持 WorkSpace版本的 WorkSpaces 客户端？ 635
我使用的 WorkSpaces 客户端版本已达到 EOL。我还能报告相关问题吗？ 635
我在已达到 EOL 的操作系统上使用支持的 WorkSpaces 客户端版本。我还能报告相关问题吗？ 635
扩展 SDK 开发人员指南 636
文档历史记录 637
早期更新 643
..... dcxlvi

什么是 Amazon WorkSpaces？

借助 Amazon WorkSpaces，您可以为用户预置基于云的虚拟桌面（称为 WorkSpaces）。这些桌面可以运行 Microsoft Windows、Amazon Linux 2、Ubuntu Linux、Rocky Linux 或 Red Hat Enterprise Linux。WorkSpaces 无需购买和部署硬件或安装复杂的软件。您可以根据需求的变更，快速添加或删除用户。用户可以从多个设备或 Web 浏览器访问自己的虚拟桌面。

Amazon WorkSpaces 允许您根据您的组织和用户需求，在 WorkSpaces 个人版和 WorkSpaces Pools 之间进行选择。

- WorkSpaces 个人版 - 如果您需要专为需要预置高度个性化桌面供其专用的用户量身定制的永久虚拟桌面，请选择 WorkSpaces 个人版。这类似于分配给个人的物理台式计算机。有关更多信息，请参阅 在 WorkSpaces 个人版中创建 WorkSpace。
- WorkSpaces Pools - 选择 WorkSpaces Pools 的非永久虚拟桌面，此类桌面专为需要访问托管在临时基础结构上的精心设置的桌面环境的用户量身定制。有关更多信息，请参阅 管理 WorkSpaces Pools 。

您可通过多种方式设置 WorkSpaces 桌面：

- 从一系列硬件配置、软件配置和 Amazon 区域中进行选择。有关更多信息，请参阅 Amazon WorkSpaces 捆绑包和the section called “创建自定义映像和捆绑包”。
- 如果您的 WorkSpaces 运行的是 Windows，您可以自带许可证和应用程序，也可以从适用于桌面应用程序的 Amazon Marketplace 中购买应用程序。
- 如果您的 WorkSpaces 运行的是 Windows 10 或 11，则可以将 WorkSpaces 加入 Microsoft Entra ID，这样，您的用户就可以使用其现有的 Entra ID 凭证获得对 Microsoft 365 Apps 企业版的无缝访问权。您也可以将 WorkSpaces 注册到 Intune，以便使用 Intune 管理您的虚拟桌面。有关更多信息，请参阅 使用个人版创建专用的 Microsoft Entra ID 目录 WorkSpaces 。要详细了解 Microsoft Entra ID，请参阅 What is Microsoft Entra ID?。要详细了解 Microsoft Intune，请参阅 Microsoft Intune securely manages identities, manages apps, and manages devices。
- 选择 PCoIP 或 DCV 协议。有关更多信息，请参阅 WorkSpaces 个人协议。
- 为您的用户创建独立的托管 Microsoft Active Directory，或将 WorkSpace 连接到您的本地 Active Directory，以便用户使用其现有凭证来无缝访问企业资源。有关更多信息，请参阅 the section called “管理 WorkSpaces 目录”。
- 用于管理 WorkSpace 的工具与您用来管理本地桌面的工具相同。
- 使用多重身份验证 (MFA)，以增强安全性。

- 使用 Amazon Key Management Service (Amazon KMS) 来加密静态数据、磁盘 I/O 和卷快照。
- 选择允许用户用于访问其 WorkSpace 的 IP 地址。
- 选择 WorkSpace 的按月或按小时计费。有关更多信息，请参阅 WorkSpaces 定价。

有关使用 WorkSpaces 的更多信息，请参阅：

- Amazon WorkSpaces 资源 - 包括白皮书、博客文章、网络研讨会和 re:Invent 会议
- 在云中预调配桌面
- 部署 Amazon WorkSpaces 的最佳实践
- Amazon WorkSpaces 常见问题
- 有关 WorkSpaces 定价详细信息和示例，请参阅 WorkSpaces 定价。

使用客户端应用程序连接到 WorkSpaces

您可以使用受支持设备上的客户端应用程序连接到 WorkSpaces，也可以在受支持的操作系统上使用支持的 Web 浏览器进行连接。

> **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
- iPad
- Android 设备
- Fire 平板电脑
- 零客户端设备（只有 PCoIP 支持 Teradici 零客户端设备。）

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

带上你自己的 Windows 桌面许可证 WorkSpaces

为了遵守 Microsoft 许可条款，请在Amazon云端专为你设计的硬件 WorkSpaces上Amazon运行 BYOL。通过提供您自己的许可证，您可以为用户提供一致的体验。有关更多信息，请参阅WorkSpaces 定价。

> **Important**
>
> 已从一个版本的 Windows 11 升级到较新版本的 Windows 11（Windows 功能/版本升级）的 Windows 11 系统不支持创建映像。例如，升级到 24H2 的 Windows 11 23H2 系统不能用于创建映像。但是， WorkSpaces 映像创建过程支持 Windows 累积更新或安全更新。

主题

- 使用自带 Windows 桌面许可证 WorkSpaces
- 关于上传和创建 BYOL 映像的视频
- 在 WorkSpaces 中关联 BYOL 账户
- 常见错误消息及其解决方案
- Sysprep 错误消息和错误修复列表

使用自带 Windows 桌面许可证 WorkSpaces

按照以下步骤在亚马逊中导入和使用您自己的 Windows 桌面许可证 WorkSpaces

在亚马逊上使用 Windows BYOL 的先决条件 WorkSpaces

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 non-GPU-enabled捆绑包（Graphics.g4dn、.g4dn、Graphics 和以外的捆绑包 GraphicsPro），请确认每个区域至少要使用 50 个 GraphicsPro。 WorkSpaces 这些 50 WorkSpaces 可以是 AlwaysOn 和的任意组合 AutoStop WorkSpaces。要在专用硬件 WorkSpaces 上运行，则要求 WorkSpaces 每个区域至少使用 50 个。为了符合 Microsoft 的许可要求，你必须在专用硬件 WorkSpaces 上运行。专用硬件在Amazon侧面配置，因此您的 VPC 可以保持默认租期。

如果您计划使用支持 GPU 的捆绑包（Graphics.g4dn、 GraphicsPro .g4dn、Graphics 和 GraphicsPro），请确认在专用硬件上每月在一个区域中至少运行 4 AlwaysOn 或 20 个 GPU 支持。AutoStop WorkSpaces

> **Note**
>
> - 作为图像导入过程的一部分，Amazon自动检索系统日志以解决图像导入错误，提供故障排除帮助，并向用户提供准确的错误消息。
> - Graphics.g4dn、 GraphicsPro .g4dn、Graphics 和 GraphicsPro 捆绑包在非洲（开普敦）地区和以色列（特拉维夫）地区不可用。
> - 要 WorkSpaces 在非洲（开普敦）地区跑步，你需要 WorkSpaces 在非洲（开普敦）地区跑至少400分。
> - 为了获得最佳视频会议体验，建议使用 Power（4 个 vCPU，16 GB 或更大内存）捆绑包。

- WorkSpaces 可以使用 /16 IP 地址范围内的管理接口。管理接口连接到用于交互式流媒体的安全 WorkSpaces 管理网络。这样可以 WorkSpaces 管理你的 WorkSpaces. 有关更多信息，请参阅 网络接口。为此，您必须至少从下列 IP 地址范围之一中保留一个 /16 网络掩码，并确保您选择的 IP 地址范围在您的网络中不会发生冲突：
  - 10.0.0.0/8
  - 100.64.0.0/10
  - 172.16.0.0/12
  - 192.168.0.0/16
  - 198.18.0.0/15

> **Note**
>
> - 在您采用该 WorkSpaces 服务时，可用的管理接口 IP 地址范围经常发生变化。要确定当前有哪些范围可用，请运行 list-available-management-cidr-ranges Amazon Command Line Interface (Amazon CLI) 命令。
> - 除了您选择的 /16 CIDR 块外，54.239.224.0/20 IP 地址范围还用于所有区域的管理接口流量。Amazon

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 22H2（2022 年 11 月更新）
- Windows 10 Enterprise LTSC 2019（1809）
- Windows 10 Enterprise LTSC 2021（21H2）
- Windows 11 Enterprise 23H2（2023 年 10 月发布）

你需要使用支持的 Windows 操作系统版本的 Windows 虚拟机映像或 Windows ISO 映像文件：

- 登录微软 365 管理中心，下载企业版 ISO 镜像。在 Visual Studio 订阅门户上登录您的订阅以获取可用下载内容。请勿使用从不提供企业版 ISO 的 Windows 11 公共下载网站上下载的 ISO 文件。
- 要使用自定义的虚拟机映像，请在导入之前验证您的映像。
- 导入过程中不支持加密 AMIs 。可以在配置最终 WorkSpaces 版本后启用加密。
- 不支持默认 EBS 加密。在导入图像之前，请在 EC2 控制台中禁用默认加密。
- 对于 Windows 11 映像， WorkSpaces 需要启用 UEFI 启动模式。有关 EC2 Image Builder 如何检测启动模式的更多信息，请参阅《虚拟机 Import/Export 用户指南》中的 “虚拟机导入/导出” 支持的卷类型和文件系统。
- 所有支持的操作系统版本都支持您使用的Amazon区域中可用的所有计算类型 WorkSpaces。微软不再支持的 Windows 版本不能保证能正常运行，Support 也不支持这些版本。Amazon

> **Note**
>
> 目前，BYOL 不支持 Windows 11 版本。

第 1 步：为你的账户启用 BYOL

在确认自己满足将 Windows BYOL 与一起使用的先决条件后 WorkSpaces，需要启用您的帐户才能使用 BYOL 映像。

1. 在 WorkSpaces 控制台中，导航至 “账户设置” 页面。
2. 在“自带许可（BYOL）”部分，您会看到账户的 BYOL 启用状态。如果状态显示账户未启用，请选择开始使用 BYOL 按钮。
3. 在 BYOL 页面上，选择“为账户启用 BYOL”。

> **Note**
>
> 为账户启用 BYOL 仅适用于单个区域。请记下您当前所在的区域，如果您想使用其他区域，请在为账户启用 BYOL 前切换到相应区域。

4. 将出现一个弹出模式，确认您了解使用 BYOL WorkSpaces 的最低要求。确认您已了解相关要求，然后选择“启用账户”。

> **Note**
>
> 如果您打算将 Graphics WorkSpaces 与 BYOL 配合使用，请创建 Su Amazon pport 请求单。控制台尚不支持启用 Graphics BYOL。 WorkSpaces

5. 在大多数情况下，账户会自动启用。但是，有些账户需要进一步审核。刷新后，您会在 BYOL 页面上看到启用状态。
6. 为账户启用 BYOL 后，请继续执行下一步。

（可选）在导入之前验证映像

> **Note**
>
> 此步骤仅适用于要导入的自定义虚拟机映像。如果您要导入的是 Windows ISO，则可跳过此步骤。

如果您要导入自定义的虚拟机映像，我们建议您运行 WorkSpaces Image Checker 工具，以确保您的虚拟机与 WorkSpaces兼容。映像检查程序工具会运行一系列测试，并且可以帮助修复兼容性问题。

下载映像兼容性检查程序脚本

在下载并运行映像兼容性检查程序脚本之前，请验证虚拟机上是否安装了最新的 Windows 安全更新。此脚本在运行时会禁用 Windows 更新服务。

1.
2. 在 `Downloads` 文件夹中，创建一个 `BYOL` 文件夹。
3. 从 `ImageCompatibilityChecker.zip` 中提取文件并将其复制到 `Downloads\BYOL` 文件夹。
4. 删除 `Downloads\ImageCompatibilityChecker.zip` 文件夹，以便仅保留提取的文件。

检查是否未启用 Windows 虚拟机 BitLocker。

确保未启用 Windows 虚拟机 BitLocker

1. 以管理员身份打开 PowerShell。
2. 运行如下命令：

```
manage-bde -off  DriveLetter:
```

3. BitLocker 通过运行以下命令来检查的状态：

```
manage-bde -Status  DriveLetter:
```

4. 确保显示的值与以下值相匹配：
   - BitLocker 版本-无
   - 转换状态 – 已完全解密
   - 加密百分比 – 0.0%
   - 加密方法 - 无
   - 保护状态 - 保护已关闭
   - 锁定状态：已解锁

执行以下步骤以运行映像兼容性检查程序脚本。

运行映像兼容性检查程序脚本

1. 以管理员身份打开 PowerShell。
   1. 选择 Windows 的“开始”按钮。
   2. 右键单击 Windows PowerShell。
   3. 选择以管理员身份运行。
   4. 如果出现用户账户控制提示，请选择是。
2. 在 PowerShell 命令提示符处，切换到 “图像兼容性检查器” 脚本所在的目录。例如，如果脚本位于 `Downloads\BYOL` 目录中，请输入以下命令并按 Enter：

   ```
   cd C:\Users\username\Downloads\BYOL
   ```

3. 输入以下命令以更新计算机上的 PowerShell 执行策略。这样可以运行映像兼容性检查程序脚本：

```
Set-ExecutionPolicy AllSigned
```

4. 当系统提示您确认是否更改 PowerShell 执行策略时，请输入A以指定 Yes to All。
5. 输入以下命令以运行映像兼容性检查程序脚本：

   ```
   .\ImageCompatibilityChecker.exe
   ```

6. 如果有安全通知出现，请按 R 键以运行一次。
7. 在 “WorkSpaces 图像验证” 对话框中，选择 “运行测试”。
8. 每个测试完成后，您都可以查看测试的状态。对于状态为 FAILED (失败) 的任何测试，请选择 Info (信息) 以显示有关如何解决导致失败的问题的信息。如果任何测试显示了状态 WARNING (警告)，请选择 Fix All Warnings (修复所有警告) 按钮。
9. 适当时，请解决导致测试故障和警告的任何问题，然后重复 Step 7 和 Step 8，直到 VM 通过所有测试。您在导出 VM 之前必须解决所有故障和警告。
10. BYOL 脚本检查程序将生成两个日志文件：`WorkSpacesImageCompatabilityCheckLog`*`YYYY-MM-DD_HHmmss`*`.txt` 和 `ImageInfo.text`。这两个文件位于映像兼容性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。

    您还将看到运行 Sysprep 的提示。关闭提示，暂时不要运行 Sysprep。

12. 关闭虚拟机并将其导出。有关更多信息，请参阅《虚拟机 Import/Export 用户指南》中的将虚拟机从其虚拟化环境中导出。
13. （可选）启动虚拟机并再次运行映像兼容性检查程序脚本。应通过所有验证。屏幕将再次弹出，上面有一个用于运行 Sysprep 的按钮。选择运行 Sysprep。如果 Sysprep 成功，则可以将您在步骤 12 中导出的虚拟机导入到亚马逊弹性计算云 (Amazon)。 EC2

    如果 Sysprep 不成功，请查看 `%WINDIR%\System32\Sysprep\Panther` 路径中的 Sysprep 日志，从步骤 12 回滚到导出的虚拟机，解决报告的问题，然后通过导出固定虚拟机再次完成步骤 12。然后，重新运行映像兼容性检查程序脚本，以确保问题已得到解决。

    Sysprep 失败的最常见原因是未针对所有用户卸载现代 AppX 程序包。使用 `Remove-AppxPackage` PowerShell cmdlet 移除 AppX 软件包。

14. 将您在步骤 12 中导出的虚拟机导入到 Amazon EC2。

步骤 2：使用 WorkSpaces 控制台创建 BYOL 映像

执行以下步骤导入您的图像并创建 WorkSpaces BYOL 映像：

1. 转至导航窗格并选择映像，然后选择导入映像。
2. 根据基础映像选项和要导入的映像类型，按照导入映像页面上的步骤进行操作：
   - 虚拟机导入：导入已经自定义的虚拟机映像。您可以导入 VHDX、VMDK 或 OVF 文件。
   - ISO 导入：导入从 Microsoft 下载的未自定义的 Windows ISO 映像。
   - AMI 导入 — 导入现有亚马逊 EC2 AMI 以用作您的 WorkSpaces BYOL 映像。
3. 请执行以下操作之一：
   - 对于虚拟机导入选项，请将您的文件上传到 Amazon S3，然后指定文件要导入的位置。请注意，您使用的 S3 存储桶必须与您打算部署 BYOL WorkSpaces 的区域相同。
   - 对于 ISO 导入：导入从 Microsoft 下载的未自定义的 Windows ISO 映像。请注意，您使用的 S3 存储桶必须与您打算部署 BYOL WorkSpaces 的区域相同。
   - 对于AMI 导入，请指定 AMI ID。
4. 转至基础设施配置。

   WorkSpaces 自动创建 Amazon EC2 Image Builder 管道来构建 BYOL 映像。基础架构配置定义了如何配置 EC2 Image Builder 来构建您的映像。您可以使用以下设置对其进行自定义：

   - 服务默认值：创建并使用默认 IAM 角色和策略来构建映像。
   - 使用现有基础设施配置-提供在 Amazon Im EC2 age Builder 中设置的自定义基础设施配置。有关更多信息，请参阅 I EC2 mage Builder 用户指南中的创建基础设施配置。
5. 前往高级设置并选择是否要在图像遇到导入错误时终止 EC2 构建实例。
   - 如果您选择在出现故障时终止实例，则在映像导入工作流程中，您将无法访问实例来调试错误。
   - 如果您选择不终止实例，则可以使用该实例来调试错误，但运行该 EC2 实例可能会产生额外费用。
6. 转至映像详情以指定映像的属性：包括映像名称。
   - 映像名称：映像的唯一标识符。
   - 计算类型：指定此映像应使用非图形/基础硬件还是图形硬件

- 操作系统版本：选择映像的 Windows 操作系统版本
- 语义版本-为图像定义语义版本，该版本将存储在 Image Builder EC2 中。有关更多信息，请参阅 Image Builder 用户指南中的 Image Builder 中的EC2 语义版本控制

> **Note**
>
> 在 BYOL 导入过程中，将在您的Amazon账户中创建 EC2 Image Builder 资源。为了创建映像，系统会自动创建名为 `AWSServiceRoleForImageBuilder` 的服务相关角色（若该角色尚未存在）。此角色将包含Amazon托管策略`AWSServiceRoleForImageBuilder`。您还必须拥有 VM Import/Export 所需的权限才能导入自定义虚拟机映像。

创建映像时，控制台映像页面上的状态将显示为待处理。BYOL 摄取过程至少需要 90 分钟。

导入映像时出现的错误将与建议解决方案一起显示在映像页面上。详细日志可在亚马逊导入图像时创建的 Image Builder 日志组 CloudWatch 下找到。可能的错误类型如下：

- 图像错误-Image Builder 无法生成 EC2 图像。修复虚拟化环境中的问题并导入新映像。
- Image Builder 错误：尝试构建映像时出错。查看亚马逊上的 Image Builder 日志，了解更多 CloudWatch 详情
- EC2 错误-您的图像存在无法自动修复的问题。要解决这些错误，您可以连接到 Amazon EC2 实例（如果该实例设置为在构建失败时不终止）并直接执行修复。然后，您可以从“映像”页面重试导入。
- 自动修复错误-这些问题已由自动修复。 WorkSpaces无需进一步操作。

有关常见错误的详细信息，请参阅常见错误消息及其解决方案。

步骤 3：选择 BYOL 管理接口的 IP 地址范围

BYOL 在专用硬件上 WorkSpaces 运行，以符合微软许可条款。为了支持这一点，我们创建了 BYOL 管理接口，以便在您 WorkSpaces 和Amazon托管 WorkSpaces 管理网络之间建立安全连接。有关更多信息，请参阅网络接口。

如果您在同一地区有另一个Amazon账户启用了 BYOL，则应在账户之间使用相同的管理界面来保留更少的 IP 地址。为此，请不要选择管理接口 IP 地址范围，可参阅下面的关联 BYOL 账户。

选择管理接口 IP 地址范围

1. 返回账户设置中的 BYOL 页面。

2. 在选择 IP 范围部分中，选择选择 IP 范围按钮。
3. 通过提供您的网络上可用的 IP 地址范围来输入搜索范围。 WorkSpaces 返回与您的搜索相匹配的可用的 /16 网络掩码 IP 地址范围。
4. 选择可用的 IP 地址范围（以 CIDR 数据块的形式显示）。

> **Note**
>
> 为管理接口选择 IP 范围后，便无法更改。

关联 BYOL 账户

如果您在同一地区有另一个启用了 BYOL 的Amazon账户，该账户共享相同的付款人账户，则应在账户之间使用相同的管理界面来预留更少的 IP 地址。关联账户还可以避免满足每个账户的最低 BYOL 要求，因为最低要求是在关联账户之间共享的。如果您在同一个付款人账户下没有启用了 BYOL 的另一账户，请跳过此步骤。

要关联到现有 BYOL 账户，请不要选择 IP 地址范围。

关联 BYOL 账户

1. 登录已启用 BYOL WorkSpaces 的Amazon账户。
2. 导航至账户设置中的 BYOL 页面。
3. 在选择 IP 范围部分中，选择账户关联部分下的发送邀请按钮。
4. 提供未启用 BYOL 且您希望关联的账户的账户 ID。Amazon

> **Note**
>
> 这两个账户必须在同一区域使用 BYOL。

5. 关联邀请发送后，返回尚未启用 BYOL 的Amazon账户。在账户设置页面中，您将看到一条横幅通知，显示您有待处理的 BYOL 账户关联邀请。在横幅中选择查看邀请。
6. 确认账户关联邀请。

如果您想对同一付款人账户下的两个账户使用不同的管理界面，请联系 Su Amazon pport 寻求帮助。

第 4 步：使用中的 BYOL 映像创建自定义捆绑包 WorkSpaces

按照中的说明创建 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，请参阅为 WorkSpaces 个人版创建自定义 WorkSpaces 镜像和捆绑包。

第 5 步：为 Amazon 创建专用目录 WorkSpaces

要将 BYOL 映像用于 WorkSpaces，必须为此目的创建一个目录。

要为创建目录 WorkSpaces，请参阅为 WorkSpaces 个人创建目录。确保在创建目录 WorkSpaces 时选择 “启用专用”。

> **Important**
>
> 如果您在注册目录时看不到 “启用专用 WorkSpaces ” 选项，请确保已完成在您的账户和地区启用 BYOL 的步骤。
> 如果你已经注册了未在专用硬件上运行的 Microsoft AD Amazon 托管目录或 AD Connector 目录，则可以为此目的设置一个新的Amazon托管微软 AD 目录或 AD Connector 目录。WorkSpaces 您也可以取消注册该目录，然后将其重新注册为专用 WorkSpaces目录。要了解有关注册和取消注册现有Amazon目录服务目录的更多信息，请参阅向 WorkSpaces 个人注册现有Amazon目录服务目录。

第 6 步：启动 BYOL WorkSpaces

启动你的 BYOL WorkSpaces 个人版

要启动个人账户 WorkSpaces，请参阅在 WorkSpaces 个人版 WorkSpace 中创建。

启动你的 BYOL 池 WorkSpaces

要启动矿 WorkSpaces 池，你必须启动个人账户 WorkSpace，创建该个人的镜像 WorkSpace，然后使用该镜像启动池。

为 BYOL 池 WorkSpaces 创建映像

1. 使用您要用于 WorkSpaces 矿池的 BYOL 镜像启动个人 WorkSpace 账户。有关如何启动 WorkSpaces 个人版的信息，请参阅在个人版 WorkSpace 中 WorkSpaces 创建。
2. 登录个人版 WorkSpace 并确保所有的 Windows 更新都已安装。

3. 更新您的 Amazon EC2 配置。要使用 Windows 10 更新您的 EC2 配置，请参阅安装最新版本的 EC2 Config。要使用 Windows 11 更新您的 EC2 配置，请参阅安装最新版本的 EC2 Launch。
4. 添加 Windows Defender 排除列表。有关更多信息，请参阅 Add an exclusion to Windows Security。

   在 Windows Defender 中将以下文件夹添加到排除列表中：

   - `C:\Program Files\Amazon\`
   - `C:\ProgramData\Amazon\*`
   - `C:\Program Files\NICE\`
   - `C:\ProgramData\NICE\`
   - `C:\Program Files (x86)\AWS Tools\*`
   - `C:\Program Files (x86)\AWS SDK for .NET\*`
   - `C:\AWSEUC\`（这适用于会话脚本）
5. 输入以下命令，在启动时禁用 Windows 更新。
6. 以管理员身份打开 PowerShell。

   1. 选择 Windows 的“开始”按钮。
   2. 右键单击 Windows PowerShell。
   3. 选择以管理员身份运行。
   4. 如果出现用户账户控制提示，请选择是。
7. 运行以下命令：

```
New-Item -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate" -Force
```

```
New-Item -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU" -Force
```

```
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU"
 -Name "NoAutoUpdate" -Value 1 -Force
```

8. 重新启动 WorkSpace。有关更多信息，请参阅 WorkSpaces 个人版 WorkSpace 中的重启。

   > **Note**
   >
   > 我们建议您在开始为 BYOL WorkSpaces 池创建映像之前执行以下操作。

- 删除不必要的启动应用程序。
- 删除或禁用不必要的计划任务。打开“开始”菜单，选择计划任务，选择要禁用的任务，然后选择禁用。

9. 通过输入以下命令，在重新启动后运行映像检查程序。

```
C:\Program Files\Amazon\ImageChecker.exe
```

10. 解决映像检查程序发现的任何错误。有关更多信息，请参阅“解决映像检查程序检测到的问题的提示”。
11. 所有测试均通过图像检查器后，返回 WorkSpaces 控制台。
12. 在导航窗格中 WorkSpaces，选择个人。选择 BYOL 个人 WorkSpaces，然后选择 “操作”、“创建图像”。
13. 在导航窗格中，选择映像。在映像下，检查是否已创建映像。

现在，您可以使用您创建的映像启动 P WorkSpaces ools。有关启动 WorkSpaces 池的更多信息，请参阅创建 WorkSpaces 池。

关于上传和创建 BYOL 映像的视频

有关上传 BYOL 映像的演示，请观看以下视频。

有关使用 Microsoft Hyper-V 创建 BYOL 映像的演示，请观看以下视频。

有关使用 VMware Workstation 创建 BYOL 映像的演示，请观看以下视频。

在 WorkSpaces 中关联 BYOL 账户

您可以使用 BYOL 链接来关联账户和共享 BYOL 配置。BYOL 配置包括您账户使用的 CIDR 范围，以及您通过 Windows 许可证创建 WorkSpaces 时使用的映像。所有关联的账户共享相同的底层硬件基础结构。

启用 BYOL 关联的账户是底层硬件基础结构的主要所有者，称为源账户。源账户管理对底层硬件基础结构的访问权限。目标账户是指与源账户关联的账户。

> **Important**
>
> Amazon GovCloud (US) Region中没有用于 BYOL 账户关联的 API。

> **Note**
>
> 您要关联的 Amazon 账户必须是您组织的一部分（在同一付款人账户下）。您只能关联同一区域内的账户。

关联源账户和目标账户

1. 使用 CreateAccountLinkInvitation API 将邀请链接从源账户发送到目标账户。
2. 使用 AcceptAccountLinkInvitation API 接受来自目标账户的待处理链接。
3. 使用 GetAccountLink 或 ListAccountLinks API 验证是否已建立链接。

常见错误消息及其解决方案

BYOL 导入不支持安装了处于活动状态的 Microsoft Office 的系统。

导入前必须卸载 Microsoft Office。有关更多信息，请参阅从 PC 上卸载 Office。

BYOL 导入要求系统没 PCo有 IP 代理。

卸载 PCo IP 代理。有关卸载 PCo IP 代理的信息，请参阅卸载 Mac 版 Teradici PCo IP 软件客户端

BYOL 导入需要禁用 Windows 更新。

按照以下步骤禁用 Windows 更新：

1. 按 Windows 键 + R。 键入 `services.msc`，然后按 Enter。
2. 右键单击 Windows 更新，然后选择属性。
3. 在常规选项卡下，将启动类型设置为禁用。
4. 选择停止。

5. 单击应用，然后选择确定。
6. 重新启动您的计算机。

BYOL 导入需要启用自动挂载。

您必须启用自动挂载。以管理员身份在 PowerShell 中运行以下命令：

```
C:\> diskpart
DISKPART> automount enable
```

已启用自动挂载新卷。

BYOL 导入需要启用 WorkSpaces _BYOL 帐户

WorkSpaces必须启用 _BYOL 帐户。有关更多信息，请参阅使用亚马逊 WorkSpaces 控制台为您的账户启用 BYOL 的 BYOL。

BYOL 导入要求网络接口使用 DHCP 自动分配 IP 地址。网络接口当前使用静态 IP 地址。

必须更改网络接口才能使用 DHCP。有关更多信息，请参阅更改 TCP/IP 设置。

BYOL 导入需要本地磁盘上超过 20 GB 的空间。

本地磁盘必须有足够的空间，并且需要您腾出 20 GB 或更多空间。

BYOL 导入要求系统具有 1 个本地驱动器。还有其他本地驱动器、可移动驱动器或网络驱动器。

用于导入 BYOL WorkSpace 映像的 Amazon 系统映像上只能有 C 盘。删除所有其他驱动器，包括虚拟驱动器。

BYOL 导入需要 Windows 10 或 Windows 11。

使用 Windows 10 或 Windows 11 操作系统。

BYOL 导入需要未加入 AD 域的系统。

必须取消系统与 AD 域的连接。有关更多信息，请参阅 Azure Active Directory 设备管理常见问题。

BYOL 导入需要未加入 Azure 域的系统。

必须取消系统与 Azure 域的连接。有关更多信息，请参阅 Azure Active Directory 设备管理常见问题。

BYOL 导入需要禁用 Windows 公共防火墙。

必须禁用公共防火墙配置文件。有关更多信息，请参阅打开或关闭 Microsoft Defender 防火墙。

BYOL 导入需要没有 VMware 工具的系统。

VMWare 必须卸载工具。有关更多信息，请参阅在 VMware Fusion 中卸载和手动安装 VMware 工具 (1014522)。

BYOL 导入要求本地磁盘容量小于 80 GB。

磁盘必须小于 80 GB。减小磁盘大小。

BYOL 导入需要本地驱动器上的分区少于 2 个。此外，所有 Windows 10 分区都必须采用 MBR 分区，所有 Windows 11 分区都必须采用 GPT 分区。

对于 Windows 10，卷必须采用 MBR 分区，对于 Windows 11，卷必须采用 GPT 分区。有关更多信息，请参阅管理磁盘。

BYOL 导入需要完成所有需要重启的待处理更新。

安装所有更新并重启操作系统。

BYOL 导入要求将其禁 AutoLogon 用。

要禁用 AutoLogon 注册表，请执行以下操作：

1. 按 Windows 键 + R，然后在命令提示符处键入 `Regedit.exe`。
2. 向下滚动到 `HKEY_LOCAL_Machine\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon`
3. 为 `DontDisplayLastUserName` 添加一个值。
4. 对于类型，输入 `REG_SZ`。
5. 对于值，请输入 `0`。

> **Note**
>
> - 值 `DontDisplayLastUserName` 决定登录对话框是否显示上次登录 PC 的用户的用户名。
> - 默认情况下，该值不存在。如果存在，则必须将其设置为，`0`否则的值`DefaultUser`将被擦除并 AutoLogon 失败。

BYOL 导入需要启用 `RealTimeIsUniversal`。

RealTimeUniversal 必须启用注册表项。有关更多信息，请参阅为 Windows Server 2008 和更高版本配置时间设置。

BYOL 导入要求系统具有一个可启动分区。

可启动分区的数量不得超过一个。

移除其他分区

1. 按 Windows 徽标 + R 键，打开运行框。输入 `msconfig`，并按键盘上的 Enter 键，打开“系统配置”窗口。
2. 从窗口中选择启动选项卡，然后检查要使用的操作系统是否设置为当前操作系统；默认操作系统。如果未设置，请从窗口中选择所需的操作系统，然后在同一窗口中选择设置为默认值。
3. 要删除其他分区，请选择该分区，然后选择删除、应用、确定。

如果错误仍然出现，请从安装光盘或修复光盘启动计算机，然后按照以下步骤操作。

1. 跳过初始语言屏幕，然后在主安装屏幕上选择修复计算机。
2. 在选择选项屏幕上，选择问题排查。
3. 在高级选项屏幕上，选择命令提示符。
4. 在命令提示符处输入 `bootrec.exe /fixmbr`，然后按 Enter。

BYOL 导入需要 64 位系统。

必须使用 64 位操作系统映像。有关更多信息，请参阅 BYOL 支持的 Windows 版本。

BYOL 导入需要使用尚未就地升级的系统。该系统已就地升级。

Windows 必须尚未从以前的版本升级。

BYOL 导入要求系统上未安装防病毒软件。

必须卸载防病毒软件。运行 Image Compatibility Checker 以获取要卸载的防病毒软件的详细信息。

BYOL 导入要求 Windows 10 系统使用旧版启动模式。

Windows 10 BootMode 必须使用旧版 BIOS。有关更多信息，请参阅启动模式。

BYOL 导入要求禁用 Windows 预留存储状态

禁用预留存储状态

1. 安装所有 Windows 更新并重启操作系统。
2. 确保没有新的更新。
3. 以管理员身份在 PowerShell 中运行以下命令之一：
   - `Set-WindowsReservedStorageState -State Disabled`
   - `DISM.exe /Online /Set-ReservedStorageState /State:Disabled`
4. 重启系统。

> **Note**
>
> 如果预留存储正在使用中，则可能无法将其禁用，并且会返回以下错误消息：`This operation is not supported when reserved storage is in use. Please wait for any servicing operations to complete and then try again later.`

BYOL 导入有正在使用的受限驱动器号。

`D:`云端硬盘是受限制的驱动器号 WorkSpaces。请确保 `D:` 在从映像启动实例期间未被使用或不会被映射。

BYOL 导入的操作系统映像与所选的流式传输协议不兼容。

所选的流媒体协议不支持正在导入的图像，请参阅使用 WorkSpaces 控制台创建 BYOL 映像。

BYOL 导入与内存完整性不兼容。

在的 Windows 操作系统上启用凭据保护时，不支持内存完整性。 WorkSpace已检测到内存完整性，在图像导入过程中无法禁用 UEFILock 该完整性。请导入 UEFILock 禁用映像，请参阅禁用凭据保护。

BYOL 导入要求禁用 Bitlocker 状态。

禁用 Bitlocker：

1. 以管理员身份打开 PowerShell。
2. 运行如下命令：

```
manage-bde -off  DriveLetter:
```

3. BitLocker 通过运行以下命令来检查的状态：

```
manage-bde -Status  DriveLetter:
```

4. 确保显示的值与以下值相匹配：

   - BitLocker 版本-无
   - 转换状态 – 已完全解密
   - 加密百分比 – 0.0%
   - 加密方法 - 无
   - 保护状态 - 保护已关闭
   - 锁定状态 - 已解锁

WorkSpaces 由于自定义镜像存在时间同步问题，创建失败

默认情况下，自定义映像作为默认 NTP 服务器发送到“time.windows.com”。如果无法访问 NTP 服务器，则可能会出现时间同步问题，从而导致 RDP/Skylight 证书验证失败和 SSL 连接问题，从而阻止 WorkSpaces 创建。

如果您遇到时间同步问题，请更新 NTP 服务器以使用 Amazon Time Sync Service（位于 169.254.169.123）。有关更多信息，请参阅 Configure the time for your Windows instance。

Sysprep 错误消息和错误修复列表

您要导入的 AMI 安装了 AppX 程序包。将其移除并重新导入映像。

可能仍会为您的用户安装现代 AppX 程序包。通过运行 Powershell `cmdlet`、`Remove-AppxPackage` 来删除 AppX 程序包。

> **Note**
>
> 在 BYOL 导入过程中，将清理违规的 AppX 程序包，并重试 Sysprep。如果映像导入过程持续失败，则意味着需要手动清理 AppX 程序包。

您要导入的 AMI 已启用预留存储空间。Windows 更新后将其禁用，然后重新导入映像。

禁用预留存储空间

1. 打开注册表编辑器，输入 `regedit.exe`。
2. 导航到以下注册表项：`HKLM\Software\Microsoft\Windows\CurrentVersion\ReserveManager`。
3. 将 `ShippedWithReserves` 参数的值从 `1` 更改为 `0`。
4. 将 `ActiveScenario` 的值更改为 `0`。
5. 使用以下命令在 Windows 中禁用预留存储空间：

```
DISM.exe /Online /Set-ReservedStorageState /State:Disabled
```

您要导入的 AMI 已安装防病毒或防间谍软件。将其移除并重新导入映像。

必须卸载防病毒软件。运行 Image Compatibility Checker 以获取要卸载的防病毒软件的详细信息。有关更多信息，请参阅 （可选）在导入之前验证映像。

在 AMI Sysprep 期间，您正在导入的 AMI 发生了未知错误。

无法确定 Sysprep 失败的原因。通过以下网址联系 Amazon 支持：https://aws.amazon.com/support。

使用和管理 WorkSpaces 个人

WorkSpaces Personal 提供永久虚拟桌面，专为需要配置高度个性化的桌面供其专用的用户量身定制，类似于分配给个人的物理台式机。

每个 WorkSpace 都与虚拟私有云 (VPC) 以及用于存储和管理您 WorkSpaces 和用户信息的目录相关联。有关更多信息，请参阅 the section called “VPC 要求”。目录要么由服务管理，要么通过该 WorkSpaces 服务管理，后者提供以下选项：Simple AD Amazon Directory Service、AD Connector 或微软 AD Active Directory（也称为Amazon托管微软 AD）的Amazon目录服务。有关更多信息，请参阅 Amazon Directory Service 管理指南。

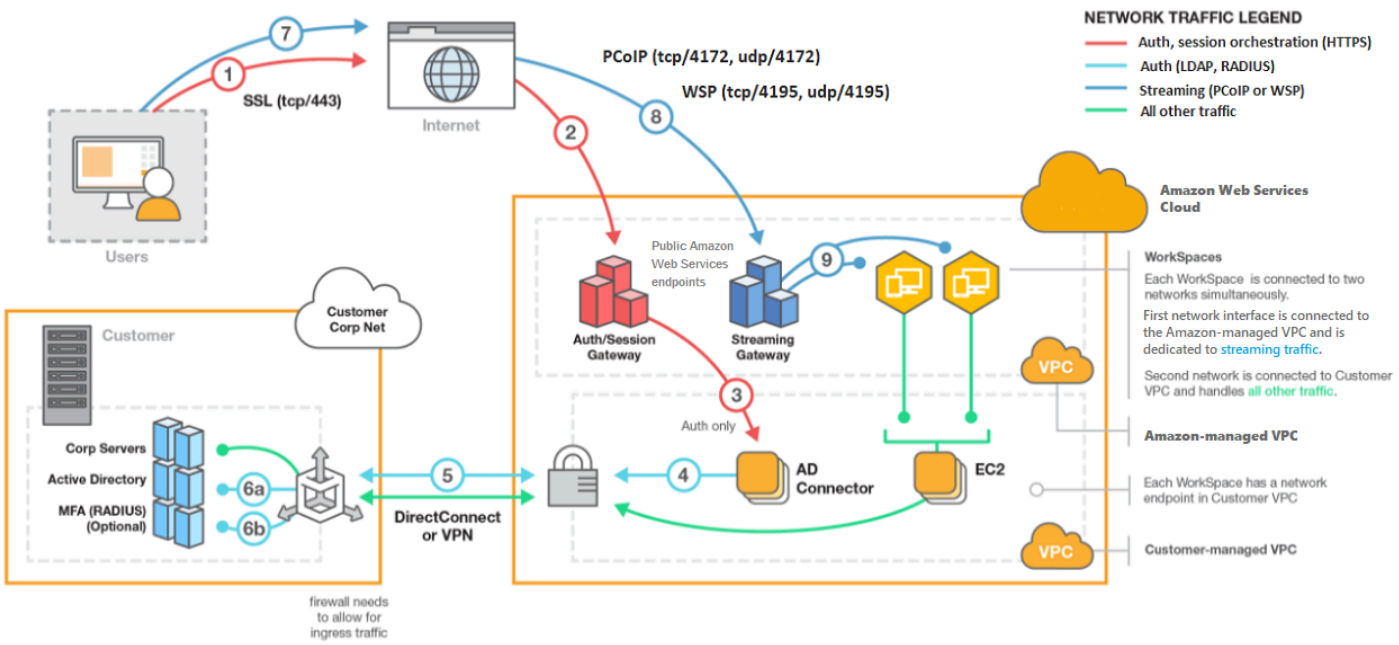
WorkSpaces 使用您的 IAM 身份中心（适用于由亚马逊管理的目录 WorkSpaces）、Simple AD、AD Connector 或微软 AD Amazon 托管目录对用户进行身份验证。用户使用 WorkSpaces 支持的设备上的客户端应用程序或者（对于 Windows WorkSpaces，则使用 Web 浏览器）访问他们的，然后使用自己的目录凭据登录。登录信息被发送到身份验证网关，该网关将流量转发到的 WorkSpace目录。用户通过身份验证后，系统会通过流式传输网关来启动流式传输流量。

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

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

下图显示了使用 AD Connec WorkSpaces tor 的架构。

Amazon WorkSpaces Architectural Diagram



使用 WorkSpaces 个人版创建 WorkSpace 的选项

可以通过多种方法创建 WorkSpace。您可以使用快速设置说明、高级设置说明或从以下选项中进行选择：

- 为 WorkSpaces 个人版创建 Amazon 托管 Microsoft AD 目录
- 为 WorkSpaces 个人创建一个 Simple AD 目录
- 为 WorkSpaces 个人版创建 AD Connector
- 在 Amazon 托管的 Microsoft AD 目录与本地域之间创建 WorkSpaces 个人版的信任关系
- 使用个人版创建专用的 Microsoft Entra ID 目录 WorkSpaces
- 使用 “个 WorkSpaces 人” 创建专用的自定义目录

开始使用 WorkSpaces 个人版

作为首次使用的 WorkSpaces 用户，您可以选择使用快速设置或高级设置来设置您的 WorkSpaces 个人账户。以下教程介绍如何配置基于云的桌面，即WorkSpace使用 WorkSpaces 和Amazon Directory Service。

> **Note**
>
> 要开始使用 WorkSpaces 池，请参阅配置 SAML 2.0 并创建 WorkSpaces 池目录。

WorkSpaces 个人快速设置

在本教程中，你将学习如何使用 WorkSpaces 和预配置虚拟的、基于云的微软 Windows、亚马逊 Linux 2、Ubuntu Linux、Rocky Linux 或红帽企业 Linux 桌面 WorkSpace，也就是所谓的。Amazon Directory Service

本教程使用快速设置选项来启动你的 WorkSpace。只有当您从未启动过时，此选项才可用 WorkSpace。或者，请参阅 为 WorkSpaces 个人版创建目录。

> **Note**
>
> 此快速设置选项和教程不适用于 WorkSpaces 矿池。

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

任务

- 开始前的准备工作
- 快速设置的用途
- 步骤 1：启动 WorkSpace

- 步骤 2：连接到 WorkSpace
- 步骤 3：清除（可选）
- 后续步骤

开始前的准备工作

在您开始之前，确保您满足以下要求：

- 您必须拥有一个Amazon帐户才能创建或管理 WorkSpace。用户不需要Amazon帐户即可连接和使用他们的 WorkSpaces。
- WorkSpaces 并非在每个地区都可用。验证支持的区域，然后为您选择一个区域 WorkSpaces。有关支持的区域的更多信息，请参阅按Amazon地区WorkSpaces 定价。

继续操作之前仔细阅读并理解以下内容也很有帮助：

- 启动时 WorkSpace，必须选择一个 WorkSpace 捆绑包。有关更多信息，请参阅 Amazon WorkSpaces 捆绑包和亚马逊 WorkSpaces 定价。
- 启动时 WorkSpace，必须选择要与捆绑包一起使用的协议（PCoIP 或 DCV）。有关更多信息，请参阅 WorkSpaces 个人协议。
- 启动时 WorkSpace，必须为用户指定个人资料信息，包括用户名和电子邮件地址。用户通过指定密码完成其配置文件。有关 WorkSpaces 和用户的信息存储在目录中。有关更多信息，请参阅 the section called “管理 WorkSpaces 目录”。

快速设置的用途

快速设置将代表您完成以下任务：

- 创建 IAM 角色以允许 WorkSpaces 服务创建弹性网络接口并列出您的 WorkSpaces目录。此角色的名称为 `workspaces_DefaultRole`。
- 创建虚拟私有云 (VPC)。如果您想改用现有 VPC，请确保其满足为 WorkSpaces 个人版配置 VPC中提及的要求，然后按照为 WorkSpaces 个人版创建目录中列出的其中一个教程中的步骤进行操作。选择与要使用的 Active Directory 类型对应的教程。
- 在 VPC 中@@ 设置一个 Simple AD 目录并将其启用 WorkDocs。此 Simple AD 目录用于存储用户和 WorkSpace 信息。通过快速设置Amazon Web Services 账户创建的第一个是您的管理员Amazon Web Services 账户。† 该目录还有一个管理员账户。有关更多信息，请参阅《Amazon Directory Service 管理指南》中的创建的内容。

- 创建指定的Amazon Web Services 账户并将其添加到目录中。
- 创建 WorkSpaces。每个人都会 WorkSpace收到一个公有 IP 地址以提供互联网接入。运行模式是 AlwaysOn。有关更多信息，请参阅 在 WorkSpaces 个人版中管理跑步模式。
- 向指定的用户发送邀请电子邮件。如果您的用户没有收到邀请电子邮件，请参阅发送邀请电子邮件。

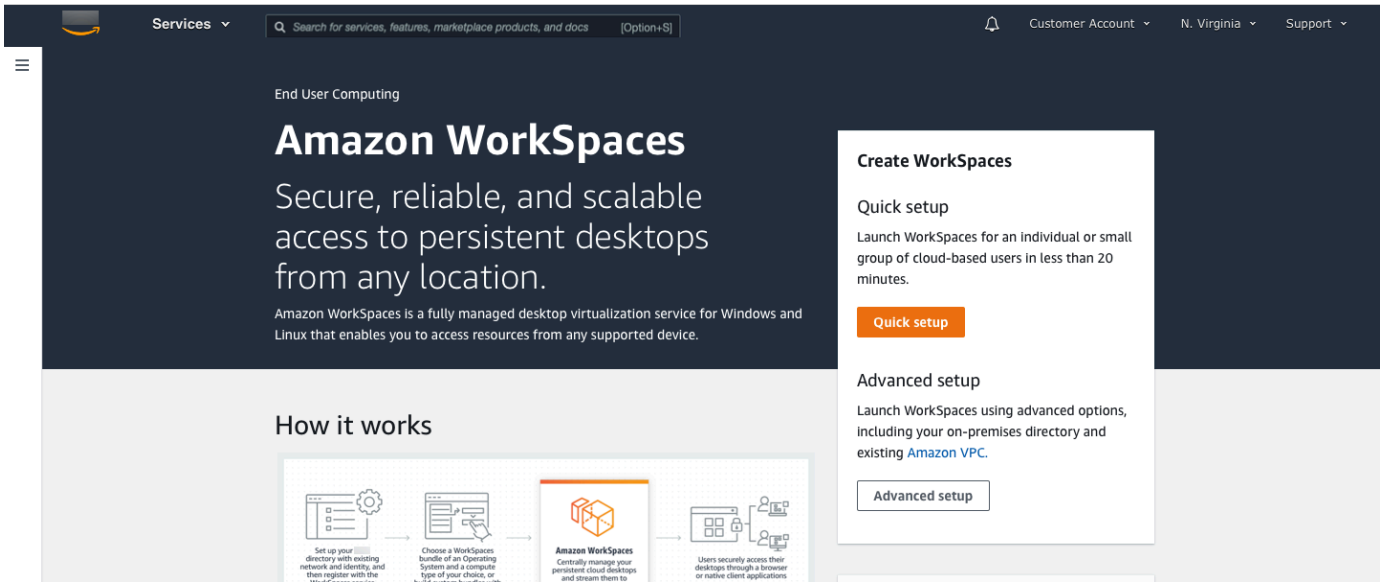
† 通过快速设置Amazon Web Services 账户创建的第一个是您的管理员Amazon Web Services 账户。您无法Amazon Web Services 账户从 WorkSpaces 控制台更新此内容。请勿与任何其他人共享此账户的信息。要邀请其他用户使用 WorkSpaces，请Amazon Web Services 账户为他们创建新的。

步骤 1：启动 WorkSpace

使用快速设置，你可以在几分钟 WorkSpace 内启动你的第一个。

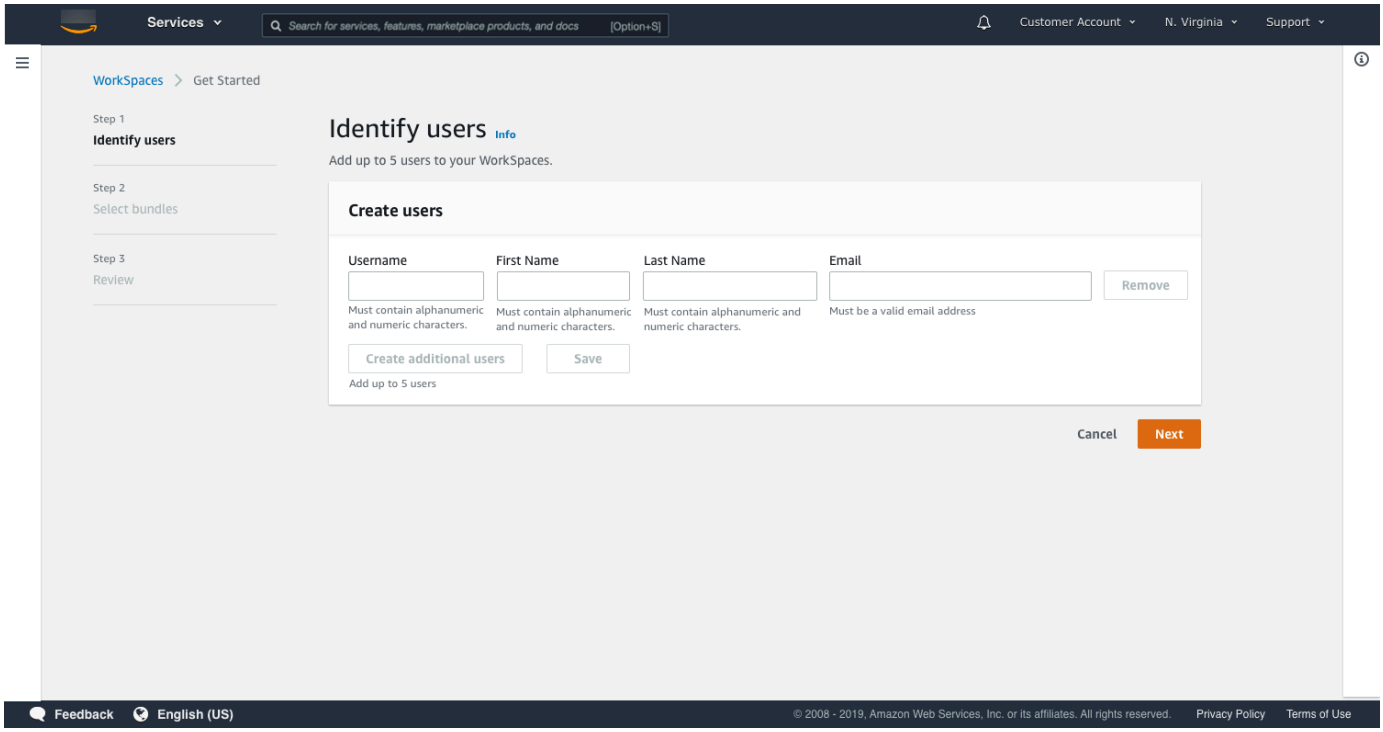
要启动 WorkSpace

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 选择 Quick setup (快速设置)。如果您没有看到此按钮，则可能是您已经在该地区启动了，或者您使用的区域不支持快速设置。 WorkSpace 在这种情况下，请参阅为 WorkSpaces 个人版创建目录。

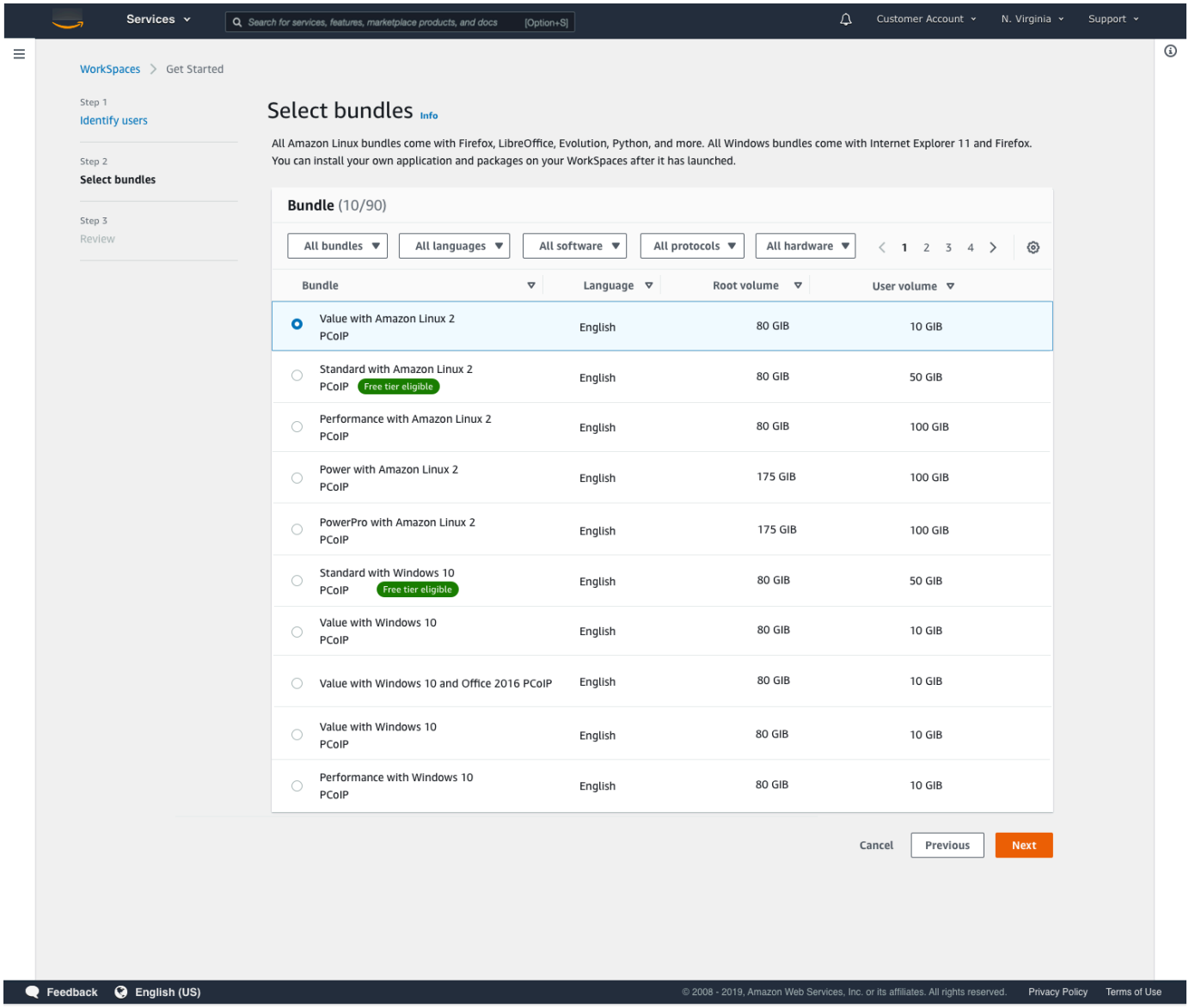


3. 对于识别用户，输入用户名、名字、姓氏和电子邮件。然后选择下一步。

> **Note**
>
> 如果这是您第一次使用 WorkSpaces，我们建议您为自己创建一个用户以进行测试。



4. 对于分发包，请为用户选择具有相应协议（PCoIP 或 DCV）的捆绑包（硬件和软件）。有关亚马逊可用的各种公共捆绑包的更多信息 WorkSpaces，请参阅 Amazon WorkSpaces 捆绑包。



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

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

步骤 2：连接到 WorkSpace

收到邀请电子邮件后，您可以使用自己选择的客户端连接到。 WorkSpace 登录后，客户端会显示 WorkSpace桌面。

要连接到 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，因为您需要用它来连接到您的 WorkSpace。

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

2. 查看 Amazon WorkSpaces 用户指南中的WorkSpaces客户，了解有关每位客户要求的更多信息，然后执行以下任一操作：

   - 根据系统提示，下载一个客户端应用程序或启动 Web Access。
   - 如果没有提示您并且尚未安装客户端应用程序，请打开 并下载其中一个客户端应用程序或启动 Web Access。

   > **Note**
   >
   > 您不能使用网络浏览器（网络访问）连接亚马逊 Linux WorkSpaces。

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

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

步骤 3：清除（可选）

如果您完成了为本教程创建的，则可以将其删除。 WorkSpace 有关更多信息，请参阅 the section called “删除 WorkSpace”。

> **Note**
>
> Simple AD 可供您免费使用 WorkSpaces。如果连续 30 天 WorkSpaces 未在您的 Simple AD 目录中使用，则该目录将自动取消注册以供亚马逊使用 WorkSpaces，并且将根据Amazon Directory Service定价条款向您收取该目录的费用。
> 要删除空目录，请参阅删除 WorkSpaces 个人版目录。如果您删除了 Simple AD 目录，则在想要 WorkSpaces 重新开始使用时可以随时创建一个新目录。

后续步骤

您可以继续自定义刚 WorkSpace 刚创建的。例如，您可以安装软件，然后从中创建自定义软件包 WorkSpace。您还可以为您 WorkSpaces和您的 WorkSpaces 目录执行各种管理任务。有关更多信息，请参阅以下文档。

- 为 WorkSpaces 个人版创建自定义 WorkSpaces 图片和捆绑包
- 管理 WorkSpaces 个人版
- 管理 WorkSpaces 个人版的目录

要创建其他 WorkSpaces，请执行以下任一操作：

- 如果您想继续使用通过快速设置创建的 VPC 和 Simple AD 目录，则可以按照 “ WorkSpace 使用简单 AD 启动教程在 WorkSpaces 个人版中创建 WorkSpace” 部分中的步骤 WorkSpaces 为其他用户进行添加。
- 如果您需要使用其他目录类型或需要使用现有的 Active Directory，请参阅为 WorkSpaces 个人版创建目录中的相应教程。

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

开始使用 WorkSpaces 个人高级设置

在本教程中，您将学习如何使用 WorkSpaces 和配置虚拟的、基于云的微软 Windows、Amazon Linux、Ubuntu Linux 或红帽企业 Linux 桌面桌面（称为 a WorkSpace）。Amazon Directory Service

本教程使用高级设置选项来启动你的 WorkSpace。

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

任务

- 开始前的准备工作
- 使用高级设置启动你的 WorkSpace

开始前的准备工作

在开始之前，请确保您有一个可用于创建或管理的Amazon帐户 WorkSpace。用户无需Amazon帐户即可连接和使用他们的 WorkSpaces.

在继续之前，请仔细阅读并理解以下概念：

- 启动时 WorkSpace，必须选择一个 WorkSpace 捆绑包。有关更多信息，请参阅 Amazon WorkSpaces 捆绑包。
- 启动时 WorkSpace，必须选择要与捆绑包一起使用的协议（PCoIP 或 DCV）。有关更多信息，请参阅 WorkSpaces 个人协议。
- 启动时 WorkSpace，必须为用户指定个人资料信息，包括用户名和电子邮件地址。用户通过指定密码完成其配置文件。有关 WorkSpaces 和用户的信息存储在目录中。有关更多信息，请参阅 the section called “管理 WorkSpaces 目录”。

使用高级设置启动你的 WorkSpace

要使用高级设置来启动你的，请执行 WorkSpace以下操作：

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 选择以下一种目录类型，然后选择下一步：
    - Amazon微软 AD 托管
    - Simple AD
    - AD Connector
3. 输入目录信息。

4. 从两个不同的可用区选择 VPC 中的两个子网。有关更多信息，请参阅配置具有公有子网的 VPC。
5. 查看您的目录信息，然后选择创建目录。

在 WorkSpaces 个人版中创建 WorkSpace

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

创建个人 WorkSpace 之前，需执行以下操作之一来创建目录：

- 创建 Simple AD 目录。
- 创建 Amazon Directory Service for Microsoft Active Directory，也称为 Amazon 托管的 Microsoft AD。
- 使用 Active Directory Connector 连接到现有 Microsoft Active Directory。
- 在 Amazon 托管的 Microsoft AD 目录与本地域之间创建信任关系。
- 创建一个使用 Microsoft Entra ID 作为身份源的专用目录（通过 IAM Identity Center）。目录中的 WorkSpaces 已加入本机 Entra ID，并通过 Microsoft Windows Autopilot 用户驱动模式注册到 Microsoft Intune。

  > **Note**
  > 此类目录目前仅支持 Windows 10 和 11 自带许可个人 WorkSpaces。

- 创建一个使用您所选的身份提供者作为身份源的专用目录（通过 IAM Identity Center）。目录中的 WorkSpaces 已加入本机 Entra ID，并通过 Microsoft Windows Autopilot 用户驱动模式注册到 Microsoft Intune。

  > **Note**
  > 此类目录目前仅支持 Windows 10 和 11 自带许可个人 WorkSpaces。

现在，您已经创建了一个目录，接下来可以创建个人 WorkSpace。

创建个人 WorkSpace

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。

2. 在导航窗格中，选择 WorkSpaces。
3. 依次选择启动 WorkSpaces、个人。
4. 选择创建 WorkSpaces。
5. 在注册（可选）下，您可以选择根据我的使用案例向我推荐选项，以获取有关您要使用的 WorkSpace 类型的建议。如果您知道要使用的个人 WorkSpaces，则可跳过此步骤。
6. 选择下一步。WorkSpaces 会注册您的 AD Connector。
7. 在配置 WorkSpaces 下，输入以下详细信息：
   - 对于捆绑包，从以下捆绑包类型中选择要用于 WorkSpaces 的捆绑包类型。
     - 使用基础 WorkSpaces 捆绑包 - 从下拉列表中选择一个捆绑包。要了解您选择的捆绑包类型的更多信息，请选择捆绑包详细信息。要比较为池提供的捆绑包，请选择比较所有捆绑包。
     - 使用您自己的自定义或 BYOL 捆绑包 - 选择您之前创建的捆绑包。要创建自定义捆绑包，请参阅为 WorkSpaces 个人版创建自定义 WorkSpaces 图片和捆绑包。

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

   - 对于运行模式，从以下选项中进行选择，配置个人 WorkSpace 的即时可用性和付费方式（按月或按小时）：
     - AlwaysOn - 按月支付费用以无限次使用您的 WorkSpaces。该模式最适合将 WorkSpace 作为主桌面全职使用的用户。
     - AutoStop - 按小时计费。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。
   - 对于标签，指定要使用的键对值。键可以是具有特定关联值的一般类别，例如“project”、“owner”或“environment”。
8. 在选择目录下，输入以下详细信息：
   - 选择您创建的目录。要创建目录，请选择创建目录。有关创建个人目录的更多信息，请参阅向 WorkSpaces 个人版注册现有 Amazon Directory Service 目录。
   - 通过执行以下操作，从该目录中选择要预置个人 WorkSpaces 的用户。
     1. 选择创建用户。

   2. 输入用户的用户名、名字、姓氏和电子邮件地址。要添加其他用户，请选择创建其他用户并输入他们的信息。

9. 在自定义（可选）下，您可以为所有用户或特定用户自定义捆绑包、根和用户卷加密以及用户卷。
10. 选择“创建 WorkSpaces”。WorkSpace 的初始状态是“待处理”。创建完毕后，状态会变为“可用”，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。
11. 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。

> **Note**
>
> - 如果使用的是 AD Connector 或信任关系，则不会自动发送这些邀请。
> - 如果用户已存在于 Active Directory 中，则不会发送邀请电子邮件。相反，请务必手动向用户发送邀请电子邮件。有关更多信息，请参阅 发送邀请电子邮件。
> - 在所有区域，邀请电子邮件的文本均为英语（美国）。在以下区域，英语文本前面有第二种语言：
> - 亚太地区（首尔）：韩语
> - 亚太地区（东京）：日语
> - 加拿大（中部）：法语（加拿大）
> - 中国（宁夏）：简体中文

连接到 WorkSpace

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

连接到 WorkSpace

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

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

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

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

后续步骤

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

- 为 WorkSpaces 个人版创建自定义 WorkSpaces 图片和捆绑包
- 管理 WorkSpaces 个人版
- 管理 WorkSpaces 个人版的目录
- 删除 WorkSpaces 个人版中的 WorkSpace

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

WorkSpaces 个人网络协议和访问权限

作为 WorkSpace 管理员，您必须了解如何管理 WorkSpaces 网络和访问权限，首先是协议。

WorkSpaces 个人协议

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

要求

只有满足以下最低要求才支持 DCV WorkSpaces 。

主机代理要求：

- Windows 主机代理版本 2.0.0.312 或更高版本
- Ubuntu 主机代理版本 2.1.0.501 或更高版本
- Amazon Linux 2 主机代理版本 2.0.0.596 或更高版本
- Rocky Linux 主机代理版本 2.1.0.1628 或更高版本
- Red Hat Enterprise Linux 主机代理 2.1.0.1628 或更高版本

客户端要求：

- Windows 原生客户端版本 5.1.0.329 或更高版本
- macOS 原生客户端版本 5.5.0 或更高版本
- Ubuntu 22.04 客户端版本 2024.x 或更高版本
- 亚马逊 WorkSpaces 瘦客户机（有关更多信息，请参阅亚马逊 WorkSpaces 瘦客户机文档）
- Web Access

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

何时使用 DCV

- 如果您需要更高的 loss/latency 容忍度来支持您的最终用户网络条件。例如，有些用户正在全球 WorkSpaces 范围内访问或使用不可靠的网络。
- 如果您需要用户使用智能卡进行身份验证或在会话中使用智能卡。
- 如果您在会话中需要网络摄像头支持功能。
- 如果你需要在支持 Windows Server 2022 WorkSpaces 的捆绑包中使用 Web Access。

- 如果你需要使用 Ubuntu WorkSpaces。
- 如果你需要使用基于 Windows 或 Ubuntu GPU 的捆绑包（Graphics.g4dn 和.g4dn）。 GraphicsPro
- 如果你需要你的用户在会话中使用身份验证 WebAuthn 器（例如 YubiKey 或 Windows Hello）进行身份验证。

何时使用 PCo IP

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

> **Note**
>
> - 目录中可以混合使用 PCo IP 和 DCV WorkSpaces 。
> - 用户可以同时拥有 PCo IP 和 DCV WorkSpace ，前提 WorkSpaces 是两者位于不同的目录中。同一个用户不能在同一个目录 WorkSpace 中拥有 PCo IP 和 DCV。有关为用户创建多个 WorkSpaces 项目的更多信息，请参阅在 WorkSpaces 个人版中为用户创建多个 WorkSpaces。
> - 您可以使用迁移功能在两个协议 WorkSpace 之间 WorkSpaces 迁移，该功能需要重新构建 WorkSpace。有关更多信息，请参阅 以 WorkSpaces 个人 WorkSpace 方式迁移。
> - 如果您 WorkSpace 是使用 PCo IP 捆绑包创建的，则可以修改流媒体协议以在两个协议之间迁移，而无需重建，同时保留根卷。有关更多信息，请参阅修改协议。
> - 为了获得最佳的视频会议体验，我们建议仅使用 Power PowerPro、GeneralPurpose .4xlarge 或 GeneralPurpose .8xlarge 套装。

以下主题提供了有关如何管理 WorkSpaces 个人网络和访问权限的更多详细信息：

为 WorkSpaces 个人版配置 VPC

WorkSpaces 在虚拟私有云 (VPC) 中启动您的 WorkSpaces。

在公有子网中，您可以为您的 WorkSpaces 创建具有两个私有子网的 VPC 以及一个 NAT 网关。或者，您可以为 WorkSpaces 创建具有两个公有子网的 VPC，并将公有 IP 地址或弹性 IP 地址与各个 WorkSpace 关联。

有关 VPC 设计注意事项的更多信息，请参阅 Amazon WorkSpaces 部署中 VPC 和联网的最佳实践与部署 WorkSpaces 的最佳实践 - VPC 设计。

目录

- 要求
- 配置具有私有子网和 NAT 网关的 VPC
- 通过公有子网配置 VPC

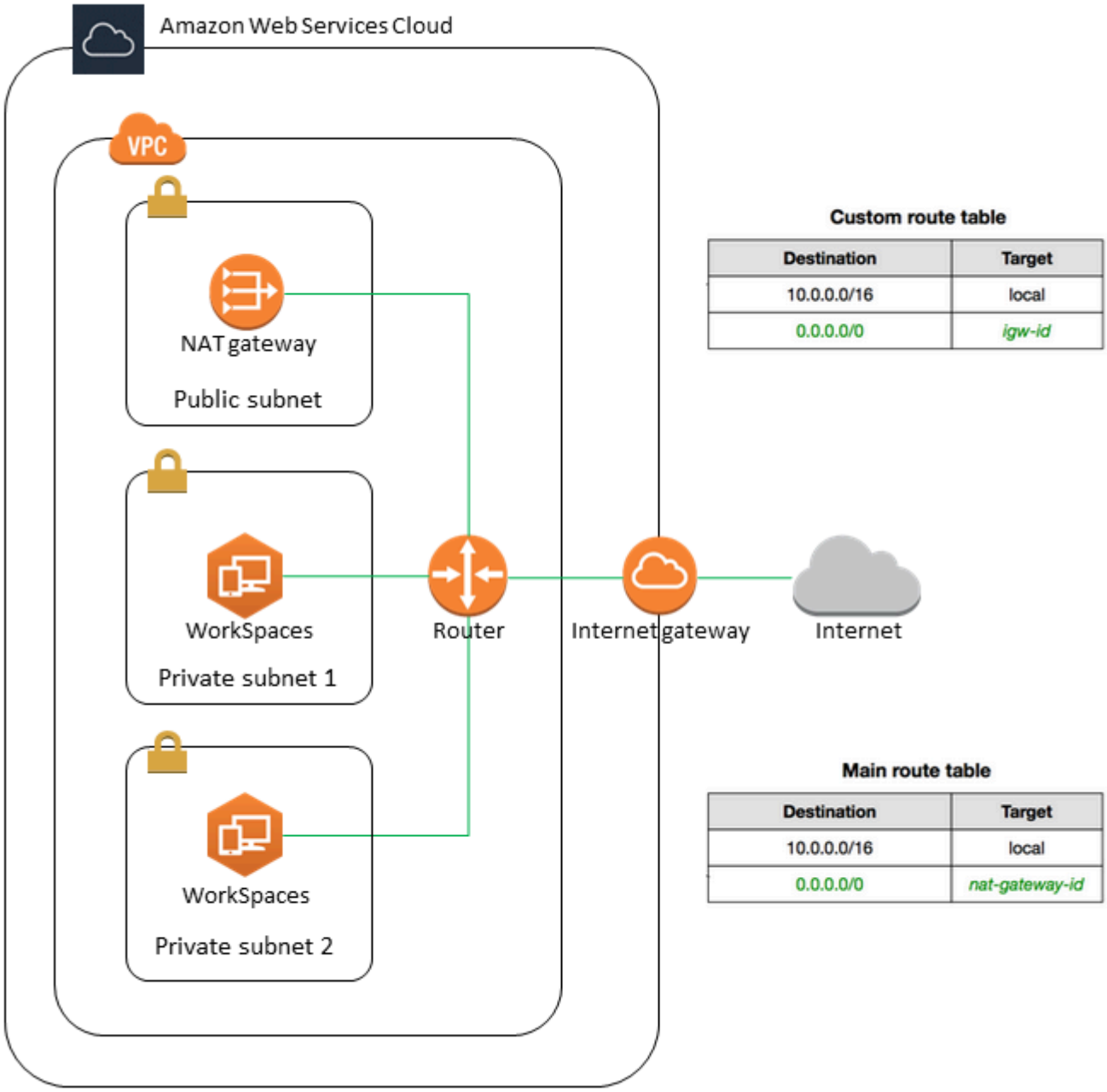
要求

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

> **Note**
>
> Amazon WorkSpaces 可在每个受支持区域的部分可用区中使用。要确定用于 WorkSpaces 的 VPC 子网可以使用哪些可用区，请参阅WorkSpaces 个人版的可用区。

配置具有私有子网和 NAT 网关的 VPC

如果您使用 Amazon Directory Service 来创建 Amazon 托管的 Microsoft AD 或 Simple AD，建议您使用一个公有子网和两个私有子网来配置 VPC。配置您的目录以在私有子网中启动 WorkSpace。要向私有子网中的 WorkSpace 提供互联网访问，请在公有子网中配置一个 NAT 网关。



创建具有一个公有子网和两个私有子网的 VPC

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

5. 若要配置子网，请执行以下操作：
   a. 对于 Number of Availability Zones（可用区域数量），根据您的需求选择 1 或 2。
   b. 展开自定义 AZ，然后选择您的可用区。否则，Amazon 将为您选择可用区。要做出适当的选择，请参阅 WorkSpaces 个人版的可用区。
   c. 对于 Number of public subnets（公有子网数量），确保每个可用区有一个公有子网。
   d. 对于私有子网数量，确保每个可用区至少有一个私有子网。
   e. 为每个子网输入一个 CIDR 块。有关更多信息，请参阅《Amazon VPC 用户指南》中的子网大小调整。
6. 对于 NAT 网关，请选择每个 AZ 1 个。
7. 选择创建 VPC。

IPv6 CIDR 块

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

要解决此问题，您可以在启动 Graphics 服务包之前，在 WorkSpaces 子网上暂时禁用自动分配 IPv6 地址设置，并在启动 Graphics 服务包之后重新启用此设置（如果需要），这样所有其他服务包就可以接收所需的 IP 地址。

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

通过公有子网配置 VPC

如果您愿意，您可以创建具有两个公有子网的 VPC。要为公有子网中的 WorkSpace 提供互联网访问，请配置目录以便手动或自动向每个 WorkSpace 分配一个弹性 IP 地址。

任务

- 第 1 步：创建 VPC
- 步骤 2：将公有 IP 地址分配到您的 WorkSpaces

第 1 步：创建 VPC

如下所示创建具有一个公有子网的 VPC。

创建 VPC

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

IPv6 CIDR 块

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

要解决此问题，您可以在启动 Graphics 服务包之前，在 WorkSpaces 子网上暂时禁用自动分配 IPv6 地址设置，并在启动 Graphics 服务包之后重新启用此设置（如果需要），这样所有其他服务包就可以接收所需的 IP 地址。

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

步骤 2：将公有 IP 地址分配到您的 WorkSpaces

您可以自动或手动将公有 IP 地址分配到 WorkSpaces。要使用自动分配，请参阅the section called “配置自动公有 IP 地址”。要手动分配公有 IP 地址，请使用以下过程。

手动为 WorkSpace 分配公有 IP 地址

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。

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

为 WorkSpaces 个人版配置 Amazon Global Accelerator（AGA）

您可以在 WorkSpaces 目录级别启用 Amazon Global Accelerator（AGA），也可以为运行 DCV 协议的单个 WorkSpaces 启用。启用后，该服务会自动将流式传输流量路由到最近的 Amazon 边缘站点和 Amazon 全球网络，而不会造成拥堵且可实现冗余。这有助于提供响应速度更快、更稳定的流式传输体验。WorkSpaces 服务负责全面管理 AGA 的使用情况，并且受出站数据量限制的约束。

目录

- 要求
- 限制
- 出站数据限制
- 为 WorkSpaces 目录启用 AGA
- 为单个 WorkSpaces 启用 AGA

要求

- WorkSpaces 使用一系列公有 IPv4 地址作为专用的 Amazon Global Accelerator（AGA）端点。确保为通过 AGA 访问 WorkSpaces 的设备配置防火墙策略。如果 AGA 端点被防火墙阻

止，WorkSpaces 的流式传输流量将不会通过 AGA 进行路由。有关每个 Amazon 区域中 AGA 端点 IP 范围的更多信息，请参阅 DCV 网关服务器。

- 要通过 AGA 访问 WorkSpaces，用户必须使用 WorkSpaces 客户端版本 5.23 或更高版本。

限制

- 您只能为 DCV WorkSpaces 启用 AGA。如果您在 WorkSpaces 目录级别启用 AGA，则它将仅应用于目录中的 DCV WorkSpaces。
- 您无法为同时启用 FIPS 和 IP 访问控制组的目录（或目录中的 WorkSpaces）启用 AGA。在为目录启用 AGA 之前，必须禁用 FIPS 或 IP 访问控制组。

出站数据限制

以下是 WorkSpaces 捆绑包适用的数据量限制。

- Value、Standard 和 Performance 捆绑包：包括每位用户每月 20 GB 的 AGA 出站数据。
- Power、PowerPro 和 Graphics 捆绑包：包括每位用户每月 50 GB 的 AGA 出站数据。

这些出站数据限制旨在满足用户从其 WorkSpaces 进行流式传输的数据使用需求。超出限制后，WorkSpaces 服务可能会限制 AGA 使用，并根据具体情况将 WorkSpaces 流量从 AGA 路由出去。

为 WorkSpaces 目录启用 AGA

您可以在目录级别配置 AGA 设置。这些设置将应用于目录中的所有 DCV WorkSpaces，除非被单个 WorkSpaces 的设置覆盖。

为目录启用 AGA

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。
3. 在目录 ID 列下，选择要为其配置 AGA 设置的目录的目录 ID。
4. 在目录详细信息页面上，向下滚动到 Amazon Global Accelerator（AGA）配置部分，然后选择编辑。
5. 选择启用 AGA（自动）。

6. 默认情况下，系统会选中始终使用 TCP 和 AGA。如果您取消选中该选项，您的 WorkSpaces 客户端会根据客户端上的 DCV 流式传输协议设置来确定 AGA 是使用 TCP 还是 UDP。
7. 选择 Save。

为 WorkSpaces 目录启用 AGA 后，目录中的 DCV WorkSpaces 会从下一个会话开始使用 AGA 进行流式传输。无需重新启动。

为单个 WorkSpaces 启用 AGA

您可以为单个 WorkSpaces 配置 AGA 设置，这些设置会覆盖从与该 WorkSpaces 关联的目录中继承的设置。

为单个 WorkSpaces 启用 AGA

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，依次选择 WorkSpaces、个人版。
3. 在工作空间 ID 列下，选择要为其配置 AGA 设置的工作空间的工作空间 ID。
4. 在 WorkSpaces 详细信息页面上，向下滚动到 Amazon Global Accelerator（AGA）配置部分，然后选择编辑。
5. 选择手动覆盖此工作空间的 AGA 配置。
6. 选择启用 AGA（自动）。
7. 默认情况下，系统会选中始终使用 TCP 和 AGA。如果您取消选中该选项，您的 WorkSpaces 客户端会根据客户端上的 DCV 流式传输协议设置来确定 AGA 是使用 TCP 还是 UDP。
8. 选择 Save。

WorkSpaces 个人版的可用区

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

可用区由区域代码后跟一个字母标识符表示；例如，`us-east-1a`。为确保资源分配到区域的各可用区，我们将可用区独立映射到每个 Amazon 账户的名称。例如，您的 `us-east-1a` 账户的可用区 Amazon 可能与另一 `us-east-1a` 账户的 Amazon 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 Amazon 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 仅可在每个受支持区域的部分可用区中使用。下表列出了每个区域中您可以使用的可用区 ID 列表。要查看您账户中可用区 ID 到可用区的映射，请参阅《Amazon RAM 用户指南》中的您的资源的 AZ ID。

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

区域名称	区域代码	支持的 AZ ID
欧洲（巴黎）	eu-west-3	euw3-az1, euw3-az2, euw3-az3
南美洲（圣保罗）	sa-east-1	sae1-az1, sae1-az3
非洲（开普敦）	af-south-1	afs1-az1, afs1-az2, afs1-az3
以色列（特拉维夫）	il-central-1	ilc1-az1, ilc1-az2, ilc1-az3
Amazon GovCloud（美国西部）	us-gov-west-1	usgw1-az1 ，usgw1-az2 ，usgw1-az3
Amazon GovCloud（美国东部）	us-gov-east-1	usge1-az1 ，usge1-az2 ，usge1-az3

有关可用区和 AZ ID 的更多信息，请参阅《Amazon EC2 用户指南》中的区域、可用区和本地区域。

WorkSpaces 个人的 IP 地址和端口要求

要连接到您的 WorkSpaces，您的 WorkSpaces 客户端所连接的网络必须为各种Amazon服务的 IP 地址范围（按子集分组）开放某些端口。这些地址范围因Amazon地区而异。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 Amazon IP 地址范围的更多信息，请参阅中的 AmazonIP 地址范围Amazon Web Services 一般参考。

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

用于客户端应用程序的端口

WorkSpaces 客户端应用程序需要通过以下端口进行出站访问：

端口 53 (UDP)

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

端口 443 (UDP 和 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：

- 所在区域中的AMAZON WorkSpace 子集。

端口 4172 (UDP 和 TCP)

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

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

端口 4195（UDP 和 TCP）

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

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

> **Note**
>
> - 如果防火墙使用有状态筛选功能，则会自动打开临时（也称为动态）端口，以便允许返回通信。如果您的防火墙使用无状态筛选功能，则需要明确打开临时端口，以便允许返回通信。根据您的配置，需要打开的临时端口范围有所不同。
> - UDP 流量不支持代理服务器功能。如果您选择使用代理服务器，则客户端应用程序对 Amazon WorkSpaces 服务进行的 API 调用也会被代理。API 调用和桌面流量都应通过同一个代理服务器。
> - 为了获得最佳性能， WorkSpaces 客户端应用程序首先尝试使用 UDP (QUIC) 进行流式传输。如果客户端网络仅允许 TCP，则将使用 TCP。 WorkSpaces Web 客户端将通过 TCP

端口 4195 或 443 进行连接。如果端口 4195 被屏蔽，则客户端将仅尝试通过端口 443 进行连接。

要添加到允许列表的域和 IP 地址

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

要添加到允许列表的域和 IP 地址

类别	域或 IP 地址
客户端自动更新	• 在中国（宁夏）区域： https://workspaces-client-updates.s3.cn-northwest-1.amazonaws.com.cn
连接检查	https://connectivity.amazonworkspaces.awsapps.cn
客户端指标（适用于 3.0 及以上的 WorkSpaces 客户端应用程序）	域名 (IPv4): • 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

类别	域或 IP 地址
	• 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.eu-west-3.amazonaws.com • https://skylight-client-ds.sa-east-1.amazonaws.com • https://skylight-client-ds.af-south-1.amazonaws.com • https://skylight-client-ds.il-central-1.amazonaws.com • 在 AmazonGovCloud （美国西部）区域： https://skylight-client-ds.us-gov-west-1.amazonaws.com • 在 AmazonGovCloud （美国东部）区域： https://skylight-client-ds.us-gov-east-1.amazonaws.com • 在 AmazonGovCloud （美国西部）区域： https://skylight-client-ds.us-gov-west-1.amazonaws.com • 在 AmazonGovCloud （美国东部）区域： https://skylight-client-ds.us-gov-east-1.amazonaws.com

类别	域或 IP 地址
	• 在中国（宁夏）区域： https://skylight-client-ds.cn-northwest-1.amazonaws.com.cn 域名 (IPv6): • https://skylight-client-ds.eu-west-2.api.aws • https://skylight-client-ds.eu-west-1.api.aws • https://skylight-client-ds.us-east-1.api.aws • https://skylight-client-ds.ap-southeast-1.api.aws • https://skylight-client-ds.sa-east-1.api.aws • https://skylight-client-ds.ap-northeast-1.api.aws • https://skylight-client-ds.us-west-2.api.aws • https://skylight-client-ds.ap-southeast-2.api.aws • https://skylight-client-ds.ap-south-1.api.aws • https:// skylight-client-ds .af-south-1.api.aw • https://skylight-client-ds.eu-central-1.api.aws • https://skylight-client-ds.ap-northeast-2.api.aws • https:// skylight-client-ds .il-central-1.api.aw • https://skylight-client-ds.ca-central-1.api.aws • https://skylight-client-ds。 us-gov-east-1.api.aws • https://skylight-client-ds。 us-gov-west-1.api.aws

类别	域或 IP 地址
动态消息服务（适用于 3.0 以上的 WorkSpaces 客户端应用程序）	域名 (IPv4): • https://ws-client-service.us-east-1.amazonaws.com • https://ws-client-service.us-west-2.amazonaws.com • 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.eu-west-3.amazonaws.com • https://ws-client-service.sa-east-1.amazonaws.com • https://ws-client-service.af-south-1.amazonaws.com • https://ws-client-service.il-central-1.amazonaws.com

类别	域或 IP 地址
	• 在 AmazonGovCloud （美国西部）区域： https://ws-client-service.us-gov-west-1.amazonaws.com • 在 AmazonGovCloud （美国东部）区域： https://ws-client-service.us-gov-east-1.amazonaws.com • 在中国（宁夏）区域： https://ws-client-service.cn-northwest-1.amazonaws.com.cn 域名 (IPv6): • https://ws-client-service.eu-west-2.api.aws • https://ws-client-service.eu-west-1.api.aws • https://ws-client-service.us-east-1.amazonaws.com • https://ws-client-service.ap-southeast-1.api.aws • https://ws-client-service.sa-east-1.api.aws • https://ws-client-service.ap-northeast-1.api.aws • https://ws-client-service.us-west-2.api.aws • https://ws-client-service.ap-southeast-2.api.aws • https://ws-client-service.ap-south-1.api.aws • https:// ws-client-service .af-south-1.api.aw • https://ws-client-service.eu-central-1.api.aws • https://ws-client-service.ap-northeast-2.api.aws

类别	域或 IP 地址
	• https:// ws-client-service .il-central-1.api.aw • https://ws-client-service.ca-central-1.api.aws • https://ws-client-service。 us-gov-east-1.api.aws • https://ws-client-service。 us-gov-west-1.api.aws
目录设置	在中国（宁夏）区域： • 客户目录设置： https://workspaces-clients-properties.s3.cn-northwest-1.amazonaws.com.cn • 客户目录级别联合品牌的登录页面图形： https://workspaces-client-assets.s3.cn-northwest-1.amazonaws.com.cn • 用于设计登录页面的 CSS 文件： https://workspaces-clients-css.s3.cn-northwest-1.amazonaws.com.cn/workspaces_v3.css
运行状况检查 (DRP) 服务器	运行状况检查服务器

类别	域或 IP 地址
用户登录页面	• https://af-south-1.signin.aws • https://af-south-1.signin.aws.amazon.com • https://af-south-1.sso.signin.aws • https://af-south-1.apps.signin.aws • https://ap-south-1.signin.aws • https://ap-south-1.signin.aws.amazon.com • https://ap-south-1.sso.signin.aws • https://ap-south-1.apps.signin.aws • https://ap-southeast-1.signin.aws • https://ap-southeast-1.signin.aws.amazon.com • https://ap-southeast-1.sso.signin.aws • https://ap-southeast-1.apps.signin.aws • https://ap-southeast-2.signin.aws • https://ap-southeast-2.signin.aws.amazon.com • https://ap-southeast-2.sso.signin.aws • https://ap-southeast-2.apps.signin.aws • https://ap-northeast-1.signin.aws • https://ap-northeast-1.signin.aws.amazon.com • https://ap-northeast-1.sso.signin.aws • https://ap-northeast-1.apps.signin.aws • https://ap-northeast-2.signin.aws • https://ap-northeast-2.signin.aws.amazon.com • https://ap-northeast-2.sso.signin.aws • https://ap-northeast-2.apps.signin.aws • https://ca-central-1.signin.aws

类别	域或 IP 地址
	• https://ca-central-1.signin.aws.amazon.com • https://ca-central-1.sso.signin.aws • https://ca-central-1.apps.signin.aws • https://eu-central-1.signin.aws • https://eu-central-1.signin.aws.amazon.com • https://eu-central-1.sso.signin.aws • https://eu-central-1.apps.signin.aws • https://eu-west-1.signin.aws • https://eu-west-1.signin.aws.amazon.com • https://eu-west-1.sso.signin.aws • https://eu-west-1.apps.signin.aws • https://eu-west-2.signin.aws • https://eu-west-2.signin.aws.amazon.com • https://eu-west-2.sso.signin.aws • https://eu-west-2.apps.signin.aws • https://eu-west-3.signin.aws • https://eu-west-3.signin.aws.amazon.com • https://eu-west-3.sso.signin.aws • https://eu-west-3.apps.signin.aws • https://il-central-1.signin.aws • https://il-central-1.signin.aws.amazon.com • https://il-central-1.sso.signin.aws • https://il-central-1.apps.signin.aws • https://sa-east-1.signin.aws • https://sa-east-1.signin.aws.amazon.com • https://sa-east-1.sso.signin.aws • https://sa-east-1.apps.signin.aws • https://us-east-1.signin.aws • https://us-east-1.signin.aws.amazon.com

类别	域或 IP 地址
	• https://us-east-1.sso.signin.aws • https://us-east-1.apps.signin.aws • https://us-west-2.signin.aws • https://us-west-2.signin.aws.amazon.com • https://us-west-2.sso.signin.aws • https://us-west-2.apps.signin.aws • https://us-gov-east-1.signin-fips.amazonaws-us-gov.com • https://us-gov-east-1.sso.signin-fips.aws-us-gov.com • https://us-gov-east-1.apps.signin-fips.aws-us-gov.com • https://us-gov-west-1.signin.amazonaws-us-gov.com • https://us-gov-west-1.sso.signin.aws-us-gov.com • https://us-gov-west-1.apps.signin.aws-us-gov.com https://*directory_id* .awsapps.com/ Note directory id 是客户的域。 在 AmazonGovCloud （美国西部）和 AmazonGovCloud （美国东部）区域： https://login.us-gov-home.awsapps.com/directory/*directory id*/

类别	域或 IP 地址
	Note directory id 是客户的域。
WS 代理	
WorkSpaces API 端点	• 中国（宁夏）区域 https:// workspaces.cn-northwest-1.amazonaws.com：.cn

类别	域或 IP 地址
WorkSpaces SAML 单点登录 (SSO) 的终端节点	域: • https://euc-sso-sm.us-east-1.amazonaws.com/v1/报告心跳 • https://euc-sso-sm-fips.us-east-1.amazonaws.com/v1/报告心跳 • https://euc-sso-sm.us-west-2.amazonaws.com/v1/报告心跳 • https://euc-sso-sm-fips.us-west-2.amazonaws.com/v1/报告心跳 • https://euc-sso-sm.ap-south-1.amazonaws.com/v1/报告心跳 • https://euc-sso-sm.ap-northeast-2.amazonaws.com/v1/报告心跳 • https://euc-sso-sm.ap-southeast-1.amazonaws.com/v1/报告心跳 • https://euc-sso-sm.ap-southeast-2.amazonaws.com/v1/报告心跳 • https://euc-sso-sm.ap-northeast-1.amazonaws.com/v1/报告心跳 • https://euc-sso-sm.eu-central-1.amazonaws.com/v1/报告心跳 • https://euc-sso-sm.eu-west-2.amazonaws.com/v1/报告心跳 • https://euc-sso-sm.eu-west-3.amazonaws.com/v1/报告心跳 • https://euc-sso-sm.af-south-1.amazonaws.com/v1/报告心跳 • https://euc-sso-sm.il-central-1.amazonaws.com/v1/报告心跳 • https://euc-sso-sm.us-gov-west-1.amazonaws.com/v1/报告心跳

类别	域或 IP 地址
	• https://euc-sso-sm-fips.us-gov-west-1.amazonaws.com/v1/报告心跳 • https://euc-sso-sm.us-gov-east-1.amazonaws.com/v1/报告心跳 • https://euc-sso-sm-fips.us-gov-east-1.amazonaws.com/v1/报告心跳

要添加到 IP 允许列表中的域和 PCo IP 地址

类别	域或 IP 地址
PCoIP 会话网关 (PSG)	PCoIP 网关服务器
会话代理 (PCM)	• 中国（宁夏）区域 https://skylight-cm.cn-northwest-1.amazonaws.com：.cn

要添加到 DCV 允许列表的域和 IP 地址

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

运行状况检查服务器

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

Region	运行状况检查主机名	IP 地址
中国（宁夏）	drp-zhy.amazonworkspaces.com	52.82.90.186 52.83.43.32

Region	运行状况检查主机名	IP 地址
		52.83.110.158 52.83.248.61

PCoIP 网关服务器

WorkSpaces 使用 PCo IP 通过端口 4172 将桌面会话流式传输到客户端。对于其 PCo IP 网关服务器， WorkSpaces 使用少量的 Amazon EC2 公共 IPv6 地址 IPv4 和地址。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，当支持并且可以访问网关 IPv6 时，WorkSpaces 客户端会优先考虑 IPv6 连接。如果 IPv6 不可用，则会回退到 IPv4。

Region	区域代码	公有 IP 地址范围
中国（宁夏）		52.83.58.0 - 52.83.58.255 69.235.162.0 - 69.235.162.255

DCV 网关服务器

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

> **Note**
>
> 对于非 BYOL WorkSpaces 池，无法保证 IP 地址范围。您必须将 DCV 网关域名列入许可名单。有关更多信息，请参阅 DCV 网关域名。

WorkSpaces 为其 DCV 网关服务器使用少量的 Amazon EC2 公共 IPv6 地址 IPv4 和地址。这使您能够为访问 WorkSpaces的设备设置更精细的防火墙策略。 WorkSpaces 为专用Amazon全球加速器 (AGA) 端点使用单独的公有 IPv4 地址范围。如果您计划为自己启用 AGA，请务必将防火墙策略配置为

允许名单 IP 范围。 WorkSpaces请注意，当支持并且可以访问网关 IPv6 时， WorkSpaces 客户端会优先考虑 IPv6 连接。如果 IPv6 不可用，则会回退到 IPv4。

如果您使用 AGA + IPv6，则需要将该范围中的 IPv6 CIDR 范围列入许可名单。GLOBALACCELERATOR有关更多信息，请参阅《Amazon Global Accelerator 开发人员指南》中的 Global Accelerator 边缘服务器的位置和 IP 地址范围。

Region	区域代码	公有 IP 地址范围
中国（宁夏）		140.65.96.0/22

DCV 网关域名

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

Region	域：
中国（宁夏）	DCV 不支持此区域。

网络接口

每个 WorkSpace 都有以下网络接口：

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

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

> **Warning**
>
> 请勿修改或删除连接到的任何网络接口 WorkSpace。这样做可能会导致无法 WorkSpace 访问或无法访问互联网。例如，如果您在目录级别启用了弹性 IP 地址的自动分配，则会在启动弹

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

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。

Region	IP 地址范围
中国（宁夏）	198.19.0.0/16

管理接口端口

必须在所有人的管理网络接口上打开以下端口 WorkSpaces：

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

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

  如果你通过其中一个 WorkSpaces 公共捆绑包使用 Office，则用于激活 Office 的 Microsoft KMS 的 IP 地址会有所不同。要确定该 IP 地址，请找到的管理接口的 IP 地址 WorkSpace，然后将最后两个二进制八位数替换为。`64.250`例如，如果管理接口的 IP 地址为 192.168.3.5，则用于激活 Office 的 Microsoft KMS 的 IP 地址为 192.168.64.250。
- 当 WorkSpace 主机配置为使用代理服务器 WorkSpaces 时，DCV 的出站 TCP 到 IP 地址 127.0.0.2。
- 源自环回地址 127.0.01 的通信。

在正常情况下，该 WorkSpaces 服务会为您 WorkSpaces配置这些端口。如果安装了任何安全软件或防火墙软件 WorkSpace 来阻塞这些端口中的任何一个，则 WorkSpace 可能无法正常运行或无法访问。

主接口端口

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

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

- TCP/UDP 389 - LDAP
- TCP/UDP 445 - SMB
- TCP/UDP 636 - LDAPS (LDAP over TLS/SSL)
- TCP 1024-65535 - RPC 动态端口
- TTCP 3268-3269 - 全局目录

如果安装了任何安全软件或防火墙软件 WorkSpace 来阻塞这些端口中的任何一个，则 WorkSpace 可能无法正常运行或无法访问。

WorkSpaces 个人版客户端网络要求

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

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

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

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

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

受到影响。如果 RTT 介于 200 毫秒和 375 毫秒之间，则性能会降低。如果 RTT 超过 375 毫秒，WorkSpaces 客户端连接将终止。

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

要查看从您所在位置到各个 Amazon 区域的 RTT，请使用 Amazon WorkSpaces 连接运行状况检查。

- 要将网络摄像头与 DCV 配合使用，建议最低上传带宽为每秒 1.7 兆比特。
- 如果用户通过虚拟专用网络 (VPN) 访问 WorkSpace，则连接必须支持至少 1200 字节的最大传输单位 (MTU)。

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

- 客户端需要通过 HTTPS 访问由该服务和 Amazon Simple Storage Service (Amazon S3) 托管的 WorkSpaces 资源。客户端不支持应用程序级别的代理重定向。HTTPS 访问是必需的，以便用户可以成功完成注册并访问自己的 WorkSpace。
- 要允许从 PCoIP 零客户端设备进行访问，您必须使用适用于 WorkSpaces 的 PCoIP 协议包。您还必须在 Teradici 中启用网络时间协议 (NTP)。有关更多信息，请参阅 为 WorkSpaces 个人版设置 PCoIP 零客户端。

您可以按照以下说明验证客户端设备是否符合网络要求。

验证 3.0+ 客户端的网络要求

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

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

客户端应用程序将会测试网络连接、端口以及往返时间，并报告这些测试的结果。

3. 关闭 Network (网络) 对话框以返回到登录页面。

验证 1.0+ 和 2.0+ 客户端的网络要求

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

将 WorkSpaces 个人版访问限定于受信任设备

默认情况下，用户可以从任何连接到互联网的受支持设备访问自己的 WorkSpace。如果您的公司仅限受信任设备（也称为托管设备）访问公司数据，则您可以通过有效的证书将 WorkSpace 访问限定为受信任设备。

> **Note**
>
> 目前，只有通过 Amazon Directory Service（包括 Simple AD、AD Connector 和 Amazon Managed Microsoft AD 目录）来管理 WorkSpaces 个人版目录时，此功能才可用。

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 WorkSpace 客户端应用程序无法验证设备是否可信，则会阻止从此设备进行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，然后客户端会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。

支持的客户端

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

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

> **Note**
>
> 在为特定客户端启用访问权限时，请确保阻止其他不需要的设备类型的访问权限。有关此操作的详细信息，请参阅下文的步骤 3.7。

第 1 步：创建证书

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

要求

- 根证书必须是 Base64 编码的证书文件 (采用 CRT、CERT 或 PEM 格式)。
- 根证书必须满足以下正则表达式模式，这意味着除最后一行外，每行编码的长度必须正好为 64 个字符：`-{5}BEGIN CERTIFICATE-{5}\u000D?\u000A([A-Za-z0-9/+]{64} \u000D?\u000A)*[A-Za-z0-9/+]{1,64}={0,2}\u000D?\u000A-{5}END CERTIFICATE-{5}(\u000D?\u000A)`。
- 设备证书必须包含公用名。

- 设备证书必须包含以下扩展：`Key Usage: Digital Signature` 和 `Enhanced Key Usage: Client Authentication`。
- 从设备证书到受信任根证书颁发机构的证书链中的所有证书都必须安装在客户端设备上。
- 证书链支持的最大长度为 4。
- WorkSpaces 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。建议使用带 RSA 的 SHA256、带 ECDSA 的 SHA256、带 ECDSA 的 SHA381 或带 ECDSA 的 SHA512。
- 对于 macOS，如果设备证书位于系统密钥链中，建议您授权 WorkSpaces 客户端应用程序访问此类证书。否则，用户必须在登录或重新连接时，输入密钥链凭证。

第 2 步：为受信任设备部署客户端证书

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

WorkSpaces 客户端应用程序按如下方式搜索证书：

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

第 3 步：配置限制

在受信任设备上部署客户端证书后，您可以在目录级别启用受限访问权限。这需要 WorkSpaces 客户端应用程序验证设备上的证书，然后再允许用户登录到 WorkSpace。

配置限制

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。
3. 选择目录，然后选择 Actions、Update Details。

4. 展开 Access Control Options。
5. 在针对每种设备类型，指定哪些设备可以访问 WorkSpaces 下，选择可信设备。
6. 最多导入 2 个根证书。对于每个根证书，请执行以下操作：
   a. 选择 Import（导入）。
   b. 将证书文本复制到表单中。
   c. 选择 Import（导入）。
7. 指定其他类型的设备是否可以访问 WorkSpaces。
   a. 向下滚动到 Other Platforms (其他平台) 部分。默认情况下，禁用 WorkSpaces Linux 客户端，用户可以从其 iOS 设备、Android 设备、Web Access、 和 PCoIP 零客户端设备访问其 WorkSpaces。
   b. 选择要启用的设备类型并清除要禁用的设备类型。
   c. 要阻止来自所有选定设备类型的访问，请选择 Block。
8. 选择更新并退出。

将 SAML 2.0 与 WorkSpaces 个人版集成

> **Note**
>
> 只有通过 Amazon Directory Service（包括 Simple AD、AD Connector 和 Amazon Managed Microsoft AD 目录）来管理 WorkSpaces 个人版目录时，SAML 2.0 才可用。该功能不适用于由 Amazon WorkSpaces 管理的目录，这些目录通常使用 IAM Identity Center 进行用户身份验证，而不是 SAML 2.0 联合身份验证。

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

身份验证工作流

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

- 当流由 IdP 启动时。例如，当用户使用 Web 浏览器在 IdP 用户门户中选择应用程序时。

- 当流由 WorkSpaces 客户端启动时。例如，当用户打开客户端应用程序并登录时。

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

由身份提供者 (IdP) 启动的客户端应用程序流

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

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

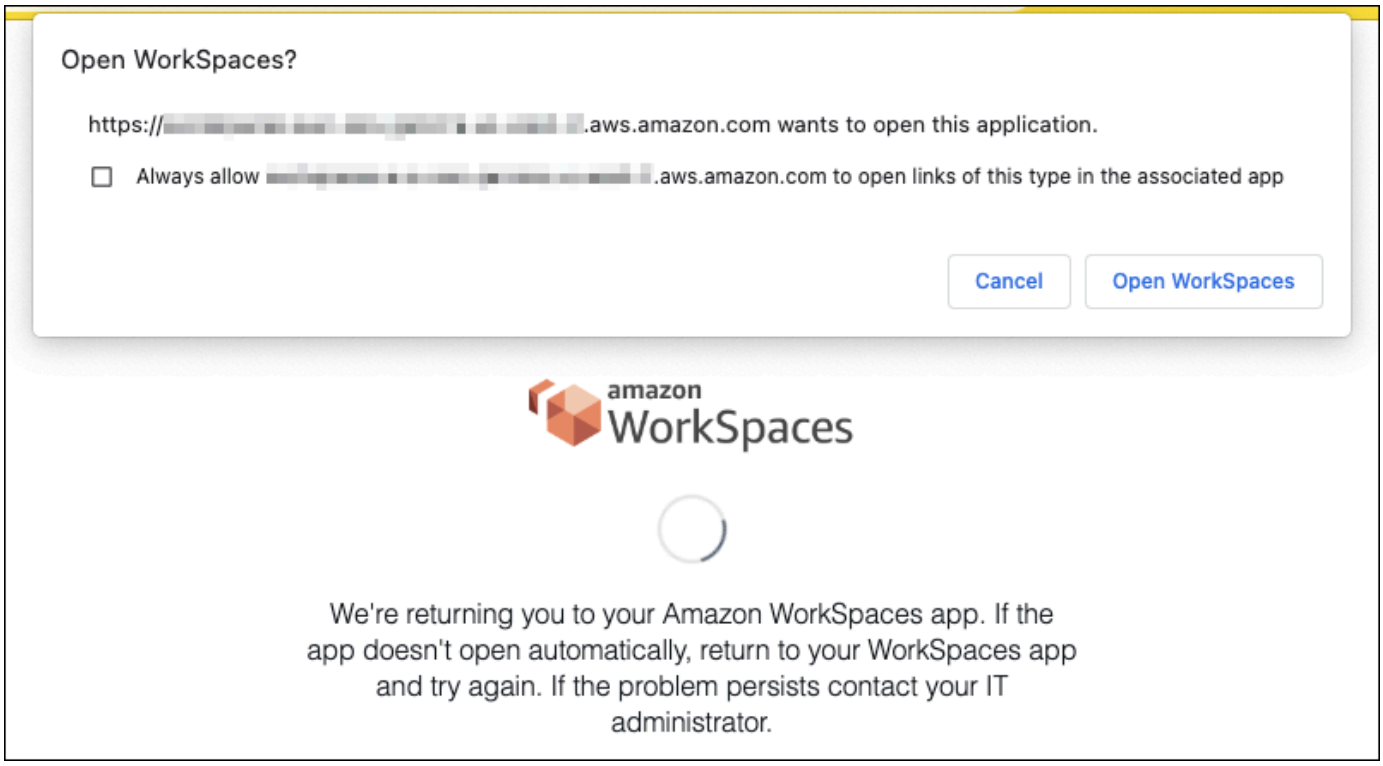
4. WorkSpaces 客户端应用程序现已注册，用户可以单击继续登录 WorkSpaces，以继续登录。

由 WorkSpaces 客户端启动的流

客户端启动的流允许用户在登录 IdP 后登录其 WorkSpaces。

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

3. 登录 IdP 后，系统会将用户重定向到弹出窗口。按照提示允许您的 Web 浏览器打开客户端应用程序。



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

为个人版设置 SAML 2.0 WorkSpaces

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

内容

- 要求
- 先决条件
- 步骤 1：在 IAM 中Amazon创建 SAML 身份提供商
- 步骤 2：创建 SAML 2.0 联合身份验证 IAM 角色
- 步骤 3：为 IAM 角色嵌入内联策略

- 步骤 4：配置 SAML 2.0 身份提供者
- 步骤 5：为 SAML 身份验证响应创建断言
- 步骤 6：配置联合身份验证的中继状态
- 步骤 7：在您的 WorkSpaces 目录上启用与 SAML 2.0 的集成

要求

- 以下区域提供 SAML 2.0 身份验证：
  - 美国东部（弗吉尼亚州北部）区域
  - 美国西部（俄勒冈州）区域
  - 非洲（开普敦）区域
  - 亚太地区（孟买）区域
  - 亚太地区（首尔）区域
  - 亚太地区（新加坡）区域
  - 亚太地区（悉尼）区域
  - 亚太地区（东京）区域
  - 加拿大（中部）区域
  - 欧洲地区（法兰克福）区域
  - 欧洲地区（爱尔兰）区域
  - 欧洲地区（伦敦）区域
  - 南美洲（圣保罗）区域
  - 以色列（特拉维夫）区域
  - AmazonGovCloud （美国西部）
  - AmazonGovCloud （美国东部）
- 要将 SAML 2.0 身份验证与一起使用 WorkSpaces，IdP 必须通过深度链接目标资源或中继状态端点 URL 支持未经请求的 IDP 发起的 SSO。的示例 IdPs 包括 ADFS、Azure AD、Duo 单点登录、Okta 和。 PingFederate PingOne有关更多信息，请参阅 IdP 文档。
- SAML 2.0 身份验证将在使用 Simple AD WorkSpaces 启动时起作用，但不建议这样做，因为 Simple AD 未与 SAML 2.0 集成。 IdPs
- 以下 WorkSpaces 客户端支持 SAML 2.0 身份验证。SAML 2.0 身份验证不支持其他客户端版本。打开 Amazon WorkSpaces 客户端下载以查找最新版本：
  - Windows 客户端应用程序 5.1.0.3029 或更高版本

- macOS 客户端 5.x 或更高版本
- 适用于 Ubuntu 22.04 2024.1 或更高版本、Ubuntu 20.04 24.1 或更高版本的 Linux 客户端
- Web Access

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

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

先决条件

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

1. 配置您的 IdP 以集成与该目录一起使用的 Microsoft 活动目录中的用户身份。 WorkSpaces 对于具有 a 的用户 WorkSpace，Active Directory 用户的AMAccount姓名和电子邮件属性以及 SAML 声明值必须匹配，用户才能 WorkSpaces 使用 IdP 登录。有关将 Active Directory 与 IdP 集成的更多信息，请参阅您的 IdP 文档。
2. 配置 IdP 以与 Amazon 建立信任关系
   - 有关配置Amazon联合的更多信息，请参阅将第三方 SAML 解决方案提供商与Amazon集成。相关示例包括 IdP 与 Amazon IAM 集成以访问Amazon管理控制台。
   - 使用您的 IdP 生成和下载联合身份验证元数据文档，该文档将您的组织描述为 IdP。此签名 XML 文档用于建立信赖方信任关系。将该文件保存您稍后可通过 IAM 控制台访问的位置。
3. 使用 WorkSpaces 管理控制台 WorkSpaces 为创建或注册目录。有关更多信息，请参阅管理目录 WorkSpaces。以下目录类型支持 WorkSpaces SAML 2.0 身份验证：
   - AD Connector
   - Amazon微软 AD 托管
4. WorkSpace 为可以使用支持的目录类型登录 IdP 的用户创建。您可以使用 WorkSpaces 管理控制台或 WorkSpaces API 创建。 WorkSpace Amazon CLI有关更多信息，请参阅使用启动虚拟桌面 WorkSpaces。

步骤 1：在 IAM 中Amazon创建 SAML 身份提供商

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

步骤 2：创建 SAML 2.0 联合身份验证 IAM 角色

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

为 SAML IdP 创建 IAM 角色

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

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

5. 对于 Attribute，选择 SAML:sub_type。
6. 对于值，输入 `persistent`。该值限制角色访问 SAML 用户流式传输请求，其中包括值为 persistent 的 SAML 主题类型断言。如果 SAML:sub_type 为 persistent，则在来自特定用户的所有 SAML 请求中，您的 IdP 会为 NameID 元素发送相同的唯一值。有关 SAML: sub_type 断言的更多信息，请参阅使用基于 SAML 的联合身份验证进行 API 访问的 “在基于 SAML 的联合身份验证中唯一标识用户” 部分。Amazon
7. 检查您的 SAML 2.0 信任信息，确认正确的可信实体和条件，然后选择 Next: Permissions。
8. 在 Attach permissions policies (附加权限策略) 页面上，选择 Next: Tags (下一步：标签)。
9. （可选）为要添加的每个标签输入键和值。有关更多信息，请参阅标记 IAM 用户和角色。
10. 完成此操作后，选择 Next: Review (下一步：审核)。稍后您将为此角色创建并嵌入内联策略。
11. 对于角色名称，输入有助于标识此角色作用的名称。由于多个实体可能引用该角色，因此，角色创建完毕后，您将无法编辑角色名称。
12. （可选）对于角色描述，输入新角色的描述。

13. 检查角色详细信息，然后选择创建角色。
14. 将 sts: TagSession 权限添加到您的新 IAM 角色的信任策略中。有关更多信息，请参阅在 Amazon STS 中传递会话标签。在新 IAM 角色的详细信息中，选择信任关系选项卡，然后选择编辑信任关系*。当 “编辑信任关系” 策略编辑器打开时，添加 sts: TagSession * 权限，如下所示：

    JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Federated": "arn:aws:iam::111122223333:saml-provider/
IDENTITY-PROVIDER"
            },
            "Action": [
                "sts:AssumeRoleWithSAML",
                "sts:TagSession"
            ],
            "Condition": {
                "StringEquals": {
                    "SAML:aud": "https://signin.aws.amazon.com/saml"
                }
            }
        }
    ]
}
```

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

步骤 3：为 IAM 角色嵌入内联策略

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

> **Important**
>
> 该`workspaces:Stream`操作不支持Amazon根据源 IP 管理访问权限的 IAM 策略。要管理的 IP 访问控制 WorkSpaces，请使用 IP 访问控制组。此外，在使用 SAML 2.0 身份验证时，您可在 SAML 2.0 IdP 提供 IP 访问控制策略时使用此类策略。

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

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "workspaces:Stream",
            "Resource": "arn:aws:workspaces:us-east-1:123456789012:directory/
DIRECTORY-ID",
            "Condition": {
                "StringEquals": {
                    "workspaces:userId": "${saml:sub}"
                }
            }
        }
    ]
}
```

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

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

步骤 4：配置 SAML 2.0 身份提供者

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

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

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

> **Note**
>
> 如果您的最终用户在使用相同的 SAML 2.0 身份提供商 (IdP) 时经常在多个不同的 WorkSpaces 用户身份之间切换，请确保将 IdP 配置为在每次登录尝试时强制进行身份验证 ForceAuthn ()。这可以防止您的 IdP 重复使用现有 SSO 会话，否则当您的用户切换到另一个 SSO 会话时，这可能会导致身份验证失败。 WorkSpace有关启用 ForceAuthn （或等效）设置的指导，请参阅您的 IdP 文档。

步骤 5：为 SAML 身份验证响应创建断言

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

如果您的 IdP 中尚未配置此信息，请提供以下内容：

- SAML 主题 NameID – 登录用户的唯一标识符。该值必须与 WorkSpaces 用户名相匹配，并且通常是 Active Directory 用户的 “AMAccount名称” 属性。
- SAML 主题类型（值设为 `persistent`）– 将值设为 `persistent` 可确保在来自特定用户的所有 SAML 请求中，您的 IdP 会为 `NameID` 元素发送相同的唯一值。请确保您的 IAM 策略包含一个条件，仅允许将 SAML sub_type 设置为 `persistent` 的 SAML 请求（如步骤 2：创建 SAML 2.0 联合身份验证 IAM 角色中所述）。
- 将 **Name** 属性设置为 **`https://aws.amazon.com/SAML/Attributes/Role`** 的 **Attribute** 元素 - 此元素中包含一个或多个 `AttributeValue` 元素，以列出您的 IdP 将用户映射到哪个 IAM 角色和 SAML IdP。角色和 IdP 以逗号分隔的一对指定。 ARNs预期值的一个示例是 `arn:aws:iam::ACCOUNTNUMBER:role/ROLENAME,arn:aws:iam::ACCOUNTNUMBER:saml-provider/PROVIDERNAME`。
- **AttributeName**属性设置为的元素 **`https://aws.amazon.com/SAML/Attributes/RoleSessionName`** — 此元素包含一个元素，该`AttributeValue`元素为为 SSO 颁发的Amazon临时证书提供标识符。`AttributeValue` 元素中的值长度必须介于 2 到 64 个字符之间，只能包含字母数字字符、下划线和以下字符：_ . : / = + - @。它不能包含空格。该值通常是电子邮件地址或用户主体名 (UPN)。该值不应包含空格，如用户的显示名称。
- 将 **Name** 属性设置为 **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`** 的 **Attribute** 元素 - 此元素包含一个可提供用户电子邮件地址的 `AttributeValue` 元素。该值必须与 WorkSpaces 目录中定义的 WorkSpaces 用户电子邮件地址相匹配。标签值可能包括字母、数字、空格和 _ . : / = + - @ 字符的组合。有关更多信息，请参阅《IAM 用户指南》中的标记 IAM 用户和 Amazon STS 的规则。
- 将 **Name** 属性设置为 **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:UserPrincipalName`** 的 **Attribute** 元素（可选）- 此元素包含一个为登录用户提供 Active Directory `userPrincipalName` 的 `AttributeValue` 元素。必须采用 `username@domain.com` 格式提供该值。此参数与基于证书的身份验证一起使用，作为最终用户证书中的主题备用名称。有关更多信息，请参阅基于证书的身份验证。
- 将 **Name** 属性设置为 **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:ObjectSid`** 的 **Attribute** 元素（可选）- 此元素包含一个为登录用户提供 Active Directory 安全标识符 (SID) 的 `AttributeValue` 元素。此参数与基于证书的身份验证一起使用，以启用到 Active Directory 用户的强映射。有关更多信息，请参阅基于证书的身份验证。
- 将 **Name** 属性设置为 **`https://aws.amazon.com/SAML/Attributes/PrincipalTag:ClientUserName`** 的 **Attribute** 元素（可选）- 此元素包含一个提供备用用户名格式的 `AttributeValue` 元素。如果您的用例需要用户名格式（例如`corp\username`、或）`username@corp.example.com`才能使用 WorkSpaces 客户端登录`corp.example.com\username`，请使用此属性。标签键和值可以包含字母、数字、空格以及 _ : / . + = @ - 字符的任意

组合。有关更多信息，请参阅《IAM 用户指南》中的标记 IAM 用户和 Amazon STS 的规则。要声明 `corp\username` 或 `corp.example.com\username` 格式，请将 SAML 断言中的 \ 替换为 /。

- **`AttributeName`**属性设置为 At https://aws.amazon.com/SAML/ tributes/: DomainPrincipalTag（可选）的元素 — 此元素包含一个为登录用户提供 Active Directory DNS 完全限定域名 (FQDN) 的元素`AttributeValue`。当用户的 Active Directory `userPrincipalName` 包含备用后缀时，此参数用于基于证书的身份验证。必须采用 `domain.com` 提供该值，包括所有子域名。
- **`AttributeName`**属性设置为 A https://aws.amazon.com/SAML/ ttributes/SessionDuration（可选）的元素 — 此元素包含一个`AttributeValue`元素，用于指定在要求重新进行身份验证之前，用户的联合流媒体会话可以保持活动状态的最长时间。默认值为 3600 秒（60 分钟）。有关更多信息，请参阅 SAML `SessionDurationAttribute`。

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

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

步骤 6：配置联合身份验证的中继状态

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

以下为中继状态 URL 格式：

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

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

或者，如果您使用跨区域重定向 WorkSpaces，则可以将注册代码替换为与主区域和故障转移区域中的目录关联的完全限定域名 (FQDN)。有关更多信息，请参阅 Amazon 的跨区域重定向。 WorkSpaces 使用跨区域重定向和 SAML 2.0 身份验证时，需要使用与每个区域关联的中继状态端点，为 SAML

2.0 身份验证启用主目录和故障转移目录，并使用 IdP 进行独立配置。这将允许用户在登录前注册其 WorkSpaces 客户端应用程序时正确配置 FQDN，并允许用户在故障转移事件期间进行身份验证。

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

支持 WorkSpaces SAML 2.0 身份验证的区域

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

Region	中继状态端点
欧洲地区（法兰克福）区域	workspaces.euc-sso.eu-central-1.aws.amazon.com
欧洲地区（爱尔兰）区域	workspaces.euc-sso.eu-west-1.aws.amazon.com
欧洲地区（伦敦）区域	workspaces.euc-sso.eu-west-2.aws.amazon.com
南美洲（圣保罗）区域	workspaces.euc-sso.sa-east-1.aws.amazon.com
以色列（特拉维夫）区域	workspaces.euc-sso.il-central-1.aws.amazon.com
AmazonGovCloud （美国西部）	• workspaces.euc-so。 us-gov-west-1。 amazonaws-us-gov.com • (FIPS) 工作空间。 euc-sso-fips。 us-gov-west-1。 amazonaws-us-gov.com Note 有关更多信息，请参阅 AmazonGov Cloud （美国）用户指南 WorkSpaces中的 Amazon。

Region	中继状态端点
AmazonGovCloud （美国东部）	• workspaces.euc-so。 us-gov-east-1。 amazonaws-us-gov.com • (FIPS) 工作空间。 euc-sso-fips。 us-gov-east-1。 amazonaws-us-gov.com Note 有关更多信息，请参阅 AmazonGov Cloud （美国）用户指南 WorkSpaces中的 Amazon。

通过身份提供者（IdP）发起的流，您可以选择指定要用于 SAML 2.0 联合身份验证的客户端。为此，请在中继状态 URL 的末尾、`&client=` 后面指定 `native` 或 `web`。在中继状态 URL 中指定参数时，相应的会话将自动在指定的客户端中启动。

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

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

启用与 SAML 2.0 的集成

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在导航窗格中，选择目录。
3. 选择您的 “目录 ID” WorkSpaces。
4. 在身份验证下，选择编辑。
5. 选择编辑 SAML 2.0 身份提供者。
6. 选中启用 SAML 2.0 身份验证。
7. 对于用户访问 URL 和 IdP 深层链接参数名称，输入适用于您 IdP 和您在步骤 1 中配置的应用程序的值。如果您省略此参数，则 IdP 深度链接参数名称的默认值RelayState为 “”。下表列出了应用程序的各种身份提供者所独有的用户访问 URL 和参数名称。

要添加到允许列表的域和 IP 地址

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

身份提供者	参数	用户访问 URL
PingFederate	`TargetResource`	`https://<host>/idp/startSSO.ping?PartnerSpId=<sp_id>`
PingOne 适用于企业	`TargetResource`	`https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=<app_id>&idpid=<idp_id>`

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

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

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

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

> **Note**
>
> PCoWeb 访问不支持带有 SAML 的 IP。

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

基于证书的身份验证和个人 WorkSpaces

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

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

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

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

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

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

有关使用 Amazon 配置基于证书的身份验证的更多信息 WorkSpaces，请参阅如何为 Amazon 配置基于证书的身份验证 WorkSpaces和在高度监管的环境中使用应用程序进行基于证书的身份验证的设计注意事项以及。 WorkSpaces WorkSpaces

先决条件

在启用基于证书的身份验证之前，请完成以下步骤。

1. 使用 SAML 2.0 集成配置您的 WorkSpaces 目录，以使用基于证书的身份验证。有关更多信息，请参阅与 SAML 2.0 WorkSpaces 集成。
2. 在 SAML 断言中配置 `userPrincipalName` 属性。有关更多信息，请参阅为 SAML 身份验证响应创建断言。

3. 在 SAML 断言中配置 `ObjectSid` 属性。这是对 Active Directory 用户执行强映射所必须的属性。如果该属性与 SAML_Subject `NameID` 中指定的用户的 Active Directory 安全标识符 (SID) 不匹配，则基于证书的身份验证将失败。有关更多信息，请参阅为 SAML 身份验证响应创建断言。

> **Note**
>
> 根据微软 KB5 014754 的说法，在 2025 年 9 月 10 日之后，该`ObjectSid`属性将成为基于证书的身份验证的必备属性。

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

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

6. 使用名为 `euc-private-ca` 的键标记您的私有 CA，以指定该 CA 用于 EUC 基于证书的身份验证。该键不需要值。有关更多信息，请参阅管理私有 CA 的标签。
7. 基于证书的身份验证使用虚拟智能卡进行登录。按照 Active Directory 中使用第三方证书颁发机构启用智能卡登录的指导原则，执行以下步骤：

- 使用域控制器证书配置域控制器，以对智能卡用户进行身份验证。如果您在 Active Directory 中配置了 Active Directory 证书服务企业 CA，则系统会自动使用启用智能卡登录的证书注册域控制器。如果您没有 Active Directory 证书服务，请参阅对第三方 CA 的域控制器证书的要求。您可以使用 Amazon 私有 CA 创建域控制器证书。如果这样做，请不要使用为短期证书配置的私有 CA。

> **Note**
>
> 如果您正在使用Amazon Managed Microsoft AD，则可以在 EC2 实例上配置证书服务以满足域控制器证书的要求。有关Amazon Managed Microsoft AD配置Amazon Launch Wizard了 Active Directory 证书服务的部署示例，请参阅。 Amazon私有 CA 可以配置为 Active Directory 证书服务 CA 的从属机构，也可以在使用时将其配置为自己的根Amazon Managed Microsoft AD。
> Amazon Managed Microsoft AD和 Active Directory 证书服务的另一项配置任务是创建从控制器 VPC 安全组到运行证书服务的 EC2 实例的出站规则，允许 TCP 端口 135 和 49152-65535 启用证书自动注册。此外，正在运行的 EC2 实例必须允许域实例（包括域控制器）通过相同的端口进行入站访问。有关查找安全组的更多信息，Amazon Managed Microsoft AD请参阅配置您的 VPC 子网和安全组。

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

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

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

> **Note**
>
> - 当 WorkSpaces 台式机加入域时，Active Directory 必须自动将 CA 分发给受信任的根证书颁发机构和企业 NTAuth 存储。

启用基于证书的身份验证

要启用基于证书的身份验证，请完成以下步骤。

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在导航窗格中，选择目录。
3. 选择您的目录 ID WorkSpaces。
4. 在身份验证下，单击编辑。
5. 单击编辑基于证书的身份验证。
6. 选中启用基于证书的身份验证。
7. 确认您的私有 CA ARN 已关联到列表中。私有 CA 应位于同一个Amazon账户中Amazon Web Services 区域，并且必须使用有权出现在列表中的密钥 euc-private-ca进行标记。
8. 单击 Save Changes（保存更改）。基于证书的身份验证现已启用。
9. 重启你的 Windows WorkSpaces on DCV 捆绑包以使更改生效。有关更多信息，请参阅重启 a WorkSpace。
10. 重启后，当用户使用支持的客户端通过 SAML 2.0 进行身份验证时，将不再收到输入域密码的提示。

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

管理基于证书的身份验证

CA 证书

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

最终用户证书

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

审核报告

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

日志记录和监控

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

启用跨账户 PCA 共享

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

与 CBA 一起使用共享的私有 WorkSpaces CA 资源

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

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

访问加入 Microsoft Entra ID 的 WorkSpaces 个人版

您可以创建加入 Microsoft Entra ID 并注册到 Intune 的 Windows 10 或 11 BYOL 个人版 WorkSpaces。有关更多详细信息，请参阅 使用个人版创建专用的 Microsoft Entra ID 目录 WorkSpaces 。

身份验证工作流

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

- 当工作流由 IdP 启动时。例如，当用户使用 Web 浏览器在 Entra ID 用户门户中选择应用程序时。
- 当工作流由 WorkSpaces 客户端启动时。例如，当用户打开客户端应用程序并登录时。

在这些示例中，用户输入 `user@example.onmicrosoft.com` 以登录 IdP。在 Entra ID 上，系统将企业应用程序配置为与 IAM Identity Center 相集成。用户在使用 IAM Identity Center 作为身份源连接到 Entra ID 租户的目录中创建自己的用户名所对应的 WorkSpace。此外，用户在自己的设备上安装 WorkSpaces 客户端应用程序，或者用户在 Web 浏览器中使用 Web Access。

由身份提供者 (IdP) 启动的客户端应用程序流

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

1. 用户使用其 Web 浏览器登录 IdP（Microsoft Entra ID）。
2. 登录 IdP 后，用户从 IdP 用户门户中选择 Amazon IAM Identity Center 应用程序。
3. 系统在浏览器中将用户重定向到 Amazon 访问门户。然后，用户选择 WorkSpaces 图标。
4. 系统将用户重定向到下一页，并自动打开 WorkSpaces 客户端应用程序。如果客户端应用程序未自动打开，请选择打开 Amazon WorkSpaces 应用程序。

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

由 WorkSpaces 客户端启动的流

客户端启动的流允许用户在登录 IdP 后登录其 WorkSpaces。

1. 用户启动 WorkSpaces 客户端应用程序（如果尚未运行），然后单击继续登录 WorkSpaces。
2. 系统会将用户重定向到其默认 Web 浏览器以登录 IdP。如果用户已经在浏览器中登录 IdP，则无需再次登录，可以跳过此步骤。
3. 登录 IdP 后，系统会将用户重定向到弹出窗口。按照提示允许您的 Web 浏览器打开客户端应用程序。
4. 系统在 Windows 登录屏幕上将用户重定向到 WorkSpaces 客户端应用程序。
5. 用户使用自己的 Entra ID 用户名和凭证登录到 Windows。

新用户体验

如果您是首次登录加入 Microsoft Entra ID 的 Windows WorkSpaces，则必须体验开箱即用体验（OOBE）。在 OOBE 期间，WorkSpaces 会加入到 Entra ID。您可以通过配置分配给您为 WorkSpaces 创建的 Microsoft Intune 设备组的 Autopilot 配置文件，来自定义 OOBE 体验。有关更多信息，请参阅 步骤 3：配置 Windows Autopilot 用户驱动模式。

在 “个人” 中 WorkSpaces 使用智能卡进行身份验证

DCV 捆绑包 WorkSpaces 上的 Windows 和 Linux 允许使用通用访问卡 (CAC) 和个人身份验证 (PIV) 智能卡进行身份验证。

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

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

内容

- 要求
- 限制
- 目录配置
- 启用适用于 Windows 的智能卡 WorkSpaces
- 为 Ubuntu、Rocky Linux 和红帽企业 Linux 启用智能卡 WorkSpaces
- 为亚马逊 Linux 2 启用智能卡 WorkSpaces

要求

- 会话前身份验证需要 Active Directory Connector (AD Connector) 目录。AD Connector 使用基于证书的相互传输层安全行协议身份验证（相互 TLS），通过基于硬件或软件的智能卡证书对 Active Directory 的用户进行身份验证。有关如何配置 AD Connector 和本地目录的更多信息，请参阅目录配置。
- 要在 Windows 或 Linux 上使用智能卡 WorkSpace，用户必须使用亚马逊 WorkSpaces Windows 客户端版本 3.1.1 或更高版本、mac WorkSpaces OS 客户端版本 3.1.5 或更高版本，或 Ubuntu 22.04 客户端版本 2024.1 WorkSpaces 或更高版本（Ubuntu 20.04 客户端不支持智能卡身份验证）。 WorkSpaces 有关在 Windows 和 macOS 客户端上使用智能卡的更多信息，请参阅亚马逊 WorkSpaces 用户指南中的智能卡支持。
- 根 CA 和智能卡证书必须满足某些要求。有关更多信息，请参阅《Amazon Directory Service 管理指南》中的在 AD Connector 中启用 mTLS 身份验证以用于智能卡以及 Microsoft 文档中的证书要求。

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

  - 证书 userPrincipalName (SAN) 字段中的 AD 用户 subjectAltName (UPN)。建议为用户的默认 UPN 颁发智能卡证书。

> **Note**
>
> 亚马逊 Linux 2 WorkSpaces 依靠 UPN 进行 certificate-to-user映射。较新的 Linux WorkSpaces，例如 Ubuntu、Rocky Linux 和红帽企业 Linux WorkSpaces，支持更安全的映射方法。

- 客户端身份验证 (1.3.6.1.5.5.7.3.2) 扩展密钥使用 (EKU) 属性。
- 智能卡登录 (1.3.6.1.4.1.311.20.2.2) EKU 属性。

- 对于会话前身份验证，需要在线证书状态协议 (OCSP) 来检查证书吊销。对于会话中身份验证，建议使用 OCSP，但不是必需的。

> **Note**
>
> 默认情况下，Ubuntu WorkSpaces、Rocky Linux WorkSpaces 和 Red Hat Enterprise Linux WorkSpaces 需要 OCSP 进行会话内身份验证，而这些系统中的 OCSP 验证要求 OCSP 响应者启用 NONCE 扩展以防止重播攻击。要禁用 NONCE 扩展，必须完全禁用会话中 OCSP 验证。要在 Ubuntu、Rocky Linux 和红帽企业 Linux 中禁用 OCSP 验证 WorkSpaces，请创建一个`/etc/sssd/conf.d/disable-ocsp.conf`包含以下内容的新文件：
>
> ```
> [sssd]
> certificate_verification = no_ocsp
> ```

限制

- 目前仅支持 WorkSpaces Windows 客户端应用程序版本 3.1.1 或更高版本、mac WorkSpaces OS 客户端应用程序版本 3.1.5 或更高版本 WorkSpaces 以及 Ubuntu 22.04 客户端应用程序版本 2024.1 或更高版本。 WorkSpaces 智能卡身份验证不支持 Ubuntu 20.04 或更早版本的客户端应用程序。
- 只有在 64 位版本的 WorkSpaces Windows 上运行时，Windows 客户端应用程序 3.1.1 或更高版本才支持智能卡。
- 目前只支持 AD Connector 目录进行智能卡身份验证。
- 会话中身份验证在所有支持 DCV 的区域均可用。以下区域提供会话前身份验证：
  - 亚太地区（悉尼）区域
  - 亚太地区（东京）区域
  - 欧洲地区（爱尔兰）区域

  - Amazon GovCloud （美国东部）区域
  - Amazon GovCloud （美国西部）区域
  - 美国东部（弗吉尼亚州北部）区域
  - 美国西部（俄勒冈州）区域
- 对于 Linux 或 Windows 上的会话内身份验证和会话前身份验证 WorkSpaces，目前一次只能使用一张智能卡。可以同时使用多张卡，但不支持。
- 对于会话前身份验证，目前不支持在同一目录上同时启用智能卡身份验证和登录身份验证。
- 目前仅支持 CAC 和 PIV 卡。其他类型基于硬件或软件的智能卡也可能起作用，但它们尚未经过与 DCV 配合使用的全面测试。

目录配置

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

AD Connector 目录配置

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

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

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

本地目录配置 In addition to configuring your AD Connector directory:

- 确保向本地目录的域控制器颁发的证书设置了 “KDC 身份验证” 扩展密钥用法 (EKU)。为此，请使用 Active Directory 域服务 (AD DS) 默认 Kerberos 身份验证证书模板。请勿使用域控制器证书模板或域控制器身份验证证书模板，因为这些模板不包含智能卡身份验证所需的设置。
- 对于 Linux WorkSpaces，请确保颁发智能卡证书的 CA 的 OCSP 响应器已启用 NONCE 扩展。如果无法启用，则必须在 Ubuntu、Rocky Linux 和红帽企业 Linux 中禁用会话中 OCSP 验证。

WorkSpaces要禁用 OCSP 验证，请创建一个`/etc/sssd/conf.d/disable-ocsp.conf`包含以下内容的新文件：

```
[sssd]
certificate_verification = no_ocsp
```

启用适用于 Windows 的智能卡 WorkSpaces

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

检测 Windows 锁屏并断开会话连接

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

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

启用会话内或会话前身份验证

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

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

允许用户在浏览器中使用智能卡

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

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

例如，您可以安装适用于 Windows 的 64 位版本的 OpenSC 来支持 PKCS #11，然后使用以下组策略设置，其中 *`NAME_OF_DEVICE`* 是您要用来标识 PKCS #11 的任何值，例如 `OpenSC`，其中

PATH_TO_LIBRARY_FOR_DEVICE 是 PKCS #11 模块的路径。此路径应指向扩展名为 .DLL 的库，例如 `C:\Program Files\OpenSC Project\OpenSC\pkcs11\onepin-opensc-pkcs11.dll`。

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

> **Tip**
>
> 如果您使用的是 OpenSC，也可以通过运行 `pkcs11-register.exe` 程序，将 OpenSC `pkcs11` 模块加载到 Firefox 中。要运行此程序，请双击 `C:\Program Files\OpenSC Project\OpenSC\tools\pkcs11-register.exe` 中的文件，或者打开命令提示符窗口并运行以下命令：
>
> ```
> "C:\Program Files\OpenSC Project\OpenSC\tools\pkcs11-register.exe"
> ```
>
> 要验证 OpenSC `pkcs11` 模块是否已加载到 Firefox 中，请执行以下操作：
>
> 1. 如果 Firefox 已经在运行，请将其关闭。
> 2. 打开 Firefox。选择右上角的菜单按钮 ，然后选择选项。
> 3. 在关于: 首选项页面上，在左侧导航窗格中选择隐私与安全。
> 4. 在证书下，选择安全设备。
> 5. 在设备管理器对话框中，您应该在左侧导航栏中看到 OpenSC 智能卡框架 (0.21)，当您选择它时，它应该具有以下值：
>
> 模块：`OpenSC smartcard framework (0.21)`
>
> 路径：`C:\Program Files\OpenSC Project\OpenSC\pkcs11\onepin-opensc-pkcs11.dll`

问题排查

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

可能导致问题的一些常见问题：

- 槽与证书的映射不正确。

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

通常，最好只有一个用于智能卡身份验证的证书，该证书映射到智能卡的第一个槽。

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

为 Ubuntu、Rocky Linux 和红帽企业 Linux 启用智能卡 WorkSpaces

要在 Ubuntu、Rocky Linux 和 Red Hat Enterprise Linux WorkSpaces 上启用智能卡，你需要在 WorkSpace 镜像中包含所有 CAs 发行智能卡和所有颁发域控制器证书的中间 CA 证书。 CAs

获取您的 CA 证书

您可以通过多种方式获取 CA 证书：

- 您可以使用第三方证书颁发机构的 CA 证书包。
- 您可以使用 Web 注册网站导出自己的 CA 证书，该网站是`http://`*`ip_address`*`/certsrv`或`http://`*`fqdn`*`/certsrv`，其中*`ip_address`*和*`fqdn`*是 CA 服务器的 IP 地址和完全限定域名 (FQDN)。有关使用 Web 注册网站的更多信息，请参阅 Microsoft 文档中的如何导出根证书颁发机构证书。
- 您可以使用以下步骤从运行 Active Directory 证书服务 (AD CS) 的 CA 服务器中导出 CA 证书。有关安装 AD CS 的信息，请参阅 Microsoft 文档中的安装证书颁发机构。

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

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

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

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

将您的 CA 证书添加到 Linux WorkSpaces

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

- 将您的 CA 证书导入私有 PEM 捆绑包，该包定义了 Linux WorkSpaces 上的 SSSD 的信任根）。
- 更新 SSSD、PAM 和 Kerberos 配置，其中包括在置备期间启用`PKINIT`（使用证书而不是密码进行 Kerberos 身份验证）。 WorkSpace

以下过程说明如何使用`enable_smartcard`脚本导入 CA 证书以及如何为 Linux 启用智能卡身份验证 WorkSpaces。

1. 创建一个启用了 DCV 协议 WorkSpace 的新 Linux。在 Amazon WorkSpaces 控制台 WorkSpace 中启动时，请务必在 “选择捆绑包” 页面上为协议选择 DCV，然后选择一个 Linux WorkSpaces 公共捆绑包。
2. 在新创建的文件中 WorkSpace，确保`/etc/skylight.conf`文件在`[features]`章节中有`pam_smartcard = true`行：

   ```
   [features]
   pam_smartcard = true
   ```

   > **Note**
   >
   > 如果尚未将所有用户配置为使用强`altSecurityIdentities`证书映射，您也可以在中的同一`[features]`部分中添加一`smartcard_weak_mapping = true`行`/etc/skylight.conf`以支持旧版映射方法，但我们建议尽快迁移这些用户以使用强映射方法。

3. 在 WorkSpace，以 root 身份运行以下命令*pem-path1*，其中*pem-path2*、等是文件的路径，每个文件都包含智能卡和域控制器证书信任链中的一个 CA 证书。所有这些文件都应采用 PEM 格式，每个文件包含一个证书。可以使用 Glob 模式（例如`*.pem`）

   ```
   /usr/lib/skylight/enable_smartcard --ca-cert pem-path1 pem-path2 pem-path3 ...
   ```

> **Note**
>
> 在运行上述命令 WorkSpace 之前，请确保在上安装了其他依赖包，并以 root 身份使用以下命令。
>
> 对于 Rocky Linux 和红帽企业 Linux WorkSpaces：
>
> ```
> dnf install sssd-dbus libsss_simpleifp sssd-tools krb5-pkinit opensc
> ```
>
> 对于 Ubuntu WorkSpaces 来说：
>
> ```
> apt install krb5-pkinit opensc
> ```

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

允许用户在 Firefox 中使用智能卡

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

1. 在你 WorkSpace 用来创建 WorkSpace 映像的上，创建一个名`policies.json`为的新文件，其中*`PREFIX`*位于`/usr/lib64`基于 Fedora 的系统（亚马逊 Linux 2 *`PREFIX`*`/firefox/distribution/`、红帽企业 Linux 和 Rocky Linux WorkSpaces）和基于 Debian 的系统（Ubuntu）`/usr/lib`上。 WorkSpaces
2. 在 JSON 文件中，添加以下 SecurityDevices 策略，其中*`NAME_OF_DEVICE`*是您要用来标识`pkcs`模块的任何值。例如，您可能想使用 `"OpenSC"` 这样的值：

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

```
}
```

问题排查

当会话前设置为使用密码身份验证时，智能卡身份验证的故障排除更容易——在会话配置期间，Linux 会 WorkSpaces 自动将主机身份验证模式首选项切换为基于密码或基于智能卡的身份验证模式，具体取决于所使用的会话前身份验证方法。如果智能卡身份验证存在任何问题，则使用密码会话前身份验证断开连接并重新连接会将工作空间重置为主机上的密码身份验证。要手动将 Linux WorkSpaces 实例切换到智能卡身份验证，请以 root 身份运行`/usr/lib/skylight/resume_smartcard`命令。

Linux WorkSpaces 使用 OpenSC 软件来处理智能卡。该软件附带诸如`pkcs11-tool`和`pkcs15-tool`之类的工具，可用于解决智能卡问题。这些工具可用于检查智能卡读卡器、单个令牌以及每个智能卡令牌上的 PIV 插槽或证书。

`openssl`命令行工具可以帮助解决信任链、OCSP 响应器或缺失 KUs/EKUs（密 usage/extended 钥使用）标志的问题，尤其是与从智能卡中提取公共证书`pkcs15-tool`的功能结合使用时。

常见故障排除选项：

- 首先从智能卡中提取证书（通常是 PIV 插槽 9A）并将其保存为：*card-cert.pem*`pkcs15-tool --read-certificate 1 > `*card-cert.pem*
- 根据信任数据库验证提取的证书 WorkSpace：`openssl verify -verbose -CAfile /etc/sssd/pki/sssd_auth_ca_db.pem -cert `*card-cert.pem*
- 从提取的智能卡证书中获取 OCSP 网址：`openssl x509 -noout -ocsp_uri -in `*card-cert.pem*
- 验证 OCSP 响应是否表明证书有效并且包含 NONCE:`openssl ocsp -issuer /etc/sssd/pki/sssd_auth_ca_db.pem -CAfile /etc/sssd/pki/sssd_auth_ca_db.pem -cert `*card-cert.pem*` -text -url `*OCSP_URI*，其中*OCSP_URI*是上面的 OCSP 网址。
- 检查域控制器证书是否被视为可信：`openssl s_client -connect `*DC_HOSTNAME*`:636 -showcerts | openssl verify -verbose -CAfile /etc/sssd/pki/sssd_auth_ca_db.pem`，其中*DC_HOSTNAME*是 Active Directory 域中其中一个域控制器的主机名。
- 确认域控制器证书已设置 KDC 身份验证 EKU（扩展密钥用法）：。`openssl s_client -connect `*DC_HOSTNAME*`:636 -showcerts | openssl x509 -noout -text`
- 尝试手动 PKINIT，看看是否有任何错误代码可以用来缩小问题范围：`KRB5_TRACE=/dev/stdout kinit -X X509_user_identity=PKCS11:opensc-pkcs11.so:certid=`*01*` -V`，卡上四个

主 PIV 插槽之一的数量在*01*哪里 —— 01 for 9A、02 for 等。9C大多数卡在插槽 9A 中都有用于用户身份验证的证书。

- 检查系统是否能够将智能卡证书映射到 AD 用户（以 root 身份执行）：`dbus-send --print-reply --system --dest=org.freedesktop.sssd.infopipe /org/freedesktop/sssd/infopipe/Users org.freedesktop.sssd.infopipe.Users.FindByCertificate string:"$(<card-cert.pem)"`。这可以与启用 SSSD 的调试日志记录相结合。

最常见的已知问题：

- 智能卡证书的信任链不完整-使用`enable_smartcard`脚本导入证书时，必须提供所有根证书和中间 CA 证书的完整列表。如果由于列表中缺少根 CA 证书而并非所有导入的证书都可信，则该`enable_smartcard`工具将显示错误，但它无法检测到何时缺少整个信任链或其中一个信任链中最内层的中间 CA 证书。在这种情况下，它将毫无错误地导入证书，但是智能卡证书或域控制器证书仍可能被视为不受信任。
- 缺少域控制器证书的信任链-如果域控制器证书由与智能卡不同的 CA 颁发（例如，通用访问卡 (CAC)），则需要将该 CA 信任链与颁发 CA 证书的智能卡一起导入。
- OCSP 响应器中缺乏 NONCE 扩展支持-Linux WorkSpaces 要求智能卡发卡机构的 OCSP 响应器启用 NONCE 扩展。如果无法启用，则必须完全禁用 OCSP 验证。
- 域控制器证书缺失 KDC `Authentication` EKU (OID 1.3.6.1.5.2.3.1)-要使智能卡身份验证起作用，需要重新颁发域控制器证书，以包括 KDC 身份验证 EKU。
- 域控制器证书已过期-要使智能卡身份验证起作用，必须保留域控制器证书 up-to-date。
- 使用弱映射方法将智能卡证书映射到 AD 中的用户——传统上， subjectAltName 属性中的 UPN 字段用于将证书映射到 AD 中的用户，并期望与 userPrincipalName 属性匹配。这不再被视为一种安全的映射方法，并且在默认情况下是不允许的。可以通过向`enable_smartcard`命令传递`--allow-weak-mapping`参数并在`/etc/skylight.conf`文件中的`[features]`部分中添加`smartcard_weak_mapping = true`行来重新启用它，但是更好的解决方案是使用一种强大的映射方法。有关更多详细信息，请参阅账户关联文档。

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

- `opensc-explorer`
- `opensc-tool`
- `pkcs11_inspect`
- `pkcs11_listcerts`

- `pkcs15-tool`

启用调试日志记录

- `/etc/sssd/sssd.conf`为每个单独的部分添加一`debug_level = LEVEL`行，其中`LEVEL`是所需的详细程度，从 1 到 10。然后可以在`/var/log/sssd/`目录中找到每个相应部分的日志。有关更多详细信息，请参阅此处和此处的 SSSD 文档。

为亚马逊 Linux 2 启用智能卡 WorkSpaces

> **Note**
>
> DCV WorkSpaces 上的 Amazon Linux 2 目前存在以下限制：
>
> - 不支持剪贴板、音频输入、视频输入和时区重定向。
> - 不支持多个显示器。

要在 Amazon Linux 2 上启用智能卡 WorkSpaces，您需要在 WorkSpace 镜像中包含 PEM 格式的根 CA 证书文件。

获取根 CA 证书

您可以通过以下几种方式获取根 CA 证书：

- 您可以使用由第三方证书颁发机构运营的根 CA 证书。
- 您可以使用 Web 注册网站导出自己的根 CA 证书，该网站为 `http://ip_address/certsrv` 或 `http://fqdn/certsrv`，其中 *`ip_address`* 和 *`fqdn`* 分别是根证书 CA 服务器的 IP 地址和完全限定域名 (FQDN)。有关使用 Web 注册网站的更多信息，请参阅 Microsoft 文档中的如何导出根证书颁发机构证书。
- 您可以使用以下步骤，从运行 Active Directory 证书服务 (AD CS) 的根 CA 证书服务器导出根 CA 证书。有关安装 AD CS 的信息，请参阅 Microsoft 文档中的安装证书颁发机构。

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

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

有关运行 certutil 的更多信息，请参阅 Microsoft 文档中的 certutil。

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

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

将您的根 CA 证书添加到您的亚马逊 Linux 2 WorkSpaces

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

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

以下过程说明了如何使用`enable_smartcard`脚本将根 CA 证书添加到 Amazon Linux 2 WorkSpaces 以及如何为亚马逊 Linux 2 启用智能卡 WorkSpaces。

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

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

> **Note**
>
> Amazon Linux 2 WorkSpaces 假设智能卡上的证书是针对用户的默认用户主体名称 (UPN) 颁发的，例如*sAMAccountName*@*domain*，其中*domain*是完全限定的域名 (FQDN)。

要使用备用 UPN 后缀，请参阅 `run /usr/lib/skylight/enable_smartcard --help`，了解更多信息。备用 UPN 后缀的映射对每个用户来说都是唯一的。因此，必须对每个用户单独执行映射 WorkSpace。

3. （可选）默认情况下，所有服务都允许在 Amazon Linux 2 上使用智能卡身份验证 WorkSpaces。要将智能卡身份验证仅限于特定服务，必须编辑 `/etc/pam.d/system-auth`。取消 `pam_succeed_if.so` 对应的 `auth` 行的注释，并根据需要编辑服务列表。

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

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

允许用户在 Firefox 中使用智能卡

您可以通过向您的亚马逊 Linux 2 WorkSpace 映像添加 SecurityDevices 策略来允许您的用户在 Firefox 中使用智能卡。有关向 Firefox 添加系统范围策略的更多信息，请参阅上的 Mozilla 策略模板。GitHub

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

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

问题排查

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

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

可能导致问题的一些常见问题：

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

通常，最好只有一个用于智能卡身份验证的证书，该证书映射到智能卡的第一个槽。

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

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

启用调试日志记录

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

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

3. 在 /etc/pam.d/system-auth-ac 文件中，编辑 auth 操作，并将 debug 或 debug_sensitive 参数添加到 pam_krb5.so。

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

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

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

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

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

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

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

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

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

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

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

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

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

为 WorkSpaces 个人版提供互联网访问权限

您的 WorkSpace 必须具有互联网的访问权限，以便您将更新安装到操作系统以及部署应用程序。您可以使用以下选项之一，以允许虚拟私有云 (VPC) 中的 WorkSpace 访问互联网。

选项

- 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 WorkSpaces。

有关这些选项的更多信息，请参阅 为 WorkSpaces 个人版配置 VPC。

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 Linux Extras 库

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

```
{
  "Statement": [
    {
        "Sid": "AmazonLinux2AMIRepositoryAccess",
        "Principal": "*",
        "Action": [
            "s3:GetObject"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::amazonlinux.*.amazonaws.com/*"
        ]
```

```
    }
  ]
}
```

WorkSpaces 个人安全组

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

> **Warning**
>
> 避免修改、删除或分离 _controllers 和 _workspacesMembers 安全组。修改或删除这些安全组时要小心，因为修改或删除这些安全组后，您将无法重新创建和重新添加它们。有关更多信息，请参阅适用于 Linux 实例的亚马逊 EC2安全组或适用于 Windows 实例的亚马逊 EC2 安全组。

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

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

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

向 WorkSpaces 目录中添加安全组

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在导航窗格中，选择目录。
3. 选择目录，然后选择 Actions、Update Details。
4. 展开 Security Group 并选择一个安全组。
5. 选择更新并退出。

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

向现有安全组添加安全组 WorkSpace

1. 查找需要更新的每 WorkSpace 个 IP 地址。
   a. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
   b. 展开每个 WorkSpace 并记录其 WorkSpace IP 地址。
2. 找到每个弹性网卡 WorkSpace 并更新其安全组分配。
   a. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
   b. 在网络与安全下，选择网络接口。
   c. 搜索您在步骤 1 中记录的第一个 IP 地址。
   d. 选择与该 IP 地址关联的 ENI，选择操作，然后选择更改安全组。
   e. 选择新安全组，然后选择保存。
   f. 根据需要对其他任何过程重复此过程 WorkSpaces。

WorkSpaces 个人版的 IP 访问控制组

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

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

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

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

> **Note**
>
> - IP 访问控制组不允许为 NAT 使用动态 IP 地址。如果您使用 NAT，请将其配置为使用静态 IP 地址而不是动态 IP 地址。确保 NAT 在 WorkSpace 会话期间通过同一静态 IP 地址路由所有 UDP 流量。
> - IP 访问控制组用于控制用户可将其流式传输会话连接到 WorkSpaces 的 IP 地址。用户仍然可以使用 Amazon WorkSpaces 的公共 API 从任何 IP 地址执行诸如重启、重建、关闭等功能。
> - 为目录配置用于流式传输的 VPC 端点时，IP 访问控制组不适用。
> - 更改 IP 访问控制时，活动会话不会立即中断；更改仅应用于新会话。

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

创建 IP 访问控制组

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

创建 IP 访问控制组

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择 IP Access Controls。
3. 选择 Create IP Group。
4. 在 Create IP Group (创建 IP 组) 对话框中，输入组的名称和描述，然后选择 Create (创建)。
5. 选择所需组，然后选择 Edit。
6. 对于每个 IP 地址，选择 Add Rule。对于 Source (来源)，输入 IP 地址或 IP 地址范围。对于说明，输入说明。添加完规则后，选择 Save。

将 IP 访问控制组与目录关联

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

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

将 IP 访问控制组与目录关联

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。
3. 选择目录，然后选择 Actions、Update Details。
4. 展开 IP Access Control Groups，并选择一个或多个 IP 访问控制组。
5. 选择更新并退出。

复制 IP 访问控制组

您可以使用现有的 IP 访问控制组作为创建新 IP 访问控制组的基础。

从现有的 IP 访问控制组创建一个 IP 访问控制组

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
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。

删除 IP 访问控制组

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

在可以删除 IP 访问控制组之前，必须将其与任何目录解除关联。

删除 IP 访问控制组

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。
3. 对于每个与 IP 访问控制组关联的目录，请选择该目录，然后选择 Actions、Update Details。展开 IP Access Control Groups (IP 访问控制组)，清除 IP 访问控制组的复选框，然后选择 Update and Exit (更新并退出)。

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

为 WorkSpaces 个人版设置 PCoIP 零客户端

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

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

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

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

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

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

WorkSpaces 在 WorkSpaces 个人版中为你的 Linux 启用 SSH 连接

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

要启用 SSH 连接，您可以创建新的安全组或更新现有安全组，然后添加规则以允许入站流量用于此目的。安全组用作相关实例的防火墙，可在实例级别控制入站和出站的数据流。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 Linux。 WorkSpaces有关更多信息，请参阅 the section called “安全组”。

有关视频教程，请参阅如何 WorkSpaces 使用 SSH 连接到我的 Linux Amazon？ 在 Amazon 知识中心上。本教程 WorkSpaces 仅适用于亚马逊 Linux 2。

内容

- 通过 SSH 连接到 Linux 的先决条件 WorkSpaces
- 启用与目录中所有 Linux WorkSpaces 的 SSH 连接
- 中基于密码的身份验证 WorkSpaces
- 启用与特定 Linux 的 SSH 连接 WorkSpace
- WorkSpace 使用 Linux 或 Putty 连接到 Linux

通过 SSH 连接到 Linux 的先决条件 WorkSpaces

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

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

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

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

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

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在导航窗格中，请选择 WorkSpaces。
3. 在列表中 WorkSpaces，选择 WorkSpace 要启用 SSH 连接的。
4. 在 “运行模式” 列中，确认 WorkSpace状态为 “可用”。
5. 单击 WorkSpace 名称左侧的箭头以显示行内摘要，并记下以下信息：
   - WorkSpace 知识产权。这是的私有 IP 地址 WorkSpace。

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

查找您连接到的 Active Directory 域的 NetBIOS 名称

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

启用与目录中所有 Linux WorkSpaces 的 SSH 连接

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

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

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中，选择 Security Groups（安全组）。
3. 选择创建安全组。
4. 键入安全组的名称（可选）和描述。
5. 对于 VP C，请选择 WorkSpaces 包含要启用 SSH 连接的 VPC。
6. 在 Inbound (入站) 选项卡上，选择 Add Rule (添加规则)，然后执行以下操作：
   - 对于 Type，选择 SSH。
   - 对于 Protocol (协议)，在您选择 SSH 时会自动指定 TCP。
   - 对于 Port Range (端口范围)，在您选择 SSH 时会自动指定 22。
   - 对于 “源”，指定用户将用于连接的计算机的公有 IP 地址的 CIDR 范围。 WorkSpaces例如，公司网络或家庭网络。
   - 对于 Description (描述)（可选），键入规则的描述。
7. 选择创建。
8. 将此安全组附加到您的 WorkSpaces。有关将此安全组添加到您的的更多信息 WorkSpaces，请参阅 WorkSpaces 个人安全组。如果您想自动将其他安全组附加到您的 WorkSpaces，请参阅此博客文章。

中基于密码的身份验证 WorkSpaces

在新创建的 Linux 中启用密码身份验证 WorkSpaces

1. 启动 WorkSpaces 客户端并登录到您的 WorkSpace。
2. 打开终端窗口。
3. 在终端窗口中，运行以下命令，以在 cloud-init 中启用 SSH 密码身份验证。

```
sudo bash -c 'touch /etc/cloud/cloud.cfg.d/15_sshpwauth.cfg && echo "ssh_pwauth:
 true" > /etc/cloud/cloud.cfg.d/15_sshpwauth.cfg && sudo rm /var/lib/cloud/
instance/sem/config_set_passwords && sudo cloud-init single --name set-passwords'
```

该脚本将执行以下操作：

- 在 cloud-init 目录 `/etc/cloud/cloud.cfg.d/` 中创建配置文件。
- 修改配置文件，以告知 cloud-init 启用 SSH 密码身份验证。
- 重置 `set-passwords` cloud-init 模块，使其可以再次运行。
- 单独运行 `set-passwords` cloud-init 模块。这会将启用 SSH 密码身份验证的文件写入 SSH 配置目录 `/etc/ssh/sshd_config.d/`，然后重新启动 SSHD，以便立即进行设置。

这将对您启用 SSH 密码身份验证 WorkSpace ，并且将在自定义映像中保留。如果您仅在 SSHD 配置文件中启用 SSH 密码身份验证，而不配置 cloud-init，则在某些 Linux 上，该设置将无法通过映像保留。 WorkSpaces有关更多信息，请参阅 cloud-init 模块文档中的设置密码。

在现有 Linux 中禁用密码身份验证 WorkSpaces

1. 启动 WorkSpaces 客户端并登录到您的 WorkSpace。
2. 打开终端窗口。
3. 在终端窗口中，运行以下命令，以在 cloud-init 中禁用 SSH 密码身份验证。

```
sudo bash -c 'touch /etc/cloud/cloud.cfg.d/15_sshpwauth.cfg && echo "ssh_pwauth:
 false" > /etc/cloud/cloud.cfg.d/15_sshpwauth.cfg && sudo rm /var/lib/cloud/
instance/sem/config_set_passwords && sudo cloud-init single —name set-passwords'
```

该脚本将执行以下操作：

- 在 cloud-init 目录 `/etc/cloud/cloud.cfg.d/` 中创建配置文件。
- 修改配置文件，以告知 cloud-init 禁用 SSH 密码身份验证。
- 重置 `set-passwords` cloud-init 模块，使其可以再次运行。
- 单独运行 `set-passwords` cloud-init 模块。这会将启用 SSH 密码身份验证的文件写入 SSH 配置目录 `/etc/ssh/sshd_config.d/`，然后重新启动 SSHD，以便立即进行设置。

这会立即禁用中的 SSH， WorkSpace 并且将在自定义映像中保留。

启用与特定 Linux 的 SSH 连接 WorkSpace

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

向现有安全组添加规则以允许入站 SSH 流量流向特定 Linux WorkSpace

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

WorkSpace 使用 Linux 或 Putty 连接到 Linux

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

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

WorkSpace 使用 Linux 连接到 Linux

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

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

   以下是 SSH 命令的示例，其中：

   - *NetBIOS_NAME*是任何公司
   - 这*Username* 是 janedoe
   - 这*WorkSpace IP*是 203.0.113.25

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

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

WorkSpace 使用 Putty 连接到 Linux

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

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

```
NetBIOS_NAME\Username@WorkSpaceIP
```

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

   有关 SSH 命令的示例，请参阅上一过程中的步骤 1。

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

WorkSpaces 个人版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。

- the section called “路由表配置”
- the section called “Windows 组件”
- the section called “Linux 组件”
- the section called “Ubuntu 组件”
- the section called “Rocky Linux 组件 ”
- the section called “Red Hat Enterprise Linux 的组件 ”

必需路由表配置

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 Amazon Support 或 Amazon 客户团队。

Windows 所需的服务组件

在 Windows WorkSpaces 上，这些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，请确保它不会干扰安装在以下位置的服务组件。

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

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

- C:\Program Files\Amazon

- C:\ProgramData\Amazon

32 位 PCoIP 代理

自 2021 年 3 月 29 日起，我们将 PCoIP 代理从 32 位更新为 64 位。对于使用 PCoIP 协议的 Windows WorkSpaces，这意味着 Teradici 文件的位置已从 `C:\Program Files (x86)\Teradici` 更改为 `C:\Program Files\Teradici`。由于我们在常规维护时段内更新了 PCoIP 代理，因此在过渡期间，您的一些 WorkSpaces 使用 32 位代理的时间可能比其他 WorkSpaces 更长。

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

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

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

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

Linux 所需的服务组件

在 Amazon Linux WorkSpaces 上，这些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。

> **Note**
>
> 对 `/etc/pcoip-agent/pcoip-agent.conf` 以外的其他文件进行更改可能会导致您的 WorkSpaces 停止运行，并可能需要您对其进行重建。有关修改 `/etc/pcoip-agent/`

pcoip-agent.conf 的信息，请参阅 WorkSpaces 在 WorkSpaces 个人版中管理你的 Amazon Linux 2。

- /etc/dhcp/dhclient.conf
- /etc/logrotate.d/pcoip-agent
- /etc/logrotate.d/pcoip-server
- /etc/os-release
- /etc/pam.d/pcoip
- /etc/pam.d/pcoip-session
- /etc/pcoip-agent
- /etc/profile.d/system-restart-check.sh
- /etc/X11/default-display-manager
- /etc/yum/pluginconf.d/halt_os_update_check.conf
- /etc/systemd/system/euc-analytic-agent.service
- /lib/systemd/system/pcoip.service
- /lib/systemd/system/pcoip-agent.service
- /lib64/security/pam_self.so
- /usr/bin/pcoip-fne-view-license
- /usr/bin/pcoip-list-licenses
- /usr/bin/pcoip-validate-license
- /usr/bin/euc-analytics-agent
- /usr/lib/firewalld/services/pcoip-agent.xml
- /usr/lib/modules-load.d/usb-vhci.conf
- /usr/lib/pcoip-agent
- /usr/lib/skylight
- /usr/lib/systemd/system/pcoip.service
- /usr/lib/systemd/system/pcoip.service.d/
- /usr/lib/systemd/system/skylight-agent.service
- /usr/lib/tmpfiles.d/pcoip-agent.conf

- /usr/lib/yum-plugins/halt_os_update_check.py
- /usr/sbin/pcoip-agent
- /usr/sbin/pcoip-register-host
- /usr/sbin/pcoip-support-bundler
- /usr/share/doc/pcoip-agent
- /usr/share/pcoip-agent
- /usr/share/selinux/packages/pcoip-agent.pp
- /usr/share/X11
- /var/crash/pcoip-agent
- /var/lib/pcoip-agent
- /var/lib/skylight
- /var/log/pcoip-agent
- /var/log/skylight
- /var/logs/wsp
- /var/log/eucanalytics

Ubuntu 所需的服务组件

在 Ubuntu WorkSpaces 上，这些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/X11/default-display-manager
- /etc/dcv
- /etc/default/grub.d/zz-hibernation.cfg
- /etc/netplan
- /etc/os-release
- /etc/pam.d/dcv
- /etc/pam.d/dcv-graphical-sso
- /etc/sssd/sssd.conf
- /etc/wsp

- /etc/systemd/system/euc-analytic-agent.service
- /lib64/security/pam_self.so
- /usr/lib/skylight
- /usr/lib/systemd/system/dcvserver.service
- /usr/lib/systemd/system/dcvsessionlauncher.service
- /usr/lib/systemd/system/skylight-agent.service
- /usr/lib/systemd/system/wspdcvhostadapter.service
- /usr/share/X11
- /usr/bin/euc-analytics-agent
- /var/lib/skylight
- /var/log/skylight
- /var/log/eucanalytics

Rocky Linux 所需的服务组件

在 Red Hat Enterprise Linux WorkSpaces 上，这些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/dcv
- /etc/os-release
- /etc/pam.d/dcv-graphical-sso
- /etc/pam.d/dcv
- /etc/systemd/system/euc-analytic-agent.service
- /etc/wsp
- /usr/bin/euc-analytics-agent
- /usr/lib/skylight
- /usr/lib/systemd/system/dcvserver.service
- /usr/lib/systemd/system/dcvsessionlauncher.service
- /usr/lib/systemd/system/skylight-agent.service
- /usr/lib/systemd/system/wspdcvhostadapter.service

- /usr/lib/systemd/system/xdcv-console.path
- /usr/lib/systemd/system/xdcv-console.service
- /usr/lib/systemd/system/xdcv-console-update.service
- /usr/share/X11
- /var/lib/skylight
- /var/log/eucanalytics
- /var/log/skylight

Red Hat Enterprise Linux 的必需服务组件

在 Red Hat Enterprise Linux WorkSpaces 上，这些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/dcv
- /etc/os-release
- /etc/pam.d/dcv-graphical-sso
- /etc/pam.d/dcv
- /etc/systemd/system/euc-analytic-agent.service
- /etc/wsp
- /usr/bin/euc-analytics-agent
- /usr/lib/skylight
- /usr/lib/systemd/system/dcvserver.service
- /usr/lib/systemd/system/dcvsessionlauncher.service
- /usr/lib/systemd/system/skylight-agent.service
- /usr/lib/systemd/system/wspdcvhostadapter.service
- /usr/lib/systemd/system/xdcv-console.path
- /usr/lib/systemd/system/xdcv-console.service
- /usr/lib/systemd/system/xdcv-console-update.service
- /usr/share/X11
- /var/log/eucanalytics
- /var/log/skylight

管理 WorkSpaces 个人版的目录

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。
- Amazon Managed Microsoft AD - 创建在 Amazon 上托管的 Microsoft Active Directory。
- Simple AD - 创建与 Microsoft Active Directory 兼容的目录，该目录由 Samba 4 提供支持，并在 Amazon 上托管。
- Cross trust - 在您的 Amazon Managed Microsoft AD 目录与本地域之间创建信任关系。
- Microsoft Entra ID - 创建一个使用 Microsoft Entra ID 作为其身份源的目录（通过 IAM Identity Center）。目录中的个人 WorkSpaces 使用 Microsoft Entra 的本机身份验证加入，并通过 Microsoft Windows Autopilot 用户驱动模式注册到 Microsoft Intune。使用 Microsoft Entra ID 的目录仅支持 Windows 10 和 11 自带许可 WorkSpaces。
- 自定义 - 创建一个使用您选择的身份提供者的目录（通过 IAM Identity Center）。目录中的 WorkSpaces 使用您选择的设备管理解决方案（例如 JumpCloud）进行管理。使用自定义身份提供者的目录仅支持 Windows 10 和 11 自带许可 WorkSpaces。

有关演示如何设置这些目录和启动 WorkSpace 的教程，请参阅为 WorkSpaces 个人版创建目录。

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

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

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

WorkSpaces 将失败。复制区域内的 Amazon WorkSpaces 不支持使用 Amazon Managed Microsoft AD 进行多区域复制。

- Simple AD 和 AD Connector 供您免费使用，可用于 WorkSpaces。如果连续 30 天没有一起使用 WorkSpaces 与您的 Simple AD 或 AD Connector 目录，则系统将自动取消注册该目录，无法再将其用于 Amazon WorkSpaces，而且将根据 Amazon Directory Service 定价条款向您收取该目录的费用。

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

目录

- 向 WorkSpaces 个人版注册现有 Amazon Directory Service 目录
- 为 WorkSpaces 个人版选择组织部门
- 为 WorkSpaces 个人版配置自动公有 IP 地址
- 控制对 WorkSpaces 个人版的设备访问
- 管理 WorkSpaces 个人版的本地管理员权限
- 更新 WorkSpaces 个人版的 AD Connector 账户（AD Connector）
- WorkSpaces 个人版的多重身份验证（AD Connector）
- 为 WorkSpaces 个人版创建目录
- 更新 WorkSpaces 个人版的 DNS 服务器
- 删除 WorkSpaces 个人版目录
- 为 WorkSpaces 个人设置 Active Directory 管理工具

向 WorkSpaces 个人版注册现有 Amazon Directory Service 目录

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

要求

要注册要在 WorkSpaces 中使用的目录，必须满足以下要求：

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

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

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

注册现有 Amazon Directory Service 目录

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。
3. 选择创建目录。
4. 在创建目录页面，对于 WorkSpaces 类型，选择个人。对于 WorkSpace 设备管理，选择 Amazon Directory Service。
5. 选择您要在 Amazon Directory Service 中的目录表中注册的目录
6. 选择来自不同可用区的 VPC 的两个子网。这些子网将用于启动您的 WorkSpaces。有关更多信息，请参阅 WorkSpaces 个人版的可用区。

   > **Note**
   >
   > 如果您不知道要选择哪些子网，请选择无首选项。

7. 对于启用自助服务权限，选择是以使用户能够重建其 WorkSpaces、更改卷大小、计算类型和运行模式。启用操作可能会影响您为 Amazon WorkSpaces 支付的费用。否则，请选择否。
8. 选择 Register。Registered 最初的值是 `REGISTERING`。注册完成后，该值为 `Yes`。

注册 Amazon Directory Service 目录后，您可以创建个人 WorkSpace。有关更多信息，请参阅 在 WorkSpaces 个人版中创建 WorkSpace。

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《Amazon Directory Service 管理指南》中的删除您的目录。

取消注册目录

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。
3. 选择目录。
4. 选择 Actions、Deregister。
5. 当系统提示进行确认时，选择 Confirm。取消注册完成后，该目录将取消注册并从列表中删除。

为 WorkSpaces 个人版选择组织部门

> **Note**
>
> 此功能仅适用于通过 Amazon Directory Service（包括 AD Connector、Amazon Managed Microsoft AD 和 Simple AD）管理的目录。

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

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。

选择组织单位

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。
3. 选择您的目录。
4. 在“目标域和组织部门”下，选择编辑。
5. 要查找 OU，您可以在“目标和组织部门”下，开始键入 OU 的全部或部分名称，然后选择要使用的 OU。
6. （可选）选择 OU 的区分名称，使用自定义 OU 覆盖您选择的 OU。
7. 选择保存。
8. (可选) 重建现有的 WorkSpace 以更新 OU。有关更多信息，请参阅 重建 WorkSpaces 个人版中的 WorkSpace。

为 WorkSpaces 个人版配置自动公有 IP 地址

在自动分配公有 IP 地址后，系统将从 Amazon 提供的公有地址池中为您启动的每个 WorkSpace 分配一个公有 IP 地址。如果公有子网中的 WorkSpace 具有公有 IP 地址，则其能够通过互联网网关访问互联网。在启用自动分配功能之前已经存在的 WorkSpaces 不会收到公有地址，直到您重新构建它们。

请注意，如果您的 WorkSpaces 处于私有子网中并且您为虚拟私有云(VPC) 配置了 NAT 网关，或者如果您的 WorkSpaces 位于公有子网中并且您手动为其分配了弹性 IP 地址，则无需自动分配公有地址。有关更多信息，请参阅 为 WorkSpaces 个人版配置 VPC。

> **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。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. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。
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. 选择更新。

控制对 WorkSpaces 个人版的设备访问

您可以根据设备平台指定有权访问 WorkSpaces 的设备类型。您可以使用证书将 WorkSpaces 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. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。

3. 选择您的目录。
4. 在“访问控制”选项下，选择编辑。
5. 在“可信设备”下，选择全部允许、可信设备或全部拒绝，以指定哪些设备类型可以访问 WorkSpaces。有关更多信息，请参阅 将 WorkSpaces 个人版访问限定于受信任设备。
6. 选择 Save。

管理 WorkSpaces 个人版的本地管理员权限

> **Note**
>
> 此功能仅适用于通过 Amazon Directory Service（包括 AD Connector、Amazon Managed Microsoft AD 和 Simple AD）管理的目录。

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. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。
3. 选择您的目录。
4. 在“本地管理员设置”下，选择编辑。
5. 要确保用户为本地管理员，请选择启用本地管理员设置。
6. 选择 Save。

更新 WorkSpaces 个人版的 AD Connector 账户（AD Connector）

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

更新 AD Connector 账户

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。

3. 选择您的目录，然后选择查看详细信息。
4. 在 AD Connector 账户下，选择编辑。
5. 输入新账户的登录凭证。
6. 选择保存。

WorkSpaces 个人版的多重身份验证（AD Connector）

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

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

启用多重身份验证

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。
3. 选择您的目录，然后选择 Actions、Update Details。
4. 展开 Multi-Factor Authentication，然后选择 Enable Multi-Factor Authentication。
5. 对于 RADIUS server IP address(es)，键入您的 RADIUS 服务器端点的 IP 地址，以逗号隔开，或键入您的 RADIUS 服务器负载均衡器的 IP 地址。
6. 对于 Port，键入 RADIUS 服务器用来通信的端口。您的本地网络必须允许默认 RADIUS 服务器端口 (1812) 上来自 AD Connector 的入站流量。
7. 对于 Shared secret code 和 Confirm shared secret code，键入您的 RADIUS 服务器的共享密码。
8. 对于 Protocol，为您的 RADIUS 服务器选择协议。
9. 对于 Server timeout，键入等待 RADIUS 服务器作出响应的时间 (以秒为单位)。该值必须在 1 到 50 之间。
10. 对于 Max retries，键入尝试与 RADIUS 服务器通信的最多次数。该值必须在 0 到 10 之间。
11. 选择更新并退出。

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

为 WorkSpaces 个人版创建目录

WorkSpaces 个人版允许您使用通过 Amazon Directory Service 托管的目录，来存储和管理 WorkSpace 及用户的相关信息。使用以下选项创建 WorkSpaces 个人版目录：

- 创建 Simple AD 目录。
- 创建 Amazon Directory Service for Microsoft Active Directory，也称为 Amazon 托管的 Microsoft AD。
- 使用 Active Directory Connector 连接到现有 Microsoft Active Directory。
- 在 Amazon 托管的 Microsoft AD 目录与本地域之间创建信任关系。
- 创建一个专用 Microsoft Entra ID WorkSpaces 目录。
- 创建专用的自定义 WorkSpaces 目录。

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

创建目录前的工作

- WorkSpaces 并非在所有区域均可用。请确认受支持的区域，并为您的 WorkSpaces 选择一个区域。有关受支持区域的更多信息，请参阅按 Amazon 区域划分的 WorkSpaces 定价。
- 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 WorkSpaces 个人版配置 VPC。必须通过虚拟专用网络 (VPN) 连接或 Amazon Direct Connect 将 VPC 连接到您的本

地网络。有关更多信息，请参阅《Amazon Directory Service 管理指南》中的 AD Connector 先决条件。

- 从 WorkSpace 提供对互联网的访问。有关更多信息，请参阅 为 WorkSpaces 个人版提供互联网访问权限。

有关如何删除空目录的信息，请参阅删除 WorkSpaces 个人版目录。如果您删除了 Simple AD 或 AD Connector 目录，则当您想重新开始使用 WorkSpaces 时，可以随时创建一个新的目录。

目录

- 确定 WorkSpaces 个人版目录的计算机名称
- 为 WorkSpaces 个人版创建 Amazon 托管 Microsoft AD 目录
- 为 WorkSpaces 个人创建一个 Simple AD 目录
- 为 WorkSpaces 个人版创建 AD Connector
- 在 Amazon 托管的 Microsoft AD 目录与本地域之间创建 WorkSpaces 个人版的信任关系
- 使用个人版创建专用的 Microsoft Entra ID 目录 WorkSpaces
- 使用 “个 WorkSpaces 人” 创建专用的自定义目录

确定 WorkSpaces 个人版目录的计算机名称

根据您启动的 WorkSpace 类型（Amazon Linux、Ubuntu 或 Windows），Amazon WorkSpaces 控制台中为 WorkSpace 显示的计算机名称值会有所不同。WorkSpace 的计算机名称可以采用以下一种格式：

- Amazon Linux：A-*xxxxxxxxxxxxx*
- Red Hat Enterprise Linux：R-*xxxxxxxxxxxxx*
- Rocky Linux：R-*xxxxxxxxxxxxx*
- Ubuntu：U-*xxxxxxxxxxxxx*
- Windows：IP-C*xxxxxx* 或 WSAMZN-*xxxxxxx* 或 EC2AMAZ-*xxxxxxx*

对于 Windows WorkSpaces，计算机名称格式由捆绑包类型决定；对于从公共捆绑包或基于公共映像的自定义捆绑包创建的 WorkSpaces，则由创建公共映像的时间决定。

从 2020 年 6 月 22 日起，从公共捆绑包中推出的 Windows WorkSpaces 的计算机名称采用 WSAMZN-*xxxxxxx* 格式，而不是 IP-C*xxxxxx* 格式。

对于基于公共映像的自定义捆绑包，如果公共映像是在 2020 年 6 月 22 日之前创建的，则计算机名称采用 EC2AMAZ-*xxxxxxx* 格式。如果公共映像是在 2020 年 6 月 22 日当天或之后创建的，则计算机名称采用 WSAMZN-*xxxxxxx* 格式。

对于自带许可 (BYOL) 捆绑包，默认情况下，计算机名称使用 DESKTOP-*xxxxxxx* 或 EC2AMAZ-*xxxxxxx* 格式。

如果您在自定义或 BYOL 捆绑包中为计算机名称指定了自定义格式，则您的自定义格式将覆盖这些默认格式。要指定自定义格式，请参阅为 WorkSpaces 个人版创建自定义 WorkSpaces 图片和捆绑包。

> **Important**
>
> 创建 WorkSpace 后，您可以放心地更改其计算机名称。例如，您可以在 WorkSpace 上使用命令 `Rename-Computer` 或远程执行 PowerShell 脚本。然后，更新后的 WorkSpace 计算机名称值将显示在 Amazon WorkSpaces 控制台中。

为 WorkSpaces 个人版创建 Amazon 托管 Microsoft AD 目录

在本教程中，我们将创建 Amazon 托管 Microsoft AD 目录。要了解使用其他选项的教程，请参阅为 WorkSpaces 个人版创建目录。

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

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

创建 Amazon 托管的 Microsoft AD 目录

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。

2. 在导航窗格中，选择目录。
3. 选择创建目录。
4. 在创建目录页面，对于 WorkSpaces 类型，选择个人。然后，对于 WorkSpace 设备管理，选择 Amazon Directory Service。
5. 选择创建目录，这将打开 Amazon Directory Service 上的设置目录页面
6. 选择 Amazon 托管 Microsoft AD，然后选择下一步。
7. 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 WorkSpaces 个人版的 DNS 服务器中的步骤操作，确保您的 WorkSpaces 得到正确更新。

   c. 对于 NetBIOS 名称，为目录输入一个短名称（例如，workspaces）。
   d. 对于 Admin 密码和确认密码，输入目录管理员账户的密码。有关密码要求的更多信息，请参阅《Amazon Directory Service 管理指南》中的创建您的 Amazon Managed Microsoft AD 目录。
   e. （可选）对于描述，输入目录的描述。
   f. 对于 VPC，选择您创建的 VPC。
   g. 对于 Subnets，选择两个私有子网 (具有 CIDR 块 `10.0.1.0/24` 和 `10.0.2.0/24`)。
   h. 选择下一步。
8. 选择创建目录。
9. 您将返回到 WorkSpaces 控制台上的“创建目录”页面。目录的初始状态是 `Requested`，然后是 `Creating`。目录创建完成后（这可能需要几分钟），状态会变为 `Active`。

创建了 Amazon 托管 Microsoft AD 目录后，您可以将其注册到 Amazon WorkSpaces。有关更多信息，请参阅 向 WorkSpaces 个人版注册现有 Amazon Directory Service 目录。

为 WorkSpaces 个人创建一个 Simple AD 目录

在本教程中，我们将启动使用 Sim WorkSpace ple AD 的。要了解使用其他选项的教程，请参阅为 WorkSpaces 个人版创建目录。

> **Note**
>
> - Simple AD 并非在所有Amazon地区都可用。请查看受支持的区域，并为您的 Simple AD 目录选择一个区域。有关 Simple AD 支持的区域的更多信息，请参阅 AmazonDirectory Service 的区域可用性。
> - Simple AD 可供您免费使用 WorkSpaces。如果连续 30 天 WorkSpaces 未在您的 Simple AD 目录中使用，则该目录将自动取消注册以供亚马逊使用 WorkSpaces，并且将根据Amazon Directory Service定价条款向您收取该目录的费用。
> - S@@ imple AD 目前仅支持 IPv4 寻址，这意味着在创建目录时，关联的 VPC 将配置 IPv4 CIDR 块，并且不支持 IPv6 网络。

当你创建 Simple AD 目录时。 Amazon Directory Service创建两个目录服务器，分别位于您的 VPC 的私有子网中。目录最初没有任何用户。在创建用户之后添加用户 WorkSpace。有关更多信息，请参阅在 WorkSpaces 个人版中创建 WorkSpace。

创建 Simple AD 目录

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在导航窗格中，选择目录。
3. 选择创建目录。
4. 在 “创建目录” 页面上，为WorkSpaces 类型选择 “个人”。然后，要进行WorkSpace 设备管理，请选择 AmazonDirectory Service。
5. 选择 “创建目录”，这将打开 Directory Service 上的 “设置Amazon目录” 页面
6. 选择 Simple AD，然后选择下一步。
7. 按以下说明配置目录：
   a. 在组织名称中，输入目录的唯一组织名称（例如， my-example-directory）。此名称的字符数不得少于 4 个，仅包含字母数字字符和连字符 (-)，并以连字符以外的其他字符开头或结尾。
   b. 对于目录 DNS 名称，输入目录的完全限定名称（例如，example.com）。

> **Important**
>
> 如果您需要在启动后更新 DNS 服务器 WorkSpaces，请按照中的步骤进行操作，更新 WorkSpaces 个人版的 DNS 服务器以确保正确更新 WorkSpaces 您的服务器。

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《Amazon Directory Service 管理指南》中的如何创建 Microsoft AD 目录。

e. （可选）对于描述，输入目录的描述。

f. 对于目录大小，选择小。

g. 对于 VPC，选择您创建的 VPC。

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

i. 选择下一步。

8. 选择创建目录。

9. 您将返回到 WorkSpaces 控制台上的 “创建目录” 页面。目录的初始状态是 `Requested`，然后是 `Creating`。目录创建完成后（这可能需要几分钟），状态会变为 `Active`。

在目录创建期间发生的情况

WorkSpaces 代表您完成以下任务：

- 创建 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 中设置一个 Simple AD 目录，用于存储用户和WorkSpace 信息。此目录的管理员账户具有用户名 Administrator 和指定的密码。
- 创建两个安全组，一个用于目录控制器，另一个用于目录 WorkSpaces 中的安全组。

创建 Simple AD 目录后，您可以将其注册到亚马逊 WorkSpaces。有关更多信息，请参阅 向 WorkSpaces 个人版注册现有 Amazon Directory Service 目录。

为 WorkSpaces 个人版创建 AD Connector

在本教程中，我们将创建 AD Connector。要了解使用其他选项的教程，请参阅为 WorkSpaces 个人版创建目录。

创建 AD Connector

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

创建 AD Connector

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。
3. 选择创建目录。
4. 在创建目录页面，对于 WorkSpaces 类型，选择个人。然后，对于 WorkSpace 设备管理，选择 Amazon Directory Service。
5. 选择创建目录，这将打开 Amazon Directory Service 上的设置目录页面
6. 选择 Amazon 托管 Microsoft AD，然后选择下一步。
7. 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。
8. 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）。
9. 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）。
10. 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。
11. 对于 Connector 账户密码和确认密码，输入本地用户的密码。
12. 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 WorkSpaces 个人版的 DNS 服务器中的步骤操作，确保您的 WorkSpaces 得到正确更新。

13. （可选）对于描述，输入目录的描述。
14. 保持 Size 为 Small。
15. 对于 VPC，选择您的 VPC。
16. 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。
17. 选择创建目录。
18. 您将返回到 WorkSpaces 控制台上的“创建目录”页面。目录的初始状态是 `Requested`，然后是 `Creating`。目录创建完成后（这可能需要几分钟），状态会变为 `Active`。

在 Amazon 托管的 Microsoft AD 目录与本地域之间创建 WorkSpaces 个人版的信任关系

在本教程中，我们将在 Amazon 托管的 Microsoft AD 目录与本地域之间创建信任关系。要了解使用其他选项的教程，请参阅为 WorkSpaces 个人版创建目录。

> **Note**
>
> 当 Amazon Managed Microsoft AD 配置有与本地目录的信任关系时，在单独的受信任域中通过 Amazon Web Services 账户启动 WorkSpaces 的情况下可以使用该 AD。但是，使用 Simple AD 或 AD Connector 的 WorkSpaces 无法为受信任域中的用户启动 WorkSpaces。

设置信任关系

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

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

2. 在 Amazon 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《Amazon Directory Service 管理指南》中的教程：创建 Amazon Managed Microsoft AD 与本地域之间的信任关系。

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

> **Note**
>
> - Red Hat Enterprise Linux、Rocky Linux 和 Ubuntu WorkSpaces 使用系统安全服务进程守护程序（SSSD）进行 Active Directory 集成，SSSD 不支持林信任。改为配置外部信任。建议对 Amazon Linux、Ubuntu、Rocky Linux 和 Red Hat Enterprise Linux WorkSpaces 使用双向信任。
> - 您不能使用 Web 浏览器（Web Access）连接到 Linux WorkSpaces。

使用个人版创建专用的 Microsoft Entra ID 目录 WorkSpaces

在本教程中，我们创建了自带许可证 (BYOL) Windows 10 和 11 个人版 WorkSpaces ，它们是加入并注册微软 Intune 的微软 Entra ID。在创建此类目录之前 WorkSpaces，您需要先为 Entra ID-WorkSpaces joined 创建一个专用的 WorkSpaces 个人目录。

> **Note**
>
> 除非洲（开普敦）、以色列（特拉维夫）和中国（宁夏）外，Microsoft Entra 已加入个人 WorkSpaces 版可在亚马逊 WorkSpaces 提供服务的所有Amazon地区使用。

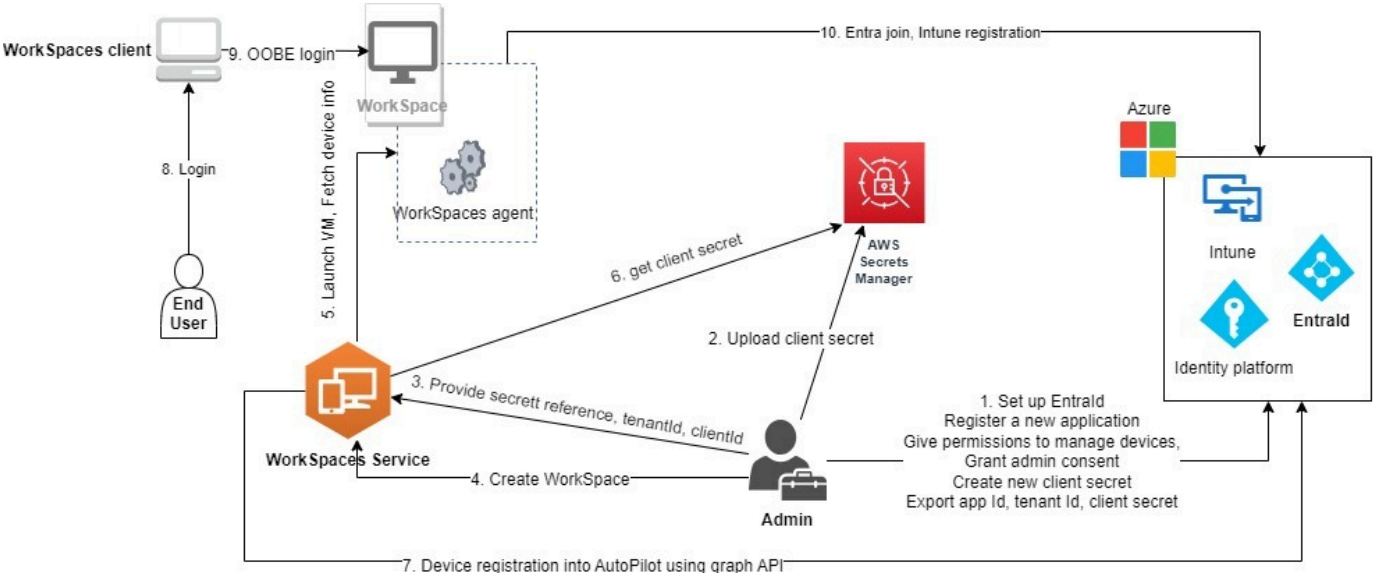
内容

- 概述
- 要求和限制
- 步骤 1：启用 IAM Identity Center 并与 Microsoft Entra ID 同步
- 步骤 2：注册 Microsoft Entra ID 应用程序以授予 Windows Autopilot 权限
- 步骤 3：配置 Windows Autopilot 用户驱动模式
- 步骤 4：创建Amazon Secrets Manager密钥

- 第 5 步：创建专用的微软 Entra ID 目录 WorkSpaces
- 为 WorkSpaces 目录配置 IAM 身份中心应用程序（可选）
- 创建跨区域 IAM Identity Center 集成（可选）

概述

微软 Entra ID 个人 WorkSpaces 目录包含启动已加入的 Microsoft Entra ID 所需的所有信息 WorkSpaces ，这些信息已分配给使用微软 Entra ID 管理的用户。用户信息 WorkSpaces 通过 Amazon IAM Identity Center 提供，该中心充当身份代理，将您的员工身份从 Entra ID 带到Amazon。微软 Windows Autopilot 用户驱动模式用于完成 WorkSpaces Intune 注册和 Entra 加入。下图说明了 Autopilot 过程。



要求和限制

- Microsoft Entra ID P1 计划或更高版本。
- Microsoft Entra ID 和 Intune 已启用并具有角色分配。
- Intune 管理员 - 管理 Autopilot 部署配置文件所必需的。
- 全局管理员 - 为分配给步骤 3 中创建的应用程序的 API 权限授予管理员同意所必需的。无需此权限即可创建应用程序。但是，全局管理员需要提供管理员对应用程序权限的同意。
- 向你的用户分配 Windows 10/11 VDA E3 或 E5 用户订阅许可证。 WorkSpaces
- Entra ID 目录仅支持 Windows 10 或 11 个人 WorkSpaces自带许可证。以下是受支持的版本。
  - Windows 10 版本 21H2（2021 年 12 月更新）
  - Windows 10 版本 22H2（2022 年 11 月更新）

- Windows 11 Enterprise 23H2（2023 年 10 月发布）
- Windows 11 Enterprise 22H2（2022 年 10 月发布）
- Windows 11 Enterprise 24H2（2024 年 10 月发布）
- 您的帐户已启用自带许可证 (BYOL)，并且您的Amazon帐户中已导入有效的 Windows 10 或 11 BYOL 映像。有关更多信息，请参阅 带上你自己的 Windows 桌面许可证 WorkSpaces。
- 微软 Entra ID 目录仅支持 Windows 10 或 11 BYOL 个人版。 WorkSpaces
- Microsoft Entra ID 目录仅支持 DCV 协议。
- 如果你使用防火墙 WorkSpaces，请确保它不会阻止 Microsoft Intune 和 Windows Autopilot 端点的出站流量。有关详细信息，请参阅 Network endpoints for Microsoft Intune - Microsoft Intune 和 Windows Autopilot requirements。
- Microsoft Entra ID 目录不支持位于美国政府社区云高级服务（GCCH）和美国国防部（DoD）环境中的 Microsoft Entra ID 租户。

步骤 1：启用 IAM Identity Center 并与 Microsoft Entra ID 同步

要创建 Microsoft Entra ID 加入 Microsoft Entra ID 的个人 WorkSpaces 信息并将其分配给你的 Entra ID 用户，你必须Amazon通过 IAM 身份中心向其提供用户信息。推荐使用 Amazon IAM 身份中心来管理用户对Amazon资源的访问权限。有关更多信息，请参阅什么是 IAM Identity Center？。这是一次性设置。

如果您没有可与您的集成的现有 IAM Identity Center 实例 WorkSpaces，我们建议您在与您的相同区域创建一个 WorkSpaces。如果您在其他地区拥有现有的 Amazon Identity Center 实例，则可以设置跨区域集成。有关跨区域设置的更多信息，请参阅the section called “ 创建跨区域 IAM Identity Center 集成（可选）”。

> **Note**
>
> 中不支持 WorkSpaces 和 IAM 身份中心之间的跨区域集成。Amazon GovCloud (US) Region

1. 在您Amazon的 Organizations 中启用 IAM Identity Center，尤其是在您使用多账户环境的情况下。您还可以创建 IAM Identity Center 账户实例。要了解更多信息，请参阅启用 Amazon IAM 身份中心。每个 WorkSpaces 目录可以与一个 IAM Identity Center 实例、组织或账户相关联。

   如果您正在使用组织实例并尝试在其中一个成员账户中创建 WorkSpaces 目录，请确保您拥有以下 IAM Identity Center 权限。

- "sso:DescribeInstance"
- "sso:CreateApplication"
- "sso:PutApplicationGrant"
- "sso:PutApplicationAuthenticationMethod"
- "sso:DeleteApplication"
- "sso:DescribeApplication"
- "sso:getApplicationGrant"

有关更多信息，请参阅管理对 IAM Identity Center 资源的访问权限概览。此外，请确保没有服务控制策略 (SCPs) 阻止这些权限。要了解更多信息 SCPs，请参阅服务控制策略 (SCPs)。

2. 配置 IAM Identity Center 和 Microsoft Entra ID，自动将您 Entra ID 租户中的选定或所有用户同步到 IAM Identity Center 实例。有关更多信息，请参阅使用 Microsoft Entra ID 和 IAM 身份中心配置 SAML 和 SCIM 和教程：配置 Amazon IAM 身份中心以实现自动用户配置。
3. 验证你在 Microsoft Entra ID 上配置的用户是否已正确同步到 Amazon IAM 身份中心实例。如果您在 Microsoft Entra ID 中看到错误消息，则表明 Entra ID 中用户的配置方式是 IAM Identity Center 不支持的方式。该错误消息将会识别出此问题。例如，如果 Entra ID 中的用户对象缺少名字、 and/or 姓氏和显示名称，您将收到一条类似的错误消息。`"2 validation errors detected: Value at 'name.givenName' failed to satisfy constraint: Member must satisfy regular expression pattern: [\\p{L}\\p{M}\\p{S}\\p{N}\\p{P}\\t\\n\\r ]+; Value at 'name.givenName' failed to satisfy constraint: Member must have length greater than or equal to 1"`相关详情，请参阅特定用户无法从外部 SCIM 提供者同步到 IAM Identity Center。

> **Note**
>
> WorkSpaces 使用 Entra ID UserPrincipalName (UPN) 属性来识别单个用户，其局限性如下：
>
> - UPNs 长度不能超过 63 个字符。
> - 如果您在为用户分配后更改 UPN，则 WorkSpace 除非您 WorkSpace 将 UPN 更改回以前的状态，否则用户将无法连接到他们的 UPN。

步骤 2：注册 Microsoft Entra ID 应用程序以授予 Windows Autopilot 权限

WorkSpaces Personal 使用微软 Windows Autopilot 用户驱动模式注册 WorkSpaces 微软 Intune 并加入微软 Entra ID。

要允许亚马逊 WorkSpaces 在 Autopilot 中注册 WorkSpaces 个人版，你必须注册一个授予必要的 Microsoft Graph API 权限的微软 Entra ID 应用程序。有关注册 Entra ID 应用程序的更多信息，请参阅 Quickstart: Register an application with the Microsoft identity platform。

我们建议在您的 Entra ID 应用程序中提供以下 API 权限。

- 要创建需要加入 Entra ID 的新个人 WorkSpace ，需要获得以下 API 权限。
  - `DeviceManagementServiceConfig.ReadWrite.All`
- 当您终止个人 WorkSpace 或重建个人时，将使用以下权限。

> **Note**
>
> 如果您不提供这些权限，则 WorkSpace 会被终止，但不会从您的 Intune 和 Entra ID 租户中移除这些权限，您必须分别将其删除。

  - `DeviceManagementServiceConfig.ReadWrite.All`
  - `Device.ReadWrite.All`
  - `DeviceManagementManagedDevices.ReadWrite.All`
- 这些权限需要管理员同意。有关更多信息，请参阅 Grant tenant-wide admin consent to an application。

接下来，您必须为 Entra ID 应用程序添加客户端密钥。有关更多信息，请参阅 Add credentials。请务必记住客户端密钥字符串，因为在步骤 4 中创建 Amazon Secrets Manager 密钥时将需要该字符串。

步骤 3：配置 Windows Autopilot 用户驱动模式

确保您熟悉 Step by step tutorial for Windows Autopilot user-driven Microsoft Entra join in Intune。

为 Autopilot 配置 Microsoft Intune

1. 登录 Microsoft Intune 管理中心
2. 为个人 WorkSpaces创建新的自动驾驶设备组。有关更多信息，请参阅 Create device groups for Windows Autopilot。

a. 依次选择组、新组

b. 对于 Group type，选择 Security。

c. 对于会员类型，选择动态设备。

d. 选择编辑动态查询，以创建动态会员规则。该规则应采用以下格式：

```
(device.devicePhysicalIds -any (_ -eq "[OrderID]:WorkSpacesDirectoryName"))
```

> **Important**
>
> `WorkSpacesDirectoryName`应与您在步骤 5 中创建的 Entra ID WorkSpaces 个人目录的目录名相匹配。这是因为在将虚拟桌面 WorkSpaces 注册到 Autopilot 时，目录名称字符串用作组标签。此外，组标签会映射到 Microsoft Entra 设备上的 `OrderID` 属性。

3. 依次选择设备、Windows、注册。在注册选项中，选择自动注册。对于 MDM 用户范围，选择全部。

4. 创建 Autopilot 部署配置文件。有关更多信息，请参阅 Create an Autopilot deployment profile。

   a. 对于 Windows Autopilot，依次选择部署配置文件、创建配置文件。

   b. 在 Windows Autopilot 部署配置文件屏幕中，选择创建配置文件下拉菜单，然后选择 Windows PC。

   c. 在 “创建个人资料” 屏幕中，在 Out-of-box体验 (OOBE) 页面上。对于部署模式，选择用户驱动。对于加入 Microsoft Entra ID，选择加入 Microsoft Entra。您可以为已加入 Entra ID 的个人 WorkSpaces 自定义计算机名称，方法是在 “应用设备名称模板” 中选择 “是”，创建在注册期间命名设备时使用的模板。

   d. 在分配页面上，对于分配至，选择选定的组。选择选择要包含的组，然后选择您刚刚在 2 中创建的 Autopilot 设备组。

步骤 4：创建Amazon Secrets Manager密钥

您必须在中创建密钥Amazon Secrets Manager才能安全地存储您在中创建的 Entra ID 应用程序的信息，包括应用程序 ID 和客户端密钥。步骤 2：注册 Microsoft Entra ID 应用程序以授予 Windows Autopilot 权限这是一次性设置。

创建密Amazon Secrets Manager钥

1. 在 Amazon Key Management Service 中创建客户自主管理型密钥。稍后将使用该密钥来加密Amazon Secrets Manager密钥。请勿使用默认密钥来加密您的密钥，因为 WorkSpaces 服务无法访问默认密钥。按照以下步骤创建密钥。

   a. 在 https://console.aws.amazon.com/km Amazon KMS s 处打开控制台。

   b. 要更改Amazon Web Services 区域，请使用页面右上角的区域选择器。

   c. 选择创建密钥。

   d. 在配置密钥页面上，为密钥类型选择对称。对于密钥用法，选择加密和解密。

   e. 在 “查看” 页面的密钥策略编辑器中，通过在密钥策略中包含以下权限，确保允许 WorkSpaces 服务的委托人`workspaces.amazonaws.com`访问密钥。

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "workspaces.amazonaws.com"
        ]
    },
    "Action": [
        "kms:Decrypt",
        "kms:DescribeKey"
    ],
    "Resource": "*"
 }
```

2. 使用上Amazon Secrets Manager一步中创建的密Amazon KMS钥在上创建密钥。

   a. 打开 Secrets Manager 控制台，网址为https://console.aws.amazon.com/secretsmanager/。

   b. 选择存储新密钥。

   c. 在选择密钥类型页面上，为密钥类型选择其他密钥类型。

   d. 对于键/值对，在密钥框中输入“application_id”，然后复制步骤 2 中的 Entra ID 应用程序 ID，并将其粘贴到值框中。

   e. 选择添加行，在密钥框中输入“application_password”，然后复制步骤 2 中的 Entra ID 应用程序客户端密钥，并将其粘贴到值框中。

   f. 从加密Amazon KMS密钥下拉列表中选择您在上一步中创建的密钥。

   g. 选择下一步。

h. 在配置密钥页面，输入密钥名称和描述。

i. 在资源权限部分，选择编辑权限。

j. 通过在资源权限中包含以下资源策略，确保允许 WorkSpaces 服务委托人`workspaces.amazonaws.com`访问密钥。

JSON

```
{
  "Version":"2012-10-17",
  "Statement" : [ {
    "Effect" : "Allow",
    "Principal" : {
      "Service" : [ "workspaces.amazonaws.com"]
    },
    "Action" : "secretsmanager:GetSecretValue",
    "Resource" : "*"
  } ]
}
```

第 5 步：创建专用的微软 Entra ID 目录 WorkSpaces

创建一个专门的 WorkSpaces 目录，用于存储已加入 Microsoft Entra ID WorkSpaces 和 Entra ID 的用户的信息。

创建 Entra ID 目录 WorkSpaces

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在导航窗格中，选择目录。
3. 在 “创建目录” 页面上，为WorkSpaces 类型选择 “个人”。要进行WorkSpace 设备管理，请选择微软 Entra ID。
4. 对于 Microsoft Entra 租户 ID，请输入你希望目录加入的 WorkSpaces 微软 Entra ID 租户 ID。创建目录后，您将无法更改租户 ID。
5. 对于 Entra ID 应用程序 ID 和密码，请从下拉列表中选择您在步骤 4 中创建的Amazon Secrets Manager密钥。创建目录后，您将无法更改与目录关联的密钥。但是，您可以随时通过Amazon Secrets Manager控制台更新密钥的内容，包括 Entra ID 应用程序 ID 及其密码，网址为https://console.aws.amazon.com/secretsmanager/。

6. 如果您的 IAM Identity Center 实例与您的 WorkSpaces目录位于同一Amazon区域，则对于用户身份源，请从下拉列表中选择您在步骤 1 中配置的 IAM 身份中心实例。创建目录后，您将无法更改与目录关联的 IAM Identity Center 实例。

   如果您的 IAM Identity Center 实例与您的 WorkSpaces 目录位于不同的Amazon区域，请选择启用跨区域，然后从下拉列表中选择该区域。

   > **Note**
   >
   > 如果您在其他区域拥有现有的 IAM Identity Center 实例，则必须选择加入才能设置跨区域集成。有关跨区域设置的更多信息，请参阅the section called “ 创建跨区域 IAM Identity Center 集成（可选）”。

7. 对于目录名称，输入目录的唯一名称（例如，`WorkSpacesDirectoryName`）。

   > **Important**
   >
   > 目录名称应与 `OrderID` 一致，为您在步骤 3 中使用 Microsoft Intune 创建的 Autopilot 设备组构建动态查询时使用过它。将个人注册 WorkSpaces 到 Windows Autopilot 时，目录名称字符串用作群组标签。组标签会映射到 Microsoft Entra 设备上的 `OrderID` 属性。

8. （可选）对于描述，输入目录的描述。
9. 对于 VP C，请选择您用来启动的 VPC WorkSpaces。有关更多信息，请参阅 为 WorkSpaces 个人版配置 VPC。
10. 对于子网，选择来自不同可用区的 VPC 的两个子网。这些子网将用于启动您的个人 WorkSpaces 网络。有关更多信息，请参阅 WorkSpaces 个人版的可用区。

    > **Important**
    >
    > 确保子网中 WorkSpaces 启动的用户可以访问互联网，这是用户登录到 Windows 桌面时所必需的。有关更多信息，请参阅 为 WorkSpaces 个人版提供互联网访问权限。

11. 在 “配置” 中，选择 “启用专用” WorkSpace。你必须启用它才能创建专用的 WorkSpaces 个人目录才能启动 Windows 10 或 11 个人 WorkSpaces版自带许可证 (BYOL)。

> **Note**
>
> 如果您未在 “配置 WorkSpace” 下看到 “启用专用” 选项，则说明您的账户尚未启用 BYOL。要为账户启用 BYOL，请参阅带上你自己的 Windows 桌面许可证 WorkSpaces。

12. （可选）在 “标签” 中，指定要在目录 WorkSpaces 中用于个人的 key pair 值。
13. 查看目录摘要，然后选择创建目录。连接目录需要几分钟时间。目录的初始状态是 `Creating`。目录创建完毕后，状态会变为 `Active`。

创建目录后，系统还会自动代表您创建 IAM Identity Center 应用程序。要查找应用程序的 ARN，请转到目录的摘要页面。

现在，你可以使用该目录启动已注册微软 Intune 并加入微软 Entra ID 的 Windows 10 或 11 个人 WorkSpaces 版。有关更多信息，请参阅 在 WorkSpaces 个人版中创建 WorkSpace。

创建 WorkSpaces 个人目录后，您可以创建个人目录 WorkSpace。有关更多信息，请参阅 在 WorkSpaces 个人版中创建 WorkSpace。

为 WorkSpaces 目录配置 IAM 身份中心应用程序（可选）

创建目录后，系统还会自动创建相应的 IAM Identity Center 应用程序。您可以在目录详细信息页面的“摘要”部分，找到应用程序的 ARN。默认情况下，Identity Center 实例中的所有用户 WorkSpaces 无需配置相应的 Identity Center 应用程序即可访问其分配的用户。但是，您可以通过为 IAM Identity Center 应用程序配置用户分配来管理用户对目录的访问权限。 WorkSpaces

为 IAM Identity Center 应用程序配置用户分配

1. 使用 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 在Amazon托管应用程序选项卡上，为 WorkSpaces 目录选择应用程序。应用程序名称采用以下格式：`WorkSpaces.wsd-xxxxx`，其中`wsd-xxxxx`是 WorkSpaces 目录 ID。
3. 依次选择操作、编辑详细信息。
4. 将用户和组分配方法从不需要分配更改为需要分配。
5. 选择保存更改。

在您进行此更改后，Identity Center 实例中的用户将失去其分配的访问权限， WorkSpaces 除非他们被分配给应用程序。要将用户分配给应用程序，请使用Amazon CLI命令`create-application-assignment`将用户或组分配给应用程序。有关更多信息，请参阅 Amazon CLI 命令参考。

创建跨区域 IAM Identity Center 集成（可选）

我们建议您的实例 WorkSpaces 和关联的 IAM Identity Center 实例位于同一Amazon区域。但是，如果您已经在与您所在区域不同的区域配置了 IAM Identity Center 实例，则可以创建跨区域集成。WorkSpaces 当您创建跨区域 WorkSpaces 和 IAM Identity Center 集成时，您可以进行跨区域调用 WorkSpaces ，以访问和存储来自您的 IAM Identity Center 实例的信息，例如用户和群组属性。

> **Important**
>
> Amazon 仅 WorkSpaces 支持组织级实例的跨区域 IAM 身份中心和 WorkSpaces 集成。WorkSpaces 不支持账户级实例的跨区域 IAM 身份中心集成。有关 IAM Identity Center 实例类型及其应用场景的更多信息，请参阅了解 IAM Identity Center 实例的类型。

如果您在 WorkSpaces 目录和 IAM Identity Center 实例之间创建跨区域集成，则由于跨区域调用，您在部署时 WorkSpaces 和登录期间可能会遇到更高的延迟。延迟的增加与您所在 WorkSpaces 地区和 IAM 身份中心区域之间的距离成正比。建议针对您的特定应用场景执行延迟测试。

您可以在步骤 5：创建专用 Microsoft Entra ID WorkSpaces 目录期间启用跨区域 IAM 身份中心连接。对于用户身份源，从下拉菜单中选择您在the section called “步骤 1：启用 IAM Identity Center 并与 Microsoft Entra ID 同步”中配置的 IAM Identity Center 实例。

> **Important**
>
> 创建后，您无法更改与目录关联的 IAM Identity Center 实例。

使用 “个 WorkSpaces 人” 创建专用的自定义目录

在创建 Windows 10 和 11 BYOL 个人 WorkSpaces 版并将其分配给使用 Amazon IAM 身份中心身份提供商 (IdPs) 管理的用户之前，您必须创建一个专用的自定义 WorkSpaces 目录。个人版 WorkSpaces 未加入任何 Microsoft Active Directory，但可以使用你选择的移动设备管理 (MDM) 解决方案进行管理，例如 JumpCloud。有关的更多信息 JumpCloud，请参阅这篇文章。要了解使用其他选项的教程，请参阅为 WorkSpaces 个人版创建目录。

> **Note**
>
> - Amazon WorkSpaces 无法创建或管理在自定义目录中 WorkSpaces 启动的个人用户账户。作为管理员，您必须对其进行管理。

- 除非洲（开普敦）、以色列（特拉维夫）和中国（宁夏）外，所有提供亚马逊 WorkSpaces 服务的Amazon地区均提供定制 WorkSpaces 目录。
- Amazon WorkSpaces 无法 WorkSpaces 使用自定义目录创建或管理用户账户。要确保你使用的 MDM 代理软件可以在 Windows 上创建用户配置文件 WorkSpaces，请联系 MDM 解决方案提供商。创建用户配置文件允许您的用户从 Windows 登录屏幕登录 Windows 桌面。

内容

- 要求和限制
- 步骤 1：启用 IAM Identity Center 并与身份提供者连接
- 步骤 2：创建专用的自定义 WorkSpaces 目录

要求和限制

- 自定义 WorkSpaces 目录仅支持 Windows 10 或 11 个人自带许可证 WorkSpaces。
- 自定义 WorkSpaces 目录仅支持 DCV 协议。
- 确保为您的Amazon帐户启用 BYOL，并且您拥有自己的Amazon KMS服务器，您的个人 WorkSpaces 可以访问该服务器以激活 Windows 10 和 11。有关更多信息，请参阅 带上你自己的 Windows 桌面许可证 WorkSpaces。
- 确保在导入账户的 BYOL 映像上预安装 MDM 代理软件。Amazon

步骤 1：启用 IAM Identity Center 并与身份提供者连接

要将用户信息分配 WorkSpaces 给由您的身份提供商管理的用户，必须Amazon通过 Amazon IAM Identity Center 向其提供用户信息。我们建议使用 IAM 身份中心来管理您的用户对Amazon资源的访问权限。有关更多信息，请参阅什么是 IAM Identity Center？。这是一次性设置。

将用户信息提供给 Amazon

1. 启用 IAM 身份中心Amazon。您可以在Amazon组织中启用 IAM Identity Center，尤其是在您使用多账户环境的情况下。您还可以创建 IAM Identity Center 账户实例。有关更多信息，请参阅启用 Amazon IAM 身份中心。每个 WorkSpaces 目录可以与一个 IAM 身份中心组织或账户实例关联。每个 IAM 身份中心实例都可以与一个或多个 WorkSpaces 个人目录关联。

   如果您正在使用组织实例并尝试在其中一个成员账户中创建 WorkSpaces 目录，请确保您拥有以下 IAM Identity Center 权限。

- "sso:DescribeInstance"
- "sso:CreateApplication"
- "sso:PutApplicationGrant"
- "sso:PutApplicationAuthenticationMethod"
- "sso:DeleteApplication"
- "sso:DescribeApplication"
- "sso:getApplicationGrant"

有关更多信息，请参阅管理对 IAM Identity Center 资源的访问权限概览。确保没有服务控制策略 (SCPs) 阻止这些权限。要了解更多信息 SCPs，请参阅服务控制策略 (SCPs)。

2. 配置 IAM Identity Center 和您的身份提供者（IdP），自动将用户从您的 IdP 同步到您的 IAM Identity Center 实例。有关更多信息，请参阅入门教程并选择要使用的 IdP 的特定教程。例如，使用 IAM 身份中心连接您的 JumpCloud 目录平台。
3. 验证您在 IdP 上配置的用户是否已正确同步到 Amazon IAM Identity Center 实例。第一次同步最多可能需要一个小时，具体取决于您 IdP 的配置。

步骤 2：创建专用的自定义 WorkSpaces 目录

创建专门的 WorkSpaces 个人目录，用于存储有关您的个人 WorkSpaces 和用户的信息。

创建专用的自定义 WorkSpaces 目录

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在导航窗格中，选择目录。
3. 选择创建目录。
4. 在 “创建目录” 页面上，对于WorkSpaces类型，选择 “个人”。要进行WorkSpace 设备管理，请选择自定义。
5. 对于用户身份源，从下拉列表中选择您在步骤 1 中配置的 IAM Identity Center 实例。创建目录后，您将无法更改与目录关联的 IAM Identity Center 实例。

> **Note**
> 您必须为该目录指定 IAM Identity Center 实例，否则您将无法 WorkSpaces 使用 WorkSpaces 控制台使用该目录启动个人版。 WorkSpaces 没有关联身份中心的目录仅与 WorkSpaces 核心合作伙伴解决方案兼容。

6. 对于目录名称，输入目录的唯一名称。
7. 对于 VP C，请选择您用来启动的 VPC WorkSpaces。有关更多信息，请参阅 为 WorkSpaces 个人版配置 VPC。
8. 对于子网，选择来自不同可用区的 VPC 的两个子网。这些子网将用于启动您的个人 WorkSpaces 网络。有关更多信息，请参阅 WorkSpaces 个人版的可用区。

> **Important**
> 确保子网中 WorkSpaces 启动的用户可以访问互联网，这是用户登录到 Windows 桌面时所必需的。有关更多信息，请参阅 为 WorkSpaces 个人版提供互联网访问权限。

9. 在 “配置” 中，选择 “启用专用” WorkSpace。要启动 “自带许可证” (BYOL) Windows 10 或 11 WorkSpaces 个人版，你必须启用它才能创建专用的个人 WorkSpaces目录。
10. （可选）在 “标签” 中，指定要在目录 WorkSpaces 中用于个人的 key pair 值。
11. 查看目录摘要，然后选择创建目录。连接目录需要几分钟时间。目录的初始状态是 `Creating`。目录创建完毕后，状态会变为 `Active`。

创建目录后，系统还会自动代表您创建 IAM Identity Center 应用程序。要查找应用程序的 ARN，请转到目录的摘要页面。

现在，你可以使用该目录启动已注册微软 Intune 并加入微软 Entra ID 的 Windows 10 或 11 个人 WorkSpaces 版。有关更多信息，请参阅 在 WorkSpaces 个人版中创建 WorkSpace。

创建 WorkSpaces 个人目录后，您可以创建个人目录 WorkSpace。有关更多信息，请参阅 在 WorkSpaces 个人版中创建 WorkSpace。

更新 WorkSpaces 个人版的 DNS 服务器

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

您可以通过以下方式使用新的 DNS 设置更新 WorkSpaces：

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

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

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

最佳实践

在您更新 DNS 服务器设置时，建议遵循以下最佳实践：

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

步骤 1：在您的 WorkSpaces 上更新 DNS 服务器设置

在以下过程中，当前和新的 DNS 服务器 IP 地址的参考值如下所示：

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

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

更新 Windows WorkSpaces 的 DNS 服务器设置

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

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

使用注册表编辑器更新 DNS 注册表设置

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

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

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

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

使用 PowerShell 更新 DNS 注册表设置

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

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

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

您应该收到如下所示的输出。

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

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

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

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

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

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

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

更新 Amazon Linux 2 WorkSpaces 的 DNS 服务器设置

如果您有 1 个以上的 Amazon Linux 2 WorkSpace，建议您使用配置管理解决方案来分发和实施策略。例如，您可以使用 Ansible。

更新 Amazon Linux 2 WorkSpace 上的 DNS 服务器设置

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

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

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

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

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

更新 Ubuntu WorkSpaces 的 DNS 服务器设置

如果您有 1 个以上的 Ubuntu WorkSpace，建议您使用配置管理解决方案来分发和实施策略。例如，您可以使用 Landscape。

更新 Ubuntu WorkSpace 上的 DNS 服务器设置

1. 在 Ubuntu WorkSpace 上，打开终端窗口，并运行以下命令。您必须具有根用户权限才能编辑此文件。要成为根用户，可以使用 sudo -i 命令，也可以运行所有命令，如 sudo 所示。

```
sudo vi /etc/netplan/zz-workspaces-domain.yaml
```

2. 在 yaml 文件中，您将看到以下 nameserver 命令。

```
nameservers:
    search:[Your domain FQDN]
    addresses:[OldIP1, OldIP2]
```

将 *OldIP1* 和 *OldIP2* 替换为 *NewIP1* 和 *NewIP2*。

如果您有多个 DNS 服务器 IP 地址，请将它们添加为逗号分隔的值。例如 [*NewDNSIP1*, *NewDNSIP2*, *NewDNSIP3*]。

3. 保存 yaml 文件。
4. 运行命令 sudo netplan apply 以应用更改。
5. 运行命令 resolvectl status 以验证是否正在使用新的 DNS IP 地址。

6. 继续执行步骤 2，在 Active Directory 中更新 DNS 服务器设置。

更新 Red Hat Enterprise Linux WorkSpaces 的 DNS 服务器设置

如果您有 1 个以上的 Red Hat Enterprise Linux WorkSpace，建议您使用配置管理解决方案来分发和实施策略。例如，您可以使用 Ansible。

更新 Red Hat Enterprise Linux WorkSpace 上的 DNS 服务器设置

1. 在 Red Hat Enterprise Linux WorkSpace 上，打开终端窗口并运行以下命令。您必须具有根用户权限才能编辑此文件。要成为根用户，可以使用 `sudo -i` 命令，也可以运行所有命令，如 `sudo` 所示。

```
sudo nmcli conn modify CustomerNIC ipv4.dns 'NewIP1 NewIP2'
```

2. 运行以下命令。

```
sudo systemctl restart NetworkManager
```

3. 要检查已更新的 DNS 和网络配置，请运行以下命令。

```
nmcli device show eth1
```

4. 继续执行步骤 2，在 Active Directory 中更新 DNS 服务器设置。

步骤 2：更新 Active Directory 的 DNS 服务器设置

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

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

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

更新 DNS 服务器设置后，继续执行步骤 3。

步骤 3：测试更新的 DNS 服务器设置

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

在以下过程中，当前和新的 DNS 服务器 IP 地址的参考值如下所示：

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

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

测试更新后的 Windows WorkSpaces 的 DNS 服务器设置

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

   ```
   nslookup AD_Name
   ```

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

   ```
   Server:  Full_AD_Name
   Address:  NewIP1

   Name:    AD_Name
   Addresses:  OldIP2
             NewIP1
   ```

5. 如果输出与预期不符，或者收到任何错误，请重复步骤 1。
6. 等待一个小时，确认没有报告任何用户问题。验证 *NewIP1* 是否正在获取 DNS 查询并做出答复。
7. 确认第一台 DNS 服务器运行正常后，重复步骤 1 更新第二台 DNS 服务器，这次将 *OldIP2* 替换为 *NewIP2*。然后重复步骤 2 和步骤 3。

测试更新后的 Linux WorkSpaces 的 DNS 服务器设置

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

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

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

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

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

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

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

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

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

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

删除 WorkSpaces 个人版目录

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

删除目录时会发生什么

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

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

删除 Entra ID 或自定义 WorkSpaces 目录

Entra ID WorkSpaces 目录允许您创建已加入 Entra ID 的 Windows 10 或 11 BYOL WorkSpaces。有关更多信息，请参阅 使用个人版创建专用的 Microsoft Entra ID 目录 WorkSpaces 。

自定义 WorkSpaces 目录允许您创建未加入 Active Directory 域的 WorkSpaces，但需使用您自己的设备管理软件和 IAM Identity Center。有关更多信息，请参阅 使用 “个 WorkSpaces 人” 创建专用的自定义目录。

删除 Entra ID 或自定义 WorkSpaces 目录

1. 删除目录中的所有 WorkSpace。有关更多信息，请参阅 删除 WorkSpaces 个人版中的 WorkSpace。

2. 在导航窗格中，选择目录。
3. 选择目录。
4. 依次选择操作、删除。
5. 如果提示进行确认，请输入删除。

删除 Amazon Directory Service 目录

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

取消注册目录

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。
3. 选择目录。
4. 选择 Actions、Deregister。
5. 当系统提示您确认时，选择 Deregister (取消注册)。取消注册完成后，Registered 的值为 No。

要删除目录

1. 删除目录中的所有 WorkSpace。有关更多信息，请参阅 删除 WorkSpaces 个人版中的 WorkSpace。
2. 查找并删除注册到目录的所有应用程序和服务。有关更多信息，请参阅《Amazon Directory Service 管理指南》中的删除您的目录。
3. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
4. 在导航窗格中，选择目录。
5. 选择目录，然后选择 Actions、Deregister。
6. 当系统提示您确认时，选择 Deregister (取消注册)。
7. 再次选择目录，然后选择 Actions 和 Delete。
8. 当系统提示进行确认时，选择 Delete（删除）。

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

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

为 WorkSpaces 个人设置 Active Directory 管理工具

您将使用 WorkSpaces 目录管理工具（例如 Active Directory 管理工具）为目录执行大多数管理任务。但是，您将使用 WorkSpaces 控制台执行一些与目录相关的任务。有关更多信息，请参阅 管理 WorkSpaces 个人版的目录。

如果您使用Amazon托管 Microsoft AD 或 Simple AD 创建包含五个或更多目录的目录 WorkSpaces，我们建议您对亚马逊 EC2 实例进行集中管理。尽管您可以在上安装目录管理工具 WorkSpace，但使用 Amazon EC2 实例是一种更强大的解决方案。

设置 Active Directory 管理工具

1. 启动一个 Amazon EC2 Windows 实例，然后使用以下选项之一将其加入您的 WorkSpaces 目录：
   - 如果您还没有现有 Amazon EC2 Windows 实例，则可以在启动实例时将该实例加入您的目录域。有关更多信息，请参阅《Amazon Directory Service管理指南》中的无缝加入 Windows EC2 实例。
   - 如果您已经有一个 Amazon EC2 Windows 实例，则可以手动将其加入您的目录。有关更多信息，请参阅《Amazon Directory Service 管理指南》中的手动添加 Windows 实例。
2. 在亚马逊 EC2 Windows 实例上安装 Active Directory 管理工具。有关更多信息，请参阅《Amazon Directory Service 管理指南》中的安装 Active Directory 管理工具。

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

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

3. 按照如下步骤以目录管理员身份运行工具：
   a. 在 Windows 开始菜单上，打开 Windows 管理工具。
   b. 按住 Shift 键，右键单击您要使用的工具快捷方式，然后选择以其他用户身份运行。
   c. 输入管理员登录凭证。在 Simple AD 中，用户名为**`Administrator`**；对于Amazon托管 Microsoft AD，管理员是**`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，不适用于Amazon托管 AD 创建的目录。有关使用Amazon托管 AD 创建的目录，请参阅《管理指南》中的 “在Amazon托管 Microsoft AD 中 Amazon Directory Service管理用户和群组”。

1. 打开“Active Directory 用户和计算机”工具。
2. 导航到您的域下的用户文件夹并选择要提升的用户。
3. 选择操作、属性。
4. 在 “***`username`***属性” 对话框中，选择 “成员为”。
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

您只能在启动的过程中从亚马逊 WorkSpaces 控制台创建新用户 WorkSpace，并且不能通过亚马逊 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**
>
> 必须先删除 WorkSpace 分配给该用户的用户，然后才能移除该用户。有关更多信息，请参阅删除 WorkSpaces 个人版中的 WorkSpace。

用于管理用户和组的过程取决于您使用的目录类型。

- 如果你使用的是Amazon托管 Microsoft AD，请参阅《管理指南》中的 “在Amazon托管 Microsoft AD 中Amazon Directory Service管理用户和群组”。
- 如果您使用的是 Simple AD，请参阅《Amazon Directory Service 管理指南》中的在 Simple AD 中管理用户和组。
- 如果通过 AD Connector 或信任关系使用 Microsoft Active Directory，则可以使用 Active Directory 模块来管理用户和组。

重置用户密码

在为现有用户重置密码时，不要设置 User must change password at next logon。否则，用户将无法连接到他们 WorkSpaces的。相反，应为每位用户分配一个安全的临时密码，然后要求用户在下 WorkSpace 次登录时手动更改密码。

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

管理 WorkSpaces 个人版中的用户

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

目录

- 在 “ WorkSpaces 个人” 中管理用户
- 在 WorkSpaces 个人版中为用户创建多个 WorkSpaces
- 自定义用户登录其 WorkSpaces 个人版中 WorkSpaces 的方式
- 为 WorkSpaces 个人版中的用户启用自助式 WorkSpace 管理功能
- 为 WorkSpaces 个人版用户启用 Amazon Connect 音频优化
- 在 WorkSpaces 个人版中启用诊断日志上传

在 “ WorkSpaces 个人” 中管理用户

作为的管理员 WorkSpaces，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 控制台编辑的用户信息 WorkSpace。

> **Note**
>
> 只有当你使用Amazon托管 Microsoft AD 或 Simple AD 时，此功能才可用。如果通过 AD Connector 或信任关系使用 Microsoft Active Directory，则可以使用 Active Directory 模块来管理用户和组。如果你使用 Microsoft Entra ID 或自定义 WorkSpaces 目录，则可以使用微软 Entra ID 或你的身份提供商来管理用户和群组。

要编辑用户信息

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在导航窗格中，请选择 WorkSpaces。
3. 选择一个用户，然后依次选择操作、编辑用户。
4. 根据需要，更新名字、姓氏和电子邮件地址。
5. 选择更新。

添加或删除用户

您只能在启动的过程中从亚马逊 WorkSpaces 控制台创建用户 WorkSpace，并且不能通过亚马逊 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 WorkSpaces 目录管理工具（例如 Active Directory 管理工具）为目录执行大多数管理任务。有关更多信息，请参阅 为 WorkSpaces 个人设置 Active Directory 管理工具。

> **Important**
>
> 必须先删除 WorkSpace 分配给该用户的用户，然后才能移除该用户。有关更多信息，请参阅 删除 WorkSpaces 个人版中的 WorkSpace。

用于管理用户和组的过程取决于您使用的目录类型。

- 如果你使用的是Amazon托管 Microsoft AD，请参阅《管理指南》中的 “在Amazon托管 Microsoft AD 中Amazon Directory Service管理用户和群组”。
- 如果您使用的是 Simple AD，请参阅《Amazon Directory Service 管理指南》中的在 Simple AD 中管理用户和组。
- 如果通过 AD Connector 或信任关系使用 Microsoft Active Directory，则可以使用 Active Directory 模块来管理用户和组。

发送邀请电子邮件

您可以根据需要向用户手动发送邀请电子邮件。

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

要重新发送邀请电子邮件

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。

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

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

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

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

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

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

自定义用户登录其 WorkSpaces 个人版中 WorkSpaces 的方式

自定义您的用户对 WorkSpace 的访问，方法为使用统一资源标识符 (URI) 提供与您组织内的现有工作流程集成的经简化的登录体验。例如，您可以使用 WorkSpace 注册代码自动生成为您的用户注册的登录 URI。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身份验证 (MFA)，则用户的用户名和 MFA 代码将自动在其客户端登录页上输入。

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

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

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

要使用 URI 访问其 WorkSpaces，用户必须先打开 https://clients.amazonworkspaces.awsapps.cn/ 并按照说明操作，为设备安装客户端应用程序。

Windows 和 macOS 计算机上的 Firefox 和 Chrome 浏览器、Ubuntu Linux 18.04、20.04 和 22.04 计算机上的 Firefox 浏览器以及 Windows 计算机上的 Internet Explorer 和 Microsoft Edge 浏览器都支

持 URI 访问。有关 WorkSpaces 客户端的更多信息，请参阅《Amazon WorkSpaces 用户指南》中的 WorkSpaces 客户端。

> **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 WorkSpace 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，建议您在数据组件中使用百分号编码以避免歧义：
>
> `@ : / ? & =`
>
> 例如，如果您有包含其中任一字符的用户名，则应该对 URI 中的这些用户名进行百分号编码。有关更多信息，请参阅统一资源标识符 (URI)：一般语法。

支持的语法	描述
workspaces://	打开 WorkSpace 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 WorkSpace 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 WorkSpace 注册代码注册用户。此外，在客户端登录页上的用户名字段中自动输入用户名。
workspaces://username@registrationcode?MFACode=mfa	使用用户的 WorkSpace 注册代码注册用户。此外，在客户端登录页上的用户名字段中自动输入用户名，在同一页上的 MFA 代码字段中自动输入多重身份验证 (MFA) 代码。
workspaces://@registrationcode?MFACode=mfa	使用用户的 WorkSpace 注册代码注册用户。此外，在客户端登录页上的 MFA code (MFA 代码) 字段中自动输入多重验证 (MFA) 代码。

> **Note**
>
> 如果用户在从 Windows 客户端连接到 WorkSpace 后打开了一个 URI 链接，新的 WorkSpace 会话将打开，其原始 WorkSpace 会话将保持打开状态。如果用户在从 macOS、iPad 或 Android 客户端连接到 WorkSpace 后打开了一个 URI 链接，则不会有新的 WorkSpace 会话打开；只有其原始 WorkSpace 会话会保持打开状态。

为 WorkSpaces 个人版中的用户启用自助式 WorkSpace 管理功能

在 WorkSpaces 中，您可以为用户启用自助式 WorkSpace 管理功能，使他们能够更好地控制其体验。这也可以减少 IT 支持人员的 WorkSpaces 工作负载。当您启用自助服务功能时，用户可以直接从其 WorkSpaces 客户端执行以下一项或多项任务：

- 将其凭证缓存在其客户端上。这使其能够重新连接到 WorkSpace，而无需重新输入凭证。
- 重新启动（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。
- 重建其 WorkSpace。

支持的客户端

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

为您的用户启用自助服务管理功能

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。
3. 选择要启用自助式管理功能的目录。
4. 向下滚动到“自助服务权限”，然后选择编辑。根据需要启用或禁用以下选项以确定用户可从其客户端执行的 WorkSpace 管理任务：

- 记住我 - 用户可以通过选择登录屏幕上的记住我或保持登录状态复选框，选择是否在其客户端上缓存其凭证。这些凭证仅缓存到 RAM 中。当用户选择缓存其凭证时，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。
- 从客户端重启 WorkSpace - 用户可以重新启动（重启）其 WorkSpace。重新启动操作将断开用户与 WorkSpace 的连接，然后关闭并重启它。用户数据、操作系统和系统设置不受影响。
- 增加卷大小 - 用户可以将其 WorkSpace 上的根卷和用户卷扩展至指定大小，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 根卷和用户卷包含无法更改的集合组。可用组包括：[根 (GB)，用户 (GB)]: [80，10]、[80，50]、[80，100]、[175 至 2000，100 至 2000]。有关更多信息，请参阅 修改 WorkSpaces 个人版中的 WorkSpace。

  对于新建的 WorkSpace，用户必须先等待 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为：更改 WorkSpace 计算类型、切换 WorkSpace 运行模式、重启 WorkSpace 或重建 WorkSpace。完成此过程后，必须重新启动 WorkSpace 才能使更改生效。此过程可能需要一个小时。

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

- 更改计算类型 - 用户可以在计算类型（捆绑包）之间切换 WorkSpace。对于新建的 WorkSpace，用户必须先等待 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，WorkSpace 将自动重新启动。此过程可能需要一个小时。

  > **Note**
  >
  > 如果用户更改 WorkSpace 计算类型，这可能会更改 WorkSpace 的账单费率。

- 切换运行模式 - 用户可以在 AlwaysOn 和 AutoStop 运行模式之间切换他们的 WorkSpace。有关更多信息，请参阅 在 WorkSpaces 个人版中管理跑步模式。

> **Note**
>
> 如果用户切换 WorkSpace 的运行模式，这将更改 WorkSpace 的账单费率。

- 从客户端重建 WorkSpace - 用户可以将 WorkSpace 的操作系统重建到其原始状态。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。对于新建的 WorkSpace，用户必须先等待 12 小时，然后才能重建 WorkSpace。在重建 WorkSpace 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。此过程可能需要一个小时。
- 诊断日志上传 - 用户可以在不中断 WorkSpaces 客户端使用的情况下，直接将 WorkSpaces 客户端日志文件上传到 WorkSpaces 以排查相关问题。如果您为用户启用诊断日志上传，或者让您的用户自行启用该功能，则日志文件将自动发送到 WorkSpaces。您可以在 WorkSpaces 流式传输会话之前或期间启用诊断日志上传。

5. 选择 Save。

为 WorkSpaces 个人版用户启用 Amazon Connect 音频优化

在 WorkSpaces 管理控制台中，您可以为 WorkSpaces 队列启用 Amazon Connect 联系人控制面板 (CCP) 音频优化，以增强安全性并启用原生音质音频。启用 CCP 音频优化后，CCP 音频将由客户端端点处理，同时 WorkSpaces 用户可以在其 WorkSpaces 内与 CCP 进行交互。

Amazon Connect 联系人控制面板 (CCP) 音频优化适用于：

- WorkSpaces Windows 客户端。
- Amazon Linux 和 Windows WorkSpaces。
- 使用 PCoIP 或 DCV 的 WorkSpaces。

要求

- 您必须使用 Amazon Connect 进行设置。
- 您必须使用 Amazon Connect 流 API 创建一个不含呼叫信令的媒体 CCP，从而构建自定义 CCP。这样，会在本地桌面上使用标准 CCP 处理媒体，并使用不含媒体的 CCP 通过远程连接处理信号发送和呼叫控制。有关 Amazon Connect 流 API 的更多信息，请通过以下网址参见 GitHub 存储库：https://github.com/aws/amazon-connect-streams。您构建的自定义 CCP 是 Amazon Connect 代理将在其 WorkSpaces 内使用的 CCP。

- 您必须在 Amazon Connect 支持的 WorkSpaces 客户端端点上安装 Web 浏览器。要查看支持的浏览器列表，请参阅 Amazon Connect 支持的浏览器。

> **Note**
>
> 如果您的用户使用不受支持的浏览器，则当他们尝试登录 CCP 时，系统会要求他们下载支持的浏览器。

启用 Amazon Connect 音频优化

为用户启用 Amazon Connect 音频优化：

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。
3. 选择目录，然后选择 Actions、Update Details。
4. 展开 Amazon Connect 音频优化。

> **Note**
>
> 在使用 Amazon Connect 进行配置之前，选择更新，以保存之前在管理控制台中进行的所有未保存的更改。

5. 选择配置 Amazon Connect。
6. 输入 Amazon Connect 联系人控制面板 (CCP) 名称。

> **Note**
>
> 用户插件菜单中将使用您为 CCP 提供的名称。选择一个对您的用户有意义的名称。

7. 输入 Amazon Connect 生成的 Amazon Connect 联系人控制面板 URL。有关获取 URL 的更多信息，请参阅提供对联系人控制面板的访问权限。
8. 选择创建 Amazon Connect。

更新目录的 Amazon Connect 音频优化详细信息

更新目录的 Amazon Connect 音频优化详细信息：

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。
3. 选择目录，然后选择 Actions、Update Details。
4. 展开 Amazon Connect 音频优化。

> **Note**
>
> 在使用 Amazon Connect 进行配置之前，选择更新，以保存之前在管理控制台中进行的所有未保存的更改。

5. 选择配置 Amazon Connect。
6. 选择编辑。
7. 选择目录，然后选择 Actions、Update Details。
8. 更新 Amazon Connect 联系人控制面板的名称和 URL。
9. 选择保存。

删除目录的 Amazon Connect 音频优化

删除目录的 Amazon Connect 音频优化：

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。
3. 选择目录，然后选择 Actions、Update Details。
4. 展开 Amazon Connect 音频优化。

> **Note**
>
> 在使用 Amazon Connect 进行配置之前，选择更新，以保存之前在管理控制台中进行的所有未保存的更改。

5. 选择配置 Amazon Connect。
6. 选择删除 Amazon Connect。

有关更多信息，请参阅代理培训指南。

在 WorkSpaces 个人版中启用诊断日志上传

要排查 WorkSpaces 客户端问题，请启用自动诊断日志上传功能。目前，Windows、macOS、Linux 和 Web Access 客户端支持此项功能。

> **Note**
>
> WorkSpaces 客户端诊断日志上传功能目前在 Amazon GovCloud（美国西部）区域不提供。

诊断日志上传

借助诊断日志上传功能，您可以在不中断 WorkSpaces 客户端使用的情况下，直接将 WorkSpaces 客户端日志文件上传到 WorkSpaces 以排查相关问题。如果您为用户启用诊断日志上传，或者让您的用户自行启用该功能，则日志文件将自动发送到 WorkSpaces。您可以在 WorkSpaces 流式传输会话之前或期间启用诊断日志上传。

要从托管设备自动上传诊断日志，请安装支持诊断上传的 WorkSpaces 客户端。默认情况下，日志上传处于启用状态。您可以通过以下任一方式修改设置：

选项 1：使用 Amazon 控制台

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。
3. 选择要启用诊断日志的目录名称。
4. 向下滚动到自助服务权限。
5. 选择查看详细信息
6. 选择编辑。
7. 选择诊断日志上传。
8. 选择保存。

选项 2：使用 API 调用

您可以编辑目录设置以启用或禁用 WorkSpaces Windows、macOS 和 Linux 客户端，以便使用 API 调用自动上传诊断日志。如果启用，则当客户端出现问题时，日志将发送到 WorkSpaces，而无需用户交互。有关更多信息，请参阅 WorkSpaces API 参考。

您也可以让用户选择是否在安装客户端后启用自动诊断日志上传。有关更多信息，请参阅 WorkSpaces Windows 客户端应用程序、WorkSpaces macOS 客户端应用程序以及 WorkSpaces Linux 客户端应用程序。

> **Note**
>
> - 诊断日志不包含敏感信息。您可以在目录级别为用户禁用自动诊断日志上传，或者允许您的用户自行禁用这些功能。
> - 要访问诊断日志上传功能，您需要安装以下版本的 WorkSpaces 客户端：
> - Windows 客户端 5.4.0 或更高版本
> - macOS 客户端 5.8.0 或更高版本
> - Ubuntu 22.04 客户端 2023.1
> - Ubuntu 20.04 客户端 2023.1
> - 也可以使用 Web Access 客户端访问诊断日志上传功能

管理 WorkSpaces 个人版

您可以使用 WorkSpaces 控制台管理您的 WorkSpaces。

要执行目录管理任务，请参见the section called “设置目录管理”。

> **Note**
>
> - 确保在 WorkSpaces 上更新网络依赖驱动程序，例如 ENA、NVMe 和 PV 驱动程序。您应该至少每 6 个月更新一次。有关更多信息，请参阅安装或升级弹性网络适配器（ENA）驱动程序、Windows 实例的 Amazon NVMe 驱动程序以及升级 Windows 实例上的 PV 驱动程序。
> - 确保定期将 EC2Config、EC2Launch 和 EC2Launch V2 代理更新到最新版本。您应该至少每 6 个月更新一次。有关更多信息，请参阅更新 EC2Config 和 EC2Launch。

目录

- WorkSpaces 在 WorkSpaces 个人版中管理你的 Windows
- WorkSpaces 在 WorkSpaces 个人版中管理你的 Amazon Linux 2
- 以个人模式管理你的 Ubuntu WorkSpaces WorkSpaces

- 管理你的洛基 Linux WorkSpaces
- 管理你的红帽企业 Linux WorkSpaces
- 优化 WorkSpaces 个人版的 WorkSpaces 以实现实时通信
- 在 WorkSpaces 个人版中管理跑步模式
- 在 “ WorkSpaces 个人” 模式下管理应用程序
- 修改 WorkSpaces 个人版中的 WorkSpace
- 在 WorkSpaces 个人版中自定义品牌
- 在 WorkSpaces 个人版中为资源添加标签
- WorkSpaces 个人版的维护
- WorkSpaces 以 WorkSpaces 个人身份加密
- 重启 WorkSpaces 个人版中的 WorkSpace
- 重建 WorkSpaces 个人版中的 WorkSpace
- 还原 WorkSpaces 个人版中的 WorkSpace
- 升级 WorkSpaces 个人版中的 Windows BYOL WorkSpaces
- 以 WorkSpaces 个人 WorkSpace 方式迁移
- 删除 WorkSpaces 个人版中的 WorkSpace

WorkSpaces 在 WorkSpaces 个人版中管理你的 Windows

你可以使用组策略对象 (GPOs) 来应用设置来管理 Windows WorkSpaces 或属于你的 Windows WorkSpaces 目录的用户。

> **Note**
>
> - 如果你使用 Microsoft Entra ID 或自定义 WorkSpaces 目录，则可以使用微软 Entra ID 或你的身份提供商来管理用户和群组。有关更多信息，请参阅使用个人版创建专用的 Microsoft Entra ID 目录 WorkSpaces 。
> - Linux 实例不遵循组策略。有关管理亚马逊 Linux 的信息 WorkSpaces，请参阅 WorkSpaces 在 WorkSpaces 个人版中管理你的 Amazon Linux 2。

Amazon 建议您为 WorkSpaces 计算机对象创建一个组织单位，为 WorkSpaces 用户对象创建一个组织单元。

要使用特定于 Amazon 的组策略设置 WorkSpaces，您必须为您正在使用的协议（ PCoIP 或 DCV）安装组策略管理模板。

> **Warning**
>
> 组策略设置可能会影响 WorkSpace 用户体验，如下所示：
>
> - 实现交互式登录消息以显示登录横幅可防止用户访问他们的。 WorkSpaces PCoIP WorkSpaces 当前不支持交互式登录消息组策略设置。DCV 支持登录消息 WorkSpaces，用户在接受登录横幅后必须重新登录。启用“基于证书的登录”时，不支持登录消息。
> - 通过组策略设置禁用可移动存储会导致登录失败，从而导致用户登录到无权访问驱动器 D 的临时用户配置文件。
> - 通过组策略设置将用户从远程桌面用户本地组中移除会阻止这些用户通过 WorkSpaces 客户端应用程序进行身份验证。有关此组策略设置的更多信息，请参阅 Microsoft 文档中的允许通过远程桌面服务登录。
> - 如果您从 “允许本地登录” 安全策略中移除内置 WorkSpaces 用户组，则您 PCo的 IP 用户将无法 WorkSpaces 通过 WorkSpaces 客户端应用程序连接到他们。您 PCo的 IP WorkSpaces 也不会收到 PCo IP 代理软件的更新。 PCoIP 代理更新可能包含安全修复和其他修复程序，或者它们可能会为您启用新功能 WorkSpaces。有关使用此安全策略的更多信息，请参阅 Microsoft 文档中的允许本地登录。
> - 组策略设置可用于限制驱动器访问。如果将组策略设置配置为限制对驱动器 C 或驱动器 D 的访问，则用户无法访问他们的 WorkSpaces。要防止此问题发生，请确保您的用户可以访问驱动器 C 和驱动器 D。
> - WorkSpaces 音频输入功能需要内部的本地登录访问权限。 WorkSpace默认情况下，Windows WorkSpaces 的音频输入功能处于启用状态。但是，如果您的组策略设置限制了用户的本地登录 WorkSpaces，则音频输入将无法在您的上运行。 WorkSpaces如果删除该组策略设置，则下次重新启动后将启用音频输入功能。 WorkSpace有关此组策略设置的更多信息，请参阅 Microsoft 文档中的允许本地登录。
>
> 有关启用或禁用音频输入重定向的更多信息，请参阅为 IP 配置音频输入重定向 PCo或为 DCV 配置音频输入重定向。
> - 使用组策略将 Windows 电源计划设置为 “平衡” 或 “省电模式”，可能会 WorkSpaces 导致您在它们处于闲置状态时进入睡眠状态。我们强烈建议使用组策略将 Windows 电源计划设置为高性能。有关更多信息，请参阅 我的 Windows 闲置时会 WorkSpace 进入睡眠状态。
> - 某些组策略设置会在用户从会话断开连接时迫使其注销。用户在其上打开的所有应用程序 WorkSpaces 都将关闭。

- DCV WorkSpaces 目前不支持 “为处于活动状态但处于空闲状态的远程桌面服务会话设置时间限制”。避免在 DCV 会话期间使用它，因为即使有活动且会话未处于闲置状态，也会导致断开连接。

有关使用 Active Directory 管理工具进行操作的信息 GPOs，请参阅为 WorkSpaces 个人设置 Active Directory 管理工具。

内容

- 为 DCV 安装组策略管理模板文件
- 管理 DCV 的组策略设置
- 安装 PCo IP 的组策略管理模板
- 管理 PCo IP 的组策略设置
- 设置 Kerberos 票证的最长使用期限
- 配置用于互联网访问的设备代理服务器设置
  - 代理桌面流量
  - 关于使用代理服务器的建议
- 启用 Amazon WorkSpaces for Zoom 会议媒体插件支持
  - 为 DCV 启用 Zoom Meeting Media Plugin
    - 先决条件
    - 开始前的准备工作
    - 安装 Zoom 组件
  - 启用适用于 PCo IP 的 Zoom 会议媒体插件
    - 先决条件
    - 在 Windows WorkSpaces 主机上创建注册表项
    - 问题排查

为 DCV 安装组策略管理模板文件

要使用使用 DCV WorkSpaces 时特有的组策略设置，必须将 DCV 的组策略管理模板`wsp.admx`和`wsp.adml`文件添加到目录的域控制器的 WorkSpaces 中央存储区。有关 `.admx` 和 `.adml` 文件的更多信息，请参阅如何在 Windows 中创建和管理组策略管理模板的中央存储。

以下过程介绍了如何创建中央存储并向其中添加管理模板文件。对已加入目录的目录管理 WorkSpace 或 Amazon EC2 实例执行以下步骤。 WorkSpaces

为 DCV 安装组策略管理模板文件

1. 在正在运行的 Windows WorkSpace 中，复制`C:\Program Files\Amazon\WSP`目录中的`wsp.admx`和`wsp.adml`文件。
2. 在目录管理 WorkSpace 或已加入 WorkSpaces 目录的 Amazon EC2 实例上，打开 Windows 文件资源管理器，然后在地址栏中输入贵组织的完全限定域名 (FQDN)，例如`\\example.com`。
3. 打开 `sysvol` 文件夹。
4. 打开带有 *FQDN* 名称的文件夹。
5. 打开 `Policies` 文件夹。您现在应该位于 `\\`*FQDN*`\sysvol\`*FQDN*`\Policies` 中。
6. 如果该文件尚不存在，请创建一个名为 `PolicyDefinitions` 的文件夹。
7. 打开 `PolicyDefinitions` 文件夹。
8. 将 `wsp.admx` 文件复制到 `\\`*FQDN*`\sysvol\`*FQDN*`\Policies\PolicyDefinitions` 文件夹中。
9. 在 `PolicyDefinitions` 文件夹中创建名为 `en-US` 的文件夹。
10. 打开 `en-US` 文件夹。
11. 将 `wsp.adml` 文件复制到 `\\`*FQDN*`\sysvol\`*FQDN*`\Policies\PolicyDefinitions\en-US` 文件夹中。

验证管理模板文件是否已正确安装

1. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)。
2. 扩大森林（森林:***FQDN***）。
3. 展开域。
4. 展开您的 FQDN（例如，`example.com`）。
5. 展开组策略对象。
6. 选择默认域策略，打开上下文（右键单击）菜单，然后选择编辑。

> **Note**
>
> 如果支持的域 WorkSpaces 是 Amazon Managed Microsoft AD 目录，则无法使用默认域策略来创建 GPO。相反，您必须在具有委派权限的域容器下创建和链接 GPO。
> 使用创建目录时 Amazon Managed Microsoft AD， Amazon Directory Service 会在域根目录下创建一个*yourdomainname*组织单位 (OU)。此 OU 的名称基于您在创建目录时键入的 NetBIOS 名称。如果您未指定 NetBIOS 名称，则此名称将默认为您目录 DNS 名称的第一部分（例如，如果目录 DNS 名称为 `corp.example.com`，则 NetBIOS 名称将为 `corp`）。
> 要创建您的 GPO，请不要选择默认域策略，而是选择 O *yourdomainname* U（或该组织下的任何 OU），打开上下文（右键单击）菜单，然后选择在此域中创建 GPO，然后将其链接到此处。
> 有关 *yourdomainname* OU 的更多信息，请参阅《Amazon Directory Service 管理指南》中的创建内容。

7. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 DCV。
8. 现在，您可以使用此 DCV 组策略对象来修改使用 DCV WorkSpaces 时特有的组策略设置。

管理 DCV 的组策略设置

使用组策略设置来管理使用 DCV WorkSpaces 的 Windows

1. 确保在 WorkSpaces目录的域控制器的中央存储区中安装了最新的 DCV WorkSpaces 组策略管理模板。
2. 验证管理模板文件是否已正确安装。有关更多信息，请参阅 验证管理模板文件是否已正确安装。

配置对 DCV 的打印机支持

默认情况下， WorkSpaces 启用基本远程打印，它提供的打印功能有限，因为它在主机端使用通用打印机驱动程序来确保打印兼容。

连接到 Windows 的 Windows 客户端的高级远程打印 WorkSpaces允许您使用打印机的特定功能，例如双面打印，但需要在主机端和客户端安装匹配的打印机驱动程序。

您可以根据需要使用组策略设置来配置打印机支持。

基本打印与高级打印

方面	基础打印	高级打印
已使用的驱动程序	通用 XPS 驱动程序	打印机专用驱动程序
驱动程序安装	自动	手册（主机和客户端）
功能	仅限标准打印	完整的打印机功能（双面打印、纸盒选择、表面处理等）

何时使用高级打印：-双面（双面）打印-特定纸盒选择-精加工选项（装订、打孔）-标签打印（例如 Zebra 打印机）-色彩管理以及打印机的其他高级功能。

配置打印机 Support

配置打印机支持

1. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
2. 打开配置远程打印设置。
3. 在 Configure remote printing (配置远程打印) 对话框中，执行下列操作之一：
   - 对于基本打印：选择 “启用”。要自动使用客户端计算机当前的默认打印机，请选择 “将本地默认打印机映射到远程主机”。
   - 对于高级打印：选择 “启用”，然后选择 “启用高级打印”。要自动使用客户端计算机当前的默认打印机，请选择 “将本地默认打印机映射到远程主机”。启用该策略后，您需要在主机和客户端安装匹配的打印机驱动程序。
   - 要禁用打印，请选择禁用。
4. 选择确定。
5. 组策略设置更改将在下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：
   - 重启 WorkSpace （在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
   - 在管理命令提示符处，输入 **`gpupdate /force`**。

配置高级打印机重定向

先决条件

1. WorkSpaces 主机代理：版本 2.2.0.2116 或更高版本
2. Windows 客户端：版本 5.31.0 或更高版本
3. 打印机驱动程序：必须在 WorkSpace 和客户端设备上都安装匹配的打印机驱动程序

> **Note**
> 只有连接到 Windows 的 Windows 客户端才支持高级打印 WorkSpaces。macOS、Linux 和 Web 客户端将使用基本打印。

驱动程序版本匹配

选择 “高级打印” 后，将支持三种驱动程序验证模式：

驱动程序验证模式

Mode	行为	何时使用
仅限姓名（默认）	仅匹配驱动程序名称，忽略版本	需要最大兼容性
部分匹配	匹配 Major.Minor 版本（例如 10.6.x.x）	平衡兼容性和功能
精确匹配	需要精确的版本匹配	专用打印机（例如 Zebra 标签打印机）

要配置验证模式，请在 GPO 的打印机驱动程序验证下拉列表中设置仅名称、部分匹配或完全匹配。

> **Note**
> 当驱动程序验证失败时， WorkSpaces 会自动回退到基本打印。

验证配置

1. Connect 到 WorkSpace.
2. 打开 “设置” > “设备” > “打印机和扫描仪”。
3. 验证您的本地打印机是否显示有 “已重定向” 前缀。
4. 打印测试文档并单击 “打印机属性” 以验证高级选项是否可用。

问题排查

高级功能不可用：-验证是否在 GPO 中选择了 “启用高级打印”-根据您的验证模式检查驱动程序版本是否匹配-考虑使用部分验证模式而不是精确验证模式。请务必重新启动以使 GPO 上的任何更改生效。

打印机未出现：-验证是否已启用 “配置远程打印”-确保打印机已连接到客户端设备-重新启动 WorkSpace 会话

打印作业失败：-检查客户端上的驱动程序版本和 WorkSpace -查看日志，网址为：**`C:\ProgramData\Amazon\WSP\Logs\agentsession.log`**-在日志中查找 “已启用高级打印”

启用详细日志：在 “组策略” 中，在 “计算机配置” > “策略” > “管理模板” > “A ma zon > WSP” 下将配置日志详细程度设置为调试。

为 DCV 配置剪贴板重定向（复制/粘贴）

默认情况下， WorkSpaces 支持双向（复制/粘贴）剪贴板重定向。对于 Windows WorkSpaces，您可以使用组策略设置来禁用此功能或配置允许剪贴板重定向的方向。

为 Windows 配置剪贴板重定向 WorkSpaces

1. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
2. 打开 Configure clipboard redirection 设置。
3. 在配置剪贴板重定向对话框中，选择启用或禁用。

   启用配置剪贴板重定向后，以下剪贴板重定向选项将变为可用：

   - 选择复制并粘贴，以允许双向剪贴板复制和粘贴重定向。
   - 选择仅复制，以仅允许将数据从服务器剪贴板复制到客户端剪贴板。
   - 选择仅粘贴，以仅允许将数据从客户端剪贴板粘贴到服务器剪贴板。
4. 选择确定。

5. 组策略设置更改将在下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：
   - 重启 WorkSpace （在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
   - 在管理命令提示符处，输入 **`gpupdate /force`**。

已知限制

启用剪贴板重定向后 WorkSpace，如果您从 Microsoft Office 应用程序中复制大于 890 KB 的内容，则该应用程序可能会变慢或在长达 5 秒钟内没有响应。

为 DCV 设置会话恢复超时

网络连接中断时，您的活动 WorkSpaces 客户端会话将断开。 WorkSpaces 如果网络连接在一定时间内恢复，则适用于 Windows 和 macOS 的客户端应用程序会尝试自动重新连接会话。默认的会话恢复超时时间为 20 分钟（1200 秒），但您可以修改该值 WorkSpaces ，因为该值由您的域的组策略设置控制。

要设置自动会话恢复超时值

1. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
2. 打开启用/禁用自动重新连接设置。
3. 在启用/禁用自动重新连接对话框中，选择启用，然后将重新连接超时（秒）设置为所需的超时时间（以秒为单位）
4. 选择确定。
5. 组策略设置更改将在下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：
   - 重启 WorkSpace （在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
   - 在管理命令提示符处，输入 **`gpupdate /force`**。

为 DCV 配置视频输入重定向

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

为 Windows 配置视频输入重定向 WorkSpaces

1. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
2. 打开启用/禁用视频输入重定向设置。
3. 在启用/禁用视频输入重定向对话框中，选择启用或禁用。
4. 选择确定。
5. 组策略设置更改将在下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：
   - 重启 WorkSpace （在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
   - 在管理命令提示符处，输入 **`gpupdate /force`**。

为 DCV 配置音频输入重定向

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

为 Windows 配置音频输入重定向 WorkSpaces

1. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
2. 打开启用/禁用音频输入重定向设置。
3. 在启用/禁用音频输入重定向对话框中，选择启用或禁用。
4. 选择确定。
5. 组策略设置更改将在下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：
   - 重启 WorkSpace （在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
   - 在管理命令提示符处，输入 **`gpupdate /force`**。

为 DCV 配置音频输出重定向

默认情况下， WorkSpaces 会将数据重定向到本地发言人。如果 Windows 需要 WorkSpaces，您可以使用组策略设置来禁用此功能。

为 Windows 配置音频输出重定向 WorkSpaces

1. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
2. 打开启用/禁用音频输出重定向设置。
3. 在启用/禁用音频输出重定向对话框中，选择启用或禁用。
4. 选择确定。
5. 组策略设置更改将在下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：
   - 重新启动 WorkSpace。在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作 > 重启 WorkSpaces。
   - 在管理命令提示符处，输入 **`gpupdate /force`**。

禁用 DCV 的时区重定向

默认情况下，工作区内的时间设置为镜像用于连接的客户端的时区 WorkSpace。此行为是通过时区重定向控制的。您可能需要关闭时区定向的原因有多种。例如：

- 您的公司希望所有员工在特定时区中工作（即使某些员工在其他时区）。
- 您在 a 中有计划任务 WorkSpace ，这些任务本应在特定时区的特定时间运行。
- 经常出差的用户希望将自己留 WorkSpaces 在一个时区，以保持一致性和个人喜好。

如果 Windows 需要 WorkSpaces，您可以使用组策略设置来禁用此功能。

禁用 Windows 的时区重定向 WorkSpaces

1. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
2. 打开启用/禁用时区重定向设置。
3. 在启用/禁用时区重定向对话框中，选择禁用。
4. 选择确定。
5. 组策略设置更改将在下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：
   - 重启 WorkSpace （在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
   - 在管理命令提示符处，输入 **`gpupdate /force`**。

6. 将的时区设置 WorkSpaces 为所需的时区。

的时区现在 WorkSpaces 是静态的，不再反映客户端计算机的时区。

配置 DCV 安全设置

对于 DCV，传输中数据使用 TLS 1.2 加密技术进行加密。默认情况下，允许使用以下所有密码进行加密，客户端和服务器协商使用哪种密码：

- ECDHE-RSA--GCM-AES128 SHA256
- ECDHE-ECDSA--GCM-AES128 SHA256
- ECDHE-RSA--GCM-AES256 SHA384
- ECDHE-ECDSA--GCM-AES256 SHA384
- ECDHE-RSA--AES128 SHA256
- ECDHE-RSA--AES256 SHA384

对于 Windows WorkSpaces，您可以使用组策略设置来修改 TLS 安全模式以及添加新密码套件或阻止某些密码套件。配置安全设置组策略对话框中提供了这些设置和支持的密码套件的详细说明。

配置 DCV 安全设置

1. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
2. 打开配置安全设置。
3. 在配置安全设置对话框中，选择启用。添加要允许的密码套件，并删除要屏蔽的密码套件。有关这些设置的更多信息，请参阅配置安全设置对话框中提供的说明。
4. 选择确定。
5. 组策略设置更改将在的下一次组策略更新之后以及您重新启动 WorkSpace会话之后生效。WorkSpace要应用组策略更改，请执行下列操作之一：
   - 要重启 WorkSpace，请在 Amazon WorkSpaces 控制台中选择 WorkSpace，然后选择操作，重启 WorkSpaces。
   - 在管理命令提示符处，输入 **`gpupdate /force`**。

为 DCV 配置扩展

默认情况下，对 WorkSpaces 扩展的支持处于禁用状态。如果需要，您可以通过以下方式 WorkSpace 将您的配置为使用扩展程序：

- 服务器和客户端 - 为服务器和客户端启用扩展
- 仅限服务器 - 仅为服务器启用扩展
- 仅限客户端 - 仅为客户端启用扩展

对于 Windows WorkSpaces，您可以使用组策略设置来配置扩展程序的使用。

为 DCV 配置扩展

1. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
2. 打开配置扩展设置。
3. 在配置扩展对话框中，选择启用，然后设置所需的支持选项。选择仅限客户端、服务器和客户端或仅限服务器。
4. 选择确定。
5. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及您重新启动 WorkSpace会话之后生效。要应用组策略更改，请执行下列操作之一：
   - 重新启动 WorkSpace。在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces。
   - 在管理命令提示符处，输入 **`gpupdate /force`**。

为 DCV 配置智能卡重定向

默认情况下，Amazon WorkSpaces 不支持使用智能卡进行会话前身份验证或会话中身份验证。会话前身份验证是指在用户登录时执行的智能卡身份验证。 WorkSpaces会话中身份验证是指登录后执行的身份验证。

如果需要，您可以使用组策略设置为 Windows WorkSpaces 启用会话前和会话中身份验证。还必须使用 EnableClientAuthentication API 操作或enable-client-authentication Amazon CLI 命令通过 AD Connector 目录设置启用会话前身份验证。有关更多信息，请参阅《Amazon Directory Service 管理指南》中的为 AD Connector 启用智能卡身份验证。

> **Note**
>
> 要在 Windows 中使用智能卡 WorkSpaces，需要执行其他步骤。有关更多信息，请参阅 在 “个人” 中 WorkSpaces 使用智能卡进行身份验证。

为 Windows 配置智能卡重定向 WorkSpaces

1. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
2. 打开启用/禁用智能卡重定向设置。
3. 在启用/禁用智能卡重定向对话框中，选择启用或禁用。
4. 选择确定。
5. 组策略设置更改将在会 WorkSpace话重新启动后生效。要应用组策略更改，请重启 WorkSpace（在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。

WebAuthn (FIDO2) DCV 的重定向

默认情况下，Amazon WorkSpaces 启用 WebAuthn 重定向，允许用户使用其本地 FIDO2兼容的安全密钥和生物识别身份验证器来运行在其中的应用程序。 WorkSpace此功能可安全地将身份验证请求从中的应用程序重定向 WorkSpace 到用户的本地设备，从而可以无缝访问身份验证方法，包括 Yubikeys 和 Windows Hello。

Amazon WorkSpaces 支持两个版本的 WebAuthn 重定向：

- 标准 WebAuthn-对于基于浏览器的应用程序，需要浏览器扩展程序（在 Windows 和 Linux WorkSpaces 上均受支持）
- 增强 WebAuthn-无需浏览器扩展，具有额外的本机应用程序支持， WorkSpaces 仅在 Windows 上支持

标准 WebAuthn 重定向

标准 WebAuthn 重定向需要浏览器扩展程序，以便将 WebAuthn 提示重定向到客户端设备。

版本要求

- Windows WorkSpaces：DCV 主机代理版本 2.0.0.1425 或更高版本
- 客户端版本：

- Windows 客户端：5.19.0 或更高版本
- Mac 客户端：5.19.0 或更高版本
- Linux 客户端：2024.0 或更高版本

上支持的浏览器 WorkSpaces

- Google Chrome 116+
- Microsoft Edge 116+

增强的 WebAuthn 重定向

增强的 WebAuthn 重定向功能消除了对浏览器扩展的需求，并支持在支持 WebAuthn 身份验证的本机 Windows 应用程序中 WebAuthn 进行身份验证。

版本要求

- Windows WorkSpaces：DCV 主机代理版本 2.1.0.2000 或更高版本
- 客户端版本：
  - Windows 客户端：5.29.0 或更高版本
  - Mac 客户端：5.29.0 或更高版本

主要优势

- 无需浏览器扩展程序
- 提高性能
- 支持原 WebAuthn 生 Windows 应用程序
- 跨浏览器和桌面应用程序的无缝身份验证体验

上支持的浏览器 WorkSpaces

- Google Chrome 116+
- Microsoft Edge 116+

配置 WebAuthn 重定向

为 Windows 配置 WebAuthn 重定向 WorkSpaces

1. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 DCV。
2. 打开 “配置 WebAuthn 重定向” 设置。
3. 在 “配置 WebAuthn 重定向” 对话框中，选择 “启用” 或 “禁用”。
4. 选择确定。
5. 组策略设置更改将在会 WorkSpace 话重新启动后生效。要应用组策略更改，请转至 Amazon WorkSpaces 控制台并选择，重新启动 WorkSpace。 WorkSpace 然后，选择操作，重新启动 WorkSpaces。

> **Note**
>
> 此组策略设置启用 WebAuthn 重定向。使用的版本（标准版或增强版）取决于您的主机代理版本和操作系统支持。

配置 WebAuthn 进程兼容性

启用 WebAuthn 重定向后，您可以通过进程兼容性列表配置允许哪些应用程序和WebAuthn 进程使用 WebAuthn 重定向。

默认进程兼容性列表

默认情况下，以下进程已启用 WebAuthn 重定向：

```
['chrome.exe','msedge.exe','island.exe','firefox.exe','dcvwebauthnnativemsghost.exe','msedgeweb
```

标准版所需的流程 WebAuthn

- `dcvwebauthnnativemsghost.exe`-此过程是标准版 WebAuthn 功能所必需的，使用标准版时必须保留在兼容性列表中 WebAuthn。

配置 WebAuthn 进程兼容性列表

1. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 DCV。
2. 打开 “配置 WebAuthn 重定向” 设置。

3. 选择 Enabled (已启用)。
4. 在WebAuthn 进程兼容性列表字段中，指定与 WebAuthn 重定向兼容的进程名称列表。
   - 使用默认列表作为起点
   - 根据需要为您的环境添加其他进程名称
5. 选择确定。
6. 组策略设置更改将在会 WorkSpace 话重新启动后生效。

进程兼容性列表指南

- 对于标准版 WebAuthn：请务必包含`dcvwebauthnnativemsghost.exe`在列表中
- 自定义应用程序：添加您的环境中需要 WebAuthn 支持的任何其他`.exe`进程名称
- 格式：使用逗号分隔的进程名称，用方括号括起来，每个进程名称用单引号引起来

自定义进程列表示例

```
['chrome.exe','msedge.exe','firefox.exe','dcvwebauthnnativemsghost.exe','msedgewebview2.exe','M
```

从标准版过渡到增强版 WebAuthn

从标准版升级 WebAuthn 到增强版时 WebAuthn，用户需要先卸载或禁用之前为标准版安装的 Amazon DCV WebAuthn 重定向浏览器扩展程序， WebAuthn 然后才能使用增强版。 WebAuthn

为什么这一步很重要？

- 增强版无需浏览器扩展程序即可原生 WebAuthn 处理重定向
- 将扩展程序保持启用状态将默认为标准 WebAuthn 重定向

安装 Amazon DCV WebAuthn 重定向扩展（仅限标准 WebAuthn 版）

> **Note**
>
> 本节仅适用于标准版 WebAuthn。增强版 WebAuthn 不需要浏览器扩展。

启用 Amazon DCV WebAuthn 重定向扩展 WebAuthn 后，用户需要安装 Amazon DCV 重定向扩展才能使用该功能，方法是执行以下任一操作：

- 系统将提示用户在其浏览器中启用浏览器扩展。

> **Note**
>
> 这是一次性浏览器提示。当您将 DCV 代理版本更新为 2.0.0.1425 或更高版本时，您的用户将收到通知。如果您的最终用户不需要 WebAuthn 重定向，他们只需从浏览器中删除扩展程序即可。您也可以使用 GPO 策略阻止 WebAuthn 重定向扩展安装提示。

- 您可以使用 GPO 策略为用户强制安装重定向扩展程序。如果您启用了 GPO 策略，则当您的用户启动支持的浏览器并访问 Internet 时，扩展将自动安装。
- 用户可以使用 Microsoft Edge 加载项或 Chrome 网上商店，手动安装扩展。

了解 WebAuthn 重定向扩展原生消息

WebAuthn Chrome 和 Edge 浏览器中的重定向使用浏览器扩展程序和本机消息传递主机。原生消息传递主机是一个用于实现扩展程序与主机应用程序之间通信的组件。在典型配置中，浏览器默认允许所有原生消息传递主机。但是，您可以选择使用原生消息传递阻止列表，其中 * 的值表示除非明确允许，否则所有原生消息传递主机都将被拒绝。在这种情况下，您需要通过在允许列表中明确指定值`com.dcv.webauthnredirection.nativemessagehost`来启用 Amazon DCV WebAuthn 重定向原生消息主机。

有关更多信息，请按照您的浏览器适用的指南进行操作：

- 对于 Google Chrome，请参阅 Native Messaging allowed hosts。
- 对于 Microsoft Edge，请参阅 Native Messaging。

使用组策略管理和安装浏览器扩展

您可以使用组策略安装 Amazon DCV WebAuthn 重定向扩展，既可以从您的域集中安装加入 Active Directory (AD) 域的会话主机，也可以使用本地组策略编辑器安装每个会话主机。此过程因您使用的浏览器而有所不同。

对于 Microsoft Edge

1. 下载并安装 Microsoft Edge 管理模板。
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)。
3. 扩大森林（森林:***FQDN***）。

4. 展开域。
5. 展开您的 FQDN（例如，`example.com`）。
6. 展开组策略对象。
7. 选择默认域策略，打开上下文（右键单击）菜单，然后选择编辑。
8. 依次选择计算机配置、管理模板、Microsoft Edge 和扩展
9. 打开配置扩展管理设置，并将其设置为启用。
10. 在配置扩展管理设置下，输入以下内容：

```
{"ihejeaahjpbegmaaegiikmlphghlfmeh":
{"installation_mode":"force_installed","update_url":"https://edge.microsoft.com/
extensionwebstorebase/v1/crx"}}
```

11. 选择确定。
12. 组策略设置更改将在会 WorkSpace 话重新启动后生效。要应用组策略更改，请转至 Amazon WorkSpaces 控制台并选择，重新启动 WorkSpace。 WorkSpace 然后，选择操作，重新启动 WorkSpaces）。

> **Note**
>
> 您可以通过应用以下配置管理设置来阻止安装扩展：
>
> ```
> {"ihejeaahjpbegmaaegiikmlphghlfmeh":
> {"installation_mode":"blocked","update_url":"https://edge.microsoft.com/
> extensionwebstorebase/v1/crx"}}
> ```

对于 Google Chrome

1. 下载并安装 Google Chrome 管理模板。如需了解详情，请参阅将 Chrome 浏览器政策设置为托管 PCs。
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)。
3. 扩大森林（森林:***FQDN***）。
4. 展开域。
5. 展开您的 FQDN（例如，`example.com`）。

6. 展开组策略对象。
7. 选择默认域策略，打开上下文（右键单击）菜单，然后选择编辑。
8. 依次选择计算机配置、管理模板、Google Chrome 和扩展
9. 打开配置扩展管理设置，并将其设置为启用。
10. 在配置扩展管理设置下，输入以下内容：

```
{"mmiioagbgnbojdbcjoddlefhmcocfpmn":
{ "installation_mode":"force_installed","update_url":"https://clients2.google.com/
service/update2/crx"}}
```

11. 选择确定。
12. 组策略设置更改将在会 WorkSpace 话重新启动后生效。要应用组策略更改，请转至 Amazon WorkSpaces 控制台并选择，重新启动 WorkSpace。 WorkSpace 然后，选择操作，重新启动 WorkSpaces）。

> **Note**
>
> 您可以通过应用以下配置管理设置来阻止安装扩展：
>
> ```
> {"mmiioagbgnbojdbcjoddlefhmcocfpmn":
> { "installation_mode":"blocked","update_url":"https://clients2.google.com/
> service/update2/crx"}}
> ```

为 DCV 配置 WebRTC 重定向

WebRTC 重定向通过将音频和视频处理 WorkSpaces 从本地客户端卸载到本地客户端来增强实时通信，从而提高性能并减少延迟。但是，WebRTC重定向并不普遍，需要第三方应用程序供应商与之开发特定的集成。 WorkSpaces默认情况下，WebRTC 重定向未启用。 WorkSpaces要使用 WebRTC 重定向，请确保满足以下条件：

- 第三方应用程序供应商集成
- WorkSpaces 扩展通过组策略设置启用
- WebRTC 重定向已启用
- WebRTC 重定向浏览器扩展已安装并启用

> **Note**
>
> 此重定向是作为扩展实现的，需要您使用组策略设置启用对 WorkSpaces 扩展的支持。如果扩展遭到禁用，WebRTC 重定向将无法运行。

要求

DCV 的 WebRTC 重定向需要满足以下条件：

- DCV 主机代理 2.0.0.1622 或更高版本
- WorkSpaces 客户：
  - Windows 5.21.0 或更高版本
  - Web 客户端
- WorkSpaces 运行亚马逊 DCV WebRTC 重定向扩展程序时安装的网络浏览器：
  - Google Chrome 116+
  - Microsoft Edge 116+

启用或禁用 Windows 版 WebRTC 重定向 WorkSpaces

如果需要，您可以使用组策略设置启用或禁用对 WorkSpaces Windows版WebRTC重定向的支持。如果您禁用或未配置此设置，WebRTC 重定向将遭到禁用。

启用该功能后，与 Amazon 集成的网络应用程序 WorkSpaces 将能够将 WebRTC API 调用重定向到本地客户端。

要为 Windows 配置 WebRTC 重定向 WorkSpaces

1. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
2. 打开配置 WebRTC 重定向设置。
3. 在配置 WebRTC 重定向对话框中，选择启用或禁用。
4. 选择确定。
5. 组策略设置更改将在会 WorkSpace 话重新启动后生效。要应用组策略更改，请转至 Amazon WorkSpaces 控制台并选择，重新启动 WorkSpace。 WorkSpace 然后，选择操作，重新启动 WorkSpaces）。

安装 Amazon DCV WebRTC 重定向扩展

在启用 WebRTC 重定向功能后，用户需要安装 Amazon DCV WebRTC 重定向扩展才能使用该功能，方法是执行以下任一操作：

- 系统将提示用户在其浏览器中启用浏览器扩展。

> **Note**
>
> 作为一次性浏览器提示，当您启用 WebRTC 重定向时，用户将收到通知。

- 您可以使用以下 GPO 策略，为用户强制安装重定向扩展。如果您启用 GPO 策略，则当用户启动支持的浏览器并访问 Internet 时，扩展将自动安装。
- 用户可以使用 Microsoft Edge 加载项或 Chrome 网上商店，手动安装扩展。

使用组策略管理和安装浏览器扩展

您可以使用组策略安装 Amazon DCV WebRTC 重定向扩展，既可以从您的域集中安装已加入 Active Directory（AD）域的会话主机，也可以为每个会话主机使用本地组策略编辑器。此过程将根据您使用的浏览器而有所不同。

对于 Microsoft Edge

1. 下载并安装 Microsoft Edge 管理模板。
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)。
3. 扩大森林（森林:***FQDN***）。
4. 展开域。
5. 展开您的 FQDN（例如，`example.com`）。
6. 展开组策略对象。
7. 选择默认域策略，打开上下文（右键单击）菜单，然后选择编辑。
8. 依次选择计算机配置、管理模板、Microsoft Edge 和扩展
9. 打开配置扩展管理设置，并将其设置为启用。
10. 在配置扩展管理设置下，输入以下内容：

```
{"kjbbkjjiecchbcdoollhgffghfjnbhef":
{"installation_mode":"force_installed","update_url":"https://edge.microsoft.com/
extensionwebstorebase/v1/crx"}}
```

11. 选择确定。
12. 组策略设置更改将在会 WorkSpace 话重新启动后生效。要应用组策略更改，请转至 Amazon WorkSpaces 控制台并选择，重新启动 WorkSpace。 WorkSpace 然后，选择操作，重新启动 WorkSpaces）。

> **Note**
>
> 您可以通过应用以下配置管理设置来阻止安装扩展：
>
> ```
> {"kjbbkjjiecchbcdoollhgffghfjnbhef":
> {"installation_mode":"blocked","update_url":"https://edge.microsoft.com/
> extensionwebstorebase/v1/crx"}}
> ```

对于 Google Chrome

1. 下载并安装 Google Chrome 管理模板。如需了解详情，请参阅将 Chrome 浏览器政策设置为托管 PCs。
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)。
3. 扩大森林（森林:***FQDN***）。
4. 展开域。
5. 展开您的 FQDN（例如，`example.com`）。
6. 展开组策略对象。
7. 选择默认域策略，打开上下文（右键单击）菜单，然后选择编辑。
8. 依次选择计算机配置、管理模板、Google Chrome 和扩展
9. 打开配置扩展管理设置，并将其设置为启用。
10. 在配置扩展管理设置下，输入以下内容：

```
{"diilpfplcnhehakckkpmcmibmhbingnd":
{ "installation_mode":"force_installed","update_url":"https://clients2.google.com/
service/update2/crx"}}
```

11. 选择确定。
12. 组策略设置更改将在会 WorkSpace 话重新启动后生效。要应用组策略更改，请转至 Amazon WorkSpaces 控制台并选择，重新启动 WorkSpace。 WorkSpace 然后，选择操作，重新启动 WorkSpaces）。

> **Note**
>
> 您可以通过应用以下配置管理设置来阻止安装扩展：
>
> ```
> {"diilpfplcnhehakckkpmcmibmhbingnd":
> { "installation_mode":"blocked","update_url":"https://clients2.google.com/
> service/update2/crx"}}
> ```

配置 DCV 屏幕锁定时断开会话连接

如果需要，可以在检测到 Windows 锁屏时断开用户的 WorkSpaces 会话。要从 WorkSpaces 客户端重新连接，用户可以使用自己的密码或智能卡进行身份验证，具体取决于为其 WorkSpaces启用了哪种类型的身份验证。

默认情况下，该组策略设置处于禁用状态。如果需要，您可以使用组策略设置启用在检测到 Windows 锁屏时断 WorkSpaces 开会话连接。

> **Note**
>
> - 此组策略设置适用于密码身份验证的会话和智能卡身份验证的会话。
> - 要在 Windows 中使用智能卡 WorkSpaces，需要执行其他步骤。有关更多信息，请参阅 在“个人”中 WorkSpaces 使用智能卡进行身份验证。

为 Windows 配置屏幕锁定时断开连接会话 WorkSpaces

1. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。

2. 打开启用/禁用屏幕锁定时断开会话连接设置。
3. 在启用/禁用屏幕锁定时断开会话连接对话框中，选择启用或禁用。
4. 选择确定。
5. 组策略设置更改将在下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：
   - 重启 WorkSpace（在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
   - 在管理命令提示符处，输入 **`gpupdate /force`**。

为 DCV 配置屏幕截图保护

屏幕捕获保护可防止来自本地客户端工具的屏幕截图、屏幕录制和屏幕共享 WorkSpaces 会话。启用后，尝试从客户端捕获屏幕内容将显示背景或黑色矩形，这有助于保护敏感信息免遭泄露。

要求

DCV 的屏幕截图保护需要满足以下条件：

- DCV 主机代理版本 2.2.0.2116 或更高版本
- WorkSpaces 客户：
  - Windows 5.30.2 或更高版本
  - macOS 5.30.2 或更高版本

> **Note**
>
> - Linux 客户端、Web 访问或 PCo IP 协议不支持此功能。
> - 保护适用于从客户端设备启动的捕获。用户仍然可以从内部截取屏幕截图。 WorkSpace
> - 该功能与 MS Teams 上的屏幕共享不兼容。

已知限制条件

- 该功能无法阻止物理摄像机捕捉屏幕。
- 该功能不能防止直接通过 RDP 连接到主机服务器。

- 该功能无法防止从 WorkSpace 自身内部发起的捕获尝试，包括协作和聊天工具的屏幕共享功能。
- 启用后，所有捕获方法都将被阻止（选择性屏蔽不可用）。
- 如果启用该功能并尝试捕捉视频（例如，尝试屏幕共享客户端窗口），macOS 客户端窗口可能会变灰。

为 Windows 配置屏幕截图保护 WorkSpaces

1. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
2. 打开 “配置屏幕截图保护” 设置。
3. 在 “配置屏幕截图保护” 对话框中，选择 “启用” 或 “禁用”。
4. 选择确定。
5. 组策略设置更改将在下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：
   a. 重新启动 WorkSpace （在 WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重新启动 WorkSpaces）。
   b. 在管理命令提示符处，输入 `gpupdate /force`。

为 DCV 配置间接显示驱动程序（IDD）

默认情况下， WorkSpaces 支持使用间接显示驱动程序 (IDD)。如果 Windows 需要 WorkSpaces，您可以使用组策略设置来禁用此功能。

要为 Windows 配置间接显示驱动程序 (IDD) WorkSpaces

1. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
2. 打开 “启用 Amazon 间接显示驱动程序” 设置。
3. 在 “启用 Amazon 间接显示驱动程序” 对话框中，选择 “启用” 或 “禁用”。
4. 选择确定。
5. 组策略设置更改将在下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：
   a. 重新启动 WorkSpace （在 WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重新启动 WorkSpaces）。
   b. 在管理命令提示符处，输入 `gpupdate /force`。

配置 DCV 的显示设置

WorkSpaces 允许您配置多种不同的显示设置，包括最大帧速率、最低图像质量、最大图像质量和 YUV 编码。根据所需的图像质量、响应能力和色彩准确度，调整这些设置。

默认情况下，最大帧速率值为 25。最大帧速率值用于指定允许的最大每秒帧数 (fps)。值 0 表示无限制。

默认情况下，最低图像质量值为 30。可以对最低图像质量进行优化，以获得最佳图像响应能力或最佳图像质量。为了获得最佳响应能力，请减少最低质量。要获得最佳质量，请增加最低质量。

- 最佳响应能力的理想值介于 30 和 90 之间。
- 最佳质量的理想值介于 60 和 90 之间。

默认情况下，最大图像质量值为 80。最大图像质量不会影响图像的响应能力或质量，但会设置最大值以限制网络使用量。

默认情况下，图像编码设置为 YUV42 0。选择 “启用 YUV444编码” 可启用 YUV444 编码以实现高色彩精度。

对于 Windows WorkSpaces，您可以使用组策略设置来配置最大帧速率、最低图像质量和最大图像质量值。

配置 Windows 的显示设置 WorkSpaces

1. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
2. 打开配置显示设置设置。
3. 在配置显示设置对话框中，选择启用，然后将最大帧速率 (fps)、最低图像质量和最大图像质量值设置为所需的级别。
4. 选择确定。
5. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及您重新启动 WorkSpace会话之后生效。要应用组策略更改，请执行下列操作之一：
    - 重启 WorkSpace. Amazon WorkSpaces 控制台，选择 WorkSpace，然后选择操作，重启 WorkSpaces
    - 在管理命令提示符处，输入 **`gpupdate /force`**。

为 DC VSync V 的仅限 Amazon 虚拟显示屏的驱动程序进行配置

默认情况下， WorkSpaces 支持将该 VSync 功能用于仅限 Amazon 虚拟显示屏的驱动程序。如果 Windows 需要 WorkSpaces，您可以使用组策略设置来禁用此功能。

要为 Windows VSync 进行配置 WorkSpaces

1. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
2. 打开 “仅限 Amazon 虚拟显示器驱动程序” 设置的 “启用” VSync 功能。
3. 在 “仅 Amazon 虚拟显示器驱动程序” 对话框的 “启用” VSync 功能中，选择 “启用” 或 “禁用”。
4. 选择确定。
5. 组策略设置更改将在下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作：

   a. WorkSpace 通过执行以下任一操作重新启动：

      i. 选项 1-在 WorkSpaces 控制台中，选择 WorkSpace 要重新启动的。然后，选择操作，重新启动 WorkSpaces。

      ii. 选项 2 - 在管理命令提示符处，输入 `gpupdate /force`。

   b. 要应用设置 WorkSpace ，请重新连接到。

   c. 再次重启 WorkSpace。

配置 DCV 的日志详细程度

默认情况下，DCV 的日志详细级别设置 WorkSpaces 为 Info。您可以将日志级别设置为详细程度级别（从最不详细到最详细），详见此处：

- 错误 - 最不详细
- 警告
- 信息 - 默认
- 调试 - 最详细

对于 Windows WorkSpaces，您可以使用组策略设置来配置日志详细级别。

为 Windows 配置日志详细级别 WorkSpaces

1. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。

2. 打开配置日志详细程度设置。
3. 在配置日志详细程度对话框中，选择启用，然后将日志详细程度级别设置为调试、错误、信息或警告。
4. 选择确定。
5. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及您重新启动 WorkSpace会话之后生效。要应用组策略更改，请执行下列操作之一：
   - 重新启动 WorkSpace。在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces。
   - 在管理命令提示符处，输入 **`gpupdate /force`**。

为 DCV 配置空闲断开连接超时

WorkSpaces 允许您配置用户在连接到、断开连接之前可以处于非活动状态的时间长度。 WorkSpace 以下为用户活动输入示例：

- 键盘事件
- 鼠标事件（光标移动、滚动、单击）
- 触控笔事件
- 触摸事件（点击触摸屏、平板电脑）
- 游戏手柄事件
- 文件存储操作（上传、下载、目录创建、列表项）
- 网络摄像头流式传输

音频输入、音频输出和像素更改不符合用户活动条件。

启用空闲断开连接超时后，您可以选择通知您的用户，即：除非互动，否则他们的会话将在配置的时间内断开连接。

默认情况下，空闲断开连接超时处于禁用状态，超时值设置为 0 分钟，通知处于禁用状态。如果启用此策略设置，则空闲断开连接超时值默认为 60 分钟，空闲断开连接警告值默认为 60 秒。对于 Windows WorkSpaces，您可以使用组策略设置来配置此功能。

为 Windows 配置空闲断开连接超时 WorkSpaces

1. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。

2. 打开配置空闲断开连接超时设置。
3. 在配置空闲断开连接超时对话框中，选择启用，然后设置所需的断开连接超时值（以分钟为单位），也可以选择设置警告计时器值（以秒为单位）。
4. 选择应用、确定。
5. 组策略设置的更改会在您应用更改后立即生效。

为 DCV 配置文件传输

默认情况下，Amazon WorkSpaces 会禁用文件传输功能。您可以启用它以允许用户在其本地计算机和 WorkSpaces 会话之间上传和下载文件。这些文件将保存在会 WorkSpaces 话的 “我的存储” 文件夹中。

在 Windows 上启用文件传输 WorkSpaces

1. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
2. 打开配置会话存储设置。
3. 在配置会话存储对话框中，选择启用。
4. （可选）指定用于会话存储的文件夹（例如，`c:/session-storage`）。如果未指定，则会话存储的默认文件夹将是主文件夹。
5. 您可以使用以下文件传输选项之一 WorkSpaces 进行配置：
   - 选择 `Download and Upload`，允许双向文件传输。
   - 选择仅`Upload Only`允许将文件从本地计算机上传到您的 WorkSpaces 会话。
   - 选择仅`Download Only`允许将文件从您的 WorkSpaces 会话下载到本地计算机。
6. 选择确定。
7. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及您重新启动 WorkSpace会话之后生效。要应用组策略更改，请执行下列操作之一：
   - 重新启动 WorkSpace。在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces。
   - 在管理命令提示符处，输入 **`gpupdate /force`**。

为 DCV 配置 USB 重定向

概述

从版本 2.2.0.2047 开始， WorkSpaces 亚马逊支持基于 DCV 的 WorkSpaces Windows 的通用 USB 重定向，允许用户在其虚拟桌面环境中访问本地 USB 设备。此功能补充了针对特定设备类别的现有优化重定向解决方案。

> **Note**
>
> Amazon 建议仅在没有经过优化的重定向解决方案的设备上使用通用重定向。如果可用，经过优化的重定向解决方案可提供更好的性能。

先决条件

- WorkSpaces 使用 DCV 协议版本为 2.2.0.2047 或更高版本的 Windows
- 最新版本的 WorkSpaces Windows 客户端（版本 5.30.0 或更高版本）
- 配置组策略设置的管理权限

配置

默认情况下，USB 重定向处于禁用状态。您可以使用组策略对象 (GPO) 启用该功能。启用该功能后，您可以将设备添加到允许列表中进行重定向。默认情况下，不在许可名单中的设备无法进行重定向。

组策略配置

使用组策略为 DCV 配置 USB 重定向

1. Connect 到 Windows WorkSpaces。
2. 从`C:\Program Files\Amazon\WSP`文件夹中复制策略模板文件（`wsp.admx`和`wsp.adml`）。
3. 粘贴`wsp.admx`到`C:\Windows\PolicyDefinitions`文件夹。
4. 粘贴`wsp.adml`到`C:\Windows\PolicyDefinitions\en-US`文件夹。
5. 启动本地 GPO 编辑器 (gpedit.msc)。
6. 导航到本地计算机策略 > 计算机配置 > 管理模板 > Amazon > WSP。
7. 在 WSP 设置中配置启用/禁用 USB。
8. 选择 “启用” 以激活 USB 重定向。

> **Note**
>
> 对此设置的更改将在下次连接时生效。

设备管理

启用 USB 重定向后，您可以在 GPO 中配置设备许可名单，以添加要支持重定向的设备。

设备许可名单配置

USB 重定向遵循默认的 “全部拒绝” 安全立场。管理员必须使用以下格式将设备添加到 GPO 的许可名单，从而明确允许这些设备：

```
Name, Base class, Subclass, Protocol, Id Vendor, Id Product, Support Auto-share, Skip
 reset
// Use * to skip any values
```

示例：

添加带有供应商 ID/Product ID 的设备：

```
Credit Card Reader, *, *, *, 0x0483, 0x2016, 1, 0
// Allows Credit Card Reader with VID 0x0483 and PID 0x2016 with auto-share support
```

添加具有类/子类的设备：

```
3D Mouse Devices, 03, 01, *, *, *, 1, 0
// Allows all 3D mice using HID class (03), boot interface subclass (01), with auto-
share support
```

> **Note**
>
> 在将设备添加到许可名单之前，先对其进行兼容性和性能测试。

安全考虑因素

最佳实践

- 如果支持的设备可用，请使用专用的重定向方法，以获得最佳性能和兼容性。例如，对于诸如此类的安全密钥 YubiKey，请 WebAuthn 改用重定向。
- 实施严格的设备许可名单。
- 通过审核日志监控设备访问情况。
- 在允许使用新设备之前，请先评估数据安全影响。

为 DCV 配置网络摄像头分辨率

使用此设置来配置网络摄像头分辨率设置。如果启用此策略设置，则可以指定：

- 最大网络摄像头分辨率：它指定可从提供的分辨率中选择的最大网络摄像头分辨率。如果缺少此值或（0, 0），则使用默认值。
- 首选的网络摄像头分辨率：它指定客户端提供的分辨率中首选的网络摄像头分辨率。如果不支持指定的分辨率，则会选择最接近的匹配分辨率。如果缺少此值或（0, 0），则使用默认值。

如果您禁用或未配置此策略设置，则使用默认分辨率。

为 Windows 配置网络摄像头分辨率 WorkSpaces

1. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
2. 打开配置网络摄像头分辨率设置。
3. 在 “配置网络摄像头分辨率” 对话框中，选择 “启用”，然后设置摄像头最大分辨率（以像素为单位） and/or 首选摄像头分辨率（以像素为单位）。
4. 选择确定。
5. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及您重新启动 WorkSpace会话之后生效。要应用组策略更改，请执行下列操作之一：
    - 重新启动 WorkSpace。在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces。
    - 在管理命令提示符处，输入 **`gpupdate /force`**。

配置 DCV 的服务器键盘布局使用情况

此设置可控制是否使用服务器端键盘布局进行按键解析，而不是使用默认的客户端键盘布局。对此设置的更改将在下次连接时生效。有关键盘操作的更多详情，请参阅 Amazon WorkSpaces 用户指南。

如果启用此策略设置，则可以选择以下选项之一：

- 始终关闭：始终使用客户端布局
- 始终打开：始终使用服务器布局

如果您禁用或未配置此策略设置，则使用始终关闭选项。

> **Note**
>
> 亚马逊 WorkSpaces Windows 客户端版本 5.29.2 或更高版本以及亚马逊 m WorkSpaces acOS 客户端版本 5.30.0 或更高版本支持此功能。

配置 Windows 的服务器键盘布局使用情况 WorkSpaces

1. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、Amazon 和 WSP。
2. 打开配置服务器键盘布局使用设置。
3. 在配置服务器键盘布局使用对话框中，选择启用，然后设置服务器键盘布局选项。
4. 选择确定。
5. 组策略设置更改将在的下一次组策略更新之后 WorkSpace 以及您重新启动 WorkSpace会话之后生效。要应用组策略更改，请执行下列操作之一：
   - 重新启动 WorkSpace。在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces。
   - 在管理命令提示符处，输入 **`gpupdate /force`**。

安装 PCo IP 的组策略管理模板

要在使用 PCo IP 协议 WorkSpaces 时使用 Amazon 特有的组策略设置，您必须添加适用于您的 PCo IP 代理版本（32 位或 64 位）的组策略管理模板。 WorkSpaces

> **Note**
>
> 如果您混合使用 32 位和 64 位代理，则可以对 32 位代理使用组策略管理模板，并且您的组策略设置将同时应用于 32 位和 64 位代理。 WorkSpaces 当所有人 WorkSpaces 都在使用 64 位代理时，可以切换到使用 64 位代理的管理模板。

确定 WorkSpaces 您使用的是 32 位代理还是 64 位代理

1. 登录到 WorkSpace，然后通过选择 “查看”、“发送 Ctrl + Alt + Delete” 或右键单击任务栏并选择 “任务管理器” 来打开任务管理器。
2. 在任务管理器中，转到详细信息选项卡，右键单击列标题，然后选择选择列。
3. 在选择列对话框中，选择平台，然后选择确定。
4. 在 “详细信息” 选项卡上`pcoip_agent.exe`，查找，然后在 “平台” 列中检查其值，以确定 PCo IP 代理是 32 位还是 64 位。（您可能会看到 32 位和 64 位 WorkSpaces 组件的混合；这是正常现象。）

安装 PCo IP 的组策略管理模板（32 位）

要使用与 32 位 IP 代理一起使用 PCo IP 协议 WorkSpaces 时特有的组策略设置，必须安装 PCo IP 的组策略管理模板。 PCo对已加入目录的目录管理 WorkSpace 或 Amazon EC2 实例执行以下步骤。

有关使用.adm 文件的更多信息，请参阅 Microsoft 文档中的管理组策略管理模板 (.adm) 文件的建议。

安装 PCo IP 的组策略管理模板

1. 在正在运行的 Windows WorkSpace 中，复制`C:\Program Files (x86)\Teradici\PCoIP Agent\configuration`目录中的`pcoip.adm`文件。
2. 在目录管理 WorkSpace 或已加入您的 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)，然后导航到您的域中包含您的 WorkSpaces 计算机账户的组织单位。
3. 打开计算机账户组织单位对应的上下文 (右键单击) 菜单，然后选择在这个域中创建 GPO 并在此处链接...。
4. 在 “新建 GPO” 对话框中，输入 GPO 的描述性名称，例如WorkSpaces 计算机策略，并将 S ource Starter GPO 设置为（无）。选择确定。
5. 打开新 GPO 的上下文（右键单击）菜单，然后选择 Edit (编辑)。
6. 在组策略管理编辑器中，依次选择计算机配置、策略和管理模板。从主菜单中依次选择操作和添加/删除模板。

7. 在添加/删除模板对话框中，单击添加，选择之前复制的 `pcoip.adm` 文件，然后依次选择打开和关闭。
8. 关闭组策略管理编辑器。现在，您可以使用该 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 或已加入您的 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)，然后导航到您的 WorkSpaces 计算机账户并选择 WorkSpaces GPO。在主菜单中依次选择操作和编辑。
2. 在组策略管理编辑器中，选择计算机配置、策略、管理模板、经典管理模板和 PCoIP 会话变量。
3. 现在，您可以使用此 PCoIP 会话变量组策略对象来修改使用 PCo IP WorkSpaces 时特定于 Amazon 的组策略设置。

> **Note**
>
> 要允许用户覆盖您的设置，请选择可覆盖的管理员设置；否则，请选择不可覆盖的管理员设置。

安装 PCo IP 的组策略管理模板（64 位）

要使用特定于 WorkSpaces 使用 PCo IP 协议的组策略设置，必须将组策略管理模板`PCoIP.admx`和 PCo IP `PCoIP.adml` 文件添加到 WorkSpaces目录的域控制器的中央存储区。有关 `.admx` 和 `.adml` 文件的更多信息，请参阅如何在 Windows 中创建和管理组策略管理模板的中央存储。

以下过程介绍了如何创建中央存储并向其中添加管理模板文件。对已加入目录的目录管理 WorkSpace 或 Amazon EC2 实例执行以下步骤。 WorkSpaces

安装 PCo IP 的组策略管理模板文件

1. 在正在运行的 Windows WorkSpace 中，复制`C:\Program Files\Teradici\PCoIP Agent\configuration\policyDefinitions`目录中的`PCoIP.admx`和`PCoIP.adml`文件。`PCoIP.adml` 文件位于该目录的 `en-US` 子文件夹中。
2. 在目录管理 WorkSpace 或已加入 WorkSpaces 目录的 Amazon EC2 实例上，打开 Windows 文件资源管理器，然后在地址栏中输入贵组织的完全限定域名 (FQDN)，例如`\\example.com`。
3. 打开 `sysvol` 文件夹。
4. 打开带有 *`FQDN`* 名称的文件夹。

5. 打开 Policies 文件夹。您现在应该位于 *FQDN*\sysvol*FQDN*\Policies 中。
6. 如果该文件尚不存在，请创建一个名为 PolicyDefinitions 的文件夹。
7. 打开 PolicyDefinitions 文件夹。
8. 将 PCoIP.admx 文件复制到 *FQDN*\sysvol*FQDN*\Policies\PolicyDefinitions 文件夹中。
9. 在 PolicyDefinitions 文件夹中创建名为 en-US 的文件夹。
10. 打开 en-US 文件夹。
11. 将 PCoIP.adml 文件复制到 *FQDN*\sysvol*FQDN*\Policies\PolicyDefinitions\en-US 文件夹中。

验证管理模板文件是否已正确安装

1. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc)。
2. 扩大森林（森林:***FQDN***）。
3. 展开域。
4. 展开您的 FQDN（例如，example.com）。
5. 展开组策略对象。
6. 选择默认域策略，打开上下文（右键单击）菜单，然后选择编辑。

> **Note**
>
> 如果支持的域 WorkSpaces 是 Amazon Managed Microsoft AD 目录，则无法使用默认域策略来创建 GPO。相反，您必须在具有委派权限的域容器下创建和链接 GPO。
> 使用创建目录时 Amazon Managed Microsoft AD， Amazon Directory Service 会在域根目录下创建一个*yourdomainname*组织单位 (OU)。此 OU 的名称基于您在创建目录时键入的 NetBIOS 名称。如果您未指定 NetBIOS 名称，则此名称将默认为您目录 DNS 名称的第一部分（例如，如果目录 DNS 名称为 corp.example.com，则 NetBIOS 名称将为 corp）。
> 要创建您的 GPO，请不要选择默认域策略，而是选择 O *yourdomainname* U（或该组织下的任何 OU），打开上下文（右键单击）菜单，然后选择在此域中创建 GPO，然后将其链接到此处。
> 有关 *yourdomainname* OU 的更多信息，请参阅《Amazon Directory Service 管理指南》中的创建内容。

7. 在组策略管理编辑器中，选择计算机配置、策略、管理模板和 PCoIP 会话变量。
8. 现在，您可以使用此 PCoIP 会话变量组策略对象来修改使用 PCo IP WorkSpaces 时特有的组策略设置。

> **Note**
>
> 要允许用户覆盖您的设置，请选择可覆盖的管理员设置；否则，请选择不可覆盖的管理员设置。

管理 PCo IP 的组策略设置

使用组策略设置来管理使用 PCo IP WorkSpaces 的 Windows。

为 PCo IP 配置打印机支持

默认情况下， WorkSpaces 启用基本远程打印，它提供的打印功能有限，因为它在主机端使用通用打印机驱动程序来确保打印兼容。

Windows 客户端的高级远程打印让您可以使用打印机的特定功能（如双面打印），但需要在主机端安装匹配的打印机驱动程序。

远程打印实施为虚拟通道。如果虚拟通道被禁用，远程打印无法正常工作。

对于 Windows WorkSpaces，您可以根据需要使用组策略设置来配置打印机支持。

配置打印机支持

1. 确保已安装最新的 IP WorkSpaces 组策略管理模板（32 位）或最新 PCo的 IP WorkSpaces 组策略管理模板（64 位）。 PCo
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc) 并导航到 PCoIP 会话变量。
3. 打开配置远程打印设置。
4. 在 Configure remote printing (配置远程打印) 对话框中，执行下列操作之一：
   - 要启用高级远程打印，请选择已启用，然后在选项、Configure remote printing (配置远程打印) 下，选择 Basic and Advanced printing for Windows clients (适用于 Windows 客户端的基本和高级打印)。要自动使用客户端计算机的当前默认打印机，选择 Automatically set default printer (自动设置默认打印机)。

- 要禁用打印，请选择 Enabled (已启用)，然后在 Options (选项)、Configure remote printing (配置远程打印) 下选择 Printing disabled (已禁用打印)。

5. 选择确定。
6. 组策略设置更改将在下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：
   - 重启 WorkSpace （在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
   - 在管理命令提示符处，输入 **`gpupdate /force`**。

默认情况下，本地打印机自动重定向被禁用。您可以使用组策略设置来启用此功能，以便每次连接到您的本地打印机时都将您的本地打印机设置为默认打印机 WorkSpace。

> **Note**
>
> 本地打印机重定向不适用于亚马逊 Linux WorkSpaces。

启用本地打印机自动重定向

1. 确保已安装最新的 IP WorkSpaces 组策略管理模板（32 位）或最新 PCo的 IP WorkSpaces 组策略管理模板（64 位）。 PCo
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc) 并导航到 PCoIP 会话变量。
3. 打开配置远程打印设置。
4. 选择启用，然后在选项、配置远程打印下，选择以下一个选项：
   - 适用于 Windows 客户端的基本和高级打印
   - 基本打印
5. 选择自动设置默认打印机，然后选择确定。
6. 组策略设置更改将在下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：
   - 重启 WorkSpace （在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
   - 在管理命令提示符处，输入 **`gpupdate /force`**。

为 IP 配置剪贴板重定向（复制/粘贴） PCo

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

要启用或禁用剪贴板重定向

1. 确保已安装最新的 IP WorkSpaces 组策略管理模板（32 位）或最新 PCo的 IP WorkSpaces 组策略管理模板（64 位）。 PCo
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc) 并导航到 PCoIP 会话变量。
3. 打开 Configure clipboard redirection 设置。
4. 在配置剪贴板重定向对话框中，选择启用，然后选择以下设置之一以确定允许剪贴板重定向的方向。完成后，选择确定。
   - 双向禁用
   - 仅对客户端（WorkSpace 本地计算机）启用代理
   - 仅启用客户端到代理（本地计算机到 WorkSpace）
   - 双向启用
5. 组策略设置更改将在下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：
   - 重启 WorkSpace （在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
   - 在管理命令提示符处，输入 **`gpupdate /force`**。

已知限制

启用剪贴板重定向后 WorkSpace，如果您从 Microsoft Office 应用程序中复制大于 890 KB 的内容，则该应用程序可能会变慢或在长达 5 秒钟内没有响应。

为 PCo IP 设置会话恢复超时

网络连接中断时，您的活动 WorkSpaces 客户端会话将断开。 WorkSpaces 如果网络连接在一定时间内恢复，则适用于 Windows 和 macOS 的客户端应用程序会尝试自动重新连接会话。默认的会话恢复超时时间为 20 分钟，但您可以修改该值 WorkSpaces ，因为该值由您的域的组策略设置控制。

要设置自动会话恢复超时值

1. 确保已安装最新的 IP WorkSpaces 组策略管理模板（32 位）或最新 PCo的 IP WorkSpaces 组策略管理模板（64 位）。 PCo
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc) 并导航到 PCoIP 会话变量。
3. 打开 Configure Session Automatic Reconnection Policy 设置。
4. 在 Configure Session Automatic Reconnection Policy 对话框中，选择 Enabled，将 Configure Session Automatic Reconnection Policy 选项设置为所需的超时 (以分钟为单位)，然后选择 OK。
5. 组策略设置更改将在下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：
   - 重启 WorkSpace（在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
   - 在管理命令提示符处，输入 **`gpupdate /force`**。

为 IP 配置音频输入重定向 PCo

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

> **Note**
>
> 如果你的组策略设置限制了用户的本地登录 WorkSpaces，那么音频输入将无法在你的。WorkSpaces如果删除该组策略设置，则下次重新启动后将启用音频输入功能。 WorkSpace有关此组策略设置的更多信息，请参阅 Microsoft 文档中的允许本地登录。

启用或禁用音频输入重定向

1. 确保已安装最新的 IP WorkSpaces 组策略管理模板（32 位）或最新 PCo的 IP WorkSpaces 组策略管理模板（64 位）。 PCo
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc) 并导航到 PCoIP 会话变量。
3. 在 PCoIP 会话设置中打开 “启用/禁用音频”。
4. 在 PCoIP 会话中启用/禁用音频对话框中，选择启用或禁用。

5. 选择确定。
6. 组策略设置更改将在下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：
   - 重启 WorkSpace （在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
   - 在管理命令提示符处，输入 **`gpupdate /force`**。

禁用 IP 的时区重定 PCo向

默认情况下，工作区内的时间设置为镜像用于连接的客户端的时区 WorkSpace。此行为是通过时区重定向控制的。您可能需要关闭时区定向的原因有多种：

- 您的公司希望所有员工在特定时区中工作（即使某些员工在其他时区）。
- 您在 a 中有计划任务 WorkSpace ，这些任务本应在特定时区的特定时间运行。
- 经常出差的用户希望将自己留 WorkSpaces 在一个时区，以保持一致性和个人喜好。

如果 Windows 需要 WorkSpaces，您可以使用组策略设置来禁用此功能。

禁用时区重定向

1. 确保已安装最新的 IP WorkSpaces 组策略管理模板（32 位）或最新 PCo的 IP WorkSpaces 组策略管理模板（64 位）。 PCo
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc) 并导航到 PCoIP 会话变量。
3. 打开配置时区重定向设置。
4. 在配置时区重定向对话框中，选择禁用。
5. 选择确定。
6. 组策略设置更改将在下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：
   - 重启 WorkSpace （在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
   - 在管理命令提示符处，输入 **`gpupdate /force`**。
7. 将的时区设置 WorkSpaces 为所需的时区。

的时区现在 WorkSpaces 是静态的，不再反映客户端计算机的时区。

配置 PCo IP 安全设置

对于 PCo IP，传输中的数据使用 TLS 1.2 加密和 Sigv4 请求签名进行加密。 PCoIP 协议使用加密 UDP 流量和 AES 加密，用于流式传输像素。使用端口 4172（TCP 和 UDP）的流式传输连接通过 AES-128 和 AES-256 密码进行加密，但加密默认为 128 位。您可以使用 “配置 PCo IP 安全设置” 组策略设置将此默认值更改为 256 位。

您还可以使用此组策略设置来修改 TLS 安全模式以及屏蔽某些密码套件。配置 PCo IP 安全设置组策略对话框中提供了这些设置和支持的密码套件的详细说明。

配置 PCo IP 安全设置

1. 确保已安装最新的 IP WorkSpaces 组策略管理模板（32 位）或最新 PCo的 IP WorkSpaces 组策略管理模板（64 位）。 PCo
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc) 并导航到 PCoIP 会话变量。
3. 打开 “配置 PCo IP 安全设置” 设置。
4. 在 “配置 PCo IP 安全设置” 对话框中，选择 “启用”。要将流媒体流量的默认加密设置为 256 位，请转到 “PCoIP 数据加密密码” 选项，然后仅选择 AES-256-GCM。
5. （可选）调整 TLS 安全模式设置，然后列出要屏蔽的所有密码套件。有关这些设置的更多信息，请参阅 “配置 PCo IP 安全设置” 对话框中提供的说明。
6. 选择确定。
7. 组策略设置更改将在下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：
   - 重启 WorkSpace （在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
   - 在管理命令提示符处，输入 **`gpupdate /force`**。

为 IP 配置 USB 重定 PCo向

> **Note**
>
> 亚马逊 WorkSpaces 目前仅支持 YubiKey U2F 的 USB 重定向。其他类型的 USB 设备可能会被重定向，但它们不受支持，也可能无法正常运行。

为 IP 启用 USB 重定 PCo向

1. 确保已安装最新的 IP WorkSpaces 组策略管理模板（32 位）或最新 PCo的 IP WorkSpaces 组策略管理模板（64 位）。 PCo
2. 在目录管理 WorkSpace 或加入 WorkSpaces 目录的 Amazon EC2 实例上，打开组策略管理工具 (gpmc.msc) 并导航到 PCoIP 会话变量。
3. 打开启用/禁用 PCoIP 会话的 USB 设置。
4. 选择启用，然后选择确定。
5. 打开 “配置 PCo IP USB 允许和不允许的设备规则” 设置。
6. 选择启用，然后在输入 USB 授权表（最多十条规则）下，配置您的 USB 设备允许列表规则。
   - 授权规则 - 110500407。此值是供应商 ID (VID) 和产品 ID (PID) 的组合。 VID/PID 组合的格式为 1xxxxyyyy，其中 xxxx 是十六进制格式的 VID，yyyy 是十六进制格式的 PID。在本例中，1050 是 VID，0407 是 PID。有关更多 YubiKey USB 值，请参阅 YubiKey USB ID 值。
7. 在输入 USB 授权表（最多十条规则）下，配置您的 USB 设备屏蔽列表规则。
   - 对于取消授权规则，设置一个空字符串。这意味着仅允许授权列表中的 USB 设备。

   > **Note**
   > 您最多可以定义 10 条 USB 授权规则和最多 10 条 USB 取消授权规则。使用竖线 (|) 字符分隔多个规则。有关 authorization/unauthorization 规则的详细信息，请参阅适用于 Windows 的 Teradici PCo IP 标准代理。

8. 选择确定。
9. 组策略设置更改将在下一次组策略更新之后 WorkSpace 以及会 WorkSpace 话重新启动后生效。要应用组策略更改，请执行下列操作之一：
   - 重启 WorkSpace （在 Amazon WorkSpaces 控制台中，选择 WorkSpace，然后选择操作，重启 WorkSpaces）。
   - 在管理命令提示符处，输入 **`gpupdate /force`**。

设置生效后，除非通过 USB 设备规则设置配置了限制， WorkSpaces 否则所有支持的 USB 设备都可以重定向到。

设置 Kerberos 票证的最长使用期限

如果您尚未禁用 Windows 的 “记住我” 功能 WorkSpaces，则您的 WorkSpace 用户可以使用其 WorkSpaces 客户端应用程序中的 “记住我” 或 “让我保持登录状态” 复选框来保存其凭据。此功能允许用户在客户端应用程序保持运行 WorkSpaces时轻松连接到他们的。他们的凭证安全地缓存到 Kerberos 票证中，时间可达其最长使用期限。

如果您 WorkSpace 使用 AD Connector 目录，则可以按照微软 Windows 文档中 WorkSpaces 用户票证的最长使用寿命中的步骤通过组策略修改用户的 Kerberos 票证的最大生命周期。

要启用或禁用 Remember Me 功能，请参阅 为 WorkSpaces 个人版中的用户启用自助式 WorkSpace 管理功能。

配置用于互联网访问的设备代理服务器设置

默认情况下， WorkSpaces 客户端应用程序使用在设备操作系统设置中为 HTTPS（端口 443）流量指定的代理服务器。Amazon WorkSpaces 客户端应用程序使用 HTTPS 端口进行更新、注册和身份验证。

> **Note**
>
> 不支持需要使用登录凭证进行身份验证的代理服务器。

您可以按照 Microsoft 文档中配置设备代理和互联网连接设置中的步骤， WorkSpaces 通过组策略为 Windows 配置设备代理服务器设置。

有关在 WorkSpaces Windows 客户端应用程序中配置代理设置的更多信息，请参阅 Amazon WorkSpaces 用户指南中的代理服务器。

有关在 WorkSpaces macOS 客户端应用程序中配置代理设置的更多信息，请参阅 A mazon WorkSpaces 用户指南中的代理服务器。

有关在 WorkSpaces Web Access 客户端应用程序中配置代理设置的更多信息，请参阅 Amazon WorkSpaces 用户指南中的代理服务器。

代理桌面流量

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

对于 DCV WorkSpaces， WorkSpaces Windows 客户端应用程序（版本 5.1 及更高版本）和 macOS 客户端应用程序（版本 5.4 及更高版本）支持使用 HTTP 代理服务器处理端口 4195 TCP 流量。不支持 TLS 解密和检查。

DCV 不支持使用代理来处理通过 UDP 进行的桌面流量。只有 WorkSpaces Windows 和 macOS 桌面客户端应用程序和网络访问支持使用代理来处理 TCP 流量。

> **Note**
>
> 如果您选择使用代理服务器，则客户端应用程序对 WorkSpaces 服务进行的 API 调用也会被代理。API 调用和桌面流量都应通过同一个代理服务器。

关于使用代理服务器的建议

我们不建议使用代理服务器来处理您的 WorkSpaces 桌面流量。

Amazon WorkSpaces 桌面流量已经过加密，因此代理并不能提高安全性。代理代表网络路径中的额外跳跃，它可能会通过引入延迟来影响流式传输质量。如果代理的大小不合适，无法处理桌面流式传输流量，则代理也可能会降低吞吐量。此外，大多数代理不是为支持长时间运行 WebSocket (TCP) 连接而设计的，可能会影响直播质量和稳定性。

如果您必须使用代理，请将代理服务器尽可能靠近 WorkSpace客户端，最好位于同一网络中，以避免增加网络延迟，因为这可能会对直播质量和响应能力产生负面影响。

启用 Amazon WorkSpaces for Zoom 会议媒体插件支持

使用 Zoom VDI 插件，Zoom 支持针对基于 DCV 和 PCo IP Windows WorkSpaces 的优化实时通信。直接的客户端通信允许视频通话绕过基于云的虚拟桌面，并在用户内部进行会议时提供类似本地的 Zoom 体验。 WorkSpace

为 DCV 启用 Zoom Meeting Media Plugin

在安装 Zoom VDI 组件之前，请更新您的 WorkSpaces 配置以支持 Zoom 优化。

先决条件

在使用该插件之前，请确保您满足以下要求。

- 带有 Zoom V DI 插件的 Windows WorkSpaces 客户端版本 5.10.0+ 版本 5.17.10+

- 在你的 WorkSpaces — Zoom VDI Meeting 客户端版本 5. 17.10+

开始前的准备工作

1. 启用扩展组策略设置。有关更多信息，请参阅 为 DCV 配置扩展。
2. 禁用自动重新连接组策略设置。有关更多信息，请参阅 为 DCV 设置会话恢复超时。

安装 Zoom 组件

要启用缩放优化，请在您的 Windows 上安装 Zoom 提供的两个组件 WorkSpaces。有关更多信息，请参阅 Using Zoom for Amazon Web Services。

1. 在您的中安装 Zoom VDI Meeting 客户端 5.12.6+ 版。 WorkSpace
2. 在安装你的客户端上安装 Zoom VDI 插件（Windows Universal Installer）5.12.6+ 版 WorkSpace
3. 通过确认您的 VDI 插件状态在 Zoom VDI 客户端中显示为已连接，验证插件是否在优化 Zoom 流量。有关更多信息，请参阅如何确认 Amazon WorkSpaces 优化。

启用适用于 PCo IP 的 Zoom 会议媒体插件

拥有 Active Directory 管理员权限的用户可以使用其组策略对象（GPO）生成注册表项。这允许用户使用强制更新将注册表项发送到您域 WorkSpaces 中的所有 Windows。或者，具有管理权限的用户也可以在其 WorkSpaces 主机上单独安装注册表项。

先决条件

在使用该插件之前，请确保您满足以下要求。

- Windows WorkSpaces 客户端版本 5.4.0+，带有 Zoom VDI 插件版本 5.12.6+。
- 在你的 WorkSpaces — Zoom VDI Meeting 客户端版本 5.12.6+ 中。

在 Windows WorkSpaces 主机上创建注册表项

完成以下步骤在 Windows WorkSpaces 主机上创建注册表项。在 Windows 上使用 Zoom 需要注册表项 WorkSpaces。

1. 以管理员身份打开 Windows 注册表编辑器。
2. 转到 `\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Amazon`。

3. 如果扩展密钥不存在，请右键单击并选择新建 > 密钥，然后将其命名为 Extension。
4. 在新的扩展密钥中，右键单击并选择新建 > DWORD，然后将其命名为 enable。名称必须为小写。
5. 选择新的 DWORD，并将值更改为 1。
6. 重启计算机以完成该过程。
7. 在您的 WorkSpaces 主机上，下载并安装最新的 Zoom VDI 客户端。在您的 WorkSpaces 客户端（5.4 或更高版本）上，下载并安装适用于亚马逊 WorkSpaces的最新 Zoom VDI 客户端插件。有关更多信息，请参阅 Zoom 支持网站 上的 VDI 版本和下载内容。

启动 Zoom 开始视频通话。

问题排查

完成以下操作对 Windows 上的 Zoom 进行故障排除 WorkSpaces。

- 确认注册表项激活并已正确应用。
- 转到 `C:\ProgramData\Amazon\Amazon WorkSpaces Extension`。您应查看 `wse_core_dll`。
- 确保主机和客户端上的版本正确且相同。

如果您仍然遇到困难，请 Amazon Web Services 支持 使用Amazon Web Services 支持 中心联系。

您可以使用以下示例将 GPO 应用为目录管理员。

- WSE.adml

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitionResources xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" revision="1.0"
 schemaVersion="1.0" xmlns="http://www.microsoft.com/GroupPolicy/PolicyDefinitions">
    <!-- 'displayName' and 'description' don't appear anywhere. All Windows native
 GPO template files have them set like this. -->
    <displayName>enter display name here</displayName>
    <description>enter description here</description>

    <resources>
    <stringTable>
        <string id="SUPPORTED_ProductOnly">N/A</string>
        <string id="Amazon">Amazon</string>
```

```
        <string id="Amazon_Help">Amazon Group Policies</string>
        <string id="WorkspacesExtension">Workspaces Extension</string>
        <string id="WorkspacesExtension_Help">Workspace Extension Group Policies</
string>

        <!-- Extension Itself -->
        <string id="ToggleExtension">Enable/disable Extension Virtual Channel</
string>
        <string id="ToggleExtension_Help">
Allows two-way Virtual Channel data communication for multiple purposes

By default, Extension is disabled.</string>

    </stringTable>
    </resources>
</policyDefinitionResources>
```

- WSE.admx

```
<?xml version="1.0" encoding="utf-8"?>
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance" revision="1.0" schemaVersion="1.0" xmlns="http://
www.microsoft.com/GroupPolicy/PolicyDefinitions">
    <policyNamespaces>
        <target prefix="WorkspacesExtension"
 namespace="Microsoft.Policies.Amazon.WorkspacesExtension" />
    </policyNamespaces>
    <supersededAdm fileName="wse.adm" />
    <resources minRequiredRevision="1.0" />
    <supportedOn>
        <definitions>
            <definition name="SUPPORTED_ProductOnly"
 displayName="$(string.SUPPORTED_ProductOnly)"/>
        </definitions>
    </supportedOn>
    <categories>
        <category name="Amazon" displayName="$(string.Amazon)"
 explainText="$(string.Amazon_Help)" />
        <category name="WorkspacesExtension"
 displayName="$(string.WorkspacesExtension)"
 explainText="$(string.WorkspacesExtension_Help)">
            <parentCategory ref="Amazon" />
        </category>
    </categories>
```

```
    <policies>
        <policy name="ToggleExtension" class="Machine"
 displayName="$(string.ToggleExtension)" explainText="$(string.ToggleExtension_Help)"
 key="Software\Policies\Amazon\Extension" valueName="enable">
            <parentCategory ref="WorkspacesExtension" />
            <supportedOn ref="SUPPORTED_ProductOnly" />
            <enabledValue>
                <decimal value="1" />
            </enabledValue>
            <disabledValue>
                <decimal value="0" />
            </disabledValue>
        </policy>
    </policies>
</policyDefinitions>
```

WorkSpaces 在 WorkSpaces 个人版中管理你的 Amazon Linux 2

对于需要 RPM Package Manager (RPM) 的工作负载，我们建议使用 Red Hat Enterprise Linux 或 Rocky Linux。Amazon Linux 2 可能无法提供您可能需要的某些应用程序和库的最新版本，例如 Firefox 和 glibc。

由于 Linux 实例不遵循组策略，因此建议您使用配置管理解决方案进行分发和实施策略。例如，您可以使用 Ansible。

> **Note**
>
> 本地打印机重定向不适用于亚马逊 Linux WorkSpaces。

控制 Amazon Linux 上的 DCV 行为 WorkSpaces

DCV 的行为受 `wsp.conf` 文件中的配置设置控制，该文件位于 `/etc/wsp/` 目录中。要部署和实施对策略的更改，请使用支持 Amazon Linux 的配置管理解决方案。任何更改将在代理启动后生效。

> **Note**
>
> - 如果您对`wsp.conf`文件进行了不正确或不支持的更改，则策略更改可能不会应用于您WorkSpace上新建立的连接。

- DCV 捆绑包 WorkSpaces 上的 Amazon Linux 目前存在以下限制：
  - 目前仅在 AmazonGovCloud （美国西部）和 AmazonGovCloud （美国东部）提供。
  - 不支持视频输入。
  - 不支持屏幕锁定时断开会话连接。

下面各部分介绍了如何启用或禁用某些功能。

为 DCV 配置剪贴板重定向 Amazon Linux WorkSpaces

默认情况下， WorkSpaces 支持剪贴板重定向。如果需要，可以使用 DCV 配置文件配置此功能。当您断开连接并重新连接时，此设置就会生效。 WorkSpace

要为 DCV 配置剪贴板重定向 Amazon Linux WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `wsp.conf` 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2.

```
clipboard = X
```

其中可能的值*X*为：

`enabled` - 启用双向剪贴板重定向（默认）

`disabled` - 禁用双向剪贴板重定向

`paste-only` - 剪贴板重定向已启用，但仅允许您从本地客户端设备复制内容并将其粘贴到远程主机桌面

`copy-only` - 剪贴板重定向已启用，但仅允许您从远程主机桌面复制内容并将其粘贴到本地客户端设备

为 DCV 启用或禁用音频输入重定向 Amazon Linux WorkSpaces

默认情况下， WorkSpaces 支持音频输入重定向。如果需要，可以使用 DCV 配置文件禁用此功能。当您断开连接并重新连接到时，此设置就会生效。 WorkSpace

启用或禁用 DCV 的音频输入重定向 Amazon Linux WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `wsp.conf` 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 将以下行添加到文件的末尾。

```
audio-in = X
```

其中可能的值*X*为：

`enabled` - 启用音频输入重定向（默认）

`disabled` - 禁用音频输入重定向

为 DCV 启用或禁用时区重定向 Amazon Linux WorkSpaces

默认情况下，工作区内的时间设置为镜像用于连接的客户端的时区 WorkSpace。此行为是通过时区重定向控制的。您可能需要关闭时区重定向的原因有多种，例如以下原因：

- 您的公司希望所有员工在特定时区中工作（即使某些员工在其他时区）。
- 您在 a 中有计划任务 WorkSpace ，这些任务本应在特定时区的特定时间运行。
- 经常出差的用户希望将自己留 WorkSpaces 在一个时区，以保持一致性和个人喜好。

如果需要，可以使用 DCV 配置文件配置此功能。此设置在断开连接并重新连接到后生效。WorkSpace

要为 DCV 启用或禁用 Amazon Linux 的时区重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `wsp.conf` 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp-agent/wsp.conf
```

2. 将以下行添加到文件的末尾。

```
timezone_redirect= X
```

其中可能的值*X*为：

启用 - 启用时区重定向（默认）

禁用 - 禁用时区重定向

控制 PCo IP 代理在 Amazon Linux 上的行为 WorkSpaces

PCoIP 代理的行为由文件中的配置设置控制，该`pcoip-agent.conf`文件位于`/etc/pcoip-agent/`目录中。要部署和实施对策略的更改，请使用支持 Amazon Linux 的配置管理解决方案。任何更改将在代理启动后生效。重新启动代理会结束所有打开的连接并重新启动窗口管理器。要应用任何更改，我们建议重新启动。 WorkSpace

> **Note**
>
> 如果您对`pcoip-agent.conf`文件进行了不正确或不支持的更改，则可能会导致无法运行。WorkSpace 如果您 WorkSpace 停止工作，则可能需要 WorkSpace 使用 SSH 连接到您的以回滚更改，或者您可能需要重新构建 WorkSpace。

下面各部分介绍了如何启用或禁用某些功能。要查看可用设置的完整列表，请在任何 Amazon Linux 上`man pcoip-agent.conf`从终端运行 WorkSpace。

为 PCo IP 配置剪贴板重定向 Amazon Linux WorkSpaces

默认情况下， WorkSpaces 支持剪贴板重定向。如果需要，可以使用 PCo IP 代理会议禁用此功能。此设置将在您重新启动时生效 WorkSpace。

要为 PCo IP 配置剪贴板重定向 Amazon Linux WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `pcoip-agent.conf` 文件。

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
   ```

2. 将以下行添加到文件的末尾。

   ```
   pcoip.server_clipboard_state = X
   ```

   其中可能的值*X*为：

   0 - 禁用双向剪贴板重定向

1 - 启用双向剪贴板重定向

2 - 启用剪贴板重定向，但仅限从客户端剪贴到代理（允许复制，但仅限从本地客户端设备粘贴到远程主机桌面）

3 - 启用剪贴板重定向，但仅限从代理剪贴到客户端（允许复制，但仅限从远程主机桌面粘贴到本地客户端设备）

> **Note**
>
> 剪贴板重定向是作为虚拟通道实施的。如果禁用了虚拟通道，则剪贴板重定向将不起作用。要启用虚拟频道，请参阅 Teradici 文档中的 PCoIP 虚拟频道。

为 IP 启用或禁用音频输入重定向 PCo Amazon Linux WorkSpaces

默认情况下， WorkSpaces 支持音频输入重定向。如果需要，可以使用 PCo IP 代理会议禁用此功能。此设置将在您重新启动时生效 WorkSpace。

要启用或禁用 IP 的音频输入重定向 PCo Amazon Linux WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `pcoip-agent.conf` 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
```

2. 将以下行添加到文件的末尾。

```
pcoip.enable_audio = X
```

其中可能的值*X*为：

0 - 禁用音频输入重定向

1 - 启用音频输入重定向

为 PCo IP 启用或禁用 Amazon Linux 的时区重定向 WorkSpaces

默认情况下，工作区内的时间设置为镜像用于连接的客户端的时区 WorkSpace。此行为是通过时区重定向控制的。您可能需要关闭时区重定向的原因有多种，例如以下原因：

- 您的公司希望所有员工在特定时区中工作（即使某些员工在其他时区）。
- 您在 a 中有计划任务 WorkSpace ，这些任务本应在特定时区的特定时间运行。
- 经常出差的用户希望将自己留 WorkSpaces 在一个时区，以保持一致性和个人喜好。

如果 Linux 需要 WorkSpaces，可以使用 PCo IP 代理会议来禁用此功能。此设置将在您重新启动时生效 WorkSpace。

要为 PCo IP 启用或禁用 Amazon Linux 的时区重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `pcoip-agent.conf` 文件。

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/pcoip-agent/pcoip-agent.conf
   ```

2. 将以下行添加到文件的末尾。

   ```
   pcoip.enable_timezone_redirect= X
   ```

   其中可能的值*X*为：

   0 - 禁用时区重定向

   1 - 启用时区重定向

向 Amazon Linux WorkSpaces 管理员授予 SSH 访问权限

默认情况下，只有域管理员组中分配的用户和账户才能使用 SSH 连接到 Amazon Linux WorkSpaces 。

我们建议您在 Active Directory 中为 Amazon Linux WorkSpaces 管理员创建一个专门的管理员组。

为 Linux_WorkSpaces_Admins Active Directory 组的成员启用 sudo 访问权限

1. 使用 `visudo` 编辑 `sudoers` 文件，如下例所示。

```
[example\username@workspace-id ~]$ sudo visudo
```

2. 添加以下行。

```
%example.com\\Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

在您创建专用管理员组之后，请按照以下步骤为组的成员启用登录。

启用 Linux_ WorkSpaces _Admins Active Directory 组成员的登录

1. 使用提升的权限编辑 `/etc/security/access.conf`。

```
[example\username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. 添加以下行。

```
+:(example\Linux_WorkSpaces_Admins):ALL
```

有关启用 SSH 连接的更多信息，请参阅 WorkSpaces 在 WorkSpaces 个人版中为你的 Linux 启用 SSH 连接。

替换亚马逊 Linux 的默认外壳 WorkSpaces

要覆盖 Linux 的默认外壳 WorkSpaces，我们建议您编辑用户的`~/.bashrc`文件。例如，要使用 `Z shell` 而不是 `Bash` shell，请将以下行添加到 `/home/`*`username`*`/.bashrc`。

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
>
> 进行此更改后，必须重新启动 WorkSpace 或注销 WorkSpace（而不仅仅是断开连接），然后重新登录才能使更改生效。

保护自定义存储库免遭未授权访问

要控制对自定义存储库的访问，建议使用 Amazon Virtual Private Cloud (Amazon VPC) 中内置的安全功能，而不使用密码。例如，使用网络访问控制列表 (ACLs) 和安全组。有关这些功能的更多信息，请参阅《Amazon VPC 用户指南》中的安全性。

如果必须使用密码来保护存储库，请确保创建您的 yum 存储库定义文件，如 Fedora 文档中的存储库定义文件所示。

使用 Amazon Linux Extras 库存储库

利用 Amazon Linux，您可以使用 Extras 库，在您的实例上安装应用程序和软件更新。有关使用额外库的信息，请参阅《亚马逊 Linux 实例 EC2 用户指南》中的附加库 (Amazon Linux)。

> **Note**
>
> 如果您使用的是亚马逊 Linux 存储库，则您的亚马逊 Linux WorkSpaces 必须能够访问互联网，或者您必须为该存储库和主 Amazon Linux 存储库配置虚拟私有云 (VPC) 终端节点。有关更多信息，请参阅 为 WorkSpaces 个人版提供互联网访问权限。

在 Linux 上使用智能卡进行身份验证 WorkSpaces

Linux WorkSpaces on DCV 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 在 “个人” 中 WorkSpaces 使用智能卡进行身份验证。

配置用于互联网访问的设备代理服务器设置

默认情况下， WorkSpaces 客户端应用程序使用在设备操作系统设置中为 HTTPS（端口 443）流量指定的代理服务器。Amazon WorkSpaces 客户端应用程序使用 HTTPS 端口进行更新、注册和身份验证。

> **Note**
>
> 不支持需要使用登录凭证进行身份验证的代理服务器。

您可以按照 Microsoft 文档中配置设备代理和互联网连接设置中的步骤， WorkSpaces 通过组策略为 Linux 配置设备代理服务器设置。

有关在 WorkSpaces Windows 客户端应用程序中配置代理设置的更多信息，请参阅 Amazon WorkSpaces 用户指南中的代理服务器。

有关在 WorkSpaces macOS 客户端应用程序中配置代理设置的更多信息，请参阅 A mazon WorkSpaces 用户指南中的代理服务器。

有关在 WorkSpaces Web Access 客户端应用程序中配置代理设置的更多信息，请参阅 Amazon WorkSpaces 用户指南中的代理服务器。

代理桌面流量

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

对于 DCV WorkSpaces， WorkSpaces Windows 客户端应用程序（版本 5.1 及更高版本）和 macOS 客户端应用程序（版本 5.4 及更高版本）支持使用 HTTP 代理服务器处理端口 4195 TCP 流量。不支持 TLS 解密和检查。

DCV 不支持使用代理来处理通过 UDP 进行的桌面流量。只有 WorkSpaces Windows 和 macOS 桌面客户端应用程序和网络访问支持使用代理来处理 TCP 流量。

> **Note**
>
> 如果您选择使用代理服务器，则客户端应用程序对 WorkSpaces 服务进行的 API 调用也会被代理。API 调用和桌面流量都应通过同一个代理服务器。

关于使用代理服务器的建议

我们不建议使用代理服务器来处理您的 WorkSpaces 桌面流量。

Amazon WorkSpaces 桌面流量已经过加密，因此代理并不能提高安全性。代理代表网络路径中的额外跳跃，它可能会通过引入延迟来影响流式传输质量。如果代理的大小不合适，无法处理桌面流式传输流量，则代理也可能会降低吞吐量。此外，大多数代理不是为支持长时间运行 WebSocket (TCP) 连接而设计的，可能会影响直播质量和稳定性。

如果您必须使用代理，请将代理服务器尽可能靠近 WorkSpace 客户端，最好位于同一网络中，以避免增加网络延迟，因为这可能会对直播质量和响应能力产生负面影响。

以个人模式管理你的 Ubuntu WorkSpaces WorkSpaces

你的 Ubuntu WorkSpaces 捆绑包包括订阅 Canonical 的 Ubuntu Pro。与 Windows 和 Amazon Linux 一样 WorkSpaces，Ubuntu WorkSpaces 已加入域名，因此你可以使用 Active Directory 用户和群组来：

- 管理你的 Ubuntu WorkSpaces
- 为用户提供对这些内容 WorkSpaces 的访问权限

您可以使用组策略管理 Ubun WorkSpaces tu。 ADsys有关更多信息，请参阅 Ubuntu Active Directory 集成常见问题。您还可以使用其他配置和管理解决方案，例如 Landscape 和 Ansible。

控制 Ubuntu 上的 DCV 行为 WorkSpaces

DCV 的行为受 `wsp.conf` 文件中的配置设置控制，该文件位于 `/etc/wsp/` 目录中。要部署和实施对策略的更改，请使用支持 Ubuntu 的配置管理解决方案。任何更改将在代理启动后生效。

> **Note**
>
> 如果您对`wsp.conf`策略做出了不正确或不支持的更改，则可能不会应用于与您的 WorkSpace 新建立的连接。

下面各部分介绍了如何启用或禁用某些功能。

为 Ubuntu 启用或禁用剪贴板重定向 WorkSpaces

默认情况下， WorkSpaces 支持剪贴板重定向。如果需要，可以使用 DCV 配置文件禁用此功能。

启用或禁用 Ubuntu 的剪贴板重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `wsp.conf` 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 将以下行添加到 `[policies]` 组的末尾。

```
clipboard = X
```

其中可能的值*X*为：

启用 - 启用双向剪贴板重定向（默认）

禁用 - 禁用双向剪贴板重定向

仅粘贴 - 剪贴板重定向已启用，但仅允许您从本地客户端设备复制内容并将其粘贴到远程主机桌面

仅复制 - 剪贴板重定向已启用，但仅允许您从远程主机桌面复制内容并将其粘贴到本地客户端设备

启用或禁用 Ubuntu 的音频输入重定向 WorkSpaces

默认情况下， WorkSpaces 支持音频输入重定向。如果需要，可以使用 DCV 配置文件禁用此功能。

启用或禁用 Ubuntu 的音频输入重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `wsp.conf` 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 将以下行添加到 `[policies]` 组的末尾。

```
audio-in = X
```

其中可能的值*X*为：

启用 - 启用音频输入重定向（默认）

禁用 - 禁用音频输入重定向

为 Ubuntu 启用或禁用视频输入重定向 WorkSpaces

默认情况下， WorkSpaces 支持视频输入重定向。如果需要，可以使用 DCV 配置文件禁用此功能。

启用或禁用 Ubuntu 的视频输入重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `wsp.conf` 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 将以下行添加到 [policies] 组的末尾。

```
video-in = X
```

其中可能的值*X*为：

启用 - 启用视频输入重定向（默认）

禁用 - 禁用视频输入重定向

启用或禁用 Ubuntu 的时区重定向 WorkSpaces

默认情况下，工作区内的时间设置为镜像用于连接的客户端的时区 WorkSpace。此行为是通过时区重定向控制的。您可能需要关闭时区重定向的原因有多种，例如以下原因：

- 您的公司希望所有员工在特定时区中工作（即使某些员工在其他时区）。
- 您在 a 中有计划任务 WorkSpace ，这些任务本应在特定时区的特定时间运行。
- 您的用户经常旅行，并希望将他们留 WorkSpaces 在同一个时区，以保持一致性和个人偏好。

如果需要，可以使用 DCV 配置文件配置此功能。

启用或禁用 Ubuntu 的时区重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 wsp.conf 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 将以下行添加到 [policies] 组的末尾。

```
timezone-redirection = X
```

其中可能的值*X*为：

启用 - 启用时区重定向（默认）

禁用 - 禁用时区重定向

启用或禁用 Ubuntu 的打印机重定向 WorkSpaces

默认情况下， WorkSpaces 支持打印机重定向。如果需要，可以使用 DCV 配置文件禁用此功能。

启用或禁用 Ubuntu 的打印机重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `wsp.conf` 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 将以下行添加到 `[policies]` 组的末尾。

```
remote-printing = X
```

其中可能的值*X*为：

启用 - 启用打印机重定向（默认）

禁用 - 禁用打印机重定向

启用或禁用 DCV 屏幕锁定时断开会话连接

启用屏幕锁定时断开会话，允许您的用户在检测到锁屏时结束 WorkSpaces 会话。要从 WorkSpaces 客户端重新连接，用户可以使用自己的密码或智能卡进行身份验证，具体取决于为其 WorkSpaces启用了哪种类型的身份验证。

默认情况下， WorkSpaces 不支持屏幕锁定时断开会话连接。如果需要，可以使用 DCV 配置文件启用此功能。

启用或禁用 Ubuntu 的屏幕锁定时断开连接会话 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `wsp.conf` 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 将以下行添加到 `[policies]` 组的末尾。

```
disconnect-on-lock = X
```

其中可能的值*X*为：

启用 - 启用屏幕锁定时断开连接

禁用 - 禁用屏幕锁定时断开连接（默认）

向 Ubuntu WorkSpaces 管理员授予 SSH 访问权限

默认情况下，只有域管理员组中分配的用户和帐户才能使用 SSH 连接到 Ubuntu WorkSpaces 。要允许其他用户和账户 WorkSpaces 使用 SSH 连接到 Ubuntu，我们建议你在 Active Directory 中为 Ubuntu 管理员创建一个专门的 WorkSpaces 管理员组。

为 **`Linux_WorkSpaces_Admins`** Active Directory 组的成员启用 sudo 访问权限

1. 使用 `visudo` 编辑 `sudoers` 文件，如下例所示。

```
[username@workspace-id ~]$ sudo visudo
```

2. 添加以下行。

```
%Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

在您创建专用管理员组之后，请按照以下步骤为组的成员启用登录。

为 **`Linux_WorkSpaces_Admins`** Active Directory 组的成员启用登录

1. 使用提升的权限编辑 `/etc/security/access.conf`。

```
[username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. 添加以下行。

```
+:(Linux_WorkSpaces_Admins):ALL
```

使用 Ubunt WorkSpaces u，在为 SSH 连接指定用户名时无需添加域名，而且默认情况下，密码身份验证处于禁用状态。要通过 SSH 进行连接，你需要在 Ubuntu `$HOME/.ssh/authorized_keys` 上将 SSH 公钥添加`/etc/ssh/sshd_config`到 WorkSpace，或者编辑设置为 PasswordAuthentication 。`yes`有关启用 SSH 连接的更多信息，请参阅为您的 Linux 启用 SSH 连接 WorkSpaces。

覆盖 Ubuntu 的默认外壳 WorkSpaces

要覆盖 Ubuntu 的默认外壳 WorkSpaces，我们建议您编辑用户的`~/.bashrc`文件。例如，要使用 `Z shell` 而不是 `Bash` shell，请将以下行添加到 `/home/username/.bashrc`。

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
> 进行此更改后，必须重新启动 WorkSpace 或注销 WorkSpace （而不仅仅是断开连接），然后重新登录才能使更改生效。

在 Ubuntu 上使用智能卡进行身份验证 WorkSpaces

Ubuntu WorkSpaces 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 在 “个人” 中 WorkSpaces 使用智能卡进行身份验证。

配置用于互联网访问的设备代理服务器设置

默认情况下， WorkSpaces 客户端应用程序使用在设备操作系统设置中为 HTTPS（端口 443）流量指定的代理服务器。Amazon WorkSpaces 客户端应用程序使用 HTTPS 端口进行更新、注册和身份验证。

> **Note**
>
> 不支持需要使用登录凭证进行身份验证的代理服务器。

您可以按照 Microsoft 文档中配置设备代理和互联网连接设置中的步骤， WorkSpaces 通过组策略为 Ubuntu 配置设备代理服务器设置。

有关在 WorkSpaces Windows 客户端应用程序中配置代理设置的更多信息，请参阅 Amazon WorkSpaces 用户指南中的代理服务器。

有关在 WorkSpaces macOS 客户端应用程序中配置代理设置的更多信息，请参阅 A mazon WorkSpaces 用户指南中的代理服务器。

有关在 WorkSpaces Web Access 客户端应用程序中配置代理设置的更多信息，请参阅 Amazon WorkSpaces 用户指南中的代理服务器。

代理桌面流量

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

对于 DCV WorkSpaces， WorkSpaces Windows 客户端应用程序（版本 5.1 及更高版本）和 macOS 客户端应用程序（版本 5.4 及更高版本）支持使用 HTTP 代理服务器处理端口 4195 TCP 流量。不支持 TLS 解密和检查。

DCV 不支持使用代理来处理通过 UDP 进行的桌面流量。只有 WorkSpaces Windows 和 macOS 桌面客户端应用程序和网络访问支持使用代理来处理 TCP 流量。

> **Note**
>
> 如果您选择使用代理服务器，则客户端应用程序对 WorkSpaces 服务进行的 API 调用也会被代理。API 调用和桌面流量都应通过同一个代理服务器。

关于使用代理服务器的建议

我们不建议使用代理服务器来处理您的 WorkSpaces 桌面流量。

Amazon WorkSpaces 桌面流量已经过加密，因此代理并不能提高安全性。代理代表网络路径中的额外跳跃，它可能会通过引入延迟来影响流式传输质量。如果代理的大小不合适，无法处理桌面流式传输流

量，则代理也可能会降低吞吐量。此外，大多数代理不是为支持长时间运行 WebSocket (TCP) 连接而设计的，可能会影响直播质量和稳定性。

如果您必须使用代理，请将代理服务器尽可能靠近 WorkSpace 客户端，最好位于同一网络中，以避免增加网络延迟，因为这可能会对直播质量和响应能力产生负面影响。

管理你的洛基 Linux WorkSpaces

你可以使用 Ansible 等配置和管理解决方案来管理 Rocky Linux WorkSpaces 。

> **Note**
>
> 您不得删除、修改或掩盖 Rocky Linux 软件之内或本身包含的任何版权、商标或其他专有或保密声明。

控制 Rocky Linux 上的 DCV 行为 WorkSpaces

DCV 的行为受 `wsp.conf` 文件中的配置设置控制，该文件位于 `/etc/wsp/` 目录中。要部署和实施对策略的更改，请使用支持 Rocky Linux 的配置管理解决方案。任何更改将在代理启动后生效。

> **Note**
>
> 如果您对`wsp.conf`策略做出了不正确或不支持的更改，则可能不会应用于与您的 WorkSpace 新建立的连接。

下面各部分介绍了如何启用或禁用某些功能。

为 Rocky Linux 启用或禁用剪贴板重定向 WorkSpaces

默认情况下， WorkSpaces 支持剪贴板重定向。如果需要，可以使用 DCV 配置文件禁用此功能。

为 Rocky Linux 启用或禁用剪贴板重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `wsp.conf` 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 将以下行添加到 `[policies]` 组的末尾。

```
clipboard = X
```

其中可能的值*X*为：

启用 - 启用双向剪贴板重定向（默认）

禁用 - 禁用双向剪贴板重定向

仅粘贴 - 剪贴板重定向已启用，但仅允许您从本地客户端设备复制内容并将其粘贴到远程主机桌面

仅复制 - 剪贴板重定向已启用，但仅允许您从远程主机桌面复制内容并将其粘贴到本地客户端设备

为 Rocky Linux 启用或禁用音频输入重定向 WorkSpaces

默认情况下， WorkSpaces 支持音频输入重定向。如果需要，可以使用 DCV 配置文件禁用此功能。

为 Rocky Linux 启用或禁用音频输入重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `wsp.conf` 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 将以下行添加到 `[policies]` 组的末尾。

```
audio-in = X
```

其中可能的值*X*为：

启用 - 启用音频输入重定向（默认）

禁用 - 禁用音频输入重定向

为 Rocky Linux 启用或禁用视频输入重定向 WorkSpaces

默认情况下， WorkSpaces 支持视频输入重定向。如果需要，可以使用 DCV 配置文件禁用此功能。

为 Rocky Linux 启用或禁用视频输入重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `wsp.conf` 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 将以下行添加到 `[policies]` 组的末尾。

```
video-in = X
```

其中可能的值*X*为：

启用 - 启用视频输入重定向（默认）

禁用 - 禁用视频输入重定向

为 Rocky Linux 启用或禁用时区重定向 WorkSpaces

默认情况下，工作区内的时间设置为镜像用于连接的客户端的时区 WorkSpace。此行为是通过时区重定向控制的。您可能需要关闭时区重定向的原因有多种，例如以下原因：

- 您的公司希望所有员工在特定时区中工作（即使某些员工在其他时区）。
- 您在 a 中有计划任务 WorkSpace ，这些任务本应在特定时区的特定时间运行。
- 您的用户经常旅行，并希望将他们留 WorkSpaces 在同一个时区，以保持一致性和个人偏好。

如果需要，可以使用 DCV 配置文件配置此功能。

为 Rocky Linux 启用或禁用时区重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `wsp.conf` 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 将以下行添加到 `[policies]` 组的末尾。

```
timezone-redirection = X
```

其中可能的值*X*为：

启用 - 启用时区重定向（默认）

禁用 - 禁用时区重定向

为 Rocky Linux 启用或禁用打印机重定向 WorkSpaces

默认情况下， WorkSpaces 支持打印机重定向。如果需要，可以使用 DCV 配置文件禁用此功能。

为 Rocky Linux 启用或禁用打印机重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `wsp.conf` 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 将以下行添加到 `[policies]` 组的末尾。

```
remote-printing = X
```

其中可能的值*X*为：

启用 - 启用打印机重定向（默认）

禁用 - 禁用打印机重定向

启用或禁用 DCV 屏幕锁定时断开会话连接

启用屏幕锁定时断开会话，允许您的用户在检测到锁屏时结束 WorkSpaces 会话。要从 WorkSpaces 客户端重新连接，用户可以使用自己的密码或智能卡进行身份验证，具体取决于为其 WorkSpaces启用了哪种类型的身份验证。

默认情况下， WorkSpaces 不支持屏幕锁定时断开会话连接。如果需要，可以使用 DCV 配置文件启用此功能。

在 Rocky Linux 上启用或禁用屏幕锁定时断开连接会话 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `wsp.conf` 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 将以下行添加到 `[policies]` 组的末尾。

```
disconnect-on-lock = X
```

其中可能的值*X*为：

启用 - 启用屏幕锁定时断开连接

禁用 - 禁用屏幕锁定时断开连接（默认）

向 Rocky Linux WorkSpaces 管理员授予 SSH 访问

默认情况下，只有域管理员组中分配的用户和帐户才能使用 SSH 连接到 Rock WorkSpaces y Linux。要允许其他用户和账户 WorkSpaces 使用 SSH 连接到 Rocky Linux，我们建议你在 Active Directory 中为 Rocky Linux WorkSpaces 管理员创建一个专门的管理员群组。

为 **`Linux_WorkSpaces_Admins`** Active Directory 组的成员启用 sudo 访问权限

1. 使用 `visudo` 编辑 `sudoers` 文件，如下例所示。

```
[username@workspace-id ~]$ sudo visudo
```

2. 添加以下行。

```
%Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

在您创建专用管理员组之后，请按照以下步骤为组的成员启用登录。

为 **`Linux_WorkSpaces_Admins`** Active Directory 组的成员启用登录

1. 使用提升的权限编辑 `/etc/security/access.conf`。

```
[username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. 添加以下行。

```
+:(Linux_WorkSpaces_Admins):ALL
```

使用 Rocky Linux WorkSpaces ，在为 SSH 连接指定用户名时无需添加域名，并且默认情况下，密码身份验证处于禁用状态。要通过 SSH 进行连接，你需要在 Rocky Linux `$HOME/.ssh/authorized_keys` 上将 SSH 公钥添加`/etc/ssh/sshd_config`到 WorkSpace，或者编辑设置为 PasswordAuthentication `yes`。有关启用 SSH 连接的更多信息，请参阅为您的 Linux 启用 SSH 连接 WorkSpaces。

覆盖 Rocky Linux 的默认外壳 WorkSpaces

要覆盖 Rocky Linux 的默认外壳 WorkSpaces，我们建议您编辑用户的`~/.bashrc`文件。例如，要使用 `Z shell` 而不是 `Bash` shell，请将以下行添加到 `/home/username/.bashrc`。

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
>
> 进行此更改后，必须重新启动 WorkSpace 或注销 WorkSpace （而不仅仅是断开连接），然后重新登录才能使更改生效。

在 Rocky Linux 上使用智能卡进行身份验证 WorkSpaces

Rocky Linux WorkSpaces 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 在 “个人” 中 WorkSpaces 使用智能卡进行身份验证。

管理你的红帽企业 Linux WorkSpaces

与 Windows 和亚马逊 Linux 一样 WorkSpaces，红帽企业 Linux WorkSpaces 是加入域的，因此你可以使用 Active Directory 用户和群组来：

- 管理您的红帽企业 Linux WorkSpaces

- 为用户提供对这些内容 WorkSpaces 的访问权限

您可以使用使用组策略管理红帽企业 WorkSpaces Linux ADsys。有关更多信息，请参阅 Red Hat Enterprise Linux Active Directory 集成常见问题。您还可以使用其他配置和管理解决方案，例如 Landscape 和 Ansible。

控制红帽企业 Linux 上的 DCV 行为 WorkSpaces

DCV 的行为受 `wsp.conf` 文件中的配置设置控制，该文件位于 `/etc/wsp/` 目录中。要部署和实施对策略的更改，请使用支持 Red Hat Enterprise Linux 的配置管理解决方案。任何更改将在代理启动后生效。

> **Note**
>
> 如果您对`wsp.conf`策略做出了不正确或不支持的更改，则可能不会应用于与您的 WorkSpace 新建立的连接。

下面各部分介绍了如何启用或禁用某些功能。

为红帽企业 Linux 启用或禁用剪贴板重定向 WorkSpaces

默认情况下， WorkSpaces 支持剪贴板重定向。如果需要，可以使用 DCV 配置文件禁用此功能。

为红帽企业 Linux 启用或禁用剪贴板重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `wsp.conf` 文件。

   ```
   [domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
   ```

2. 将以下行添加到 `[policies]` 组的末尾。

   ```
   clipboard = X
   ```

   其中可能的值*X*为：

   启用 - 启用双向剪贴板重定向（默认）

   禁用 - 禁用双向剪贴板重定向

仅粘贴 - 剪贴板重定向已启用，但仅允许您从本地客户端设备复制内容并将其粘贴到远程主机桌面

仅复制 - 剪贴板重定向已启用，但仅允许您从远程主机桌面复制内容并将其粘贴到本地客户端设备

为红帽企业 Linux 启用或禁用音频输入重定向 WorkSpaces

默认情况下， WorkSpaces 支持音频输入重定向。如果需要，可以使用 DCV 配置文件禁用此功能。

为红帽企业 Linux 启用或禁用音频输入重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `wsp.conf` 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 将以下行添加到 `[policies]` 组的末尾。

```
audio-in = X
```

其中可能的值*X*为：

启用 - 启用音频输入重定向（默认）

禁用 - 禁用音频输入重定向

为红帽企业 Linux 启用或禁用视频输入重定向 WorkSpaces

默认情况下， WorkSpaces 支持视频输入重定向。如果需要，可以使用 DCV 配置文件禁用此功能。

为红帽企业 Linux 启用或禁用视频输入重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `wsp.conf` 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 将以下行添加到 `[policies]` 组的末尾。

```
video-in = X
```

其中可能的值*X*为：

启用 - 启用视频输入重定向（默认）

禁用 - 禁用视频输入重定向

为红帽企业 Linux 启用或禁用时区重定向 WorkSpaces

默认情况下，工作区内的时间设置为镜像用于连接的客户端的时区 WorkSpace。此行为是通过时区重定向控制的。您可能需要关闭时区重定向的原因有多种，例如以下原因：

- 您的公司希望所有员工在特定时区中工作（即使某些员工在其他时区）。
- 您在 a 中有计划任务 WorkSpace ，这些任务本应在特定时区的特定时间运行。
- 您的用户经常旅行，并希望将他们留 WorkSpaces 在同一个时区，以保持一致性和个人偏好。

如果需要，可以使用 DCV 配置文件配置此功能。

为红帽企业 Linux 启用或禁用时区重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `wsp.conf` 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 将以下行添加到 `[policies]` 组的末尾。

```
timezone-redirection = X
```

其中可能的值*X*为：

启用 - 启用时区重定向（默认）

禁用 - 禁用时区重定向

为红帽企业 Linux 启用或禁用打印机重定向 WorkSpaces

默认情况下， WorkSpaces 支持打印机重定向。如果需要，可以使用 DCV 配置文件禁用此功能。

为红帽企业 Linux 启用或禁用打印机重定向 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `wsp.conf` 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 将以下行添加到 `[policies]` 组的末尾。

```
remote-printing = X
```

其中可能的值*X*为：

启用 - 启用打印机重定向（默认）

禁用 - 禁用打印机重定向

启用或禁用 DCV 屏幕锁定时断开会话连接

启用屏幕锁定时断开会话，允许您的用户在检测到锁屏时结束 WorkSpaces 会话。要从 WorkSpaces 客户端重新连接，用户可以使用自己的密码或智能卡进行身份验证，具体取决于为其 WorkSpaces启用了哪种类型的身份验证。

默认情况下， WorkSpaces 不支持屏幕锁定时断开会话连接。如果需要，可以使用 DCV 配置文件启用此功能。

为红帽企业 Linux 启用或禁用屏幕锁定时断开连接会话 WorkSpaces

1. 通过以下命令，使用提升的权限在编辑器中打开 `wsp.conf` 文件。

```
[domain\username@workspace-id ~]$ sudo vi /etc/wsp/wsp.conf
```

2. 将以下行添加到 `[policies]` 组的末尾。

```
disconnect-on-lock = X
```

其中可能的值*X*为：

启用 - 启用屏幕锁定时断开连接

禁用 - 禁用屏幕锁定时断开连接（默认）

向红帽企业 Linux WorkSpaces 管理员授予 SSH 访问权限

默认情况下，只有域管理员组中分配的用户和账户才能使用 SSH 连接到红帽企业 Linux WorkSpaces 。要让其他用户和账户通过 SSH 连接到红帽企业 Linux，我们建议您在 WorkSpaces Active Directory 中为红帽企业 Linux WorkSpaces 管理员创建一个专门的管理员组。

为 **`Linux_WorkSpaces_Admins`** Active Directory 组的成员启用 sudo 访问权限

1. 使用 `visudo` 编辑 `sudoers` 文件，如下例所示。

```
[username@workspace-id ~]$ sudo visudo
```

2. 添加以下行。

```
%Linux_WorkSpaces_Admins ALL=(ALL) ALL
```

在您创建专用管理员组之后，请按照以下步骤为组的成员启用登录。

为 **`Linux_WorkSpaces_Admins`** Active Directory 组的成员启用登录

1. 使用提升的权限编辑 `/etc/security/access.conf`。

```
[username@workspace-id ~]$ sudo vi /etc/security/access.conf
```

2. 添加以下行。

```
+:(Linux_WorkSpaces_Admins):ALL
```

使用红帽企业 Linux， WorkSpaces 您无需在为 SSH 连接指定用户名时添加域名，而且默认情况下，密码身份验证处于禁用状态。要通过 SSH 进行连接，您需要在红帽企业 Linux `$HOME/.ssh/authorized_keys` 上将 SSH 公钥添加到 WorkSpace，或者编辑`/etc/ssh/sshd_config`

PasswordAuthentication 以设置为yes。有关启用 SSH 连接的更多信息，请参阅为您的 Linux 启用 SSH 连接 WorkSpaces。

覆盖红帽企业 Linux 的默认外壳 WorkSpaces

要覆盖红帽企业 Linux 的默认外壳 WorkSpaces，我们建议您编辑用户的~/.bashrc文件。例如，要使用 Z shell 而不是 Bash shell，请将以下行添加到 /home/username/.bashrc。

```
export SHELL=$(which zsh)
[ -n "$SSH_TTY" ] && exec $SHELL
```

> **Note**
>
> 进行此更改后，必须重新启动 WorkSpace 或注销 WorkSpace（而不仅仅是断开连接），然后重新登录才能使更改生效。

在红帽企业 Linux 上使用智能卡进行身份验证 WorkSpaces

红帽企业 Linux WorkSpaces 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 在 “个人” 中 WorkSpaces 使用智能卡进行身份验证。

优化 WorkSpaces 个人版的 WorkSpaces 以实现实时通信

Amazon WorkSpaces 提供多种技术来促进 Microsoft Teams、Zoom、Webex 等统一通信 (UC) 应用程序的部署。在当代应用程序环境中，大多数 UC 应用程序都包含各种功能，包括一对一聊天室、协作群聊频道、无缝文件存储和交换、直播活动、网络研讨会、广播、交互式屏幕共享和控制、白板以及离线音频/视频消息传递功能。其中大部分功能可作为标准功能在 WorkSpaces 上无缝使用，而无需进行额外的微调或增强。但是，值得注意的是，实时通信元素（尤其是一对一通话和集体小组会议）是该规则的例外。成功整合此类功能通常需要在 WorkSpaces 部署过程中专门投入精力和进行规划。

计划在 Amazon WorkSpaces 上实施 UC 应用程序的实时通信功能时，您有三种不同的实时通信 (RTC) 配置模式可供选择。具体选择取决于您打算向用户提供的一个或多个特定应用程序以及您计划使用的客户端设备。

本文档重点介绍如何优化 Amazon WorkSpaces 中最常见 UC 应用程序的用户体验。有关特定于 WorkSpaces Core 的优化，请参阅合作伙伴特定的文档。

主题

- 媒体优化模式概述
- 使用哪种 RTC 优化模式？
- RTC 优化指南

媒体优化模式概述

以下是可用的媒体优化选项。

选项 1：媒体优化的实时通信（媒体优化 RTC）

在此模式下，第三方 UC 和 VoIP 应用程序在远程 WorkSpace 上执行，而其媒体框架则分载到支持的客户端进行直接通信。以下 UC 应用程序在 Amazon WorkSpaces 上使用这种方法：

- Zoom Meetings
- Cisco Webex Meetings
- Microsoft Teams 2.0（公开预览版）

要使媒体优化的 RTC 模式运行，UC 应用供应商应使用一种可用的软件开发工具包（SDK）（例如 DCV Extension SDK），开发与 WorkSpaces 的集成。此模式要求在客户端设备上安装 UC 组件。

有关配置此模式的更多信息，请参阅配置媒体优化的 RTC。

选项 2：会话中优化的实时通信（会话中优化的 RTC）

在此模式下，未更改的 UC 应用程序在 WorkSpace 上运行，通过 DCV 将音频和视频流量引导到客户端设备。来自麦克风的本地音频和来自网络摄像头的视频流被重定向到 WorkSpace，从而供 UC 应用程序使用。此模式提供了广泛的应用程序兼容性，并有效地将 UC 应用程序从远程 WorkSpace 传输到各种客户端平台。您无需将 UC 应用程序组件部署到客户端设备。

有关配置此模式的更多信息，请参阅配置会话中优化 RTC。

选项 3：直接实时通信（直接 RTC）

在此模式下，在 WorkSpace 中运行的应用程序将控制位于用户桌面或客户端操作系统上的物理或虚拟电话机。这样一来，音频流量会直接从用户工作站的物理电话或在客户端设备上运行的虚拟电话传送到远程呼叫对等端。在此模式下运行的应用程序的重要实例包括：

- Amazon WorkSpaces 的 Amazon Connect 优化

- Genesys Cloud WebRTC Media Helper
- Microsoft Teams SIP Gateway
- Microsoft Teams 台式电话和 Teams 显示屏
- 通过 UC 应用程序的拨入或“拨打我的电话”功能参与音频会议。

有关配置此模式的更多信息，请参阅配置直接 RTC。

使用哪种 RTC 优化模式？

可以同时使用不同的 RTC 优化模式，也可以将其设置为后备模式相互补充。例如，可以考虑为 Cisco Webex 会议启用媒体优化 RTC。此配置可确保用户在通过桌面客户端访问 WorkSpace 时体验优化的通信。但是，在从缺乏 UC 优化组件的共享互联网自助服务亭访问 Webex 的情况下，Webex 将无缝过渡到会话中优化 RTC 模式以保持功能。当用户使用多个 UC 应用程序时，RTC 配置模式可能会根据其独特要求而有所不同。

下表列出了常见的 UC 应用程序功能，并定义了哪种 RTC 配置模式可提供最佳结果。

功能	直接 RTC	媒体优化 RTC	会话中优化的 RTC
一对一聊天	不需要 RTC 配置		
群聊室	不需要 RTC 配置		
群组音频会议	最佳	最佳	好
群组视频会议	好	最佳	好
一对一音频通话	最佳	最佳	好
一对一视频通话	好	最佳	好
白板	不需要 RTC 配置		
音频/视频片段/消息传送	不适用	好	最佳
文件共享	不适用	取决于 UC 应用程序	最佳
屏幕共享和控制	不适用	取决于 UC 应用程序	最佳

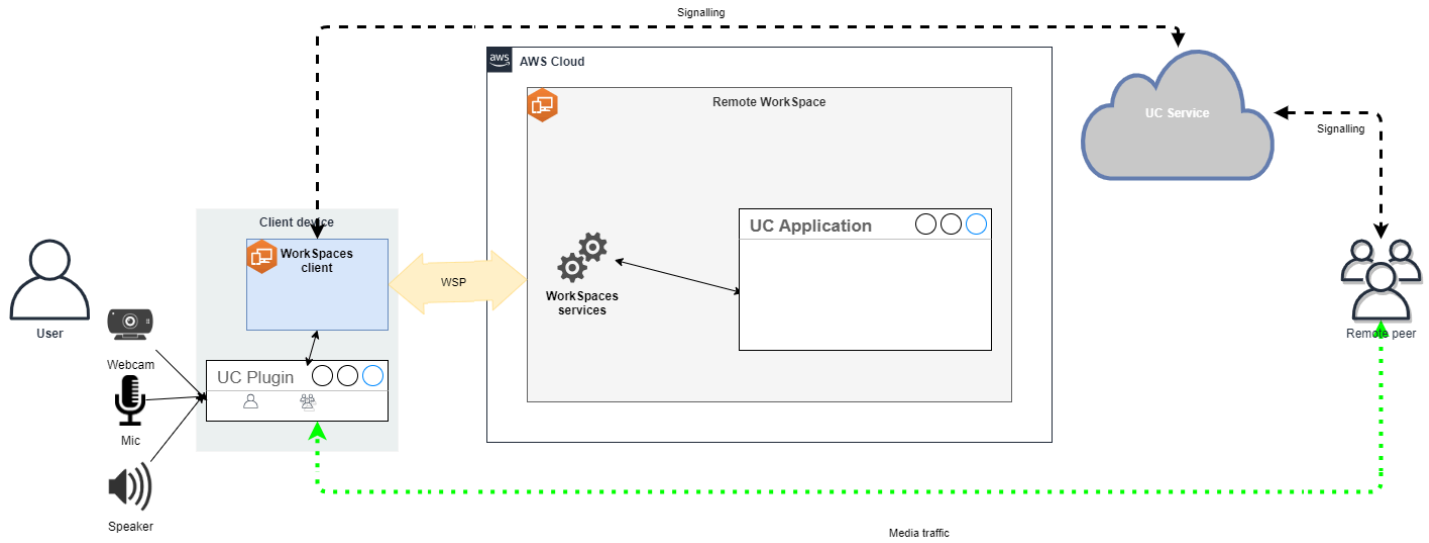
功能	直接 RTC	媒体优化 RTC	会话中优化的 RTC
网络研讨会/广播活动	不适用	好	最佳

RTC 优化指南

配置媒体优化的 RTC

UC 应用程序供应商使用 Amazon 提供的 SDK，使媒体优化的 RTC 模式成为可能。该架构要求 UC 供应商开发特定于 UC 的插件或扩展并将其部署到客户端。

该 SDK 含有 DCV Extension SDK 等公开可用选项和自定义私有版本，可在 WorkSpace 内运行的 UC 应用程序模块和客户端的插件之间建立控制通道。通常，此控制通道会指示客户端扩展发起或加入呼叫。通过客户端扩展建立呼叫后，UC 插件会捕获来自麦克风的音频和来自网络摄像头的视频，然后将其直接传输到 UC 云或呼叫对等端。传入的音频在本地播放，视频叠加在远程客户端 UI 上。控制通道负责传递呼叫的状态。



Amazon WorkSpaces 目前支持以下具有媒体优化 RTC 模式的应用程序：

- Zoom Meetings（适用于 PCoIP 和 DCV WorkSpaces）
- Cisco Webex Meetings（仅适用于 DCV WorkSpaces）
- Microsoft Teams 2.0（公开预览版）（仅适用于 DCV WorkSpaces）

如果您使用的应用程序不在该列表中，建议您联系应用程序供应商并请求支持 WorkSpaces 媒体优化 RTC。要加快此流程，请建议对方通过 aws-av-offloading@amazon.com 联系。

虽然媒体优化 RTC 模式增强了呼叫性能并最大限度地降低了 WorkSpace 资源利用率，但它确实存在某些局限性：

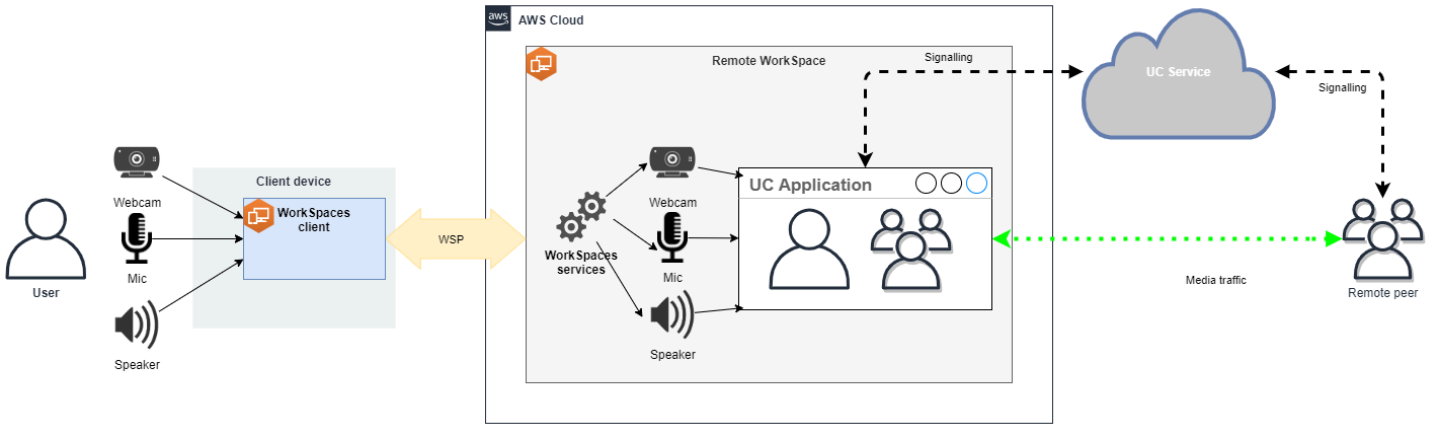
- UC 客户端扩展必须安装在客户端设备上。
- UC 客户端扩展需要独立管理和更新。
- UC 客户端扩展可能在某些客户端平台上不可用，例如移动平台或 Web 客户端。
- 在此模式下，某些 UC 应用程序功能可能会受到限制；例如，屏幕共享行为可能会有所不同。
- 使用客户端扩展可能不适合自带设备 (BYOD) 或共享自助服务亭等场景。

如果媒体优化的 RTC 模式经过证明不适合您的环境，或者某些用户无法安装客户端扩展，则建议将会话中优化 RTC 模式配置为后备选项。

配置会话中优化 RTC

在会话中优化 RTC 模式下，UC 应用程序无需任何修改即可在 WorkSpace 上运行，从而提供类似于本地的体验。应用程序生成的音频和视频流由 DCV 捕获并传输到客户端。在客户端，捕获麦克风（在 DCV 和 PCoIP WorkSpaces 上）和网络摄像头（仅在 DCV WorkSpaces 上）信号，将其重定向回 WorkSpace，然后无缝传递到 UC 应用程序。

值得注意的是，此选项可确保出色的兼容性，即使使用旧版应用程序也是如此，从而提供连贯的用户体验（无论应用程序的来源如何）。会话中优化也适用于 Web 客户端。



DCV 经过精心优化，可增强远程 RTC 模式的性能。优化措施包括：

- 利用基于 UDP 的自适应 QUIC 传输，确保高效的数据传输。
- 建立低延迟音频路径，便于快速音频输入和输出。
- 实施经过语音优化的音频编解码器，以保持音频质量，同时降低 CPU 和网络利用率。

- 网络摄像头重定向，实现网络摄像头功能的集成。
- 配置网络摄像头分辨率以优化性能。
- 集成自适应显示编解码器，以平衡速度和视觉质量。
- 音频抖动校正，保证流畅的音频传输。

这些优化共同有助于在远程 RTC 模式下提供稳定而流畅的体验。

大小调整建议

要有效支持远程 RTC 模式，必须确保适当调整 Amazon WorkSpaces 的大小。远程 WorkSpace 必须满足或超过相应统一通信 (UC) 应用程序的系统要求。下表概述了用于视频和音频通话的常用 UC 应用程序支持和推荐的最低 WorkSpaces 配置：

			视频通话		音频通话		
应用程序	RTC 应用程序的 CPU 要求	RTC 应用程序的内存要求	支持的最低 WorkSpace	推荐的 WorkSpace	支持的最低 WorkSpace	推荐的 WorkSpace	参考
Microsoft Teams	需要 2 个内核，推荐 4 个内核	4.0 GB 内存	节能（4 个 vCPU，16 GB 内存）	• PowerPr 8 个 vCPU，3 GB 内存） • GeneralP rpose.4xl arge（16 个 vCPU，6 GB 内存） • GeneralP rpose.8xl arge（32 个 vCPU，1	性能（2 个 vCPU，8 GB 内存）	• PowerPr 8 个 vCPU，3 GB 内存） • GeneralP rpose.4xl arge（16 个 vCPU，6 GB 内存） • GeneralP rpose.8xl arge（32 个 vCPU，1	Microsoft Teams 的硬件要求

			视频通话		音频通话		
应用程序	RTC 应用程序的 CPU 要求	RTC 应用程序的内存要求	支持的最低 WorkSpace	推荐的 WorkSpace	支持的最低 WorkSpace	推荐的 WorkSpace	参考
				GB 内存）		GB 内存）	
Zoom	需要 2 个内核，推荐 4 个内核	4.0 GB 内存	节能（4 个 vCPU，16 GB 内存）	• PowerPro 8 个 vCPU，3 GB 内存） • GeneralPurpose.4xlarge（16 个 vCPU，6 GB 内存） • GeneralPurpose.8xlarge（32 个 vCPU，1 GB 内存）	性能（2 个 vCPU，8 GB 内存）	• PowerPro 8 个 vCPU，3 GB 内存） • GeneralPurpose.4xlarge（16 个 vCPU，6 GB 内存） • GeneralPurpose.8xlarge（32 个 vCPU，1 GB 内存）	Zoom 系统要求：Windows、macOS、Linux

			视频通话		音频通话		
应用程序	RTC 应用程序的 CPU 要求	RTC 应用程序的内存要求	支持的最低 WorkSpace	推荐的 WorkSpace	支持的最低 WorkSpace	推荐的 WorkSpace	参考
Webex	需要 2 个内核	4.0 GB 内存	节能（4 个 vCPU，16 GB 内存）	• PowerPro 8 个 vCPU，3 GB 内存） • GeneralPurpose.4xlarge（16 个 vCPU，6 GB 内存） • GeneralPurpose.8xlarge（32 个 vCPU，1 GB 内存）	性能（2 个 vCPU，8 GB 内存）	• PowerPro 8 个 vCPU，3 GB 内存） • GeneralPurpose.4xlarge（16 个 vCPU，6 GB 内存） • GeneralPurpose.8xlarge（32 个 vCPU，1 GB 内存）	Webex 服务的系统要求

值得注意的是，视频会议在视频编码和解码时使用了大量资源。在物理计算机场景中，这些任务会分载到 GPU。在非 GPU WorkSpaces 中，这些任务在 CPU 上与远程协议编码并行执行。因此，对于经常进行视频流或视频通话的用户，强烈建议选择 PowerPro 或更高配置。

屏幕共享还会消耗大量资源，分辨率越高，资源消耗就会增加。因此，在非 GPU WorkSpaces 中，屏幕共享通常仅限于较低的帧速率。

通过 DCV 利用基于 UDP 的 QUIC 传输

UDP 传输特别适合传输 RTC 应用程序。为了显著提高效率，请确保将您的网络设置为通过 DCV 使用 QUIC 传输。请注意，基于 UDP 的传输仅适用于本机客户端。

为 WorkSpaces 配置 UC 应用程序

要增强视频处理能力（例如背景模糊、虚拟背景、反应或主持直播活动），选择支持 GPU 的 WorkSpace 对于实现最佳性能至关重要。

大多数 UC 应用程序都提供以下相关指导：禁用高级视频处理以降低非 GPU WorkSpaces 上的 CPU 使用率。

有关更多信息，请参阅以下资源。

- Microsoft Teams：虚拟化桌面基础架构中的 Teams
- Zoom Meetings：管理不兼容的 VDI 插件的用户体验
- Webex：适用于虚拟桌面基础架构 (VDI) 的 Webex 应用程序部署指南 - 管理适用于 VDI 的 Webex 应用程序并排除其问题 [Webex 应用程序]
- Google Meet：使用 VDI

启用双向音频和网络摄像头重定向

默认情况下，Amazon WorkSpaces 本质上支持音频输入、音频输出和摄像头通过视频输入重定向。但是，如果由于任何特定原因禁用了这些功能，则您可以按照提供的指导重新启用重定向。有关更多信息，请参阅《Amazon WorkSpaces 管理指南》中的为 DCV 启用或禁用视频输入重定向。连接后，用户需要选择要在会话中使用的摄像头。有关更多信息，用户应参阅《Amazon WorkSpaces 用户指南》中的网络摄像头和其他视频设备。

限制网络摄像头的最大分辨率

对于使用 Power、PowerPro、GeneralPurpose.4xlarge 或 GeneralPurpose.8xlarge WorkSpaces 进行视频会议的用户，强烈建议限制重定向网络摄像头的最大分辨率。就 PowerPro、GeneralPurpose.4xlarge 或 GeneralPurpose.8xlarge 而言，建议的最大分辨率为宽 640 像素，高 480 像素。就节能而言，建议的最大分辨率为宽 320 像素，高 240 像素。

完成以下步骤，配置网络摄像头的最大分辨率。

1. 打开 Windows 注册表编辑器。

2. 导航到以下注册表路径：

```
HKEY_USERS/S-1-5-18/Software/GSettings/com/nicesoftware/dcv/webcam
```

3. 创建一个名为 `max-resolution` 的字符串值，并将其设置为 `(X,Y)` 格式所需的分辨率，其中 X 表示水平像素数（宽度），Y 表示垂直像素数（高度）。例如，指定 `(640,480)`)，以表示宽度为 640 像素、高度为 480 像素的分辨率。

启用语音优化的音频配置

默认情况下，WorkSpaces 设置为从 WorkSpaces 向客户端传送 7.1 高保真音频，从而确保出色的音乐播放质量。但是，如果您的主要使用案例涉及音频或视频会议，则将音频编解码器配置文件修改为语音优化设置可以节省 CPU 和网络资源。

完成以下步骤，将音频配置文件设置为语音优化。

1. 打开 Windows 注册表编辑器。
2. 导航到以下注册表路径：

```
HKEY_USERS/S-1-5-18/Software/GSettings/com/nicesoftware/dcv/audio
```

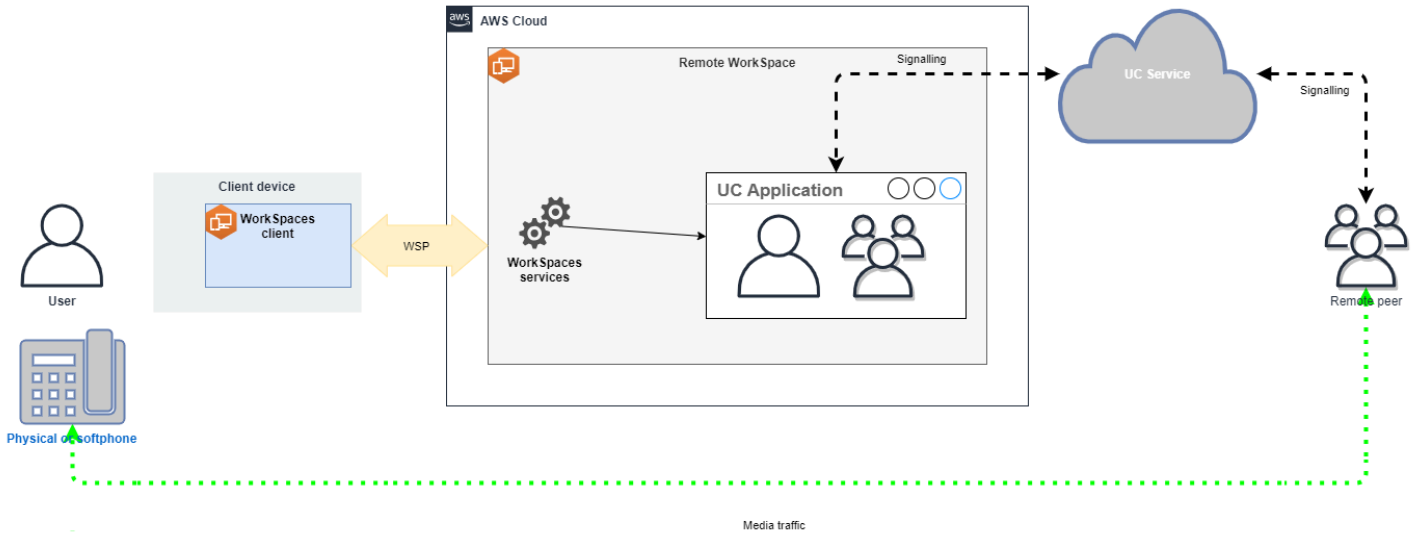
3. 创建名为 `default-profile` 的字符串值，并将其设置为 `voice`。

使用高质量头戴式耳机进行音频和视频通话

为了增强音频体验并防止回声，使用高质量的头戴式耳机至关重要。使用台式机扬声器可能会导致通话的远程端出现回声问题。

配置直接 RTC

直接 RTC 模式的配置取决于特定的统一通信 (UC) 应用程序，不需要对 WorkSpaces 的配置进行任何更改。以下列表简单编译了针对各种 UC 应用程序的优化。



- Microsoft Teams：
  - 规划 SIP Gateway
  - Microsoft 365 中的音频会议
  - 规划 Teams 语音解决方案
- Zoom Meetings：
  - 启用或禁用长途电话拨入号码
  - 使用桌面电话呼叫控制
  - 桌面电话伴侣模式
- Webex：
  - Webex 应用程序 | 使用桌面电话拨打电话
  - Webex 应用程序 | 支持的通话选项
- BlueJeans：
  - 从台式电话拨入会议
- Genesys：
  - Genesys Cloud WebRTC Media Helper
- Amazon Connect：
  - Amazon WorkSpaces 的 Amazon Connect 优化
- Google Meet：
  - 在视频会议中针对音频使用电话

在 WorkSpaces 个人版中管理跑步模式

的运行模式 WorkSpace 决定了它的即时可用性以及支付方式（按月还是按小时）。创建时，可以在以下运行模式之间进行选择 WorkSpace：

- AlwaysOn—在支付固定的月费以无限使用您的 WorkSpaces. 此模式最适合将 WorkSpace全职时间用作主桌面的用户。
- AutoStop— WorkSpaces 按小时支付费用时使用。使用此模式，您 WorkSpaces 将在指定的断开连接时间后停止连接，并保存应用程序和数据的状态。

有关更多信息，请参阅WorkSpaces 定价。

AutoStop WorkSpaces

要设置自动停止时间，请在亚马逊 WorkSpaces 控制台 WorkSpace 中选择，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，这意味着断开连接一小时后会自动 WorkSpace 停止。 WorkSpace

断开连接 WorkSpace 且 AutoStop 时间段到期后，可能需要几分钟 WorkSpace 才能自动停止。但是，一旦 AutoStop 时间段到期，计费就会停止，并且不会向您收取额外时间的费用。

当 WorkSpaces 支持休眠时，桌面的状态将保存到的根卷中。 WorkSpace用户登录时会 WorkSpace 恢复。所有打开的文档和正在运行的程序都恢复到其保存状态，并且所有 WorkSpaces 操作系统都支持休眠。

AutoStop Graphics.g4dn、.g4dn、 GraphicsPro Graphics 和 GeneralPurpose .4xlarge 或 .8xlarge 不 GraphicsPro支持休眠。 GeneralPurposeWindows 11 24H2 AutoStop WorkSpaces 不支持休眠状态，也不会保留休眠状态。 applications/data 我们建议您在 WorkSpaces 每次使用完毕后保存所做的工作，以免丢失数据。

对于 Bring Your Own L AutoStop WorkSpaces icense (BYOL)，大量的并发登录可能会显著延长 WorkSpaces 可用时间。如果您预计会有许多用户同时登录您的 BYOL AutoStop WorkSpaces ，请咨询您的客户经理以获取建议。

> **Important**
>
> AutoStop WorkSpaces 只有在 WorkSpaces 断开连接时才会自动停止。

WorkSpace 只有在以下情况下才会断开连接 A：

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

作为最佳实践， AutoStop WorkSpace 用户应在每天使用完 WorkSpaces 毕后手动断开与他们的连接。要手动断开连接，请 WorkSpaces从 Linux、macOS WorkSpace 或 Windows WorkSpaces 客户端应用程序的亚马逊 WorkSpaces菜单中选择 “断开连接” 或 “退出亚马逊”。对于 Android 或 iPad，从侧边栏菜单中选择断开连接。

AutoStop WorkSpaces 在以下情况下可能不会自动停止：

- 如果客户端设备仅处于锁定状态、处于睡眠状态或处于非活动状态（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 WorkSpaces 应用程序仍在运行，就 WorkSpace 可能无法断开连接，因此 WorkSpace 可能不会自动停止。
- WorkSpaces 只有在用户使用 WorkSpaces 客户端时才能检测到断开连接。如果用户使用的是第三方客户端，则 WorkSpaces 可能无法检测到断开连接，因此 WorkSpaces 可能不会自动停止，也可能无法暂停计费。

修改运行模式

您可以随时切换运行模式。

修改的运行模式 WorkSpace

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在导航窗格中，请选择 WorkSpaces。
3. 选择 WorkSpace 要修改的，然后选择操作、修改运行模式。
4. 选择新的运行模式，AlwaysOn或 AutoStop，然后选择 “保存”。

要修改的运行模式， WorkSpace 请使用 Amazon CLI

使用 modify-workspace-properties 命令。

停止并启动 AutoStop WorkSpace

断开连接后，它们会在指定的断开连接时间后自动停止，按小时计费将暂停。 AutoStop WorkSpaces 要进一步优化成本，您可以手动暂停与之相关的小时费用 AutoStop WorkSpaces。 WorkSpace停靠点以及所有应用程序和数据都将保存，以备用户下次登录时使用 WorkSpace。

当用户重新连接到已停止的服务器时 WorkSpace，它会从中断的地方恢复，通常不到 90 秒。

您可以重新启动（重新启动） AutoStop WorkSpaces 可用或处于错误状态。

要停止 AutoStop WorkSpace

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在导航窗格中，请选择 WorkSpaces。
3. 选择 WorkSpace 要停止，然后选择操作、停止 WorkSpaces。
4. 当系统提示您确认时，选择 Stop WorkSpace。

要开始 AutoStop WorkSpace

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在导航窗格中，请选择 WorkSpaces。
3. 选择 “开始” WorkSpaces ，然后选择 “操作”、“开始” WorkSpaces。
4. 当系统提示您确认时，选择 Start WorkSpace。

要移除与之相关的固定基础设施成本 AutoStop WorkSpaces，请将其 WorkSpace 从您的账户中删除。有关更多信息，请参阅 删除 WorkSpaces 个人版中的 WorkSpace。

要停止并启动， AutoStop WorkSpace 请使用 Amazon CLI

使用停止WorkSpaces和启动WorkSpaces命令。

在 “ WorkSpaces 个人” 模式下管理应用程序

启动后 WorkSpace，你可以在 WorkSpaces 控制台 WorkSpace 上看到与你关联的所有应用程序包的列表。

要查看与您关联的所有应用程序包的列表 WorkSpace

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。

2. 从左侧导航窗格中选择WorkSpaces。
3. 选择， WorkSpace 然后选择 “查看详细信息”。
4. 在 “应用程序” 下，找到与此 WorkSpace相关的应用程序列表及其安装状态。

您可以通过以下方式更新您的 WorkSpace 应用程序包：

- 在您的设备上安装应用程序包 WorkSpace
- 从您的应用程序包中卸载应用程序包 WorkSpace
- 安装应用程序包并卸载您的应用程序包上的另一组应用程序包 WorkSpace

> **Note**
>
> - 要更新应用程序包，其状态 WorkSpace 必须为`AVAILABLE`或`STOPPED`。
> - 管理应用程序仅适用于 Windows WorkSpaces。
> - 管理应用程序仅适用于通过 Amazon订阅的应用程序捆绑包。

管理应用程序支持的捆绑包

“管理应用程序” 允许您在上安装和卸载以下应用程序 WorkSpaces。对于 Microsoft Office 2016 捆绑包和 Microsoft Office 2019，您只能卸载。

- 微软 Office LTSC 专业版 Plus 2024
- 微软 Visio LTSC 专业版 2024
- 微软 2024 年专业项目
- 微软 Office LTSC 标准 2024
- 微软 Visio LTSC 标准 2024
- 2024 年微软 Project 标准
- Microsoft Office LTSC Professional Plus 2021
- Microsoft Visio LTSC Professional 2021
- Microsoft Project Professional 2021
- Microsoft Office LTSC Standard 2021
- Microsoft Visio LTSC Standard 2021

- Microsoft Project Standard 2021
- Microsoft Visual Studio Professional 2022
- Microsoft Visual Studio Enterprise 2022

下表显示了支持和不支持的应用程序与操作系统组合列表：

	Microso Office Profess nal Plus 2016（ 位）	Microso Office Profess nal Plus 2019（ 位）	微软 LTSC Office Profess nal Plus / 标准 2024（ 位	微软 Project Profess nal / 标准 2024（ 位）	微软 Visio Professional / 标准 2024（64 位）	Microso LTSC Office Profess nal Plus/ Stan dard 2021 (64-bit)	Microso Project Profess nal/ Stand ard 2021（ 位）	Microso LTSC Visio Profess nal/ Stand ard 2021（ 位）	Microsoft Visual Studio Professio nal/ Enter prise 2022
Window Server 2016	卸载	不支持	不支持	不支持	不支持	不支持	不支持	不支持	不支持
Window Server 2019	不支持	卸载	不支持	不支持	不支持	安装/卸载	安装/卸载	安装/卸载	不支持
Window Server 2022	不支持	卸载	安装/卸载	安装/卸载	安装/卸载	安装/卸载	安装/卸载	安装/卸载	安装/卸载
Window 10	卸载	卸载	不支持	不支持	不支持	安装/卸载	安装/卸载	安装/卸载	安装/卸载
Window 11	卸载	卸载	安装/卸载	安装/卸载	安装/卸载	安装/卸载	安装/卸载	安装/卸载	安装/卸载

Important

- 微软Office/Visio/Project必须遵循相同的版本。例如，您不能将标准应用程序与专业应用程序混合使用。
- 微软Office/Visio/Project必须遵循相同的版本。例如，您不能将 2019 应用程序与 2021 应用程序混合使用。
- Valu Office/Visio/Project 2021 Standard/Professional e、Graphics 和 GraphicsPro WorkSpaces 捆绑包不支持 Microsoft。
- 不再支持微软 Office/Visio/Project 2010 和 2013 版本（标准版或专业版）。
- 超值套装不支持 Microsoft Office/Visio/Project 2024（标准版或专业版）。
- 另外，2025 年 10 月 14 日之后，将不再支持采用 Office 2016 或 Office 2019 的应用程序捆绑包。我们建议将你的 WorkSpaces 捆绑包与这些 Office 版本一起迁移到使用 Office 2021 或 Office 2024。有关更多信息，请参阅在 WorkSpaces 个人版中管理应用程序。
- 微软 Office、Project 和 Visio 在 2024 年版本中需要高达 25 GB 的可用空间，2021 年版本需要高达 20 GB 的可用空间。
- 微软 Visual Studio 2022 企业版/专业版不支持超值、标准、显卡和 GraphicsPro WorkSpaces 捆绑包。Performance 捆绑包可用于资源密集度较低的 Visual Studio 工作负载。但是，为了获得最佳效果，我们建议使用四核或更高捆绑包类型的 Visual Studio。捆绑包类型 Power、通用用途.4xLarge PowerPro、通用用途.8xLarge、Graphics.g4dn 和.g4dn 符合此要求。 GraphicsPro有关更多信息，请参阅 Visual Studio 2022 Product Family System Requirements。
- 当你从中卸载适用于 Microsoft Office 2016 的 Plus 应用程序包时，你将无法访问该亚马逊 WorkSpaces 捆绑包中包含的任何趋势科技解决方案。 WorkSpaces如果您想继续在 Amazon 上使用趋势科技解决方案 WorkSpaces，可以在Amazon 市场上单独购买。
- 要使用 install/uninstall Microsoft 365 应用程序，你需要引入自己的工具和安装程序，管理应用程序工作流程不能 install/uninstall Microsoft 365 应用程序。
- 您可以 installed/uninstalled 通过 “管理应用程序” 创建 WorkSpaces 带有应用程序的自定义映像。
- 对于选择加入的区域，例如非洲（开普敦），必须在目录级别启用 WorkSpaces 互联网连接。

在上更新应用程序包 WorkSpace

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在导航窗格中，请选择 WorkSpaces。
3. 选择， WorkSpace 然后选择 “操作”、“管理应用程序”。
4. 在 “当前应用程序” 下，您将看到已安装在此应用程序上的应用程序包列表 WorkSpace ，在 “选择应用程序” 下，您可以看到可供在此上安装的应用程序包列表。 WorkSpace
5. 要在此 WorkSpace上安装应用程序包，请执行以下操作：
   a. 选择要在此上安装的应用程序包 WorkSpace，然后选择 “关联”。
   b. 重复上一步以安装其他应用程序捆绑包。
   c. 安装应用程序捆绑包时，您将在当前应用程序下看到它们，其状态为 `Pending install deployment`。
6. 要从中卸载应用程序包，请执行以下操作 WorkSpace：
   a. 在选择应用程序下，选择要卸载的应用程序捆绑包，然后选择取消关联。
   b. 重复上一步以卸载其他应用程序捆绑包。
   c. 卸载应用程序捆绑包时，您将在当前应用程序下看到它们，其状态为 `Pending uninstall deployment`。
7. 要恢复捆绑包安装或安装状态，请执行以下一项操作。
   - 如果要从 `Pending uninstall deployment` 状态还原捆绑包，请选择要还原的应用程序，然后选择关联。
   - 如果要从 `Pending install deployment` 状态还原捆绑包，请选择要还原的应用程序，然后选择取消关联。
8. 在您选择安装或卸载的应用程序捆绑包处于待处理状态后，选择部署应用程序。

   > **Important**
   > 选择 “部署应用程序” 后，最终用户会话将终止，并且在安装或卸载应用程序时 WorkSpaces 将无法访问。

9. 要确认您的操作，请键入确认。选择强制，以安装或卸载处于错误状态的应用程序捆绑包。
10. 监控应用程序捆绑包的进度：

a. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。

b. 在导航窗格中，请选择 WorkSpaces。您可以在状态下看到状态，包括以下内容。

   - 正在更新 - 应用程序捆绑包更新仍在进行中。
   - A@@ VAILABLE/ STOPED-应用程序包更新已完成， WorkSpace 并且已恢复到其原始状态。

c. 要监视应用程序包的安装或卸载状态，请选择 WorkSpace 并选择查看详细信息。在应用程序下，您可以在状态下看到状态，包括 `Pending install`、`Pending uninstall` 和 `Installed`。

> **Note**
>
> 如果您的用户发现他们通过托管应用程序新安装的应用程序包未激活许可证，则可以手动 WorkSpace 重启。您的用户可以在重启后开始使用这些应用程序。如需其他支持，请联系 Amazon Support。

在上更新微软 Visual Studio 2022 工作负载 WorkSpace

默认情况下，Microsoft Visual Studio 2022 安装了以下工作负载，需要 18 GB 的硬盘空间：

- Visual Studio 核心编辑器
- Azure 开发
- 数据存储和处理
- .NET 桌面开发
- NET Multi-platform App UI 开发
- ASP.NET 和 Web 开发
- Node.js 开发

用户可以灵活地添加或删除工作负载和单个组件，从而使他们能够根据自己的特定要求定制应用程序。请务必注意，安装更多工作负载需要更多的磁盘空间。要详细了解工作负载配置，请参阅 Modify Visual Studio workloads, components, and language packs。

使用 “管理应用程序” 管理 WorkSpaces 已修改

在上安装或卸载应用程序包后 WorkSpaces，以下操作可能会影响现有配置。

- WorkSpace Re@@ store a WorkSpace-恢复后，会根据运行正常时创建的根卷和用户卷的最新快照，重新创建根卷和用户卷。 WorkSpace 每 12 小时拍摄一次完整 WorkSpace 快照。有关更多信息，请参阅恢复 WorkSpace。请确保至少等待 12 小时后再恢复使用 WorkSpaces “管理应用程序” 修改过的内容。使用管理应用程序修改 WorkSpaces 过的下一个完整快照恢复之前的完整快照将导致以下结果：
  - WorkSpaces 使用 “管理应用程序” 工作流程安装在您的应用程序包上的应用程序包将从您的应用程序中删除， WorkSpaces 但许可证仍会被激活，并且 WorkSpaces 将向您收取这些应用程序的费用。要恢复这些应用程序包， WorkSpaces 您需要再次运行管理应用程序工作流程，卸载应用程序以重新启动，然后重新安装。
  - WorkSpaces 使用 “管理应用程序” 工作流程从您的应用程序中删除的应用程序包将重新出现在您 WorkSpaces的。但是，这些应用程序捆绑包将无法正常运行，因为许可证激活缺失。要删除这些应用程序包，请从中手动卸载这些应用程序包。 WorkSpaces
- 重建 a WorkSpace-重建 WorkSpace 会重新创建根卷。有关更多信息，请参阅重新构建 WorkSpace。重建使用 WorkSpaces “管理应用程序” 修改过的内容将导致以下结果：
  - WorkSpaces 使用 “管理应用程序” 工作流程在您上安装的应用程序捆绑包将从您的应用程序中移除并停用。 WorkSpaces为了恢复这些应用程序， WorkSpaces 您需要再次运行 “管理应用程序” 工作流程。
  - WorkSpaces 通过 “管理应用程序” 工作流程从您的 “管理应用程序” 工作流程中删除的应用程序捆绑包将安装并激活。 WorkSpaces要从中移除这些应用程序包 WorkSpaces，您需要再次运行管理应用程序工作流程。
- Migr@@ ate a WorkSpace-迁移过程使用目标捆绑包映像中的新根卷和原始 WorkSpace包上次可用快照中的用户卷来重新创建。 WorkSpace WorkSpace 使用新 ID 创建了一个新的 WorkSpace ID。有关更多信息，请参阅迁 WorkSpace移使用管理应用程序修改 WorkSpaces 的迁移将导致以下结果：
  - 源中的所有应用程序包都 WorkSpaces 将被移除并停用。新的目标 WorkSpaces 将继承目标 WorkSpaces 包中的应用程序。源 WorkSpaces 应用程序捆绑包将按整月计费，但目标捆绑包中的应用程序捆绑包将按比例计费。

修改 WorkSpaces 个人版中的 WorkSpace

启动 WorkSpace 后，您可以通过以下三种方式修改其配置：

- 您可以更改其根卷的大小（对于 Windows，为驱动器 C；对于 Linux，为 /）及其用户卷（对于 Windows，为驱动器 D；对于 Linux，为 /home）。
- 您可以更改其计算类型以选择新的捆绑包。
- 如果您的 WorkSpace 是使用 PCoIP 捆绑包创建的，则您可以使用 Amazon CLI 或 Amazon WorkSpaces API 修改流式传输协议。

要查看 WorkSpace 的当前修改状态，请选择箭头以显示有关该 WorkSpace 的更多详细信息。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`。您无法同时更改卷大小和计算类型。

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 WorkSpaces 个人版中的用户启用自助式 WorkSpace 管理功能。

修改卷大小

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。

> **Note**
>
> 展开 WorkSpace 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 175 GB、最低用户卷容量为 100 GB 的 GeneralPurpose.4xlarge 或 GeneralPurpose.8xlarge 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.g4dn、GraphicsPro.g4dn、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（重新启动）WorkSpace。

> **Note**
>
> 如果您希望您的用户能够在磁盘大小增加过程中使用其 WorkSpace，请在调整 WorkSpace 的卷大小之前，确保 WorkSpace 的状态为 `AVAILABLE`，而不是 `STOPPED`。如果 WorkSpaces 的状态为 `STOPPED`，则在磁盘大小增加过程中无法启动它们。

在大多数情况下，增加磁盘大小的过程最多可能需要两个小时。但是，如果您要修改大量 WorkSpaces 的卷大小，则该过程可能需要更长的时间。如果您有大量 WorkSpaces 需要修改，建议您联系 Amazon Web Services 支持 以寻求帮助。

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.g4dn、GraphicsPro.g4dn、Graphics 或 GraphicsPro WorkSpace，否则，当用户卷为 100 GB 时，根卷不能小于 175 GB。Graphics.g4dn、GraphicsPro.g4dn、Graphics 和 GraphicsPro WorkSpaces 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。

修改 WorkSpace 的根卷

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择 WorkSpace，然后依次选择操作和修改根卷。
4. 在根卷大小下，选择卷大小或选择自定义以输入自定义卷大小。
5. 选择保存更改。
6. 完成增加磁盘大小后，必须重启 WorkSpace，才能使更改生效。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。

修改 WorkSpace 的用户卷

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择 WorkSpace，然后依次选择操作和修改用户卷。
4. 在用户卷大小下，选择卷大小或选择自定义以输入自定义卷大小。
5. 选择保存更改。
6. 完成增加磁盘大小后，必须重启 WorkSpace，才能使更改生效。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 WorkSpace 的卷大小

使用带有 `RootVolumeSizeGib` 或 `UserVolumeSizeGib` 属性的 modify-workspace-properties 命令。

修改计算类型

您可以在标准、节能、性能、PowerPro GeneralPurpose.4xlarge 和 GeneralPurpose.8xlarge 计算类型之间切换 WorkSpace。有关这些计算类型的更多信息，请参阅 Amazon WorkSpaces 捆绑包。

> **Note**
>
> - 如果您的源操作系统是 Windows Server 2022 或 Windows 11 以外的任何操作系统，则无法将计算类型从 PowerPro 更改为 GeneralPurpose。
> - 如果您要将计算类型从不支持 GPU 的捆绑包修改为 GeneralPurpose.4xlarge 或 GeneralPurpose.8xlarge，则您的 WorkSpaces 必须满足 175 GB 的最小根卷大小和 100 GB 的最小用户卷大小。要增加 WorkSpaces 的卷大小，请参阅 修改卷大小。
> - 您可以将计算类型从 Graphics.g4dn 更改为 GraphicsPro.g4dn，或者从 GraphicsPro.g4dn 更改为 Graphics.g4dn。您无法将 Graphics.g4dn 和 GraphicsPro.g4dn 的计算类型更改为任何其他值。
> - 2023 年 11 月 30 日之后，不再支持 Graphics 捆绑包。建议将您的 WorkSpaces 迁移到 Graphics.g4dn 捆绑包。有关更多信息，请参阅 以 WorkSpaces 个人 WorkSpace 方式迁移。
> - GraphicsPro 捆绑包的生命周期将于 2025 年 10 月 31 日结束。建议您在 2025 年 10 月 31 日之前将 GraphicsPro WorkSpaces 迁移到支持的捆绑包。有关更多信息，请参阅 以 WorkSpaces 个人 WorkSpace 方式迁移。
> - 您无法将 Graphics 和 GraphicsPro 的计算类型更改为任何其他值。

当您请求更改计算时，WorkSpaces 会使用新的计算类型重启 WorkSpace。WorkSpaces 会保留 WorkSpace 的操作系统、应用程序、数据以及存储设置。

请求较大计算类型的申请每 6 小时可以提一次，而请求较小计算类型的申请每 30 天可以提一次。对于新启动的 WorkSpace，您必须等待 6 个小时之后才能请求更大的计算类型。

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，WorkSpace 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 的计算类型

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择 WorkSpace，然后依次选择操作和修改计算类型。
4. 在计算类型下，选择一种计算类型。
5. 选择保存更改。

更改 WorkSpace 的计算类型

使用带有 `ComputeTypeName` 属性的 modify-workspace-properties 命令。

修改协议

> **Note**
> 修改协议目前在中国区域不可用。

如果您的 WorkSpace 是使用 PCoIP 捆绑包创建的，则您可以使用 Amazon CLI 或 Amazon WorkSpaces API 修改流式传输协议。这样，您就可以在不使用 WorkSpace 迁移功能的情况下，使用现有 WorkSpace 迁移协议。这还允许您使用 DCV 并维护根卷，而无需在迁移过程中重新创建现有 PCoIP WorkSpaces。

- 如果您的 WorkSpace 是使用 PCoIP 捆绑包创建的且不是启用了 GPU 的 WorkSpace，则您只能修改协议。
- 在将协议修改为 DCV 之前，请确保您的 WorkSpace 满足 DCV WorkSpace 的以下要求。
  - WorkSpaces 客户端支持 DCV
  - 部署 WorkSpace 的区域支持 DCV

- DCV 的 IP 地址和端口要求已开放。有关更多信息，请参阅 WorkSpaces 的 IP 地址和端口要求。
- 确保您当前的捆绑包在 DCV 中可用。
- 为了获得最佳视频会议体验，建议仅使用 Power、PowerPro、GeneralPurpose.4xlarge 或 GeneralPurpose.8xlarge。

> **Note**
>
> - 我们强烈建议您在开始更改协议之前使用非生产 WorkSpaces 进行测试。
> - 如果您将协议从 PCoIP 修改为 DCV，然后将协议修改回 PCoIP，将无法通过 Web Access 连接到 WorkSpaces。

更改 WorkSpace 的协议

1. [可选] 重启 WorkSpaces 并等到其处于 `AVAILABLE` 状态后再修改协议。
2. [可选] 使用 `describe-workspaces` 命令列出 WorkSpaces 属性。确保其处于 `AVAILABLE` 状态且其当前 `Protocol` 准确无误。
3. 使用 `modify-workspace-properties` 命令并将 `Protocols` 属性从 `PCOIP` 修改为 `DCV`，或者反过来。

```
aws workspaces modify-workspace-properties
--workspace-id <value>
--workspace-properties "Protocols=[WSP]"
```

> **Important**
>
> `Protocols` 属性区分大小写。确保使用 `PCOIP` 或 `DCV`。

4. 运行命令后，最多 20 分钟后即可重启 WorkSpace 并完成必要配置。
5. 再次使用 `describe-workspaces` 命令列出 WorkSpace 属性，并验证其是否处于 `AVAILABLE` 状态以及当前 `Protocols` 属性是否已更改为正确的协议。

> **Note**
>
> - 修改 WorkSpace 的协议不会更新控制台中的捆绑包描述。启动捆绑包描述不会更改。

- 如果 WorkSpace 在 20 分钟后仍处于 UNHEALTHY 状态，请在控制台中重启 WorkSpace。

6. 您现在可以连接到 WorkSpace 了。

在 WorkSpaces 个人版中自定义品牌

Amazon WorkSpaces 允许您使用 API，利用自己的品牌徽标、IT 支持信息、忘记密码链接和登录消息来自定义 WorkSpace 登录页面的外观，从而为用户打造熟悉的 WorkSpaces 体验。您的品牌将显示在用户的 WorkSpace 登录页面上，而不是默认的 WorkSpaces 品牌标识。

支持以下客户端：

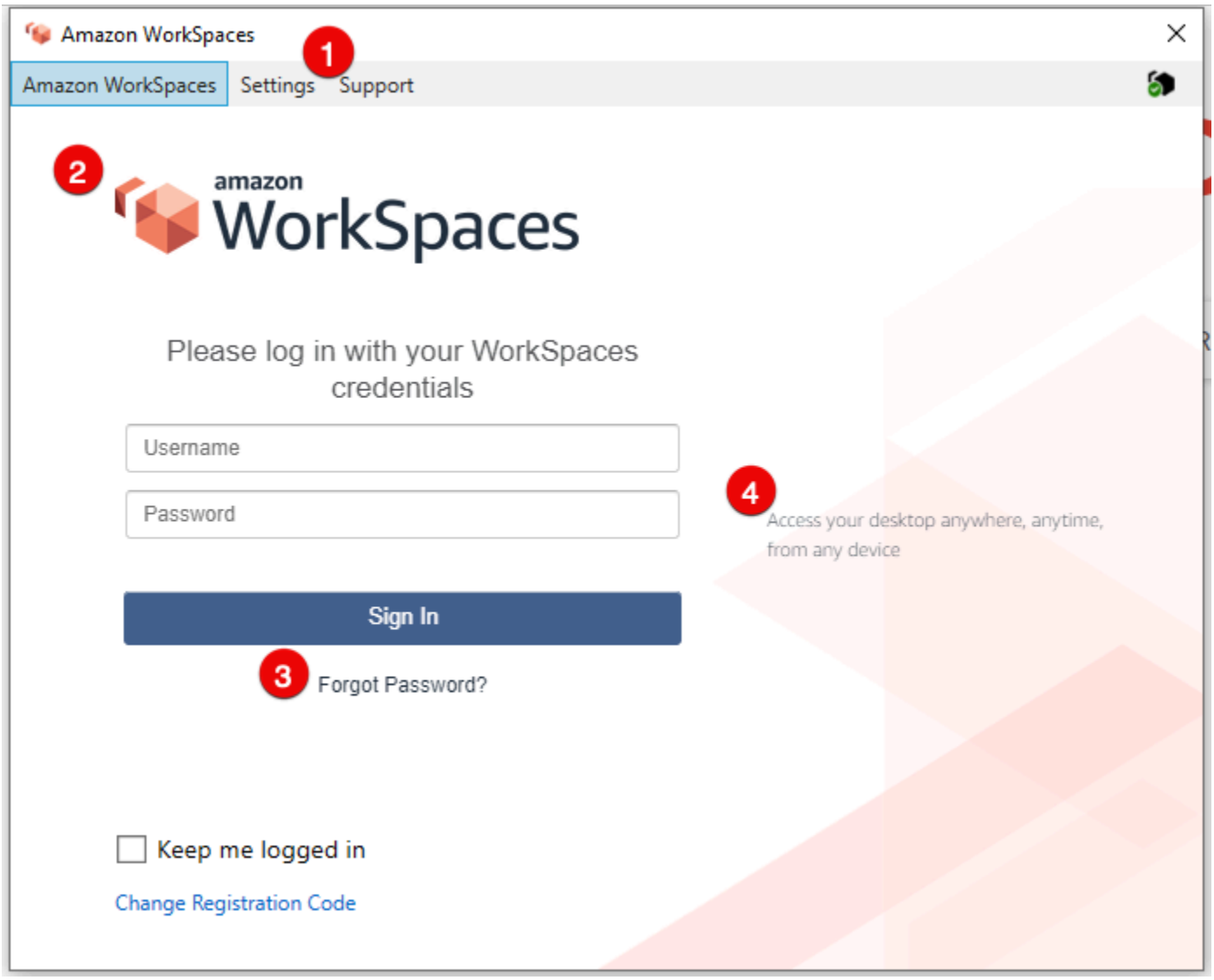
- Windows
- Linux
- Android
- MacOS
- iOS
- Web Access

> **Note**
>
> 要使用 Amazon GovCloud (US) Region中的 ClientBranding API 修改品牌元素，请使用 5.10.0 版 WorkSpaces 客户端。

导入自定义品牌

要导入您的客户端品牌自定义，请使用包含以下元素的操作 `ImportClientBranding`。有关更多信息，请参阅 ImportClientBranding API 参考。

> **Important**
>
> 客户端品牌属性面向公众。确保您不包含敏感信息。



1. 支持链接
2. 徽标
3. 忘记密码链接
4. 登录消息

自定义品牌元素

品牌元素	描述	要求和建议
支持链接	允许您指定支持电子邮件链接，供用户联系以获取有关其 WorkSpaces 的帮助。您可以	• 对于每种平台类型，`SupportEmail` 和 `SupportLink` 参数相互排

品牌元素	描述	要求和建议
	使用 `SupportEmail` 属性或使用 `SupportLink` 属性提供指向您支持页面的链接。	斥。您可以为每种平台类型指定单个参数，但不能同时指定两者。 • 默认电子邮件地址是 `workspaces-feedback@amazon.com` 。 • 长度限制：最小长度为 1。最大长度为 200。

徽标	允许您使用 `Logo` 属性自定义组织的徽标。	• 唯一接受的图像格式是从 `.png` 文件转换的二进制数据对象。
		• 建议的分辨率：
		  • Android：978 x 190
		  • 台式机：319 x 55
		  • iOS@2x：110 x 200
		  • iOS@3x：1650 x 300

忘记密码链接	允许您使用 ForgotPasswordLink 属性添加网址，用户在忘记 WorkSpace 密码时可以访问该网址。	长度限制：长度下限为 1。最大长度为 200。

品牌元素	描述	要求和建议
登录消息	允许您使用登录屏幕上的 `LoginMessage` 属性自定义消息。	• 长度约束：最小长度为 0。与 HTML 标签和不同的字体大小集成时的最大长度为 2000 个字符。对于没有 HTML 标签的默认情况，建议将登录消息保持在 600 个字符以内。 • 支持的 HTML 标签：`a, b, blockquote, br, cite, code, dd, dl, dt, div, em, i, li, ol, p, pre, q, small, span, strike, strong, sub, sup, u, ul`

以下是使用 ImportClientBranding 的示例代码片段。

Amazon CLI 版本 2

> **Warning**
>
> 导入自定义品牌会覆盖您在该平台中使用自定义数据指定的属性。它还会使用默认自定义品牌属性值覆盖您未指定的属性。您必须包含不想覆盖的任何属性的数据。

```
aws workspaces import-client-branding \
--cli-input-json file://~/Downloads/import-input.json \
--region us-west-2
```

导入 JSON 文件应与以下示例代码类似：

```
{
    "ResourceId": "<directory-id>",
    "DeviceTypeOsx": {
```

```
        "Logo":
 "iVBORw0KGgoAAAANSUhEUgAAAAIAAAACCAYAAABytg0kAAAAC0lEQVR42mNgQAcAABIAAeRVjecAAAAASUVORK5CYII="
        "ForgotPasswordLink": "https://amazon.com/",
        "SupportLink": "https://amazon.com/",
        "LoginMessage": {
            "en_US": "Hello!!"
        }
    }
}
```

以下 Java 代码段示例将徽标图片转换为 base64 编码的字符串：

```
// Read image as BufferImage
BufferedImage bi = ImageIO.read(new File("~/Downloads/logo.png"));

// convert BufferedImage to byte[]
ByteArrayOutputStream baos = new ByteArrayOutputStream();
ImageIO.write(bi, "png", baos);
byte[] bytes = baos.toByteArray();

//convert byte[] to base64 format and print it
String bytesBase64 = Base64.encodeBase64String(bytes);
System.out.println(bytesBase64);
```

以下 Python 代码段示例将徽标图片转换为 base64 编码的字符串：

```
# Read logo into base64-encoded string
with open("~/Downloads/logo.png", "rb") as image_file:
    f = image_file.read()
    base64_string = base64.b64encode(f)
    print(base64_string)
```

Java

> **Warning**
>
> 导入自定义品牌会覆盖您在该平台中使用自定义数据指定的属性。它还会使用默认自定义品牌属性值覆盖您未指定的属性。您必须包含不想覆盖的任何属性的数据。

```
// Create WS Client
```

```
WorkSpacesClient client = WorkSpacesClient.builder().build();

// Read image as BufferImage
BufferedImage bi = ImageIO.read(new File("~/Downloads/logo.png"));

// convert BufferedImage to byte[]
ByteArrayOutputStream baos = new ByteArrayOutputStream();
ImageIO.write(bi, "png", baos);
byte[] bytes = baos.toByteArray();

// Create import attributes for the plateform
DefaultImportClientBrandingAttributes attributes =
        DefaultImportClientBrandingAttributes.builder()
                .logo(SdkBytes.fromByteArray(bytes))
                .forgotPasswordLink("https://aws.amazon.com/")
                .supportLink("https://aws.amazon.com/")
                .build();

// Create import request
ImportClientBrandingRequest request =
        ImportClientBrandingRequest.builder()
                .resourceId("<directory-id>")
                .deviceTypeOsx(attributes)
                .build();

// Call ImportClientBranding API
ImportClientBrandingResponse response = client.importClientBranding(request);
```

Python

> **Warning**
>
> 导入自定义品牌会覆盖您在该平台中使用自定义数据指定的属性。它还会使用默认自定义品牌属性值覆盖您未指定的属性。您必须包含不想覆盖的任何属性的数据。

```
import boto3

# Read logo into bytearray
with open("~/Downloads/logo.png", "rb") as image_file:
    f = image_file.read()
    bytes = bytearray(f)
```

```
# Create WorkSpaces client
client = boto3.client('workspaces')

# Call import API
response = client.import_client_branding(
    ResourceId='<directory-id>',
    DeviceTypeOsx={
        'Logo': bytes,
        'SupportLink': 'https://aws.amazon.com/',
        'ForgotPasswordLink': 'https://aws.amazon.com/',
        'LoginMessage': {
            'en_US': 'Hello!!'
        }
    }
)
```

PowerShell

```
#Requires -Modules @{ ModuleName="AWS.Tools.WorkSpaces"; ModuleVersion="4.1.56"}

# Specify Image Path
$imagePath = "~/Downloads/logo.png"

# Create Byte Array from image file
$imageByte = ([System.IO.File]::ReadAllBytes($imagePath))

# Call import API
Import-WKSClientBranding -ResourceId <directory-id> `
    -DeviceTypeLinux_LoginMessage @{en_US="Hello!!"} `
    -DeviceTypeLinux_Logo $imageByte `
    -DeviceTypeLinux_ForgotPasswordLink "https://aws.amazon.com/" `
    -DeviceTypeLinux_SupportLink "https://aws.amazon.com/"
```

要预览登录页面，请启动 WorkSpaces 应用程序或网页登录页面。

> **Note**
>
> 更改最多可能需要 1 分钟才会显示。

描述自定义品牌

要查看您当前拥有的客户端品牌自定义的详细信息，请使用操作 `DescribeCustomBranding`。下面是使用 DescribeClientBranding 的示例脚本。有关更多信息，请参阅 DescribeClientBranding API 参考。

```
aws workspaces describe-client-branding \
--resource-id <directory-id> \
--region us-west-2
```

删除自定义品牌

要删除您的客户端品牌自定义，请使用操作 `DeleteCustomBranding`。下面是使用 DeleteClientBranding 的示例脚本。有关更多信息，请参阅 DeleteClientBranding API 参考。

```
aws workspaces delete-client-branding \
--resource-id <directory-id> \
--platforms DeviceTypeAndroid DeviceTypeIos \
--region us-west-2
```

> **Note**
>
> 更改最多可能需要 1 分钟才会显示。

在 WorkSpaces 个人版中为资源添加标签

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 Amazon 资源和组织数据（包括账单数据）的一种简单却强有力的方式。

向现有资源添加标签时，这些标签直到下个月的第一天才会出现在成本分配报告中。例如，如果您在 7 月 15 日向现有 WorkSpace 添加标签，则直到 8 月 1 日，这些标签才会出现在您的成本分配报告中。有关更多信息，请参阅《Amazon Billing 用户指南》中的使用成本分配标签。

> **Note**
>
> 要在 Cost Explorer 中查看您的 WorkSpaces 资源标签，必须按照《Amazon Billing 用户指南》中的激活用户定义的成本分配标签中的说明激活已应用于 WorkSpaces 资源的标签。

尽管标签会在激活 24 小时后显示，但与这些标签关联的值可能需要 4 到 5 天才能显示在 Cost Explorer 中。此外，要在 Cost Explorer 中显示和提供成本数据，已标记的 WorkSpaces 资源必须在此期间产生费用。Cost Explorer 仅显示标签激活时及以后的成本数据。目前没有可用的历史数据。

您可以添加标签的资源

- 您可以在创建以下资源时为其添加标签 — WorkSpaces、导入的图像和 IP 访问控制组。
- 您可以为以下类型的现有资源添加标签 — WorkSpaces、注册的目录、自定义捆绑包、图像和 IP 访问控制组。

标签限制

- 每个资源的标签数上限 – 50
- 最大密钥长度 - 127 个 Unicode 字符
- 最大值长度 - 255 个 Unicode 字符
- 标签键和值区分大小写。允许使用的字符包括可用 UTF-8 格式表示的字母、空格和数字，以及以下特殊字符： + - = 。_ : / @。请不要使用前导空格或尾随空格。
- 请勿在标签名称或值中使用 `aws:` 或 `aws:workspaces:` 前缀，因为它们专为 Amazon 使用预留。您无法编辑或删除带这些前缀的标签名称或值。

使用控制台（目录、WorkSpaces 或 IP 访问控制组）更新现有资源的标签

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择以下资源类型之一：目录、WorkSpaces 或 IP 访问控制。
3. 选择相应资源以打开其详细信息页面。
4. 执行以下一个或多个操作：
   - 要更新标签，请编辑键和值的值。
   - 要添加标签，请选择 Add Tag，然后编辑 Key 和 Value 的值。
   - 要删除标签，请选择标签旁边的删除图标 (X)。
5. 完成更新标签后，选择 Save (保存)。

使用控制台更新现有资源的标签（图像或捆绑包）

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择以下资源类型之一：捆绑包或图像。
3. 选择相应资源以打开资源详细信息页。
4. 在标签下，选择管理标签。
5. 执行以下一个或多个操作：
   - 要更新标签，请编辑键和值的值。
   - 要添加标签，请选择添加新标签，然后编辑键和值的值。
   - 要删除标签，请选择标签旁边的删除。
6. 更新标签后，选择保存更改。

使用 Amazon CLI 更新现有资源的标签

使用 create-tags 和 delete-tags 命令

WorkSpaces 个人版的维护

建议您定期维护 WorkSpaces。WorkSpaces 会为您的 WorkSpaces 安排默认维护时段。在维护时段内，WorkSpace 会根据需要从 Amazon WorkSpaces 安装重要更新并重启。如果有操作系统更新，则也会从 WorkSpace 配置为使用的操作系统更新服务器安装这些更新。维护过程中，您的 WorkSpace 可能无法使用。

默认情况下，您的 Windows WorkSpace 配置为从 Windows 更新接收更新。要为 Windows 配置您自己的自动更新机制，请参阅 Windows Server Update Services (WSUS) 和配置管理器的文档。

要求

您的 WorkSpace 必须具有互联网的访问权限，以便您将更新安装到操作系统以及部署应用程序。有关更多信息，请参阅 the section called “互联网访问”。

AlwaysOn WorkSpaces 的维护时段

对于 AlwaysOn WorkSpace，维护时段由操作系统设置决定。默认时段为 WorkSpace 所在时区每个星期日凌晨 00:00 至 04:00 的四小时时段。默认情况下，AlwaysOn WorkSpace 的时区为该 WorkSpace 所在 Amazon 区域的时区。但是，如果您从另一个区域连接且时区重定向处于启用状态，然后断开连接，则 WorkSpace 的时区将被更新为您连接时所在区域的时区。

您可以使用组策略禁用 Windows WorkSpaces 的时区重定向。您可以使用 PCoIP 代理配置禁用 Linux WorkSpaces 的时区重定向功能。

对于 Windows WorkSpaces，您可以使用组策略配置维护时段；请参阅配置组策略设置以进行自动更新。您不能为 Linux WorkSpace 配置维护时段。

AutoStop WorkSpaces 的维护时段

AutoStop WorkSpace 每月自动启动一次，以便安装重要更新。维护时段自当月第三个星期一开始，最长为两周，每天 00:00 至 05:00，时区为该 WorkSpace 所在 Amazon 区域的时区。可以在维护时段中的任意一天维护 WorkSpace。在此时间段内，仅保留超过 7 天的 WorkSpaces。

在 WorkSpace 进行维护的时间段内，WorkSpace 的状态设置为 `MAINTENANCE`。

尽管您无法修改用于维护 AutoStop WorkSpaces 的时区，但您可以按如下方式禁用 AutoStop WorkSpaces 的维护时段。如果您禁用维护模式，您的 WorkSpace 将不会重启且不会进入 `MAINTENANCE` 状态。

禁用维护模式

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。
3. 选择目录，然后选择 Actions、Update Details。
4. 展开 Maintenance Mode。
5. 要启用自动更新，请选择 Enabled。如果您倾向于手动管理更新，请选择 Disabled。
6. 选择更新并退出。

手动维护

如果您愿意，您可以按照自己的计划维护 WorkSpace。当您执行维护任务时，建议您将 WorkSpace 的状态更改为维护。维护完成后，将 WorkSpace 的状态更改为可用。

当 WorkSpace 处于维护模式下时，会发生以下行为：

- WorkSpace 不会对重启、停止、启动或重建的请求作出响应。
- 用户无法登录到 WorkSpace。
- AutoStop WorkSpace 不会休眠。

使用控制台更改 WorkSpace 的状态

> **Note**
>
> 要更改 WorkSpace 的状态，WorkSpace 必须处于可用状态。当 WorkSpace 未处于可用状态时，修改状态设置不可用。

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择您的 WorkSpace，然后依次选择操作和修改状态。
4. 在修改状态下，选择可用或维护。
5. 选择 Save。

使用 Amazon CLI 更改 WorkSpace 的状态

使用 modify-workspace-state 命令。

WorkSpaces 以 WorkSpaces 个人身份加密

WorkSpaces 已与 Amazon Key Management Service (Amazon KMS) 集成。这使您能够 WorkSpaces 使用密Amazon KMS钥对存储卷进行加密。当你启动 a 时 WorkSpace，你可以加密根卷（对于微软 Windows，是 C 盘；对于 Linux，/）和用户卷（对于 Windows，是 D 盘；对于 Linux，/home）。这样可以确保静态存储的数据、卷中的磁盘 I/O 数据以及从卷创建的快照都经过加密。

> **Note**
>
> - BitLocker Amazon 不支持加密 WorkSpaces。

内容

- 前提条件
- 限制
- 使用 WorkSpaces 加密概述 Amazon KMS
- WorkSpaces 加密上下文
- 授 WorkSpaces 予代表您使用 KMS 密钥的权限

- 加密 WorkSpace
- 查看已加密 WorkSpaces

前提条件

在开始加密过程之前，您需要一个密Amazon KMS钥。此 KMS 密钥可以是适用于亚马逊的Amazon托管 KMS 密钥 WorkSpaces（aws/workspaces），也可以是对称的客户托管 KMS 密钥。

- Amazon托管 KMS 密钥 — 在您首次 WorkSpace 从 WorkSpaces 控制台启动某个地区的未加密密钥时，Amazon WorkSpaces 会自动在您的账户中创建Amazon托管 KMS 密钥（aws/workspaces）。您可以选择此Amazon托管 KMS 密钥来加密您的用户和根卷 WorkSpace。有关更多信息，请参阅使用 WorkSpaces 加密概述 Amazon KMS。

  您可以查看此Amazon托管 KMS 密钥，包括其策略和授权，并可以在Amazon CloudTrail日志中跟踪其使用情况，但您无法使用或管理此 KMS 密钥。亚马逊 WorkSpaces 创建并管理此 KMS 密钥。只有 Amazon WorkSpaces 可以使用此 KMS 密钥，并且 WorkSpaces 只能使用它来加密您账户中的 WorkSpaces 资源。

  Amazon托管 KMS 密钥（包括 Amazon WorkSpaces 支持的密钥）每年轮换一次。有关详细信息，请参阅《Amazon Key Management Service开发人员指南》中的轮换Amazon KMS密钥。
- 客户托管 KMS 密钥 — 或者，您可以选择使用Amazon KMS创建的对称客户托管 KMS 密钥。您可以查看、使用和管理此 KMS 密钥，包括设置其策略。有关创建 KMS 密钥的更多信息，请参阅《Amazon Key Management Service 开发人员指南》中的创建密钥。有关使用 Amazon KMS API 创建 KMS 密钥的更多信息，请参阅Amazon Key Management Service开发人员指南中的使用密钥。

  除非您决定启用自动密钥轮换，否则客户托管 KMS 密钥不会自动轮换。有关详细信息，请参阅《Amazon Key Management Service开发人员指南》中的轮换Amazon KMS密钥。

> **Important**
>
> 手动轮换 KMS 密钥时，必须同时启用原始 KMS 密钥和新的 KMS 密钥，这样Amazon KMS才能解密原始 KMS 密钥加密后的密钥。 WorkSpaces 如果您不想保持原始 KMS 密钥处于启用状态，则必须重新创建 WorkSpaces并使用新的 KMS 密钥对其进行加密。

您必须满足以下要求才能使用密Amazon KMS钥加密您的 WorkSpaces：

- KMS 密钥必须是对称的。Amazon WorkSpaces 不支持非对称 KMS 密钥。有关区分对称和非对称 KMS 密钥的信息，请参阅《Amazon Key Management Service 开发人员指南》中的识别对称和非对称 KMS 密钥。
- KMS 密钥必须已启用。要确定是否启用 KMS 密钥，请参阅《Amazon Key Management Service 开发人员指南》中的显示 KMS 密钥详细信息。
- 您必须拥有与 KMS 密钥相关联的正确权限和策略。有关更多信息，请参阅 第 2 部分：使用 IAM 策略向 WorkSpaces 管理员授予额外权限。

限制

- 您无法加密现有的 WorkSpace。启动 WorkSpace 时必须对其进行加密。
- 不支持使用加密 WorkSpace 镜像创建自定义镜像。
- 目前不支持对加密文件 WorkSpace 禁用加密。
- WorkSpaces 在启用根卷加密的情况下启动，可能需要长达一个小时才能进行配置。
- 要重新启动或重建加密的 WorkSpace，请先确保Amazon KMS密钥已启用；否则，密钥 WorkSpace 将无法使用。要确定是否启用 KMS 密钥，请参阅《Amazon Key Management Service 开发人员指南》中的显示 KMS 密钥详细信息。

使用 WorkSpaces 加密概述 Amazon KMS

使用加密卷创建 WorkSpaces 时， WorkSpaces 使用亚马逊弹性区块存储 (Amazon EBS) Elastic Block Store 来创建和管理这些卷。Amazon EBS 通过行业标准的 AES-256 算法，利用数据密钥加密您的卷。Amazon EBS 和亚马逊都 WorkSpaces 使用您的 KMS 密钥来处理加密卷。有关 EBS 卷加密的更多信息，请参阅《亚马逊 EC2 用户指南》中的 Ama zon EBS 加密。

当您 WorkSpaces 使用加密卷启动时， end-to-end过程如下所示：

1. 您可以指定用于加密的 KMS 密钥以及用于的用户和目录 WorkSpace。此操作会创建一项授权，该授权仅 WorkSpaces 允许为此使用您的 KMS 密钥 WorkSpace，也就是说，仅允许与指定用户和目录 WorkSpace关联的用户使用您的 KMS 密钥。
2. WorkSpaces 为创建加密的 EBS 卷 WorkSpace 并指定要使用的 KMS 密钥以及该卷的用户和目录。此操作将创建一项授权，允许 Amazon EBS 仅将您的 KMS 密钥用于该卷 WorkSpace 和卷，也就是说，仅适用于与指定用户和目录 WorkSpace 关联的，并且仅用于指定的卷。

3. Amazon EBS 请求使用您的 KMS 密钥加密的卷数据密钥，并指定 WorkSpace 用户的 Active Directory 安全标识符 (SID) 和Amazon Directory Service目录 ID 以及亚马逊 EBS 卷 ID 作为加密上下文。
4. Amazon KMS创建新的数据密钥，使用您的 KMS 密钥对其进行加密，然后将加密的数据密钥发送到 Amazon EBS。
5. WorkSpaces 使用 Amazon EBS 将加密卷附加到您的 WorkSpace。Amazon EBS Amazon KMS 通过`Decrypt`请求将加密的数据密钥发送到，并指定 WorkSpace 用户的 SID、目录 ID 和卷 ID，后者用作加密上下文。
6. Amazon KMS使用您的 KMS 密钥解密数据密钥，然后将纯文本数据密钥发送到 Amazon EBS。
7. Amazon EBS 使用纯文本数据密钥加密所有传入和传出加密卷的数据。Amazon EBS 会将纯文本数据密钥保存在内存中，直至卷连接到 WorkSpace。
8. Amazon EBS 将加密的数据密钥（接收于Step 4）与卷元数据一起存储，以备将来重启或重建时使用。 WorkSpace
9. 当您使用删除 WorkSpace （或使用 WorkSpaces API 中的`TerminateWorkspaces`操作）时，WorkSpaces Amazon EBS 会停用允许他们使用您的 KMS 密钥进行此 WorkSpace操作的授权。Amazon Web Services 管理控制台

WorkSpaces 加密上下文

WorkSpaces 不会将您的 KMS 密钥直接用于加密操作（例如`EncryptDecryptGenerateDataKey`、、等），这意味着 WorkSpaces 不向包含加密上下文的请求发送请求。Amazon KMS但是，当 Amazon EBS 请求您的加密卷的加密数据密钥时 WorkSpaces（Step 3在使用 WorkSpaces 加密概述 Amazon KMS）以及请求该数据密钥的纯文本副本（Step 5）时，它会在请求中包含加密上下文。

加密上下文提供了额外的身份验证数据 (AAD)，Amazon KMS用于确保数据完整性。加密上下文也会写入您的Amazon CloudTrail日志文件，这可以帮助您了解使用给定的 KMS 密钥的原因。Amazon EBS 会对加密上下文使用以下内容：

- 与之关联的 Active Directory 用户的安全标识符 (SID) WorkSpace
- 与之关联的Amazon Directory Service目录的目录 ID WorkSpace
- Amazon EBS 加密卷的卷 ID

以下示例显示了 Amazon EBS 使用的加密上下文的 JSON 表示形式：

```
{
```

```
  "aws:workspaces:sid-directoryid":
 "[S-1-5-21-277731876-1789304096-451871588-1107]@[d-1234abcd01]",
  "aws:ebs:id": "vol-1234abcd"
}
```

授 WorkSpaces 予代表您使用 KMS 密钥的权限

您可以在 WorkSpaces（aws/workspaces）的Amazon托管 KMS 密钥或客户托管的 KMS 密钥下保护您的 WorkSpace 数据。如果您使用客户托管的 KMS 密钥，则需要授予代表账户 WorkSpaces 管理员使用 KMS 密钥的 WorkSpaces 权限。默认情况下，的Amazon WorkSpaces托管 KMS 密钥具有所需的权限。

要准备您的客户托管的 KMS 密钥以供使用 WorkSpaces，请按以下步骤操作。

1. 将您的 WorkSpaces 管理员添加到 KMS 密钥的密钥策略中的密钥用户列表中
2. 通过 IAM 策略为您的 WorkSpaces 管理员提供更多权限

您的 WorkSpaces 管理员还需要获得使用权限 WorkSpaces。有关这些权限的更多信息，请参阅 的身份和访问管理 WorkSpaces。

第 1 部分：将 WorkSpaces 管理员添加为关键用户

要向 WorkSpaces 管理员授予他们所需的权限，您可以使用Amazon Web Services 管理控制台或 Amazon KMS API。

将 WorkSpaces 管理员添加为 KMS 密钥的密钥用户（控制台）

1. 登录Amazon Web Services 管理控制台并在 https://console.aws.amazon.com/km s 处打开 Amazon Key Management Service (Amazon KMS) 控制台。
2. 要更改Amazon Web Services 区域，请使用页面右上角的区域选择器。
3. 在导航窗格中，选择客户托管密钥。
4. 选择首选客户托管 KMS 密钥的密钥 ID 或别名。
5. 选择 Key policy (密钥策略) 选项卡。在 Key users（密钥用户）下，选择 Add（添加）。
6. 在 IAM 用户和角色列表中，选择与您的 WorkSpaces 管理员对应的用户和角色，然后选择添加。

将 WorkSpaces 管理员添加为 KMS 密钥 (API) 的密钥用户

1. 使用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。将与您的 WorkSpaces 管理员对应的 IAM 用户和角色添加到向关键用户授予权限的策略声明中。然后保存文件。
3. 使用PutKeyPolicy操作将密钥策略应用于 KMS 密钥。

第 2 部分：使用 IAM 策略向 WorkSpaces 管理员授予额外权限

如果您选择客户托管的 KMS 密钥用于加密，则必须建立 IAM 策略，允许 Amazon WorkSpaces 代表您的账户中启动加密的 IAM 用户使用 KMS 密钥 WorkSpaces。该用户还需要获得使用Amazon的权限 WorkSpaces。有关创建和编辑 IAM 用户策略的更多信息，请参阅《IAM 用户指南》中的管理 IAM 策略和 的身份和访问管理 WorkSpaces。

WorkSpaces 加密需要对 KMS 密钥的有限访问权限。以下是您可以使用的一个示例密钥策略。此策略将可以管理 Amazon KMS 密钥的主体与可以使用此密钥的主体分开。在使用此示例密钥策略之前，请将示例账户 ID 和 IAM 用户名替换为您账户中的实际值。

第一条语句与默认Amazon KMS密钥策略相匹配。它授予您的账户使用 IAM 策略控制对 KMS 密钥的访问的权限。第二和第三条语句分别定义了Amazon哪些委托人可以管理和使用密钥。第四条语句Amazon KMS允许与集成的Amazon服务代表指定的委托人使用密钥。该语句允许 Amazon 服务创建和管理授权。该声明使用条件元素，将对 KMS 密钥的授予限制为Amazon服务代表您账户中的用户进行的授权。

> **Note**
>
> 如果您的 WorkSpaces 管理员使用创建 WorkSpaces 加密卷，则管理员需要列出别名和列出密钥的权限（`"kms:ListAliases"`和`"kms:ListKeys"`权限）。Amazon Web Services 管理控制台如果您的 WorkSpaces 管理员仅使用 Amazon WorkSpaces API（不使用控制台），则可以省略`"kms:ListAliases"`和`"kms:ListKeys"`权限。

JSON

```
{
  "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:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::123456789012:user/Alice"},
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": "*",
      "Condition": {"Bool": {"kms:GrantIsForAWSResource": "true"}}
    }
  ]
```

```
}
```

用于加密的用户或角色的 IAM 策略 WorkSpace 必须包括对客户托管的 KMS 密钥的使用权限以及对的访问 WorkSpaces权限。要向 IAM 用户或角色 WorkSpaces 授予权限，您可以将以下示例策略附加到 IAM 用户或角色。

JSON

```
{
    "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 Amazon KMS。它为用户提供了对 KMS 密钥的只读访问权限以及创建授权的能力。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:Describe*",
                "kms:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

如果您想在策略中指定 KMS 密钥，请使用类似于以下内容的 IAM 策略。将示例 KMS 密钥 ARN 替换为有效值。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "kms:CreateGrant",
      "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Resource": "*"
    }
  ]
}
```

加密 WorkSpace

要加密 WorkSpace

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 选择 Launch WorkSpaces 并完成前三个步骤。
3. 对于 “WorkSpaces 配置” 步骤，请执行以下操作：
   a. 选择要加密的卷：根卷、用户卷或这两种卷。
   b. 对于加密密钥，请选择一个Amazon KMS密钥，即 Amazon 创建的Amazon托管 KMS 密钥 WorkSpaces 或您创建的 KMS 密钥。您选择的 KMS 密钥必须是对称的。Amazon WorkSpaces 不支持非对称 KMS 密钥。
   c. 选择下一步。
4. 选择启动 WorkSpaces。

查看已加密 WorkSpaces

要从 WorkSpaces 控制台查看哪些 WorkSpaces 和卷已加密，请WorkSpaces从左侧的导航栏中进行选择。“卷加密” 列显示 WorkSpace 每个卷加密是启用还是禁用。要查看哪些特定卷已加密，请展开 WorkSpace 条目以查看 “加密卷” 字段。

重启 WorkSpaces 个人版中的 WorkSpace

有时，您可能需要手动重启（重新启动）WorkSpace。重启 WorkSpace 会将用户连接断开，然后执行 WorkSpace 的关闭和重启操作。为避免数据丢失，请确保用户先保存任意打开的文档和其他应用程序文件，然后您再重启 WorkSpace。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 Amazon KMS 密钥已启用；否则 WorkSpace 将变得不可用。要确定是否启用 KMS 密钥，请参阅《Amazon Key Management Service 开发人员指南》中的显示 KMS 密钥详细信息。

要重启 WorkSpace

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。

2. 在导航窗格中，选择 WorkSpaces。
3. 选择要重启的 WorkSpace，然后依次选择操作、重启 WorkSpaces。
4. 当系统提示您确认时，选择 Reboot WorkSpaces。

使用 Amazon CLI 重启 WorkSpace

使用 reboot-workspaces 命令。

批量重启 WorkSpaces

使用 amazon-workspaces-admin-module。

重建 WorkSpaces 个人版中的 WorkSpace

重建 WorkSpace 将重新创建启动 WorkSpace 的捆绑包的最新映像的根卷、其用户卷及其主弹性网络接口。与还原 WorkSpace 相比，重建 WorkSpace 会删除更多的数据，但它只需要您拥有用户卷的快照即可。要还原 WorkSpace，请参阅还原 WorkSpaces 个人版中的 WorkSpace。

重建 WorkSpace 将导致以下情况的出现：

- 根卷（对于 Microsoft Windows，为驱动器 C；对于 Linux，为 /）使用创建 WorkSpace 时使用的捆绑包的最新映像进行刷新。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，都会拍摄这些用户卷的快照。依次选择操作、重建/还原 WorkSpace 时，将显示最新快照的日期和时间。

  重建 WorkSpace 时，还将在重建完成后不久（通常在 30 分钟内）拍摄新快照。
- 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 以 WorkSpaces 个人 WorkSpace 方式迁移。

您只能在满足以下条件时重建 WorkSpace：

- WorkSpace 的状态必须为 `AVAILABLE`、`ERROR`、`UNHEALTHY`、`STOPPED` 或 `REBOOTING`。要重建处于 `REBOOTING` 状态的 WorkSpace，您必须使用 RebuildWorkSpaces API 操作或 rebuild-workspaces Amazon 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 Amazon KMS 密钥已启用；否则 WorkSpace 将变得不可用。要确定是否启用 KMS 密钥，请参阅《Amazon Key Management Service 开发人员指南》中的显示 KMS 密钥详细信息。

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择要重建的 WorkSpace，然后依次选择操作、重建/还原 WorkSpace。
4. 在快照下，选择快照的时间戳。
5. 选择 Rebuild (重建)。

使用 Amazon CLI 重建 WorkSpace

使用 rebuild-workspaces 命令。

故障排除

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。

重建已加入 Microsoft Entra ID 的 WorkSpaces

当用户在重建后首次登录 WorkSpace 时，他们需要再次体验开箱即用体验（OOBE），这与为他们分配新 WorkSpace 时类似。因此，将在 WorkSpace 上创建一个新的用户配置文件文件夹，以覆盖原始用户配置文件文件夹。因此，在重建加入 Entra 的 WorkSpace 期间，原始用户配置文件文件夹中的内容将保存在重建后的 WorkSpace 的 `D:\Users\<USERNAME%MMddyyTHHmmss%.NotMigrated>` 下。用户需要将原始配置文件内容从 `D:\Users\<USERNAME%MMddyyTHHmmss%.NotMigrated>` 复制到用户配置文件文件夹 D:\Users\<USERNAME> 中，才能还原所有用户配置文件数据，包括桌面图标、快捷方式和数据文件。

> **Note**
>
> 对于加入 Microsoft Entra ID 的 WorkSpaces，我们建议尽可能使用“还原 WorkSpaces”，而不是“重建 WorkSpaces”。

还原 WorkSpaces 个人版中的 WorkSpace

还原 WorkSpace 将使用在 WorkSpace 运行状况良好时拍摄的每个卷的快照来重新创建根卷和用户卷。还原 WorkSpace 会将根卷和用户卷上的数据回滚到创建快照的时间点。重建 WorkSpace 只会回滚用户卷上的数据。这意味着，还原要求您同时拥有根卷和用户卷的快照，而重建 WorkSpace 只需要用户卷的快照。要重建 WorkSpace，请参阅重建 WorkSpaces 个人版中的 WorkSpace。

还原 WorkSpace 将导致以下情况的出现：

- 根卷（对于 Microsoft Windows，为驱动器 C；对于 Linux，为 /）将还原到使用快照指定的日期和时间。在创建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，为驱动器 D；对于 Linux，为 /home）将重新创建，日期和时间为使用快照指定的日期和时间。用户卷的当前内容将被覆盖。

还原点

依次选择操作和重建/还原 WorkSpace 时，将显示用于操作的快照的日期和时间。要通过 Amazon CLI 验证用于操作的快照的日期和时间，请使用 describe-workspace-snapshots 命令。

拍摄快照时

根卷和用户卷的快照是在以下基础上拍摄的。

- 首次创建 WorkSpace 之后 - 通常，根卷和用户卷的初始快照是在 WorkSpace 创建后不久（通常在 30 分钟内）拍摄的。在某些 Amazon 区域，创建 WorkSpace 后可能需要几个小时才能拍摄初始快照。

  如果在拍摄初始快照之前 WorkSpace 运行状况不佳，则无法还原 WorkSpace。在这种情况下，您可以尝试重建 WorkSpace 或联系 Amazon Support 寻求帮助。
- 正常使用期间 - 每 12 小时安排一次在还原 WorkSpace 时使用的自动快照。如果 WorkSpace 运行状况良好，则将同时创建根卷和用户卷的快照。如果 WorkSpace 运行状况不佳，则仅针对用户卷创建快照。
- WorkSpace 还原后 - 还原 WorkSpace 时，将在还原完成后不久（通常在 30 分钟内）拍摄新快照。在某些 Amazon 区域，还原 WorkSpace 后可能需要几个小时才能拍摄这些快照。

  还原 WorkSpace 后，如果 WorkSpace 在拍摄新快照之前运行状况不佳，则无法再次还原 WorkSpace。在这种情况下，您可以尝试重建 WorkSpace 或联系 Amazon Support 寻求帮助。

您只能在满足以下条件时还原 WorkSpace：

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

还原 WorkSpace

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择要还原的 WorkSpace，然后依次选择操作、重建/还原 WorkSpace。
4. 在快照下，选择快照的时间戳。
5. 选择还原。

使用 Amazon CLI 还原 WorkSpace

使用 restore-workspace 命令。

升级 WorkSpaces 个人版中的 Windows BYOL WorkSpaces

在您的 Windows 自带许可 (BYOL) WorkSpaces 上，可以使用就地升级过程升级到 Windows 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 和 11 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

- 先决条件
- 注意事项
- 已知限制条件
- 注册表项设置摘要
- 执行就地升级
- 故障排除
- 使用 PowerShell 脚本更新您的 WorkSpace 注册表

先决条件

- 如果您通过使用组策略或 System Center Configuration Manager（SCCM）推迟或暂停 Windows 10 和 11 升级，请对您的 Windows 10 和 11 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。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。如果您在驱动器 D 上有多个用户配置文件，请删除除所需配置文件之外的所有用户配置文件。

注意事项

就地升级过程使用两个注册表脚本（`enable-inplace-upgrade.ps1` 和 `update-pvdrivers.ps1`）对您的 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，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 或 11 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 和 11 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：HKLM:\Software\Amazon\WorkSpacesConfig\enable-inplace-upgrade.ps1

注册表项	类型	值
已启用	DWORD	0 – （默认值）禁用就地升级 1 – 启用就地升级
PostUpgradeRestoreProfileOnD	DWORD	0 – （默认值）在就地升级后，不尝试还原用户配置文件路径 1 – 在就地升级后，还原用户配置文件路径 (ProfileImagePath)
UserShellFoldersRedirection	DWORD	0 – 不对用户 Shell 文件夹进行重定向 1 – （默认值）在用户配置文件在 `C:\Users\%USERNAME%` 上重新生成后，将用户 Shell 文件夹重定向到 `D:\Users\%USERNAME%`
NoReboot	DWORD	0 – （默认值）允许您控制在修改用户配置文件的注册表后何时重启 1 – 在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：HKLM:\Software\Amazon\WorkSpacesConfig\update-pvdrivers.ps1

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

执行就地升级

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。

执行 Windows 10 和 11 就地升级

1. 记下要更新的 Windows 10 和 11 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，请参阅注意事项），并按以下方式设置注册表项：

   - 如果您希望在升级后用户配置文件位于驱动器 C 上，请设置：

     HKEY_LOCAL_MACHINE\SOFTWARE\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。
> - 等待 10 分钟，确保 WorkSpace 畅通无阻。

（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 和 11 版本及安装的应用程序数量，此过程可能需要 40-120 分钟。

> **Note**
>
> 就地升级过程可能至少需要一个小时。WorkSpace 实例的状态在升级期间可能显示为 `UNHEALTHY`。

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，则 Windows 会自动回滚以使用开始升级之前已安装的 Windows 10 和 11 版本。有关疑难解答的更多信息，请参阅 Microsoft 文档。

（可选）要确认更新脚本已成功执行，请验证以下键值是否设置为 1：

HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\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。

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 和 11 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。

故障排除

如果您在更新过程中遇到任何问题，可以查看以下各项以帮助排除故障：

- Windows 日志，默认情况下位于以下位置：

  `C:\Program Files\Amazon\WorkSpacesConfig\Logs\`

  `C:\Program Files\Amazon\WorkSpacesConfig\Logs\TRANSMITTED`
- Windows 事件查看器

  Windows 日志 > 应用程序 > 来源：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。

Windows 11 24H2 升级使用 ISO 错误解析

Windows 11 24H2 升级过程可能会在第二个启动阶段遇到严重的启动故障，具体而言会出现错误代码 0xC1900101 - 0x40017。出现此错误的原因通常是系统驱动程序文件丢失或损坏，导致安装无法在启动操作阶段成功完成。

错误代码：0xC1900101 - 0x40017

错误描述：在 SECOND_BOOT 阶段安装失败，出现 BOOT 操作错误

1. 确保您有 Windows 11 24H2 ISO 文件。
2. 以管理员身份打开命令提示符。
3. 使用以下命令复制所需的系统文件：

   ```
   copy "ISO-Drive:\Sources\WinSetupMon.sys" "C:\Windows\System32\Drivers\"
   ```

   将 ISO-Drive 替换为 ISO 驱动程序信息。
4. 使用以下路径验证文件副本：

   ```
   C:\Windows\System32\Drivers\
   ```
5. 使用 ISO 文件启动 Windows 11 24H2 升级。

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，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 run on the next reboot of the
 WorkSpace.

$scriptlist = ("update-pvdrivers.ps1","enable-inplace-upgrade.ps1")
$wsConfigRegistryRoot="HKLM:\Software\Amazon\WorkSpacesConfig"
$Enabled = 1
$script:ErrorActionPreference = "Stop"

foreach ($scriptName in $scriptlist)
{
```

```
    $scriptRegKey = "$wsConfigRegistryRoot\$scriptName"

    try
    {
        if (-not(Test-Path $scriptRegKey))
        {
            Write-Host "Registry key not found. Creating registry key '$scriptRegKey'
 with 'Update' enabled."
            New-Item -Path $wsConfigRegistryRoot -Name $scriptName | Out-Null
            New-ItemProperty -Path $scriptRegKey -Name Enabled -PropertyType DWord -
Value $Enabled | Out-Null
            Write-Host "Value created. '$scriptRegKey' Enabled='$((Get-ItemProperty -
Path $scriptRegKey).Enabled)'"
        }
        else
        {
            Write-Host "Registry key is already present with value '$scriptRegKey'
 Enabled='$((Get-ItemProperty -Path $scriptRegKey).Enabled)'"
            if((Get-ItemProperty -Path $scriptRegKey).Enabled -ne $Enabled)
            {
                Set-ItemProperty -Path $scriptRegKey -Name Enabled -Value $Enabled
                Write-Host "Value updated. '$scriptRegKey' Enabled='$((Get-ItemProperty
 -Path $scriptRegKey).Enabled)'"
            }
        }
    }
    catch
    {
        write-host "Stopping script, the following error was encountered:" `r`n$_ -
ForegroundColor Red
        break
    }
}
```

以 WorkSpaces 个人 WorkSpace 方式迁移

> **Note**
>
> 如果你想取消订阅或卸载 Microsoft Office 版本Amazon的许可证 WorkSpace，我们建议你使用管理应用程序。

您可以将 WorkSpace 从一个捆绑包迁移到另一个捆绑包，同时将数据保留在用户卷上。下面是一些示例方案：

- 你可以 WorkSpaces 从 Windows 7 桌面体验迁移到 Windows 10 桌面体验。
- 您可以 WorkSpaces 从 PCo IP 协议迁移到 DCV。
- 你可以 WorkSpaces 从 Windows Server 上的 32 位微软 Office 2016 版本的 WorkSpaces 捆绑包迁移到 Windows Server 2019 上的 64 位微软 Office 和支持 Windows Server 2022 的捆绑包。WorkSpaces
- 您可以 WorkSpaces 从一个公共或自定义捆绑包迁移到另一个捆绑包。例如，你可以从支持 GPU（Graphics.g4dn）迁移。 GraphicsPro.g4dn、Graphics 和 GraphicsPro) 捆绑包到 non-GPU-enabled捆绑包，反之亦然。
- 你可以将使用微软 Office WorkSpaces 的 Windows 迁移Amazon到包含微软 365 应用程序的自定义 WorkSpaces 捆绑包。迁移完成后， WorkSpaces 你将取消订阅微软 Office。
- 你可以将使用微软 Office WorkSpaces 的 Windows 迁移Amazon到没有 Office 2016/2019 订阅的 WorkSpaces捆绑包中。迁移完成后， WorkSpaces 你将取消订阅微软 Office。
- 你可以将 BYOL BYOP WorkSpaces 从 Windows 10 迁移到 Windows 11，将包含许可证的 BYOP WorkSpaces 从 Windows Server 2019 迁移到 Windows Server 2022。

有关 Amazon WorkSpaces 捆绑包的更多信息，请参阅WorkSpaces 个人版的捆绑包和映像。

迁移过程使用目标捆绑包映像中的新根卷和原始 WorkSpace包映像的最后一个可用快照中的用户卷来重新创建。 WorkSpace 迁移过程中会生成一个新的用户配置文件，以获得更好的兼容性。将重命名旧用户配置文件，然后将旧用户配置文件中的某些文件移动到新用户配置文件。（有关所移动的内容的详细信息，请参阅迁移过程中会发生什么。）

每次迁移过程最多需要一个小时 WorkSpace。启动迁移过程时，会创建一个新的 WorkSpace 迁移过程。如果发生导致无法成功迁移的错误， WorkSpace 则会恢复原始文件并将其恢复到其原始状态，然后终止新的 WorkSpace 迁移。

目录

- 迁移限制
- 迁移场景
- 迁移过程中会发生什么
- 最佳实践
- 问题排查

- 账单如何受到影响
- 迁移 WorkSpace

迁移限制

- 您不能迁移到公有或自定义 Windows 7 桌面体验捆绑包。您也不能迁移到自带许可证 (BYOL) Windows 7 捆绑包。
- 您 WorkSpaces 只能将 BYOL 迁移到其他 BYOL 捆绑包。要将 BYOL WorkSpace 从 PCo IP 迁移到 DCV，必须先使用 DCV 协议创建 BYOL 捆绑包。然后，你可以将你 PCo的 IP BYOL 迁移 WorkSpaces 到那个 DCV BYOL 捆绑包。
- 您无法将从公共或自定义捆绑包中 WorkSpace 创建的分发包迁移到 BYOL 捆绑包。
- Graphics.g4dn、 GraphicsPro .g4dn、Graphics 和 GraphicsPro 捆绑包可用于 Windows 和 Ubuntu 上的 IP 协议。 PCoGraphics.g4dn 和 GraphicsPro .g4dn 可用于 Windows 和 Ubuntu 上的 DCV 协议。显卡，还 GraphicsPro WorkSpaces 无法迁移到 DCV。
- WorkSpaces 目前不支持迁移 Linux。
- 在支持多种语言的Amazon区域中，您可以在语言包 WorkSpaces之间迁移。
- 源捆绑包和目标捆绑包必须不同。（但是，在支持多种语言的区域中，只要语言不同，就可以迁移到相同的 Windows 10 捆绑包。）如果您想 WorkSpace 使用相同的捆绑包刷新，请 WorkSpace改为重新构建。
- 您无法 WorkSpaces 跨区域迁移。
- 在某些情况下，如果迁移无法成功完成，您可能不会收到错误消息，并且可能显示迁移过程未启动。如果在尝试迁移一小时后 WorkSpace 捆绑包保持不变，则迁移不成功。请联系 Amazon Web Services 支持 中心以获取帮助。
- 您无法将 BYOP 迁移 WorkSpaces 到 PCo IP 或 DC WorkSpaces V。
- 你无法将已加入的 Active Directory 域名迁移到 WorkSpaces Microsoft Entra- WorkSpaces

迁移场景

下表显示了哪些迁移方案可用：

源操作系统	目标操作系统	是否可用？
公有或自定义捆绑包 Windows 7	公有或自定义捆绑包 Windows 10	是

源操作系统	目标操作系统	是否可用？
自定义捆绑包 Windows 7	公有捆绑包 Windows 7	否
自定义捆绑包 Windows 7	自定义捆绑包 Windows 7	否
公有捆绑包 Windows 7	自定义捆绑包 Windows 7	否
公有或自定义捆绑包 Windows 10	公有或自定义捆绑包 Windows 7	否
公有或自定义捆绑包 Windows 10	自定义捆绑包 Windows 10	是
Windows 7 BYOL 捆绑包	Windows 7 BYOL 捆绑包	否
Windows 7 BYOL 捆绑包	Windows 10 BYOL 捆绑包	是
Windows 10 BYOL 捆绑包	Windows 7 BYOL 捆绑包	否
Windows 10 BYOL 捆绑包	Windows 10 BYOL 捆绑包	是
支持 Windows Server 2016 的公有 Windows 10 捆绑包	支持 Windows Server 2019 的公有 Windows 10 捆绑包	是
支持 Windows Server 2019 的公有 Windows 10 捆绑包	支持 Windows Server 2016 的公有 Windows 10 捆绑包	是
支持 Windows Server 2016 的自定义 Windows 10 捆绑包	支持 Windows Server 2019 的公有 Windows 10 捆绑包	是
支持 Windows Server 2016 的自定义 Windows 10 捆绑包	支持 Windows Server 2022 的公有 Windows 10 捆绑包	是
支持 Windows Server 2019 的自定义 Windows 10 捆绑包	支持 Windows Server 2022 的公有 Windows 10 捆绑包	是
Windows 10 BYOP BYOL	Windows 11 BYOP BYOL	是
Windows 11 BYOP BYOL	Windows 10 BYOP BYOL	否

源操作系统	目标操作系统	是否可用？
支持 Windows Server 2019 的公有 BYOP	支持 Windows Server 2022 的公有 BYOP	是
支持 Windows Server 2022 的公有 BYOP	支持 Windows Server 2019 的公有 BYOP	否

> **Note**
>
> 基于 Windows Server 2019 的 Public Windows 10 捆绑包 PCo IP 分支无法访问 Web。

迁移过程中会发生什么

在迁移过程中，用户卷（驱动器 D）上的数据将保留，但根卷（驱动器 C）上的所有数据都将丢失。这意味着不会保留已安装的应用程序、设置和对注册表的更改。旧用户配置文件文件夹将使用 `.NotMigrated` 后缀重命名，并创建一个新的用户配置文件。

迁移过程基于原始用户卷的最后一个快照重新创建驱动器 D。在首次启动新文件夹时 WorkSpace，迁移过程会将原始`D:\Users\%USERNAME%`文件夹移动到名为的文件夹`D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated`。新的操作系统生成一个新的 `D:\Users\%USERNAME%\` 文件夹。

创建新用户配置文件后，以下用户 shell 文件夹中的文件将从旧 `.NotMigrated` 配置文件移动到新配置文件：

- `D:\Users\%USERNAME%\Desktop`
- `D:\Users\%USERNAME%\Documents`
- `D:\Users\%USERNAME%\Downloads`
- `D:\Users\%USERNAME%\Favorites`
- `D:\Users\%USERNAME%\Music`
- `D:\Users\%USERNAME%\Pictures`
- `D:\Users\%USERNAME%\Videos`

> **Important**
>
> 迁移过程尝试将文件从旧用户配置文件移动到新配置文件。迁移过程中未移动的任何文件将保留在 `D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated` 文件夹中。如果迁移成功，您可以看到哪些文件被移入 `C:\Program Files\Amazon\WorkspacesConfig\Logs\MigrationLogs`。您可以手动移动任何未自动移动的文件。
> 默认情况下，公有捆绑包禁用本地搜索索引。如果您要启用它，则默认设置为搜索 `C:\Users` 而不是搜索 `D:\Users`，因此您也需要对其进行调整。如果您已将本地搜索索引专门设置为 `D:\Users\`*`username`*，而未设置为 `D:\Users`，则迁移后可能无法对 `D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated` 文件夹中的任何用户文件使用本地搜索索引。

在迁移过程中，分配给原始标签的所有标签 WorkSpace 都将被保留，并保留 WorkSpace 的运行模式。但是，新用户 WorkSpace 会获得新的 WorkSpace ID、计算机名称和 IP 地址。

最佳实践

在迁移之前 WorkSpace，请执行以下操作：

- 将驱动器 C 上的任何重要数据备份到另一个位置。在迁移过程中，将擦除驱动器 C 上的所有数据。
- 请确保 WorkSpace 正在迁移的已有至少 12 小时的时间，以确保已创建用户卷的快照。在 Amazon WorkSpaces 控制台的 Migrat e WorkSpaces 页面上，您可以看到上次拍摄快照的时间。在迁移过程中，上一个快照之后创建的所有数据将丢失。
- 为避免潜在的数据丢失，请确保您的用户注销其账户， WorkSpaces并且在迁移过程完成后才重新登录。请注意，当它们处于`ADMIN_MAINTENANCE`模式时 WorkSpaces 无法迁移。
- 确保 WorkSpaces 要迁移的状态为`AVAILABLESTOPPED`、或`ERROR`。
- 请确保您有足够的 IP 地址供 WorkSpaces 要迁移的。在迁移期间，将为分配新的 IP 地址 WorkSpaces。
- 如果您使用脚本进行迁移 WorkSpaces，请分批迁移它们，一次不超过 25 WorkSpaces 个。

问题排查

- 如果用户在迁移后报告丢失文件，请检查其用户配置文件是否在迁移过程中未移动。您可以看到哪些文件被移入 `C:\Program Files\Amazon\WorkspacesConfig\Logs\MigrationLogs`。未移

动的文件将位于 `D:\Users\%USERNAME%MMddyyTHHmmss%.NotMigrated` 文件夹中。您可以手动移动任何未自动移动的文件。

- 如果您正在使用 API 进行迁移 WorkSpaces ，但迁移未成功，则不会使用该 API 返回的目标 WorkSpace ID，并且仍 WorkSpace将使用原始 WorkSpace ID。
- 如果迁移未成功完成，请检查 Active Directory 以查看它是否相应地被清理了。您可能需要手动删除 WorkSpaces 不再需要的内容。

账单如何受到影响

在迁移发生的当月，您需要为新迁移和原始 WorkSpaces迁移按比例支付费用。例如，如果您在 5 月 10 日将 WorkSpace A 迁移到 WorkSpace B，则将在 5 月 1 日至 5 月 10 日期间支付 WorkSpace A 费用，并在 5 月 11 日至 5 月 30 日期间支付 WorkSpace B 费用。

> **Note**
>
> 如果 WorkSpace 要将 a 迁移到不同的捆绑包类型（例如，从 “性能” 到 “Power”，或 “Value” 到 “标准”），则在迁移过程中，根卷（驱动器 C）和用户卷（驱动器 D）的大小可能会增加。如有必要，根卷增加以匹配新捆绑包的默认根卷大小。但是，如果您已为用户卷指定的大小与原始捆绑包的默认大小不同（更高或更低），则在迁移过程中会保留相同的用户卷大小。否则，迁移过程将使用源 WorkSpace 用户卷大小中较大的容量和新捆绑包的默认用户卷大小。

迁移 WorkSpace

您可以 WorkSpaces 通过亚马逊 WorkSpaces 控制台、Amazon CLI或亚马逊 WorkSpaces API 进行迁移。

要迁移 WorkSpace

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在导航窗格中，请选择 WorkSpaces。
3. 选择您的 WorkSpace ，然后选择操作，迁移 WorkSpaces。
4. 在捆绑包下，选择您要迁移到的捆绑包 WorkSpace 。

> **Note**
>
> 要将 BYOL WorkSpace 从 PCo IP 迁移到 DCV，必须先使用 DCV 协议创建 BYOL 捆绑包。然后，你可以将你 PCo的 IP BYOL 迁移 WorkSpaces 到那个 DCV BYOL 捆绑包。

5. 选择 Migrate WorkSpaces。

   Amazon WorkSpaces 控制台中`PENDING`会出现一个状态为的新 WorkSpace 内容。迁移完成后，原始 WorkSpace 迁移将终止，新迁移的状态将设置 WorkSpace 为`AVAILABLE`。

6. （可选）要删除您不再需要的任何自定义捆绑包和映像，请参阅删除 WorkSpaces 个人版中的自定义捆绑包或映像。

要 WorkSpaces 通过迁移Amazon CLI，请使用 migrat e-workspace 命令。要 WorkSpaces 通过亚马逊 WorkSpaces API 进行迁移，请参阅MigrateWorkSpace《亚马逊 WorkSpaces API 参考》。

删除 WorkSpaces 个人版中的 WorkSpace

当不再使用某个 WorkSpace 时，可以将其删除。还可以删除相关资源。

> **Warning**
>
> 删除 WorkSpace 是一项永久性操作，无法撤消。WorkSpace 用户的数据不会保留，而是会销毁。要获取有关备份用户数据的帮助，请联系 Amazon Support。

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

删除 WorkSpace

您可以删除除已暂停之外处于任何状态的 WorkSpace。

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择 WorkSpaces。
3. 选择您的 WorkSpace 并选择删除。
4. 当系统提示进行确认时，选择删除。删除 WorkSpace 大约需要 5 分钟。删除期间，WorkSpace 的状态设置为正在终止。删除完成后，WorkSpace 将从控制台中消失。
5. (可选) 要删除您不再使用的任何自定义捆绑包和映像，请参阅 删除 WorkSpaces 个人版中的自定义捆绑包或映像。
6. (可选) 删除一个目录下的所有 WorkSpace 后，可删除该目录。有关更多信息，请参阅 删除 WorkSpaces 个人版目录。
7. (可选) 删除虚拟私有云(VPC) 中用于您的目录的所有资源后，可以删除 VPC 并释放用于 NAT 网关的弹性 IP 地址。有关更多信息，请参阅《Amazon VPC 用户指南》中的删除您的 VPC 和使用弹性 IP 地址。

使用 Amazon CLI 删除 WorkSpace

使用 terminate-workspaces 命令。

WorkSpaces 个人版的捆绑包和映像

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 可用的各种公有捆绑包的更多信息，请参阅 Amazon WorkSpaces 捆绑包。

如果您已启动 Windows 或 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。

WorkSpaces 支持多种不同的操作系统（OS）、流式传输协议和捆绑包。下表提供了有关每个操作系统支持的许可、流式传输协议和捆绑包的信息。

操作系统	许可证	流式传输协议	支持的捆绑包	生命周期策略/停用日期
Windows Server 2016	包含	DCV、PCo	Value、Standard、Performance、Power、PowerPro、Graphics（已停用）、GraphicsPro、Graphics.g4dn、GraphicsPro.g4dn	2027 年 1 月 12 日
Windows Server 2019	包含	DCV、PCo	Value、Standard、Performance、Power、PowerPro、Graphics（已停用）、GraphicsPro、Graphics.g4dn、GraphicsPro.g4dn	2029 年 1 月 9 日
Windows Server 2022	包含	DCV、PCo	Standard、Performance、Power、PowerPro、GeneralPurpose.4xlarge、GeneralPurpose.8xlarge、Graphics（已停用）、GraphicsPro、Graphics.g4dn、GraphicsPro.g4dn	2031 年 10 月 14 日
Windows 10	自带许可（BYOL）	DCV、PCo	Value、Standard、Performance、Power、PowerPro、Graphics（已停用）、GraphicsPro、Graphics.g4dn、GraphicsPro.g4dn	支持中
Windows 11	自带许可（BYOL）	DCV	Standard、Performance、Power、PowerPro、GeneralPurpose.4xlarge、GeneralPurpose.8xlarge	支持中
Amazon Linux 2	包含	DCV、PCo	Value、Standard、Performance、Power、PowerPro	支持中
Ubuntu 22.04 LTS	包含	DCV	Value、Standard、Performance、Power、PowerPro、Graphics.g4dn、GraphicsPro.g4dn	2032 年 6 月

操作系统	许可证	流式传输协议	支持的捆绑包	生命周期策略/停用日期
Rocky Linux 8	包含	DCV	Value、Standard、Performance、Power、PowerPro	2029 年 5 月 31 日
Red Hat Enterprise Linux 8	包含	DCV	Value、Standard、Performance、Power、PowerPro	2029 年 5 月 31 日

> **Note**
>
> - 不再受供应商支持的操作系统版本不能保证正常工作，也不受 Amazon Support 支持。
> - 对于在 Windows 操作系统上运行的 WorkSpaces，Graphics 捆绑包仅支持 PCoIP 流式传输协议。

目录

- WorkSpaces 个人版捆绑包选项
- 为 WorkSpaces 个人版创建自定义 WorkSpaces 图片和捆绑包
- 更新 WorkSpaces 个人版的自定义捆绑包
- 在 “个 WorkSpaces 人” 中复制自定义镜像
- 共享或取消共享自定义 WorkSpaces 个人版映像
- 删除 WorkSpaces 个人版中的自定义捆绑包或映像

WorkSpaces 个人版捆绑包选项

在选择捆绑包之前，请确保要选择的捆绑包与您的 WorkSpaces “协议”、“操作系统”、“网络” 和 “计算类型” 兼容。有关协议的更多信息，请参阅 Amazon 协议 WorkSpaces。有关网络的更多信息，请参阅 Amazon WorkSpaces 客户网络要求。

> **Note**
>
> - 我们建议 PCo IP 的最大网络延迟不要超过 250 毫秒 WorkSpaces。为了获得最佳的 PCo IP WorkSpaces 用户体验，我们建议将网络延迟保持在 100 毫秒以下。当往返时间 (RTT) 超过 375 毫秒时， WorkSpaces 客户端连接将关闭。为了获得最佳 DCV 用户体验，建议将 RTT 保持在 250 毫秒以下。如果 RTT 介于 250 毫秒和 400 毫秒之间，则用户可以访问 WorkSpace，但性能将显著降低。
> - 建议您通过运行和使用复制用户日常任务的应用程序，在测试环境中测试您要选择的捆绑包的性能。
> - BYOP（自带协议）捆绑包适用于酷睿。 WorkSpaces Ama WorkSpaces zon 提供的 BYOP 捆绑包未安装 WorkSpaces 提供的流媒体协议。您将无法使用 WorkSpaces 客户端或网关进行连接。要了解 Amazon WorkSpaces Core 的分担责任模式，请参阅 A mazon WorkSpaces Core 技术合作伙伴集成指南。有关更多信息，请参阅 Amazon WorkSpaces Core。

> **Important**
>
> - GraphicsPro 捆绑包将 end-of-life于 2025 年 10 月 31 日到货。我们建议您在 2025 年 10 月 31 日之前 GraphicsPro WorkSpaces 将您的捆绑包迁移到支持的捆绑包。有关更多信息，请参阅 以 WorkSpaces 个人 WorkSpace 方式迁移。
> - 2023 年 11 月 30 日之后，不再支持 Graphics 捆绑包。我们建议切换到 Graphics.g4dn 捆绑包来使用 Graphics.g4dn 捆绑包。 WorkSpaces
> - 亚太地区（孟买）地区目前不提供显卡和 GraphicsPro 捆绑包。
> - 另外，2025 年 10 月 14 日之后，将不再支持采用 Office 2016 或 Office 2019 的应用程序捆绑包。我们建议将你的 WorkSpaces 捆绑包与这些 Office 版本一起迁移到使用 Office 2021 或 Office 2024。有关更多信息，请参阅 “在 WorkSpaces 个人版中管理应用程序”。

以下是 WorkSpaces 提供的捆绑包。有关中捆绑包的信息 WorkSpaces，请参阅 Amazon WorkSpaces 捆绑包。

经济捆绑包

此捆绑包非常适合以下用途：

- 基本的文本编辑和数据输入
- 使用量较少的 Web 浏览
- 即时消息发送

不建议将此捆绑包用于文字处理、音频和视频会议、屏幕共享、软件开发工具、商业智能应用程序和图形应用程序。

标准捆绑包

此捆绑包非常适合以下用途：

- 基本的文本编辑和数据输入
- Web 浏览
- 即时消息发送
- 电子邮件

不建议将此捆绑包用于音频和视频会议、屏幕共享、文字处理、软件开发工具、商业智能应用程序和图形应用程序。

性能捆绑包

此捆绑包非常适合以下用途：

- Web 浏览
- 文字处理
- 即时消息发送
- 电子邮件
- 电子表格
- 音频处理
- 课件

不建议将此捆绑包用于视频会议、屏幕共享、软件开发工具、商业智能应用程序和图形应用程序。

节能捆绑包

此捆绑包非常适合以下用途：

- Web 浏览
- 文字处理
- 电子邮件
- 即时消息发送
- 电子表格
- 音频处理
- 软件开发（集成式开发环境 (IDE)）
- 中级数据处理入门
- 音频和视频会议

不建议将此捆绑包用于屏幕共享、软件开发工具、商业智能应用程序和图形应用程序。

PowerPro 捆绑包

此捆绑包非常适合以下用途：

- Web 浏览
- 文字处理
- 电子邮件
- 即时消息发送
- 电子表格
- 音频处理
- 软件开发（集成式开发环境 (IDE)）
- 数据仓库
- 商业智能应用程序
- 音频和视频会议

不建议将此捆绑包用于机器学习模型训练和图形应用程序。

通用捆绑包

这些捆绑包，包括 GeneralPurpose .4xlarge 和 GeneralPurpose .8xlarge，非常适合以下内容：

- Web 浏览

- 文字处理
- 电子邮件
- 即时消息发送
- 电子表格
- 音频处理
- 软件开发（集成式开发环境 (IDE)）
- 数据仓库
- 商业智能应用程序
- 音频和视频会议
- 批处理
- 基于 CPU 的 ML（机器学习）模型训练

不建议将此捆绑包用于复杂模型的 3D 渲染、照片级逼真设计、游戏流或 ML 模型训练。

GraphicsPro 捆绑包

该套装为您提供了基本的显卡性能，以及高水平的CPU性能和内存 WorkSpaces。它非常适合以下用途：

- Web 浏览
- 文字处理
- 电子邮件
- 即时消息发送
- 电子表格
- 音频会议
- 软件开发（集成式开发环境 (IDE)）
- 数据仓库
- 商业智能应用程序
- 图形设计
- 图像处理

不建议将此捆绑包用于音频和视频会议、3D 渲染和照片级逼真设计。

Graphics.g4dn 捆绑包

该套装为您提供了高水平的显卡性能以及中等水平的 CPU 性能 WorkSpaces 和内存，非常适合以下内容：

- Web 浏览
- 文字处理
- 电子邮件
- 电子表格
- 即时消息发送
- 音频会议
- 软件开发（集成式开发环境 (IDE)）
- 中级数据处理入门
- 数据仓库
- 商业智能应用程序
- 图形设计
- CAD/CAM (computer-aided design/computer-辅助制造）

不建议将此捆绑包用于音频和视频会议、3D 渲染、照片级逼真设计和机器学习模型训练。

GraphicsPro.g4dn 捆绑包

该套装为您提供了高水平的显卡性能、CPU 性能和内存，非常适合以下内容： WorkSpaces

- Web 浏览
- 文字处理
- 电子邮件
- 电子表格
- 即时消息发送
- 音频会议
- 软件开发（集成式开发环境 (IDE)）
- 中级数据处理入门
- 数据仓库

- 商业智能应用程序
- 图形设计
- CAD/CAM (computer-aided design/computer-辅助制造)
- 视频转码
- 3D 渲染
- 照片级逼真设计
- 游戏流
- ML（机器学习）模型训练和 ML 推理

不建议将此捆绑包用于音频和视频会议。

为 WorkSpaces 个人版创建自定义 WorkSpaces 图片和捆绑包

如果你已经启动了 Windows 或 Linux WorkSpace 并对其进行了自定义，则可以从中创建自定义映像和自定义捆绑包。 WorkSpace

自定义映像仅包含的操作系统、软件和设置 WorkSpace。自定义捆绑包是该自定义映像和 WorkSpace 可以从中启动的硬件的组合。

> **Note**
>
> 确保在删除捆绑包后至少等待 2 小时，然后再创建相同名称的新捆绑包。

创建自定义映像后，您可以构建一个自定义服务包，该服务包将自定义映像与您选择的基础计算和存储配置相结合。然后，您可以在启动新包时指定此自定义捆绑包， WorkSpaces 以确保新包 WorkSpaces 具有相同的一致配置（硬件和软件）。

通过为每个服务包选择不同的计算和存储选项，您可以使用相同的自定义映像来创建各种自定义服务包。

> **Important**
>
> - 如果你打算从 Windows 10 创建映像 WorkSpace，请注意，已从 Windows 10 的一个版本升级到较新版本的 Windows 10（Windows 升级）的 Windows 10 系统不支持创建映像。feature/version 但是， WorkSpaces 映像创建过程支持 Windows 累积更新或安全更新。

- 2020 年 1 月 14 日之后，无法从公有 Windows 7 捆绑包创建映像。你可能需要考虑将你的 Windows 7 迁移 WorkSpaces 到 Windows 10。有关更多信息，请参阅 以 WorkSpaces 个人 WorkSpace 方式迁移。
- 2023 年 11 月 30 日之后，不再支持 Graphics 捆绑包。我们建议将你迁移 WorkSpaces 到 Graphics.g4dn 捆绑包。有关更多信息，请参阅 以 WorkSpaces 个人 WorkSpace 方式迁移。
- GraphicsPro 捆绑包将 end-of-life于 2025 年 10 月 31 日到货。我们建议您在 2025 年 10 月 31 日之前迁移 GraphicsPro WorkSpaces 到支持的捆绑包。有关更多信息，请参阅 the section called “迁移 WorkSpace”。
- 亚太地区（孟买）地区目前不提供显卡和 GraphicsPro 捆绑包。
- 自定义捆绑包存储量不能小于映像存储量。
- 另外，2025 年 10 月 14 日之后，将不再支持采用 Office 2016 或 Office 2019 的应用程序捆绑包。我们建议将你的 WorkSpaces 捆绑包与这些 Office 版本一起迁移到使用 Office 2021。有关更多信息，请参阅 “在 WorkSpaces 个人版中管理应用程序”。

自定义捆绑包的成本与创建这些捆绑包的公有捆绑包的成本相同。有关定价的更多信息，请参阅 Amazon WorkSpaces 定价。

内容

- 创建 Windows 自定义映像的要求
- 创建 Linux 自定义映像的要求
- 最佳实践
- （可选）步骤 1：为映像指定自定义计算机名称格式
- 步骤 2：运行映像检查程序
- 步骤 3：创建自定义映像和自定义捆绑包
- Windows WorkSpaces 自定义镜像中包含的内容
- Linux WorkSpace 自定义镜像中包含的内容

创建 Windows 自定义映像的要求

> **Note**
>
> Windows 目前将 1 GB 定义为 1,073,741,824 字节。客户需要确保 C 盘上有超过 12,884,901,888 字节（或 12 GiB）的可用空间，并且用户配置文件小于 10,737,418,240 字节（或 10 GiB）才能创建 a 的映像。 WorkSpace

- 的状态 WorkSpace 必须为 “可用”，其修改状态必须为 “无”。
- WorkSpaces 图像上的所有应用程序和用户配置文件都必须与 Microsoft Sysprep 兼容。
- 所有要包括在映像中的应用程序都必须安装在 C 驱动器上。
- 对于 Windows 7 WorkSpaces，其总大小（文件和数据）必须小于 10 GB。
- 对于 Windows 7 WorkSpaces，C驱动器必须有至少 12 GB 的可用空间。
- 在上运行的所有应用程序服务都 WorkSpace 必须使用本地系统帐户而不是域用户凭据。例如，不能有使用域用户凭证运行的 Microsoft SQL Server Express 安装。
- WorkSpace 不得加密。目前不支持通过加密 WorkSpace 设备创建映像。
- 映像中要求具有以下组件。如果没有这些组件 WorkSpaces ，您从映像中启动的将无法正常运行。有关更多信息，请参阅 the section called “必需配置和服务组件”。
  - Windows PowerShell 版本 3.0 或更高版本
  - 远程桌面服务
  - Amazon光伏驱动器
  - Windows 远程管理 (WinRM)
  - Teradici PCo IP 代理和驱动程序
  - STXHD 代理和驱动程序
  - Amazon和 WorkSpaces 证书
  - Skylight 代理

创建 Linux 自定义映像的要求

- 的状态 WorkSpace 必须为 “可用”，其修改状态必须为 “无”。
- 所有将包括在映像中的应用程序都必须安装在用户卷（/home 目录）之外。
- 根卷 (/) 的使用率必须低于 97%。

- WorkSpace 不得加密。目前不支持通过加密 WorkSpace 设备创建映像。
- 映像中要求具有以下组件。如果没有这些组件 WorkSpaces ，你从镜像中启动的将无法正常运行：
  - Cloud-init
  - Teradici PCo IP 或 DCV 代理和驱动程序
  - Skylight 代理

最佳实践

在从创建图像之前 WorkSpace，请执行以下操作：

- 使用未连接到您的生产环境的单独 VPC。
- 在私有子网 WorkSpace 中部署，并使用 NAT 实例处理出站流量。
- 使用小的 Simple AD 目录。
- 使用源的最小卷大小 WorkSpace，然后在创建自定义捆绑包时根据需要调整音量大小。
- 在上安装所有操作系统更新（Windows 功能/版本更新除外）和所有应用程序更新。 WorkSpace有关更多信息，请参阅本主题开始处的重要提示。
- 从中删除不应 WorkSpace 包含在捆绑包中的缓存数据（例如，浏览器历史记录、缓存文件和浏览器 Cookie）。
- 从中删除不应 WorkSpace 包含在捆绑包中的配置设置（例如，电子邮件配置文件）。
- 使用 DHCP 切换到动态 IP 地址设置。
- 确保您没有超过某个地区允许的 WorkSpace 图片配额。默认情况下，每个区域允许您使用 40 WorkSpace 张图片。如果您已达到此配额，创建映像的新尝试将失败。要请求增加配额，请使用 WorkSpaces 限制表单。
- 确保您不是在尝试使用加密镜像创建镜像 WorkSpace。目前不支持通过加密 WorkSpace 设备创建映像。
- 如果您正在上运行任何防病毒软件 WorkSpace，请在尝试创建映像时将其禁用。
- 如果您启用了防火墙 WorkSpace，请确保它没有阻塞任何必要的端口。有关更多信息，请参阅 WorkSpaces 个人的 IP 地址和端口要求。
- 对于 Windows WorkSpaces，在创建映像之前不要配置任何组策略对象 (GPOs)。
- 对于 Windows WorkSpaces，在创建映像之前不要自定义默认用户配置文件 (`C:\Users\Default`)。我们建议通过对用户个人资料进行任何自定义 GPOs，并在创建图像后应用这些设置。 GPOs 可以很容易地修改或回滚，因此与对默认用户配置文件所做的自定义相比，不容易出错。

- 对于 Linux WorkSpaces，另请参阅 “为亚马逊 WorkSpaces 提供 Linux 映像做好准备的最佳实践” 白皮书。
- 如果您想在启用了 DCV 的 Linux WorkSpaces 上使用智能卡，在 “个人” 中 WorkSpaces 使用智能卡进行身份验证请参阅，了解在创建映像 WorkSpace 之前必须对 Linux 进行的自定义。
- 请务必更新网络依赖驱动程序 NVMe，例如 ENA 和 PV 驱动程序 WorkSpaces。您应该至少每 6 个月更新一次。有关更多信息，请参阅安装或升级弹性网络适配器（ENA）驱动程序、Windows 实例的 Amazon NVMe 驱动程序以及升级 Windows 实例上的 PV 驱动程序。
- 确保定期将 EC2 Config、 EC2 Launc EC2 h 和 Launch V2 代理更新到最新版本。您应该至少每 6 个月更新一次。有关更多信息，请参阅更新 EC2 Config 并 EC2启动。

（可选）步骤 1：为映像指定自定义计算机名称格式

对于从您的自定义或自带许可证 (BYOL) 映像 WorkSpaces 启动的，您可以为计算机名称格式指定自定义前缀，而不是使用默认的计算机名称格式。要指定自定义前缀，请按照与您的映像类型相对应的步骤进行操作。

为自定义映像指定自定义计算机名称格式

> **Note**
>
> 默认情况下，Windows 10 的计算机名称格式为，Windows 11 `DESKTOP-XXXXX` WorkSpaces 的计算机名称格式 WorkSpaces 为`WORKSPA-XXXXX`。

1. 在你 WorkSpace 用来创建自定义图像的上，`C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xml`在记事本或其他文本编辑器中打开。有关使用 `Unattend.xml` 文件的更多信息，请参阅 Microsoft 文档中的应答文件 (unattend.xml)。

   > **Note**
   >
   > 要通过您的 Windows 文件资源管理器访问 C: 驱动器 WorkSpace，请在地址栏**`C:\`**中输入。

2. 在 `<settings pass="specialize">` 部分，确保将 `<ComputerName>` 设置为星号 (*)。如果将 `<ComputerName>` 设置为任何其他值，则您的自定义计算机名称设置将被忽略。有关该`<ComputerName>`设置的更多信息，请参阅 Microsoft 文档 ComputerName中的。

3. 在 `<settings pass="specialize">` 部分，将 `<RegisteredOrganization>` 和 `<RegisteredOwner>` 设置为您的首选值。

   在 Sysprep 期间，您为 `<RegisteredOwner>` 和 `<RegisteredOrganization>` 指定的值将连接在一起，组合字符串的前 7 个字符用于创建计算机名称。例如，如果您为 `<RegisteredOrganization>` 指定 **`Amazon.com`**，为 `<RegisteredOwner>` 指定 **`EC2`**。对于基于 Windows 10 的映像， WorkSpaces 使用自定义捆绑包的计算机名称将以 EC2 AMAZ-开头。*xxxxxxx*对于基于 Windows 11 的映像， WorkSpaces 使用自定义软件包的计算机名称将以 WORKSPA-开头。*xxxxxxx*

   > **Note**
   >
   > - Sysprep 会忽略 `<settings pass="oobeSystem">` 部分中的 `<RegisteredOrganization>` 和 `<RegisteredOwner>` 值。
   > - **<** RegisteredOrganization **>** 和 **<** RegisteredOwner **>** 都是必填值。

4. 保存对 `Unattend.xml` 文件的更改。

为 BYOL 映像指定自定义计算机名称格式

1. 如果您使用的是 Windows 10，请在记事本或其他文本编辑器中打开 `C:\Program Files\Amazon\Ec2ConfigService\Sysprep2008.xml`。如果您使用的是 Windows 11，请打开 `C:\ProgramData\Amazon\EC2Launch\sysprep\OOBE_unattend.xml`。
2. 在 `<settings pass="specialize">` 部分，如果您使用的是 Windows 10，请取消注释 `<ComputerName>*</ComputerName>`。如果您使用的是 Windows 11，则无需取消注释此部分。确保将 `<ComputerName>` 设置为星号（`*`）。如果将 `<ComputerName>` 设置为任何其他值，则您的自定义计算机名称设置将被忽略。有关该`<ComputerName>`设置的更多信息，请参阅 Microsoft 文档 ComputerName中的。
3. 在 `<settings pass="specialize">` 部分，将显示适用于 Windows 10 和 Windows 11 的 `<RegisteredOrganization>` 字段。默认情况下，`<RegisteredOwner>` 标签仅会出现在 Windows 10 中。如果您使用的是 Windows 11，则需要添加此标签。将 `<RegisteredOrganization>` 和 `<RegisteredOwner>` 设置为您的首选值。

   在 Sysprep 期间，您为 `<RegisteredOwner>` 和 `<RegisteredOrganization>` 指定的值将连接在一起，组合字符串的前 7 个字符用于创建计算机名称。例如，如果您为 for

`<RegisteredOrganization>` 和 **`Amazon.com EC2`** for 指定`<RegisteredOwner>`，则根据您的自定义捆绑包 WorkSpaces 创建的计算机名称将以 EC2 AMAZ-*xxxxxxx* 开头。

> **Note**
>
> - Sysprep 会忽略 `<settings pass="oobeSystem">` 部分中的 `<RegisteredOrganization>` 和 `<RegisteredOwner>` 值。
> - < RegisteredOrganization > 和 < RegisteredOwner > 都是必填值。

4. 如果您使用的是 Windows 10，请将您的更改保存到 `Sysprep2008.xml` 文件。如果您使用的是 Windows 11，请将您的更改保存到 `OOBE_unattend.xml`

步骤 2：运行映像检查程序

> **Note**
>
> 图像检查器仅适用于 Window WorkSpaces s。如果您要从 Linux 中创建映像 WorkSpace，请跳至步骤 3：创建自定义映像和自定义捆绑包。

要确认您的 Windows 是否 WorkSpace 满足创建映像的要求，我们建议您运行图像检查器。Image Checker 会对要 WorkSpace 用来创建图像的进行一系列测试，并就如何解决发现的任何问题提供指导。

> **Important**
>
> - WorkSpace 必须通过 Image Checker 运行的所有测试，然后才能使用它来创建图像。
> - 在运行映像检查器之前，请验证您的 WorkSpace设备上是否安装了最新的 Windows 安全和累积更新。

要获取映像检查程序，请执行以下操作之一：

- 重启你的 WorkSpace. 系统会在重新启动期间自动下载映像检查程序并将其安装在 `C:\Program Files\Amazon\ImageChecker.exe` 中。

- 从 zip 下载亚马逊 WorkSpaces 图片检查器并解压缩文件。 `ImageChecker.exe`将此文件复制到 `C:\Program Files\Amazon\`。

运行映像检查程序

1. 打开 `C:\Program Files\Amazon\ImageChecker.exe` 文件。
2. 在 “Amazon WorkSpaces 图像检查器” 对话框中，选择 “运行”。
3. 每个测试完成后，您都可以查看测试的状态。

   对于状态为 FAILED (失败) 的任何测试，请选择 Info (信息) 以显示有关如何解决导致失败的问题的信息。有关如何解决这些问题的更多信息，请参阅解决映像检查程序检测到的问题的提示。

   如果任何测试显示了状态 WARNING (警告)，请选择 Fix All Warnings (修复所有警告) 按钮。

   该工具在映像检查程序所在的同一目录中生成输出日志文件。默认情况下，此文件位于 `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log` 中。

   > **Tip**
   > 请勿删除此日志文件。如果出现问题，此日志文件可能有助于进行故障排除。

4. 如果适用，请解决任何导致测试失败和警告的问题，然后重复运行图像检查器的过程，直到 WorkSpace通过所有测试。在创建映像之前，必须先解决所有失败和警告。
5. WorkSpace 通过所有测试后，您会看到一条验证成功消息。您现在已准备好创建自定义服务包。

解决映像检查程序检测到的问题的提示

除了咨询以下提示以解决映像检查程序检测到的问题之外，请务必查看映像检查程序日志文件：`C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log`。

PowerShell 必须安装 3.0 或更高版本

安装最新版本的微软 Windows PowerShell。

> **Important**
> 的 PowerShell 执行策略 WorkSpace 必须设置为允许RemoteSigned脚本。要检查执行策略，请运行 Get-ExecutionPolicy PowerShell 命令。如果执行策略未设置为 “不受限制” 或

RemoteSigned，请运行 Set-ExecutionPolicy — ExecutionPolicy RemoteSigned 命令来更改执行策略的值。该RemoteSigned设置允许在 Amazon 上执行脚本 WorkSpaces，这是创建映像所必需的。

只可存在 C 和 D 驱动器

用于映像的 a WorkSpace 上只能存在C和D驱动器。删除所有其他驱动器，包括虚拟驱动器。

无法检测到由于 Windows 更新而挂起的重启

- 在重启 Windows 以完成安装安全更新或累积更新之前，无法运行创建映像过程。重启 Windows 以应用这些更新，并确保不需要安装任何其他挂起的 Windows 安全更新或累积更新。
- 已从一个版本的 Windows 10 升级到较新版本的 Windows 10（Windows 升 feature/version 级）的 Windows 10 系统不支持创建映像。但是， WorkSpaces 映像创建过程支持 Windows 累积更新或安全更新。

Sysprep 文件必须存在且不能为空

如果您的 Sysprep 文件有问题，请联系Amazon Web Services 支持中心修复您的 Confi EC2 g 或 EC2 Launch。

用户配置文件大小必须小于 10 GB

对于 Windows 7 WorkSpaces，用户配置文件 (`D:\Users\`*`username`*) 的总容量必须小于 10 GB。根据需要删除文件以减小用户配置文件的大小。

驱动器 C 必须有足够的可用空间

对于 Windows 7 WorkSpaces，驱动器上必须有至少 12 GB 的可用空间C。根据需要删除文件以释放 C 驱动器上的空间。对于 Windows 10 WorkSpaces，如果您收到一条FAILED消息并且磁盘空间超过 2GB，请忽略。

无法在域账户下运行任何服务

要运行 “创建映像” 进程， WorkSpace 不能在域帐户下运行任何服务。所有服务必须在本地账户下运行。

在本地账户下运行服务

1. 打开 `C:\Program Files\Amazon\ImageChecker_yyyyMMddhhmmss.log` 并查找在域账户下运行的服务列表。
2. 在 Windows 搜索框中，输入 **`services.msc`** 以打开 Windows 服务管理器。
3. 在 Log On As (登录身份) 下，查找在域账户下运行的服务。（以本地系统、本地服务或网络服务身份运行的服务不会干扰映像创建。）
4. 选择在域账户下运行的服务，然后选择操作)、属性。
5. 打开 Log On (登录) 选项卡。在 Log on as (登录身份)下，选择 Local System account (本地系统账户)。
6. 选择确定。

WorkSpace 必须配置为使用 DHCP

必须将上的所有网络适配器配置 WorkSpace 为使用 DHCP 而不是静态 IP 地址。

将所有网络适配器设置为使用 DHCP

1. 在 Windows 搜索框中，输入 **`control panel`** 以打开控制面板。
2. 选择网络和 Internet。
3. 选择网络和共享中心。
4. 选择更改适配器设置，然后选择适配器。
5. 选择更改此连接的设置。
6. 在 “网络” 选项卡上，选择 “互联网协议版本 4 (TCP/IPv4)”，然后选择 “属性”。
7. 在 “互联网协议版本 4 (TCP/IPv4) 属性” 对话框中，选择 “自动获取 IP 地址”。
8. 选择确定。
9. 对上的所有网络适配器重复此过程 WorkSpace。

必须启用远程桌面服务

创建映像过程需要启用远程桌面服务。

启用远程桌面服务

1. 在 Windows 搜索框中，输入 **`services.msc`** 以打开 Windows 服务管理器。

2. 在名称列中，找到远程桌面服务。
3. 选择远程桌面服务，然后选择操作、属性。
4. 在常规选项卡上，对于启动类型，选择手动或自动。
5. 选择确定。

用户配置文件必须存在

你 WorkSpace 用来创建图像的必须有用户个人资料 (`D:\Users\`*`username`*)。如果此测试失败，请联系 Amazon Web Services 支持 中心寻求帮助。

必须正确配置环境变量路径

本地计算机的环境变量路径缺少 System32 和 Windows PowerShell 的条目。要创建映像，需要这些条目。

配置环境变量路径

1. 在 Windows 搜索框中，输入 **`environment variables`**，然后选择编辑系统环境变量。
2. 在系统属性对话框中，打开高级选项卡，然后选择环境变量。
3. 在环境变量对话框的系统变量下，选择路径条目，然后选择编辑。
4. 选择新建，然后添加以下路径：

   ```
   C:\Windows\System32
   ```

5. 再次选择新建，然后添加以下路径：

   ```
   C:\Windows\System32\WindowsPowerShell\v1.0\
   ```

6. 选择确定。
7. 重新启动 WorkSpace。

> **Tip**
>
> 项目在环境变量路径中显示的顺序至关重要。要确定正确的顺序，您可能需要将您的环境变量路径 WorkSpace 与来自新创建 WorkSpace 或新 Windows 实例的环境变量路径进行比较。

必须启用 Windows 模块安装程序

创建映像过程要求启用 Windows 模块安装程序服务。

启用 Windows 模块安装程序服务

1. 在 Windows 搜索框中，输入 **`services.msc`** 以打开 Windows 服务管理器。
2. 在名称列中，找到 Windows 模块安装程序。
3. 选择 Windows 模块安装程序，然后选择操作、属性。
4. 在常规选项卡上，对于启动类型，选择手动或自动。
5. 选择确定。

必须禁用 Amazon SSM 代理

创建映像过程要求禁用 Amazon SSM 代理服务。

禁用 Amazon SSM 代理服务

1. 在 Windows 搜索框中，输入 **`services.msc`** 以打开 Windows 服务管理器。
2. 在名称列中，找到 Amazon SSM 代理。
3. 选择 Amazon SSM 代理，然后选择操作、属性。
4. 在常规选项卡上，对于启动类型，选择已禁用。
5. 选择确定。

SSL3 并且必须启用 TLS 版本 1.2

要针对 Windows SSL/TLS 进行配置，请参阅微软 Windows 文档中的如何启用 TLS 1.2。

上只能存在一个用户配置文件 WorkSpace

上只能有一个用于创建图像 WorkSpace 的 WorkSpaces 用户个人资料 (`D:\Users\`*`username`*)。删除所有不属于目标用户的用户个人资料 WorkSpace。

要使图像创建起作用，上面 WorkSpace 只能有三个用户配置文件：

- WorkSpace(`D:\Users\`*`username`*) 的目标用户的用户个人资料

- 默认用户配置文件（也称为默认配置文件）
- 管理员用户配置文件

如果有其他用户配置文件，则可以通过 Windows 控制面板中的高级系统属性将其删除。

删除用户配置文件

1. 要访问高级系统属性，请执行以下操作之一：
   - 按 Windows 键 + 暂停中断，然后在控制面板 > 系统和安全 > 系统对话框的左侧窗格中，选择高级系统设置。
   - 在 Windows 搜索框中，输入 **`control panel`**。在“控制面板”中，选择系统和安全，然后选择“系统”，随后在控制面板 > 系统和安全 > 系统对话框的左侧窗格中，选择高级系统设置。
2. 在系统属性对话框的高级选项卡上，选择用户配置文件下的设置。
3. 如果除了管理员配置文件、默认配置文件和目标 WorkSpaces用户的配置文件之外还列出了任何配置文件，请选择该其他配置文件并选择删除。
4. 当询问您是否要删除此配置文件时，请选择是。
5. 如有必要，请重复步骤 3 和 4，删除不属于该的任何其他配置文件 WorkSpace。
6. 选择确定两次并关闭控制面板。
7. 重新启动 WorkSpace。

没有 AppX 程序包可以处于暂存状态

一个或多个 AppX 程序包处于暂存状态。这可能导致在映像创建过程中出现 Sysprep 错误。

删除所有暂存的 AppX 程序包

1. 在 Windows 搜索框中，输入 **`powershell`**。选择以管理员身份运行。
2. 当询问“你要允许此应用对你的设备进行更改吗?”时，选择是。
3. 在 Windows PowerShell 窗口中，输入以下命令以列出所有暂存的 AppX 软件包，然后在每个命令后按 Enter。

```
$workSpaceUserName = $env:username
```

```
$allAppxPackages = Get-AppxPackage -AllUsers
```

```
$packages = $allAppxPackages |    Where-Object { `
                                ($_.PackageUserInformation -like "*S-1-5-18*" -
and !($_.PackageUserInformation -like "*$workSpaceUserName*")) -and `
                                ($_.PackageUserInformation -like "*Staged*" -or
 $_.PackageUserInformation -like "*Installed*")) -or `
                                ((!($_.PackageUserInformation -like "*S-1-5-18*") -
and $_.PackageUserInformation -like "*$workSpaceUserName*") -and `
                                $_.PackageUserInformation -like "*Staged*")
                                }
```

4. 输入以下命令以删除所有暂存的 AppX 程序包，然后按 Enter 键。

```
$packages | Remove-AppxPackage -ErrorAction SilentlyContinue
```

5. 再次运行映像检查程序。如果此测试仍然失败，请输入以下命令以删除所有 AppX 程序包，然后在每个程序包之后按 Enter 键。

```
Get-AppxProvisionedPackage -Online | Remove-AppxProvisionedPackage -Online -
ErrorAction SilentlyContinue
```

```
Get-AppxPackage -AllUsers | Remove-AppxPackage -ErrorAction SilentlyContinue
```

Windows 必须尚未从以前的版本升级

已从一个版本的 Windows 10 升级到较新版本的 Windows 10（Windows 升 feature/version 级）的 Windows 系统不支持创建映像。

要创建映像 WorkSpace ，请使用尚未进行 Windows feature/version 升级的。

Windows 重置计数不得为 0

重置功能允许您延长 Windows 试用版的激活期。创建映像过程要求重置计数为 0 以外的值。

检查 Windows 重置计数

1. 在 Windows 开始菜单上，选择 Windows 系统，然后选择命令提示符。
2. 在命令提示符窗口中，键入以下命令，然后按 Enter。

```
cscript C:\Windows\System32\slmgr.vbs /dlv
```

要将重置计数重置为非 0 的值，请参阅 Microsoft Windows 文档中的 Sysprep（通用化）Windows 安装。

其他故障排查提示

如果您 WorkSpace 通过了 Image Checker 运行的所有测试，但仍然无法从中创建图像 WorkSpace，请检查是否存在以下问题：

- 确保 WorkSpace 未将分配给域访客群组中的用户。要检查是否有任何域帐户，请运行以下 PowerShell命令。

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

- WorkSpaces 仅适用于 Windows 7：如果在创建映像期间复制用户配置文件时出现问题，请检查是否存在以下问题：
  - 长的配置文件路径可能会导致映像创建错误。请确保用户配置文件中所有文件夹的路径少于 261 个字符。
  - 确保将配置文件的文件夹的完全权限授予系统和所有应用程序包。
  - 如果用户配置文件中的任何文件被进程锁定或在映像创建过程中正在使用，则复制配置文件时可能会失败。
- 某些组策略对象 (GPOs) 会在 Config 服务或 La EC2 unch 脚本在 Windows 实例 EC2配置期间请求 RDP 证书指纹时限制访问该指纹。在尝试创建映像之前，请将其移 WorkSpace 至继承受阻且未 GPOs应用的新组织单位 (OU)。
- 请确保 Windows 远程管理 (WinRM) 服务配置为自动启动。执行以下操作：
  1. 在 Windows 搜索框中，输入 **`services.msc`** 以打开 Windows 服务管理器。
  2. 在名称列中，找到 Windows 远程管理(WS-Management)。
  3. 选择 Windows 远程管理(WS-Management)，然后选择操作、属性。
  4. 在常规选项卡上，对于启动类型，选择自动。
  5. 选择确定。

步骤 3：创建自定义映像和自定义捆绑包

验证 WorkSpace 图片后，您可以继续创建自定义图像和自定义捆绑包。

创建自定义映像和自定义服务包

1. 如果您仍处于连接状态 WorkSpace，请在 WorkSpaces 客户端应用程序中选择 Amazon WorkSpaces 并断开连接，从而断开连接。
2. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
3. 在导航窗格中，请选择 WorkSpaces。
4. 选择打开 WorkSpace 其详细信息页面，然后选择创建图像。如果的状态为 “ WorkSpace 已停止”，则必须先启动它（选择 “操作”，“开始” WorkSpaces），然后才能选择 “操作”、“创建映像”。

   > **Note**
   >
   > 要以编程方式创建图像，请使用 CreateWorkspaceImage API 操作。有关更多信息，请参阅 Amazon WorkSpaces API 参考 CreateWorkspaceImage中的。

5. 将显示一条消息，提示您在继续操作 WorkSpace之前重新启动（重新启动）。重新启动后，您的 Amazon WorkSpaces 软件会 WorkSpace 更新到最新版本。

   关闭消息并 WorkSpace 按照中的步骤进行操作，重新启动您的重启 WorkSpaces 个人版中的 WorkSpace。完成后，重复执行此过程中的Step 4，但这次在显示重启消息时，选择下一步。要创建映像，其状态 WorkSpace 必须为 “可用”，其修改状态必须为 “无”。
6. 输入映像名称和有助于您识别映像的描述，然后选择 创建映像。在创建映像时，的状态 WorkSpace 为已暂停且 WorkSpace 不可用。

   > **Note**
   >
   > 输入映像描述时，确保不要使用特殊字符“-”，否则会出现错误。

7. 在导航窗格中，选择映像。当状态 WorkSpace 变为 “可用”（这可能需要 45 分钟）时，映像就完成了。
8. 选择映像，然后选择操作、创建捆绑包。

   > **Note**
   >
   > 要以编程方式创建捆绑包，请使用 CreateWorkspaceBundle API 操作。有关更多信息，请参阅 Amazon WorkSpaces API 参考 CreateWorkspaceBundle中的。

9. 输入服务包的名称和描述，然后执行以下操作：

- 对于 Bundle 硬件类型，请选择 WorkSpaces 从此自定义捆绑包启动时要使用的硬件。
- 在存储设置中，选择根卷和用户卷大小的默认组合之一，或者选择自定义，然后为根卷大小和用户卷大小输入值（最多 2000 GB）。

  根卷（对于 Microsoft Windows，为 C 驱动器；对于 Linux，为 /）和用户卷（对于 Windows，为 D 驱动器；对于 Linux，为 /home）的默认可用大小组合如下所示：

  - 根：80 GB，用户：10 GB、50 GB 或 100 GB
  - 根：175 GB，用户：100 GB
  - 仅适用于 Graphics.g4dn、 GraphicsPro .g4dn、Graphics， GraphicsPro WorkSpaces 仅限：root：100 GB，用户：100 GB

  此外，您可以将根卷和用户卷分别扩展到最大 2000 GB。

  > **Note**
  >
  > 为确保数据得以保留，启动后不能减小根卷或用户卷的大小 WorkSpace。相反，请确保在启动时指定这些卷的最小大小 WorkSpace。
  >
  > - 您可以启动 “超值”、“标准”、“性能”、“Power”，或者 PowerPro WorkSpace 根卷的容量至少为 80 GB，用户卷的容量至少为 10 GB。
  > - 您可以启动 GeneralPurpose .4xlarge 或 GeneralPurpose .8x WorkSpace large，根卷的最小容量为 175GB，用户卷的容量至少为 100 GB。
  > - 你可以启动 Graphics.g4dn、 GraphicsPro .g4dn、Graphics，或者 GraphicsPro WorkSpace 根卷至少为 100 GB，用户卷至少为 100 GB。

10. 选择创建捆绑包。
11. 要确认您的捆绑包是否已创建，请选择捆绑包，并检查该捆绑包已列出。

Windows WorkSpaces 自定义镜像中包含的内容

当你从 Windows 7 或 10 创建映像时 WorkSpace，`C`驱动器的全部内容都包含在内。

对于 Windows 10 WorkSpaces，中的用户配置文件`D:\Users\`*`username`*不包含在自定义映像中。

对于 Windows 7 WorkSpaces，中`D:\Users\`*`username`*包含用户配置文件的所有内容，但以下内容除外：

- 联系人

- Downloads
- 音乐
- 图片
- 已保存的游戏
- 视频
- 播客
- 虚拟机
- 虚拟机
- 跟踪
- appdata\local\temp
- appdata\roaming\apple computer\mobilesync\
- appdata\roaming\apple computer\logs\
- appdata\roaming\apple computer\itunes\iphone software updates\
- appdata\roaming\macromedia\flash player\macromedia.com\support\flashplayer\sys\
- appdata\roaming\macromedia\flash player\#sharedobjects\
- appdata\roaming\adobe\flash player\assetcache\
- appdata\roaming\microsoft\windows\recent\
- appdata\roaming\microsoft\office\recent\
- appdata\roaming\microsoft office\live meeting
- appdata\roaming\microsoft shared\livemeeting shared\
- appdata\roaming\mozilla\firefox\crash reports\
- appdata\roaming\mcafee\common framework\
- appdata\local\microsoft\feeds cache
- appdata\local\microsoft\windows\temporary互联网files\
- appdata\local\microsoft\windows\history\
- appdata\local\microsoft\internet explorer\domstore\
- appdata\local\microsoft\internet explorer\imagestore\
- appdata\locallow\microsoft\internet explorer\iconcache\
- appdata\locallow\microsoft\internet explorer\domstore\

- appdata\locallow\microsoft\internet explorer\imagestore\
- appdata\local\microsoft\internet explorer\recovery\
- appdata\local\mozilla\firefox\profiles\

Linux WorkSpace 自定义镜像中包含的内容

当您从 Amazon Linux 上创建映像时 WorkSpace，用户卷 (/home) 的全部内容都将被删除。删除内容中包括根卷 (/) 的内容，但以下适用文件夹和密钥除外：

- /tmp
- /var/spool/mail
- /var/tmp
- /var/lib/dhcp
- /var/lib/cloud
- /var/cache
- /var/backups
- /etc/sudoers.d
- /etc/udev/rules.d/70-persistent-net.rules
- /etc/network/interfaces.d/50-cloud-init.cfg
- /var/log/amazon/ssm
- /var/log/pcoip-代理
- /var/log/skylight
- /var/lock/.skylight.domain-join.lock
- /var/lib/skylight/domain-加入状态
- /var/lib/skylight/configuration-数据
- /var/lib/skylight/config-data.json
- /home
- /etc/default/grub.d/zz-hibernation.cfg
- /etc/netplan/zz-workspaces-domain.yaml
- /etc/netplan/yy-workspaces-base.yaml

- /var/lib/AccountsService/users

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 WorkSpaces 个人版的自定义捆绑包

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

> **Important**
>
> 当您更新现有 WorkSpaces 所基于的捆绑包时，不会自动更新现有 WorkSpaces。要更新基于您已更新的捆绑包的现有 WorkSpaces，您必须重建 WorkSpaces 或删除并重新创建它们。

使用控制台更新捆绑包

1. 连接到基于该服务包的 WorkSpace 并进行所需的更改。例如，您可以应用最新的操作系统和应用程序修补程序并安装其他应用程序。

   或者，您可以创建一个新的 WorkSpace，它具有与用于创建该捆绑包的映像相同的基本软件包（Plus 或 Standard），然后进行更改。
2. 如果您仍连接到 WorkSpace，请通过在 WorkSpaces 客户端应用程序中选择 Amazon WorkSpaces 和断开连接，来断开连接。
3. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
4. 在导航窗格中，选择 WorkSpaces。
5. 选择 WorkSpace，然后选择 Actions、Create Image。如果 WorkSpace 的状态为 STOPPED，则必须先启动它（选择操作，启动 WorkSpaces），然后才能选择操作、创建映像。

6. 输入映像名称和描述，然后选择创建映像。在创建映像期间 WorkSpace 不可用。有关映像创建过程的详细信息，请参阅为 WorkSpaces 个人版创建自定义 WorkSpaces 图片和捆绑包。
7. 在导航窗格中，选择 Bundles。
8. 选择相应捆绑包以打开其详细信息页面，然后在源映像下选择编辑。
9. 在更新源映像页面上，选择所创建的映像并选择更新捆绑包。
10. 根据需要，更新任何基于该捆绑包的现有 WorkSpaces，方法是重建 WorkSpaces 或删除并重新创建它们。有关更多信息，请参阅 重建 WorkSpaces 个人版中的 WorkSpace。

以编程方式更新捆绑包

要以编程方式更新捆绑包，请使用 UpdateWorkspaceBundle API 操作。有关此操作的更多信息，请参阅《Amazon WorkSpaces API 参考》中的 UpdateWorkSpaceBundle。

在 “个 WorkSpaces 人” 中复制自定义镜像

您可以在区域内或跨Amazon区域复制自定义 WorkSpaces 映像。复制映像将导致创建完全相同的映像（具有其自己的唯一标识符）。

只要另一个区域已启用自带许可 (BYOL)，您就可以将 BYOL 映像复制到目标区域。确保为所有相关账户和区域启用 BYOL。

> **Note**
>
> 在中国（宁夏）区域，您只能复制同一区域内的映像。
> 在 Amazon GovCloud (US) Region s 中，要将图像复制到其他地区或从其他Amazon地区复制图像，请联系 Supp Amazon ort。
> 在选择加入区域中，要将图像复制到其他区域，请联系 Su Amazon pport。有关选择加入区域的更多信息，请参阅可用区域。

您也可以复制其他Amazon账户与您共享的图像。有关共享映像的更多信息，请参阅共享或取消共享自定义 WorkSpaces 个人版映像。

在区域内或跨区域复制映像不收取额外费用。但需遵循目标区域中的映像数量配额。有关 Amazon WorkSpaces 配额的更多信息，请参阅Amazon WorkSpaces 配额。

用于复制映像的 IAM 权限

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

以下示例策略允许用户将指定的映像复制到指定区域的指定账户中。

JSON

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

> **Important**
>
> 如果您正在创建 IAM 策略，用于为不拥有共享映像的账户复制此类映像，则无法在 ARN 中指定账户 ID。您必须改用账户 ID 的 `*`，如以下示例策略所示。
>
> JSON
>
> ```
> {
>  "Version":"2012-10-17",
>  "Statement": [
>  {
>  "Effect": "Allow",
>  "Action": [
>  "workspaces:DescribeWorkspaceImages",
>  "workspaces:CopyWorkspaceImage"
> ```

```
        ],
        "Resource": [
            "arn:aws:workspaces:us-east-1:*:workspaceimage/wsi-a1bcd2efg"
        ]
      }
    ]
}
```

只有当账户拥有要复制的映像时，您才能在 ARN 中指定该账户 ID。

有关使用 IAM 的更多信息，请参阅 的身份和访问管理 WorkSpaces。

批量复制映像

您可以使用控制台逐个复制映像。要批量复制图像，请使用 CopyWorkspaceImage API 操作或 Amazon Command Line Interface (Amazon CLI) 中的copy-workspace-image命令。有关更多信息，请参阅 CopyWorkspaceImageAmazon WorkSpaces API 参考或Amazon CLI命令参考 copy-workspace-image中的。

> **Important**
>
> 在复制共享镜像之前，请务必确认该镜像是从正确的Amazon账户共享的。要确定图片是否已共享并查看拥有图片的Amazon账户 ID，请使用DescribeWorkSpaceImages和DescribeWorkspaceImagePermissionsAPI 操作或中的describe-workspace-images和describe-workspace-image-permissions命令Amazon CLI。

使用控制台复制映像

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在导航窗格中，选择映像。
3. 选择映像，然后选择操作、复制映像。
4. 在 “选择目的地” 中，选择要将图像复制到的Amazon区域。
5. 对于副本名称，输入复制映像的新名称，对于描述，输入复制映像的描述。
6. （可选）在标签下，为复制的映像输入标签。有关更多信息，请参阅 在 WorkSpaces 个人版中为资源添加标签。

7. 选择复制映像。

共享或取消共享自定义 WorkSpaces 个人版映像

您可以在同一 Amazon 区域内的 Amazon 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 Amazon 区域。有关复制映像的更多信息，请参阅在 “个 WorkSpaces 人” 中复制自定义镜像。

> **Note**
>
> 在中国（宁夏）区域，您只能复制同一区域内的映像。
> 在 Amazon GovCloud (US) Region中，要将映像复制到其他 Amazon 区域或从此类区域复制映像，请联系 Amazon Support。

共享映像不会产生额外的费用。但需遵循 Amazon 区域中的映像数量配额。在收件人复制共享映像之前，该映像不会计入收件人账户的配额。有关 Amazon WorkSpaces 配额的更多信息，请参阅 Amazon WorkSpaces 配额。

要删除共享映像，您必须首先取消共享映像，然后才能将其删除。

共享自带许可映像

您只能与启用 BYOL 的 Amazon 账户共享自带许可 (BYOL) 映像。您想要与其共享 BYOL 映像的 Amazon 账户也必须是您组织的一部分（在同一付款人账户下）。

> **Note**
>
> 目前，Amazon GovCloud（美国西部）和 Amazon GovCloud（美国东部）区域不支持跨 Amazon 账户共享 BYOL 映像。要在 Amazon GovCloud（美国西部）和 Amazon GovCloud（美国东部）区域跨账户共享 BYOL 映像，请联系 Amazon Support。

与您共享的映像

如果与您共享映像，则您可以复制此类映像。然后，您可以使用共享映像的副本创建用于启动新 WorkSpaces 的捆绑包。

> **Important**
>
> 在复制共享映像之前，请务必确认该映像是从正确的 Amazon 账户共享的。要以编程方式确定映像是否已共享，请在 Amazon 命令行界面 (CLI) 中使用 DescribeWorkSpaceImages 和 DescribeWorkSpaceImagePermissions API 操作或 describe-workspace-images 和 describe-workspace-image-permissions 命令。

为与您共享的映像显示的创建日期是该映像最初的创建日期，而不是与您共享映像的日期。

如果映像已与您共享，则您无法与其他账户进一步共享该映像。

共享映像

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择映像。
3. 选择映像以打开其详细信息页面。
4. 在映像详细信息页面的共享账户部分，选择添加账户。
5. 在添加账户页面的添加要与之共享的账户下，输入要与之共享映像的账户的账户 ID。

   > **Important**
   >
   > 在共享映像之前，请确认您正在共享到正确的 Amazon 账户 ID。

6. 选择共享映像。

   > **Note**
   >
   > 要使用共享映像，收件人账户必须先复制该映像。然后，收件人账户可以使用共享映像的副本创建用于启动新 WorkSpaces 的捆绑包。

停止共享映像

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择映像。
3. 选择映像以打开其详细信息页面。

4. 在映像详细信息页面的共享账户部分，选择要停止共享的 Amazon 账户，然后选择取消共享。
5. 当系统提示您确认取消共享映像时，选择取消共享。

> **Note**
>
> 如果要在取消共享映像后将其删除，则必须先取消与其共享的所有账户的共享。

如果您停止共享映像，则收件人账户将无法再复制映像。但是，收件人账户中已存在的共享映像的任何副本都将保留在该账户中，并且可以从这些副本启动新的 WorkSpaces。

以编程方式共享或取消共享映像

要以编程方式共享或取消共享映像，请使用 UpdateWorkSpaceImagePermission API 操作或 update-workspace-image-permission Amazon Command Line Interface (Amazon CLI) 命令。要确定映像是否已共享，请使用 DescribeWorkSpaceImagePermissions API 操作或 describe-workspace-image-permissions CLI 命令。

删除 WorkSpaces 个人版中的自定义捆绑包或映像

您可以根据需要，删除未使用的自定义捆绑包或自定义映像。

删除捆绑包

要删除捆绑包，必须先删除基于捆绑包的所有 WorkSpaces。

使用控制台删除捆绑包

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择 Bundles。
3. 选择捆绑包，然后选择删除。
4. 当系统提示进行确认时，选择 Delete（删除）。

以编程方式删除捆绑包

要以编程方式删除捆绑包，请使用 DeleteWorkspaceBundle API 操作。有关更多信息，请参阅《Amazon WorkSpaces API 参考》中的 DeleteWorkSpaceBundle。

> **Note**
>
> 确保在删除捆绑包后至少等待 2 小时，然后再创建相同名称的新捆绑包。

删除映像

在删除自定义服务包后，可以删除用于创建或更新该服务包的映像。

要删除映像，您必须先删除与该映像关联的所有捆绑包，或者必须更新这些捆绑包以使用其他源映像。如果映像与其他账户共享，则还必须取消共享。此外，映像不能处于待处理或正在验证状态。

使用控制台删除映像

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择映像。
3. 选择映像，然后选择删除。
4. 当系统提示进行确认时，选择 Delete（删除）。

以编程方式删除映像

要以编程方式删除映像，请使用 DeleteWorkspaceImage API 操作。有关更多信息，请参阅《Amazon WorkSpaces API 参考》中的 DeleteWorkSpaceImage。

监控 WorkSpaces 个人版

您可以使用以下功能监控您的 WorkSpaces。

CloudWatch 指标

Amazon WorkSpaces 将有关 WorkSpaces 的数据点发布到 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。

CloudWatch Events

当用户登录您的 WorkSpace 时，Amazon WorkSpaces 可以向 Amazon CloudWatch Events 提交事件。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 Amazon EventBridge 监控您的 WorkSpaces。

CloudTrail 日志

Amazon CloudTrail 提供用户、角色或 Amazon 服务在 WorkSpaces 中执行的操作记录。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。相关详情，请参阅使用 CloudTrail 记录 WorkSpaces API 调用日志。Amazon CloudTrail 会记录智能卡用户的成功和失败登录事件。有关更多信息，请参阅 了解智能卡用户的 Amazon 登录事件。

CloudWatch 网络监测仪

Amazon CloudWatch 网络监测仪可让您了解互联网问题如何影响 Amazon 上托管的应用程序与最终用户之间的互联网性能和可用性。您还可使用 CloudWatch 网络监测仪进行以下操作：

- 为一个或多个 WorkSpace 目录创建监测仪。
- 监控互联网性能。
- 针对最终用户的城市网络（包括其位置和 ASN，通常是互联网服务提供商 (ISP)）及其 WorkSpace 区域之间的问题获取警报。

网络监测仪使用 Amazon 从其全球网络足迹中捕获的连接数据来计算面向互联网流量的性能和可用性基准。网络监测仪目前无法为个人最终用户提供互联网性能，但可以在城市和 ISP 级别提供此类性能。

Amazon S3 访问日志

如果您的用户将应用程序设置数据或主文件夹数据存储在 Amazon S3 存储桶中，请考虑查看 Amazon S3 服务器访问日志来监视访问情况。这些日志提供有关对存储桶做出的请求的详细记录。对于许多应用程序而言，服务器访问日志很有用。例如，访问日志信息可能在安全和访问权限审核方面很有用。有关更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的 mazon S3 服务器访问日志记录。

使用 CloudWatch 自动控制面板监控您的 WorkSpaces 运行状况

您可以使用 CloudWatch 自动控制面板监控 WorkSpaces，该面板会收集原始数据并将其处理为可读且近乎实时的指标。这些指标会保留 15 个月，从而使您能够访问历史信息，并监控您 Web 应用程序或服务的性能。此外，可以设置用于监测特定阈值的警报，并在达到相应阈值时发送通知或执行操作。有关更多信息，请参阅《Amazon CloudWatch 用户指南》。

当您使用您的 Amazon 账户配置 WorkSpaces 时，CloudWatch 控制面板会自动创建。该控制面板允许您跨区域监控 WorkSpaces 指标，例如其运行状况和性能。您还可以将控制面板用于以下目的：

- 识别运行状况不佳的 WorkSpace 实例。
- 识别 WorkSpace 实例运行状况不佳的运行模式、协议和操作系统。
- 查看一段时间内的关键资源利用率。
- 识别异常以帮助进行故障排除。

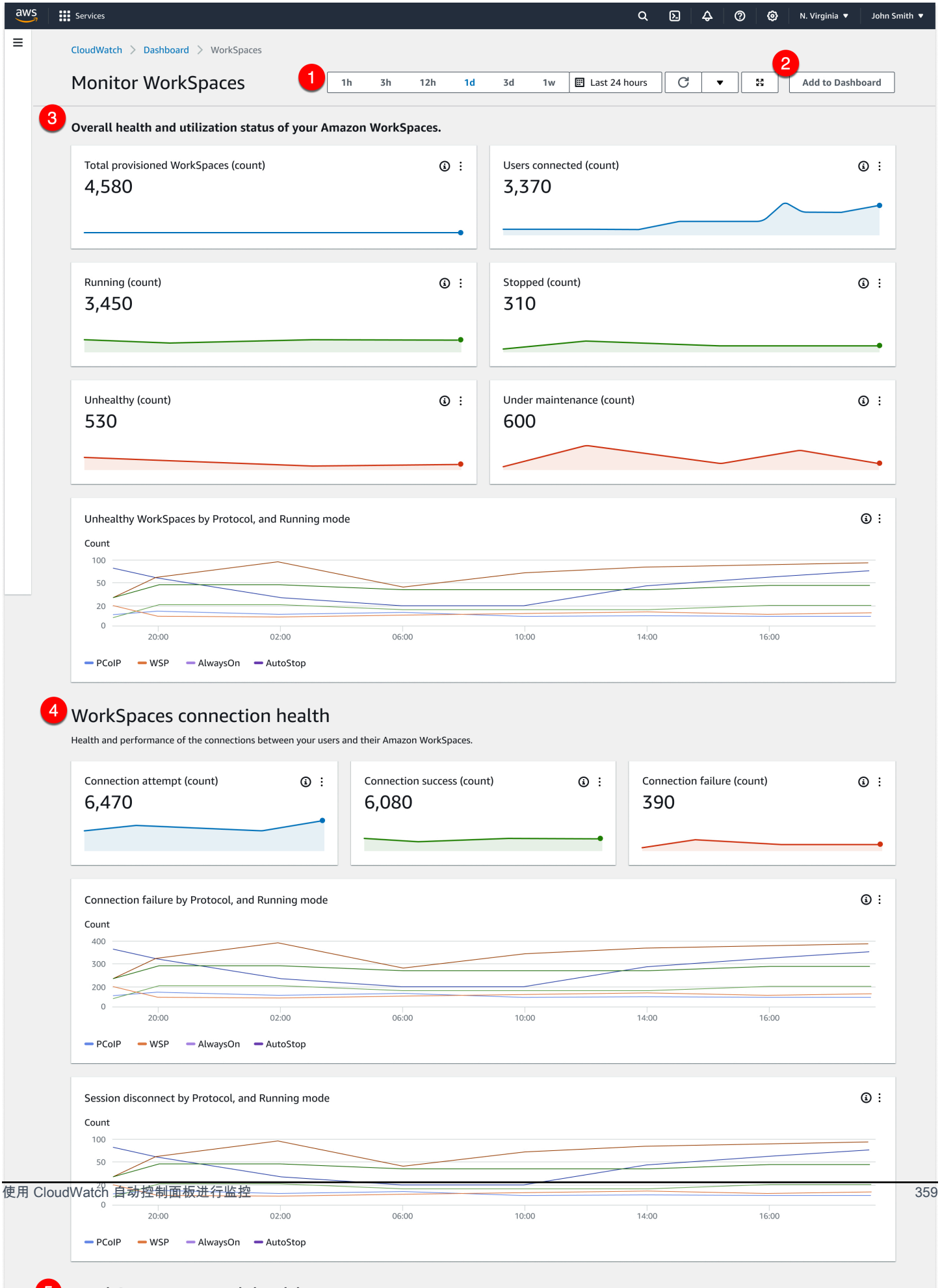
WorkSpaces CloudWatch 自动控制面板可在所有 Amazon 商业区域使用。

使用 WorkSpaces CloudWatch 自动控制面板

1. 通过 https://console.aws.amazon.com/cloudwatch/ 打开 CloudWatch 控制台。
2. 在导航窗格中，选择 Dashboards（控制面板）。
3. 选择自动控制面板选项卡。
4. 选择 WorkSpaces。

了解您的 WorkSpaces CloudWatch 自动控制面板

借助 CloudWatch 自动控制面板，您可以深入了解 WorkSpaces 资源的性能，并帮助您识别性能问题。


aws
Services
N. Virginia
John Smith
CloudWatch > Dashboard > WorkSpaces
Monitor WorkSpaces
1
1h 3h 12h 1d 3d 1w
Last 24 hours
2
Add to Dashboard
3
Overall health and utilization status of your Amazon WorkSpaces.
Total provisioned WorkSpaces (count)
4,580
Users connected (count)
3,370
Running (count)
3,450
Stopped (count)
310
Unhealthy (count)
530
Under maintenance (count)
600
Unhealthy WorkSpaces by Protocol, and Running mode
Count
100
50
20
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop
4
WorkSpaces connection health
Health and performance of the connections between your users and their Amazon WorkSpaces.
Connection attempt (count)
6,470
Connection success (count)
6,080
Connection failure (count)
390
Connection failure by Protocol, and Running mode
Count
400
300
200
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop
Session disconnect by Protocol, and Running mode
Count
100
50
0
20:00
02:00
06:00
10:00
14:00
16:00
PCoIP
WSP
AlwaysOn
AutoStop

控制面板由以下功能组成：

1. 使用时间和日期范围控件查看历史数据。
2. 向 CloudWatch 自定义控制面板中添加自定义控制面板视图。
3. 通过执行以下操作，来监控 WorkSpaces 的整体运行状况和利用率状态：
   a. 查看预置 WorkSpaces 的总数、连接的用户数、运行状况不佳和运行正常的 WorkSpace 实例数。
   b. 查看运行状况不佳的 WorkSpaces 及其不同的变量，例如协议和计算模式。
   c. 将鼠标指针悬停在折线图上，可以查看一段时间内特定协议和运行模式下运行正常或运行状况不佳的 WorkSpace 实例的数量。
   d. 选择省略号菜单，然后选择在指标中查看，以在时间尺度图表上查看指标。
4. 查看您的连接指标及其不同的变量，例如，在任何给定时间 WorkSpaces 环境中的连接尝试次数、成功连接次数和失败连接次数。
5. 查看影响用户体验的 InSession 延迟，例如，往返时间（RTT），以确定连接运行状况和数据包丢失情况，从而监控网络运行状况。
6. 查看主机性能和资源利用率，以识别和排查潜在的性能问题。

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 命令行界面或者通过以编程方式使用 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。

有关使用 CloudWatch 和警报的更多信息，请参阅 Amazon CloudWatch 用户指南。

先决条件

要获取 CloudWatch 指标，请在 `cn-northwest-1` 区域 AMAZON 子网的端口 443 上启用访问。有关更多信息，请参阅 WorkSpaces 个人的 IP 地址和端口要求。

目录

- WorkSpaces 指标
- WorkSpaces 指标的维度
- 监控示例

WorkSpaces 指标

AWS/WorkSpaces 命名空间包括以下指标。

指标	描述	维度	统计数据	单位
Available [1]	返回正常运行状态的 WorkSpaces 的数量。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	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 RunningMode Protocol ComputeType BundleId UserName ComputerName	Average、Sum、Maximum、Minimum、Data Samples	计数
ConnectionAttempt [2]	连接尝试次数。	DirectoryId	Average、Sum、Maximu	计数

指标	描述	维度	统计数据	单位
		WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	m、Minimum、Data Samples	
ConnectionSuccess [2]	成功连接的数量。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	Average、Sum、Maximum、Minimum、Data Samples	计数

指标	描述	维度	统计数据	单位
ConnectionFailure [2]	失败连接的数量。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	Average、Sum、Maximum、Minimum、Data Samples	计数
SessionLaunchTime [2、6]	发起 WorkSpaces 会话所用的时间量。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	Average、Sum、Maximum、Minimum、Data Samples	秒（时间）

指标	描述	维度	统计数据	单位
InSession Latency [2、6]	WorkSpaces 客户端和 WorkSpace 之间的往返操作时间。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	Average、Sum、Maximum、Minimum、Data Samples	毫秒（时间）
SessionDisconnect [2、6]	已关闭的连接数，包括用户启动的和失败的连接。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	Average、Sum、Maximum、Minimum、Data Samples	计数

指标	描述	维度	统计数据	单位
UserConnected [3]	用户已连接的 WorkSpaces 数量。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	Average、Sum、Maximum、Minimum、Data Samples	计数
Stopped	已停止的 WorkSpaces 的数量。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	Average、Sum、Maximum、Minimum、Data Samples	计数

指标	描述	维度	统计数据	单位
Maintenance [4]	正在维护的 WorkSpaces 的数量。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	Average、Sum、Maximum、Minimum、Data Samples	计数
TrustedDeviceValidationAttempt [5、6]	设备身份验证签名验证尝试次数。	DirectoryId	Average、Sum、Maximum、Minimum、Data Samples	计数
TrustedDeviceValidationSuccess [5、6]	成功的设备身份验证签名验证次数。	DirectoryId	Average、Sum、Maximum、Minimum、Data Samples	计数
TrustedDeviceValidationFailure [5、6]	失败的设备身份验证签名验证次数。	DirectoryId	Average、Sum、Maximum、Minimum、Data Samples	计数
TrustedDeviceCertificateDaysBeforeExpiration [6]	与该目录关联的根证书过期前所剩的天数。	CertificateId	Average、Sum、Maximum、Minimum、Data Samples	计数

指标	描述	维度	统计数据	单位
CPUUsage	使用的 CPU 资源所占的百分比。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	平均值、最大值、最小值	百分比
MemoryUsage	使用的计算机内存百分比。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	平均值、最大值、最小值	百分比

指标	描述	维度	统计数据	单位
RootVolumeDiskUsage	卷中已使用根磁盘空间的百分比。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	平均值、最大值、最小值	百分比
UserVolumeDiskUsage	卷中已使用用户磁盘空间的百分比。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	平均值、最大值、最小值	百分比

指标	描述	维度	统计数据	单位
UDPPacketLossRate [7]	在客户端和网关之间丢弃的数据包的百分比。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	平均值、最大值、最小值、数据样本	百分比
UpTime	自上次重启 WorkSpace 以来经过的时间。	DirectoryId WorkspaceId RunningMode Protocol ComputeType BundleId UserName ComputerName	平均值、最大值、最小值、数据样本	秒

[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`。这些指标以每个 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。这些指标以每个 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。此指标以每个 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。此指标以每个 WorkSpace 为粒度提供，描述 WorkSpace 何时进入维护，以及何时移除。

[5] 如果为目录启用了可信设备功能，则 Amazon WorkSpaces 将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，系统会发出这些指标以指示可信设备身份验证成功或失败。这些指标以每个目录为粒度提供，并且仅适用于 Amazon WorkSpaces Windows 和 macOS 客户端应用程序。

[6] 在 WorkSpaces Web Access 上不可用。

[7] 该指标测量平均数据包丢失率。

- 在 PCoIP 上：测量从客户端到网关的平均 UDP 数据包丢失率。

> **Note**
>
> 这是在网关上测量的。

- 在 DCV 上：测量从网关到客户端的 UDP 数据包丢失率。

> **Note**
>
> 这是在网关上测量的。

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	针对指定的 WorkSpace 筛选指标数据。WorkSpace ID 的形式为 ws-XXXXXXXXXX 。
CertificateId	针对与该目录关联的指定根证书筛选指标数据。证书 ID 的形式为 wsc-XXXXXXXXX 。
RunningMode	针对指定 WorkSpaces，按其运行模式筛选指标数据。运行模式的形式是“AutoStop”或“AlwaysOn”。
BundleId	针对指定 WorkSpaces，按协议筛选指标数据。捆绑包的形式为 wsb-XXXXXXXXXX 。
ComputeType	针对指定 WorkSpaces，按计算类型筛选指标数据。
Protocol	针对指定 WorkSpaces，按协议类型筛选指标数据。
UserName	针对指定 WorkSpaces，按用户名筛选指标数据。 **Note** UserName 不能由非 ASCII 字符组成，如以下字符： • 重音字母：é、à、ö、ñ 等 • 非拉丁字母 • 符号：©#、®#、€、£、µ、¥ 等

维度	描述
ComputerName	针对指定的 WorkSpace 筛选指标数据。参见 WorkSpaces 计算机名称的各种格式。

监控示例

以下示例展示了如何使用 Amazon CLI 响应 CloudWatch 警报，以及如何确定目录中的哪些 WorkSpaces 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 get-metric-statistics 命令获取目录中每个 WorkSpace 的 CloudWatch 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 Amazon EventBridge 监控您的 WorkSpaces

您可以使用 Amazon WorkSpaces 中的事件查看、搜索、下载、存档、分析和响应对您的 WorkSpaces 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 `WorkSpaces Access` 事件类型中找到的访问条件的文件或数据。
- 使用 Amazon Lambda 分析登录数据并执行自动操作。
- 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。
- 查找用于连接 WorkSpaces 的 WorkSpaces 客户端版本。

Amazon WorkSpaces 尽最大努力发出这些事件。事件将近乎实时传输到 EventBridge。您可以使用 EventBridge 创建触发编程操作以响应事件的规则。例如，您可以配置规则，以调用 SNS 主题发送电子邮件通知，或者调用 Lambda 函数执行某些操作。有关更多信息，请参阅 Amazon EventBridge 用户指南。

WorkSpaces 访问事件

WorkSpaces 客户端应用程序在用户成功登录 WorkSpace 时发送 `WorkSpaces Access` 事件。所有 WorkSpaces 客户端都发送这些事件。

使用 DCV 为 WorkSpaces 发出的事件需要 WorkSpaces 客户端应用程序 4.0.1 或更高版本。

事件表示为 JSON 对象。以下是 `WorkSpaces Access` 事件的示例数据。

```
{
    "version": "0",
    "id": "64ca0eda-9751-dc55-c41a-1bd50b4fc9b7",
    "detail-type": "WorkSpaces Access",
    "source": "aws.workspaces",
    "account": "123456789012",
    "time": "2023-04-05T16:13:59Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "clientIpAddress": "192.0.2.3",
        "actionType": "successfulLogin",
```

```
        "workspacesClientProductName": "WorkSpacesWebClient",
        "loginTime": "2023-04-05T16:13:37.603Z",
        "clientPlatform": "Windows",
        "directoryId": "domain/d-123456789",
        "clientVersion": "5.7.0.3472",
        "workspaceId": "ws-xyskdga"
    }
}
```

特定于事件的字段

`clientIpAddress`

客户端应用程序的 WAN IP 地址。对于 PCoIP 零客户端，这是 Teradici 身份验证客户端的 IP 地址。

`actionType`

此值始终为 `successfulLogin`。

`workspacesClientProductName`

以下值区分大小写。

- `WorkSpaces Desktop client` - Windows、macOS 和 Linux 客户端
- `Amazon WorkSpaces Mobile client` - iOS 客户端
- `WorkSpaces Mobile Client` - Android 客户端
- `WorkSpacesWebClient` - Web Access 客户端
- `AmazonWorkSpacesThinClient` - Amazon WorkSpaces 瘦客户端设备
- `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`
- `iOS`
- `Linux`
- `OSX`

- `Windows`
- `Teradici PCoIP Zero Client and Tera2`
- `Web`

`directoryId`

WorkSpace 的目录的标识符。必须在目录标识符前面加上 `domain/`。例如 `"domain/d-123456789"`。

`clientVersion`

用于连接 WorkSpaces 的客户端版本。

`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 规则来处理 WorkSpaces 事件。

先决条件

要接收电子邮件通知，请创建 Amazon Simple Notification Service 主题。

1. 通过 https://console.aws.amazon.com/sns/v3/home 打开 Amazon SNS 控制台。
2. 在导航窗格中，选择 Topics（主题）。
3. 选择创建主题。
4. 对于类型，选择标准。
5. 对于 Name（名称），请为主题输入一个名称。
6. 选择创建主题。
7. 选择创建订阅。
8. 对于协议，选择电子邮件。
9. 对于 Endpoint（端点），请输入接收通知的电子邮件地址。
10. 选择创建订阅。
11. 您将收到电子邮件消息，其主题行为：Amazon Notification - Subscription Confirmation。请按照说明确认订阅。

创建一个规则来处理 WorkSpaces 事件

1. 打开位于 https://console.aws.amazon.com/events/ 的 Amazon EventBridge 控制台。
2. 选择 Create rule (创建规则)。
3. 对于 Name（名称），请为规则输入一个名称。
4. 对于规则类型，选择具有事件模式的规则。
5. 选择下一步。
6. 对于 Event pattern（事件模式），执行以下操作：
   a. 对于事件源，选择 Amazon Web Services 服务。
   b. 对于 Amazon Web Services 服务，选择 WorkSpaces。
   c. 对于事件类型，选择 WorkSpaces 访问。
   d. 默认情况下，我们会就每个事件发送通知。如果愿意，您可以创建一种事件模式来筛选特定客户端或 WorkSpaces 的事件。
7. 选择下一步。
8. 按以下操作指定目标：
   a. 对于 Target types（目标类型），选择 Amazon Web Services 服务。
   b. 对于 Select a target（选择一个目标），选择 SNS topic（SNS 主题）。
   c. 对于主题，选择您为通知创建的 SNS 主题。
9. 选择下一步。
10. （可选）向规则添加标签。
11. 选择下一步。
12. 选择创建规则。

了解智能卡用户的 Amazon 登录事件

Amazon CloudTrail 会记录智能卡用户的成功和失败登录事件。这包括每次提示用户解决特定凭证问题或因素时捕获的登录事件，以及该特定凭证验证请求的状态。用户只有在完成所有必需的凭证质疑后才能登录，这会导致系统记录 `UserAuthentication` 事件日志。

下表记录了每个登录的 CloudTrail 事件名称及其目的。

事件名称	事件目的
CredentialChallenge	通知 Amazon 登录已请求用户解决特定的凭证质疑，并指定所需的 CredentialType 凭证（例如 SMARTCARD）。
CredentialVerification	通知用户已尝试解决特定 CredentialChallenge 请求，并指定该凭证是成功还是失败。
UserAuthentication	通知用户受到质疑的所有身份验证要求均已成功完成，并且用户已成功登录。当用户未能成功完成所需的凭证质疑时，不会记录 UserAuthentication 事件日志。

下表记录了特定登录 CloudTrail 事件中包含的其他有用事件数据字段。

事件名称	活动目的	登录事件的适用性	示例值
AuthWorkflowID	关联整个登录序列中发出的所有事件。对于每位用户登录，Amazon 登录可发出多个事件。	CredentialChallenge，CredentialVerification，UserAuthentication	“AuthWorkflowID”：“9de74b32-8362-4a01-a524-de21df59fd83”
CredentialType	通知用户已尝试解决特定 CredentialChallenge 请求，并指定该凭证是成功还是失败。	CredentialChallenge，CredentialVerification，UserAuthentication	“CredentialType”：“SMARTCARD”（目前可能的值：SMARTCARD）
LoginTo	通知用户受到质疑的所有身份验证要求均已成功完成，并且用户已成功登录。当用户未能成功完成所需的凭证质疑时，不会记录 UserAuthentication 事件日志。	UserAuthentication	“LoginTo”：“https://skylight.local”

Amazon 登录场景的示例事件

以下示例显示了适用于不同登录场景的 CloudTrail 事件的预期序列。

目录

- 使用智能卡进行身份验证时成功登录
- 仅使用智能卡进行身份验证时登录失败

使用智能卡进行身份验证时成功登录

以下事件序列捕获了成功登录智能卡的示例。

CredentialChallenge


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:29Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialChallenge",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "65551a6d-654a-4be8-90b5-bbfef7187d3a",
    "eventID": "fb603838-f119-4304-9fdc-c0f947a82116",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
```

```
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialChallenge": "Success"
    }
}
```

Successful CredentialVerification

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialVerification",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "81869203-1404-4bf2-a1a4-3d30aa08d8d5",
    "eventID": "84c0a2ff-413f-4d0f-9108-f72c90a41b6c",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialVerification": "Success"
    }
```

```
}
```

Successful UserAuthentication

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:39Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "UserAuthentication",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "6602f256-3b76-4977-96dc-306a7283269e",
        "LoginTo": "https://skylight.local",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "81869203-1404-4bf2-a1a4-3d30aa08d8d5",
    "eventID": "acc0dba8-8e8b-414b-a52d-6b7cd51d38f6",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        UserAuthentication": "Success"
    }
}
```

仅使用智能卡进行身份验证时登录失败

以下事件序列捕获了登录智能卡失败的示例。

CredentialChallenge


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:06Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialChallenge",
    "awaRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "73dfd26b-f812-4bd2-82e9-0b2abb358cdb",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "73eb499d-91a8-4c18-9c5d-281fd45ab50a",
    "eventID": "f30a50ec-71cf-415a-a5ab-e287edc800da",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialChallenge": "Success"
    }
}
```

Failed CredentialVerification


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "509318101470",
        "arn": "",
        "accountId": "509318101470",
        "accessKeyId": ""
    },
    "eventTime": "2021-07-30T17:23:13Z",
    "eventSource": "signin.amazonaws.com",
    "eventName": "CredentialVerification",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/91.0.4472.164 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "AuthWorkflowID": "73dfd26b-f812-4bd2-82e9-0b2abb358cdb",
        "CredentialType": "SMARTCARD"
    },
    "requestID": "051ca316-0b0d-4d38-940b-5fe5794fda03",
    "eventID": "4e6fbfc7-0479-48da-b7dc-e875155a8177",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "509318101470",
    "serviceEventDetails": {
        CredentialVerification": "Failure"
    }
}
```

使用Amazon CloudFormation模板创建自定义 CloudWatch 仪表板

Amazon提供了可用于为其创建自定义 CloudWatch 仪表板的Amazon CloudFormation模板 WorkSpaces。从以下Amazon CloudFormation模板选项中进行选择，以便在Amazon CloudFormation 控制台 WorkSpaces 中为您创建自定义仪表板。

开始之前要考虑的事项

在开始使用自定义 CloudWatch 仪表板之前，请考虑以下几点：

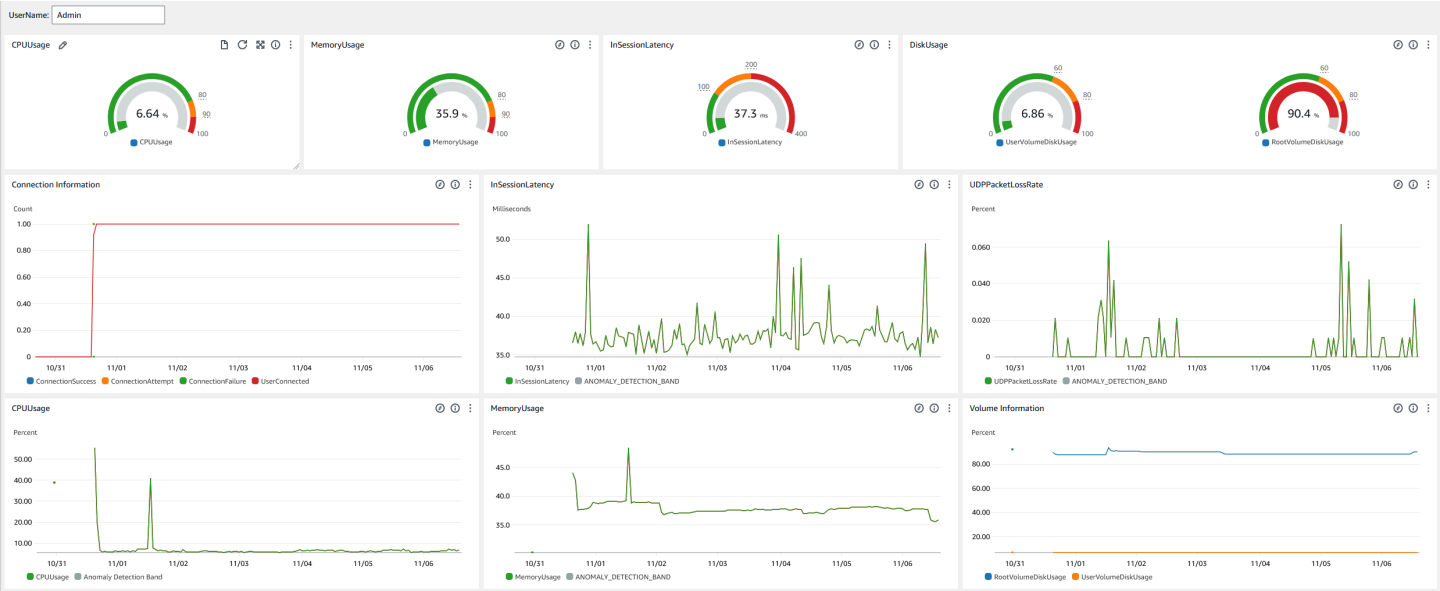
- 使用与要监控的已部署仪表板Amazon Web Services 区域相同 WorkSpaces 的方式创建仪表板。
- 您也可以使用 CloudWatch 控制台创建自定义仪表板。
- 费用可能与自定义 CloudWatch 仪表板有关。有关定价的信息，请参阅 Amazon CloudWatch 定价

帮助台控制面板

服务台仪表板显示特定指标的以下指标 WorkSpace：

- CPU 使用率
- 内存使用量
- 会话中延迟
- 根卷
- 用户卷
- 数据包丢失
- 磁盘使用量

以下是帮助台控制面板的示例。



完成以下步骤以 CloudWatch 使用创建自定义仪表板Amazon CloudFormation。

1. 在@@ Amazon CloudFormation控制台中打开 “创建堆栈” 页面。此链接打开页面，其中预先填充了帮助台自定义 CloudWatch控制面板模板的 Amazon S3 存储桶位置。
2. 在创建堆栈页面上查看默认选项。请注意，Amazon S3 网址字段已预先填充了Amazon CloudFormation模板的 Amazon S3 存储桶位置。
3. 选择下一步。
4. 在堆栈名称文本框中，输入堆栈名称。

   堆栈名称是帮助您从堆栈列表中查找特定堆栈的标识符。堆栈名称只能包含字母数字字符（区分大小写）和连字符。该名称必须以字母字符开头，且不得超过 128 个字符。
5. 在DashboardName文本框中，输入您要为仪表板命名的名称。

   控制面板名称只能包含字母数字、破折号（-）和下划线（_）。
6. 选择下一步。
7. 在配置堆栈选项页面上，查看默认选项，然后选择下一步。
8. 向下滚动到转换可能需要访问功能，然后选中复选框进行确认。然后选择 S ub mit 以创建堆栈和自定义 CloudWatch控制面板。

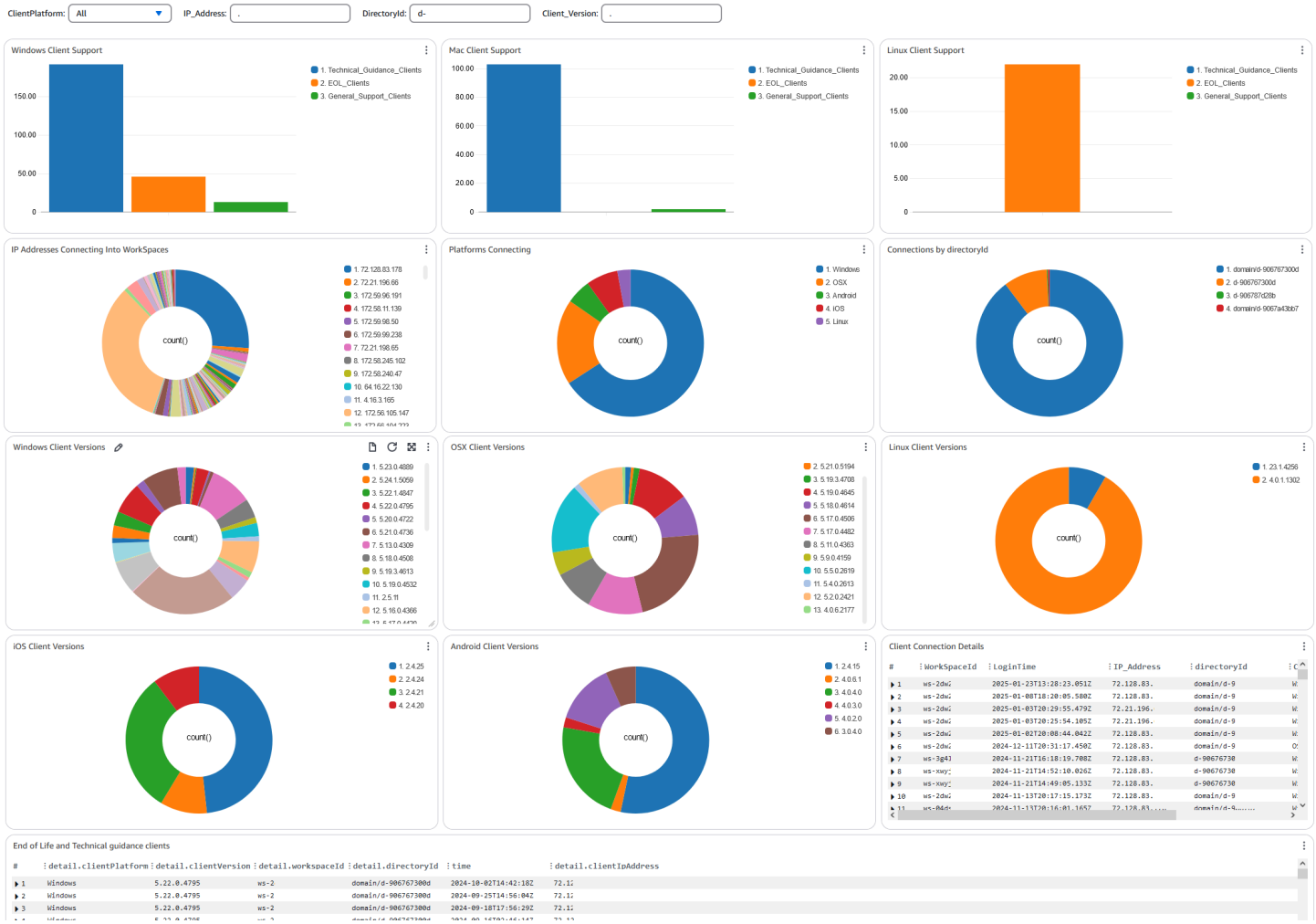
> **Important**
>
> 费用可能与自定义 CloudWatch 仪表板有关。有关定价的信息，请参阅 Amazon CloudWatch 定价

9. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
10. 在左侧导航窗格中，选择控制面板。
11. 在自定义控制面板下，选择带有您之前在此过程中输入的控制面板名称的控制面板。
12. 使用服务台示例模板，输入 UserName WorkSpace 以监控其数据。

Connection Insights 控制面板

Connection Insights 控制面板显示连接到您的客户端版本、平台和 IP 地址 WorkSpaces。通过此控制面板，您可以更好地了解用户的连接方式，以便可以使用过时的客户端主动通知用户。动态变量允许您监控 IP 地址或特定目录的详细信息。

以下是 Connection Insights 控制面板的示例。



完成以下步骤以 CloudWatch 使用创建自定义仪表板Amazon CloudFormation。

1. 在@@ Amazon CloudFormation控制台中打开 “创建堆栈” 页面。此链接打开页面，其中预先填充了 Connection Insights 自定义 CloudWatch 控制面板模板的 Amazon S3 存储桶位置。
2. 在创建堆栈页面上查看默认选项。请注意，Amazon S3 网址字段已预先填充了Amazon CloudFormation模板的 Amazon S3 存储桶位置。
3. 选择下一步。
4. 在堆栈名称文本框中，输入堆栈名称。

   堆栈名称是帮助您从堆栈列表中查找特定堆栈的标识符。堆栈名称只能包含字母数字字符（区分大小写）和连字符。该名称必须以字母字符开头，且不得超过 128 个字符。
5. 在DashboardName文本框中，输入您要为仪表板命名的名称。输入其他相关的 CloudWatch 访问组设置信息。

   控制面板名称只能包含字母数字、破折号（-）和下划线（_）。

6. 在下方 LogRetention，输入您想要保留的天数。 LogGroup
7. 在下 SetupEventBridge，选择是否要部署 EventBridge 规则以获取 WorkSpaces 访问日志。
8. 在下方 WorkSpaceAccessLogsName，输入包含 CloudWatch LogGroup WorkSpaces 访问日志的名称。
9. 选择下一步。
10. 在配置堆栈选项页面上，查看默认选项，然后选择下一步。
11. 向下滚动到转换可能需要访问功能，然后选中复选框进行确认。然后选择 S ub mit 以创建堆栈和自定义 CloudWatch控制面板。

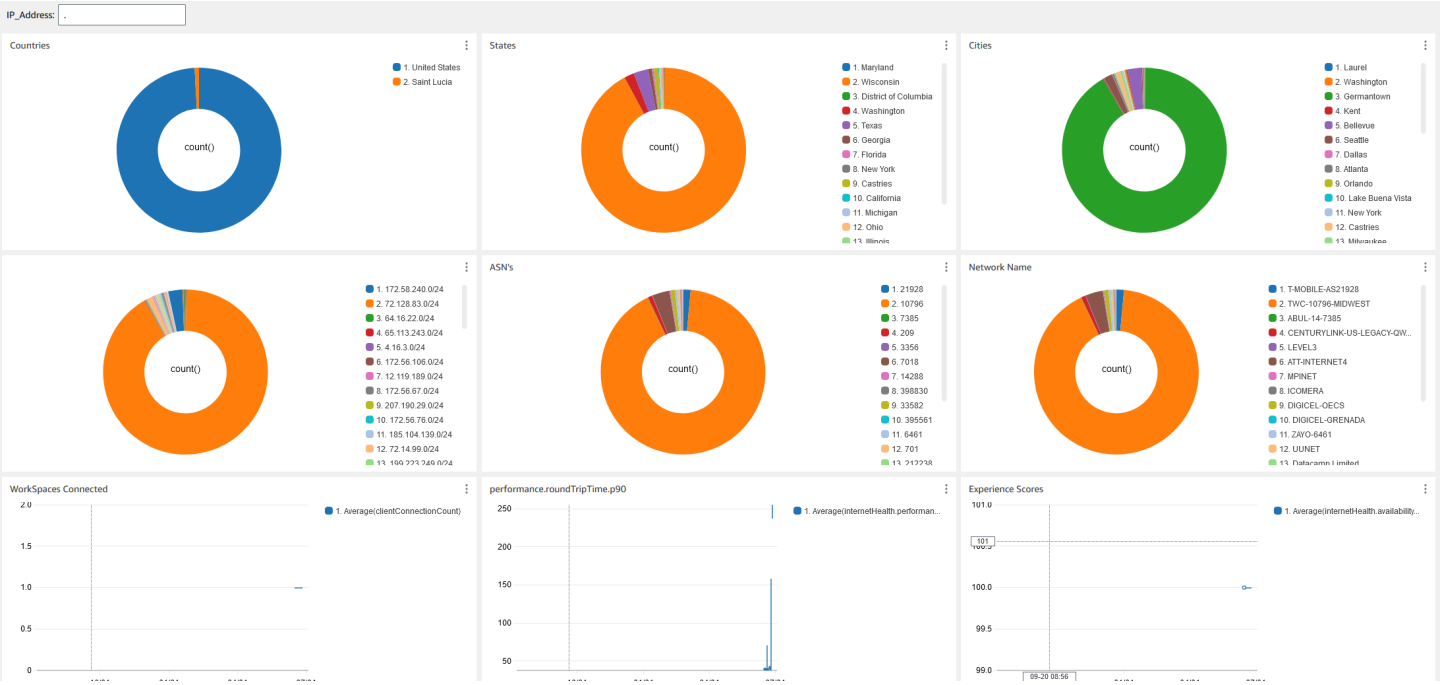
> **Important**
>
> 费用可能与自定义 CloudWatch 仪表板有关。有关定价的信息，请参阅 Amazon CloudWatch 定价

12. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
13. 在左侧导航窗格中，选择控制面板。
14. 在自定义控制面板下，选择带有您之前在此过程中输入的控制面板名称的控制面板。
15. 现在，你可以使用 Connec WorkSpace tion Insights 控制面板监控自己的数据。

Internet Monitoring 控制面板

Internet 监控控制面板显示有关您的用户用于加入其 WorkSpaces 实例的互联网服务提供商 (ISP) 的详细信息。它提供了有关城市、州、ASN、网络名称、连接数量 WorkSpaces、性能和体验分数的详细信息。您还可以使用特定的 IP 地址来获取从特定位置连接的用户的详细信息。部署 CloudWatch 互联网监控器以获取 ISP 的数据信息。有关更多信息，请参阅使用 Amazon CloudWatch 互联网监视器。

以下是 Internet Monitoring 控制面板的示例。



要在中创建自定义仪表板， CloudWatch 请使用 Amazon CloudFormation

> **Note**
>
> 在创建自定义控制面板之前，请务必使用互联网监视器创建 CloudWatch 互联网监视器。有关更多信息，请参阅使用控制台在 Amazon CloudWatch Internet Monitor 中创建监控器

1. 在@@ Amazon CloudFormation控制台中打开 “创建堆栈” 页面。此链接将打开预先填充互联网监控自定义 CloudWatch 控制面板模板的 Amazon S3 存储桶位置的页面。
2. 在创建堆栈页面上查看默认选项。请注意，Amazon S3 网址字段已预先填充了Amazon CloudFormation模板的 Amazon S3 存储桶位置。
3. 选择下一步。
4. 在堆栈名称文本框中，输入堆栈名称。

   堆栈名称是帮助您从堆栈列表中查找特定堆栈的标识符。堆栈名称只能包含字母数字字符（区分大小写）和连字符。该名称必须以字母字符开头，且不得超过 128 个字符。
5. 在DashboardName文本框中，输入您要为仪表板命名的名称。输入其他相关的 CloudWatch 访问组设置信息。

   控制面板名称只能包含字母数字、破折号（-）和下划线（_）。

6. 在下方 ResourcesToMonitor，输入您已为其启用互联网监控的目录的目录 ID。
7. 在下方 MonitorName，输入要使用的互联网监视器的名称。
8. 选择下一步。
9. 在配置堆栈选项页面上，查看默认选项，然后选择下一步。
10. 向下滚动到转换可能需要访问功能，然后选中复选框进行确认。然后选择 S ub mit 以创建堆栈和自定义 CloudWatch控制面板。

> **Important**
>
> 费用可能与自定义 CloudWatch 仪表板有关。有关定价的信息，请参阅 Amazon CloudWatch 定价

11. 打开 CloudWatch 控制台，网址为https://console.aws.amazon.com/cloudwatch/。
12. 在左侧导航窗格中，选择控制面板。
13. 在自定义控制面板下，选择带有您之前在此过程中输入的控制面板名称的控制面板。
14. 现在，您可以使用 “互联网监控” 控制面板监控您的 WorkSpace数据。

WorkSpaces 个人版的业务连续性

Amazon WorkSpaces 基于 Amazon 全球基础设施而构建，该基础设施分为 Amazon 区域和可用区。这些区域和可用区在物理隔离和数据冗余方面提供了故障恢复能力。有关更多信息，请参阅 Amazon WorkSpaces 中的故障恢复能力。

Amazon WorkSpaces 还提供跨区域重定向，该功能可与域名系统 (DNS) 路由策略配合使用，以便在用户的主 WorkSpaces 不可用时将其重定向到备用 WorkSpaces。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主区域中的 WorkSpaces 时，将他们连接到指定故障转移区域中的 WorkSpaces。

您可以使用跨区域重定向来实现区域故障恢复能力和高可用性。您也可以将其用于其他目的，例如，流量分配或在维护期间提供备用 WorkSpaces。如果您使用 Amazon 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。

Amazon WorkSpaces 多区域韧性可在辅助 WorkSpace 区域中提供自动化的冗余虚拟桌面基础设施，并可在由于中断而无法访问主区域时，简化将用户重定向到辅助区域的流程。

您可以将 WorkSpaces 多区域韧性与跨区域重定向结合使用，在辅助 WorkSpace 区域部署冗余的虚拟桌面基础设施，并设计跨区域故障转移策略，为中断事件做好准备。您也可以将该解决方案用于其他目

的，例如，流量分配或在维护期间提供备用 WorkSpaces。如果您使用 Route 53 进行 DNS 配置，则可以利用监控 CloudWatch 警报的运行状况检查。

目录

- 个人版跨区域重定向 WorkSpaces
- 个人的多区域弹性 WorkSpaces

个人版跨区域重定向 WorkSpaces

借助 Amazon 的跨区域重定向功能 WorkSpaces，您可以使用完全限定的域名 (FQDN) 作为您的注册码。 WorkSpaces跨区域重定向与您的域名系统 (DNS) 路由策略配合使用，可在主域名系统 (DNS) 路由策略 WorkSpaces 不可用 WorkSpaces 时将您的 WorkSpaces 用户重定向到替代方案。例如，通过使用 DNS 故障转移路由策略，当用户无法访问主Amazon区域 WorkSpaces 中的用户时，您可以将他们连接到您指定的故障转移区域。 WorkSpaces

您可以使用跨区域重定向和 DNS 故障转移路由策略，实现区域灾难恢复能力和高可用性。您也可以将此功能用于其他目的，例如流量分配或 WorkSpaces 在维护期间提供替代方案。如果您使用 Amazon Route 53 进行 DNS 配置，则可以利用监控亚马逊 CloudWatch 警报的运行状况检查。

要使用此功能，您必须 WorkSpaces 为两个（或更多）Amazon区域的用户进行设置。您还必须创建称为连接别名 的基于 FQDN 的特殊注册码。这些连接别名会替换您的用户特定于区域的注册码。 WorkSpaces （特定于区域的注册码仍然有效；但是，要使跨区域重定向运行，您的用户必须改用 FQDN 作为注册码。）

要创建连接别名，您需指定一个连接字符串，该字符串是您的 FQDN，如 `www.example.com` 或 `desktop.example.com`。要使用此域进行跨区域重定向，您必须向域注册商注册它并为您的域配置 DNS 服务。

创建连接别名后，将其与不同区域的 WorkSpaces 目录关联以创建关联对。每个关联对都有一个主区域和一个或多个故障转移区域。如果主区域发生中断，则您的 DNS 故障转移路由策略会将您的 WorkSpaces 用户重定向到您在故障转移区域中为他们设置的路由策略。 WorkSpaces

要指定您的主区域和故障转移区域，您需在配置 DNS 故障转移路由策略时，定义区域优先级（主区域或辅助区域）。

内容

- 前提条件
- 限制

- 步骤 1：创建连接别名
- （可选）步骤 2：与其他账户共享连接别名
- 步骤 3：将连接别名与每个区域的目录相关联
- 步骤 4：配置您的 DNS 服务并设置 DNS 路由策略
- 步骤 5：向您的 WorkSpaces 用户发送连接字符串
- 跨区域重定向架构图
- 启动跨区域重定向
- 跨区域重定向期间会发生什么
- 取消连接别名与目录的关联
- 取消共享连接别名
- 删除连接别名
- 用于关联和取消关联连接别名的 IAM 权限
- 停止使用跨区域重定向后的安全注意事项

前提条件

- 您必须拥有并注册要在连接别名中用作 FQDN 的域。如果您尚未使用其他域注册商，则可以使用 Amazon Route 53 注册您的域。有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的使用 Amazon Route 53 注册域名。

  > **Important**
  > 您必须拥有所有必要的权限才能使用与Amazon一起使用的任何域名 WorkSpaces。您同意，该域名不会违反或侵犯任何第三方的合法权利，也不会以其他方式违反适用法律。

  域名总长度不能超过 255 个字符。有关域名的更多信息，请参阅《Amazon Route 53 开发人员指南》中的 DNS 域名格式。

  跨区域重定向既适用于公有域名，也适用于私有 DNS 区域中的域名。如果您使用的是私有 DNS 区域，则必须提供虚拟专用网络 (VPN) 与包含您的虚拟私有云 (VPC) 的连接 WorkSpaces。如果您的 WorkSpaces 用户尝试使用来自公共互联网的私有 FQDN，则 WorkSpaces 客户端应用程序会返回以下错误消息：

```
"We're unable to register the WorkSpace because of a DNS server issue.
Contact your administrator for help."
```

- 您必须设置 DNS 服务并配置必要的 DNS 路由策略。跨区域重定向与您的 DNS 路由策略配合使用，可根据需要重定向您的 WorkSpaces 用户。
- 在要设置跨区域重定向的每个主区域和故障转移区域中， WorkSpaces 为用户创建。确保在每个区域的每个 WorkSpaces 目录中使用相同的用户名。为了保持您的 Active Directory 用户数据同步，我们建议您使用 AD Connector 指向您 WorkSpaces 为用户设置的每个区域中的同一个活动目录。有关创建的更多信息 WorkSpaces，请参阅 Launch WorkSpaces。

> **Important**
>
> 如果您将Amazon托管 Microsoft AD 目录配置为多区域复制，则只能注册主区域中的目录以供亚马逊 WorkSpaces使用。尝试在复制区域中注册该目录以供在 Amazon 上使用 WorkSpaces 将失败。在复制的区域 WorkSpaces 内，亚马逊不支持使用Amazon托管 Microsoft AD 进行多区域复制。

完成跨区域重定向的设置后，必须确保您的 WorkSpaces 用户使用的是基于 FQDN 的注册码，而不是其主区域的基于区域的注册码（例如）。`WSpdx+ABC12D`为此，您必须按照步骤 5：向您的 WorkSpaces 用户发送连接字符串中的步骤操作，向他们发送一封包含 FQDN 连接字符串的电子邮件。

> **Note**
>
> 如果您在 WorkSpaces 控制台中创建用户而不是在 Active Directory 中创建用户，则每当您启动新用户时，都会 WorkSpaces 自动向您的用户发送一封包含基于区域的注册码的邀请电子邮件。 WorkSpace这意味着，当您在故障转移区域 WorkSpaces 为用户进行设置时，您的用户还将自动收到有关这些故障转移的电子邮件 WorkSpaces。您需要指示您的用户忽略含有基于区域的注册码的电子邮件。

限制

- 跨区域重定向不会自动检查与主区域的连接是否失败，然后会使您无法转移 WorkSpaces 到另一个区域。换句话说，自动故障转移不会发生。

要实施自动故障转移场景，您必须将其他机制与跨区域重定向结合使用。例如，您可以将 Amazon Route 53 故障转移 DNS 路由策略与监控主区域 CloudWatch 警报的 Route 53 运行状况检查配对。如果触发了主区域的 CloudWatch 警报，则您的 DNS 故障转移路由策略会将您的 WorkSpaces 用户重定向到您在故障转移区域中为他们设置的策略。 WorkSpaces

- 只有版本 3.0.9 或更高版本的 Linux、macOS 和 Windows 客户端应用程序支持跨区域重定向。WorkSpaces 您也可以将跨区域重定向与 Web Access 配合使用。
- 除了 Amazon GovCloud (US) Region s 和中国（宁夏）Amazon地区外，所有 WorkSpaces 支持 Amazon 的地区都支持跨区域重定向。

步骤 1：创建连接别名

使用同一个Amazon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. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在控制台的右上角，为您的选择主要Amazon区域。 WorkSpaces
3. 在导航窗格中，选择 Account Settings (账户设置)。
4. 在跨区域重定向下，选择创建连接别名。
5. 对于连接字符串，输入 FQDN，例如 `www.example.com` 或 `desktop.example.com`。连接字符串最大长度为 255 个字符。它只能包含字母（A-Z 和 a-z）、数字（0-9）和以下字符：.-

   > **Important**
   >
   > 创建连接字符串后，它始终与您的Amazon账户关联。您无法使用其他账户重新创建相同的连接字符串，即使您从原始账户中删除了连接字符串的所有实例也是如此。连接字符串针对您的账户进行了全局保留。

6. （可选）在标签下，指定要与连接别名关联的任意标签。
7. 选择创建连接别名。
8. 重复这些步骤，但是在中Step 2，请务必为您的选择故障转移区域 WorkSpaces。如果您有多个故障转移区域，请对每个故障转移区域重复这些步骤。请务必使用同一个Amazon帐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Amazon地区的另一个Amazon账户共享连接别名。与另一个账户共享连接别名将向该账户授予权限，以便仅将该别名与该账户在同一区域中拥有的目录关联或取消关联。只有拥有连接别名的账户才能删除该别名。

> **Note**
>
> 一个连接别名只能与每个Amazon区域的一个目录相关联。如果您与其他Amazon账户共享连接别名，则只有一个账户（您的账户或共享账户）可以将该别名与该地区的目录相关联。

与其他Amazon账户共享连接别名

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在控制台的右上角，选择要与其他账户共享连接别名的Amazon区域。Amazon
3. 在导航窗格中，选择 Account Settings (账户设置)。
4. 在跨区域重定向关联下，选择连接字符串，然后选择操作、共享/取消共享连接别名。

   您也可以从详细信息页面共享连接别名的别名。为此，请在共享账户下，选择共享连接别名。
5. 在 “共享/取消共享连接别名” 页面的 “与账户共享” 下，输入您要在此区域中与之共享连接别名的Amazon账户 ID。Amazon
6. 选择共享。

步骤 3：将连接别名与每个区域的目录相关联

将相同的连接别名与两个或更多区域中的 WorkSpaces 目录相关联可在目录之间创建关联对。每个关联对都有一个主区域和一个或多个故障转移区域。

例如，如果您的主要区域是美国西部（俄勒冈）区域，则可以将美国西部（俄勒冈）地区的 WorkSpaces 目录与美国东部（弗吉尼亚北部）地区的目录配对。 WorkSpaces 如果主区域发生中断，则跨区域重定向将与您的 DNS 故障转移路由策略以及您在美国西部（俄勒冈）区域实施的任何运行状况检查结合使用，以将您的用户重定向到 WorkSpaces 您在美国东部（弗吉尼亚北部）区域为他们设置的区域。有关跨区域重定向体验的更多信息，请参阅跨区域重定向期间会发生什么。

> **Note**
>
> 如果您的 WorkSpaces 用户距离故障转移区域很远（例如，数千英里之外），则他们的 WorkSpaces 体验可能比平时响应不佳。要查看从您所在地前往各个Amazon地区的往返时间 (RTT)，请使用 A mazon Connection Healt WorkSpaces h Check。

将连接别名与目录关联

每个Amazon区域只能将一个连接别名与一个目录相关联。如果您与其他Amazon账户共享了连接别名，则只有一个账户（您的账户或共享账户）可以将该别名与该地区的目录相关联。

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在控制台的右上角，为您的选择主要Amazon区域。 WorkSpaces
3. 在导航窗格中，选择 Account Settings (账户设置)。
4. 在跨区域重定向关联下，选择连接字符串，然后选择操作、关联/取消关联。

   您也可以将连接别名与连接别名详细信息页面上的目录相关联。为此，请在关联的目录下，选择关联目录。
5. 在 “关联/取消关联” 页面的 “关联到目录” 下，选择要与该区域的连接别名关联的目录。Amazon

   > **Note**
   >
   > 如果您将Amazon托管 Microsoft AD 目录配置为多区域复制，则只有主区域中的目录可以与 Amazon WorkSpaces 一起使用。尝试在 Amazon 的复制区域中使用该目录 WorkSpaces 将失败。在复制的区域 WorkSpaces 内，亚马逊不支持使用Amazon托管 Microsoft AD 进行多区域复制。
6. 选择关联 。
7. 重复这些步骤，但是在中Step 2，请务必为您的选择故障转移区域 WorkSpaces。如果您有多个故障转移区域，请对每个故障转移区域重复这些步骤。请务必将相同的连接别名与每个故障转移区域中的目录相关联。

步骤 4：配置您的 DNS 服务并设置 DNS 路由策略

创建连接别名和连接别名关联对后，您可以为连接字符串中使用的域配置 DNS 服务。为此，您可以使用任何 DNS 服务提供商。如果您还没有首选 DNS 服务提供商，则可使用 Amazon Route 53。有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的将 Amazon Route 53 配置为 DNS 服务。

为域配置 DNS 服务后，您必须设置要用于跨区域重定向的 DNS 路由策略。例如，您可以使用 Amazon Route 53 运行状况检查来确定您的用户是否可以在特定区域连接到他们 WorkSpaces 。如果您的用户无法连接，则您可以使用 DNS 故障转移策略将 DNS 流量从一个区域路由到另一个区域。

有关选择 DNS 路由策略的更多信息，请参阅《Amazon Route 53 开发人员指南》中的选择路由策略。有关 Amazon Route 53 运行状况检查的更多信息，请参阅《Amazon Route 53 开发人员指南》中的 Amazon Route 53 如何检查资源的运行状况。

在设置 DNS 路由策略时，您需要连接别名与主区域中的 WorkSpaces 目录之间的关联的连接标识符。您还需要一个或多个故障转移区域中连接别名和 WorkSpaces 目录之间关联的连接标识符。

> **Note**
>
> 连接标识符与连接别名 ID 不同。连接别名 ID 以 `wsca-` 开头。

查找连接别名关联的连接标识符

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在控制台的右上角，为您的选择主要Amazon区域。 WorkSpaces
3. 在导航窗格中，选择 Account Settings (账户设置)。
4. 在跨区域重定向关联下，选择连接字符串文本 (FQDN)，以查看连接别名详细信息页面。
5. 在连接别名详细信息页面的关联的目录下，记下为连接标识符显示的值。
6. 重复这些步骤，但是在中Step 2，请务必为您的选择故障转移区域 WorkSpaces。如果您有多个故障转移区域，请重复这些步骤，查找每个故障转移区域的连接标识符。

示例：使用 Route 53 设置 DNS 故障转移路由策略

以下示例为您所在域设置了公有托管区。但是，您可以设置公有或私有托管区。有关设置托管区的更多信息，请参阅《Amazon Route 53 开发人员指南》中的使用托管区。

此示例还使用了故障转移路由策略。您可以将其他路由策略类型用于跨区域重定向策略。有关选择 DNS 路由策略的更多信息，请参阅《Amazon Route 53 开发人员指南》中的选择路由策略。

在 Route 53 中设置故障转移路由策略时，需要针对主区域进行运行状况检查。有关在 Route 53 中创建运行状况检查的更多信息，请参阅《Amazon Route 53 开发人员指南》中的创建 Amazon Route 53 运行状况检查和配置 DNS 故障转移以及创建、更新和删除运行状况检查。

如果您想在 Route 53 运行状况检查中使用 Amazon CloudWatch 警报，则还需要设置 CloudWatch 警报来监控主区域中的资源。有关的更多信息 CloudWatch，请参阅 Amazon 是什么 CloudWatch？ 在《亚马逊 CloudWatch 用户指南》中。有关 Route 53 如何在其运行状况检查中使用 CloudWatch 警报的更多信息，请参阅 Amazon Route 53 开发者指南中的 Route 53 如何确定监控 CloudWatch 警报的运行状况检查的状态和监控警 CloudWatch 报。

要在 Route 53 中设置 DNS 故障转移路由策略，您首先需要为您的域创建一个托管区。

1. 打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择托管区，然后选择创建托管区。
3. 在已创建的托管区页面上，在域名下输入您的域名（例如 `example.com`）。
4. 在类型下，选择公有托管区。
5. 选择创建托管区域。

然后为您的主区域创建运行状况检查。

1. 打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择运行状况检查，然后选择创建运行状况检查。
3. 在配置运行状况检查页面上，输入运行状况检查的名称。
4. 在要监控的内容中，选择终端节点、其他运行状况检查的状态（计算的运行状况检查）或 CloudWatch 警报状态。
5. 根据您在上一步中选择的内容，配置您的运行状况检查，然后选择下一步。
6. 在在运行状况检查失败时收到通知页面上，对于创建警报，选择是或否。
7. 选择创建运行状况检查。

在创建运行状况检查后，您可以创建 DNS 故障转移记录。

1. 打开 Route 53 控制台，网址为https://console.aws.amazon.com/route53/。
2. 在导航窗格中，选择 Hosted zones（托管区域）。
3. 在托管区页面上，选择您的域名。
4. 在域名的详细信息页面上，选择创建记录。

5. 在选择路由策略页面上，选择故障转移，然后选择下一步。
6. 在配置记录页面的基本配置下，对于记录名称，输入您的子域名。例如，如果您的 FQDN 是 `desktop.example.com`，请输入 **`desktop`**。

> **Note**
>
> 如果要使用根域，请将记录名称留空。但是，我们建议您使用子域名，例如`desktop`或`workspaces`，除非您已将该域名设置为仅用于您 WorkSpaces的。

7. 对于记录类型，选择 TXT - 用于验证电子邮件发件人和应用程序特定的值。
8. 将 TTL 秒设置保留为默认值。
9. 在 “要添加的故障切换记录” 下*`your_domain_name`*，选择 “定义故障切换记录”。

现在，您需要为主区域和故障转移区域设置故障转移记录。

示例：为您的主区域设置故障转移记录

1. 在定义故障转移记录对话框中，对于值/流量路由至，选择 IP 地址或其他值（具体取决于记录类型）。
2. 这时，将打开一个框供您输入示例文本条目。输入您主区域的连接别名关联的连接标识符。
3. 对于故障转移记录类型，选择主。
4. 在运行状况检查中，选择您为主区域创建的运行状况检查。
5. 对于记录 ID，输入描述以识别此记录。
6. 选择定义故障转移记录。您的新故障转移记录将显示在要添加的故障转移记录下*`your_domain_name`*。

示例：为您的故障转移区域设置故障转移记录

1. 在 “要添加的故障切换记录” 下*`your_domain_name`*，选择 “定义故障切换记录”。
2. 在定义故障转移记录对话框中，对于值/流量路由至，选择 IP 地址或其他值（具体取决于记录类型）。
3. 这时，将打开一个框供您输入示例文本条目。输入故障转移区域的连接别名关联的连接标识符。
4. 对于故障转移记录类型，选择辅助。
5. （可选）对于运行状况检查，输入您为故障转移区域创建的运行状况检查。
6. 对于记录 ID，输入描述以识别此记录。

7. 选择定义故障转移记录。您的新故障转移记录将显示在要添加的故障转移记录下*your_domain_name*。

如果您为主区域设置的运行状况检查失败，则您的 DNS 故障转移路由策略会将您的 WorkSpaces 用户重定向到您的故障转移区域。Route 53 继续监控您的主要区域的运行状况检查，当您的主区域的运行状况检查不再失败时，Route 53 会自动将您的 WorkSpaces 用户重定向回主区域 WorkSpaces 中的用户。

有关创建 DNS 记录的更多信息，请参阅《Amazon Route 53 开发人员指南》中的使用 Amazon Route 53 控制台创建记录。有关配置 DNS TXT 记录的更多信息，请参阅《Amazon Route 53 开发人员指南》中的 TXT 记录类型。

步骤 5：向您的 WorkSpaces 用户发送连接字符串

要确保在中断期间根据需要重定向用户，您必须 WorkSpaces 将连接字符串 (FQDN) 发送给您的用户。如果您已经向 WorkSpaces 用户发布了基于区域的注册码（例如`WSpdx+ABC12D`），则这些代码仍然有效。但是，要使跨区域重定向起作用，您的 WorkSpaces 用户在 WorkSpaces 客户端应用程序 WorkSpaces 中注册时必须使用连接字符串作为注册码。

> **Important**
>
> 如果您在 WorkSpaces 控制台中创建用户而不是在 Active Directory 中创建用户，则每当您启动新用户时，都会 WorkSpaces 自动向您的用户发送一封包含基于区域的注册码（例如`WSpdx+ABC12D`）的邀请电子邮件。 WorkSpace即使您已经设置了跨区域重定向，自动发送的新版邀请电子邮件也 WorkSpaces 包含此基于区域的注册码，而不是您的连接字符串。
> 要确保您的 WorkSpaces 用户使用的是连接字符串而不是基于区域的注册码，您必须按照以下步骤向他们发送另一封包含连接字符串的电子邮件。

向您的 WorkSpaces 用户发送连接字符串

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在控制台的右上角，为您的选择主要Amazon区域。 WorkSpaces
3. 在导航窗格中，请选择 WorkSpaces。
4. 在该WorkSpaces页面上，使用搜索框搜索要向其发送邀请的用户，然后 WorkSpace 从搜索结果中选择相应的用户。 WorkSpace 一次只能选择一个。
5. 依次选择 Actions (操作) 和 Invite User (邀请用户)。

6. 在邀请用户加入他们的 WorkSpaces页面上，您将看到一个要发送给用户的电子邮件模板。
7. （可选）如果有多个连接别名与您的 WorkSpaces 目录相关联，请从 Connection 别名字符串列表中选择您希望用户使用的连接字符串。电子邮件模板将更新以显示您选择的字符串。
8. 使用您自己的电子邮件应用程序，复制电子邮件模板文本，并将其粘贴到要发送给用户的电子邮件中。在电子邮件应用程序中，您可以根据需要修改文本。当邀请电子邮件准备就绪之后，将其发送给用户。

跨区域重定向架构图

下图描述了跨区域重定向的部署过程。

> **Note**
>
> 跨区域重定向只能推动跨区域故障转移和回退。它不利于 WorkSpaces 在辅助区域中创建和维护，也不允许跨区域数据复制。 WorkSpaces 在主区域和次要区域中，都应分开管理。

启动跨区域重定向

发生中断时，您可以手动更新 DNS 记录，也可以使用基于运行状况检查的自动路由策略，从而确定故障转移区域。建议您遵循使用 Amazon Route 53 创建灾难恢复机制中概述的灾难恢复方法。

跨区域重定向期间会发生什么

在区域故障转移期间，您的 WorkSpaces 用户将与主区域 WorkSpaces 的用户断开连接。当他们尝试重新连接时，会收到以下错误消息：

```
We can't connect to your WorkSpace. Check your network connection, and then
try again.
```

然后，系统会提示您的用户重新登录。如果他们使用 FQDN 作为注册码，则当他们再次登录时，您的 DNS 故障转移路由策略会将他们重定向到您在故障转移区域中为他们设置的路由策略。 WorkSpaces

> **Note**
>
> 在某些情况下，用户在再次登录时可能无法重新连接。如果出现这种情况，他们必须关闭并重新启动 WorkSpaces 客户端应用程序，然后尝试再次登录。

取消连接别名与目录的关联

只有拥有目录的账户才能取消连接别名与该目录的关联。

如果您已与另一个账户共享连接别名，并且该账户已将连接别名与该账户拥有的目录关联，则必须使用该账户，取消连接别名与该目录的关联。

取消连接别名与目录的关联

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在控制台的右上角，选择包含要取消关联的连接别名的Amazon区域。
3. 在导航窗格中，选择 Account Settings (账户设置)。
4. 在跨区域重定向关联下，选择连接字符串，然后选择操作、关联/取消关联。

   您也可以取消连接别名与连接别名详细信息页面的关联。为此，请在关联的目录下，选择取消关联。
5. 在关联/取消关联页面上，选择取消关联。
6. 在要求您确认取消关联的对话框中，选择取消关联。

取消共享连接别名

只有连接别名的所有者才能取消共享该别名。如果您取消与某个账户共享连接别名，则该账户将无法再将该连接别名与目录相关联。

取消共享连接别名

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在控制台的右上角，选择包含要取消共享的连接别名的Amazon区域。
3. 在导航窗格中，选择 Account Settings (账户设置)。
4. 在跨区域重定向关联下，选择连接字符串，然后选择操作、共享/取消共享连接别名。

   您也可以取消连接别名与连接别名详细信息页面的共享。为此，请在共享账户下选择取消共享。
5. 在共享/取消共享连接别名页面上，选择取消共享。
6. 在要求您确认取消共享连接别名的对话框中，选择取消共享。

删除连接别名

只有当连接别名归您的账户所有且未与目录关联时，您才能删除该别名。

如果您已与另一个账户共享连接别名，并且该账户已将连接别名与该账户拥有的目录关联，则该账户必须先取消连接别名与目录的关联，然后您才能删除该别名。

> **Important**
>
> 创建连接字符串后，它始终与您的Amazon账户关联。您无法使用其他账户重新创建相同的连接字符串，即使您从原始账户中删除了连接字符串的所有实例也是如此。连接字符串针对您的账户进行了全局保留。

> **Warning**
>
> 如果您不再使用 FQDN 作为 WorkSpaces 用户的注册码，则必须采取某些预防措施来防止出现潜在的安全问题。有关更多信息，请参阅 停止使用跨区域重定向后的安全注意事项。

删除连接别名

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在控制台的右上角，选择包含要删除的连接别名的Amazon区域。
3. 在导航窗格中，选择 Account Settings (账户设置)。
4. 在跨区域重定向关联下，选择连接字符串，然后选择删除。

   您也可以从连接别名详细信息页面删除连接别名。为此，请在页面右上角，选择删除。

   > **Note**
   >
   > 如果禁用删除按钮，请确保您是别名的所有者，并确保该别名未与目录关联。

5. 在要求您确认删除的对话框中，选择删除。

用于关联和取消关联连接别名的 IAM 权限

如果您使用 IAM 用户关联或取消关联连接别名，则该用户必须拥有 `workspaces:AssociateConnectionAlias` 和 `workspaces:DisassociateConnectionAlias` 的权限。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "workspaces:AssociateConnectionAlias",
        "workspaces:DisassociateConnectionAlias"
      ],
      "Resource": [
          "arn:aws:workspaces:us-east-1:123456789012:connectionalias/wsca-
a1bcd2efg"
      ]
    }
  ]
}
```

> **Important**
>
> 如果您正在创建 IAM 策略来关联或取消关联不拥有连接别名的账户的连接别名，则无法在 ARN 中指定账户 ID。您必须改用账户 ID 的 *，如以下示例策略所示。
>
> JSON
>
> ```
> {
>  "Version":"2012-10-17",
>  "Statement": [
>  {
>  "Effect": "Allow",
>  "Action": [
> ```

```
            "workspaces:AssociateConnectionAlias",
            "workspaces:DisassociateConnectionAlias"
        ],
        "Resource": [
            "arn:aws:workspaces:us-east-1:*:connectionalias/wsca-a1bcd2efg"
        ]
      }
    ]
}
```

只有当账户拥有要关联或取消关联的连接别名时，您才能在 ARN 中指定该账户 ID。

有关使用 IAM 的更多信息，请参阅 的身份和访问管理 WorkSpaces。

停止使用跨区域重定向后的安全注意事项

如果您不再使用 FQDN 作为 WorkSpaces 用户的注册码，则必须采取以下预防措施来防止出现潜在的安全问题：

- 请务必向 WorkSpaces 用户发放其 WorkSpaces 目录中特定于区域的注册码（例如`WSpdx+ABC12D`），并指示他们停止使用 FQDN 作为注册码。
- 如果您仍然拥有该域，请务必更新您的 DNS TXT 记录以删除该域，这样它就不会在网络钓鱼攻击中遭到利用。如果您从 DNS TXT 记录中删除此域名，而您的 WorkSpaces 用户尝试使用 FQDN 作为注册码，则他们的连接尝试将无害地失败。
- 如果您不再拥有该域名，则您的 WorkSpaces 用户必须使用其区域特定的注册码。如果他们继续尝试使用 FQDN 作为注册码，则系统可能会将其连接尝试重定向到恶意站点。

个人的多区域弹性 WorkSpaces

Amazon WorkSpaces 多区域弹性 (MRR) 使您能够在主区域因中断性事件而无法访问时将用户重定向到辅助 WorkSpaces 区域，而无需您的用户在登录到备用区域时切换注册码。 WorkSpaces待机 WorkSpaces 是 Amazon WorkSpaces 多区域弹性的一项功能，可简化备用部署的创建和管理。在辅助区域设置用户目录后，在主区域中选择要 WorkSpace 为其创建备用目录的用户目录。 WorkSpace 系统会自动将主 WorkSpace 捆绑包映像镜像到次要区域。然后，它会在您的辅助区域自动配置新的备用 WorkSpace 副本

Amazon WorkSpaces 多区域弹性建立在跨区域重定向的基础上，利用 DNS 运行状况检查和故障转移功能。它允许您使用完全限定的域名 (FQDN) 作为 WorkSpaces 注册码。当您的用户登录时 WorkSpaces，您可以根据您的 FQDN 域名系统 (DNS) 策略将他们重定向到支持的 WorkSpaces 区域。如果您使用 Amazon Route 53，我们建议您在为其设计跨区域重定向策略时使用运行状况检查来监控亚马逊 CloudWatch 警报。 WorkSpaces有关更多信息，请参阅《Amazon Route 53 开发人员指南》中的创建 Amazon Route 53 运行状况检查和配置 DNS 故障转移。

数据复制是备用模式的一项附加功能 WorkSpaces ，可将数据从主区域单向复制到辅助区域。启用数据复制后，系统和用户卷的 EBS 快照每 12 小时拍摄一次。多区域韧性会定期检查是否有新的快照。找到快照后，它会启动到辅助区域的副本。当副本到达辅助区域时，它们被用来更新辅助区域 WorkSpace。

内容

- 前提条件
- 限制
- 配置您的多区域弹性备用模式 WorkSpace
- 创建备用副本 WorkSpace
- 管理待机模式 WorkSpace
- 删除备用副本 WorkSpace
- 备用单向数据复制 WorkSpaces
- 计划预留 Amazon EC2 容量以备恢复

前提条件

- 在创建备用 WorkSpaces 服务器之前，您必须为主区域中的用户创建 WorkSpaces。有关创建的更多信息 WorkSpaces，请参阅为 WorkSpaces 个人版创建目录。
- 要在待机状态下启用数据复制 WorkSpaces，您应该将自我管理的 Active Directory 或Amazon托管 Microsoft AD 配置为复制到备用区域。有关更多信息，请参阅创建您的Amazon托管 Microsoft AD 目录和添加复制区域。
- 确保在主服务器上更新网络依赖驱动程序 NVMe，例如 ENA 和 PV 驱动程序 WorkSpaces。您应该至少每 6 个月更新一次。有关更多信息，请参阅安装或升级弹性网络适配器（ENA）驱动程序、Windows 实例的 Amazon NVMe 驱动程序以及升级 Windows 实例上的 PV 驱动程序。
- 确保定期将 EC2 Config、 EC2 Launc EC2 h 和 Launch V2 代理更新到最新版本。您应该至少每 6 个月更新一次。有关更多信息，请参阅更新 EC2 Config 并 EC2启动。

- 为了保障正确的数据复制，请确保主区域和辅助区域中的 Active Directory 与 FQDN、OU 和用户 SID 同步。
- 备用服务器的默认配额（限制） WorkSpaces 为 0。在创建备用副本之前，您需要申请增加服务配额 WorkSpace。有关更多信息，请参阅 Amazon WorkSpaces 配额。
- 确保使用客户管理的密钥对主密钥和备用密钥进行加密 WorkSpaces。您可以使用单区域密钥或多区域密钥来加密您的主密钥和备用 WorkSpaces密钥。

限制

- 待机模式 WorkSpaces 仅复制主卷的捆绑映像， WorkSpaces 但不会从主卷复制系统卷（驱动器 C）或用户卷（驱动器 D） WorkSpaces。要将系统卷（驱动器 C）或用户卷（驱动器 D）从主卷复制 WorkSpaces 到备用卷 WorkSpaces，必须启用数据复制。
- 您不能直接修改、重建、恢复或迁移备用副本 WorkSpace。
- 跨区域重定向的故障转移由您的 DNS 设置控制。要实施自动故障转移场景，您必须将其他机制与跨区域重定向结合使用。例如，您可以将 Amazon Route 53 故障转移 DNS 路由策略与监控主区域 CloudWatch 警报的 Route 53 运行状况检查配对。如果在主区域中调用 CloudWatch 警报，则您的 DNS 故障转移路由策略会将您的 WorkSpaces 用户重定向到您在故障转移区域中为他们设置的策略。 WorkSpaces
- 数据复制只有一种方式，即将数据从主区域复制到辅助区域。在待机 WorkSpaces 故障转移期间，您可以在 12 到 24 小时之间访问数据和应用程序。中断后，手动备份您在辅助服务器上创建的所有数据 WorkSpace 并注销。我们建议将您的工作保存到外部驱动器（例如网络驱动器）中，以便您可以从主驱动器访问数据 WorkSpace。
- 数据复制不支持 S Amazon imple AD。
- 在备用模式下启用数据复制时 WorkSpaces，将每 12 小时拍摄一次主卷 WorkSpaces （包括根卷和系统卷）的 EBS 快照。特定数据卷的初始快照已满，后续快照为增量快照。因此，给定对象的第一次复制 WorkSpace 将比后续复制花费更长的时间。快照是按内部计划启动的 WorkSpaces ，您无法控制时间。
- 如果主域 WorkSpace 和备用域使用同一个域 WorkSpace 加入，我们建议您只 WorkSpace 在给定的时间点连接到主域 WorkSpace 或备用域控制器，以免失去与域控制器的连接。
- 如果您将您的配置Amazon Managed Microsoft AD为多区域复制，则只能注册主区域中的目录以供使用 WorkSpaces。如果您尝试在复制区域中注册该目录以供使用 WorkSpaces，则该目录将失败。Amazon Managed Microsoft AD不支持在复制的区域 WorkSpaces 内使用多区域复制。
- 如果您已经设置了跨区域重定向，并在不使用备用区域的情况下 WorkSpaces 在主区域和次要区域中创建了跨区域重定向 WorkSpaces，则无法将辅助区域 WorkSpace 中的现有重定向直接转换为备

用 WorkSpace 区域。相反，您需要关闭辅助区域 WorkSpace 中的，在主区域中选择要 WorkSpace 为其创建备用副本的区域，然后使用备用创建备 WorkSpaces 用副本 WorkSpace。 WorkSpace

- 中断后，手动备份您在辅助服务器上创建的所有数据 WorkSpace 并注销。我们建议将您的工作保存到外部驱动器（例如网络驱动器）中，以便您可以从主驱动器访问数据 WorkSpace。
- WorkSpaces 多区域弹性目前在以下区域可用：
  - 美国东部（弗吉尼亚州北部）区域
  - 美国西部（俄勒冈州）区域
  - 欧洲地区（法兰克福）区域
  - 欧洲地区（爱尔兰）区域
- WorkSpaces 只有版本 3.0.9 或更高版本的 Linux、macOS 和 Windows 客户端应用程序支持多区域弹性。 WorkSpaces 您也可以将多区域韧性与 Web Access 结合使用。
- WorkSpaces 多区域弹性支持 Windows 和自带许可证 (BYOL)。 WorkSpaces它不支持亚马逊 Linux 2、Ubuntu、Red Hat Enterprise Linux WorkSpaces、 GeneralPurpose .4xlarge、. GeneralPurpose 8xlarge 或支持 GPU（例如 Graphics、G WorkSpaces raphics.g4dn 或.g4dn）。 GraphicsPro GraphicsPro
- 故障转移或故障恢复完成后，请等待 15 到 30 分钟，然后再连接到您的 WorkSpace。

配置您的多区域弹性备用模式 WorkSpace

配置您的多区域弹性备用副本 WorkSpace

1. 在主区域和辅助区域中设置用户目录。确保在每个区域的每个 WorkSpaces 目录中使用相同的用户名。

   为了保持您的 Active Directory 用户数据同步，我们建议您使用 AD Connector 指向您 WorkSpaces 为用户设置的每个区域中的同一个活动目录。有关创建目录的更多信息，请参阅向注册目录 WorkSpaces。

   > **Important**
   >
   > 如果您将Amazon Managed Microsoft AD目录配置为多区域复制，则只能注册主区域中的目录以供使用 WorkSpaces。尝试在复制的区域中注册该目录以供使用 WorkSpaces 将失败。Amazon Managed Microsoft AD不支持在复制的区域 WorkSpaces 内使用多区域复制。

2. WorkSpaces 为主区域的用户创建。有关创建的更多信息 WorkSpaces，请参阅 Launch WorkSpaces。
3. WorkSpace 在辅助区域创建备用副本。有关创建备用副本的更多信息 WorkSpace，请参阅创建备用实例 WorkSpace。
4. 创建连接字符串（FQDN），并将其与主区域和辅助区域中的用户目录相关联。

   您必须在账户中启用跨区域重定向，因为备用数据库建立在跨区域重 WorkSpaces 定向的基础上。按照 Amazon 跨区域重定向说明中的步骤 1-3 进行操作。 WorkSpaces
5. 配置 DNS 服务并设置 DNS 路由策略。

   您必须设置 DNS 服务并配置必要的 DNS 路由策略。跨区域重定向与您的 DNS 路由策略配合使用，可根据需要重定向您的 WorkSpaces 用户。
6. 设置完跨区域重定向后，您必须向用户发送一封包含 FQDN 连接字符串的电子邮件。有关更多信息，请参阅步骤 5：向您的 WorkSpaces 用户发送连接字符串。确保您的 WorkSpaces 用户使用的是基于 FQDN 的注册码，而不是其主要区域的基于区域的注册码（例如 WSpdx + ABC12 D）。

> **Important**
>
> - 如果您在 WorkSpaces 控制台中创建用户而不是在 Active Directory 中创建用户，则每当您启动新用户时，都会 WorkSpaces 自动向您的用户发送一封包含基于区域的注册码的邀请电子邮件。 WorkSpace这意味着，当你 WorkSpaces 为次要区域的用户进行设置时，你的用户也将自动收到这些辅助区域的电子邮件 WorkSpaces。您需要指示您的用户忽略含有基于区域的注册码的电子邮件。
> - 特定于区域的注册码仍然有效；但是，要使跨区域重定向运行，您的用户必须改用 FQDN 作为注册码。

创建备用副本 WorkSpace

在创建备用副本之前 WorkSpace，请确保已完成先决条件，包括在主区域和次要区域中创建用户目录、在主区域 WorkSpaces 为用户进行配置、在账户中配置跨区域重定向以及通过服务配额请求提高待机 WorkSpaces 限制。

创建备用副本 WorkSpace

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。

2. 在控制台的右上角，为您的选择主要Amazon区域。 WorkSpaces
3. 在导航窗格中，请选择 WorkSpaces。
4. 选择 WorkSpace 要为其创建备用副 WorkSpace 本的。
5. 选择 “操作”，然后选择 “创建待机” WorkSpace。
6. 选择要在其中创建备用副本的次要区域 WorkSpace，然后选择 “下一步”。
7. 选择辅助区域中的用户目录，然后选择下一步。
8. （可选）添加加密密钥、启用数据加密和管理标签。

   - 要添加加密密钥，请在“输入加密密钥”下方输入该密钥。
   - 要启用数据复制，请选择启用数据复制。然后，选中复选框以确认您批准额外每月收费。
   - 要添加新标签，请选择添加新标签。

   然后选择下一步。

   > **Note**
   >
   > - 如果原始文件已加密， WorkSpace 则会预填充此字段。但是，您可以选择将其替换为自己的加密密钥。
   > - 更新数据复制状态需要花几分钟时间。
   > - 使用主数据库的快照成功更新备用数据库 WorkSpace 后 WorkSpace，您可以在恢复快照下找到快照的时间戳。

9. 查看待机模式的设置， WorkSpaces 然后选择 “创建”。

   > **Note**
   >
   > - 要查看您的待机信息 WorkSpaces，请前往主要 WorkSpace 详情页面。
   > - 备用磁盘 WorkSpace 仅复制主卷的捆绑映像， WorkSpace 但不会从主卷复制系统卷（驱动器 C）或用户卷（驱动器 D） WorkSpaces。默认情况下，数据复制处于关闭状态。要将系统卷（驱动器 C）或用户卷（驱动器 D）从主卷复制 WorkSpaces 到备用卷 WorkSpaces，必须启用数据复制。

管理待机模式 WorkSpace

您不能直接修改、重建、恢复或迁移备用副本 WorkSpace。

为备用服务器启用数据复制 WorkSpace

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 前往您的主要区域，选择主 WorkSpace ID。
3. 向下滚动到 “待机 WorkSpace ” 部分，然后选择 “编辑待机” WorkSpace。
4. 选择启用数据复制。然后，选中复选框以确认您批准额外每月收费。然后，选择保存。

> **Note**
>
> - 待机模式 WorkSpaces 无法休眠。如果您停止待机模式 WorkSpace，它不会保留您未保存的工作。我们建议用户在退出待机状态 WorkSpaces之前务必保存所做的工作。
> - 要在待机状态下启用数据复制 WorkSpaces，您应该将自我管理的 Active Directory 或 Amazon托管 Microsoft AD 配置为复制到备用区域。要设置您的目录，请按照 “使用亚马逊 WorkSpaces 和Amazon目录服务构建业务连续性演练” 部分的步骤 1 至 3 或参阅在亚马逊使用多区域Amazon托管 Active D irectory。 WorkSpaces只有 Amazon 托管 Microsoft AD 的企业版支持多区域复制。
> - 更新数据复制状态需要花几分钟时间。
> - 使用主数据库的快照成功更新备用数据库 WorkSpace 后 WorkSpace，您可以在恢复快照下找到快照的时间戳。

删除备用副本 WorkSpace

您可以像终止常规备用 WorkSpace 服务器一样终止备用副本 WorkSpace。

删除备用副本 WorkSpace

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在控制台的右上角，为您的选择主要Amazon区域。 WorkSpaces
3. 在导航窗格中，请选择 WorkSpaces。

4. 选择待机模式 WorkSpace 并选择 “删除”。删除备用副本大约需要 5 分钟 WorkSpace。在删除过程中，备用服务器的状态 WorkSpace 将设置为 “正在终止”。删除完成后，备用数据库将从控制台 WorkSpace 消失。

> **Note**
>
> 删除备用数据库 WorkSpace 是一项永久性操作，无法撤消。备用 WorkSpace 用户的数据不会保留，因此会被销毁。如需有关备份用户数据的帮助，请联系 Supp Amazon ort。

备用单向数据复制 WorkSpaces

在多区域韧性中启用数据复制允许您将数据从主区域复制到辅助区域。在稳定状态下，多区域弹性 WorkSpaces 每 12 小时捕获一次主系统的快照（C 盘）和数据（D 盘）的快照。这些快照将传输到辅助区域并用于更新备用区域 WorkSpaces。默认情况下，待机状态的数据复制处于禁用状态 WorkSpaces。

为备用数据库启用数据复制后 WorkSpaces，特定数据卷的初始快照即已完成，而后续快照为增量快照。因此，给定对象的第一次复制 WorkSpace 将比后续复制花费更长的时间。快照是在预先确定的时间间隔内 WorkSpaces 触发的，用户无法控制时间。

在故障转移期间，当用户被重定向到辅助区域时，他们可以访问其备 WorkSpaces 用区域，其中包含保存 12 到 24 小时的数据和应用程序。当用户使用备用模式时 WorkSpaces，多区域弹性不会强迫他们退出备用数据库 WorkSpaces 或使用主区域的快照更新备 WorkSpaces 用副本。

中断后，用户在注销备用服务器 WorkSpaces 之前，应手动备份他们在辅助设备上创建的所有数据 WorkSpaces。当他们再次登录时，他们将被定向到主区域及其主区域 WorkSpaces。

计划预留 Amazon EC2 容量以备恢复

默认情况下，亚马逊多区域弹性 (MRR) 依赖于亚马逊 EC2 按需池。如果特定的 Amazon EC2 实例类型无法支持您的恢复，MRR 将自动尝试重复扩展实例，直到找到可用的实例类型，但在极端情况下，实例可能并不总是可用。要提高最关键实例类型的可用性，请联系 Supp WorkSpaces ortAmazon，我们将协助您进行容量规划。

WorkSpaces 个人版问题疑难解答

以下信息可以帮助您解决您的问题 WorkSpaces。

启用高级日志记录

为了帮助解决您的用户可能遇到的问题，您可以在任何 Amazon WorkSpaces 客户端上启用高级登录。

高级日志记录将生成包含诊断信息和调试级别详细信息（包括详细的性能数据）的日志文件。对于 1.0+ 和 2.0+ 的客户端，这些高级日志文件会自动上传到中的数据库。Amazon

> **Note**
>
> 要Amazon查看高级日志文件并获得有关 WorkSpaces 客户问题的技术支持，请联系Amazon Web Services 支持。有关更多信息，请参阅 Amazon Web Services 支持 中心。

为 Web Access 启用高级日志记录

为 Web Access 启用高级日志记录

1. 打开您的亚马逊 WorkSpaces 网络访问客户端。
2. 在 WorkSpaces 登录页面的顶部，选择诊断日志。
3. 在弹出对话框中，确保已启用诊断日志记录。
4. 对于日志级别，请选择高级日志记录。

在 Google Chrome、Microsoft Edge 和 Firefox 中访问日志文件

1. 打开浏览器上的上下文（右键单击）菜单或按键盘上的 Ctrl + Shift + I（或者对于 Mac，按 command + option + I），打开开发人员工具面板。
2. 在开发人员工具面板中，选择控制台选项卡以查找日志文件。

在 Safari 中访问日志文件

1. 依次选择 Safari、设置。
2. 在设置窗口中，选择高级选项卡。
3. 在菜单栏中选择“显示开发”菜单。
4. 从菜单栏的开发选项卡中，选择开发 > 显示 Web 检查器。
5. 在 Safari Web 检查器面板中，选择控制台选项卡以查找日志文件。

为 4.0+ 客户端启用高级日志记录

Windows 客户端日志存储在以下位置：

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs
```

为 Windows 客户端启用高级日志记录

1. 关闭亚马逊 WorkSpaces 客户端。
2. 打开命令提示符应用程序。
3. 启动带有`-l3`标志的 WorkSpaces 客户端。

```
c:

cd "C:\Program Files\Amazon Web Services, Inc\Amazon WorkSpaces"

workspaces.exe -l3
```

> **Note**
>
> 如果 WorkSpaces 是为一个用户而不是所有用户安装的，请使用以下命令：
>
> ```
> c:
> cd "%LocalAppData%\Programs\Amazon Web Services, Inc\Amazon
> WorkSpaces"
> workspaces.exe -l3
> ```

macOS 客户端日志存储在以下位置：

```
~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/
logs
```

为 macOS 客户端启用高级日志记录

1. 关闭亚马逊 WorkSpaces 客户端。
2. 打开终端。
3. 运行如下命令。

```
open -a workspaces --args -l3
```

为 Android 客户端启用高级日志记录

1. 关闭亚马逊 WorkSpaces 客户端。
2. 打开 Android 客户端菜单。
3. 选择支持。
4. 选择日志记录设置。
5. 选择启用高级日志记录。

要在启用高级日志记录后检索 Android 客户端的日志，请执行以下操作：

- 选择提取日志，将压缩后的日志保存在本地。

Linux 客户端日志存储在以下位置：

```
~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs
```

为 Linux 客户端启用高级日志记录

1. 关闭亚马逊 WorkSpaces 客户端。
2. 打开终端。
3. 运行如下命令。

   ```
   /opt/workspacesclient/workspacesclient -l3
   ```

为 3.0 客户端启用高级日志记录

Windows 客户端日志存储在以下位置：

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\logs
```

为 Windows 客户端启用高级日志记录

1. 关闭亚马逊 WorkSpaces 客户端。
2. 打开命令提示符应用程序。
3. 启动带有`-l3`标志的 WorkSpaces 客户端。

   ```
   c:
   ```

```
cd "C:\Program Files (x86)\Amazon Web Services, Inc\Amazon WorkSpaces"

workspaces.exe -l3
```

> **Note**
>
> 如果 WorkSpaces 是为一个用户而不是所有用户安装的，请使用以下命令：
>
> ```
> c:
> cd "%LocalAppData%\Programs\Amazon Web Services, Inc\Amazon WorkSpaces"
> workspaces.exe -l3
> ```

macOS 客户端日志存储在以下位置：

```
~/Library/"Application Support"/"Amazon Web Services"/"Amazon WorkSpaces"/logs
```

为 macOS 客户端启用高级日志记录

1. 关闭亚马逊 WorkSpaces 客户端。
2. 打开终端。
3. 运行如下命令。

   ```
   open -a workspaces --args -l3
   ```

为 Android 客户端启用高级日志记录

1. 关闭亚马逊 WorkSpaces 客户端。
2. 打开 Android 客户端菜单。
3. 选择支持。
4. 选择日志记录设置。
5. 选择启用高级日志记录。

要在启用高级日志记录后检索 Android 客户端的日志，请执行以下操作：

- 选择提取日志，将压缩后的日志保存在本地。

Linux 客户端日志存储在以下位置：

```
~/.local/share/Amazon Web Services/Amazon WorkSpaces/logs
```

为 Linux 客户端启用高级日志记录

1. 关闭亚马逊 WorkSpaces 客户端。
2. 打开终端。
3. 运行如下命令。

   ```
   /opt/workspacesclient/workspacesclient -l3
   ```

为 1.0+ 和 2.0+ 客户端启用高级日志记录

1. 打开 WorkSpaces 客户端。
2. 选择客户端应用程序右上角的齿轮图标。
3. 选择 Advanced Settings (高级设置)。
4. 选中 Enable Advanced Logging (启用高级日志记录) 复选框。
5. 选择保存。

Windows 客户端日志存储在以下位置：

```
%LOCALAPPDATA%\Amazon Web Services\Amazon WorkSpaces\1.0\Logs
```

macOS 客户端日志存储在以下位置：

```
~/Library/Logs/Amazon Web Services/Amazon WorkSpaces/1.0
```

排查特定问题

以下信息可以帮助您解决与您的特定问题有关的问题 WorkSpaces。

问题

- 我无法创建 Amazon Linux， WorkSpace 因为用户名中有无效字符
- 我为我的 Amazon Linux WorkSpace 更换了外壳，现在我无法配置 PCo IP 会话
- 我的 Amazon Linux WorkSpaces 无法启动
- WorkSpaces 在我连接的目录中启动经常失败
- 启动 WorkSpaces 失败并出现内部错误

- 当我尝试注册目录时，注册失败并使该目录处于 ERROR 状态
- 我的用户无法使用交互式登录横 WorkSpace 幅连接到 Windows
- 我的用户无法连接到 Windows WorkSpace
- 在返回登录屏幕之前，Amazon WorkSpaces 客户端会显示灰色的 “正在加载...” 屏幕一段时间。不显示其他错误消息。
- 我的用户收到消息 “WorkSpace 状态：不健康。我们无法将您连接到您的 WorkSpace。请过几分钟再试。”
- 我的用户会收到消息 “此设备无权访问 WorkSpace. 请联系您的管理员寻求帮助。”
- 我的用户在尝试连接到 WSP WorkSpace 时收到消息 “无网络。网络连接中断。请检查网络连接 尝试连接 DCV 时 WorkSpace
- WorkSpaces 客户端给我的用户带来了网络错误，但他们可以在自己的设备上使用其他支持网络的应用程序
- 我的 WorkSpace 用户看到以下错误消息：“设备无法连接到注册服务。请检查网络设置。”
- 我 PCo的 IP zero 客户端用户收到错误 “由于时间戳的原因，提供的证书无效”
- USB 打印机和其他 USB 外围设备不适用于 PCo IP 零客户端
- 我的用户跳过了更新其 Windows 或 macOS 客户端应用程序的过程，并且没有收到安装最新版本的提示
- 我的用户没有收到邀请电子邮件或密码重置电子邮件
- 我的用户在客户端登录屏幕上看不到“忘记密码？”选项
- 当我尝试在 Windows 上安装应用程序时，我收到 “系统管理员已设置策略来阻止此安装” 的消息 WorkSpace
- 我的目录 WorkSpaces 中没有可以连接到互联网
- 我的 WorkSpace 已经失去了互联网接入
- 当我尝试连接我的本地目录时收到一条“DNS unavailable”错误
- 在尝试连接到我的本地目录时，我收到一条“Connectivity issues detected”错误
- 在尝试连接到我的本地目录时，我收到一条“SRV record”错误
- 我的 Windows 闲置时会 WorkSpace 进入睡眠状态
- 我的其中 WorkSpaces 一个状态为 UNHEALTHY
- 我的 WorkSpace 意外崩溃或重启
- 同一个用户名有多个用户名 WorkSpace，但用户只能登录其中一个 WorkSpaces
- 我在亚马逊上使用 Docker 时遇到了问题 WorkSpaces

- 我的一些 API 调用收到了 ThrottlingException 错误
- 当我 WorkSpace 让它在后台运行时，我的连接一直处于断开状态
- SAML 2.0 联合身份验证不起作用。我的用户无权直播其 WorkSpaces 桌面。
- 我的用户每 60 分钟就会断开一次 WorkSpaces 会话连接。
- 我的用户在使用 SAML 2.0 身份提供商 (IdP) 启动的流程进行联合时会收到重定向 URI 错误，或者我的用户在联合到 IdP 后每次尝试从 WorkSpaces 客户端登录时，都会启动客户端应用程序的另一个实例。
- 我的用户在联合到 IdP 后尝试登录 WorkSpaces 客户端应用程序时，他们会收到一条消息：“出了点问题：启动你的应用程序时出错 WorkSpace”。
- 我的用户在联合到 IdP 后尝试登录 WorkSpaces 客户端应用程序时会收到 “无法验证标签” 的消息。
- 我的用户会收到消息“客户端和服务器无法通信，因为它们没有共同的算法”。
- 我的麦克风或网络摄像头无法在 Windows 上运行 WorkSpaces。
- 我的用户无法使用基于证书的身份验证登录，当他们连接到桌面会话时，系统会在 WorkSpaces 客户端或 Windows 登录屏幕上提示他们输入密码。
- 我正在尝试做一些需要 Windows 安装介质但 WorkSpaces 不提供安装介质的事情。
- 我想 WorkSpaces 使用在不支持的 WorkSpaces 地区创建的现有Amazon托管目录启动。
- 我想在 Amazon Linux 2 上更新 Firefox。
- 我的用户可以使用 WorkSpaces 客户端重置密码，而忽略上配置的细粒度密码策略 (FFGP) 设置。Amazon Managed Microsoft AD

我无法创建 Amazon Linux， WorkSpace 因为用户名中有无效字符

对于亚马逊 Linux WorkSpaces，用户名：

- 最多可包含 20 个字符
- 可以包含能够以 UTF-8 表示的字母、空格和数字
- 可包含以下特殊字符：_ .-#
- 不能以短划线符号 (-) 作为用户名的开头第一个字符

> **Note**
>
> 这些限制不适用于 Windows WorkSpaces。Windows WorkSpaces 支持对用户名中的所有字符使用 @ 和-符号。

我为我的 Amazon Linux WorkSpace 更换了外壳，现在我无法配置 PCo IP 会话

要覆盖 Linux 的默认外壳 WorkSpaces，请参见替换亚马逊 Linux 的默认外壳 WorkSpaces。

我的 Amazon Linux WorkSpaces 无法启动

从 2020 年 7 月 20 日起，亚马逊 Linux WorkSpaces 将使用新的许可证书。这些新证书仅与 IP 代理的 2.14.1.1、2.14.7、2.14.9 和 20.10.6 或更高版本兼容。 PCo

如果您使用 PCo的 IP 代理版本不受支持，则必须将其升级到最新版本 (20.10.6)，该版本包含与新证书兼容的最新修复和性能改进。如果您不在 7 月 20 日之前进行这些升级，则您的 Linux WorkSpaces 会话配置将失败，您的最终用户将无法连接到他们的 WorkSpaces。

将 PCo IP 代理升级到最新版本

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在导航窗格中，请选择 WorkSpaces。
3. 选择你的 Linux WorkSpace，然后选择 “操作”、“重启” 来重启它 WorkSpaces。如果 WorkSpace 状态为`STOPPED`，则必须选择 “操作”、“ WorkSpaces先启动”，然后等到其状态变为`AVAILABLE`后才能重新启动它。
4. WorkSpace 在您重新启动且其状态为`AVAILABLE`，我们建议您在执行此升级`ADMIN_MAINTENANCE`时 WorkSpace 将的状态更改为。完成后，将的状态更改 WorkSpace 为`AVAILABLE`。有关 `ADMIN_MAINTENANCE` 模式的更多信息，请参阅手动维护。

   要将 a 的状态更改 WorkSpace 为`ADMIN_MAINTENANCE`，请执行以下操作：

   a. 选择， WorkSpace 然后选择 “操作”、“修改” WorkSpace。
   b. 选择 Modify State。
   c. 对于预期状态，请选择 ADMIN_MAINTENANCE。
   d. 选择 Modify(修改)。
5. WorkSpace 通过 SSH 连接到你的 Linux。有关更多信息，请参阅 WorkSpaces 在 WorkSpaces 个人版中为你的 Linux 启用 SSH 连接。
6. 要更新 PCo IP 代理，请运行以下命令：

```
sudo yum --enablerepo=pcoip-stable install pcoip-agent-standard-20.10.6
```

7. 要验证代理版本并确认更新成功，请运行以下命令：

```
rpm -q pcoip-agent-standard
```

验证命令应产生以下结果：

```
pcoip-agent-standard-20.10.6-1.el7.x86_64
```

8. 断开与的连接 WorkSpace ，然后重新启动它。
9. 如果您将的状态设置为Step 4，请重复Step 4并将 “预期状态” 设置为`AVAILABLE`。 WorkSpace `ADMIN_MAINTENANCE`

如果您的 Linux 在升级 PCo IP 代理后 WorkSpace 仍然无法启动，请联系 Supp Amazon ort。

WorkSpaces 在我连接的目录中启动经常失败

验证是否可从您连接到目录时所指定的每个子网访问本地目录中的两个 DNS 服务器或域控制器。您可以通过在每个子网中启动一个 Amazon EC2 实例并使用两台 DNS 服务器的 IP 地址将该实例加入您的目录来验证这种连接。

启动 WorkSpaces 失败并出现内部错误

检查您的子网是否配置为自动为在子网中启动的实例分配 IPv6 地址。要检查此设置，请打开 Amazon VPC 控制台，选择子网，然后依次选择子网操作、修改自动分配 IP 设置。如果启用此设置，则无法 WorkSpaces 使用 “性能” 或 “显卡” 捆绑包启动。相反，请在启动实例时禁用此设置并手动指定 IPv6 地址。

当我尝试注册目录时，注册失败并使该目录处于 ERROR 状态

如果您尝试注册已配置为用于多区域复制的Amazon托管 Microsoft AD 目录，则可能会出现此问题。尽管可以成功注册主区域中的目录以供使用 Amazon WorkSpaces，但尝试在复制区域中注册该目录会失败。在复制的区域 WorkSpaces 内，亚马逊不支持使用Amazon托管 Microsoft AD 进行多区域复制。

我的用户无法使用交互式登录横 WorkSpace 幅连接到 Windows

如果使用交互式登录消息来显示登录横幅，则会阻止用户访问他们的 Windows。 WorkSpaces PCoIP WorkSpaces 当前不支持交互式登录消息组策略设置。将移 WorkSpaces 至未应用Interactive logon: Message text for users attempting to log on组策略的组织单位 (OU)。DCV 支持登录消息 WorkSpaces，用户在接受登录横幅后必须重新登录。

我的用户无法连接到 Windows WorkSpace

我的用户在尝试连接自己的 Windows 时收到以下错误 WorkSpaces：

```
"An error occurred while launching your WorkSpace. Please try again."
```

当 WorkSpace 无法使用 PCo IP 加载 Windows 桌面时，通常会发生此错误。请检查以下事项：

- 如果适用于 Windows 的 PCo IP 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 PCo IP 代理已卸载，请 WorkSpace 通过 Amazon WorkSpaces 控制台重启以自动重新安装。
- 如果修改WorkSpaces安全组以限制出站流量，则在长时间延迟之后，您也可能会在 Amazon WorkSpaces 客户端上收到此错误。限制出站流量会阻止 Windows 与您的目录控制器通信而导致无法进行登录。确认您的安全组 WorkSpaces 允许您通过主网络接口在所有必需的端口上与目录控制器通信。

此错误的另一个原因与用户权限分配组策略有关。如果以下组策略配置不正确，则会阻止用户访问他们的 Windows WorkSpaces：

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment (计算机配置\Windows 设置\安全设置\本地策略\用户权限分配)

- 不正确的策略：

  策略：Access this computer from the network (从网络访问此计算机)

  设置:*Domain name*\ 域计算机

  获胜 GPO：允许文件访问
- 正确的策略：

  策略：Access this computer from the network (从网络访问此计算机)

  设置:*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。

在返回登录屏幕之前，Amazon WorkSpaces 客户端会显示灰色的 “正在加载...” 屏幕一段时间。不显示其他错误消息。

此行为通常表示 WorkSpaces 客户端可以通过端口 443 进行身份验证，但无法通过端口 4172 (PCoIP) 或端口 4195 (DCV) 建立流媒体连接。当未满足网络先决条件时，可能会发生此情况。客户端的问题通常导致客户端的网络检查失败。要查看哪些运行状况检查失败，请选择网络检查图标（通常是 2.0+ 客户端登录屏幕右下角带有感叹号的红色三角形，或 3.0+ 客户端右上角的网络图标 ）。

> **Note**
>
> 此问题的最常见原因是客户端防火墙或代理阻止通过端口 4172 或 4195（TCP 和 UDP）进行访问。如果此运行状况检查失败，请检查您的本地防火墙设置。

如果网络检查通过，则的网络配置可能存在问题 WorkSpace。例如，Windows 防火墙规则可能会阻止管理界面上的端口 UDP 4172 或 4195。 WorkSpace 使用远程桌面协议 (RDP) 客户端连接到，以验证是否 WorkSpace 满足必要的端口要求。

我的用户收到消息 “WorkSpace 状态：不健康。我们无法将您连接到您的 WorkSpace。请过几分钟再试。”

此错误通常表示 SkyLightWorkSpacesConfigService 服务未响应运行状况检查。

如果您刚刚重新启动或启动 WorkSpace，请等待几分钟，然后重试。

如果 WorkSpace 已经运行了一段时间，但您仍然看到此错误，请使用 RDP 进行连接以验证该 SkyLightWorkSpacesConfigService 服务：

- 正在运行。

- 设置为自动启动。
- 可以通过管理界面 (eth0) 进行通信。
- 未被任何第三方防病毒软件阻止。

我的用户会收到消息 “此设备无权访问 WorkSpace. 请联系您的管理员寻求帮助。”

此错误表示可能发生以下情况之一：

- IP 访问控制组是在 WorkSpace 目录上配置的，但客户端 IP 地址未列入许可名单。

  检查您的目录上的设置。确认用户连接的公有 IP 地址允许访问 WorkSpace。
- 在访问控制下，不允许将设备的操作系统作为可信设备，或者您的设备在使用可信设备选项时未安装正确的证书。通过执行以下操作，将您的设备类型添加为可信设备：

  1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
  2. 在导航窗格中，选择目录。
  3. 选择您要使用的目录。
  4. 向下滚动到访问控制选项，然后选择编辑。
  5. 在可信设备下，对于要允许访问的设备类型，在下拉列表中选择全部允许。如果要仅选择安装了客户端证书的设备，请选择可信设备。
  6. 如果您在上一步中选择了可信设备，请确保已导入至少一个根证书，并且已在客户端上安装了由根证书颁发机构（CA）颁发的客户端证书。有关创建、部署和导入根证书的更多信息，请参阅将 WorkSpaces 个人版访问限定于受信任设备。
  7. 选择保存。
- 您的设备类型未被授予访问权限 WorkSpaces。通过执行以下操作，授予对您的设备类型的访问权限：

  1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
  2. 在导航窗格中，选择目录。
  3. 选择您要使用的目录。
  4. 向下滚动到其他平台，然后选择编辑。
  5. 从以下设备类型中选出您想要授予 WorkSpaces 访问权限的设备。
     - ChromeOS

- iOS
- Linux
- Web Access
- 零客户端

6. 选择保存。

我的用户在尝试连接到 WSP WorkSpace 时收到消息 “无网络。网络连接中断。请检查网络连接 尝试连接 DCV 时 WorkSpace

如果出现此错误并且您的用户没有连接问题，请确保网络防火墙上已打开端口 4195。为了 WorkSpaces 使用 DCV，用于流式传输客户端会话的端口已从 4172 更改为 4195。

WorkSpaces 客户端给我的用户带来了网络错误，但他们可以在自己的设备上使用其他支持网络的应用程序

WorkSpaces 客户端应用程序依赖于对Amazon云端资源的访问，并且需要至少提供 1 Mbps 下载带宽的连接。如果设备间歇性地连接到网络，则 WorkSpaces 客户端应用程序可能会报告网络问题。

WorkSpaces 自 2018 年 5 月起，强制使用亚马逊信任服务颁发的数字证书。在 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， WorkSpaces 并且客户端会出现网络错误。

识别由于证书失败造成的连接问题

- PCoIP 零客户端-显示以下错误消息。

```
Failed to connect. The server provided a certificate that is invalid. See below for
 details:
- The supplied certificate is invalid due to timestamp
- The supplied certificate is not rooted in the devices local certificate store
```

- 其他客户端 - 运行状况检查失败，出现互联网红色警告三角形。

解决证书问题

- Windows 客户端应用程序
- PCoIP 零客户端

- 其他客户端应用程序

Windows 客户端应用程序

使用以下解决方案之一处理证书问题。

解决方案 1：更新客户端应用程序

从 下载并安装最新的 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. 依次选择文件、添加/删除管理单元、证书和添加。
5. 在证书管理单元页面上，选择计算机账户，然后选择下一步。保留默认值本地计算机。选择结束。选择确定。
6. 展开证书 (本地计算机)，然后选择受信任的根证书颁发机构。依次选择操作、所有任务和导入。
7. 按照向导的说明，导入下载的证书。
8. 退出并重新启动 WorkSpaces 客户端应用程序。

解决方案 3：使用组策略部署 Amazon Trust Services 作为可信 CA

使用组策略将 Starfield 证书添加到该域的可信根目录 CAs 中。有关更多信息，请参阅使用策略来分配证书。

PCoIP 零客户端

要直接连接 WorkSpace 使用固件版本 6.0 或更高版本，请下载并安装亚马逊信任服务颁发的证书。

添加 Amazon Trust Services 作为可信根 CA

1. 打开 https://certs.secureserver.net/repository/。
2. 在 Starfield Certificate Chain (Starfield 证书链) 中下载具有指纹 14 65 FA 20 53 97 B8 76 FA A6 F0 A9 95 8E 55 90 E4 0F CC 7F AA 4F B7 C2 C8 67 75 21 FB 5F B6 58 的证书。

3. 上传证书至 zero 客户端。有关更多信息，请参阅 Teradici 文档中的上传证书。

其他客户端应用程序

从 Amazon Trust Services 添加 Starfield 证书 (2b071c59a0a0ae76b0eadb2bad23bad4580b69c3601b630c2eaf0613afa83f92)。有关如何添加根 CA 的更多信息，请参阅以下文档：

- Android：添加和删除证书
- macOS 和 iOS：在测试设备上安装 CA 根证书

我的 WorkSpace 用户看到以下错误消息："设备无法连接到注册服务。请检查网络设置。"

当注册服务出现故障时，您的 WorkSpace 用户可能会在 Connection Healt h Check 页面上看到以下错误消息："您的设备无法连接到 WorkSpaces 注册服务。您将无法使用注册您的设备 WorkSpaces。请检查网络设置。"

当 WorkSpaces 客户端应用程序无法访问注册服务时，就会发生此错误。通常，当 WorkSpaces 目录被删除时，就会发生这种情况。要解决此错误，请确保注册码有效且与Amazon云端的运行目录相对应。

我 PCo的 IP zero 客户端用户收到错误 "由于时间戳的原因，提供的证书无效"

如果未在 Teradici 中启用网络时间协议 (NTP)，则您 PCo的 IP 零客户端用户可能会收到证书失败错误。要设置 NTP，请参阅为 WorkSpaces 个人版设置 PCoIP 零客户端。

USB 打印机和其他 USB 外围设备不适用于 PCo IP 零客户端

从 PCo IP 代理的 20.10.4 版本开始，亚马逊默认 WorkSpaces 禁用通过 Windows 注册表进行的 USB 重定向。当您的用户使用 PCo IP 零客户端设备连接到 USB 外围设备时，此注册表设置会影响 USB 外围设备的行为 WorkSpaces。

WorkSpaces 如果您使用的是 20.10.4 或更高版本 PCo的 IP 代理，则在启用 USB 重定向之前，USB 外围设备将无法与 PCo IP 零客户端设备配合使用。

> **Note**
>
> 如果您使用的是 32 位虚拟打印机驱动程序，则还必须将这些驱动程序更新到 64 位版本。

为 PCo IP 零客户端设备启用 USB 重定向

我们建议您 WorkSpaces 通过组策略将这些注册表更改推送到您的注册表中。有关更多信息，请参阅 Teradici 文档中的配置代理和可配置的设置。

1. 将以下注册表项值设置为 1（已启用）：

   KeyPath = HKEY_LOCAL_MACHINE\ SOFTWARE\ Policies\ Teradici\ IP\ pcoip_admin PCo

   KeyName = pcoip.enable_usb

   KeyType = DWORD

   KeyValue = 1
2. 将以下注册表项值设置为 1（已启用）：

   KeyPath = HKEY_LOCAL_MACHINE\ 软件\ Policies\ Teradici\ IP\ pcoip_admin_defaul ts PCo

   KeyName = pcoip.enable_usb

   KeyType = DWORD

   KeyValue = 1
3. 如果您尚未这样做，请注销 WorkSpace，然后重新登录。您的 USB 设备现在应该可以运行了。

我的用户跳过了更新其 Windows 或 macOS 客户端应用程序的过程，并且没有收到安装最新版本的提示

当用户跳过对 Amazon WorkSpaces Windows 客户端应用程序的更新时，会设置SkipThisVersion注册表项，并且在新版本的客户端发布时不再提示他们更新客户端。要更新到最新版本，您可以按照《亚马逊 WorkSpaces 用户指南》中将 WorkSpaces Windows 客户端应用程序更新到新版本中所述编辑注册表。您也可以运行以下 PowerShell 命令：

```
Remove-ItemProperty -Path "HKCU:\Software\Amazon Web Services. LLC\Amazon WorkSpaces
\WinSparkle" -Name "SkipThisVersion"
```

当用户跳过对 Amazon WorkSpaces macOS 客户端应用程序的更新时，会设置`SUSkippedVersion`首选项，并且在新版本的客户端发布时不再提示他们更新客户端。要更新到最新版本，您可以按照《亚马逊 WorkSpaces 用户指南》中将 WorkSpaces macOS 客户端应用程序更新到新版本中所述重置此首选项。

我的用户没有收到邀请电子邮件或密码重置电子邮件

用户不会自动收到使用 AD Connector WorkSpaces 或可信域创建的欢迎电子邮件或密码重置电子邮件。如果用户已经位于 Active Directory 中，系统也不会自动发送邀请电子邮件。

要手动向这些用户发送欢迎电子邮件，请参阅 发送邀请电子邮件。

要重置用户密码，请参阅为 WorkSpaces 个人设置 Active Directory 管理工具。

我的用户在客户端登录屏幕上看不到“忘记密码？”选项

如果您使用的是 AD Connector 或受信任域，则您的用户将无法重置自己的密码。（忘记密码？WorkSpaces 客户端应用程序登录屏幕上的选项将不可用。）有关如何重置用户密码的信息，请参阅为 WorkSpaces 个人设置 Active Directory 管理工具。

当我尝试在 Windows 上安装应用程序时，我收到 “系统管理员已设置策略来阻止此安装” 的消息 WorkSpace

您可以通过修改 Windows 安装程序组策略设置来解决此问题。要将此策略部署到目录 WorkSpaces 中的多个目录，请将此设置应用于从已加入域 EC2 的实例链接到 WorkSpaces 组织单位 (OU) 的组策略对象。如果您使用 AD Connector，则可以从域控制器进行这些更改。有关使用 Active Directory 管理工具处理组策略对象的更多信息，请参阅《Amazon Directory Service 管理指南》中的安装 Active Directory 管理工具。

以下过程说明如何为 WorkSpaces 组策略对象配置 Windows 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。
2. 在 Windows WorkSpace 客户端上打开组策略管理工具，导航到 WorkSpaces 计算机帐户的 WorkSpaces 组策略对象并将其选中。从主菜单中，依次选择 Action (操作) 和 Edit (编辑)。
3. 在组策略管理编辑器中，依次选择计算机配置、策略、管理模板、经典管理模板、Windows 组件、Windows 安装程序。
4. 打开 Turn Off Windows Installer (关闭 Windows 安装程序) 设置。
5. 在 Turn Off Windows Installer (关闭 Windows 安装程序) 对话框中，将 Not Configured (未配置) 更改为 Enabled (已启用)，然后将 Disable Windows Installer (禁用 Windows 安装程序) 设置为 Never (从不)。
6. 选择确定。
7. 要应用组策略更改，请执行下列操作之一：

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

我的目录 WorkSpaces 中没有可以连接到互联网

WorkSpaces 默认情况下无法与互联网通信。您必须显式提供互联网访问。有关更多信息，请参阅 为 WorkSpaces 个人版提供互联网访问权限。

我的 WorkSpace 已经失去了互联网接入

如果您无法访问互联网，并且无法使用 RDP 连接到互联网，则此问题可能是由于的公有 IP 地址丢失所致。 WorkSpace WorkSpace WorkSpace如果您在目录级别启用了弹性 IP 地址的自动分配，则会在启动弹性 IP 地址（来自亚马逊提供的地址池） WorkSpace 时分配给您。但是，如果您将自己拥有的弹性 IP 地址关联到 WorkSpace，然后又将该弹性 IP 地址与解除关联 WorkSpace，则该弹性 IP 地址将 WorkSpace 丢失其公有 IP 地址，并且不会自动从亚马逊提供的池中获取新的 IP 地址。

要将亚马逊提供的资源池中的新公有 IP 地址与相关联 WorkSpace，您必须重新构建。 WorkSpace如果您不想重建 WorkSpace，则必须将您拥有的另一个弹性 IP 地址与关联起来 WorkSpace。

我们建议您不要在启动 WorkSpace后修改的 elastic network 接口。 WorkSpace 将弹性 IP 地址分配给后 WorkSpace， WorkSpace 会保留相同的公有 IP 地址（除非重建，在这种情况下，它将获得新的公有 IP 地址）。 WorkSpace

当我尝试连接我的本地目录时收到一条“DNS unavailable”错误

在连接您的本地目录时，您收到类似于以下内容的错误消息。

```
DNS unavailable (TCP port 53) for IP: dns-ip-address
```

AD Connector 必须能够通过 TCP 和 UDP 经由端口 53 与您的本地 DNS 服务器通信。验证您的安全组和本地防火墙是否允许经由此端口进行 TCP 和 UDP 通信。

在尝试连接到我的本地目录时，我收到一条“Connectivity issues detected”错误

在连接您的本地目录时，您收到类似于以下内容的错误消息。

```
Connectivity issues detected: LDAP unavailable (TCP port 389) for IP: ip-address
Kerberos/authentication unavailable (TCP port 88) for IP: ip-address
```

```
Please ensure that the listed ports are available and retry the operation.
```

AD Connector 必须能够通过 TCP 和 UDP 经由以下端口与您的本地域控制器通信。验证您的安全组和本地防火墙是否允许经由这些端口进行 TCP 和 UDP 通信：

- 88 (Kerberos)
- 389 (LDAP)

在尝试连接到我的本地目录时，我收到一条“SRV record”错误

在连接您的本地目录时，您收到类似于以下一项或多项内容的错误消息。

```
SRV record for LDAP does not exist for IP: dns-ip-address

SRV record for Kerberos does not exist for IP: dns-ip-address
```

在连接您的目录时，AD Connector 需要获取 `_ldap._tcp.`*`dns-domain-name`* 和 `_kerberos._tcp.`*`dns-domain-name`* SRV 记录。如果服务无法从您在连接到目录时所指定的 DNS 服务器上获取这些记录，则您会收到此错误。请确保您的 DNS 服务器包含这些 SRV 记录。有关更多信息，请参阅 Microsoft TechNet 上的 SRV 资源记录。

我的 Windows 闲置时会 WorkSpace 进入睡眠状态

要解决此问题，请使用以下步骤连接到 WorkSpace 并将电源计划更改为 “高性能”：

1. 从中 WorkSpace打开 “控制面板”，然后选择 “硬件” 或 “硬件和声音”（名称可能会有所不同，具体取决于你的 Windows 版本）。
2. 在 Power Options (电源选项) 下，选择 Choose a power plan (选择电源计划)。
3. 在选择或自定义电源计划窗格中，选择高性能电源计划，然后选择更改计划设置。
   - 如果高性能电源计划选项被禁用，请选择更改当前不可用的设置，然后选择高性能电源计划。
   - 如果看不到高性能计划，请选择显示其他计划右侧的箭头以显示它，或者在左侧导航栏中选择创建电源计划，选择高性能，为电源计划命名，然后选择下一步。
4. 在更改计划的设置: 高性能页面上，确保将关闭显示屏和（如果可用）将计算机置于睡眠状态设置为从不。
5. 如果您对高性能计划进行了任何更改，请选择保存更改（或选择创建，如果要创建新计划的话）。

如果上述步骤无法解决该问题，请执行以下操作：

1. 从中 WorkSpace打开 “控制面板”，然后选择 “硬件” 或 “硬件和声音”（名称可能会有所不同，具体取决于你的 Windows 版本）。
2. 在 Power Options (电源选项) 下，选择 Choose a power plan (选择电源计划)。
3. 在选择或自定义电源计划窗格中，选择高性能电源计划右侧的更改计划设置链接，然后选择更改高级电源设置链接。
4. 在 Power Options (高级选项) 对话框中的设置列表中，选择 Hard disk (硬盘) 左侧的加号以显示相关设置。
5. 验证 Plugged in (已插入) 的 Turn off hard disk after (在多长时间后关闭硬盘) 值是否大于 On battery (使用电池) 的值（默认值为 20 分钟）。
6. 选择 PCI Express 左侧的加号，然后为 Link State Power Management (链路状态电源管理) 执行相同的操作。
7. 验证 Link State Power Management (链路状态电源管理) 设置是否为 Off (关闭)。
8. 选择 OK (确定)（如果您更改了任何设置，则选择 Apply (应用)）以关闭对话框。
9. 在 Change settings for the plan (更改计划的设置) 窗格中，如果您更改了任何设置，请选择 Save changes (保存更改)。

我的其中 WorkSpaces 一个状态为 UNHEALTHY

该 WorkSpaces 服务会定期向 a 发送状态请求 WorkSpace。A WorkSpace 在无法响应这些请求UNHEALTHY时会被标记。导致此问题的常见原因包括：

- 上的应用程序 WorkSpace 正在阻塞网络端口，这使无法响应状态请求。 WorkSpace
- CPU 使用率过高导致无法及时响应状态请求。 WorkSpace
- 的计算机名称 WorkSpace 已更改。这可以防止在 WorkSpaces 和之间建立安全通道 WorkSpace。

您可以尝试使用以下方法来纠正这种状况：

- WorkSpace 从 WorkSpaces 控制台重新启动。
- WorkSpace 使用以下步骤连接到运行状况不佳的服务器，该步骤应仅用于故障排除：
  1. Connect 连接到与运行状况不佳 WorkSpace者位于同一目录 WorkSpace 中的操作服务器。
  2. 从操作开始 WorkSpace，使用远程桌面协议 (RDP)， WorkSpace 使用不健康用户的 IP 地址连接到运行状况不佳的服务器。 WorkSpace根据问题的严重程度，您可能无法连接到不健康的服务器 WorkSpace。

3. 如果运行状况不 WorkSpace佳，请确认满足最低端口要求。

- 确保 SkyLightWorkSpacesConfigService 服务可以响应运行状况检查。要排查此问题，请参阅我的用户收到消息 “WorkSpace 状态：不健康。我们无法将您连接到您的 WorkSpace。请过几分钟再试。”。
- WorkSpace 从 WorkSpaces 控制台重建。由于重建 WorkSpace 可能会导致数据丢失，因此只有在所有其他更正问题的尝试均未成功的情况下，才应使用此选项。

我的 WorkSpace 意外崩溃或重启

如果您的 PCo IP WorkSpace 配置反复崩溃或重新启动，并且错误日志或崩溃转储指向`spacedeskHookKmode.sys`或有问题`spacedeskHookUmode.dll`，或者如果您收到以下错误消息，则可能需要禁用 Web 访问权限： WorkSpace

```
The kernel power manager has initiated a shutdown transition.
Shutdown reason: Kernel API
```

```
The computer has rebooted from a bugcheck.
```

> **Note**
>
> - 这些故障排除步骤不适用于为 WorkSpaces DCV 配置的步骤。它们仅适用于为 WorkSpaces PCo IP 配置的。
> - 仅当您不允许用户使用 Web 访问时，才应禁用 Web 访问。

要禁用对的 Web 访问 WorkSpace，必须禁用 WorkSpaces 目录中的 Web 访问并重新启动 WorkSpace。

同一个用户名有多个用户名 WorkSpace，但用户只能登录其中一个 WorkSpaces

如果您在 Active Directory (AD) 中删除用户而不先将其删除， WorkSpace 然后将该用户添加回 Active Directory WorkSpace 并为该用户创建一个新用户，那么同一个用户名现在将在同一个目录 WorkSpaces 中包含两个用户名。但是，如果用户尝试连接到其原始设备 WorkSpace，他们将收到以下错误：

```
"Unrecognized user. No WorkSpace found under your username. Contact your administrator
 to request one."
```

此外，在 Amazon WorkSpaces 控制台中搜索用户名时只会返回新的用户名 WorkSpace，尽管两者 WorkSpaces 仍然存在。（您可以 WorkSpace 通过搜索 WorkSpace ID 而不是用户名来找到原件。）

如果您在 Active Directory 中重命名用户而不先将其删除，也会发生这种情况 WorkSpace。如果您随后将他们的用户名改回原来的用户名 WorkSpace 并为该用户创建一个新的用户名，则同一个用户名将在目录 WorkSpaces 中包含两个用户名。

出现此问题的原因是 Active Directory 使用用户的安全标识符 (SID)（而不是用户名）以唯一标识用户。当删除某个用户并在 Active Directory 中重新创建此用户时，即使用户的用户名保持不变，也会为该用户分配一个新的 SID。在搜索用户名的过程中，Amazon WorkSpaces 控制台使用 SID 在 Active Directory 中搜索匹配项。当用户连接时，Amazon WorkSpaces 客户端还使用 SID 来识别用户 WorkSpaces。

要解决此问题，请执行下列操作之一：

- 如果由于在 Active Directory 中删除了用户并在其中重新创建了该用户而发生了此问题，并且在 Active Directory 中启用了回收站功能，则您可能能够还原原始的已删除的用户对象。如果您能够恢复原始用户对象，请确保该用户可以连接到其原始对象 WorkSpace。如果可以，您可以在手动备份并将任何用户数据从新数据传输 WorkSpace 到原始数据 WorkSpace（如果需要）WorkSpace后删除新数据。
- 如果您无法恢复原始用户对象，请删除该用户的原始对象 WorkSpace。用户应该能够连接并使用他们的新 WorkSpace 版本。请务必手动备份并将所有用户数据从原始数据传输 WorkSpace 到新数据 WorkSpace。

> **Warning**
>
> 删除 WorkSpace 是一项永久性操作，无法撤消。 WorkSpace 用户的数据不会持续存在并被销毁。要获取有关备份用户数据的帮助，请联系 Amazon Support。

我在亚马逊上使用 Docker 时遇到了问题 WorkSpaces

窗户 WorkSpaces

Windows WorkSpaces 不支持嵌套虚拟化（包括使用 Docker）。有关更多信息，请参阅 Docker 文档。

Linu WorkSpaces

要在 Linux 上使用 Docker WorkSpaces，请确保 Docker 使用的 CIDR 块不与与关联的两个弹性网络接口 (ENIs) 中使用的 CIDR 块重叠。 WorkSpace如果你在 Linux 上使用 Docker 时遇到问题 WorkSpaces，请联系 Docker 寻求帮助。

我的一些 API 调用收到了 ThrottlingException 错误

WorkSpaces API 调用的默认允许速率为每秒两次 API 调用的恒定速率，允许的最大 “突发” 速率为每秒五次 API 调用。下表显示了适用于 API 请求的突发速率限制。

秒	发送的请求数	允许的 Net 请求数	Details
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。
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。

秒	发送的请求数	允许的 Net 请求数	Details
9	0	5	即使在第 8 秒没有发出任何调用，速率限制也不会增加到五次以上。

当我 WorkSpace 让它在后台运行时，我的连接一直处于断开状态

对于 Mac 用户，请查看 Power Nap 功能是否已开启。如果它处于开启状态，请将其关闭。要关闭 Power Nap，请打开终端并运行以下命令：

```
defaults write com.amazon.workspaces NSAppSleepDisabled -bool YES
```

SAML 2.0 联合身份验证不起作用。我的用户无权直播其 WorkSpaces 桌面。

出现此问题的原因可能是为 SAML 2.0 联合身份验证 IAM 角色嵌入的内联策略不包含从目录 Amazon 资源名称 (ARN) 进行流式传输的权限。IAM 角色由正在访问 WorkSpaces 目录的联合用户担任。编辑角色权限以包含目录 ARN，并确保用户在目录 WorkSpace 中有。有关更多信息，请参阅 SAML 2.0 身份验证和使用 S AML 2.0 联合进行故障排除。Amazon

我的用户每 60 分钟就会断开一次 WorkSpaces 会话连接。

如果您已将 SAML 2.0 身份验证配置为 WorkSpaces，则可能需要配置 IdP 在身份验证响应中作为 SAML 属性Amazon传递的信息，具体取决于您的身份提供商 (IdP)。这包括配置 Attribute (属性) 元素，并将 `SessionDuration` 属性设置为 `https://aws.amazon.com/SAML/Attributes/SessionDuration`。

`SessionDuration` 指定用户的联合流会话在需要重新进行身份验证之前可保持活动状态的最长时间。虽然 `SessionDuration` 是可选属性，但建议您将它包含在 SAML 身份验证响应中。如果您未指定此属性，则会话持续时间将默认为 60 分钟。

要解决此问题，请配置 IdP 以在 SAML 身份验证响应中包含 `SessionDuration` 值，并根据需要设置该值。有关更多信息，请参阅步骤 5：为 SAML 身份验证响应创建断言。

我的用户在使用 SAML 2.0 身份提供商 (IdP) 启动的流程进行联合时会收到重定向 URI 错误，或者我的用户在联合到 IdP 后每次尝试从 WorkSpaces 客户端登录时，都会启动客户端应用程序的另一个实例。

出现此错误的原因是中继状态 URL 无效。确保您的 IdP 联合设置中的中继状态正确，并且在目录属性中为 IdP 联合身份验证正确配置了用户访问 URL 和中继状态参数名称。 WorkSpaces 如果它们有效但问题仍然存在，请联系 Su Amazon pport。有关更多信息，请参阅设置 SAML。

我的用户在联合到 IdP 后尝试登录 WorkSpaces 客户端应用程序时，他们会收到一条消息：“出了点问题：启动你的应用程序时出错 WorkSpace”。

查看适用于联合身份验证的 SAML 2.0 断言。SAML Subject NameID 值必须与用户名匹配 WorkSpaces ，并且通常与 Active Direct or AMAccount y 用户的 “名称” 属性相同。此外，属性设置为的`PrincipalTag:Email`属性元素`https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`必须与 WorkSpaces 目录中定义的 WorkSpaces 用户的电子邮件地址相匹配。有关更多信息，请参阅设置 SAML。

我的用户在联合到 IdP 后尝试登录 WorkSpaces 客户端应用程序时会收到 “无法验证标签” 的消息。

查看联合身份验证的 SAML 2.0 断言中的 `PrincipalTag` 属性值，例如 `https://aws.amazon.com/SAML/Attributes/PrincipalTag:Email`。标签值可能包括字符 `_ . : / = + - @`、字母、数字和空格的组合。有关更多信息，请参阅 IAM 中的标签规则和。Amazon STS

我的用户会收到消息“客户端和服务器无法通信，因为它们没有共同的算法”。

如果您未启用 TLS 1.2，则可能会出现此问题。

我的麦克风或网络摄像头无法在 Windows 上运行 WorkSpaces。

打开“开始”菜单，查看您的隐私设置

- 开始 > 设置 > 隐私 > 相机
- 开始 > 设置 > 隐私 > 麦克风

如果它们已关闭，请将其打开。

或者， WorkSpaces 管理员可以根据需要创建组策略对象 (GPO) 来启用麦克风和/或网络摄像头。

我的用户无法使用基于证书的身份验证登录，当他们连接到桌面会话时，系统会在 WorkSpaces 客户端或 Windows 登录屏幕上提示他们输入密码。

会话基于证书的身份验证失败。如果问题仍然存在，则基于证书的身份验证失败可能是由以下问题之一导致的：

- 不支持 WorkSpaces 或客户端。使用最新 WorkSpaces 的 Windows 客户端应用程序的 DCV 捆绑包 WorkSpaces 上的 Windows 支持基于证书的身份验证。
- 在 WorkSpaces 目录上启用基于证书的身份验证后，需要重新启动。 WorkSpaces
- WorkSpaces 无法与Amazon 私有 CA证书通信或Amazon 私有 CA未颁发证书。检查 Amazon CloudTrail 以确定是否已颁发证书。有关更多信息，请参阅 管理基于证书的身份验证。
- 域控制器没有用于智能卡登录的域控制器证书，或者该证书已过期。有关更多信息，请参阅先决条件中的步骤 7，“使用域控制器证书配置域控制器以对智能卡用户进行身份验证”。
- 该证书不可信。有关更多信息，请参阅先决条件中的步骤 7，“将 CA 发布到 Active Directory”。在域控制器上运行 `certutil -viewstore -enterprise NTAuth` 以确认 CA 已发布。
- 缓存中有一个证书，但是该用户的属性已更改，从而使该证书失效。在证书Amazon Web Services 支持到期（24 小时）之前，请联系以清除缓存。有关更多信息，请参阅 Amazon Web Services 支持 中心。
- `UserPrincipalNameSAML` 属性的格式格式不正确或无法解析为用户的实际域。userPrincipalName 有关更多信息，请参阅先决条件中的步骤 1。
- 您的 SAML 断言中的（可选）`ObjectSid` 属性与 SAML_Subject `NameID` 中指定的用户的 Active Directory 安全标识符 (SID) 不匹配。确认您的 SAML 联合身份验证中的属性映射是正确的，并且您的 SAML 身份提供者正在同步 Active Directory 用户的 SID 属性。
- 有些组策略设置会修改智能卡登录的默认 Active Directory 设置，或者在从智能卡读卡器中移除智能卡时执行操作。除了上面列出的错误之外，这些设置还可能会导致其他意外行为。基于证书的身份验证向实例操作系统提供虚拟智能卡，并在登录完成后将其删除。检查智能卡的主组策略设置以及其他智能卡组策略设置和注册表项，包括智能卡删除行为。
- 私有 CA 的 CRL 分发点不在线，也无法从 WorkSpaces 或域控制器访问。有关更多信息，请参阅先决条件中的步骤 5。
- 要检查域或林 CAs 中是否存在任何陈旧内容，请在 CA `PKIVIEW.msc` 上运行以进行验证。如果有陈旧的 CAs，请使用 `PKIVIEW.msc` mmc 手动将其删除。
- 要检查 Active Directory 复制是否正常以及域中是否存在过时的域控制器，请运行 `repadmin /replsum`。

其他故障排除步骤包括查看 WorkSpaces 实例 Windows 事件日志。要检查登录失败的常见事件是 Windows 安全日志中的事件 4625：登录账户失败。

如果问题仍然存在，请与联系Amazon Web Services 支持。有关更多信息，请参阅 Amazon Web Services 支持 中心。

我正在尝试做一些需要 Windows 安装介质但 WorkSpaces 不提供安装介质的事情。

如果您使用的是Amazon提供的公共捆绑包，则可以在需要 EC2 时使用亚马逊提供的 Windows Server 操作系统安装媒体 EBS 快照。

根据这些快照创建 EBS 卷，将其附加到 Amazon EC2，然后根据需要将文件传输到文件 WorkSpace 所在的位置。如果你在 BYOL 上使用 Windows 10 WorkSpaces 并且需要安装媒体，则需要准备自己的安装媒体。有关更多信息，请参阅使用安装介质添加 Windows 组件。由于您无法将 EBS 卷直接连接到 WorkSpace，因此您需要将其连接到 Amazon EC2 实例并复制文件。

我想 WorkSpaces 使用在不支持的 WorkSpaces 地区创建的现有Amazon托管目录启动。

要 WorkSpaces 使用当前不支持的地区的目录启动 Amazon WorkSpaces，请按照以下步骤操作。

> **Note**
>
> 如果您在运行Amazon Command Line Interface命令时收到错误，请确保您使用的是最新Amazon CLI版本。有关更多信息，请参阅确认您运行的是最新版 Amazon CLI。

步骤 1：创建与您账户中另一个 VPC 的虚拟私有云 (VPC) 对等连接

1. 创建与不同区域内的 VPC 之间的 VPC 对等连接。有关更多信息，请参阅使用 VPCs 同一账户和不同区域进行创建。
2. 接受 VPC 对等连接。有关更多信息，请参阅接受 VPC 对等连接。
3. 激活 VPC 对等连接后，您可以使用 Amazon VPC 控制台Amazon CLI、或 API 查看您的 VPC 对等连接。

步骤 2：更新两个区域中 VPC 对等连接的路由表

更新您的路由表以开启通过 IPv4 或与对等 VPC 的通信 IPv6。有关更多信息，请参阅为 VPC 对等连接更新路由表。

第 3 步：创建 AD Connector 并注册亚马逊 WorkSpaces

1. 要查看 AD Connector 先决条件，请参阅 AD Connector 先决条件。
2. 通过 AD Connector 连接现有目录。有关更多信息，请参阅创建 AD Connector。
3. 当 AD Connector 状态更改为活动时，打开 Amazon Directory Service 控制台，然后为您的目录 ID 选择超链接。
4. 对于Amazon应用程序和服务，请选择 Amazon WorkSpaces 以开启对该目录的 WorkSpaces 访问权限。
5. 向注册目录 WorkSpaces。有关更多信息，请参阅向注册目录 WorkSpaces。

我想在 Amazon Linux 2 上更新 Firefox。

步骤 1：检查自动更新是否已启用

要验证是否已启用自动更新，请在上运行命令`systemctl status *os-update-mgmt.timer | grep enabled`。 WorkSpace在输出中，应该有两行显示有 `enabled` 字样。

步骤 2：启动更新

Firefox 通常会在维护时段内自动更新 Amazon Linux 2 WorkSpaces 以及系统中的所有其他软件包。但是，这取决于 WorkSpaces 您使用的类型。

- 因为 AlwaysOn WorkSpaces，每周维护时段为星期日 00:00 到 04h00，所在时区为。 WorkSpace
- 对于 AutoStop WorkSpaces. 从每月的第三个星期一开始，在长达两周的时间内，维护窗口的开放时间为每天大约 00:00 到 05h00，与该地区的时区相同。Amazon WorkSpace

有关维护时段的更多信息，请参阅 WorkSpace 维护。

您也可以通过重启 WorkSpace并在 15 分钟后重新连接来启动即时更新周期。您也可以通过输入 `sudo yum update` 来启动更新。要启动仅适用于 Firefox 的更新，请输入 `sudo yum install firefox`。

如果您无法配置对 Amazon Linux 2 存储库的访问权，并且更喜欢使用 Mozilla 构建的二进制文件安装 Firefox，请参阅 Mozilla 支持页面上的从 Mozilla 版本安装 Firefox。建议完全卸载 RPM 打包版本的 Firefox，以确保您不会错误地运行过时的版本。您可以通过运行命令 `sudo yum remove firefox` 将其卸载。

您也可以通过在另一台计算机上运行命令 `yumdownloader firefox`，从 Amazon Linux 2 存储库下载所需的 RPM 软件包。然后，将存储库侧加载到 WorkSpaces，在那里你可以使用类似`sudo yum install firefox-102.11.0-2.amzn2.0.1.x86_64.rpm`的标准YUM命令来安装它们。

> **Note**
>
> 确切的文件名将根据软件包版本而变化。

步骤 3：验证 Firefox 存储库是否已使用

亚马逊 Linux Extras 会自动为亚马逊 Linux 2 WorkSpaces 提供 Firefox 更新。2023 年 7 月 31 日之后 WorkSpaces 创建的亚马逊 Linux 2 已经激活 Firefox Extra 存储库。要验证您是否 WorkSpace 正在使用 Firefox Extra 存储库，请运行以下命令。

```
yum repolist | grep amzn2extra-firefox
```

如果使用了 Firefox Extra 存储库，则命令输出应类似于 `amzn2extra-firefox/2/x86_64 Amazon Extras repo for firefox 10`。如果未使用 Firefox Extra 存储库，则它将为空。如果未使用 Firefox Extra 存储库，您可以尝试使用以下命令手动启用它：

```
sudo amazon-linux-extras install firefox
```

如果 Firefox Extra 存储库激活仍然失败，请检查您的互联网访问并确保您的 VPC 端点未配置。要继续 WorkSpaces 通过 YUM 存储库接收 Amazon Linux 2 的 Firefox 更新，请确保 WorkSpaces 您能够访问亚马逊 Linux 2 存储库。有关在不访问互联网的情况下访问 Amazon Linux 2 存储库的更多信息，请参阅这篇知识中心文章。

我的用户可以使用 WorkSpaces 客户端重置密码，而忽略上配置的细粒度密码策略 (FFGP) 设置。Amazon Managed Microsoft AD

如果您的用户的 WorkSpaces 客户端与关联Amazon Managed Microsoft AD，则他们必须使用默认的复杂性设置重置密码。

此默认复杂度密码区分大小写，且长度必须介于 8 到 64 个字符之间。该密码必须包含下列每种类别中的至少一个字符：

- 小写字符 (a-z)
- 大写字符 (A-Z)

- 数字 (0-9)
- 非字母数字字符 (~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)

确保该密码不包含不可打印的 unicode 字符，例如空格、回车符、换行符和空字符。

如果您的组织要求您强制执行 FFGP WorkSpaces，请联系您的 Active Directory 管理员，直接从 Active Directory（而非 WorkSpaces 客户端）重置用户的密码。

个人版中的 WorkSpaces DCV 主机代理版本

DCV 主机代理是在您的 WorkSpace内部运行的主机代理。它将你的像素流式传输 WorkSpace 到客户端应用程序，并包括会话中的功能，例如双向音频和视频以及打印。有关 DCV 的更多信息，请参阅 Amazon WorkSpaces 协议。

建议将您的主机代理软件更新为最新版本。您可以手动重启 WorkSpaces 以更新 DCV 主机代理。DCV Host Agent 还会在常规 WorkSpaces 默认维护时段内自动更新。有关维护时段的更多信息，请参阅WorkSpace 维护。其中一些功能需要最新的 WorkSpaces 客户端版本。有关最新客户端版本的更多信息，请参阅WorkSpaces 客户端。

下表描述了 Personal 版 DCV 主机代理的每个版本的 WorkSpaces 变化。

发布版本	日期	更改
• Windows WorkSpaces -2.2.0.2116	2026年1月26日	• 增加了对高级打印的支持，允许在使用远程打印时访问高级打印机首选项，包括双面打印、纸盒选择等。 • 增加了屏幕捕获保护，当用户尝试从客户端使用屏幕捕获工具时，可屏蔽主机上的内容，从而防止数据泄露。 • 用于计算 TCP/QUIC 连接数的新服务器性能计数器。 • 错误修复和性能改进，包括 Firefox 对 Windows Server 2019 增强版 WebAuthn 的支持。

发布版本	日期	更改
• Windows WorkSpaces -2.0.2047	2025 年 10 月 1 日	• 提高了音频性能；添加了新的音频设备监视器，该监视器仅在远程应用程序使用麦克风音频流时才启用它，这有助于优化性能（请参阅客户端发行说明以获取兼容的客户端信息）。 • 通过引入新的键盘布局选项（服务器或客户端）来改善国际键盘体验，帮助您在特定使用案例中更自信地键入内容（请参阅客户端发行说明以获取兼容的客户端信息） • 错误修复，包括在视频会议应用程序（例如 Zoom 和 Teams）中共享主持人音频时的音频回声效果以及一般性能改进
• Windows WorkSpaces -2.0.2021	2025 年 8 月 30 日	• 缺陷修复和性能改进。
• Windows WorkSpaces -2.1.0.2000	2025 年 7 月 7 日	• 增强了对本机应用程序的 WebAuth 重定向支持。 • 缺陷修复和性能改进。
• Ubunt WorkSpaces u-2.1.0.1923	2025 年 5 月 1 日	• 缺陷修复和性能改进。
• Rocky Linux WorkSpaces -2.1.0.1843 • 红帽企业 Linux WorkSpaces -2.1.0.1843	2025 年 4 月 10 日	• 缺陷修复和性能改进。
• Windows WorkSpaces -2.1.0.1840	2025 年 3 月 19 日	• 修复了即使禁用打印机重定向 GPO 仍显示打印机列表的问题。 • 缺陷修复和性能改进。

发布版本	日期	更改
• Windows WorkSpaces -2.1.0.1792	2024 年 11 月 19 日	缺陷修复和性能改进。
• Windows WorkSpaces -2.1.0.1786	2024 年 10 月 31 日	• 将 WorkSpaces 直播协议 (WSP) 重命名为 Amazon DCV。 • 修复了使用 Avaya 应用程序的客户在 DCV 代理上的音频降噪的问题。 • 修复了用户在 PIN 提示页面上闲置时出现的 SmartCard 登录问题。 • WebAuthn 修复了在 Chrome 浏览器上首次尝试登录时出现的重定向问题。 • 缺陷修复和性能改进。
• Windows WorkSpaces -2.1.0.1757	2024 年 8 月 19 日	• 增加了对与 IAM Identity Center（IdC）集成的支持。 • 缺陷修复和性能改进。
• Windows WorkSpaces -2.1.0.1696	2024 年 7 月 29 日	• 增加了对 Windows Graphics 主机的支持。 • 增加了对 Amazon Connect 的 WebRTC 重定向支持。 • 修复了在系统启动时可能会阻止服务运行的问题。 • 缺陷修复和性能改进。

发布版本	日期	更改
• Windows WorkSpaces -2.1.0.1554	2024 年 5 月 15 日	• 增加了对空闲断开连接超时的支持。 • 增加了新的组策略设置以配置空闲断开连接超时。 • 修复 WorkSpaces 了用户修改显示设置时断开连接并显示白屏的问题。 • 缺陷修复和性能改进。
• Ubunt WorkSpaces u-2.1.0.1342	2024 年 2 月 29 日	• 将首选网络摄像头分辨率更改为介于 480x360 和 640x480 之间。 • 缺陷修复和性能改进。
• Windows WorkSpaces -2.0.0.1425	2024 年 2 月 22 日	• 增加了对在远程谷歌浏览器或 Microsoft Edge 浏览器中运行的网络应用程序发出的会话中 WebAuthn 重定向请求的支持。此功能会添加一次性浏览器提示，要求用户启用 DCV WebAuthn 重定向扩展。只有 Windows WorkSpaces 和 WorkSpaces 本机客户端支持它。 • 修复了登录时有时会出现白屏或冻屏的问题。 • 缺陷修复和性能改进。
• Windows WorkSpaces -2.0.0.1304	2024 年 1 月 11 日	• 修复了与登录期间可能冻结流式传输相关的错误。 • 修复了与日志记录相关的错误。

发布版本	日期	更改
• Windows WorkSpaces -2.0.0.1288	2023 年 11 月 16 日	• 在 Windows 10+ 上增加了对间接显示驱动程序（IDD）的支持，从而降低了 CPU 消耗并提高了流式传输性能。 • 增加了新的组策略设置以启用或禁用 IDD 驱动程序。 • 修复了与剪贴板图像透明度相关的错误。 • 修复了保留 Windows 比例系数的错误。 • 缺陷修复和性能改进。
• Windows WorkSpaces -2.0.0.1164	2023 年 10 月 13 日	• 在虚拟显示驱动程序 VSync 中添加了对的支持。 • 添加了新的组策略设置以启用或禁用 VSync。 • 改善了重新连接和可靠性问题。 • 缺陷修复和性能改进。
• 亚马逊 Linux WorkSpaces -2.0.0.1086 • Ubunt WorkSpaces u-2.1.0.1086	2023 年 8 月 18 日	• 添加了启用或禁用时区重定向的新设置。 • 延长了登录超时时间并添加了配置选项。 • 改进了网关，可在中断后更快地重新连接。 • 缺陷修复和性能改进。

发布版本	日期	更改
• 亚马逊 Linux WorkSpaces -2.0.0.907	2023 年 6 月 30 日	• 增加了对 DCV Extension SDK 的支持，以启用特定于 ISV 的集成功能。 • 更改了断开连接行为，以便通过注销终止用户的会话。 • 增加了对时区重定向的支持。 • 延长了登录超时时间并添加了配置选项。 • 修复了一些升级问题。 • 缺陷修复和性能改进。
• Windows WorkSpaces -2.0.0.829	2023 年 6 月 8 日	• 更改了断开连接的行为，以便通过注销终止用户的会话。 • 修复了与 A/V 同步和日语键盘相关的错误。 • 提高了 DCV 安装程序的可靠性。
• Ubunt WorkSpaces u-2.1.0.829	2023 年 5 月 16 日	• 更改了断开连接的行为，以便通过注销终止用户的会话。 • 增加了对 DCV Extension SDK 的支持，以启用特定于 ISV 的集成功能。 • 增加了对时区重定向的支持。 • 修复了一些升级问题。

发布版本	日期	更改
• Windows WorkSpaces -2.0.0.799	2023 年 5 月 8 日	• 通过若干可提高图像质量和性能的优化功能，增强了基于 UDP 的 QUIC 传输能力。 • 增加了对 DCV Extension SDK 的支持，以启用特定于 ISV 的集成功能。 • 添加了新的组策略设置以启用或禁用 Extension SDK。 • 改进了韩语、日语和德语键盘布局。 • 修复了与会话冻结问题、硬件加速、打印机重定向、日志详细程度和 target-fps 组策略设置相关的错误。

Note

- 有关如何检查主机代理版本的信息，请参阅最新版本的 DCV 支持哪些客户端和主机操作系统？。
- 有关如何更新主机代理版本的信息，请参阅如果我已经有 DCV WorkSpace，如何更新？ 。
- 有关 DCV macOS 客户端版本发行说明，请参阅《用户指南》中 WorkSpaces macOS 客户端应用程序部分的发行说明。 WorkSpaces
- 有关 DCV Windows 客户端版本发行说明，请参阅《 WorkSpaces 用户指南》中 WorkSpaces Windows 客户端应用程序部分的发行说明。

使用和管理 WorkSpaces Pools

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

WorkSpaces Pools 提供非永久虚拟桌面，专为需要访问临时基础结构上托管的精心挑选的桌面环境的用户量身定制。

主题

- WorkSpaces Pools 的 Amazon Web Services 区域和可用区
- 管理 WorkSpaces 池的目录
- WorkSpaces Pools 的网络和访问权限
- 创建 WorkSpaces Pools
- 管理 WorkSpaces Pools
- 将 Active Directory 与 WorkSpaces Pools 结合使用
- WorkSpaces Pools 的捆绑包和映像
- 监控 WorkSpaces Pools
- 为 WorkSpaces Pools 启用和管理永久存储
- 为 WorkSpaces Pools 用户启用应用程序设置持久性。
- WorkSpaces Pools 通知代码问题排查

WorkSpaces Pools 的 Amazon Web Services 区域和可用区

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

WorkSpaces Pools 在以下 Amazon Web Services 区域中可用。

> **Note**
>
> 有关适用于 WorkSpaces 个人版的 Amazon Web Services 区域，请参阅《Amazon Web Services 一般参考 参考指南》中的 Amazon WorkSpaces 端点和配额。

区域名称	区域	端点	协议	可用区
美国东部（弗吉尼亚州北部）	us-east-1	workspaces.us-east-1.amazonaws.com workspaces-fips.us-east-1.amazonaws.com	HTTPS HTTPS	use1-az2、use1-az4、use1-az6
美国西部（俄勒冈州）	us-west-2	workspaces.us-west-2.amazonaws.com workspaces-fips.us-west-2.amazonaws.com	HTTPS HTTPS	usw2-az1、usw2-az2、usw2-az3
亚太地区（孟买）	ap-south-1	workspaces.ap-south-1.amazonaws.com	HTTPS	aps1-az1、aps1-az3
亚太地区（首尔）	ap-northeast-2	workspaces.ap-northeast-2.amazonaws.com	HTTPS	apne2-az1、apne2-az3
亚太地区（新加坡）	ap-southeast-1	workspaces.ap-southeast-1.amazonaws.com	HTTPS	apse1-az1、apse1-az2

区域名称	区域	端点	协议	可用区
亚太地区（悉尼）	ap-southeast-2	workspaces.ap-southeast-2.amazonaws.com	HTTPS	apse2-az1、apse2-az3
亚太地区（东京）	ap-northeast-1	workspaces.ap-northeast-1.amazonaws.com	HTTPS	apne1-az1、apne1-az4
加拿大（中部）	ca-central-1	workspaces.ca-central-1.amazonaws.com	HTTPS	cac1-az1、cac1-az2
欧洲地区（法兰克福）	eu-central-1	workspaces.eu-central-1.amazonaws.com	HTTPS	euc1-az2、euc1-az3
欧洲地区（爱尔兰）	eu-west-1	workspaces.eu-west-1.amazonaws.com	HTTPS	euw1-az1、euw1-az2、euw1-az3
欧洲（伦敦）	eu-west-2	workspaces.eu-west-2.amazonaws.com	HTTPS	euw2-az2、euw2-az3

区域名称	区域	端点	协议	可用区
欧洲（巴黎）	eu-west-3	workspaces.eu-west-3.amazonaws.com	HTTPS	euw3-az1、euw3-az2、euw3-az3
南美洲（圣保罗）	sa-east-1	workspaces.sa-east-1.amazonaws.com	HTTPS	sae1-az1、sae1-az3

管理 WorkSpaces 池的目录

> **Important**
>
> “ WorkSpaces 池” 功能不适用于北京和宁夏区域。

WorkSpaces Pools 使用目录来存储和管理您 WorkSpaces 和用户的信息。在本节中，我们将向您展示如何为 WorkSpaces 池创建和管理目录。

内容

- 配置 SAML 2.0 并创建 WorkSpaces 池目录
- 更新 WorkSpaces Pools 的目录详细信息
- 删除 WorkSpaces 池目录

配置 SAML 2.0 并创建 WorkSpaces 池目录

> **Important**
>
> “ WorkSpaces 池” 功能不适用于北京和宁夏区域。

您可以通过使用 SAML 2.0 设置联合身份来启用 WorkSpaces 客户端应用程序注册和登录 WorkSpaces 池。 WorkSpaces 为此，您可以使用 Amazon Identity and Access Management（IAM）角色和中继状态 URL 来配置您的 SAML 2.0 身份提供者（IdP），并为 Amazon 启用它。这将授予您的联合用户访问 WorkSpace 池目录的权限。中继状态是用户在成功登录后被转发到的 WorkSpaces 目录端点Amazon。

> **Important**
>
> WorkSpaces 池不支持基于 IP 的 SAML 2.0 配置。

主题

- 步骤 1：考虑要求
- 步骤 2：完成先决条件
- 步骤 3：在 IAM 中创建 SAML 身份提供者
- 步骤 4：创建 WorkSpace 池目录
- 步骤 5：创建 SAML 2.0 联合身份验证 IAM 角色
- 步骤 6：配置 SAML 2.0 身份提供者
- 步骤 7：为 SAML 身份验证响应创建断言
- 步骤 8：配置联合身份验证的中继状态
- 步骤 9：在 WorkSpace 池目录上启用与 SAML 2.0 的集成
- 问题排查
- 为 P WorkSpaces ools 目录指定活动目录的详细信息

步骤 1：考虑要求

在为 P WorkSpaces ools 目录设置 SAML 时，需要满足以下要求。

- workspaces_ DefaultRole IAM 角色必须存在于您的账户中。Amazon当您使用 WorkSpaces 快速设置或之前使用启动时，系统会自动创建此角色Amazon Web Services 管理控制台。 WorkSpace 它授予 Amazon 代表您访问特定Amazon资源的 WorkSpaces权限。如果该角色已经存在，则可能需要为其附加 AmazonWorkSpacesPoolServiceAccess托管策略，Amazon WorkSpaces 使用该策略访问 WorkSpaces 池Amazon账户中的所需资源。有关更多信息，请参阅创建工作空间_ 角色 DefaultRole 和Amazon托管策略： AmazonWorkSpacesPoolServiceAccess。

- 您可以在中为支持该Amazon Web Services 区域功能的 WorkSpaces 池配置 SAML 2.0 身份验证。有关更多信息，请参阅 WorkSpaces Pools 的 Amazon Web Services 区域和可用区。
- 要将 SAML 2.0 身份验证与一起使用 WorkSpaces，IdP 必须通过深度链接目标资源或中继状态端点 URL 支持未经请求的 IdP 发起的 SSO。这方面的 IdPs 支持示例包括 ADFS、Azure AD、Duo Single Sign-On、Okta 和。 PingFederate PingOne有关更多信息，请参阅 IdP 文档。
- 仅以下 WorkSpaces 客户端支持 SAML 2.0 身份验证。要了解最新 WorkSpaces 客户，请查看 Amazon WorkSpaces 客户端下载页面。
  - Windows 客户端应用程序 5.20.0 或更高版本
  - macOS 客户端 5.20.0 或更高版本
  - Web Access

步骤 2：完成先决条件

在配置与池目录的 SAML 2.0 IdP 连接之前，请完成以下先决条件 WorkSpaces 。

- 配置 IdP 以与 Amazon 建立信任关系
- 有关配置Amazon联合的更多信息，请参阅将第三方 SAML 解决方案提供商与Amazon集成。相关示例包括将 IdP 与 IAM 进行集成以访问 Amazon Web Services 管理控制台。
- 使用您的 IdP 生成和下载联合身份验证元数据文档，该文档将您的组织描述为 IdP。此签名 XML 文档用于建立信赖方信任关系。将该文件保存您稍后可通过 IAM 控制台访问的位置。
- 使用 WorkSpaces 控制台创建 WorkSpaces 池目录。有关更多信息，请参阅 将 Active Directory 与 WorkSpaces Pools 结合使用。
- 为可以使用支持的目录类型登录 IdP 的用户创建 WorkSpaces 池。有关更多信息，请参阅 创建 WorkSpaces Pools 。

步骤 3：在 IAM 中创建 SAML 身份提供者

要开始使用，您必须在 IAM 中创建 SAML IdP。此 IdP 使用组织中 IdP 软件生成的元数据文档定义贵组织的 IdP Amazon 信任关系。有关更多信息，请参阅《Amazon Identity and Access Management 用户指南》中的创建和管理 SAML 身份提供者。有关 IdPs 在中使用 SAML 的信息 Amazon GovCloud (US) Regions，请参阅《Amazon GovCloud (US)用户指南》Amazon Identity and Access Management中的。

步骤 4：创建 WorkSpace 池目录

完成以下过程以创建 WorkSpaces 池目录。

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在导航窗格中，选择目录。
3. 选择创建目录。
4. 对于WorkSpace 类型，请选择池。
5. 在该页面的用户身份源部分：
   a. 在用户访问 URL 文本框中输入占位符值。例如，在文本框中输入 `placeholder`。稍后在您的 IdP 中设置应用程序授权后，您需要对其进行编辑。
   b. 将中继状态参数名称文本框留空。稍后在您的 IdP 中设置应用程序授权后，您需要对其进行编辑。
6. 在该页面的目录信息部分，输入目录的名称和描述。目录名称和描述必须少于 128 个字符，可以包含字母数字字符和以下特殊字符：`_ @ # % * + = : ? . / ! \ -`。目录名称和描述不能以特殊字符开头。
7. 在该页面的网络和安全部分：
   a. 选择对您的应用程序需要的网络资源有访问权的一个 VPC 和两个子网。为了提高容错能力，您应选择位于不同可用区中的两个子网。
   b. 选择允许 WorkSpaces 在您的 VPC 中创建网络链接的安全组。安全组控制允许哪些网络流量流入您的 VPC。 WorkSpaces 例如，如果您的安全组限制所有入站 HTTPS 连接，则访问您的 Web 门户的用户将无法从中加载 HTTPS 网站。 WorkSpaces
8. Active Directory 配置为可选部分。但是，如果您计划在池中使用 AD，则应在创建 WorkSpaces 池目录时指定活动目录 (AD) 详细信息。 WorkSpaces 创建 WorkSpaces 池目录的 Active Directory Config 后，您就无法对其进行编辑。有关为 WorkSpaces 池目录指定 AD 详细信息的更多信息，请参阅为 P WorkSpaces ools 目录指定活动目录的详细信息。完成该主题中概述的过程后，应返回本主题以完成创建 WorkSpaces 池目录。

   如果您不打算在 WorkSpaces 池中使用 AD，则可以跳过 A ctive Directory Config 部分。
9. 在该页面的流式传输属性部分：
   - 选择剪贴板权限行为，选择“复制到本地字符限制”（可选），“粘贴到远程会话字符限制”（可选）。
   - 选择允许或不允许打印到本地设备。
   - 选择允许或不允许诊断日志记录。
   - 选择允许或不允许智能卡登录。仅当您在本步骤前面启用了 AD 配置时，此功能才适用。
10. 在该页面的存储部分，您可以选择启用主文件夹。

11. 在该页面的 IAM 角色部分，选择一个可供所有桌面流实例使用的 IAM 角色。要创建新的 IAM 角色，请选择创建新的 IAM 角色。

    当您将账户中的 IAM 角色应用到 WorkSpace 池目录时，您可以从 WorkSpace 池 WorkSpace 中的发出 Amazon API 请求，而无需手动管理Amazon证书。有关更多信息，请参阅《Amazon Identity and Access Management 用户指南》中的创建向 IAM 用户委派权限的角色。
12. 选择创建目录。

步骤 5：创建 SAML 2.0 联合身份验证 IAM 角色

完成以下过程，在 IAM 控制台中创建 SAML 2.0 联合身份验证 IAM 角色。

1. 使用 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 在导航窗格中选择 Roles。
3. 选择创建角色。
4. 为受信任的实体类型选择 SAML 2.0 联合身份验证。
5. 对于基于 SAML 2.0 的提供者，选择您在 IAM 中创建的身份提供者。有关更多信息，请参阅在 IAM 中创建 SAML 身份提供者。
6. 选择仅允许编程访问以允许访问。
7. 对于“属性”，选择 SAML:sub_type。
8. 对于值，请输入 `https://signin.aws.amazon.com/saml`。该值限制角色访问 SAML 用户流式传输请求，其中包括值为 `persistent` 的 SAML 主题类型断言。如果 SAML:sub_type 为 persistent，则在来自特定用户的所有 SAML 请求中，您的 IdP 会为 `NameID` 元素发送相同的唯一值。有关更多信息，请参阅《Amazon Identity and Access Management 用户指南》中的唯一识别基于 SAML 的联合身份验证中的用户。
9. 选择下一步以继续。
10. 请勿在添加权限页面中进行更改或选择。选择下一步以继续。
11. 输入角色的名称和描述。
12. 选择创建角色。
13. 在角色页面上，选择您必须创建的角色。
14. 选择 Trust relationships（信任关系）选项卡。
15. 选择编辑信任策略。

16. 在编辑信任策略 JSON 文本框中，将 st TagSession s: 操作添加到信任策略。有关更多信息，请参阅《Amazon Identity and Access Management 用户指南》中的在 Amazon STS 中传递会话标签。

    结果应该类似以下示例。

```
1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Effect": "Allow",
6              "Principal": {
7                  "Federated": "arn:aws:iam::[redacted]:saml-provider/[redacted]"
8              },
9              "Action": [
10                 "sts:AssumeRoleWithSAML",
11                 "sts:TagSession"
12             ],
13             "Condition": {
14                 "StringEquals": {
15                     "SAML:sub_type": "persistent"
16                 }
17             }
18         }
19     ]
20 }
```

17. 选择更新策略。
18. 选择权限选项卡。
19. 在该页面的权限策略部分，选择添加权限，然后选择创建内联策略。
20. 在该页面的策略编辑器部分，选择 JSON。
21. 在策略编辑器 JSON 文本框中，输入以下策略。请务必替换以下内容：

    - *<region-code>*使用您在其中创建 WorkSpace 池目录的Amazon区域的代码。
    - *<account-id>*使用Amazon账户 ID。
    - *<directory-id>*使用您之前创建的目录的 ID。你可以在 WorkSpaces控制台中获得这个。

    对于中的资源Amazon GovCloud (US) Regions，请使用以下格式的 ARN：。`arn:aws-us-gov:workspaces:<region-code>:<account-id>:directory/<directory-id>`
22. 选择下一步。
23. 为策略输入名称，然后选择 Create policy (创建策略)。

步骤 6：配置 SAML 2.0 身份提供者

根据您的 SAML 2.0 IdP，您可能需要手动更新 IdP，以信任 Amazon 作为服务提供者。为此，您可以下载在 https://signin.aws.amazon.com/static/saml-metadata.xml 中找到的`saml-metadata.xml`文件，然后将其上传到您的 IdP。这会更新您 IdP 的元数据。

对于某些人来说 IdPs，更新可能已经配置好了。如果已经配置，可以跳过此步骤。如果您的 IdP 中尚未配置此更新，请查看您的 IdP 提供的文档，了解有关如何更新元数据的信息。一些提供者为您提供了以下选项：将 XML 文件的 URL 键入到控制面板并由 IdP 获取和安装该文件。另一些提供者则要求您从该 URL 处下载该文件，然后将其上传到控制面板。

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

步骤 7：为 SAML 身份验证响应创建断言

将您的 IdP 发送到的信息配置为其Amazon身份验证响应中的 SAML 属性。根据您的 IdP，可能已经配置了此类信息。如果已经配置，可以跳过此步骤。如果尚未配置，请提供以下信息：

- SAML 主题 NameID - 登录用户的唯一标识符。请勿更改此 format/value 字段的。否则，主文件夹功能将无法按预期运行，因为该用户将被视为其他用户。

  > **Note**
  >
  > 对于已加入域的 WorkSpaces 池，必须使用以的格式为用户提供`NameID`值`sAMAccountName`，或者`domain\username``username@domain.com`格式使用`userPrincipalName`或仅提供。`userName`如果您要使用 `sAMAccountName` 格式，则可以使用 NetBIOS 名称或完全限定域名（FQDN）指定域。Active Directory 单向信任方案需要 `sAMAccountName` 格式。有关更多信息，请参阅将 Active Directory 与 WorkSpaces Pools 结合使用。如果仅提供 `userName`，用户将登录到主域

- SAML 主题类型（值设为 **`persistent`**）– 将值设为 `persistent` 可确保在来自特定用户的所有 SAML 请求中，您的 IdP 会为 `NameID` 元素发送相同的唯一值。请确保您的 IAM 策略包含一个条

件，仅允许将 SAML `sub_type` 设置为 `persistent` 的 SAML 请求（如步骤 5：创建 SAML 2.0 联合身份验证 IAM 角色一节所述）。

- **`AttributeName`**属性设置为 “ https://aws.amazon.com/SAML/属性/角色” 的元素 — 此元素包含一个或多个元素，这些`AttributeValue`元素列出了您的 IDP 将用户映射到的 IAM 角色和 SAML IdP。角色和 IdP 以逗号分隔的一对指定。 ARNs预期值的一个示例是 `arn:aws:iam::<account-id>:role/<role-name>,arn:aws:iam::<account-id>:saml-provider/<provider-name>`。
- **`AttributeName`**属性设置为 A https://aws.amazon.com/SAML/ ttributes/ 的元素 RoleSessionName — 此元素包含一个`AttributeValue`元素，该元素为为 SSO 颁发的Amazon临时证书提供标识符。`AttributeValue` 元素中值的长度必须介于 2 到 64 个字符之间，只能包含字母数字字符和以下特殊字符：`_ . : / = + - @`。它不能包含空格。该值通常是电子邮件地址或用户主体名 (UPN)。该值不应包含空格，如用户的显示名称。
- **`AttributeName`**属性设置为 Att https://aws.amazon.com/SAML/ ributes/: Email 的元素 PrincipalTag — 此元素包含一个提供`AttributeValue`用户电子邮件地址的元素。该值必须与 WorkSpaces 目录中定义的 WorkSpaces 用户电子邮件地址相匹配。标签值可能包括字母、数字、空格和 `_ . : / = + - @` 字符的组合。有关更多信息，请参阅《Amazon Identity and Access Management 用户指南》中的 IAM 和 Amazon STS 的标记规则。
- （可选）**`Name`**属性设置为 A https://aws.amazon.com/SAML/ ttributes/PrincipalTag: 的**`Attribute`**元素 UserPrincipalName — 此元素包含一个`userPrincipalName`为登录用户提供 Active Directory 的`AttributeValue`元素。必须采用 `username@domain.com` 格式提供该值。此参数与基于证书的身份验证一起使用，作为最终用户证书中的主题备用名称。有关更多信息，请参阅基于证书的身份验证和个人 WorkSpaces 。
- （可选）**`Name`**属性设置为 A https://aws.amazon.com/SAML/ ttributes/PrincipalTag:ObjectSid （可选）的**`Attribute`**元素-此元素包含一个为登录用户提供 Active Directory 安全标识符 (SID) 的`AttributeValue`元素。此参数与基于证书的身份验证一起使用，以启用到 Active Directory 用户的强映射。有关更多信息，请参阅 基于证书的身份验证和个人 WorkSpaces 。
- （可选）**`Name`**属性设置为 At https://aws.amazon.com/SAML/ tributes/: Domain 的**`Attribute`**元素 PrincipalTag — 此元素包含一个为登录用户提供 Active Directory DNS 完全限定域名 (FQDN) 的元素`AttributeValue`。当用户的 Active Directory `userPrincipalName` 包含备用后缀时，此参数用于基于证书的身份验证。必须以 `domain.com` 格式提供该值，且必须包括所有子域名。
- （可选）**`Name`**属性设置为 A https://aws.amazon.com/SAML/ ttributes/ 的**`Attribute`**元素 SessionDuration — 此元素包含一个`AttributeValue`元素，用于指定在要求重新进行身份验证之前，用户的联合流媒体会话可以保持活动状态的最长时间。默认值为 `3600` 秒（60 分钟）。有关更多信息，请参阅《Amazon Identity and Access Management用户指南》SessionDurationAttribute中的 SAML。

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

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

步骤 8：配置联合身份验证的中继状态

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

以下为中继状态 URL 格式：

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

下表列出了可用 WorkSpaces SAML 2.0 身份验证的Amazon区域的中继状态端点。 Amazon无法使用 WorkSpaces 池功能的区域已被移除。

Region	中继状态端点
美国东部（弗吉尼亚州北部）区域	• workspaces.euc-sso.us-east-1.aws.amazon.com • (FIPS) 工作空间。 euc-sso-fips.us-east-1.aws.amazon.com
美国西部（俄勒冈州）区域	• workspaces.euc-sso.us-west-2.aws.amazon.com • (FIPS) 工作空间。 euc-sso-fips.us-west-2.aws.amazon.com

Region	中继状态端点
亚太地区（孟买）区域	workspaces.euc-sso.ap-south-1.aws.amazon.com
亚太地区（首尔）区域	workspaces.euc-sso.ap-northeast-2.aws.amazon.com
亚太地区（新加坡）区域	workspaces.euc-sso.ap-southeast-1.aws.amazon.com
亚太地区（悉尼）区域	workspaces.euc-sso.ap-southeast-2.aws.amazon.com
亚太地区（东京）区域	workspaces.euc-sso.ap-northeast-1.aws.amazon.com
加拿大（中部）区域	workspaces.euc-sso.ca-central-1.aws.amazon.com
欧洲地区（法兰克福）区域	workspaces.euc-sso.eu-central-1.aws.amazon.com
欧洲地区（爱尔兰）区域	workspaces.euc-sso.eu-west-1.aws.amazon.com
欧洲地区（伦敦）区域	workspaces.euc-sso.eu-west-2.aws.amazon.com
南美洲（圣保罗）区域	workspaces.euc-sso.sa-east-1.aws.amazon.com

Region	中继状态端点
AmazonGovCloud（美国西部）	• workspaces.euc-so。 us-gov-west-1。 amazonaws-us-gov.com • (FIPS) 工作空间。 euc-sso-fips。 us-gov-west-1。 amazonaws-us-gov.com Note 有关 IdPs 在中使用 SAML 的信息 Amazon GovCloud (US) Regions，请参阅 AmazonGovCloud（美国）用户指南 WorkSpaces中的 Amazon。
AmazonGovCloud（美国东部）	• workspaces.euc-so。 us-gov-east-1。 amazonaws-us-gov.com • (FIPS) 工作空间。 euc-sso-fips。 us-gov-east-1。 amazonaws-us-gov.com Note 有关 IdPs 在中使用 SAML 的信息 Amazon GovCloud (US) Regions，请参阅 AmazonGovCloud（美国）用户指南 WorkSpaces中的 Amazon。

步骤 9：在 WorkSpace 池目录上启用与 SAML 2.0 的集成

完成以下过程为 WorkSpaces 池目录启用 SAML 2.0 身份验证。

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在导航窗格中，选择目录。
3. 选择池目录选项卡。
4. 选择要编辑的目录 ID。

5. 在该页面的身份验证部分，选择编辑。
6. 选择编辑 SAML 2.0 身份提供者。
7. 对于用户访问 URL（有时也称为“SSO URL”），将占位符值替换为您的 IdP 提供给您的 SSO URL。
8. 对于 IdP 深层链接参数名称，输入适用于您的 IdP 和您配置的应用程序的参数。如果省略该参数名称，则默认值为 `RelayState`。

   下表列出了应用程序的各种身份提供商所独有的用户访问权限 URLs 和深度链接参数名称。

身份提供者	参数	用户访问 URL
ADFS	`RelayState`	https://*<host>*/adfs/ls/idpinitiatedsignon.aspx?RelayState=RPID= *<relaying-party-uri>*
Azure AD	`RelayState`	https://myapps.microsoft.com/signin/ *<app-id>*?tenantId= *<tenant-id>*
Duo Single Sign-On	`RelayState`	https://*<sub-domain>* .sso.duosecurity.com/saml2/sp/ *<app-id>*/sso
Okta	`RelayState`	https://*<sub-domain>* .okta.com/app/*<app-name>* /*<app-id>*/sso/saml
OneLogin	`RelayState`	https://*<sub-domain>* .onelogin.com/trust/saml2/http-post/sso/ *<app-id>*

身份提供者	参数	用户访问 URL
JumpCloud	`RelayState`	`https://sso.jumpcloud.com/saml2/` *`<app-id>`*
Auth0	`RelayState`	`https://`*`<default-tenant-name>`*`.us.auth0.com/samlp/`*`<client-id>`*
PingFederate	`TargetResource`	`https://`*`<host>`*`/idp/startSSO.ping?PartnerSpId=`*`<sp-id>`*
PingOne 适用于企业	`TargetResource`	`https://sso.connect.pingidentity.com/sso/sp/initsso?saasid=`*`<app-id>`*`&idpid=`*`<idp-id>`*

9. 选择保存。

> **Important**
>
> 撤销用户的 SAML 2.0 不会直接断开其会话连接。只有在超时开始后，才会删除这些会话。他们也可以使用 TerminateWorkspacesPoolSessionAPI 将其终止。

问题排查

以下信息可以帮助您解决 WorkSpaces 池的特定问题。

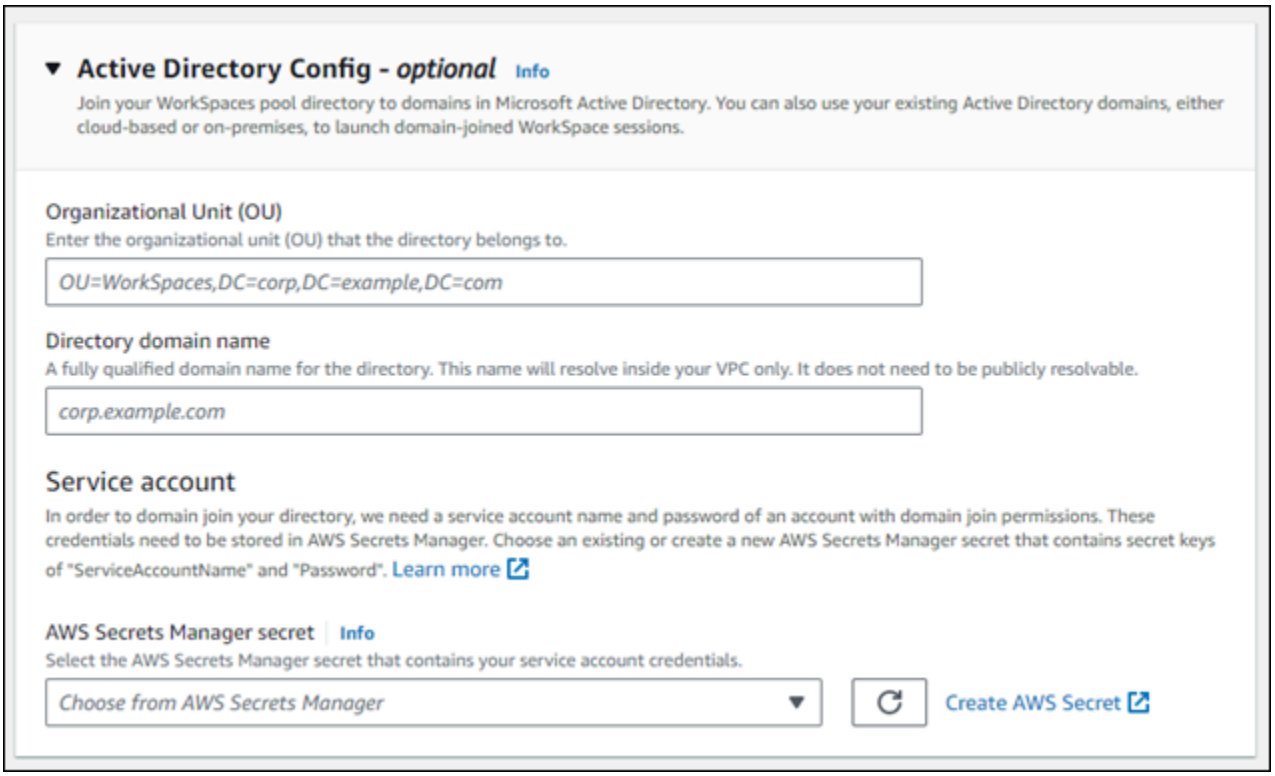
完成 SAML 身份验证后，我在 P WorkSpaces ools 客户端中收到 “无法登录” 消息

SAML 声明中的 `nameID` 和 `PrincipalTag:Email` 需要与 Active Directory 中配置的用户名和电子邮件地址相匹配。调整某些属性后，某些 IdP 可能需要更新、刷新或重新部署。如果您进行了调整，但未反映在您的 SAML 捕获中，请参阅您的 IdP 文档或支持计划，了解使更改生效所需的具体步骤。

为 P WorkSpaces ools 目录指定活动目录的详细信息

> **Important**
>
> “ WorkSpaces 池” 功能不适用于北京和宁夏区域。

在本主题中，我们将向您展示如何在 WorkSpaces 控制台的 “创建 WorkSpaces 池目录” 页面中指定 Active Directory (AD) 详细信息。在创建 WorkSpaces 池目录时，如果您计划在 WorkSpaces 池中使用 AD，则应指定 AD 详细信息。创建 WorkSpaces 池目录的 Active Directory Config 后，就无法对其进行编辑。以下是 “创建 WorkSpaces 池目录” 页面的 Active Directory Config 部分的示例。



> **Note**
>
> 配置 SAML 2.0 并创建 WorkSpaces 池目录主题概述了创建 WorkSpaces 池目录的完整过程。本页概述的过程仅代表创建 WorkSpaces 池目录的完整过程中的一部分步骤。

主题

- 为 AD 指定组织部门和目录域名
- 为 AD 指定服务账户

为 AD 指定组织部门和目录域名

完成以下步骤，在 “创建 WorkSpaces 池目录” 页面中为 AD 指定组织单位 (OU) 和目录域名。

1. 在组织单位中，输入池所属的 OU。 WorkSpace 计算机帐户位于您为 WorkSpaces 池目录指定的组织单位 (OU) 中。

   > **Note**
   >
   > OU 名称中不得包含空格。如果您指定包含空格的 OU 名称，则当它尝试重新加入 Active Directory 域时，将 WorkSpaces 无法正确循环使用计算机对象，并且无法重新加入域。

2. 对于目录域名，输入 Active Directory 域的完全限定域名（FQDN）(例如，`corp.example.com`)。每个Amazon区域只能有一个带有特定目录名称的目录配置值。

   - 你可以将你的 WorkSpaces 池目录加入到 Microsoft 活动目录中的域中。您还可以使用现有的 Active Directory 域（基于云或本地）来启动已加入域 WorkSpaces名。
   - 也可以使用Amazon Directory Service for Microsoft Active Directory（也称为Amazon Managed Microsoft AD）来创建 Active Directory 域。然后，您可以使用该域来支持您的 WorkSpaces 资源。
   - WorkSpaces 加入您的活动目录域名后，您可以：
     - 允许您的用户和应用程序从流式传输会话访问 Active Directory 资源（如打印机和文件共享）。
     - 使用组策略管理控制台 (GPMC) 中可用的组策略设置定义最终用户体验。
     - 流式传输需要用户使用 Active Directory 登录凭证进行身份验证的应用程序。
     - 将企业合规性和安全策略应用于您的 WorkSpaces 流实例。
3. 对于服务账户，继续执行本页的下一节为 AD 指定服务账户。

为 AD 指定服务账户

在目录创建过程中为 WorkSpaces 池配置 Active Directory (AD) 时，必须指定用于管理 AD 的 AD 服务帐户。这要求您提供服务帐号凭证，这些凭据必须存储在客户托管密钥中Amazon Secrets Manager并使用 Amazon Key Management Service (Amazon KMS) 客户托管密钥进行加密。在本节中，我们将向您展示如何创建Amazon KMS客户托管密钥和 Secrets Manager 密钥来存储您的 AD 服务帐号凭证。

步骤 1：创建 Amazon KMS 客户托管式密钥

完成以下步骤以创建Amazon KMS客户托管密钥

1. 在 https://console.aws.amazon.com/km Amazon KMS s 处打开控制台。
2. 要更改Amazon Web Services 区域，请使用页面右上角的区域选择器。
3. 选择创建密钥，然后选择下一步。
4. 为密钥类型选择对称，为密钥使用选择加密和解密，然后选择下一步。
5. 输入密钥的别名，例如 `WorkSpacesPoolDomainSecretKey`，然后选择下一步。
6. 不要选择密钥管理员。选择下一步以继续。
7. 不要定义密钥使用权限。选择下一步以继续。
8. 在该页面的“密钥策略”部分，添加以下内容：

```
        {
            "Sid": "Allow access for Workspaces SP",
            "Effect": "Allow",
            "Principal": {
                "Service": "workspaces.amazonaws.com"
            },
            "Action": "kms:Decrypt",
            "Resource": "*"
        }
```

结果应该类似以下示例。

```
4    "Statement": [
5        {
6            "Sid": "Enable IAM User Permissions",
7            "Effect": "Allow",
8            "Principal": {
9                "AWS": "arn:aws:iam::[redacted]:root"
10           },
11           "Action": "kms:*",
12           "Resource": "*"
13       },
14       {
15           "Sid": "Allow access for Workspaces SP",
16           "Effect": "Allow",
17           "Principal": {
18               "Service": [
19                   "workspaces.amazonaws.com"
20               ]
21           },
22           "Action": "kms:Decrypt",
23           "Resource": "*"
24       }
```

9. 选择结束。

您的Amazon KMS客户托管密钥现在可以与 Secrets Manager 一起使用了。继续执行本页的步骤 2：创建 Secrets Manager 密钥来存储 AD 服务账户凭证一节。

步骤 2：创建 Secrets Manager 密钥来存储 AD 服务账户凭证

完成以下步骤，创建 Secrets Manager 密钥来存储您的 AD 服务账户凭证。

1. 打开Amazon Secrets Manager控制台，网址为https://console.aws.amazon.com/secretsmanager/。
2. 选择 Create a new secret (创建新密钥)。
3. 选择其他密钥类型。
4. 对于第一 key/value 对，输入`Service Account Name`密钥和值的服务帐号名称，例如`domain\username`。
5. 对于第二 key/value 对，`Service Account Password`为密钥输入 a，为值输入服务帐户的密码。
6. 对于加密密钥，请选择您之前创建的Amazon KMS客户托管密钥，然后选择下一步。
7. 输入密钥的名称，例如 `WorkSpacesPoolDomainSecretAD`。
8. 在该页面的资源权限部分，选择编辑权限。
9. 输入以下权限策略：

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "workspaces.amazonaws.com"
                ]
            },
            "Action": "secretsmanager:GetSecretValue",
            "Resource": "*"
        }
    ]
```

```
}
```

10. 选择保存以保存权限策略。
11. 选择下一步以继续。
12. 不要配置自动轮换。选择下一步以继续。
13. 选择存储，以完成您密钥的存储。

您的 AD 服务账户凭证现存储在 Secrets Manager 中。继续执行本页的步骤 3：选择包含您的 AD 服务账户凭证的 Secrets Manager 密钥一节。

步骤 3：选择包含您的 AD 服务账户凭证的 Secrets Manager 密钥

完成以下过程，选择你在 Active Directory 配置中为 WorkSpaces 池目录创建的 Secrets Manager 密钥。

- 对于服务帐号，请选择包含您的服务帐号凭据的Amazon Secrets Manager密钥。完成以下步骤，创建密钥（如果尚未执行此操作）。必须使用Amazon Key Management Service客户管理的密钥对密钥进行加密。

现在，您已经完成了创建 WorkSpaces 池目录页面的 Active Directory Config 部分中的所有字段，您可以继续完成 WorkSpaces 池目录的创建。转至步骤 4：创建 WorkSpace 池目录，并从该过程的步骤 9 开始。

更新 WorkSpaces Pools 的目录详细信息

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

您可以使用 WorkSpaces Pools 控制台完成以下目录管理任务。

身份验证

您可以为 WorkSpaces Pools 配置其他身份验证选项。池需要 SAML 2.0 身份验证。

启用和配置 SAML 2.0 身份提供者身份验证

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。

2. 在导航窗格中，选择目录。
3. 选择要配置的目录。
4. 转到“身份验证”，然后选择编辑。
5. 选择编辑 SAML 2.0 身份提供者。
6. 选中启用 SAML 2.0 身份验证复选框。
7. 输入用户访问 URL，以便在联合登录期间定向 WorkSpaces Pools 客户端。
8. 输入 IdP 深层链接参数名称（可选）。
9. 选择 Save。

启用和配置基于证书的身份验证

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。
3. 选择要配置的目录。
4. 转到“身份验证”，然后选择编辑。
5. 选择编辑基于证书的身份验证。
6. 选中启用基于证书的身份验证复选框。
7. 从下拉列表中选择 Amazon Certificate Manager（ACM）私有证书颁发机构（CA）。
8. 选择 Save。

安全组

将安全组应用于目录中的 WorkSpaces Pools。

配置 WorkSpaces 虚拟桌面池的安全组

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。
3. 选择要配置的目录。
4. 转到“安全组”并选择编辑。
5. 从下拉列表中选择一个安全组。

Active Directory 配置

使用组织部门（OU）、目录域名和 Amazon Secrets Manager 密钥配置您的目录 Active Directory 配置。

配置 Active Directory

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。
3. 选择要配置的目录。
4. 转到“Active Directory 配置”，然后选择编辑。
5. 要查找组织部门（OU），您可以开始键入 OU 的全部或部分名称，然后选择要使用的 OU。

> **Note**
>
> （可选）选择 OU 后，重建现有的 WorkSpaces 以更新 OU。有关更多信息，请参阅 重建 WorkSpaces 个人版中的 WorkSpace。

6. 选择 Save。

> **Note**
>
> 创建池后，无法编辑目录域名和 Amazon Secrets Manager 密钥。

流属性

配置用户如何在池化的 WorkSpace 和本地设备之间传输数据。

配置流式传输属性

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。
3. 选择要配置的目录。
4. 转到“流式传输属性”，然后选择编辑。
5. 配置以下流式传输属性：

- 剪贴板权限
  - 从下拉列表中选择以下选项之一：
    - 允许复制和粘贴 - 允许复制到本地设备和粘贴到远程会话。
    - 允许粘贴到远程会话 - 允许粘贴到远程会话。
    - 允许复制到本地设备 - 允许复制到本地设备。
    - 已禁用
  - 选择允许或不允许打印到本地设备。
  - 选择允许或不允许诊断日志记录。
  - 选择允许或不允许智能卡登录。
  - 要启用主文件夹存储，请选择启用主文件夹。

6. 选择 Save。

IAM 角色

为您的 WorkSpaces Pools 选择 IAM 角色。

选择 IAM 角色

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。
3. 选择要配置的目录。
4. 转到 IAM 角色并选择编辑。
5. 从下拉列表中选择 IAM 角色。要创建新的 IAM 角色，请选择创建新的 IAM 角色。
6. 选择 Save。

标签

向您的 WorkSpaces Pools 添加新标签

添加新标签

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。

3. 选择要配置的目录。
4. 转到“标签”，然后选择管理标签。
5. 选择添加新标签，然后输入要使用的密钥对值。键可以是具有特定关联值的一般类别，例如“project”、“owner”或“environment”。
6. 选择保存更改。

删除 WorkSpaces 池目录

> **Important**
>
> “ WorkSpaces 池” 功能不适用于北京和宁夏区域。

完成以下过程以删除 P WorkSpaces ools 目录。

1. 在 https://console.aws.amazon.com/workspaces/v2/ home 中打开 WorkSpaces 主机。
2. 在导航窗格中，选择目录。
3. 选择目录。
4. 依次选择操作和删除。
5. 当提示您确认时**delete**，输入确认文本并选择删除。

WorkSpaces Pools 的网络和访问权限

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

以下主题提供有关如何使用户能够连接到 WorkSpaces Pools 并使 WorkSpaces Pools 能够访问网络资源和 Internet 的信息。

目录

- WorkSpaces Pools 的 Internet 访问
- 为 WorkSpaces Pools 配置 VPC

- 将 Amazon S3 VPC 终端节点用于 WorkSpaces 池功能
- 连接到 WorkSpaces Pools 的 VPC
- 用户与 WorkSpaces Pools 的连接

WorkSpaces Pools 的 Internet 访问

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

如果您 WorkSpaces Pools 中的 WorkSpaces 需要访问 Internet，则您可以通过多种方式启用它。在选择实现 Internet 访问的方法时，请考虑您的部署必须支持的用户数量以及您的部署目标。例如：

- 如果您的部署必须支持 100 个以上的并发用户，需配置具有私有子网和 NAT 网关的 VPC。
- 如果您的部署支持 100 个以内并发用户，可以使用公有子网配置新的或现有 VPC。
- 如果您的部署支持 100 个以内并发用户，并且您是初次使用 WorkSpaces Pools，希望开始使用该服务，则您可以使用默认 VPC、公有子网和安全组。

以下几部分提供了有关这些部署选项中每一项的更多信息。

- 配置具有私有子网和 NAT 网关的 VPC（推荐）- 使用此配置，您可以在私有子网中启动 WorkSpaces Pools 生成器，并在您 VPC 的公有子网中配置 NAT 网关。您的流实例会被分配一个无法直接从 Internet 访问的私有 IP 地址。

  此外，与使用默认互联网访问选项来启用 Internet 访问的配置不同，NAT 配置不限于 100 个 WorkSpaces Pools 中的 WorkSpaces。如果您的部署必须支持 100 个以上的并发用户，请使用此配置。

  您可以创建和配置新 VPC 来结合使用 NAT 网关，或将 NAT 网关添加到现有 VPC。
- 配置带公有子网的新的或现有 VPC - 使用此配置，您可以在公有子网中启动 WorkSpaces Pools。启用此选项后，WorkSpaces Pools 将在 Amazon VPC 公有子网中使用 Internet 网关来提供 Internet 连接。您的流实例会被分配一个可直接从 Internet 访问的公有 IP 地址。您可以创建新 VPC 或配置现有 VPC 用于此用途。

> **Note**
>
> 为公有子网配置新的或现有 VPC 时，WorkSpaces Pools 最多支持 100 个 WorkSpaces。如果您的部署必须支持 100 个以上的并发用户，请改为使用 NAT 网关配置。

- 使用默认 VPC、公有子网和安全组 - 如果您是初次使用 WorkSpaces Pools 并希望开始使用该服务，则可以在默认公有子网中启动 WorkSpaces Pools。启用此选项后，WorkSpaces Pools 将在 Amazon VPC 公有子网中使用 Internet 网关来提供 Internet 连接。您的流实例会被分配一个可直接从 Internet 访问的公有 IP 地址。

  默认 VPC 在 2013 年 12 月 4 日之后创建的 Amazon Web Services 账户中可用。

  默认 VPC 在各个可用区中包含一个默认公有子网，以及连接到您 VPC 的 Internet 网关。VPC 还包含默认安全组。

  > **Note**
  >
  > 当您使用默认 VPC、公有子网和安全组时，WorkSpaces Pools 最多支持 100 个 WorkSpaces。如果您的部署必须支持 100 个以上的并发用户，请改为使用 NAT 网关配置。

为 WorkSpaces Pools 配置 VPC

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

设置 WorkSpaces Pools 时，您必须指定虚拟私有云（VPC）和至少一个子网，以便在其中启动 WorkSpaces。VPC 是 Amazon Web Services Cloud 内您自己的逻辑隔离区域中的虚拟网络。子网是您的 VPC 内的 IP 地址范围。

为 WorkSpaces Pools 配置 VPC 时，您可以指定公有子网或私有子网，也可以指定两种类型子网的混合。公有子网可以通过 Internet 网关直接访问 Internet。私有子网没有直接指向 Internet 网关的路由，需要网络地址转换 (NAT) 网关或 NAT 实例来提供对 Internet 的访问。

目录

- WorkSpaces Pools 的 VPC 设置建议

- 配置具有私有子网和 NAT 网关的 VPC
- 配置带公有子网的新的或现有 VPC
- 使用默认 VPC、公有子网和安全组

WorkSpaces Pools 的 VPC 设置建议

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

创建 WorkSpaces Pools 时，可以指定要使用的 VPC 以及一个或多个子网。您可以通过指定安全组，为 VPC 提供额外的访问控制。

以下建议可帮助您更安全有效地配置 VPC。此外，它们还可以帮助您配置支持有效 WorkSpaces Pools 扩展的环境。借助有效的 WorkSpaces Pools 扩展，您可以满足当前和预期的 WorkSpaces 用户需求，同时避免不必要的资源使用和相关成本。

VPC 整体配置

- 确保您的 VPC 配置可以支持 WorkSpaces Pools 扩展需求。

  在制定 WorkSpaces Pools 扩展计划时，请记住，一个用户需要一个 WorkSpaces。因此，您的 WorkSpaces Pools 大小决定了可以同时流式传输的用户数。因此，对于您计划使用的每种实例类型，请确保 VPC 可支持的 WorkSpaces 数量大于相同实例类型的预期并发用户数量。
- 确保您的 WorkSpaces Pools 账户配额（也称为限制）足以满足您的预期需求。要请求提高配额，可以使用服务配额控制台，网址为：https://console.aws.amazon.com/servicequotas/。有关默认 WorkSpaces Pools 配额的信息，请参阅 Amazon WorkSpaces 配额。
- 如果您计划为 WorkSpaces Pools 中的 WorkSpaces 提供对 Internet 的访问权限，建议您为流实例配置包含两个私有子网的 VPC，并在公有子网中配置 NAT 网关。

  NAT 网关允许私有子网中的 WorkSpaces 连接到 Internet 或其他 Amazon 服务。但是，它会阻止 Internet 启动与这些 WorkSpaces 的连接。此外，与使用默认互联网访问选项来启用 Internet 访问的配置不同，NAT 配置支持超过 100 个 WorkSpaces。有关更多信息，请参阅 配置具有私有子网和 NAT 网关的 VPC。

弹性网络接口

- WorkSpaces Pools 创建数量与 WorkSpaces Pools 所需的最大容量匹配的弹性网络接口（网络接口）。默认情况下，每个区域的网络接口数限制为 5000。

  在为非常大的部署（例如，数千个 WorkSpaces）规划容量时，请考虑同样在同一区域中使用的 Amazon EC2 实例数量。

子网

- 如果您要为 VPC 配置多个私有子网，请在不同的可用区中配置每个子网。这样做可提高容错能力，并有助于防止出现容量不足错误。如果您在同一个可用区中使用两个子网，可能会用完 IP 地址，因为 WorkSpaces Pools 不会使用第二个子网。
- 请确保可通过您的两个私有子网访问应用程序所需的网络资源。
- 使用允许足够客户端 IP 地址数的子网掩码配置您的各个私有子网，以适应预期的最大并发用户数。此外，允许额外的 IP 地址来容纳预期的增长。有关更多信息，请参阅针对 IPv4 的 VPC 和子网大小调整。
- 如果您在使用带有 NAT 的 VPC，请至少配置一个带有 NAT 网关的公有子网以便访问 Internet，最好配置两个公有子网。在您的私有子网所在的同一可用区中配置公有子网。

  为增强容错能力并减少出现大型 WorkSpaces Pools 部署容量不足错误的可能性，请考虑将 VPC 配置扩展到第三个可用区。在此额外的可用区中包括私有子网、公有子网和 NAT 网关。

安全组

- 使用安全组向您的 VPC 提供额外的访问控制。

  属于您的 VPC 的安全组允许您控制 WorkSpaces Pools 流实例与应用程序所需网络资源之间的网络流量。这些资源可能包括其他 Amazon 服务，例如 Amazon RDS 或 Amazon FSx、许可证服务器、数据库服务器、文件服务器和应用程序服务器。
- 确保安全组提供了对应用程序所需网络资源的访问权限。

  有关安全组的一般信息，请参阅《Amazon VPC 用户指南》中的使用安全组控制指向 Amazon 资源的流量。

配置具有私有子网和 NAT 网关的 VPC

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

如果您计划为 WorkSpaces Pools 中的 WorkSpaces 提供对 Internet 的访问权限，建议您为 WorkSpaces 配置包含两个私有子网的 VPC，并在公有子网中配置 NAT 网关。您可以创建和配置新 VPC 来结合使用 NAT 网关，或将 NAT 网关添加到现有 VPC。有关其他 VPC 配置建议，请参阅 WorkSpaces Pools 的 VPC 设置建议。

NAT 网关允许私有子网中的 WorkSpaces 连接到 Internet 或其他 Amazon 服务，但是阻止 Internet 发起与这些 WorkSpaces 的连接。此外，与使用默认互联网访问选项来为 WorkSpaces 启用 Internet 访问的配置不同，此配置不限于 100 个 WorkSpace。

有关使用 NAT 网关和此配置的信息，请参阅《Amazon VPC 用户指南》中的 NAT 网关和具有公有和私有子网（NAT）的 VPC。

目录

- 创建和配置新 VPC
- 向现有 VPC 添加 NAT 网关
- 为 WorkSpaces Pools 启用 Internet 访问

创建和配置新 VPC

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

本主题介绍如何使用 VPC 向导创建具有一个公有子网和一个私有子网的 VPC。作为此过程的一部分，向导将创建 Internet 网关和 NAT 网关。它还会创建与公有子网关联的自定义路由表，并更新与私有子网关联的主路由表。NAT 网关是在您的 VPC 的公有子网中自动创建的。

使用向导创建初始 VPC 配置后，您将添加第二个私有子网。有关更多信息，请参阅《Amazon VPC 用户指南》中的具有公有和私有子网（NAT）的 VPC。

> **Note**
>
> 如果您已有 VPC，请改为完成向现有 VPC 添加 NAT 网关中的步骤。

目录

- 步骤 1：分配弹性 IP 地址
- 步骤 2：创建新 VPC
- 步骤 3：添加第二个私有子网
- 步骤 4：验证并命名子网路由表

步骤 1：分配弹性 IP 地址

在创建 VPC 之前，您必须在 WorkSpaces 区域中分配弹性 IP 地址。您必须先分配用于 VPC 的弹性 IP 地址，然后将其与 NAT 网关关联。有关更多信息，请参阅《Amazon VPC 用户指南》中的弹性 IP 地址。

> **Note**
>
> 使用弹性 IP 地址可能会产生费用。有关更多信息，请参阅 Amazon EC2 定价页面上的弹性 IP 地址。

如果您还没有弹性 IP 地址，请完成以下步骤。如果需要使用现有的弹性 IP 地址，请确保它当前不与其他实例或网络接口关联。

分配弹性 IP 地址

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中的网络与安全下，选择弹性 IP。
3. 选择 Allocate New Address (分配新地址)，然后选择 Allocate (分配)。
4. 记录弹性 IP 地址。
5. 在 Elastic IPs (弹性 IP) 窗格的右上角，单击 X 图标以关闭窗格。

步骤 2：创建新 VPC

完成以下步骤，创建具有一个公有子网和一个私有子网的新 VPC。

创建新的 VPC

1. 通过 https://console.aws.amazon.com/vpc/ 打开 Amazon VPC 控制台。
2. 在导航窗格中，选择 VPC Dashboard (VPC 控制面板)。
3. 选择 Launch VPC Wizard (启动 VPC 向导)。
4. 在 Step 1: Select a VPC Configuration (步骤 1：选择 VPC 配置) 中，选择 VPC with Public and Private Subnets (带有公有子网和私有子网的 VPC)，然后选择 Select (选择)。
5. 在 Step 2: VPC with Public and Private Subnets (步骤 2：具有公有子网和私有子网的 VPC) 中，如下所示配置 VPC：
   - 对于 IPv4 CIDR block (IPv4 CIDR 块)，为 VPC 指定 IPv4 CIDR 块。
   - 对于 IPv6 CIDR block (IPv6 CIDR 块)，保留默认值 (No IPv6 CIDR block) (无 IPv6 CIDR 块)。
   - 对于 VPC name (VPC 名称)，请键入一个唯一的 VPC 名称。
6. 按照如下所示配置公有子网：
   - 对于 Public subnet's IPv4 CIDR (公有子网的 IPv4 CIDR)，指定子网的 CIDR 块。
   - 对于 Availability Zone (可用区)，保留默认值 No Preference (无首选项)。
   - 对于 Public subnet name (公有子网名称)，键入子网的名称（例如，`WorkSpaces Public Subnet`）。
7. 按照如下所示配置第一个私有子网：
   - 对于 Private subnet's IPv4 CIDR (私有子网的 IPv4 CIDR)，指定子网的 CIDR 块。记下您指定的值。
   - 对于 Availability Zone (可用区)，选择特定区并记下您的选择。
   - 对于 Private subnet name (私有子网名称)，键入子网的名称（例如，`WorkSpaces Private Subnet1`）。
   - 对于其余字段，在适用时保留默认值。
8. 对于 Elastic IP Allocation ID (弹性 IP 分配 ID)，单击文本框并选择与您创建的弹性 IP 地址相对应的值。此地址分配给 NAT 网关。如果您没有弹性 IP 地址，请使用以下网址的 Amazon VPC 控制台创建一个：https://console.aws.amazon.com/vpc/。
9. 对于服务端点，如果您的环境需要 Amazon S3 端点，请指定一个。对于您私有网络中的用户，如果需要访问主文件夹或者启用程序设置持久性，则需要 S3 端点。

   要指定 Amazon S3 端点，请执行以下操作：

a. 选择 Add Endpoint (添加端点)。
b. 对于 Service (服务)，在列表中选择以“s3”结尾的条目（对应于在其中创建 VPC 的区域的 `com.amazonaws.region.s3` 条目）。
c. 对于 Subnet (子网)，选择 Private subnet (私有子网)。
d. 对于 Policy (策略)，保留默认值 Full Access (完全访问)。

10. 对于 Enable DNS hostnames (启用 DNS 主机名)，保留默认值 Yes (是)。
11. 对于 Hardware tenancy (硬件租赁)，保留默认值 Default (默认值)。
12. 选择创建 VPC。
13. 请注意，设置您的 VPC 可能需要几分钟。创建了 VPC 后，选择 OK。

步骤 3：添加第二个私有子网

在上一步（步骤 2：创建新 VPC）中，您创建了具有一个公有子网和一个私有子网的 VPC。执行以下步骤以添加第二个私有子网。我们建议您在与第一个私有子网不同的可用区中添加第二个私有子网。

1. 在导航窗格中，选择 Subnets(子网)。
2. 选择您在上一步骤中创建的第一个私有子网。在 Description (描述) 选项卡上的子网列表下方，记录此子网的可用区。
3. 在子网窗格的左上角，选择 Create Subnet (创建子网)。
4. 对于 Name tag (名称标签)，键入私有子网的名称（例如，`WorkSpaces Private Subnet2`）。
5. 对于 VPC，选择上一步骤中已创建的 VPC。
6. 对于 Availability Zone (可用区)，请选择一个可用区，而不是您用于第一个私有子网的可用区。选择不同的可用区可提高容错能力，并有助于防止容量不足错误。
7. 对于 IPv4 CIDR block (IPv4 CIDR 块)，请为新子网指定唯一的 CIDR 块范围。例如，如果您的第一个私有子网的 IPv4 CIDR 块范围为 `10.0.1.0/24`，则可以为新的私有子网指定 CIDR 块范围 `10.0.2.0/24`。
8. 选择创建。
9. 创建子网后，选择 Close (关闭)。

步骤 4：验证并命名子网路由表

在您创建并配置 VPC 后，请完成以下步骤来为路由表指定名称，并验证：

- 与 NAT 网关所在子网关联的路由表包含使 Internet 流量指向 Internet 网关的路由。这可确保您的 NAT 网关可以访问 Internet。
- 与私有子网关联的路由表配置为将 Internet 流量指向 NAT 网关。这使您的私有子网中的流实例可以与 Internet 通信。

1. 在导航窗格中，选择 Subnets (子网)，然后选择您创建的公有子网（例如 `WorkSpaces Public Subnet`）。
   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) 中，选择编辑图标（铅笔），键入一个名称（例如 `workspaces-public-routetable`），然后选择复选标记以保存该名称。
   c. 选中公有路由表的同时，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 VPC 的 Internet 网关发送所有其他流量。下表对这两种路由进行了说明：

目标位置	目标	描述
公有子网 IPv4 CIDR 块（例如，10.0.0/20）	本地	来自资源的所有流量，如果其目标是公有子网 IPv4 CIDR 块中的 IPv4 地址，则在 VPC 内本地路由。
目标是所有其他 IPv4 地址的流量（例如，0.0.0.0/0）	出站 (`igw-`*`ID`*)	目标是所有其他 IPv4 地址的流量将路由到由 VPC 向导创建的 Internet 网关（由 `igw-`*`ID`* 标识）。

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 Subnet1`）。
   a. 在路由表选项卡上，选择路由表的 ID。
   b. 选择路由表。在 Name (名称) 中，选择编辑图标（铅笔），输入一个名称（例如 `workspaces-private-routetable`），然后选择复选标记以保存该名称。
   c. 在 Routes (路由) 选项卡上，验证路由表包含以下路由：

目标位置	目标	描述
公有子网 IPv4 CIDR 块（例如，10.0.0/20）	本地	来自资源的所有流量，如果其目标是公有子网 IPv4 CIDR 块中的 IPv4 地址，则在 VPC 内本地路由。
目标是所有其他 IPv4 地址的流量（例如，0.0.0.0/0）	出站 (nat-*ID*)	目标是所有其他 IPv4 地址的流量将路由到 NAT 网关（由 nat-*ID* 标识）。
目标是 S3 存储桶的流量（在指定了 S3 端点时适用） [pl-*ID* (com.amazonaws. *region*.s3)]	存储 (vpce-*ID*)	目标是 S3 存储桶的流量将路由到 S3 端点（由 vpce-*ID* 标识）。

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 Subnet2）。
4. 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，请选择编辑，然后选择此路由表。

后续步骤

要使 WorkSpaces Pools 中的 WorkSpaces 能够访问 Internet，请完成为 WorkSpaces Pools 启用 Internet 访问中的步骤。

向现有 VPC 添加 NAT 网关

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

如果您已配置 VPC，请完成以下步骤，将 NAT 网关添加到 VPC。如果您需要创建新 VPC，请参阅创建和配置新 VPC。

向现有 VPC 添加 NAT 网关

1. 要创建 NAT 网关，请完成《Amazon VPC 用户指南》中的创建 NAT 网关中的步骤。
2. 验证您的 VPC 至少有一个私有子网。建议您指定不同的可用区中的两个私有子网以实现高可用性和容错能力。有关如何创建第二个私有子网的信息，请参阅步骤 3：添加第二个私有子网。
3. 更新与您的一个或多个私有子网关联的路由表，以将面向 Internet 的流量指向该 NAT 网关。这使您的私有子网中的流实例可以与 Internet 通信。为此，请完成《Amazon VPC 用户指南》中的更新您的路由表中的步骤。

后续步骤

要使 WorkSpaces Pools 中的 WorkSpaces 能够访问 Internet，请完成为 WorkSpaces Pools 启用 Internet 访问中的步骤。

为 WorkSpaces Pools 启用 Internet 访问

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

在您的 NAT 网关在 VPC 上可用后，您可以为 WorkSpaces Pools 启用 Internet 访问。您可以在创建 WorkSpaces Pools 目录时启用 Internet 访问。创建目录时，选择带有 NAT 网关的 VPC。然后，为子网 1 选择一个私有子网，以及（可选）为子网 2 选择另一个私有子网。如果您的 VPC 中还没有私有子网，则可能需要创建第二个私有子网。

通过启动您的 WorkSpaces Pools 然后连接到池中的 WorkSpace 并浏览到 Internet，您可以测试您的 Internet 连接。

配置带公有子网的新的或现有 VPC

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

如果您的 Amazon Web Services 账户是在 2013 年 12 月 4 日之后创建的，则您在每个 Amazon 区域都有一个包含默认公有子网的默认 VPC。但是，您可能希望创建自己的非默认 VPC 或配置现有 VPC

以用于 WorkSpaces Pools 目录。本主题介绍了如何配置非默认 VPC 和公有子网以用于 WorkSpaces Pools。

配置 VPC 和公有子网后，您可以通过启用默认互联网访问选项，为 WorkSpaces Pools 中的 WorkSpaces 提供 Internet 访问权限。在您启用此选项时，WorkSpaces Pools 通过将弹性 IP 地址关联到从流实例附加到您公有子网的网络接口，启用 Internet 连接。弹性 IP 地址是可通过 Internet 访问的公有 IPv4 地址。因此，我们建议您改用 NAT 网关来提供对您 WorkSpaces Pools 中 WorkSpaces 的 Internet 访问权限。此外，启用默认互联网访问时，最多支持 100 个 WorkSpaces。如果您的部署必须支持 100 个以上的并发用户，请改为使用 NAT 网关配置。

有关更多信息，请参阅配置具有私有子网和 NAT 网关的 VPC 中的步骤。有关其他 VPC 配置建议，请参阅 WorkSpaces Pools 的 VPC 设置建议。

目录

- 步骤 1：配置带公有子网的 VPC
- 步骤 2：为 WorkSpaces Pools 启用默认 Internet 访问

步骤 1：配置带公有子网的 VPC

您可以使用以下任一方法，配置自己的带公有子网的非默认 VPC：

- 创建带单个公有子网的新 VPC
- 配置现有 VPC

创建带单个公有子网的新 VPC

当您使用 VPC 向导创建新 VPC 时，向导将创建一个 Internet 网关以及一个与公有子网关联的自定义路由表。该路由表将发往 VPC 外部地址的所有流量路由到 Internet 网关。有关此配置的更多信息，请参阅《Amazon VPC 用户指南》中的带单个公有子网的 VPC。

1. 完成《Amazon VPC 用户指南》中的步骤 1：创建 VPC 中的步骤，以创建您的 VPC。
2. 要使您的 WorkSpaces 能够访问 Internet，请完成步骤 2：为 WorkSpaces Pools 启用默认 Internet 访问中的步骤。

配置现有 VPC

如果您要使用不带公有子网的现有 VPC，可以添加一个新的公有子网。除了公有子网之外，您还必须有一个连接到 VPC 的 Internet 网关，以及一个将发往 VPC 外地址的所有流量路由到 Internet 网关的路由表。如需配置这些组件，请完成以下步骤。

1. 要添加公有子网，请完成在 VPC 中创建子网中的步骤。使用您计划用于 WorkSpaces Pools 的现有 VPC。

   如果您的 VPC 配置为支持 IPv6 寻址，则会显示 IPv6 CIDR block (IPv6 CIDR 块) 列表。选择 Don't assign Ipv6 (不分配 Ipv6)。
2. 要创建 Internet 网关并将其附加到您的 VPC，请完成创建和附加 Internet 网关中的步骤。
3. 要将您的子网配置为通过 Internet 网关路由 Internet 流量，请完成创建自定义路由表中的步骤。在步骤 5 中，对于 Destination (目标)，请使用 IPv4 格式 (`0.0.0.0/0`)。
4. 要使您的 WorkSpaces 和映像生成器能够访问 Internet，请完成步骤 2：为 WorkSpaces Pools 启用默认 Internet 访问中的步骤。

步骤 2：为 WorkSpaces Pools 启用默认 Internet 访问

您可以在创建 WorkSpaces Pools 目录时启用 Internet 访问。创建目录时，选择带有公有子网的 VPC。然后，为子网 1 选择一个公有子网，以及（可选）为子网 2 选择另一个公有子网。

通过启动您的 WorkSpaces Pools 然后连接到池中的 WorkSpace 并浏览到 Internet，您可以测试您的 Internet 连接。

使用默认 VPC、公有子网和安全组

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

如果您的 Amazon Web Services 账户是在 2013 年 12 月 4 日之后创建的，则在各个 Amazon 区域中具有一个默认 VPC。默认 VPC 在各个可用区中包含一个默认公有子网，以及连接到您 VPC 的 Internet 网关。VPC 还包含默认安全组。如果您刚接触 WorkSpaces Pools 并希望开始使用该服务，则可以在创建 WorkSpaces Pools 时，保持选中默认 VPC 和安全组。然后，您可以选择至少一个默认子网。

> **Note**
>
> 如果您的 Amazon Web Services 账户是在 2013 年 12 月 4 日之前创建的，则必须创建新的 VPC 或配置现有 VPC 以用于 WorkSpaces Pools。建议您手动为 WorkSpaces Pools 配置具有两个私有子网的 VPC，并在公有子网中配置 NAT 网关。有关更多信息，请参阅 配置具有私有子网和 NAT 网关的 VPC。或者，您也可以配置具有公有子网的非默认 VPC。有关更多信息，请参阅 配置带公有子网的新的或现有 VPC。

您可以在创建 WorkSpaces Pools 目录时启用 Internet 访问。

创建目录时，选择默认 VPC。默认 VPC 名称使用以下格式：`vpc-`*`vpc-id`* `(No_default_value_Name)`。

然后，为子网 1 选择默认公有子网，以及（可选）为子网 2 选择另一个默认公有子网。默认子网名称使用以下格式：`subnet-`*`subnet-id`* `|` `(`*`IPv4 CIDR block`*`)` `| Default in` *`availability-zone`*。

通过启动您的 WorkSpaces Pools 然后连接到池中的 WorkSpace 并浏览到 Internet，您可以测试您的 Internet 连接。

将 Amazon S3 VPC 终端节点用于 WorkSpaces 池功能

> **Important**
>
> “ WorkSpaces 池” 功能不适用于北京和宁夏区域。

当您为池启用应用程序设置持久性或为 WorkSpaces 池目录启用主文件夹时，将 WorkSpaces 使用您为目录指定的 VPC 来提供对 Amazon Simple Storage Service (Amazon S3) 存储桶的访问权限。WorkSpaces 要允许 WorkSpaces 池访问您的私有 S3 终端节点，请将以下自定义策略附加到您的 Amazon S3 的 VPC 终端节点。有关私有 Amazon S3 端点的更多信息，请参阅《Amazon VPC 用户指南》中的 VPC 端点和 Amazon S3 的端点。

CommercialAmazon Web Services 区域

为商业 Amazon Web Services 区域中的资源使用以下策略。

Amazon GovCloud (US) Regions

为商业 Amazon GovCloud (US) Regions中的资源使用以下策略。

连接到 WorkSpaces Pools 的 VPC

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

要实现 WorkSpaces Pools 与网络资源和 Internet 的连接，请按如下方式配置您的 WorkSpaces。

网络接口

WorkSpaces Pools 中的每个 WorkSpace 都有以下网络接口：

- 客户网络接口提供与您的 VPC 内的资源以及 Internet 的连接，并用于将 WorkSpaces 加入您的目录。
- 管理网络接口已连接到安全的 WorkSpaces Pools 管理网络。它用于将 WorkSpace 以交互方式流式传输到用户设备，并允许 WorkSpaces Pools 管理 WorkSpace。

WorkSpaces Pools 从以下私有 IP 地址范围选择管理网络接口的 IP 地址：198.19.0.0/16。不要将此范围用于您的 VPC CIDR，或利用此范围将您的 VPC 与另一 VPC 进行对等，因为这样会造成冲突，并导致无法访问 WorkSpaces。另外，不要修改或删除附加到 WorkSpace 的任何网络接口，因为这样也可能导致无法访问 WorkSpace。

管理网络接口 IP 地址范围和端口

管理网络接口 IP 地址范围是 198.19.0.0/16。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 8300 上的入站 TCP。它用于建立流式连接。
- 端口 3128 上的出站 TCP。它用于管理 WorkSpaces。
- 端口 8000 和 8443 上的入站 TCP。它们用于管理 WorkSpaces。
- 端口 8300 上的入站 UDP。它用于通过 UDP 建立流式连接。

将管理网络接口的入站范围限制于 198.19.0.0/16。

> **Note**
>
> 对于 Amazon DCV BYOL Windows WorkSpaces 虚拟桌面池，10.0.0.0/8 IP 地址范围用于所有 Amazon 区域。（除了您为 BYOL WorkSpaces 虚拟桌面池中的管理流量选择的 /16 CIDR 数据块外，还会使用这些 IP 地址范围。）

正常情况下，WorkSpaces Pools 会为您的 WorkSpaces 正确配置这些端口。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。

请勿禁用 IPv6。如果禁用 IPv6，WorkSpaces Pools 将无法正常工作。有关为 Windows 配置 IPv6 的信息，请参阅在 Windows 中为高级用户配置 IPv6 的指南。

> **Note**
>
> WorkSpaces Pools 依赖于 VPC 中的 DNS 服务器，以便为不存在的本地域名返回不存在的域（NXDOMAIN）响应。这使得 WorkSpaces Pools 管理的网络接口能够与管理服务器通信。当您使用 Simple AD 创建目录时，Amazon Directory Service 将代表您创建两个还用作 DNS 服务器的域控制器。由于域控制器不提供 NXDOMAIN 响应，因此它们不能与 WorkSpaces Pools 一起使用。

客户网络接口端口

- 要连接 Internet，以下端口必须针对所有目标打开。如果您在使用经过修改的安全组或自定义安全组，需要手动添加必需的规则。有关更多信息，请参阅《Amazon VPC 用户指南》中的安全组规则。
  - TCP 80 (HTTP)
  - TCP 443 (HTTPS)
  - UDP 4195
- 如果您将 WorkSpaces 加入一个目录，则以下端口必须在您的 WorkSpaces Pools VPC 与目录控制器之间处于打开状态。
  - TCP/UDP 53 - DNS
  - TCP/UDP 88 - Kerberos 身份验证
  - UDP 123 - NTP
  - TCP 135 - RPC

- UDP 137-138 - Netlogon
- TCP 139 - Netlogon
- TCP/UDP 389 - LDAP
- TCP/UDP 445 - SMB
- TCP 1024-65535 - RPC 动态端口

有关端口的完整列表，请参阅 Microsoft 文档中的 Active Directory 和 Active Directory 域服务端口要求。

- 所有 WorkSpace 都要求端口 80 (HTTP) 对 IP 地址 `169.254.169.254` 开放，以允许访问 EC2 元数据服务。IP 地址范围 `169.254.0.0/16` 专供 WorkSpaces Pools 服务用于管理流量。不排除此范围可能会导致出现流式传输问题。

用户与 WorkSpaces Pools 的连接

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

用户可以通过默认公共 Internet 端点连接到 WorkSpaces Pools 中的 WorkSpaces。

默认情况下，WorkSpaces Pools 配置为通过公共 Internet 路由流连接。需要 Internet 连接来验证用户身份并提供 WorkSpaces Pools 所需的 Web 资产。要允许此流量，您必须允许允许的域中列出的域。

> **Note**
>
> 对于用户身份验证，WorkSpaces Pools 支持安全断言标记语言 2.0（SAML 2.0）。有关更多信息，请参阅 配置 SAML 2.0 并创建 WorkSpaces 池目录。

以下主题提供了有关如何启用与 WorkSpaces Pools 的用户连接的信息。

目录

- 带宽建议
- WorkSpaces Pools 用户设备的 IP 地址和端口要求
- 允许的域

带宽建议

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

要优化 WorkSpaces Pools 的性能，请确保您的网络带宽和延迟可以满足用户的需求。

WorkSpaces Pools 使用 NICE Desktop Cloud Visualization（DCV），使您的用户能够在不同的网络条件下安全地访问和流式传输您的应用程序。为了帮助减少带宽消耗，NICE DCV 使用基于 H.264 视频压缩和编码。在流式传输会话期间，应用程序的可视输出将作为 AES-256 加密像素流通过 HTTPS 进行压缩并流式传输到您的用户。收到流后，它会被解密并输出到用户的本地屏幕。当您的用户与流应用程序进行交互时，NICE DCV 协议会捕获用户输入并通过 HTTPS 将其发送回其流应用程序。

在此过程中会不断测量网络状况，并将相关信息发送回 WorkSpaces Pools。WorkSpaces Pools 通过实时更改视频和音频编码，动态响应不断变化的网络状况，为各种应用程序和网络状况生成高质量的流。

WorkSpaces Pools 流式传输会话的建议带宽和延迟取决于工作负载。例如，相比于使用企业生产力应用程序编写文档的用户，对于使用图形密集型应用程序执行计算机辅助设计任务的用户，将需要更多的带宽和更低的延迟。

下表针对基于常见工作负载的 WorkSpaces Pools 流式传输会话，提供了建议的网络带宽和延迟。

对于每个工作负载，基于单个用户在特定时间点可能需要的内容提出带宽建议。该建议未反映持续吞吐量所需的带宽。当在流式传输会话期间屏幕上仅有几个像素发生变化时，持续吞吐量会低得多。虽然可用带宽较少的用户仍然可以流式传输其应用程序，但帧速率或图像质量可能不是最佳的。

工作负载	描述	为每个用户推荐的带宽	推荐的最大往返延迟
业务线应用程序	文档编写应用程序、数据库分析实用程序	2 Mbps	< 150 毫秒
图形应用程序	计算机辅助设计和建模应用程序、照片和视频编辑	5 Mbps	< 100 毫秒

工作负载	描述	为每个用户推荐的带宽	推荐的最大往返延迟
高保真度	跨多个监视器的高保真数据集或映射	10 Mbps	< 50 毫秒

WorkSpaces Pools 用户设备的 IP 地址和端口要求

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

当使用 Internet 端点时，WorkSpaces Pools 用户设备的出站访问需要使用端口 443（TCP）和端口 4195（UDP）；如果您使用 DNS 服务器进行域名解析，则需要使用端口 53（UDP）。

- 端口 443 用于在使用 Internet 端点时在 WorkSpaces Pools 用户设备和 WorkSpaces 之间的 HTTPS 通信。通常情况下，如果最终用户在流式传输会话期间浏览 Web，则 Web 浏览器会在较高范围内随机选择一个源端口来用于流式传输流量。您必须确保允许流量返回到该端口。
- 端口 4195 用于在使用 Internet 端点时在 WorkSpaces Pools 用户设备和 WorkSpaces 之间的 UDP HTTPS 通信。目前，仅在 Windows 原生客户端中支持此功能。如果您使用的是 VPC 端点，则不支持 UDP。
- 端口 53 用于在 WorkSpaces Pools 用户设备和您的 DNS 服务器之间进行通信。此端口必须对您的 DNS 服务器的 IP 地址开放，以便解析公有域名。如果您不使用 DNS 服务器进行域名解析，则此端口是可选的。

允许的域

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

要使 WorkSpaces Pools 用户能够访问 WorkSpaces，您必须在网络上允许各种域，因为用户将从这些域中启动对 WorkSpaces 的访问。有关更多信息，请参阅 WorkSpaces 个人的 IP 地址和端口要求。请注意，该页面指定它适用于 WorkSpaces 个人版，但也适用于 WorkSpaces Pools。

> **Note**
>
> 如果您的 S3 存储桶名称中包含“.” 字符，则表示所使用的域是 `https://s3.<aws-region>.amazonaws.com`。如果您的 S3 存储桶名称中不包含“.” 字符，则表示所使用的域是 `https://<bucket-name>.s3.<aws-region>.amazonaws.com`。

创建 WorkSpaces Pools

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

设置并创建一个池，将从该池中启动和流式传输用户应用程序。

> **Note**
>
> 在创建 WorkSpaces Pools 之前，您应该创建一个目录。有关更多信息，请参阅 配置 SAML 2.0 并创建 WorkSpaces 池目录。

设置和创建池

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，依次选择 WorkSpaces、池。
3. 选择创建 WorkSpaces Pools。
4. 在注册（可选）下，您可以选择根据我的使用案例向我推荐选项，以获取有关您要使用的 WorkSpace 类型的建议。如果您知道要使用 WorkSpaces Pools，则可跳过此步骤。
5. 在配置 WorkSpaces 下，输入以下详细信息：
   - 对于名称，为池输入一个唯一的名称标识符。不允许使用特殊字符。
   - 对于描述，输入池描述（最多 256 个字符）。
   - 对于捆绑包，从以下捆绑包类型中选择要用于 WorkSpaces 的捆绑包类型。
     - 使用基础 WorkSpaces 捆绑包 - 从下拉列表中选择一个捆绑包。要了解您选择的捆绑包类型的更多信息，请选择捆绑包详细信息。要比较为池提供的捆绑包，请选择比较所有捆绑包。

- 使用您自己的自定义捆绑包 - 选择您之前创建的捆绑包。要创建自定义捆绑包，请参阅为 WorkSpaces 个人版创建自定义 WorkSpaces 图片和捆绑包。

- 对于运行模式，从以下选项中进行选择，配置池的即时可用性和付费方式：
  - AutoStop：池实例根据所选捆绑包按小时使用量收费，仅适用于与用户连接的实例。Pool 中未与用户连接的实例按较低的停止实例小时费用收费。当用户启动会话时，他们会在 1-2 分钟后开始流式传输。
  - AlwaysOn：所有池实例将按适用的小时使用量收费，即使用户未连接也是如此。此模式最适合不想等待流式传输开始的用户。
- 对于最大会话持续时间（分钟），选择流式传输会话可以保持活动状态的最长时间。在达到此限制前的五分钟，如果用户仍连接到流实例，则系统在断开连接之前将会提示用户保存任何打开的文档。在此时间过后，实例将终止并被新的实例取代。您可以在 WorkSpaces Pools 控制台中设置的最长会话持续时间为 5760 分钟（96 小时）。您可以使用 WorkSpaces Pools API 和 CLI 设置的最大会话持续时间为 432000 秒（120 小时）。
- 对于 Disconnect timeout in minutes (断开连接超时 (分钟))，请选择在用户断开连接后流式传输会话保持活动状态的时间。如果在此时间间隔内出现连接断开或网络中断的情况后，用户尝试重新连接到流式传输会话，他们将连接到其上一个会话。否则，他们会建立一个新会话，连接到新的流实例。
- 如果用户通过在池工具栏上选择结束会话或注销来结束会话，则不应用断开连接超时。系统而是会提示用户保存任何打开的文档，然后立即断开流实例的连接。用户正在使用的实例随即终止。
- 对于 Idle disconnect timeout in minutes (空闲断开连接超时 (分钟))，请选择用户在与流式传输会话断开连接以及 Disconnect timeout in minutes (断开连接超时 (分钟)) 时间间隔开始之前可以处于空闲（非活动）状态的时间。在由于处于不活动状态而断开连接之前，用户将收到通知。在 Disconnect timeout in minutes (断开连接超时 (分钟)) 中指定的时间间隔过去之前，如果他们尝试重新连接到流式传输会话，则会将他们连接到以前的会话。否则，他们会建立一个新会话，连接到新的流实例。如果将该值设置为 0，则会禁用该值。如果禁用了该值，则不会由于处于不活动状态而断开连接用户。

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

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

> **Note**
> 您的池大小受您指定的最小和最大容量限制。

  - 如果指定的容量利用率小于或高于指定的阈值，请选择添加新的横向扩展策略，然后输入用于添加指定实例的值。
  - 如果指定的容量利用率小于或高于指定的阈值，请选择添加新的横向缩减策略，然后输入用于删除指定实例的值。
- 对于标签，指定要使用的键对值。键可以是具有特定关联值的一般类别，例如“project”、“owner”或“environment”。

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

管理 WorkSpaces Pools

> **Important**
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

WorkSpaces Pools 由运行您指定的映像的 WorkSpace 组成。

目录

- WorkSpaces Pools 的运行模式
- WorkSpaces Pools 捆绑包
- 修改池
- 删除池
- WorkSpaces Pools 的自动扩缩

WorkSpaces Pools 的运行模式

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

WorkSpaces Pool 的运行模式决定其即时可用性和付费方式。在创建 WorkSpaces Pool 时，可以选择以下运行模式：

- AutoStop：WorkSpaces Pool 的实例根据所选捆绑包按小时使用量收费，仅适用于与用户连接的实例。WorkSpaces Pool 中未与用户连接的实例按较低的停止实例小时费用收费。当用户启动会话时，他们会在 1-2 分钟后开始流式传输。
- AlwaysOn：WorkSpaces Pool 的运行实例将按适用的小时使用量收费，即使用户未连接也是如此。此模式最适合不想等待流式传输开始的用户。

有关更多信息，请参阅 WorkSpaces 定价。

目录

- 修改运行模式

修改运行模式

当 WorkSpaces Pool 处于停止状态时，您可以在运行模式之间切换。

修改 WorkSpaces Pool 的运行模式

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，依次选择 WorkSpaces 和池。
3. 选择要修改的 WorkSpaces Pool 并确认其处于停止状态。然后，选择操作和修改运行模式。
4. 选择新的运行模式 AlwaysOn 或 AutoStop，然后选择保存。

使用 Amazon CLI 修改 WorkSpaces Pool 的运行模式

- 使用 update-workspaces-pool 命令。

WorkSpaces Pools 捆绑包

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

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 可用的各种公有捆绑包的更多信息，请参阅 Amazon WorkSpaces 捆绑包。

下表提供了有关每个操作系统支持的许可、流式传输协议和捆绑包的信息。

操作系统	许可证	流式传输协议	支持的捆绑包
Windows Server 2019	包含	DCV	Value、Standard、Performance、Power、PowerPro
Windows Server 2022	包含	DCV	Standard、Performance、Power、PowerPro、Graphics.G4dn、GraphicsPro.G4dn

> **Note**
>
> - 不再受供应商支持的操作系统版本不能保证正常工作，也不受 Amazon Support 支持。

修改池

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

创建 WorkSpaces Pools 后，您可以修改以下内容：

- 目录 ID（如果 WorkSpaces Pools 已停止）
- 基本详细信息
- 捆绑包和硬件
- 会话断开连接设置
- 容量和扩展
- 扩缩活动
- 标签

修改 WorkSpaces Pools

1. 在导航窗格中，依次选择 WorkSpaces、池。
2. 选择要修改的池。
3. 转到要修改的部分，然后选择编辑。
4. 进行所需的修改，然后选择保存。

删除池

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

您可以删除池以释放资源并避免您的账户产生意外费用。建议您停止任何未使用的运行中的池。

删除池

1. 在导航窗格中，依次选择 WorkSpaces、池。
2. 选择要停止的池，然后选择停止。停止池大约需要 5 分钟。
3. 当池的状态为已停止时，选择删除。

WorkSpaces Pools 的自动扩缩

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

通过使用自动扩缩，您可以自动更改池大小，使提供的可用实例满足用户需求。池大小决定了可以同时流式传输的用户数。每个用户会话都需要一个实例。您可以根据实例来指定池容量。根据您的池配置和自动扩缩策略，将提供所需数量的实例。您可以定义扩缩策略，根据各种使用率指标自动调整池的大小，并优化可用实例的数目以满足用户需求。您也可以选择关闭自动扩缩功能，并使池按固定大小运行。

> **Note**
>
> - 在制定 WorkSpaces Pools 扩缩计划时，请确保网络配置能够满足您的要求。
> - 当您使用扩缩功能时，可以使用 Application Auto Scaling API。为了针对 WorkSpaces Pools 正确应用自动扩缩功能，Application Auto Scaling 需要具有描述和更新池以及描述 Amazon CloudWatch 警报的权限，并具有代表您修改池容量的权限。

以下主题提供了相应的信息，可帮助您了解和使用 WorkSpaces Pools 自动扩缩功能。

目录

- 扩缩概念
- 使用控制台管理池扩缩
- 使用 Amazon CLI 管理池扩缩
- 其他资源

扩缩概念

WorkSpaces Pools 扩缩功能由 Application Auto Scaling 提供。有关更多信息，请参阅 Application Auto Scaling API 参考。

要高效地使用 WorkSpaces Pools 自动扩缩，您必须了解以下术语和概念。

池的最小容量/最小用户会话数

实例的最小数量。实例数不能低于该值，并且扩缩策略不会将您的池缩减到该值以下。例如，如果将池的最小容量设置为 2，则您的池永远不会少于 2 个实例。

池的最大容量/最大用户会话数

实例的最大数目。实例数不能高于该值，并且扩缩策略不会将您的池扩大到该值以上。例如，如果将池的最大容量设置为 10，则您的池永远不会超过 10 个实例。

所需的用户会话容量

正在运行或待处理的总会话数。该值表示池可以在稳定状态下支持的总并发流式传输会话数。

扩缩策略操作

扩缩策略在满足扩缩策略条件时对池执行的操作。您可以根据容量百分比或实例数目选择一个操作。例如，如果所需的用户会话容量为 4，且将扩缩策略操作设置为“添加 25% 的容量”，则在满足扩缩策略条件时，所需的用户会话容量将增加 25%，即为 5。

扩缩策略条件

触发 Scaling Policy Action 中设置的操作的条件。此条件包括扩缩策略指标、比较运算符和阈值。例如，要在池利用率高于 50% 时扩缩池，您的扩缩策略条件应为“如果容量利用率 > 50%”。

扩缩策略指标

您的扩缩策略基于该指标。以下指标可用于扩缩策略：

容量利用率

池中正在使用的实例百分比。您可以使用此指标来根据池使用率扩缩池。例如，Scaling Policy Condition (扩缩策略条件)：“如果容量利用率 < 25%”执行 Scaling Policy Action (扩展策略操作)：“删除 25% 的容量”。

可用容量

池中可供用户使用的实例数。您可以使用此指标，在您的容量中保留可供用户用来开始流式传输会话的缓冲区。例如，Scaling Policy Condition (扩展策略条件)：“如果可用容量 < 5”执行 Scaling Policy Action (扩展策略操作)：“添加 5 个实例”。

容量不足错误

因缺少容量而被拒绝的会话请求的数量。您可以使用此指标为由于容量不足而无法启动流式传输会话的用户预配置新实例。例如，Scaling Policy Condition：“如果容量不足错误 > 0”执行 Scaling Policy Action：“添加 1 个实例”。

使用控制台管理池扩缩

您可以使用 WorkSpaces 控制台通过以下两种方法之一设置和管理扩缩：在创建池期间或使用池选项卡的任何时候。创建池后，转到扩缩策略选项卡，为您的池添加新的扩缩策略。有关更多信息，请参阅创建 WorkSpaces Pools 。

对于数量不断变化的用户环境，定义扩缩策略以控制扩缩响应需求的方式。如果您需要固定数量的用户或出于其他原因而禁用扩缩，则可以设置具有固定数量的实例或用户会话的池。

为此，请将最低容量设置为所需的实例数量。将最大容量调整为至少为最小容量的值。这样可以避免验证错误，但由于池不会扩缩，因此最终会忽略最大容量。然后，删除该池的所有扩缩策略。

使用控制台设置池扩缩策略

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择池。
3. 选择池。
4. 在该池的页面上，向下滚动到“容量和扩缩”。
5. 选择编辑。
6. 编辑现有策略并在其字段中设置所需的值，然后选择保存。策略更改将在几分钟内生效。
7. 您还可以通过依次选择添加新的计划容量、添加新的横向扩展策略或添加新的横向缩减策略，来添加新的容量和扩缩策略。

以下是一个示例图，说明了在 5 个用户连接到池然后断开连接时的扩缩活动使用率。本示例来自使用以下扩缩策略值的池：

- 最小容量 = 10
- 最大容量 = 50
- 横向扩展 = 如果我的池容量利用率大于 75%，则添加 5 个实例
- 横向缩减 = 如果我的池容量利用率小于 25%，则删除 6 个实例

> **Note**
>
> 会话期间，将在横向扩展事件期间启动 5 个新实例。在横向缩减事件期间，如果有足够的实例而没有活跃的用户会话，并且实例总数未降至最低 10 个实例容量以下，则将回收 6 个实例。不会收回正在运行用户会话的实例。只收回未运行用户会话的实例。

使用 Amazon CLI 管理池扩缩

您可以使用 Amazon Command Line Interface（Amazon CLI）设置和管理池扩缩。有关诸如设置横向缩减和横向扩展冷却时间等的更高级功能，请使用 Amazon CLI。在运行扩缩策略命令之前，您必须将池注册为可扩展目标。为此，请使用下面的 register-scalable-target 命令：

```
aws application-autoscaling register-scalable-target
  --service-namespace workspaces \
  --resource-id workspacespool/PoolId \
  --scalable-dimension workspaces:workspacespool:DesiredUserSessions \
  --min-capacity 1 --max-capacity 5
```

示例

- 示例 1：根据容量利用率应用扩缩策略
- 示例 2：根据“容量不足”错误应用扩缩策略
- 示例 3：根据低容量利用率应用扩缩策略
- 示例 4：基于计划更改池容量
- 示例 5：应用目标跟踪扩缩策略

示例 1：根据容量利用率应用扩缩策略

此 Amazon CLI 示例设置一个扩缩策略，该策略在利用率 >= 75% 时将池横向扩展 25%。

以下 put-scaling-policy 命令定义一个基于利用率的扩缩策略：

```
aws application-autoscaling put-scaling-policy -- cli-input-json file://scale-out-
utilization.json
```

文件 `scale-out-utilization.json` 的内容如下所示：

```
{
    "PolicyName": "policyname",
    "ServiceNamespace": "workspaces",
    "ResourceId": "workspacespool/PoolId",
    "ScalableDimension": "workspaces:workspacespool:DesiredUserSessions",
    "PolicyType": "StepScaling",
    "StepScalingPolicyConfiguration": {
        "AdjustmentType": "PercentChangeInCapacity",
```

```
        "StepAdjustments": [
            {
                "MetricIntervalLowerBound": 0,
                "ScalingAdjustment": 25
            }
        ],
        "Cooldown": 120
    }
}
```

如果命令成功，则输出类似于以下内容，但一些详细信息是您的账户和区域独有的。在本示例中，策略标识符为 `e3425d21-16f0-d701-89fb-12f98dac64af`。

```
{"PolicyARN": "arn:aws:autoscaling:us-west-2:123456789012:scalingPolicy:e3425d21-16f0-d701-89fb-12f98dac64af:resource/workspaces/workspacespool/PoolId:policyName/scale-out-utilization-policy"}
```

现在，为此策略设置 CloudWatch 警报。使用适用于您的名称、区域、账号和策略标识符。您可以对 `-- alarm-actions` 参数使用上一条命令所返回的策略 ARN。

```
aws cloudwatch put-metric-alarm
--alarm-name alarmname \
--alarm-description "Alarm when Available User Session Capacity exceeds 75 percent" \
--metric-name AvailableUserSessionCapacity \
--namespace Amazon/WorkSpaces \
--statistic Average \
--period 300 \
--threshold 75 \
--comparison-operator GreaterThanOrEqualToThreshold \
--dimensions "Name=WorkSpaces pool ID,Value=PoolId" \
--evaluation-periods 1 --unit Percent \
--alarm-actions "arn:aws:autoscaling:your-region-code:account-
number-without-hyphens:scalingPolicy:policyid:resource/workspaces/
workspacespool/PoolId:policyName/policyname"
```

示例 2：根据“容量不足”错误应用扩缩策略

此 Amazon CLI 示例设置一个扩缩策略，该策略在池返回 `InsufficientCapacityError` 错误时将池横向扩展 1 倍。

以下命令定义一个基于“容量不足”的扩缩策略：

```
aws application-autoscaling put-scaling-policy -- cli-input-json file://scale-out-capacity.json
```

文件 `scale-out-capacity.json` 的内容如下所示：

```
{
    "PolicyName": "policyname",
    "ServiceNamespace": "workspaces",
    "ResourceId": "workspacespool/PoolId",
    "ScalableDimension": "workspaces:workspacespool:DesiredUserSessions",
    "PolicyType": "StepScaling",
    "StepScalingPolicyConfiguration": {
        "AdjustmentType": "ChangeInCapacity",
        "StepAdjustments": [
            {
                "MetricIntervalLowerBound": 0,
                "ScalingAdjustment": 1
            }
        ],
        "Cooldown": 120
    }
}
```

如果命令成功，则输出类似于以下内容，但一些详细信息是您的账户和区域独有的。在本示例中，策略标识符为 `f4495f21-0650-470c-88e6-0f393adb64fc`。

```
{"PolicyARN": "arn:aws:autoscaling:us-
west-2:123456789012:scalingPolicy:f4495f21-0650-470c-88e6-0f393adb64fc:resource/
workspaces/workspacespool/PoolId:policyName/scale-out-insufficient-capacity-policy"}
```

现在，为此策略设置 CloudWatch 警报。使用适用于您的名称、区域、账号和策略标识符。您可以对 `--alarm-actions` 参数使用上一条命令所返回的策略 ARN。

```
aws cloudwatch put-metric-alarm
--alarm-name alarmname \
--alarm-description "Alarm when out of capacity is > 0" \
--metric-name InsufficientCapacityError \
--namespace AWS/WorkSpaces \
--statistic Maximum \
--period 300 \
--threshold 0 \
```

```
--comparison-operator GreaterThanThreshold \
--dimensions "Name=Pool,Value=PoolId" \
--evaluation-periods 1 --unit Count \
--alarm-actions "arn:aws:autoscaling:your-region-code:account-
number-without-hyphens:scalingPolicy:policyid:resource/workspaces/
workspacespool/PoolId:policyName/policyname"
```

示例 3：根据低容量利用率应用扩缩策略

此 Amazon CLI 示例设置一个扩缩策略，该策略在 `UserSessionsCapacityUtilization` 较低时横向缩减池以减少实际容量。

以下命令定义一个基于“容量过多”的扩缩策略：

```
aws application-autoscaling put-scaling-policy -- cli-input-json file://scale-in-
capacity.json
```

文件 `scale-in-capacity.json` 的内容如下所示：

```
{
    "PolicyName": "policyname",
    "ServiceNamespace": "workspaces",
    "ResourceId": "workspacespool/PoolId",
    "ScalableDimension": "workspaces:workspacespool:DesiredUserSessions",
    "PolicyType": "StepScaling",
    "StepScalingPolicyConfiguration": {
        "AdjustmentType": "PercentChangeInCapacity",
        "StepAdjustments": [
            {
                "MetricIntervalUpperBound": 0,
                "ScalingAdjustment": -25
            }
        ],
        "Cooldown": 360
    }
}
```

如果命令成功，则输出类似于以下内容，但一些详细信息是您的账户和区域独有的。在本示例中，策略标识符为 `12ab3c4d-56789-0ef1-2345-6ghi7jk8lm90`。

```
{"PolicyARN": "arn:aws:autoscaling:us-
west-2:123456789012:scalingPolicy:12ab3c4d-56789-0ef1-2345-6ghi7jk8lm90:resource/
workspaces/workspacespool/PoolId:policyName/scale-in-utilization-policy"}
```

现在，为此策略设置 CloudWatch 警报。使用适用于您的名称、区域、账号和策略标识符。您可以对 `--alarm-actions` 参数使用上一条命令所返回的策略 ARN。

```
aws cloudwatch put-metric-alarm
--alarm-name alarmname \
--alarm-description "Alarm when Capacity Utilization is less than or equal to 25
 percent" \
--metric-name UserSessionsCapacityUtilization \
--namespace AWS/WorkSpaces \
--statistic Average \
--period 120 \
--threshold 25 \
--comparison-operator LessThanOrEqualToThreshold \
--dimensions "Name=Pool,Value=PoolId" \
--evaluation-periods 10 --unit Percent \
--alarm-actions "arn:aws:autoscaling:your-region-code:account-
number-without-hyphens:scalingPolicy:policyid:resource/workspaces/
workspacespool/PoolId:policyName/policyname"
```

示例 4：基于计划更改池容量

通过基于计划更改池容量，您能够扩缩池容量以响应可预测的需求变化。例如，在工作日的开始，您可能预期有特定数量的用户一次性请求流式传输连接。要基于计划更改池容量，您可以使用 Application Auto Scaling PutScheduledAction API 操作或 put-scheduled-action Amazon CLI 命令。

在更改池容量之前，您可以使用 WorkSpaces describe-workspaces-pools Amazon CLI 命令列出当前池容量。

```
aws workspaces describe-workspaces-pools --name PoolId
```

当前池容量类似于以下输出 (用 JSON 格式显示)：

```
{
    "CapacityStatus": {
        "AvailableUserSessions": 1,
        "DesiredUserSessions": 1,
```

```
        "ActualUserSessions": 1,
        "ActiveUserSessions": 0
    },
}
```

然后，使用 `put-scheduled-action` 命令创建计划操作以更改池容量。例如，以下命令在 UTC 时间每天上午 9 点将最小容量更改为 3，并将最大容量更改为 5。

> **Note**
>
> 对于 cron 表达式，以 UTC 时间指定何时执行操作。有关更多信息，请参阅 Cron 表达式。

```
aws application-autoscaling put-scheduled-action --service-namespace workspaces \
--resource-id workspacespool/PoolId \
--schedule="cron(0 9 * * ? *)" \
--scalable-target-action MinCapacity=3,MaxCapacity=5 \
--scheduled-action-name ExampleScheduledAction \
--scalable-dimension workspaces:workspacespool:DesiredUserSessions
```

要确认已成功创建用于更改池容量的计划操作，请运行 describe-scheduled-actions 命令。

```
aws application-autoscaling describe-scheduled-actions --service-namespace workspaces
 --resource-id workspacespool/PoolId
```

如果已成功创建计划的操作，则输出类似于以下内容。

```
{
    "ScheduledActions": [
        {
            "ScalableDimension": "workspaces:workspacespool:DesiredUserSessions",
            "Schedule": "cron(0 9 * * ? *)",
            "ResourceId": "workspacespool/ExamplePool",
            "CreationTime": 1518651232.886,
            "ScheduledActionARN": "<arn>",
            "ScalableTargetAction": {
                "MinCapacity": 3,
                "MaxCapacity": 5
            },
            "ScheduledActionName": "ExampleScheduledAction",
            "ServiceNamespace": "workspaces"
```

```
        }
    ]
}
```

有关更多信息，请参阅《Application Auto Scaling 用户指南》中的计划扩展。

示例 5：应用目标跟踪扩缩策略

通过目标跟踪扩缩功能，您可以为池指定容量利用率级别。

创建目标跟踪扩缩策略时，Application Auto Scaling 会自动创建和管理用于触发扩缩策略的 CloudWatch 警报。扩缩策略根据需要增加或减少容量，将容量利用率保持在指定的目标值或接近指定的目标值。为了确保应用程序可用性，池针对此指标尽快按比例横向扩展，但会逐渐横向缩减。

以下 put-scaling-policy 命令定义了一个目标跟踪扩缩策略，该策略试图将 WorkSpaces Pools 的容量利用率维持在 75%。

```
aws application-autoscaling put-scaling-policy -- cli-input-json file://config.json
```

文件 `config.json` 的内容如下所示：

```
{
  "PolicyName":"target-tracking-scaling-policy",
  "ServiceNamespace":"workspaces",
  "ResourceId":"workspacespool/PoolId",
  "ScalableDimension":"workspaces:workspacespool:DesiredUserSessions",
  "PolicyType":"TargetTrackingScaling",
  "TargetTrackingScalingPolicyConfiguration":{
    "TargetValue":75.0,
    "PredefinedMetricSpecification":{
      "PredefinedMetricType":"WorkSpacesAverageUserSessionsCapacityUtilization"
    },
    "ScaleOutCooldown":300,
    "ScaleInCooldown":300
  }
}
```

如果命令成功，则输出类似于以下内容，但一些详细信息是您的账户和区域独有的。在此示例中，策略标识符是 6d8972f3-efc8-437c-92d1-6270f29a66e7。

```
{
```

```
    "PolicyARN": "arn:aws:autoscaling:us-west-2:123456789012:scalingPolicy:6d8972f3-
efc8-437c-92d1-6270f29a66e7:resource/workspaces/workspacespool/PoolId:policyName/
target-tracking-scaling-policy",
    "Alarms": [
        {
            "AlarmARN": "arn:aws:cloudwatch:us-
west-2:123456789012:alarm:TargetTracking-workspacespool/PoolId-AlarmHigh-d4f0770c-
b46e-434a-a60f-3b36d653feca",
            "AlarmName": "TargetTracking-workspacespool/PoolId-AlarmHigh-d4f0770c-
b46e-434a-a60f-3b36d653feca"
        },
        {
            "AlarmARN": "arn:aws:cloudwatch:us-
west-2:123456789012:alarm:TargetTracking-workspacespool/PoolId-AlarmLow-1b437334-
d19b-4a63-a812-6c67aaf2910d",
            "AlarmName": "TargetTracking-workspacespool/PoolId-AlarmLow-1b437334-
d19b-4a63-a812-6c67aaf2910d"
        }
    ]
}
```

有关更多信息，请参阅《Application Auto Scaling 用户指南》中的目标跟踪扩缩策略。

其他资源

要了解有关使用 Application Auto Scaling Amazon CLI 命令或 API 操作的更多信息，请参阅以下资源：

- Amazon CLI Command Reference 的 application-autoscaling 部分
- Application Auto Scaling API 参考
- Application Auto Scaling 用户指南

将 Active Directory 与 WorkSpaces Pools 结合使用

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

您可以将 WorkSpaces Pools 中的 Windows WorkSpaces 加入 Microsoft Active Directory 中的域，并使用现有基于云或本地的 Active Directory 域，来启动加入域的流实例。您也可以使用 Amazon Directory Service for Microsoft Active Directory（也称为 Amazon Managed Microsoft AD）创建 Active Directory 域并使用该域来支持 WorkSpaces Pools 资源。有关使用 Amazon Managed Microsoft AD 的更多信息，请参阅《Amazon Directory Service 管理指南》中的 Microsoft Active Directory。

将 WorkSpaces Pools 加入 Active Directory 域后，您可以：

- 允许您的用户和应用程序从流式传输会话访问 Active Directory 资源 (如打印机和文件共享)。
- 使用组策略管理控制台 (GPMC) 中可用的组策略设置定义最终用户体验。
- 流式传输需要用户使用 Active Directory 登录凭证进行身份验证的应用程序。
- 将企业合规性和安全性策略应用于您 WorkSpaces Pools 中的 WorkSpaces。

目录

- Active Directory 域概述
- 开始将 Active Directory 与 WorkSpaces Pools 结合使用之前的准备工作
- 基于证书的身份验证
- WorkSpaces Pools Active Directory 管理
- 更多信息

Active Directory 域概述

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

将 Active Directory 域与 WorkSpaces Pools 结合使用需要了解它们如何协作以及您需要完成的配置任务。需要完成以下任务：

1. 按需配置组策略设置以定义应用程序的最终用户体验和安全要求。
2. 在 WorkSpaces Pools 中创建加入域的目录。
3. 在 SAML 2.0 身份提供者中创建 WorkSpaces Pools 应用程序并直接或通过 Active Directory 组将其分配给最终用户。

用户身份验证流程

1. 用户浏览到 `https://applications.exampleco.com`。登录页请求对用户进行身份验证。
2. 联合身份验证服务请求从组织的身份存储进行身份验证。
3. 该身份存储将对用户进行身份验证，并将身份验证响应返回到联合身份验证服务。
4. 在成功进行身份验证后，联合身份验证服务会将 SAML 断言发布到用户的浏览器。
5. 用户的浏览器会将 SAML 断言发布到 Amazon 登录 SAML 端点（`https://signin.aws.amazon.com/saml`）。Amazon登录服务将接收 SAML 请求，处理请求，验证用户身份并将身份验证令牌转发到 WorkSpaces Pools 服务。
6. 通过使用来自 Amazon 的身份验证令牌，WorkSpaces Pools 可向用户授权并向浏览器提供应用程序。
7. 用户选择一个应用程序，根据在 WorkSpaces Pools 目录上启用的 Windows 登录身份验证方法，系统会提示他们输入 Active Directory 域密码或选择智能卡。如果同时启用了这两种身份验证方法，则用户可以选择是输入域密码还是使用智能卡。也可以使用基于证书的身份验证对用户进行身份验证，从而删除提示。
8. 访问域控制器以进行用户身份验证。
9. 向域验证身份后，用户的会话从域连接开始。

从用户的角度来看，此过程以透明的方式进行。用户首先导航到您组织的内部门户，然后重定向到 WorkSpaces Pools 门户，而无需输入 Amazon 凭证。只需提供 Active Directory 域密码或智能卡凭证。

您必须先使用必需的权限和组策略设置配置 Active Directory 并创建加入域的 WorkSpaces Pools 目录，然后用户才能启动此流程。

开始将 Active Directory 与 WorkSpaces Pools 结合使用之前的准备工作

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

在将 Microsoft Active Directory 域与 WorkSpaces Pools 结合使用之前，请注意以下要求和注意事项。

目录

- Active Directory 域环境

- WorkSpaces Pools 中加入域的 WorkSpaces
- 组策略设置
- 智能卡身份验证

Active Directory 域环境

- 您必须具有一个 Microsoft Active Directory 域，以便将您的 WorkSpaces 加入其中。如果您没有 Active Directory 域或者想要使用本地 Active Directory 环境，请参阅在 Amazon Cloud 上部署 Active Directory 域服务：快速入门参考部署。
- 您必须具有一个域服务账户，该账户有权在您打算和 WorkSpaces Pools 结合使用的域中创建和管理计算机对象。有关信息，请参阅 Microsoft 文档中的《如何在 Active Directory 中创建域账户》。

  将此 Active Directory 域与 WorkSpaces Pools 关联时，提供服务账户名称和密码。WorkSpaces Pools 将使用此账户在目录中创建和管理计算机对象。有关更多信息，请参阅 授予创建和管理 Active Directory 计算机对象的权限。
- 向 WorkSpaces Pools 注册 Active Directory 域时，必须提供组织部门（OU）的可分辨名称。为此目的创建一个 OU。默认计算机容器不是 OU，不能供 WorkSpaces Pools 使用。有关更多信息，请参阅 查找组织单位的可分辨名称。
- 对于计划与 WorkSpaces Pools 结合使用的目录，必须能够通过其完全限定域名（FQDN）经由在其中启动了 WorkSpaces 的虚拟私有云（VPC）进行访问。有关更多信息，请参阅 Microsoft 文档中的 Active Directory and Active Directory Domain Services Port Requirements。

WorkSpaces Pools 中加入域的 WorkSpaces

从加入域的 WorkSpaces 流式传输应用程序需要基于 SAML 2.0 的用户联合身份验证。另外，必须使用支持加入 Active Directory 域的 Windows 映像。所有在 2017 年 7 月 24 日或之后发布的公有映像都支持加入 Active Directory 域。

组策略设置

验证以下组策略设置的配置。如果需要，请按照本节中所述更新这些设置，以便它们不会阻止 WorkSpaces Pools 对您的域用户进行身份验证和登录。否则，当您的用户尝试登录 WorkSpaces 时，可能无法成功登录。相反，会显示一条消息，通知用户“发生未知错误”。

- 计算机配置 > 管理模板 > Windows 组件 > Windows 登录选项 > 禁用或启用软件安全注意序列 – 对于服务，将此项设置为启用。

- 计算机配置 > 管理模板 > 系统 > 登录 > 排除凭据提供程序 – 确保以下 CLSID 未列出：`e7c1bab5-4b49-4e64-a966-8d99686f8c7c`
- 计算机配置 > 策略 > Windows 设置 > 安全设置 > 本地策略 > 安全选项 > 交互式登录 > 交互式登录: 尝试登录的用户的消息文本 – 将此项设置为未定义。
- 计算机配置 > 策略 > Windows 设置 > 安全设置 > 本地策略 > 安全选项 > 交互式登录 > 交互式登录: 尝试登录的用户的消息标题 – 将此项设置为未定义。

智能卡身份验证

WorkSpaces Pools 支持使用 Active Directory 域密码或智能卡 [例如通用访问卡（CAC）和个人身份验证（PIV）智能卡]，通过 Windows 登录到 WorkSpaces Pools 中的 WorkSpaces。有关如何将 Active Directory 环境配置为使用第三方证书颁发机构（CA）启用智能卡登录的信息，请参阅 Microsoft 文档中的 Guidelines for enabling smart card logon with third-party certification authorities。

基于证书的身份验证

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

您可以对加入 Microsoft Active Directory 的 WorkSpaces Pools 使用基于证书的身份验证。这样，当用户登录时，系统就不会再提示输入 Active Directory 域密码。通过对您的 Active Directory 域使用基于证书的身份验证，您可以：

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

基于证书的身份验证使用 Amazon Web Services 账户中的 Amazon 私有证书颁发机构（Amazon 私有 CA）资源。使用 Amazon 私有 CA，您可以创建私有证书颁发机构（CA）层次结构，包括根 CA 和从属 CA。您还可以创建自己的 CA 层次结构，并从中颁发对内部用户进行身份验证的证书。有关更多信息，请参阅什么是 Amazon 私有 CA。

在您使用 Amazon 私有 CA 进行基于证书的身份验证时，WorkSpaces Pools 会在为 WorkSpaces Pools 中的每个 WorkSpaces 预留会话时自动为您的用户请求证书。它使用预置了证书的虚拟智能卡对用户进行 Active Directory 身份验证。

运行 Windows 实例且加入域的 WorkSpaces Pools 支持基于证书的身份验证。

目录

- 先决条件
- 启用基于证书的身份验证
- 管理基于证书的身份验证
- 启用跨账户 PCA 共享

先决条件

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

使用基于证书的身份验证之前，请完成以下步骤。

1. 配置集成了 SAML 2.0 的 WorkSpaces Pools 目录，以使用基于证书的身份验证。有关更多信息，请参阅 配置 SAML 2.0 并创建 WorkSpaces 池目录。

   > **Note**
   >
   > 如果您要使用基于证书的身份验证，请不要启用池目录中的智能卡登录。

2. 在 SAML 断言中配置 `userPrincipalName` 属性。有关更多信息，请参阅 步骤 7：为 SAML 身份验证响应创建断言。
3. 在 SAML 断言中配置 `ObjectSid` 属性。您可以使用此属性与 Active Directory 用户进行强映射。如果 `ObjectSid` 属性与 SAML_Subject `NameID` 中指定的用户的 Active Directory 安全标识符（SID）不匹配，则基于证书的身份验证将失败。有关更多信息，请参阅 步骤 7：为 SAML 身份验证响应创建断言。

> **Note**
>
> 根据 Microsoft KB5014754，2025 年 9 月 10 日之后，基于证书的身份验证要求必须配置 `ObjectSid` 属性。

4. 将 `sts:TagSession` 权限添加到与您的 SAML 2.0 配置一起使用的 IAM 角色信任策略。有关更多信息，请参阅《Amazon Identity and Access Management 用户指南》中的在 Amazon STS 中传递会话标签。使用基于证书的身份验证时需要此权限。有关更多信息，请参阅 步骤 5：创建 SAML 2.0 联合身份验证 IAM 角色。
5. 如果您的 Active Directory 没有配置私有证书颁发机构（CA），请使用 Amazon 私有 CA 创建一个。Amazon使用基于证书的身份验证时需要私有 CA。有关更多信息，请参阅《Amazon 私有证书颁发机构 用户指南》中的规划您的 Amazon 私有 CA 部署。以下是许多基于证书的身份验证使用案例中常见的 Amazon 私有 CA 设置：
   - CA 类型选项
     - 短期证书 CA 使用模式 – 如果 CA 仅为基于证书的身份验证颁发最终用户证书，则建议使用此模式。
     - 带有根 CA 的单级层次结构 – 选择从属 CA 以将其与现有 CA 层次结构集成。
   - 密钥算法选项 – RSA 2048
   - 主题可分辨名称选项 – 使用合适的选项在 Active Directory 受信任的根证书颁发机构存储中识别此 CA。
   - 证书吊销选项 – CRL 分发

   > **Note**
   >
   > 基于证书的身份验证需要一个可从 WorkSpaces Pools 中 WorkSpaces 和域控制器访问的在线 CRL 分发点。这需要以未经身份验证的方式访问为 Amazon 私有 CA CRL 条目配置的 Amazon S3 存储桶，或者如果阻止了公共访问，则需要拥有 Amazon S3 存储桶访问权限的 CloudFront 分配。有关这些选项的更多信息，请参阅《Amazon 私有证书颁发机构 用户指南》中的规划证书吊销列表（CRL）。

6. 使用名为 `euc-private-ca` 的键标记您的私有 CA，以指定该 CA 用于 WorkSpaces Pools 基于证书的身份验证。此键不需要值。有关更多信息，请参阅《Amazon 私有证书颁发机构 用户指南》中的管理私有 CA 的标签。
7. 基于证书的身份验证使用虚拟智能卡进行登录。有关更多信息，请参阅 Guidelines for enabling smart card logon with third-party certification authorities。按照以下步骤进行操作：

a. 使用域控制器证书配置域控制器，以对智能卡用户进行身份验证。如果您在 Active Directory 中配置了 Active Directory 证书服务企业 CA，它会自动使用启用智能卡登录的证书注册域控制器。如果您没有 Active Directory 证书服务，请参阅对第三方 CA 的域控制器证书的要求。您可以使用 Amazon 私有 CA 创建域控制器证书。如果这样做，请不要使用为短期证书配置的私有 CA。

> **Note**
>
> 如果使用 Amazon Managed Microsoft AD，则可以在满足域控制器证书要求的 Amazon EC2 实例上配置证书服务。有关配置了 Active Directory 证书服务的 Amazon Managed Microsoft AD 的部署示例，请参阅将 Active Directory 部署到新的 Amazon Virtual Private Cloud。
> 使用 Amazon Managed Microsoft AD 和 Active Directory 证书服务，您还必须创建从控制器的 VPC 安全组到运行证书服务的 Amazon EC2 实例的出站规则。您必须为安全组提供对 TCP 端口 135 以及端口 49152 至 65535 的访问权限，才能启用证书自动注册。Amazon EC2 实例还必须允许域实例（包括域控制器）在这些相同的端口上进行入站访问。有关查找 Amazon Managed Microsoft AD 的安全组的更多信息，请参阅配置 VPC 子网和安全组。

b. 在 Amazon 私有 CA 控制台上导出私有 CA 证书，或者使用 SDK 或 CLI 导出私有 CA 证书。有关更多信息，请参阅导出私有证书。

c. 将私有 CA 发布到 Active Directory。登录到域控制器或已加入域的计算机。将私有 CA 证书复制到任意 *<path>**<file>*，然后以域管理员身份运行以下命令。您也可以使用组策略和 Microsoft PKI Health Tool（PKIView）发布 CA。有关更多信息，请参阅配置说明。

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

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

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

> **Note**
>
> Active Directory 必须在 WorkSpaces Pools 中的 WorkSpaces 加入域时自动将 CA 分发给受信任的根证书颁发机构和 Enterprise NTAuth 存储。

> **Note**
>
> Active Directory 域控制器必须处于兼容模式，证书强制执行才能支持基于证书的身份验证。有关更多信息，请参阅 Microsoft Support 文档中的 KB5014754 - Windows 域控制器上基于证书的身份验证更改。如果您使用的是 Amazon 托管 Microsoft AD，请参阅配置目录安全设置，以了解更多信息。

启用基于证书的身份验证

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

要启用基于证书的身份验证，请完成以下步骤。

启用基于证书的身份验证

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在导航窗格中，选择目录。
3. 选择池目录选项卡。
4. 选择要配置的目录。
5. 在该页面的身份验证部分，选择编辑。
6. 在该页面基于证书的身份验证部分，选择编辑基于证书的身份验证。
7. 选择启用基于证书的身份验证。
8. 在 Amazon Certificate Manager（ACM）私有证书颁发机构（CA）下拉列表中，选择证书。

   要显示在下拉列表中，应将私有 CA 存储在相同的 Amazon Web Services 账户和 Amazon Web Services 区域。您还必须使用名为 `euc-private-ca` 的密钥标记私有 CA。
9. 在回退模式下配置目录日志。在回退模式下，如果基于证书的身份验证不成功，用户可以使用其 AD 域密码登录。仅当用户知道自己的域密码时，才建议这样做。关闭回退功能后，如果出现锁屏或 Windows 注销，则会话可能会断开用户的连接。如果开启了回退功能，则会话会提示用户输入 AD 域密码。
10. 选择保存。

基于证书的身份验证现已启用。当用户使用加入域的 WorkSpaces 通过 SAML 2.0 向 WorkSpaces Pools 目录进行身份验证时，他们将不再收到输入域密码的提示。用户在连接到启用了基于证书的身份验证的会话时，会看到一条使用基于证书的身份验证进行连接消息。

管理基于证书的身份验证

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

启用基于证书的身份验证后，请查看以下任务。

私有 CA 证书

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

最终用户证书

Amazon 私有证书颁发机构 为 WorkSpaces Pools 基于证书的身份验证颁发的最终用户证书不需要续订或吊销。这些证书的有效期较短。WorkSpaces Pools 会为每个新会话自动颁发新证书，或者对于持续时间较长的会话，每 24 小时自动颁发一次新证书。WorkSpaces Pools 会话控制这些最终用户证书的使用。如果您结束会话，WorkSpaces Pools 将停止使用该证书。这些最终用户证书的有效期比典型 Amazon 私有证书颁发机构 CRL 分发的有效期短。因此，无需吊销最终用户证书，这些证书也不会出现在 CRL 中。

审核报告

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

日志记录和监控

您可以使用 CloudTrail 来记录 WorkSpaces Pools 对私有 CA 的 API 调用。有关更多信息，请参阅《Amazon CloudTrail 用户指南》中的什么是 Amazon CloudTrail？，以及《Amazon 私有证书颁发机构 用户指南》中的使用 CloudTrail。在 CloudTrail 事件历史记录中，您可以查看由 WorkSpaces Pools EcmAssumeRoleSession 用户名创建的 acm-pca.amazonaws.com 事件源中的 GetCertificate 和 IssueCertificate 事件名称。将针对每个 WorkSpaces Pools 基于证书的身份验证请求记录这些事件。有关更多信息，请参阅《Amazon CloudTrail 用户指南》中的使用 CloudTrail 事件历史记录查看事件。

启用跨账户 PCA 共享

> **Important**
>
> “ WorkSpaces 池” 功能不适用于北京和宁夏区域。

私有 CA（PCA）跨账户共享允许为其他账户授予使用集中式 CA 的权限。该 CA 可以通过使用 Amazon Resource Access Manager（RAM）来管理权限，从而生成和颁发证书。这样就无需在每个账户中都使用私有 CA。私有 CA 跨账户共享可以与基于 WorkSpaces 应用程序证书的身份验证 (CBA) 一起使用。Amazon Web Services 区域

要将共享的私有 CA 资源与 WorkSpaces 池 CBA 一起使用，请完成以下步骤：

1. 以集中Amazon Web Services 账户方式为 CBA 配置私有 CA。有关更多信息，请参阅 the section called “基于证书的身份验证”。
2. 与资源 WorkSpaces 池资源使用 CBA Amazon Web Services 账户 的资源共享私有 CA。为此，请按照如何使用 Amazon RAM 跨账户共享您的 ACM 私有 CA 中的步骤进行操作。您无需完成步骤 3 来创建证书。您可以与个人 Amazon Web Services 账户共享私有 CA，也可以通过 Amazon Organizations共享。如果您与个人账户共享，则需要使用Amazon Resource Access Manager控制台或接受资源账户中的共享私有 CA APIs。

   配置共享时，请确认Amazon Resource Access Manager资源账户中私有 CA 的资源共享使用`AWSRAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority`管权限模板。此模板与 P WorkSpaces ools 服务角色在颁发 CBA 证书时使用的 PCA 模板一致。
3. 共享成功后，使用资源账户中的私有 CA 控制台查看共享的私有 CA。
4. 使用 API 或 CLI 将私有 CA ARN 与 Pools 目录中的 WorkSpaces CBA 相关联。目前，P WorkSpaces ools 控制台不支持选择共享私有 CA ARNs。有关更多信息，请参阅《亚马逊 WorkSpaces服务 API 参考》。

WorkSpaces Pools Active Directory 管理

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

设置 Active Directory 并将其与 WorkSpaces Pools 结合使用的过程涉及以下管理任务。

任务

- 授予创建和管理 Active Directory 计算机对象的权限
- 查找组织单位的可分辨名称
- 在自定义映像上授予本地管理员权限
- 在用户空闲时锁定流式传输会话
- 配置 WorkSpaces Pools 以使用域信任

授予创建和管理 Active Directory 计算机对象的权限

要允许 WorkSpaces Pools 执行 Active Directory 计算机对象操作，您需要一个具有足够权限的账户。最佳实践是使用仅具有所需最低权限的账户。最低的 Active Directory 组织单位 (OU) 权限如下所示：

- 创建计算机对象
- 更改密码
- 重置密码
- 编写描述

在设置权限之前，需要先完成以下任务：

- 获取对已加入域的计算机或 EC2 实例的访问权限。
- 安装 Active Directory 用户和计算机 MMC 管理单元。有关更多信息，请参阅 Microsoft 文档中的安装或删除适用于 Windows 7 的远程服务器管理工具。
- 以拥有适当权限的域用户身份登录并修改 OU 安全设置。
- 创建或标识要向其委派权限的用户、服务账户或组。

设置最低权限

1. 在域中或域控制器上打开 Active Directory Users and Computers (Active Directory 用户和计算机)。
2. 在左侧导航窗格中，选择要在其中提供域加入权限的第一个 OU，打开上下文 (右键单击) 菜单，然后选择 Delegate Control (委派控制)。
3. 在控制委派向导页面上，依次选择下一步和添加。

4. 对于选择用户、计算机或组，选择先前创建的用户、服务账户或组，然后选择确定。
5. 在 Tasks to Delegate (要委派的任务) 页面上，选择 Create a custom task to delegate (创建要委派的自定义任务)，然后选择 Next (下一步)。
6. 依次选择只是在这个文件夹中的下列对象和计算机对象。
7. 依次选择在这个文件夹中创建所选对象和下一步。
8. 对于权限，选择读取、写入、更改密码、重置密码，然后选择下一步。
9. 在完成控制委派向导页面上，验证信息并选择完成。
10. 对需要这些权限的任何额外的 OU 重复步骤 2-9。

如果您将权限委派给组，则创建具有强密码的用户或服务账户，并将该账户添加到组中。这样该账户将拥有足够的权限将 WorkSpaces 连接到目录。在创建 WorkSpaces Pools 目录配置时需使用该账户。

查找组织单位的可分辨名称

向 WorkSpaces Pools 注册 Active Directory 域时，必须提供组织部门（OU）的可分辨名称。为此目的创建一个 OU。默认计算机容器不是 OU，不能供 WorkSpaces Pools 使用。以下步骤演示如何获得此名称。

> **Note**
>
> 可分辨名称必须以 **OU=** 开头，否则不能用于计算机对象。

需要先执行以下操作，然后才能完成此过程:

- 获取对已加入域的计算机或 EC2 实例的访问权限。
- 安装 Active Directory 用户和计算机 MMC 管理单元。有关更多信息，请参阅 Microsoft 文档中的安装或删除适用于 Windows 7 的远程服务器管理工具。
- 以拥有适当权限的域用户身份登录并读取 OU 安全属性。

查找 OU 的可分辨名称

1. 在域中或域控制器上打开 Active Directory Users and Computers (Active Directory 用户和计算机)。
2. 在查看下，确保高级功能已启用。

3. 在左侧导航窗格中，选择要用于 WorkSpaces 计算机对象的第一个 OU，打开上下文（右键单击）菜单，然后选择属性。
4. 选择属性编辑器。
5. 在属性下，对于 distinguishedName，选择 查看。
6. 对于 Value (值)，选择可分辨名称，打开上下文 (右键单击) 菜单，然后选择 Copy (复制)。

在自定义映像上授予本地管理员权限

默认情况下，Active Directory 域用户对于映像不具有本地管理员权限。您可以通过使用目录中的组策略首选项，或通过在映像上使用本地管理员账户来手动授予这些权限。为域用户授予本地管理员权限将允许该用户在 WorkSpaces Pools 中安装应用程序和创建自定义映像。

目录

- 使用组策略首选项
- 使用 WorkSpace 上的本地管理员组创建映像

使用组策略首选项

可以使用组策略首选项为 Active Directory 用户或组以及指定 OU 中的所有计算机对象授予本地管理员权限。Active Directory 用户或组必须存在才能向其授予本地管理员权限。要使用组策略首选项，需要先执行以下操作：

- 获取对已加入域的计算机或 EC2 实例的访问权限。
- 安装组策略管理控制台(GPMC) MMC 管理单元。有关更多信息，请参阅 Microsoft 文档中的安装或删除适用于 Windows 7 的远程服务器管理工具。
- 以有权创建组策略对象 (GPO) 的域用户身份登录。将 GPO 链接到相应 OU。

使用组策略首选项授予本地管理员权限

1. 在您的目录中或域控制器上，以管理员身份打开命令提示符，键入 `gpmc.msc`，然后按 Enter。
2. 在左侧控制台树中，选择将在其中创建新 GPO 的 OU，或使用现有 GPO，然后执行以下任一操作：
   - 通过打开上下文 (右键单击) 菜单并选择在此域中创建 GPO，在此处链接来创建新的 GPO。对于 Name，为该 GPO 提供一个描述性名称。
   - 选择现有 GPO。

3. 打开 GPO 的上下文菜单并选择编辑。
4. 在控制台树中，依次选择 Computer Configuration (计算机配置)、Preferences (首选项)、Windows Settings (Windows 设置)、Control Panel Settings (控制面板设置) 和 Local Users and Groups (本地用户和组)。
5. 选择 Local Users and Groups (本地用户和组)，打开上下文菜单，选择 New (新建)、Local Group (本地组)。
6. 对于 Action，选择 Update。
7. 对于 Group name，选择 Administrators (built-in)。
8. 在成员下，选择添加… 并指定 Active Directory 用户账户或组，以便为其分配流实例的本地管理员权限。对于 Action，选择 Add to this group，然后选择 OK。
9. 要将此 GPO 应用于其他 OU，请选择其他 OU，打开上下文菜单，然后选择 Link an Existing GPO (链接现有 GPO)。
10. 使用在步骤 2 中指定的新的或现有的 GPO 名称，滚动查找 GPO，然后选择 OK (确定)。
11. 对应具有此首选项的其他 OU 重复步骤 9 和 10。
12. 选择 OK (确定) 以关闭 New Local Group Properties (新建本地组属性) 对话框。
13. 再次选择 OK (确定) 以关闭 GPMC。

要将新首选项应用于 GPO，必须停止并重新启动正在运行的任何映像生成器或实例集。对于在步骤 8 中指定的 Active Directory 用户和组，将自动为它们授予对 GPO 链接到的 OU 中的映像生成器和实例集的本地管理员权限。

使用 WorkSpace 上的本地管理员组创建映像

要授予 Active Directory 用户或组对映像的本地管理员权限，您可以手动将这些用户或组添加到映像上的本地管理员组中。

Active Directory 用户或组必须存在才能向其授予本地管理员权限。

1. 连接到用于构建映像的 WorkSpace。WorkSpace 必须处于运行状态且已加入域。
2. 依次选择开始、管理工具，然后单击计算机管理。
3. 在左侧导航窗格中，选择本地用户和组并打开组文件夹。
4. 打开管理员组，选择添加...。
5. 选择要向其分配本地管理员权限的所有 Active Directory 用户或组，然后选择确定。再次选择确定以关闭管理员属性窗口。
6. 关闭“计算机管理”。

7. 要以 Active Directory 用户身份登录并测试该用户在 WorkSpaces 上是否具有本地管理员权限，请选择管理命令、切换用户，然后输入相关用户的凭证。

在用户空闲时锁定流式传输会话

WorkSpaces Pools 依赖在 GPMC 中配置的设置来在用户空闲指定时间后锁定流式传输会话。要使用 GPMC，需要先执行以下操作：

- 获取对已加入域的计算机或 EC2 实例的访问权限。
- 安装 GPMC。有关更多信息，请参阅 Microsoft 文档中的安装或删除适用于 Windows 7 的远程服务器管理工具。
- 以有权创建 GPO 的域用户身份登录。将 GPO 链接到相应 OU。

在用户空闲时自动锁定流实例

1. 在您的目录中或域控制器上，以管理员身份打开命令提示符，键入 `gpmc.msc`，然后按 Enter。
2. 在左侧控制台树中，选择将在其中创建新 GPO 的 OU，或使用现有 GPO，然后执行以下任一操作：
   - 通过打开上下文 (右键单击) 菜单并选择在此域中创建 GPO，在此处链接来创建新的 GPO。对于 Name，为该 GPO 提供一个描述性名称。
   - 选择现有 GPO。
3. 打开 GPO 的上下文菜单并选择编辑。
4. 在用户配置下，依次展开策略、管理模板、控制面板，然后选择 个性化。
5. 双击启用屏幕保护程序。
6. 在启用屏幕保护程序策略设置中，选择已启用。
7. 选择应用，然后选择确定。
8. 双击强制使用特定的屏幕保护程序。
9. 在强制使用特定的屏幕保护程序策略设置中，选择已启用。
10. 在 可执行的屏幕保护程序的名称下，输入 **`scrnsave.scr`**。启用此设置后，系统将在用户桌面上显示黑屏保护程序。
11. 选择应用，然后选择确定。
12. 双击密码保护屏幕保护程序。
13. 在密码保护屏幕保护程序策略设置中，选择已启用。

14. 选择应用，然后选择确定。
15. 双击屏幕保护程序超时。
16. 在屏幕保护程序超时策略设置中，选择已启用。
17. 对于秒，请指定在应用屏幕保护程序之前，用户必须处于空闲状态的时间长度。要将空闲时间设置为 10 分钟，请指定 600 秒。
18. 选择应用，然后选择确定。
19. 在控制台树中的用户配置下，依次展开策略、管理模板、系统，然后选择 Ctrl+Alt+Del 选项。
20. 双击删除“锁定计算机”。
21. 在删除“锁定计算机”策略设置中，选择已禁用。
22. 选择应用，然后选择确定。

配置 WorkSpaces Pools 以使用域信任

WorkSpaces Pools 支持网络资源（如文件服务器、应用程序和计算机对象）驻留在一个域中而用户对象驻留在另一个域中的 Active Directory 域环境。用于计算机对象操作的域服务账户不需要与 WorkSpaces Pools 计算机对象位于同一个域。

创建目录配置时，请指定在 Active Directory 域 (文件服务器、应用程序、计算机对象和其他网络资源驻留的位置) 中具有管理计算机对象的相应权限的服务账户。

对于以下项目，您的最终用户 Active Directory 账户必须拥有“允许身份验证”权限：

- WorkSpaces Pools 计算机对象
- 域的域控制器

有关更多信息，请参阅 授予创建和管理 Active Directory 计算机对象的权限。

更多信息

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

有关与此主题相关的更多信息，请参阅以下资源：

- Microsoft Active Directory - 有关使用 Amazon Directory Service 的信息。

WorkSpaces Pools 的捆绑包和映像

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

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 可用的各种公有捆绑包的更多信息，请参阅 Amazon WorkSpaces 捆绑包。

如果您已启动 Windows WorkSpace 并对其进行了自定义，则可以从该 WorkSpace 创建自定义映像，以便与 WorkSpaces Pools 一起使用。WorkSpaces Pools 不支持 Linux。

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，您可以在创建新的 WorkSpaces Pools 时指定此自定义捆绑包，以确保池中新的 WorkSpaces 具有相同的一致配置（硬件和软件）。

如果您需要执行软件更新或在 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。

WorkSpaces Pools 支持多种不同的操作系统（OS）、流式传输协议和捆绑包。下表提供了有关每个操作系统支持的许可、流式传输协议和捆绑包的信息。

操作系统	许可证	流式传输协议	支持的捆绑包	生命周期策略/停用日期
Windows Server 2019	包含	DCV	Value、Standard、Performance、Power、PowerPro	2029 年 1 月 9 日
Windows Server 2022	包含	DCV	Standard、Performance、Power、PowerPro、Graphics.G4dn、GraphicsPro.G4dn	2031 年 10 月 14 日

> **Note**
>
> - 不再受供应商支持的操作系统版本不能保证正常工作，也不受 Amazon Support 支持。

主题

- WorkSpaces Pools 的捆绑包选项
- 为 WorkSpaces Pools 创建自定义映像和捆绑包
- 管理 WorkSpaces Pools 的自定义映像和捆绑包
- 使用会话脚本来管理您的用户的流式传输体验

WorkSpaces Pools 的捆绑包选项

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

在选择要用于 WorkSpaces Pools 的捆绑包之前，请确保要选择的捆绑包与 WorkSpaces 的协议、操作系统、网络和计算类型兼容。建议您通过运行和使用复制用户日常任务的应用程序，在测试环境中测试您要选择的捆绑包的性能。有关协议的更多信息，请参阅 WorkSpaces 个人协议。有关网络的更多信息，请参阅 WorkSpaces 个人版客户端网络要求。

以下公有捆绑包可以与 WorkSpaces Pools 一起使用。有关 WorkSpaces 捆绑包的信息，请参阅 Amazon WorkSpaces 捆绑包。Value、Standard、Performance、Power、PowerPro

经济捆绑包

此捆绑包非常适合以下用途：

- 基本的文本编辑和数据输入
- 使用量较少的 Web 浏览
- 即时消息发送

不建议将此捆绑包用于文字处理、音频和视频会议、屏幕共享、软件开发工具、商业智能应用程序和图形应用程序。

标准捆绑包

此捆绑包非常适合以下用途：

- 基本的文本编辑和数据输入
- Web 浏览
- 即时消息发送
- 电子邮件

不建议将此捆绑包用于音频和视频会议、屏幕共享、文字处理、软件开发工具、商业智能应用程序和图形应用程序

性能捆绑包

此捆绑包非常适合以下用途：

- Web 浏览
- 文字处理
- 即时消息发送
- 电子邮件
- 电子表格
- 音频处理
- 课件

不建议将此捆绑包用于视频会议、屏幕共享、软件开发工具、商业智能应用程序和图形应用程序

节能捆绑包

此捆绑包非常适合以下用途：

- Web 浏览
- 文字处理
- 电子邮件
- 即时消息发送
- 电子表格

- 音频处理
- 软件开发（集成式开发环境 (IDE)）
- 中级数据处理入门
- 音频和视频会议

不建议将此捆绑包用于屏幕共享、软件开发工具、商业智能应用程序和图形应用程序。

PowerPro 捆绑包

此捆绑包非常适合以下用途：

- Web 浏览
- 文字处理
- 电子邮件
- 即时消息发送
- 电子表格
- 音频处理
- 软件开发（集成式开发环境 (IDE)）
- 数据仓库
- 商业智能应用程序
- 音频和视频会议

不建议将此捆绑包用于机器学习模型训练和图形应用程序

Graphics.g4dn 捆绑包

该捆绑包为您的 WorkSpaces 提供高水平图形性能以及中等水平 CPU 性能和内存，非常适合以下用途：

- Web 浏览
- 文字处理
- 电子邮件
- 电子表格
- 即时消息发送

- 音频会议
- 软件开发（集成式开发环境 (IDE)）
- 中级数据处理入门
- 数据仓库
- 商业智能应用程序
- 图形设计
- CAD/CAM（计算机辅助设计/计算机辅助制造）

不建议将此捆绑包用于音频和视频会议、3D 渲染、照片级逼真设计和机器学习模型训练

GraphicsPro.g4dn 捆绑包

该捆绑包为您的 WorkSpaces 提供高水平图形性能、CPU 性能和内存，非常适合以下用途：

- Web 浏览
- 文字处理
- 电子邮件
- 电子表格
- 即时消息发送
- 音频会议
- 软件开发（集成式开发环境 (IDE)）
- 中级数据处理入门
- 数据仓库
- 商业智能应用程序
- 图形设计
- CAD/CAM（计算机辅助设计/计算机辅助制造）
- 视频转码
- 3D 渲染
- 照片级逼真设计
- 游戏流
- ML（机器学习）模型训练和 ML 推理

不建议将此捆绑包用于音频和视频会议。

为 WorkSpaces Pools 创建自定义映像和捆绑包

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

WorkSpaces Pools 仅支持 Windows 映像和捆绑包。如果您已启动 Windows 或 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**
>
> - 自定义捆绑包存储量不能小于映像存储量。

自定义捆绑包的成本与创建这些捆绑包的公有捆绑包的成本相同。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
- 最佳实践
- 步骤 1：运行映像检查程序
- 步骤 2：创建自定义映像和自定义捆绑包
- Windows WorkSpace 自定义映像中包含的内容

创建 Windows 自定义映像的要求

> **Note**
>
> Windows 目前将 1 GB 定义为 1,073,741,824 字节。您必须确保 C 驱动器上的可用空间大于 12,884,901,888 字节（或 12 GiB），并且用户配置文件小于 10,737,418,240 字节（或 10 GiB），才能创建 WorkSpace 映像。

- WorkSpace 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 驱动器上。
- 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 WorkSpaces 将无法正常运行。有关更多信息，请参阅 the section called “必需配置和服务组件”。
  - Windows PowerShell 3.0 或更高版本
  - 远程桌面服务
  - Amazon 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
  - Amazon 和 WorkSpaces 证书
  - Skylight 代理
- WorkSpaces 虚拟桌面池仅支持最大为 200 GB 的捆绑包/映像根卷大小。创建 Windows 自定义映像时，请确保其根卷大小小于 200 GB。

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 WorkSpace 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。
- 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 个人的 IP 地址和端口要求。
- 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`)。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。
- 确保在 WorkSpaces 上更新网络依赖驱动程序，例如 ENA、NVMe 和 PV 驱动程序。您应该至少每 6 个月更新一次。有关更多信息，请参阅安装或升级弹性网络适配器（ENA）驱动程序、Windows 实例的 Amazon NVMe 驱动程序以及升级 Windows 实例上的 PV 驱动程序。
- 确保定期将 EC2Config、EC2Launch 和 EC2Launch V2 代理更新到最新版本。您应该至少每 6 个月更新一次。有关更多信息，请参阅更新 EC2Config 和 EC2Launch。

步骤 1：运行映像检查程序

要确认 Windows WorkSpace 满足映像创建的要求，建议运行映像检查程序应用程序。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。映像检查程序仅适用于 Windows WorkSpace。

> **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。

要获取映像检查程序，请执行以下操作之一：

- 重启您的 WorkSpace。系统会在重新启动期间自动下载映像检查程序并将其安装在 `C:\Program Files\Amazon\ImageChecker.exe` 中。
- 从 https://tools.amazonworkspaces.awsapps.cn/ImageChecker.zip 下载 Amazon WorkSpaces 映像检查程序，并提取 `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。

   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。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 Amazon Web Services 支持 中心，以修复您的 EC2Config 或 EC2Launch。

用户配置文件大小必须小于 10 GB

对于 Windows 7 WorkSpaces，用户配置文件 (`D:\Users\`*`username`*) 的总大小必须小于 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

对于 Windows 7 WorkSpaces，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。对于 Windows 10 WorkSpaces，如果您收到一条 `FAILED` 消息并且磁盘空间超过 2 GB，请忽略。

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. 选择确定。

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，选择互联网协议版本 4 (TCP/IPv4)，然后选择属性。
7. 在互联网协议版本 4 (TCP/IPv4) 属性对话框中，选择自动获取 IP 地址。
8. 选择确定。
9. 对 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. 选择确定。

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 Amazon Web Services 支持 中心寻求帮助。

必须正确配置环境变量路径

本地计算机的环境变量路径缺少与 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. 选择确定。
7. 重新启动 WorkSpace。

> **Tip**
>
> 项目在环境变量路径中显示的顺序至关重要。要确定正确的顺序，您可能需要将 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. 选择确定。

必须禁用 Amazon SSM 代理

创建映像过程要求禁用 Amazon SSM 代理服务。

禁用 Amazon SSM 代理服务

1. 在 Windows 搜索框中，输入 **`services.msc`** 以打开 Windows 服务管理器。
2. 在名称列中，找到 Amazon SSM 代理。
3. 选择 Amazon SSM 代理，然后选择操作、属性。
4. 在常规选项卡上，对于启动类型，选择已禁用。
5. 选择确定。

必须启用 SSL3 和 TLS 1.2 版本

要为 Windows 配置 SSL/TLS，请参阅 Microsoft Windows 文档中的如何启用 TLS 1.2。

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 Windows 键 + 暂停中断，然后在控制面板 > 系统和安全 > 系统对话框的左侧窗格中，选择高级系统设置。
   - 在 Windows 搜索框中，输入 **`control panel`**。在“控制面板”中，选择系统和安全，然后选择“系统”，随后在控制面板 > 系统和安全 > 系统对话框的左侧窗格中，选择高级系统设置。
2. 在系统属性对话框的高级选项卡上，选择用户配置文件下的设置。
3. 如果除了管理员配置文件、默认配置文件和预期 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。

其他故障排查提示

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*" }
```

- 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. 选择确定。

步骤 2：创建自定义映像和自定义捆绑包

验证 WorkSpace 映像后，请完成以下步骤，使用 WorkSpaces 控制台创建自定义映像和自定义捆绑包。要以编程方式创建映像，请使用 CreateWorkspaceImage API 操作。有关更多信息，请参阅《Amazon WorkSpaces API 参考》中的 CreateWorkspaceImage。要以编程方式创建捆绑包，请使用 CreateWorkspaceBundle API 操作。有关更多信息，请参阅《Amazon WorkSpaces API 参考》中的 CreateWorkSpaceBundle。

使用 WorkSpaces 控制台创建自定义映像和自定义捆绑包

1. 如果您仍连接到 WorkSpace，请通过在 WorkSpaces 客户端应用程序中选择 Amazon WorkSpaces 和断开连接，来断开连接。
2. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
3. 在导航窗格中，选择 WorkSpaces。
4. 选择 WorkSpace 以打开其详细信息页面，然后选择创建映像。如果 WorkSpace 的状态为已停止，则必须先启动它（选择操作、启动 WorkSpaces），然后才能选择操作、创建映像。

5. 将显示一条消息，提示您在继续操作之前重启（重新启动）WorkSpace。重启 WorkSpace 会将您的 Amazon WorkSpaces 软件更新到最新版本。

   要重启 WorkSpace，请关闭该消息并按照重启 WorkSpaces 个人版中的 WorkSpace 中的步骤操作。完成后，重复执行此过程中的Step 4，但这次在显示重启消息时，选择下一步。要创建映像，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。

   不要在描述中使用短划线（-）特殊字符。它会引发错误。
7. 在导航窗格中，选择映像。当 WorkSpace 的状态变为可用时，映像完成（此过程最多可需要 45 分钟）。
8. 选择映像，然后选择操作、创建捆绑包。
9. 输入服务包的名称和描述，然后执行以下操作：

   - 对于捆绑包硬件类型，选择从该自定义捆绑包启动 WorkSpaces 时要使用的硬件。
   - 根卷的默认可用大小组合为每个 WorkSpace 200 GB。
10. 要确认您的捆绑包是否已创建，请选择捆绑包，并检查该捆绑包已列出。

Windows WorkSpace 自定义映像中包含的内容

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

- 联系人
- Downloads
- 音乐
- 图片
- 已保存的游戏
- 视频
- 播客
- 虚拟机
- 虚拟机
- 跟踪
- appdata\local\temp

- appdata\roaming\apple computer\mobilesync\
- appdata\roaming\apple computer\logs\
- appdata\roaming\apple computer\itunes\iphone software updates\
- appdata\roaming\macromedia\flash player\macromedia.com\support\flashplayer\sys\
- appdata\roaming\macromedia\flash player\#sharedobjects\
- appdata\roaming\adobe\flash player\assetcache\
- appdata\roaming\microsoft\windows\recent\
- appdata\roaming\microsoft\office\recent\
- appdata\roaming\microsoft office\live meeting
- appdata\roaming\microsoft shared\livemeeting shared\
- appdata\roaming\mozilla\firefox\crash reports\
- appdata\roaming\mcafee\common framework\
- appdata\local\microsoft\feeds cache
- appdata\local\microsoft\windows\temporary互联网files\
- appdata\local\microsoft\windows\history\
- appdata\local\microsoft\internet explorer\domstore\
- appdata\local\microsoft\internet explorer\imagestore\
- appdata\locallow\microsoft\internet explorer\iconcache\
- appdata\locallow\microsoft\internet explorer\domstore\
- appdata\locallow\microsoft\internet explorer\imagestore\
- appdata\local\microsoft\internet explorer\recovery\
- appdata\local\mozilla\firefox\profiles\

管理 WorkSpaces Pools 的自定义映像和捆绑包

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

在 WorkSpaces 个人版和 WorkSpaces Pools 中，管理自定义映像和捆绑包的过程相同。有关如何管理映像和捆绑包的更多信息，请参阅本指南“WorkSpaces 个人版”一节中的以下文档：

Note

您可用于 WorkSpaces 个人版的自定义捆绑包与可用于 WorkSpaces Pools 的自定义捆绑包之间的主要区别在于，可以使用的操作系统和基本公有捆绑包。有关 WorkSpaces Pools 中支持的操作系统和捆绑包，请参阅

Important

WorkSpaces Pools 功能不在北京和宁夏区域提供。

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 可用的各种公有捆绑包的更多信息，请参阅 Amazon WorkSpaces 捆绑包。

下表提供了有关每个操作系统支持的许可、流式传输协议和捆绑包的信息。

Windows Server 2019	包含	DCV	Value、Standard、Performance、Power、PowerPro
Windows Server 2022	包含	DCV	Standard、Performance、Power、PowerPro、Graphics.G4dn、GraphicsPro.G4dn
操作系统	许可证	流式传输协议	支持的捆绑包

Note

- 不再受供应商支持的操作系统版本不能保证正常工作，也不受 Amazon Support 支持。

。

- 更新 WorkSpaces 个人版的自定义捆绑包.
- 在 “个 WorkSpaces 人” 中复制自定义镜像.
- 共享或取消共享自定义 WorkSpaces 个人版映像.
- 删除 WorkSpaces 个人版中的自定义捆绑包或映像.

使用会话脚本来管理您的用户的流式传输体验

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

WorkSpaces Pools 提供实例上的会话脚本。当用户的流式传输会话中发生特定事件时，您可以使用这些脚本来运行自己的自定义脚本。例如，您可以在用户的流式传输会话开始之前使用自定义脚本来准备 WorkSpaces Pools 环境。您还可以在用户完成其流式传输会话后使用自定义脚本清理流实例。

会话脚本是在 WorkSpace 映像中指定的。这些脚本在用户上下文或系统上下文中运行。如果您的会话脚本使用标准输出来编写信息、错误或调试消息，则可以选择将这些脚本保存到 Amazon Web Services 账户内的 Amazon S3 存储桶中。

目录

- 在流式传输会话开始前运行脚本
- 在流式传输会话结束后运行脚本
- 创建并指定会话脚本
- 会话脚本配置文件
- 使用 Windows PowerShell 文件
- 记录会话脚本输出
- 结合使用永久存储与会话脚本
- 为会话脚本日志启用 Amazon S3 存储桶存储

在流式传输会话开始前运行脚本

您可以将脚本配置为在用户的应用程序启动和其流式传输会话开始前运行最多 60 秒。这样做可以让您在用户开始流式传输其应用程序前自定义 WorkSpaces Pools 环境。在会话脚本运行时，会为您的用户

显示加载转盘。当您的脚本成功完成或超过最长等待时间时，用户的流式传输会话将开始。如果脚本未成功完成，则会为用户显示错误消息。但是，不会阻止您的用户使用其流式传输会话。

在指定 Windows 实例上的文件名时，您必须使用双反斜杠。例如：

```
C:\\Scripts\\Myscript.bat
```

如果未使用双反斜杠，则会显示一个错误以通知您 `.json` 文件格式不正确。

> **Note**
>
> 脚本成功完成后，它们必须返回值 0。如果脚本返回 0 以外的值，则 WorkSpaces 将向用户显示错误消息。

在流式传输会话开始前运行脚本时，会发生以下过程：

1. 您的用户连接到未加入域的 WorkSpaces Pools 中的 WorkSpace。它们使用 SAML 2.0 连接。
2. 发生下列情况之一：
   - 如果为用户启用了应用程序设置持久性，则会下载并装入用于存储用户的自定义项和 Windows 设置的应用程序设置虚拟硬盘 (VHD) 文件。在此情况下，需要 Windows 用户登录。

     有关应用程序设置持久性的信息，请参阅为 WorkSpaces Pools 用户启用应用程序设置持久性。。
   - 如果未启用应用程序设置持久性，则表示 Windows 用户已登录。
3. 您的会话脚本启动。如果为用户启用了持久性存储，则还会启动存储连接器安装。有关持久性存储的信息，请参阅为 WorkSpaces Pools 启用和管理永久存储。

   > **Note**
   >
   > 无需完成存储连接器安装即可启动流式传输会话。如果会话脚本在存储连接器安装完成之前完成，则流式传输会话将启动。
   > 有关监控存储连接器的装载状态的信息，请参阅结合使用永久存储与会话脚本。
4. 您的会话脚本完成或超时。
5. 用户的流式传输会话启动。

在流式传输会话结束后运行脚本

您还可以将脚本配置为在用户的流式传输会话结束后运行。例如，当用户从 WorkSpaces 客户端工具栏中选择结束会话或达到会话允许的最大持续时间时，您可以运行脚本。您还可以使用这些会话脚本在流实例终止之前清理您的 WorkSpaces 环境。例如，您可以使用脚本来释放文件锁定或上传日志文件。在流式传输会话结束后运行脚本时，会发生以下过程：

1. 用户的 WorkSpaces 流式传输会话结束。
2. 会话终止脚本启动。
3. 会话终止脚本完成或超时。
4. 发生 Windows 用户注销。
5. 发生以下一种情况或同时发生以下两种情况（如果适用）：
   - 如果为用户启用了应用程序设置持久性，则会卸载用于存储用户的自定义项和 Windows 设置的应用程序设置 VHD 文件，并将该文件上传到您账户中的 Amazon S3 存储桶。
   - 如果为您的用户启用持久性存储，则存储连接器将完成最终同步并进行卸载。
6. WorkSpace 已终止。

创建并指定会话脚本

完成以下过程，在 WorkSpaces 虚拟桌面池中为 WorkSpaces 创建和指定会话脚本。

1. 连接到要从中创建自定义映像的 Windows WorkSpaces。
2. 如果目录 `/AWSEUC/SessionScripts` 尚不存在，请创建它。
3. 使用会话脚本配置模板创建配置文件 `/AWSEUC/SessionScripts/config.json`（如果尚不存在）。
4. 导航到 `C:\AWSEUC\SessionScripts`，并打开 `config.json` 配置文件。

   有关会话脚本参数的信息，请参阅会话脚本配置文件。
5. 完成更改后，保存并关闭 `config.json` 文件。
6. 完成从 WorkSpace 创建映像的步骤。有关更多信息，请参阅 为 WorkSpaces Pools 创建自定义映像和捆绑包。

会话脚本配置文件

要在 Windows 实例上找到会话脚本配置文件，请导航到 `C:\AWSEUC\SessionScripts\config.json`。该文件的格式如下所示。

> **Note**
>
> 配置文件为 JSON 格式。验证您在此文件中键入的任何文本是否为有效的 JSON 格式。

```
{
  "SessionStart": {
    "executables": [
      {
        "context": "system",
        "filename": "",
        "arguments": "",
        "s3LogEnabled": true
      },
      {
        "context": "user",
        "filename": "",
        "arguments": "",
        "s3LogEnabled": true
      }
    ],
    "waitingTime": 30
  },
  "SessionTermination": {
    "executables": [
      {
        "context": "system",
        "filename": "",
        "arguments": "",
        "s3LogEnabled": true
      },
      {
        "context": "user",
        "filename": "",
        "arguments": "",
        "s3LogEnabled": true
      }
```

```
    ],
    "waitingTime": 30
  }
}
```

您可以在会话脚本配置文件中使用以下参数。

SessionStart/SessionTermination

要基于对象的名称在相应会话事件中运行的会话脚本。

类型：字符串

必需：否

允许的值：、**SessionStartSessionTermination**

WaitingTime

会话脚本的最大持续时间（以秒为单位）。

类型：整数

必需：否

约束：最大持续时间为 60 秒。如果会话脚本未在此持续时间内完成，则它们将停止。如果您需要脚本继续运行，则将其作为单独的过程启动。

Executables

要运行的会话脚本的详细信息。

类型：字符串

必需：是

约束：每个会话事件可以运行的脚本的最大数目为 2（一个用于用户上下文，一个用于系统上下文）。

Context

要在其中运行会话脚本的上下文。

类型：字符串

必需：是

允许的值：、**usersystem**

Filename

要运行的会话脚本的完整路径。如果未指定此参数，则会话脚本不会运行。

类型：字符串

必需：否

约束：文件名和完整路径的最大长度为 1000 个字符。

允许的值：、**.bat**、**.exe.sh**

> **Note**
>
> 您还可以使用 Windows PowerShell 文件。有关更多信息，请参阅 使用 Windows PowerShell 文件。

Arguments

会话脚本或可执行文件的参数。

类型：字符串

必需：否

长度约束：最大长度为 1000 个字符。

S3LogEnabled

当此参数的值设置为 **True** 时，会在您的 Amazon Web Services 账户中创建一个 S3 存储桶来存储会话脚本所创建的日志。默认情况下，该值设置为 **True**。有关更多信息，请参阅本主题后面的记录会话脚本输出 部分。

类型：布尔值

必需：否

允许的值：、**TrueFalse**

使用 Windows PowerShell 文件

要使用 Windows PowerShell 文件，请在 `filename` 参数中指定 PowerShell 文件的完整路径：

```
"filename":
"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",
```

然后，在 **arguments** 参数中指定您的会话脚本：

```
"arguments": "-File \"C:\\path\\to\\session\\script.ps1\"",
```

最后，验证 PowerShell 执行策略是否允许运行 PowerShell 文件。

记录会话脚本输出

在配置文件中启用此选项时，WorkSpaces Pools 会自动捕获写入标准输出的会话脚本的输出。此输出将上传到您账户中的 Amazon S3 存储桶。您可以查看日志文件以进行故障排除或调试。

> **Note**
>
> 当会话脚本返回一个值时或 **WaitingTime** 中设置的值已过去时（以先到者为准），将上传日志文件。

结合使用永久存储与会话脚本

启用 WorkSpaces 永久存储后，存储会在会话启动脚本运行时开始装载。如果您的脚本依赖于正在装载的永久存储，则可以等待连接器可用。WorkSpaces 在 Windows WorkSpaces 上的 Windows 注册表中维护存储连接器的装载状态，键值如下：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\AWSEUC\Storage\<provided user
                name>\<Storage connector>
```

注册表项值如下所示：

- 提供的用户名 – 通过访问模式提供的用户 ID。访问模式及其值如下所示：
  - 用户池 – 用户的电子邮件地址
  - 流式传输 URL – UserID
  - SAML – NameID。如果用户名包含斜杠（例如，域用户的 SAMAccountName），则斜杠将替换为“-”字符。
- 存储连接器 – 为用户启用的持久性存储选项的连接器。存储连接器值如下所示：

- HomeFolder

每个存储连接器注册表项都包含 MountStatus DWORD 值。下表列出了 MountStatus 的可能值。

> **Note**
> 要查看这些注册表项，必须在映像上安装 Microsoft .NET Framework 4.7.2 或更高版本。

值	描述
0	未为此用户启用存储连接器
1	存储连接器安装正在进行中
2	已成功安装存储连接器
3	存储连接器安装失败
4	存储连接器安装已启用，但尚未安装

为会话脚本日志启用 Amazon S3 存储桶存储

在会话脚本配置中启用 Amazon S3 日志记录后，WorkSpaces Pools 会从会话脚本中捕获标准输出。输出会定期上传到您的 Amazon Web Services 账户中的 S3 存储桶。对于每个 Amazon 区域，WorkSpaces Pools 会在您的账户中创建一个对于您的账户和该区域而言是唯一的存储桶。

您无需执行任何配置任务即可管理这些 S3 存储桶。它们由 WorkSpaces 服务完全托管。存储在每个存储桶中的日志文件在传输中使用 Amazon S3 的 SSL 端点进行加密，在静态期间使用 Amazon S3 托管的加密密钥进行加密。存储桶以特定格式命名，如下所述：

```
wspool-logs-<region-code>-<account-id-without-hyphens>-random-identifier
```

<region-code>

这是在其中创建 WorkSpaces Pools 并为会话脚本日志启用了 Amazon S3 存储桶存储的 Amazon 区域代码。

<account-id-without-hyphens>

您的 Amazon Web Services 账户标识符。随机 ID 确保与该区域中的其他存储桶不发生冲突。存储桶名称的第一部分 `wspool-logs` 不随账户或区域而改变。

例如，如果您在账号 `123456789012` 美国西部（俄勒冈州）（`us-west-2`）区域中的映像中指定会话脚本，则 WorkSpaces Pools 会在您账户的该区域中创建一个具有如下所示名称的 Amazon S3 存储桶。只有具有足够权限的管理员才能删除此存储桶。

```
wspool-logs-us-west-2-1234567890123-abcdefg
```

禁用会话脚本不会删除存储在 S3 存储桶中的日志文件。要永久删除日志文件，您或具备足够权限的管理员必须使用 Amazon S3 控制台或 API 执行此操作。WorkSpaces Pools 添加了一个存储桶策略，以防止意外删除存储桶。

启用会话脚本后，将为启动的每个流式传输会话创建一个唯一文件夹。

存储在您账户的 S3 存储桶中的日志文件所在的文件夹路径使用以下结构：

```
<bucket-name>/<stack-name>/<fleet-name>/<access-mode>/<user-id-SHA-256-hash>/<session-
id>/SessionScriptsLogs/<session-event>
```

<bucket-name>

存储会话脚本的 S3 存储桶的名称。该名称格式如本节中前面所述。

<stack-name>

会话来自的堆栈的名称。

<fleet-name>

运行会话脚本的 WorkSpaces Pools 的名称。

<access-mode>

用户的标识方式：`custom` 表示 WorkSpaces API 或 CLI，`federated` 表示 SAML，`userpool` 表示用户池中的用户。

<user-id-SHA-256-hash>

用户特定的文件夹名称。此名称是使用从用户标识符生成的小写 SHA-256 哈希十六进制字符串创建的。

<session-id>

用户的流式传输会话的标识符。每个用户流式传输会话均生成一个唯一 ID。

<session-event>

生成会话脚本日志的事件。事件值为：`SessionStart` 和 `SessionTermination`。

以下示例文件夹结构适用于从 test-stack 和 test-fleet 启动的流式传输会话。会话使用用户 ID `testuser@mydomain.com` 的 API（来自 Amazon Web Services 账户 ID `123456789012`）和美国西部（俄勒冈州）区域（`us-west-2`）中的设置组 `test-stack`：

```
wspool-logs-us-west-2-1234567890123-abcdefg/test-stack/test-fleet/custom/
a0bcb1da11f480d9b5b3e90f91243143eac04cfccfbdc777e740fab628a1cd13/05yd1391-4805-3da6-
f498-76f5x6746016/SessionScriptsLogs/SessionStart/
```

此示例文件夹结构包含一个用于用户上下文会话启动脚本的日志文件，以及一个用于系统上下文会话启动脚本的日志文件（如果适用）。

监控 WorkSpaces Pools

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

监控是维护 WorkSpaces Pools 的可靠性、可用性和性能的重要环节。

目录

- WorkSpaces Pools 指标和维度

WorkSpaces Pools 指标和维度

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

Amazon WorkSpaces 将以下 WorkSpaces Pools 指标和维度信息发送到 Amazon CloudWatch。

WorkSpaces Pools 每分钟向 CloudWatch 发送一次指标。`AWS/Workspaces` 命名空间包括以下指标。

池使用情况指标

指标	描述
`ActiveUserSessionCapacity`	当前用于流式传输会话的用户会话数。 单位：计数 有效统计数据：Average、Minimum、Maximum
`ActualUserSessionCapacity`	可用于流式传输或当前正在流式传输的池会话总数。 `ActualUserSessionCapacity = AvailableUserSessionCapacity + ActiveUserSessionCapacity` 单位：计数 有效统计数据：Average、Minimum、Maximum
`AvailableUserSessionCapacity`	当前可供用户流式传输的空闲池会话数量。 `AvailableUserSessionCapacity = ActualUserSessionCapacity - ActiveUserSessionCapacity` 单位：计数 有效统计数据：Average、Minimum、Maximum
`PendingUserSessionCapacity`	正在为您的池预置的会话数量。表示预置完成后池可以支持的额外流式传输会话数。 单位：计数 有效统计数据：Average、Minimum、Maximum
`UserSessionsCapacityUtilization`	使用以下公式计算池中正在使用的会话百分比。

指标	描述
	`UserSessionCapacityUtilization = (ActiveUserSession Capacity / ActualUserSessionCapacity) * 100` 监控此指标有助于做出关于增加或减少池所需容量值的决定。 单位：百分比 有效统计数据：Average、Minimum、Maximum
`DesiredUserSessionCapacity`	正在运行或待处理的总会话数。该值表示池可以在稳定状态下支持的总并发流式传输会话数。 `DesiredUserSessionCapacity = ActualUserSessionCapacity + PendingUserSessionCapacity` 单位：计数 有效统计数据：Average、Minimum、Maximum
`InsufficientCapacityError`	因缺少容量而被拒绝的会话请求的数量。 您可以设置告警，使用此指标来通知等待流式传输会话的用户。 单位：计数 有效统计数据：Average、Minimum、Maximum、Sum

为 WorkSpaces Pools 启用和管理永久存储

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

WorkSpaces Pools 支持永久存储的主文件夹。作为 WorkSpaces Pools 管理员，您必须了解如何执行以下任务来为您的用户启用并管理永久存储。

目录

- 为您的 WorkSpaces Pools 用户启用并管理主文件夹

为您的 WorkSpaces Pools 用户启用并管理主文件夹

在您为 WorkSpaces Pools 启用主文件夹时，用户可以在其流式传输会话期间访问永久存储文件夹。您的用户不必进行任何额外配置即可访问其主文件夹。用户存储在其主文件夹中的数据会自动备份到您的 Amazon Web Services 账户的 Amazon Simple Storage Service（Amazon S3）存储桶中，并且可以在后续会话中供这些用户使用。

使用 Amazon S3 的 SSL 端点对文件和文件夹进行传输中加密。使用 Amazon S3 托管的加密密钥对文件和文件夹进行静态加密。

主文件夹存储在位于以下默认位置的 WorkSpaces Pools 中的 WorkSpaces：

- 对于单个会话、未加入域的 Windows WorkSpaces：`C:\Users\PhotonUser\My Files\Home Folder`
- 已加入域的 Windows WorkSpaces：`C:\Users\%username%\My Files\Home Folder`

作为管理员，如果您要将应用程序配置为保存到此主文件夹，请使用适用的路径。在某些情况下，您的用户可能无法找到其主文件夹，因为有些应用程序无法识别将主文件夹显示为文件浏览器中的顶级文件夹的重定向。如果是这种情况，您的用户可以通过浏览到文件浏览器中的相同目录来访问其主文件夹。

目录

- 与计算密集型应用程序关联的文件和目录
- 为您的 WorkSpaces Pools 用户启用主文件夹
- 管理您的主文件夹

与计算密集型应用程序关联的文件和目录

在 WorkSpaces Pools 流式传输会话期间，与保存基本生产应用程序所需的文件和目录相比，将与计算密集型应用程序关联的大型文件和目录保存到永久存储所花费的时间可能更长。例如，与保存执行单次写入操作的应用程序创建的文件相比，应用程序保存大量数据或频繁修改相同文件所需的时间可能更长。保存许多小文件也可能需要更长时间。

如果您的用户保存与计算密集型应用程序关联的文件和目录，而且 WorkSpaces Pools 永久存储选项的性能不如预期，我们建议您使用服务器消息块（SMB）解决方案，例如适用于 Windows File Server 的

Amazon FSx 或 Amazon Storage Gateway 文件网关。以下是与更适合与这些 SMB 解决方案一起使用的计算密集型应用程序关联的文件和目录示例：

- 集成式开发环境（IDE）的工作区文件夹
- 本地数据库文件
- 图形仿真应用程序创建的暂存空间文件夹

有关更多信息，请参阅《Amazon Storage Gateway 用户指南》中的文件网关。

为您的 WorkSpaces Pools 用户启用主文件夹

在启用主文件夹之前，您必须执行以下操作：

- 检查您是否具备执行某些 Amazon S3 操作的正确 Amazon Identity and Access Management（IAM）权限。
- 使用根据 2017 年 5 月 18 日当日或之后发布的 Amazon 基本映像创建的某个映像。
- 通过配置 Internet 访问或 Amazon S3 的 VPC 端点，启用从您的虚拟私有云（VPC）到 Amazon S3 的网络连接。有关更多信息，请参阅WorkSpaces Pools 的网络和访问权限和将 Amazon S3 VPC 终端节点用于 WorkSpaces 池功能。

您可以在创建目录时启用或禁用主文件夹（请参阅配置 SAML 2.0 并创建 WorkSpaces 池目录），或在创建目录后使用 WorkSpaces Pools 的 Amazon Web Services 管理控制台 进行启用或禁用。对于每个 Amazon 区域，主文件夹由 Amazon S3 存储桶提供支持。

在您首次为某个 Amazon 区域中的 WorkSpaces Pools 目录启用主文件夹时，服务会在该同一区域内您的账户中创建一个 Amazon S3 存储桶。这个存储桶用于存储该区域中所有用户和所有目录的主文件夹的内容。有关更多信息，请参阅 Amazon S3 存储桶存储。

在创建目录时启用主文件夹

- 按照配置 SAML 2.0 并创建 WorkSpaces 池目录中的步骤操作，并确保选中了 Enable Home Folders (启用主文件夹)。

为现有目录启用主文件夹

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在左侧导航窗格中，选择目录，然后选择要为其启用主文件夹的目录。

3. 在目录列表下方，选择存储并选择启用主文件夹。
4. 在 Enable Home Folders (启用主文件夹) 对话框中，选择 Enable (启用)。

管理您的主文件夹

目录

- 禁用主文件夹
- Amazon S3 存储桶存储
- 主文件夹内容同步
- 主文件夹格式
- 其他资源

禁用主文件夹

您可以禁用目录的主文件夹（已存储在主文件夹中的用户内容不会丢失）。禁用目录的主文件夹会产生以下影响：

- 连接到目录的活动流式传输会话的用户将收到一条错误消息，告知他们无法再将内容存储在其主文件夹中。
- 使用已禁用主文件夹的目录的任何新会话都不会显示主文件夹。
- 为一个目录禁用主文件夹不会为其他目录禁用主文件夹。
- 即使对所有目录禁用了主文件夹，WorkSpaces Pools 也不会删除用户内容。

要还原对目录主文件夹的访问，请按照此主题中前述的步骤重新启用主文件夹。

在创建目录时禁用主文件夹

- 按照配置 SAML 2.0 并创建 WorkSpaces 池目录中的步骤操作，并确保清除了 Enable Home Folders (启用主文件夹) 选项。

为现有目录禁用主文件夹

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在左侧导航窗格中，选择目录，然后选择要为其启用主文件夹的目录。
3. 在目录列表下方，选择存储并清除启用主文件夹。

4. 在 Disable Home Folders (禁用主文件夹) 对话框中，键入 `CONFIRM`（区分大小写）来确认您的选择，然后选择 Disable (禁用)。

Amazon S3 存储桶存储

WorkSpaces Pools 使用在您的账户中创建的 Amazon S3 存储桶来管理存储在主文件夹中的用户内容。对于每个 Amazon 区域，WorkSpaces Pools 都会在您的账户中创建存储桶。从该区域中目录的流式传输会话生成的所有用户内容都存储在该存储桶中。存储桶完全由服务托管，管理员不必输入任何内容或进行任何配置。存储桶以特定格式命名，如下所述：

```
wspool-home-folder-<region-code>-<account-id-without-hyphens>-<random-identifier>
```

其中，*<region-code>* 为创建目录的 Amazon 区域代码，*<account-id-without-hyphens>* 为您的 Amazon Web Services 账户 ID，*>random-identifier<* 为 WorkSpaces 服务生成的随机标识号。存储桶名称的第一部分 `wspool-home-folder-` 不随账户或区域而改变。

例如，如果您为账号 123456789012 在美国西部（俄勒冈州）（us-west-2）区域中的目录启用主文件夹，则此服务会在该区域中创建一个具有所示名称的 Amazon S3 存储桶。只有具有足够权限的管理员才能删除此存储桶。

```
wspool-home-folder-us-west-2-123456789012
```

如上文所述，对目录禁用主文件夹不会删除存储在 Amazon S3 存储桶中的任何用户内容。要永久删除用户内容，必须由具备足够访问权限的管理员在 Amazon S3 控制台中进行。WorkSpaces Pools 添加了一个存储桶策略，以防止意外删除存储桶。

主文件夹内容同步

启用主文件夹后，WorkSpaces Pools 会为每个用户创建一个唯一的文件夹，用于存储其内容。创建该文件夹作为唯一的 Amazon S3 前缀，该前缀使用 Amazon Web Services 账户和区域的 S3 存储桶中的用户名哈希。WorkSpaces Pools 在 Amazon S3 中创建主文件夹后，会将该文件夹中访问的内容从 S3 存储桶复制到 WorkSpace。这使用户能够在流式传输会话期间从 WorkSpace 池中的 WorkSpace 快速访问其主文件夹内容。您对 S3 存储桶中用户主文件夹内容所做的更改，以及用户在 WorkSpace 池中的 WorkSpace 上对其主文件夹内容所做的更改将在 Amazon S3 和 WorkSpaces Pools 之间同步，如下所示。

1. 在用户的 WorkSpaces Pools 流式传输会话开始时，WorkSpaces Pools 会对为该用户存储在您 Amazon Web Services 账户和区域的 Amazon S3 存储桶中的主文件夹文件进行编目。

2. 用户的主文件夹内容还会存储在其流式传输的 WorkSpaces Pools 中的 WorkSpace。当用户访问 WorkSpace 上的主文件夹时，将显示已编目文件列表。
3. 只有当用户在流式传输会话期间使用流应用程序打开文件后，WorkSpaces Pools 才会将文件从 S3 存储桶下载到 WorkSpace。
4. WorkSpaces Pools 将文件下载到 WorkSpace 后，将在访问文件后进行同步
5. 如果用户在流式传输会话期间更改了此文件，则 WorkSpaces Pools 会定期或在流式传输会话结束时将文件的新版本从 WorkSpace 上传到 S3 存储桶。但是，在流式传输会话期间，不会再次从 S3 存储桶下载该文件。

以下各部分介绍了在 Amazon S3 中添加、替换或删除用户的主文件夹文件时的同步行为。

目录

- 同步您添加到 Amazon S3 中用户主文件夹中的文件
- 同步您替换的 Amazon S3 中用户主文件夹中的文件
- 同步您从 Amazon S3 中的用户主文件夹中删除的文件

同步您添加到 Amazon S3 中用户主文件夹中的文件

如果您将新文件添加到 S3 存储桶中用户的主文件夹，则 WorkSpaces Pools 会在几分钟内对该文件进行编目，并将其显示在用户主文件夹中的文件列表中。但是，只有在用户在流式传输会话期间使用应用程序打开文件后，才会将此文件从 S3 存储桶下载到 WorkSpace。

同步您替换的 Amazon S3 中用户主文件夹中的文件

如果用户在流式传输会话期间打开 WorkSpaces Pools 中 WorkSpace 上主文件夹中的文件，并且在该用户处于活动状态的流式传输会话期间，您将 S3 存储桶中其主文件夹中的相同文件替换为新版本，则不会立即将该文件的新版本下载到 WorkSpace。只有在用户启动新的流式传输会话并再次打开文件后，才会将新版本从 S3 存储桶下载到 WorkSpace。

同步您从 Amazon S3 中的用户主文件夹中删除的文件

如果用户在流式传输会话期间打开 WorkSpaces Pools 中 WorkSpace 上主文件夹中的文件，并且在该用户处于活动状态的流式传输会话期间，您将该文件从 S3 存储桶中的主文件夹中删除，则此文件将在用户执行以下任一操作之后从 WorkSpace 中删除：

- 再次打开主文件夹
- 刷新主文件夹

主文件夹格式

用户文件夹的层次结构视用户启动流式传输会话的方式而定，如以下章节所述。

SAML 2.0

对于使用 SAML 联合创建的会话，用户文件夹的结构如下：

```
bucket-name/user/federated/user-id-SHA-256-hash/
```

在本例中，*user-id-SHA-256-hash* 是文件夹名称 (使用在 SAML 联合请求中传递的 NameID SAML 属性值生成的小写 SHA-256 哈希十六进制字符串创建)。要区分隶属两个不同的域的同名用户，请在发送 SAML 请求时使用 NameID 格式的 domainname\username。有关更多信息，请参阅 配置 SAML 2.0 并创建 WorkSpaces 池目录。

下面的示例文件夹结构适用于使用 SAML 联合且 NameID 为 SAMPLEDOMAIN\testuser、账户 ID 为 123456789012、区域为美国西部（俄勒冈）的会话访问：

```
wspool-home-folder-us-west-2-123456789012/user/
federated/8dd9a642f511609454d344d53cb861a71190e44fed2B8aF9fde0C507012a9901
```

当 NameID 字符串的一部分或全部是大写（如示例中的域名 *SAMPLEDOMAIN*）时，WorkSpaces Pools 会根据字符串中使用的大写生成哈希值。使用此示例，SAMPLEDOMAIN\testuser 的哈希值为 8DD9A642F511609454D344D53CB861A71190E44FED2B8AF9FDE0C507012A9901。在该用户的文件夹中，此值显示为小写，如下所示：8dd9a642f511609454d344d53cb861a71190e44fed2B8aF9fde0C507012a9901。

您可以通过网站或网上提供的开源编码库生成 NameID 的 SHA-256 哈希值，并据此确定特定用户的文件夹。

其他资源

有关管理 Amazon S3 存储桶和最佳实践的更多信息，请参阅《Amazon Simple Storage Service 用户指南》中的以下主题：

- 您可以使用 Amazon S3 策略为用户提供对用户数据的离线访问。有关更多信息，请参阅《IAM 用户指南》中的 Amazon S3：允许 IAM 用户以编程方式和在控制台中访问其 S3 主目录。
- 您可以为存储在 WorkSpaces Pools 使用的 Amazon S3 存储桶中的内容启用文件版本控制。有关详细信息，请参阅使用版本控制。

为 WorkSpaces Pools 用户启用应用程序设置持久性。

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

WorkSpaces Pools 支持基于 Windows 的目录的持久性应用程序设置。这意味着，用户的应用程序自定义项和 Windows 设置将在每个流式传输会话之后自动保存，并在下一个会话期间应用。用户可配置的持久性应用程序设置的示例包括但不限于：浏览器收藏夹、设置、网页会话、应用程序连接配置文件、插件和 UI 自定义项。这些设置将保存到您账户在 Amazon 区域内的 Amazon Simple Storage Service（Amazon S3）存储桶中，该存储桶启用了应用程序设置持久性。它们在每个 WorkSpaces Pools 流式传输会话中均可用。

> **Note**
>
> 可能会对存储在 S3 存储桶中的数据收取标准 Amazon S3 费用。有关更多信息，请参阅 Amazon S3 定价。

目录

- 应用程序设置持久性如何工作
- 启用应用程序设置持久性
- 管理用户应用程序设置的 VHD

应用程序设置持久性如何工作

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

持久性应用程序设置将保存到一个虚拟硬盘 (VHD) 文件中。当用户首次从启用了应用程序设置持久性的目录流式传输应用程序时，将创建此文件。如果与该目录关联的 WorkSpace 池所基于的映像包含默认应用程序和 Windows 设置，将对用户的首个流式传输会话使用这些默认设置。

当流式传输会话结束时，VHD 将卸载并上传到您账户的 Amazon S3 存储桶中。首次为 Amazon 区域中的目录启用持久性应用程序设置时，即会创建该存储桶。该存储桶对于您的 Amazon 账户和区域而言是唯一的。VHD 在传输中使用 Amazon S3 SSL 端点进行加密，在静态期间使用 Amazon 托管的 CMK 进行加密。

VHD 将装载到 `C:\Users\%username%` 和 `D:\%username%` 的 WorkSpace 中。如果您的 WorkSpace 未加入 Active Directory 域，则 Windows 用户名是 PhotonUser。如果您的 WorkSpace 已加入 Active Directory 域，则 Windows 用户名为已登录用户的用户名。

应用程序设置持久性无法跨不同的操作系统版本工作。例如，如果为 WorkSpace 池启用应用程序设置持久性且该池使用 Windows Server 2019 映像，则在将 WorkSpace 池更新为使用运行不同的操作系统的映像（例如 Windows Server 2022）时，不会为目录用户保存之前流式传输会话中的设置。相反，在更新 WorkSpace Pools 以使用新映像后，当用户从 WorkSpace 启动流式传输会话时，将创建新的 Windows 用户配置文件。但是，如果对映像上的同一操作系统应用更新，则会保存之前的流式传输会话中的用户自定义项和设置。如果将对同一操作系统的更新应用于映像，则在用户从 WorkSpace 启动流式传输会话时，将使用相同的 Windows 用户配置文件。

> **Important**
>
> WorkSpaces Pools 仅在 WorkSpace 加入 Microsoft Active Directory 域时支持依赖 Microsoft Data Protection API 的应用程序。如果 WorkSpace 未加入 Active Directory 域，则 Windows 用户 PhotonUser 在每个 WorkSpace 上均不同。由于 DPAPI 安全模型的运行方式，用户的密码不会为在此情况下使用 DPAPI 的应用程序保留。如果 WorkSpace 已加入 Active Directory 域并且用户是域用户，则 Windows 用户名为已登录用户的用户名，并且用户的密码将为使用 DPAPI 的应用程序保留。

WorkSpace 池自动将所有文件和文件夹保存在此路径中，但以下文件夹除外：

- 联系人
- 桌面
- Documents
- Downloads
- 链接
- 图片
- Saved Games

- Searches
- 视频

在这些文件夹之外创建的文件和文件夹将保存在 VHD 中并同步到 Amazon S3。对于池，默认 VHD 最大大小为 5 GB。保存的 VHD 的大小是它所包含的文件和文件夹的总大小。WorkSpaces Pools 会自动为用户保存 `HKEY_CURRENT_USER` 注册表配置单元。对于新用户（Amazon S3 中不存在配置文件的用户），WorkSpaces Pools 使用默认配置文件创建初始配置文件。此配置文件是在映像生成器的以下位置创建的：`C:\users\default`。

> **Note**
>
> 整个 VHD 必须先下载到 WorkSpace，然后流式传输会话才能开始。因此，包含大量数据的 VHD 可能会使流式传输会话的开始时间延迟。有关更多信息，请参阅 启用应用程序设置持久性的最佳实践。

启用应用程序设置持久性时，您必须指定一个设置组。设置组确定从这个目录将哪些已保存的应用程序设置用于流式传输会话。WorkSpaces Pools 为设置组创建一个新 VHD 文件，该文件单独存储在您 Amazon 账户的 S3 存储桶中。如果该设置组在各目录之间共享，将在每个目录中使用相同的应用程序设置。如果目录需要自己的应用程序设置，请为目录指定一个唯一的设置组。

启用应用程序设置持久性

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

目录

- 启用应用程序设置持久性的先决条件
- 启用应用程序设置持久性的最佳实践
- 如何启用应用程序设置持久性

启用应用程序设置持久性的先决条件

要启用应用程序设置持久性，您必须先执行以下操作：

- 使用从 Amazon 在 2017 年 12 月 7 日或之后发布的基本映像创建的映像。
- 通过配置 Internet 访问或 Amazon S3 的 VPC 端点，启用从您的虚拟私有云（VPC）到 Amazon S3 的网络连接。有关更多信息，请参阅 WorkSpaces Pools 的网络和访问权限中的主文件夹和 VPC 端点 部分。

启用应用程序设置持久性的最佳实践

要启用应用程序设置持久性而不提供对 WorkSpaces 的 Internet 访问，请使用 VPC 端点。此端点必须位于 WorkSpaces Pools 中 WorkSpaces 所连接到的 VPC 中。您必须附加一个自定义策略才能使 WorkSpaces Pools 能够访问端点。有关如何创建自定义策略的信息，请参阅WorkSpaces Pools 的网络和访问权限中的“主文件夹和 VPC 端点”部分。有关私有 Amazon S3 端点的更多信息，请参阅《Amazon VPC 用户指南》中的 VPC 端点和 Amazon S3 的端点。

如何启用应用程序设置持久性

在创建目录时或创建目录之后，您可以使用 WorkSpaces 控制台启用或禁用应用程序设置持久性。对于每个 Amazon 区域，持久性应用程序设置存储在您账户的 S3 存储桶中。

当您首次为 Amazon 区域中的目录启用应用程序设置持久性时，WorkSpaces Pools 会在 Amazon 账户所在的同一区域中创建一个 S3 存储桶。此存储桶存储该 Amazon 区域中所有用户和所有目录的应用程序设置 VHD 文件。有关更多信息，请参阅管理用户应用程序设置的 VHD中的 Amazon S3 存储桶设置。

在创建目录期间启用应用程序设置持久性

- 按照配置 SAML 2.0 并创建 WorkSpaces 池目录中的步骤操作，并确保选中了 Enable Application Settings Persistence (启用应用程序设置持久性)。

为现有目录启用应用程序设置持久性

1. 打开 WorkSpaces 控制台，网址为：https://console.aws.amazon.com/workspaces/v2/home。
2. 在左侧导航窗格中，选择池，然后选择要为其启用应用程序持久性的池。
3. 在该页面的设置部分，选择编辑。
4. 在该页面的应用程序持久性部分，选择启用应用程序设置持久性。
5. 选择保存更改。

新的流式传输会话现在便已启用应用程序设置持久性。

管理用户应用程序设置的 VHD

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

目录

- Amazon S3 存储桶存储
- 重置用户的应用程序设置
- 启用 Amazon S3 对象版本控制和恢复用户的应用程序设置
- 增加应用程序设置 VHD 的大小

Amazon S3 存储桶存储

启用应用程序设置持久性时，用户的应用程序自定义项和 Windows 设置将自动保存到一个虚拟硬盘（VHD）文件中，该文件存储在您 Amazon 账户中创建的 Amazon S3 存储桶中。对于每个 Amazon 区域，WorkSpaces Pools 会在您的账户中创建一个对于您的账户和该区域而言是唯一的存储桶。用户所配置的所有应用程序设置都将存储在该区域的这个存储桶中。

您不需要执行任何配置任务来管理这些 S3 存储桶；它们完全由 WorkSpaces Pools 服务托管。存储在每个存储桶中的 VHD 文件在传输中使用 Amazon S3 的 SSL 端点进行加密，在静态期间使用 Amazon 托管的 CMK 进行加密。存储桶以特定格式命名，如下所述：

```
wspool-app-settings-<region-code>-<account-id-without-hyphens>-<random-identifier>
```

region-code

这是在其中创建具有应用程序设置持久性的目录的 Amazon 区域代码。

account-id-without-hyphens

您的 Amazon 账户 ID 随机标识符确保与该区域中的其他存储桶不发生冲突。存储桶名称的第一部分 `wspool-app-settings` 不随账户或区域而改变。

例如，如果您为位于美国西部（俄勒冈州）（us-west-2）区域，账号为 123456789012 的目录启用应用程序设置持久性，则 WorkSpaces Pools 会在您账户的该区域中创建一个具有如下所示名称的 Amazon S3 存储桶。只有具有足够权限的管理员才能删除此存储桶。

```
wspool-app-settings-us-west-2-1234567890123-abcdefg
```

禁用应用程序设置持久性不会删除存储在 S3 存储桶中的任何 VHD。要永久删除设置 VHD，您或具备足够权限的管理员必须使用 Amazon S3 控制台或 API 执行此操作。WorkSpaces Pools 添加了一个存储桶策略，以防止意外删除存储桶。

启用应用程序设置持久性后，将为每个设置组创建一个唯一的文件夹来存储设置 VHD。S3 存储桶中该文件夹的层次结构取决于用户启动流式传输会话的方式，如下面一节所述。

存储在您账户的 S3 存储桶中的设置 VHD 所在的文件夹路径使用以下结构：

```
bucket-name/Windows/prefix/settings-group/access-mode/user-id-SHA-256-hash
```

bucket-name

存储用户应用程序设置的 S3 存储桶的名称。该名称格式如本节中前面所述。

###：）

Windows 版本特定的前缀。例如，Windows Server 2012 R2 的 v4。

settings-group

设置组值。此值将应用于共享相同应用程序设置的一个或多个目录。

access-mode

用户的标识方式：`custom` 表示 WorkSpaces Pools API 或 CLI，`federated` 表示 SAML，`userpool` 表示用户池用户。

user-id-SHA-256-hash

用户特定的文件夹名称。此名称是使用从用户 ID 生成的小写 SHA-256 哈希十六进制字符串创建的。

下面的示例文件夹结构应用于一个流式传输会话，将使用用户 ID 为 `testuser@mydomain.com`、Amazon Web Services 账户 ID 为 `123456789012` 的 API 或 CLI 及美国西部（俄勒冈）区域（us-west-2）中的 `test-stack` 设置组访问该会话：

```
wspool-app-settings-us-west-2-1234567890123-abcdefg/Windows/v4/test-stack/custom/
a0bcb1da11f480d9b5b3e90f91243143eac04cfccfbdc777e740fab628a1cd13
```

您可以通过网站或网上提供的开源编码库生成用户 ID 的小写 SHA-256 哈希值，并据此确定特定用户的文件夹。

重置用户的应用程序设置

要重置用户的应用程序设置，您必须从 Amazon 账户中的 S3 存储桶找到并删除 VHD 及关联的元数据文件。请确保在用户的活动流式传输会话期间不执行此操作。在您删除用户的 VHD 文件及元数据文件之后，下次用户从启用了应用程序设置持久性的流实例启动会话时，WorkSpaces Pools 会为该用户创建一个新的设置 VHD。

重置用户的应用程序设置

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Bucket name (存储桶名称) 列表中，选择包含要重置的应用程序设置 VHD 的 S3 存储桶。
3. 找到该 VHD 所在的文件夹。有关如何导航 S3 存储桶文件夹结构的更多信息，请参阅本主题前面的 Amazon S3 存储桶存储。
4. 在 Name (名称) 列表中，选中该 VHD 和 REG 旁的复选框，选择 More (更多)，然后选择 Delete (删除)。
5. 在 Delete objects (删除对象) 对话框中，验证 VHD 和 REG 已列出，然后选择 Delete (删除)。

下次用户从启用了应用程序设置持久性并带有适用设置组的池进行流式传输时，将创建一个新的应用程序设置 VHD。此 VHD 将在会话结束时保存到 S3 存储桶中。

启用 Amazon S3 对象版本控制和恢复用户的应用程序设置

当您的用户更改其应用程序设置时，您可以使用 Amazon S3 对象版本控制和生命周期策略来管理这些设置。通过 Amazon S3 对象版本控制，您可以保留、检索和还原设置 VHD 的每个版本。这使您可以从意外用户操作和应用程序故障进行恢复。如果启用了版本控制，每个流式传输会话之后，应用程序设置 VHD 的新版本将同步到 Amazon S3。新版本不会覆盖早期版本，因此如果您的用户设置发生问题，可以恢复到 VHD 的上一个版本。

> **Note**
>
> 应用程序设置 VHD 的每个版本都将作为一个单独对象保存到 Amazon S3 中，并且需要支付相应费用。

默认情况下在 S3 存储桶中不启用对象版本控制，因此您必须显式启用它。

为应用程序设置 VHD 启用对象版本控制

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Bucket name (存储桶名称) 列表中，选择要启用对象版本控制的应用程序设置 VHD 所在的 S3 存储桶。
3. 选择属性。
4. 依次选择 Versioning (版本控制)、Enable versioning (启用版本控制)，然后选择 Save (保存)。

要终止应用程序设置 VHD 的较旧版本，您可以使用 Amazon S3 生命周期策略。有关信息，请参阅《Amazon Simple Storage Service 用户指南》中的如何为 S3 存储桶创建生命周期策略？

恢复用户的应用程序设置 VHD

通过从适用的 S3 存储桶删除 VHD 的较新版本，您可以恢复到用户应用程序设置 VHD 的早期版本。当用户是否具有活动的流式传输会话时，请不要执行此操作。

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Bucket name (存储桶名称) 列表中，选择要恢复到的用户应用程序设置 VHD 版本所在的 S3 存储桶。
3. 找到并选择该 VHD 所在的文件夹。有关如何导航 S3 存储桶文件夹结构的信息，请参阅本主题前面的 Amazon S3 存储桶存储。

   选择该文件夹时，即会显示设置 VHD 及关联的元数据文件。
4. 要显示 VHD 及元数据文件版本的列表，请选择 Show (显示)。
5. 找到要恢复到的 VHD 版本。
6. 在 Name (名称) 列表中，选中该 VHD 及关联元数据文件的较新版本旁的复选框，选择 More (更多)，然后选择 Delete (删除)。
7. 确认要恢复到的应用程序设置 VHD 及关联的元数据文件是这些文件的最新版本。

下次用户从启用了应用程序设置持久性并带有适用设置组的池进行流式传输时，将显示用户设置的已恢复版本。

增加应用程序设置 VHD 的大小

对于池，默认 VHD 最大大小为 5 GB。如果用户需要额外的应用程序设置空间，您可以将适用的应用程序设置 VHD 下载到 Windows 计算机以对其进行扩展。然后，将 S3 存储桶中的当前 VHD 替换为更大的一个 VHD。当用户是否具有活动的流式传输会话时，请不要执行此操作。

> **Note**
>
> 要减小虚拟硬盘（VHD）的物理大小，请在结束会话之前清除回收站。这还能减少上传和下载时间，并改善整体用户体验。

增加应用程序设置 VHD 的大小

> **Note**
>
> 必须先下载完整 VHD，然后用户才能流式传输应用程序。增加应用程序设置 VHD 的大小可能会增加用户启动应用程序流式传输会话所需的时间。

1. 通过以下网址打开 Amazon S3 控制台：https://console.aws.amazon.com/s3/。
2. 在 Bucket name (存储桶名称) 列表中，选择包含要扩展的应用程序设置 VHD 的 S3 存储桶。
3. 找到并选择该 VHD 所在的文件夹。有关如何导航 S3 存储桶文件夹结构的信息，请参阅本主题前面的 Amazon S3 存储桶存储。

   选择该文件夹时，即会显示设置 VHD 及关联的元数据文件。
4. 将 `Profile.vhdx` 文件下载到 Windows 计算机上的一个目录中。下载完成后，请勿关闭您的浏览器，因为稍后您将再次使用浏览器上传扩展的 VHD。
5. 要使用 Diskpart 将 VHD 的大小增加到 7 GB，请以管理员身份打开命令提示符，并键入以下命令。

   ```
   diskpart
   ```

   ```
   select vdisk file="C:\path\to\application\settings\profile.vhdx"
   ```

   ```
   expand vdisk maximum=7000
   ```
6. 然后，键入以下 Diskpart 命令找到和附加该 VHD，并显示卷列表：

   ```
   elect vdisk file="C:\path\to\application\settings\profile.vhdx"
   ```

   ```
   attach vdisk
   ```

```
list volume
```

在输出中，记下标签为“AwsEucUsers”的卷编号。在下一步中，您将选择此卷，以便可将其扩大。

7. 键入以下命令，其中，*<volume-number>* 是列表卷输出中的编号。

```
select volume <volume-number>
```

8. 键入以下命令：

```
extend
```

9. 键入以下命令，确认 VHD 上该分区的大小是否已按预期增加（在此示例中为 7 GB）：

```
diskpart
```

```
select vdisk file="C:\path\to\application\settings\profile.vhdx"
```

```
list volume
```

10. 键入以下命令分离 VHD，以便可将其上传：

```
detach vdisk
```

11. 返回带有 Amazon S3 控制台的浏览器，依次选择上传、添加文件，然后选择扩大的 VHD。
12. 选择上传。

上传 VHD 后，下次用户从启用了应用程序设置持久性并带有适用设置组的池进行流式传输时，可以使用更大的应用程序设置 VHD。

WorkSpaces Pools 通知代码问题排查

以下是您在设置 Active Directory 并将其与 WorkSpaces 结合使用时可能遇到的域加入问题的通知代码和解决步骤。

DOMAIN_JOIN_ERROR_ACCESS_DENIED

消息：访问被拒绝。

解决方案：在目录中指定的服务账户无权创建计算机对象或重用现有对象。验证权限并启动 WorkSpaces Pools。

DOMAIN_JOIN_ERROR_LOGON_FAILURE

消息：用户名或密码不正确。

解决方案：目录配置中指定的服务账户具有无效的用户名或密码。更新目录中配置的 Amazon Secrets Manager 密钥中的凭证，然后再次启动 WorkSpaces Pools。

DOMAIN_JOIN_NERR_PASSWORD_EXPIRED

消息：此用户的密码已过期。

解决方案：Amazon Secrets Manager 密钥中服务账户的密码已过期。首先，停止 WorkSpaces Pools。接下来，更改在 WorkSpaces 目录中指定的密钥的密码。然后，启动 WorkSpaces Pools。

DOMAIN_JOIN_ERROR_DS_MACHINE_ACCOUNT_QUOTA_EXCEEDED

消息：您的计算机无法加入域。您超出了允许在此域中创建的最大计算机账户数。请联系您的系统管理员重置或增加此限制。

解决方案：在目录上指定的服务账户无权创建计算机对象或重用现有对象。验证权限并启动 WorkSpaces Pools。

DOMAIN_JOIN_ERROR_INVALID_PARAMETER

消息：参数不正确。如果 `LpName` 参数为 NULL 或 `NameType` 参数指定为 `NetSetupUnknown` 或未知名称类型，则会返回此错误。

解决方案：当 OU 的可分辨名称错误时，会发生此错误。验证 OU，然后重试。如果继续遇到此错误，请联系 Amazon Web Services 支持。有关更多信息，请参阅 Amazon Web Services 支持 中心。

DOMAIN_JOIN_ERROR_MORE_DATA

消息：有更多数据可用。

解决方案：当 OU 的可分辨名称错误时，会发生此错误。验证 OU，然后重试。如果继续遇到此错误，请联系 Amazon Web Services 支持。有关更多信息，请参阅 Amazon Web Services 支持 中心。

DOMAIN_JOIN_ERROR_NO_SUCH_DOMAIN

消息：指定域名不存在或无法访问。

解决方案：流实例无法联系您的 Active Directory 域。要确保网络连接，请确认您的 VPC、子网和安全组设置。

DOMAIN_JOIN_NERR_WORKSTATION_NOT_STARTED

消息：工作站服务尚未启动。

解决方案：启动工作站服务时出错。确保该服务已在您的映像中启用。如果继续遇到此错误，请联系 Amazon Web Services 支持。有关更多信息，请参阅 Amazon Web Services 支持 中心。

DOMAIN_JOIN_ERROR_NOT_SUPPORTED

消息：不支持此请求。如果在 `lpServer` 参数中指定了远程计算机而该远程计算机不支持此调用，将返回此错误。

解决方案：联系 Amazon Web Services 支持 以寻求帮助。有关更多信息，请参阅 Amazon Web Services 支持 中心。

DOMAIN_JOIN_ERROR_FILE_NOT_FOUND

消息：系统找不到指定的文件。

解决方案：当提供了无效的组织单位 (OU) 可分辨名称时，会发生此错误。可分辨名称必须以 **OU=** 开头。请验证 OU 可分辨名称并重试。

DOMAIN_JOIN_INTERNAL_SERVICE_ERROR

消息：账户已存在。

解决方法：此错误可能发生在以下情况中：

- 如果问题与权限无关，请查看 Netdom 日志中是否存在错误，并确保您提供的 OU 正确无误。
- 在目录中指定的服务账户无权创建计算机对象或重用现有对象。如果属于这种情况，请验证权限并启动 WorkSpaces Pools。
- WorkSpaces 创建计算机对象后，将从创建它的 OU 中移动该对象。在这种情况下，将成功创建第一个 WorkSpaces Pools，但使用该计算机对象的任何新 WorkSpaces Pools 都将失败。当 Active Directory 在指定 OU 中搜索计算机对象并检测到域中其他位置存在具有相同名称的对象时，域加入将失败。
- 在 WorkSpaces 目录中指定的 OU 名称在目录中的逗号前后包含空格。在这种情况下，当 WorkSpaces Pools 尝试重新加入 Active Directory 域时，WorkSpaces 无法正确循环计算机对象，并且无法成功重新加入域。要解决 WorkSpaces Pools 的此问题，请执行以下操作：

  1. 停止 WorkSpaces Pools。

2. 编辑 WorkSpaces Pools 的 Active Directory 域设置，以删除 WorkSpaces Pools 加入的目录和目录 OU。
3. 更新 WorkSpaces 目录以指定不包含空格的 OU。
4. 编辑 WorkSpaces Pools 的 Active Directory 域设置，使用更新的目录 OU 指定目录。

要解决 WorkSpaces Pools 的此问题，请执行以下操作：

1. 删除 WorkSpaces Pools。
2. 更新 WorkSpaces 目录以指定不包含空格的 OU。
3. 创建新的 WorkSpaces Pools 并使用更新的目录 OU 指定目录。

WORKSPACES_POOL_SESSION_RESERVATION_ERROR

消息：对于与您的 WorkSpaces Pools 关联的子网，我们目前没有足够的容量来容纳可用区 [us-west-1] 中请求的会话。我们的系统将预置额外的容量。同时，请使用以下可用区之一更改或关联不同的子网：[us-west-2、us-west-3]。

解决方案：等待 EC2 有足够的容量或更新目录上其他可用区的子网。

INSUFFICIENT_CAPACITY_ERROR_WORKSPACES_POOL_AZ

消息：我们目前在可用区 [<impacted az>] 中没有足够的容量来容纳所请求的会话。我们的系统将预置额外的容量。同时，请使用其他可用区更改另一个子网或将其关联到您的 WorkSpaces Pools。

解决方案：等待 Amazon EC2 有足够的容量或更新目录上其他可用区的子网。

INVALID_CUSTOMER_SUBNET_CIDR_BLOCK

消息：您的子网包括使用不可用的 CIDR 范围。请在当前 /18 范围之外更新您的子网。

解决方案：等待 EC2 有足够的容量或更新目录上其他可用区的子网。

Amazon WorkSpaces 中的安全性

Amazon 十分重视云安全性。作为 Amazon 客户，您将从专为满足大多数安全敏感型企业的要求而打造的数据中心和网络架构中受益。

安全性是 Amazon 和您的共同责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云安全性 – Amazon 负责保护在 Amazon 云中运行 Amazon 服务的基础结构。Amazon 还向您提供可安全使用的服务。作为Amazon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 Amazon 服务。
- 云中的安全性 - 您的责任由您使用的Amazon服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

此文档将帮助您了解如何在使用 WorkSpaces 时应用责任共担模式。它说明了如何配置 WorkSpaces 以实现您的安全性和合规性目标。您还会了解如何使用其他 Amazon 服务来帮助您监控和保护 WorkSpaces 资源。

目录

- Amazon WorksPaces 中的数据保护
- 的身份和访问管理 WorkSpaces
- Amazon WorkSpaces 的合规性验证
- Amazon WorkSpaces 中的故障恢复能力
- Amazon 的基础设施安全 WorkSpaces
- WorkSpaces 中的更新管理

Amazon WorksPaces 中的数据保护

Amazon责任共担模式适用于 Amazon WorkSpaces 中的数据保护。如该模式中所述，Amazon 负责保护运行所有 Amazon Web Services 云 的全球基础结构。您负责维护对托管在此基础结构上的内容的控制。您还负责您所使用的 Amazon Web Services 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。

出于数据保护目的，建议您保护 Amazon Web Services 账户 凭证并使用 Amazon IAM Identity Center 或 Amazon Identity and Access Management（IAM）设置单个用户。这样，每个用户只获得履行其工作职责所需的权限。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。
- 使用 SSL/TLS 与 Amazon 资源进行通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用 Amazon CloudTrail 设置 API 和用户活动日记账记录。有关使用 CloudTrail 跟踪来捕获 Amazon 活动的信息，请参阅《Amazon CloudTrail 用户指南》中的使用 CloudTrail 跟踪。
- 使用 Amazon 加密解决方案以及 Amazon Web Services 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 中的敏感数据。
- 如果在通过命令行界面或 API 访问 Amazon 时需要经过 FIPS 140-3 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-3 版》。

强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括处理 WorkSpaces 或其他 Amazon Web Services 服务时使用控制台、API、Amazon CLI 或 Amazon SDK。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

静态加密

您可以从 Amazon Key Management Service 使用 Amazon KMS 密钥来加密 WorkSpaces 的存储卷。有关更多信息，请参阅 WorkSpaces 以 WorkSpaces 个人身份加密。

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 通过行业标准的 AES-256 算法，利用数据密钥加密您的卷。有关更多信息，请参阅《Amazon EC2 用户指南》中的 Amazon EBS 加密。

传输中加密

对于 PCoIP，传输中数据使用 TLS 1.2 加密和 SigV4 请求签名进行加密。PCoIP 协议使用带有 AES 加密的加密的 UDP 流量来传输像素。通过端口 4172（TCP 和 UDP）的流连接使用 AES-128 和 AES-256 密码进行加密，但加密默认为 128 位。您可以将此默认值更改为 256 位，方法是：使用适用于 Windows WorkSpaces 的配置 PCoIP 安全设置组策略设置，或修改 Amazon Linux WorkSpaces `pcoip-agent.conf` 文件中的 PCoIP 安全设置。

要详细了解 Amazon WorkSpaces 的组策略管理，请参阅 WorkSpaces 在 WorkSpaces 个人版中管理你的 Windows 中的配置 PCo IP 安全设置。要详细了解如何修改 `pcoip-agent.conf` 文件，请参阅 Teradici 文档中的控制 PCo IP 代理在 Amazon Linux 上的行为 WorkSpaces和 PCoIP 安全设置。

对于 DCV，在流式传输和控制传输中数据时通过 AES-256 加密算法，针对 UDP 流量使用 TLS 1.3 加密技术进行加密，针对 TCP 流量使用 TLS 1.2 加密技术进行加密。

的身份和访问管理 WorkSpaces

默认情况下，IAM 用户没有 WorkSpaces 资源和操作权限。要允许 IAM 用户管理 WorkSpaces 资源，您必须创建明确授予他们权限的 IAM 策略，并将该策略附加到需要这些权限的 IAM 用户或群组。

> **Note**
>
> Amazon WorkSpaces 不支持将 IAM 凭证配置到 WorkSpace（例如使用实例配置文件）。

要提供访问权限，请为您的用户、组或角色添加权限：

- 通过身份提供商在 IAM 中托管的用户：

  创建适用于身份联合验证的角色。按照《IAM 用户指南》中针对第三方身份提供商创建角色（联合身份验证）的说明进行操作。
- IAM 用户：
  - 创建您的用户可以担任的角色。按照《IAM 用户指南》中为 IAM 用户创建角色的说明进行操作。
  - （不推荐使用）将策略直接附加到用户或将用户添加到用户组。按照《IAM 用户指南》中向用户添加权限（控制台）中的说明进行操作。

以下是 IAM 的其他资源：

- 有关 IAM 策略的更多信息，请参阅《IAM 用户指南》中的策略和权限。
- 有关 IAM 的更多信息，请参阅身份和访问管理 (IAM) 和 IAM 用户指南。
- 有关在 IAM 权限策略中使用的 WorkSpaces特定资源、操作和条件上下文密钥的更多信息，请参阅 IA M 用户指南 WorkSpaces中的 A mazon 操作、资源和条件密钥。
- 有关可帮助您创建 IAM 策略的工具，请参阅 Amazon 策略生成器。您还可以使用 IAM Policy Simulator 来测试策略是允许还是拒绝对 Amazon 的特定请求。

内容

- 策略示例
- 在 IAM 策略中指定 WorkSpaces 资源

- 创建工作空间_ 角色 DefaultRole
- 创建 AmazonWorkSpacesPCAAccess 服务角色
- Amazon的托管策略 WorkSpaces
- 对流媒体实例的访问权限 WorkSpaces 和脚本
- Amazon WorkSpaces 控制台操作权限参考

策略示例

> **Important**
>
> “ WorkSpaces 池” 功能不适用于北京和宁夏区域。

以下示例显示了政策声明，您可以使用这些声明来控制 IAM 用户对 Amazon 的权限 WorkSpaces。

示例 1：授予执行 WorkSpaces 个人和矿池任务的访问权限

以下政策声明授予 IAM 用户执行 WorkSpaces个人和池任务的权限。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ds:*",
                "workspaces:*",
                "application-autoscaling:DeleteScalingPolicy",
                "application-autoscaling:DeleteScheduledAction",
                "application-autoscaling:DeregisterScalableTarget",
                "application-autoscaling:DescribeScalableTargets",
                "application-autoscaling:DescribeScalingActivities",
                "application-autoscaling:DescribeScalingPolicies",
                "application-autoscaling:DescribeScheduledActions",
                "application-autoscaling:PutScalingPolicy",
                "application-autoscaling:PutScheduledAction",
                "application-autoscaling:RegisterScalableTarget",
```

```
                "cloudwatch:DeleteAlarms",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:PutMetricAlarm",
                "ec2:AssociateRouteTable",
                "ec2:AttachInternetGateway",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateInternetGateway",
                "ec2:CreateNetworkInterface",
                "ec2:CreateRoute",
                "ec2:CreateRouteTable",
                "ec2:CreateSecurityGroup",
                "ec2:CreateSubnet",
                "ec2:CreateTags",
                "ec2:CreateVpc",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreateRole",
                "iam:GetRole",
                "iam:ListRoles",
                "iam:PutRolePolicy",
                "kms:ListAliases",
                "kms:ListKeys",
                "secretsmanager:ListSecrets",
                "tag:GetResources",
                "sso-directory:SearchUsers",
                "sso:CreateApplication",
                "sso:DeleteApplication",
                "sso:DescribeApplication",
                "sso:DescribeInstance",
                "sso:GetApplicationGrant",
                "sso:ListInstances",
```

```
                "sso:PutApplicationAssignmentConfiguration",
                "sso:PutApplicationAuthenticationMethod",
                "sso:PutApplicationGrant"
            ],
            "Resource": "*"
        },
        {
            "Sid": "iamPassRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "workspaces.amazonaws.com"
                }
            }
        }
    ]
}
```

示例 2：授予执行 WorkSpaces 个人任务的权限

以下政策声明授予 IAM 用户执行所有 WorkSpaces 个人任务的权限。

尽管在使用 API `Action` 和命令行工具时，Amazon WorkSpaces 完全支持和`Resource`元素，但要 WorkSpaces 从中使用 AmazonAmazon Web Services 管理控制台，IAM 用户必须拥有以下操作和资源的权限：

- 行动：`"ds:*"`
- 资源：`"Resource": "*"`

以下示例策略说明如何允许 IAM 用户使用 WorkSpaces 来自的 Amazon Amazon Web Services 管理控制台。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
```

```
        "Effect": "Allow",
        "Action": [
          "workspaces:*",
          "ds:*",
          "iam:GetRole",
          "iam:CreateRole",
          "iam:PutRolePolicy",
          "iam:CreatePolicy",
          "iam:AttachRolePolicy",
          "iam:ListRoles",
          "kms:ListAliases",
          "kms:ListKeys",
          "ec2:CreateVpc",
          "ec2:CreateSubnet",
          "ec2:CreateNetworkInterface",
          "ec2:CreateInternetGateway",
          "ec2:CreateRouteTable",
          "ec2:CreateRoute",
          "ec2:CreateTags",
          "ec2:CreateSecurityGroup",
          "ec2:DescribeInternetGateways",
          "ec2:DescribeSecurityGroups",
          "ec2:DescribeRouteTables",
          "ec2:DescribeVpcs",
          "ec2:DescribeSubnets",
          "ec2:DescribeNetworkInterfaces",
          "ec2:DescribeAvailabilityZones",
          "ec2:AttachInternetGateway",
          "ec2:AssociateRouteTable",
          "ec2:AuthorizeSecurityGroupEgress",
          "ec2:AuthorizeSecurityGroupIngress",
          "ec2:DeleteSecurityGroup",
          "ec2:DeleteNetworkInterface",
          "ec2:RevokeSecurityGroupEgress",
          "ec2:RevokeSecurityGroupIngress",
          "secretsmanager:ListSecrets",
          "sso-directory:SearchUsers",
          "sso:CreateApplication",
          "sso:DeleteApplication",
          "sso:DescribeApplication",
          "sso:DescribeInstance",
          "sso:GetApplicationGrant",
          "sso:ListInstances",
```

```
        "sso:PutApplicationAssignmentConfiguration",
        "sso:PutApplicationAuthenticationMethod",
        "sso:PutApplicationGrant"
      ],
      "Resource": "*"
    },
    {
      "Sid": "iamPassRole",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "workspaces.amazonaws.com"
        }
      }
    }
  ]
}
```

示例 3：授予执行资源 WorkSpaces 池任务的权限

以下政策声明授予 IAM 用户执行所有 P WorkSpaces ools 任务的权限。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "workspaces:*",
                "application-autoscaling:DeleteScalingPolicy",
                "application-autoscaling:DeleteScheduledAction",
                "application-autoscaling:DeregisterScalableTarget",
                "application-autoscaling:DescribeScalableTargets",
                "application-autoscaling:DescribeScalingActivities",
                "application-autoscaling:DescribeScalingPolicies",
                "application-autoscaling:DescribeScheduledActions",
                "application-autoscaling:PutScalingPolicy",
```

```
                "application-autoscaling:PutScheduledAction",
                "application-autoscaling:RegisterScalableTarget",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:PutMetricAlarm",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreateRole",
                "iam:GetRole",
                "iam:ListRoles",
                "iam:PutRolePolicy",
                "secretsmanager:ListSecrets",
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Sid": "iamPassRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "workspaces.amazonaws.com"
                }
            }
        },
        {
            "Action": "iam:CreateServiceLinkedRole",
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/aws-service-
role/workspaces.application-autoscaling.amazonaws.com/
AWSServiceRoleForApplicationAutoScaling_WorkSpacesPool",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "workspaces.application-
autoscaling.amazonaws.com"
```

```
                }
            }
        }
    ]
}
```

示例 4：为 BYO WorkSpaces L 执行所有任务 WorkSpaces

以下政策声明授予 IAM 用户执行所有 WorkSpaces任务的权限，包括创建自带许可证 (BYOL) WorkSpaces 所需的 Amazon EC2 任务。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ds:*",
                "workspaces:*",
                "ec2:AssociateRouteTable",
                "ec2:AttachInternetGateway",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateInternetGateway",
                "ec2:CreateNetworkInterface",
                "ec2:CreateRoute",
                "ec2:CreateRouteTable",
                "ec2:CreateSecurityGroup",
                "ec2:CreateSubnet",
                "ec2:CreateTags",
                "ec2:CreateVpc",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeImages",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
```

```
                "ec2:DescribeVpcs",
                "ec2:ModifyImageAttribute",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "iam:CreateRole",
                "iam:GetRole",
                "iam:PutRolePolicy",
                "kms:ListAliases",
                "kms:ListKeys"
            ],
            "Resource": "*"
        },
        {
            "Sid": "iamPassRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "workspaces.amazonaws.com"
                }
            }
        }
    ]
}
```

在 IAM 策略中指定 WorkSpaces 资源

要在政策声明的`Resource`元素中指定 WorkSpaces 资源，请使用该资源的 Amazon 资源名称 (ARN)。您可以通过允许或拒绝使用您的 IAM 策略声明`Action`元素中指定的 API 操作来控制对 WorkSpaces 资源的访问权限。 WorkSpaces 定义 ARNs 分发包 WorkSpaces、IP 组和目录。

WorkSpace ARN

WorkSpace ARN 的语法如下例所示。

```
arn:aws:workspaces:region:account_id:workspace/workspace_identifier
```

区域

所在 WorkSpace 的区域（例如，`us-east-1`）。

account_id

Amazon账户的 ID，不带连字符（例如，`123456789012`）。

workspace_identifier

的 ID WorkSpace （例如，`ws-a1bcd2efg`）。

以下是标识特定`Resource`内容的策略声明元素的格式 WorkSpace。

```
"Resource": "arn:aws:workspaces:region:account_id:workspace/workspace_identifier"
```

您可以使用*通配符指定 WorkSpaces 属于特定区域中特定账户的所有账户。

WorkSpace 池 ARN

WorkSpace 池 ARN 的语法如下例所示。

```
arn:aws:workspaces:region:account_id:workspacespool/workspacespool_identifier
```

区域

所在 WorkSpace 的区域（例如，`us-east-1`）。

account_id

Amazon账户的 ID，不带连字符（例如，`123456789012`）。

workspacespool_identifier

WorkSpace 池的 ID（例如，`ws-a1bcd2efg`）。

以下是标识特定`Resource`内容的策略声明元素的格式 WorkSpace。

```
"Resource":
 "arn:aws:workspaces:region:account_id:workspacespool/workspacespool_identifier"
```

您可以使用*通配符指定 WorkSpaces 属于特定区域中特定账户的所有账户。

ARN 证书

WorkSpace 证书 ARN 的语法如下例所示。

```
arn:aws:workspaces:region:account_id:workspacecertificate/
workspacecertificateidentifier
```

区域

所在 WorkSpace 的区域（例如，`us-east-1`）。

account_id

Amazon账户的 ID，不带连字符（例如，`123456789012`）。

workspacecertificate_identifier

WorkSpace 证书的 ID（例如，`ws-a1bcd2efg`）。

以下是标识特定 WorkSpace 证书的策略声明`Resource`元素的格式。

```
"Resource":
 "arn:aws:workspaces:region:account_id:workspacecertificate/
workspacecertificate_identifier"
```

您可以使用*通配符指定 WorkSpaces 属于特定区域中特定账户的所有账户。

映像 ARN

WorkSpace 图片 ARN 的语法如下例所示。

```
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

Amazon账户的 ID，不带连字符（例如，`123456789012`）。

bundle_identifier

WorkSpace 图像的 ID（例如，`wsi-a1bcd2efg`）。

以下是用于标识某个特定映像的策略语句的 `Resource` 元素的格式。

```
"Resource": "arn:aws:workspaces:region:account_id:workspaceimage/image_identifier"
```

您可以使用 * 通配符来指定属于特定区域中特定账户的所有映像。

服务包 ARN

服务包 ARN 具有以下示例中显示的语法。

```
arn:aws:workspaces:region:account_id:workspacebundle/bundle_identifier
```

区域

所在 WorkSpace 的区域（例如，us-east-1）。

account_id

Amazon账户的 ID，不带连字符（例如，123456789012）。

bundle_identifier

WorkSpace 捆绑包的 ID（例如，wsb-a1bcd2efg）。

以下是用于标识某个特定服务包的策略语句的 Resource 元素的格式。

```
"Resource": "arn:aws:workspaces:region:account_id:workspacebundle/bundle_identifier"
```

您可以使用 * 通配符来指定属于特定区域中特定账户的所有捆绑包。

IP 组 ARN

IP 组 ARN 具有以下示例中显示的语法。

```
arn:aws:workspaces:region:account_id:workspaceipgroup/ipgroup_identifier
```

区域

所在 WorkSpace 的区域（例如，us-east-1）。

account_id

Amazon账户的 ID，不带连字符（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

所在 WorkSpace 的区域（例如，`us-east-1`）。

account_id

Amazon账户的 ID，不带连字符（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

Amazon账户的 ID，不带连字符（例如，123456789012）。

connectionalias_identifier

连接别名的 ID（例如，wsca-12345a67b8）。

以下是用于标识某个特定连接别名的策略语句的 Resource 元素的格式。

```
"Resource":
 "arn:aws:workspaces:region:account_id:connectionalias/connectionalias_identifier"
```

您可以使用 * 通配符来指定属于特定区域中特定账户的所有连接别名。

不支持资源级权限的 API 操作

您不能使用以下 API 操作指定资源 ARN：

- AssociateIpGroups
- CreateIpGroup
- CreateTags
- DeleteTags
- DeleteWorkspaceImage
- DescribeAccount
- DescribeAccountModifications
- DescribeIpGroups
- DescribeTags
- DescribeWorkspaceDirectories
- DescribeWorkspaceImages
- DescribeWorkspaces
- DescribeWorkspacesConnectionStatus
- DisassociateIpGroups

- `ImportWorkspaceImage`
- `ListAvailableManagementCidrRanges`
- `ModifyAccount`

对于不支持资源级权限的 API 操作，必须指定以下示例中显示的资源语句。

```
"Resource": "*"
```

不支持对共享资源进行账号级限制的 API 操作

对于以下 API 操作，当资源不归账户所有时，您无法在资源 ARN 中指定账户 ID：

- `AssociateConnectionAlias`
- `CopyWorkspaceImage`
- `DisassociateConnectionAlias`

对于这些 API 操作，只有当该账户拥有要处理的资源时，您才能在资源 ARN 中指定账户 ID。当账户不拥有资源时，您必须为账户 ID 指定 `*`，如以下示例中所示。

```
"arn:aws:workspaces:region:*:resource_type/resource_identifier"
```

创建工作空间_ 角色 DefaultRole

在使用 API 注册目录之前，必须验证名为 `workspaces_DefaultRole` 的角色是否存在。此角色由快速设置创建，或者您 WorkSpace 使用启动时创建Amazon Web Services 管理控制台，它会向 Amazon 授予代表您访问特定Amazon资源的 WorkSpaces 权限。如果此角色不存在，您可以使用以下程序创建它。

创建 workspaces_ 角色 DefaultRole

1. 登录Amazon Web Services 管理控制台并打开 IAM 控制台，网址为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. 在选择受信任实体的类型下，选择其他 Amazon 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. 选择下一步: 权限。
8. 在附加权限策略页面上，选择Amazon托管策略AmazonWorkSpacesServiceAccessAmazonWorkSpacesSelfServiceAccess、和AmazonWorkSpacesPoolServiceAccess。有关这些托管策略的更多信息，请参阅Amazon的托管策略 WorkSpaces。
9. 在设置权限边界下，建议您不要使用权限边界，因为可能会与附加到此角色的策略发生冲突。此类冲突可能会阻止角色的某些必要权限。
10. 选择下一步：标签。
11. 在 Add tags (optional) (添加标签(可选)) 页面上，根据需要添加标签。
12. 选择下一步：审核。
13. 在审核页面上，对于角色名称，输入 **workspaces_DefaultRole**。
14. （可选）对于角色描述，请输入描述。
15. 选择创建角色。
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. 选择更新信任策略。

创建 AmazonWorkSpacesPCAAccess 服务角色

在用户使用基于证书的身份验证方式登录之前，您必须先验证名为 `AmazonWorkSpacesPCAAccess` 的角色是否存在。此角色是在您使用对目录启用基于证书的身份验证时创建的Amazon Web Services

管理控制台，它授予 Amazon 代表您访问Amazon 私有 CA资源的 WorkSpaces权限。如果由于您未使用控制台管理基于证书的身份验证而导致此角色不存在，则您可以使用以下步骤创建此角色。

要创建 AmazonWorkSpacesPCAAccess 服务角色，请使用 Amazon CLI

1. 使用以下文本创建名为 `AmazonWorkSpacesPCAAccess.json` 的 JSON 文件。

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "prod.euc.ecm.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

2. 根据需要调整`AmazonWorkSpacesPCAAccess.json`路径并运行以下Amazon CLI命令来创建服务角色并附加AmazonWorkspacesPCAAccess托管策略。

```
aws iam create-role --path /service-role/ --role-name AmazonWorkSpacesPCAAccess --
assume-role-policy-document file://AmazonWorkSpacesPCAAccess.json
```

```
aws iam attach-role-policy –role-name AmazonWorkSpacesPCAAccess –policy-arn
 arn:aws:iam::aws:policy/AmazonWorkspacesPCAAccess
```

Amazon的托管策略 WorkSpaces

与自己编写策略相比，使用Amazon托管策略可以更轻松地向用户、群组和角色添加权限。创建仅为团队提供所需权限的 IAM 客户托管策略需要时间和专业知识。使用Amazon托管策略快速入门。这些政策涵盖常见用例，可在您的Amazon账户中使用。有关Amazon托管策略的更多信息，请参阅 IAM 用户指南中的Amazon托管策略。

Amazon服务维护和更新Amazon托管策略。您无法更改Amazon托管策略中的权限。服务偶尔可能会向Amazon托管策略添加其他权限以支持新功能。此类更新会影响附加策略的所有身份（用户、组和角色）。当推出新功能或有新操作可用时，服务最有可能更新Amazon托管策略。服务不会从Amazon托管策略中移除权限，因此策略更新不会破坏您的现有权限。

此外，还Amazon支持跨多个服务的工作职能的托管策略。例如，`ReadOnlyAccess`Amazon托管策略提供对所有Amazon服务和资源的只读访问权限。当服务启动新特征时，Amazon 会为新操作和资源添加只读权限。有关工作职能策略的列表和说明，请参阅 IAM 用户指南中的适用于工作职能的 Amazon 托管式策略。

Amazon托管策略： AmazonWorkSpacesAdmin

> **Note**
>
> 列出的权限仅适用于 SDK，不适用于控制台。控制台需要 Amazon WorkSpaces 控制台操作权限参考中列出的其他权限。

该政策允许访问Amazon的 WorkSpaces 管理操作。它提供以下权限：

- `workspaces`-允许访问对 WorkSpaces 个人资源和资源 WorkSpaces 池资源执行管理操作。
- `kms` - 允许访问列出和描述 KMS 密钥以及列出别名。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonWorkSpacesAdmin",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:ListAliases",
                "kms:ListKeys",
                "workspaces:CreateTags",
                "workspaces:CreateWorkspaceImage",
                "workspaces:CreateWorkspaces",
                "workspaces:CreateWorkspacesPool",
```

```
                "workspaces:CreateStandbyWorkspaces",
                "workspaces:DeleteTags",
                "workspaces:DeregisterWorkspaceDirectory",
                "workspaces:DescribeTags",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaces",
                "workspaces:DescribeWorkspacesPools",
                "workspaces:DescribeWorkspacesPoolSessions",
                "workspaces:DescribeWorkspacesConnectionStatus",
                "workspaces:ModifyCertificateBasedAuthProperties",
                "workspaces:ModifySamlProperties",
                "workspaces:ModifyStreamingProperties",
                "workspaces:ModifyWorkspaceCreationProperties",
                "workspaces:ModifyWorkspaceProperties",
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces",
                "workspaces:RegisterWorkspaceDirectory",
                "workspaces:RestoreWorkspace",
                "workspaces:StartWorkspaces",
                "workspaces:StartWorkspacesPool",
                "workspaces:StopWorkspaces",
                "workspaces:StopWorkspacesPool",
                "workspaces:TerminateWorkspaces",
                "workspaces:TerminateWorkspacesPool",
                "workspaces:TerminateWorkspacesPoolSession",
                "workspaces:UpdateWorkspacesPool"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon托管策略： AmazonWorkspacesPCAAccess

此托管策略允许访问您Amazon账户中的 Certifice Manager 私有证书颁发机构（私有 CA）资源，以进行基于证书的身份验证。Amazon它包含在 AmazonWorkSpacesPCAAccess 角色中，并提供以下权限：

- `acm-pca`-允许访问Amazon私有 CA 以管理基于证书的身份验证。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "acm-pca:IssueCertificate",
                "acm-pca:GetCertificate",
                "acm-pca:DescribeCertificateAuthority"
            ],
            "Resource": "arn:*:acm-pca:*:*:*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/euc-private-ca": "*"
                }
            }
        }
    ]
}
```

Amazon托管策略： AmazonWorkSpacesSelfServiceAccess

该政策允许用户访问 Amazon WorkSpaces 服务，以执行由用户发起的 WorkSpaces 自助操作。它包含在 `workspaces_DefaultRole` 角色中，它提供以下权限：

- `workspaces`-允许用户访问自助 WorkSpaces 管理功能。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "workspaces:RebootWorkspaces",
                "workspaces:RebuildWorkspaces",
                "workspaces:ModifyWorkspaceProperties"
```

```
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Amazon托管策略： AmazonWorkSpacesServiceAccess

本政策允许客户账户访问亚马逊 WorkSpaces 服务，以启动 WorkSpace。它包含在 `workspaces_DefaultRole` 角色中，它提供以下权限：

- `ec2`-允许访问管理与关联的 Amazon EC2 资源 WorkSpace，例如网络接口。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeNetworkInterfaces"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Amazon托管策略： AmazonWorkSpacesPoolServiceAccess

> **Important**
>
> “ WorkSpaces 池” 功能不适用于北京和宁夏区域。

此策略用于 workspaces_DefaultRole，它 WorkSpaces 用于访问客户Amazon账户中必需的 Pools 资源。 WorkSpaces 有关更多信息，请参阅 创建工作空间_ 角色 DefaultRole 。它提供以下权限：

- ec2-允许访问管理与 WorkSpaces 池关联的 Amazon EC2 资源 VPCs，例如子网、可用区、安全组和路由表。
- s3 - 允许访问权限以对日志、应用程序设置和主文件夹功能所需的 Amazon S3 存储桶执行操作。

CommercialAmazon Web Services 区域

以下政策 JSON 适用于广告Amazon Web Services 区域。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ProvisioningWorkSpacesPoolPermissions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeRouteTables",
                "s3:ListAllMyBuckets"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "WorkSpacesPoolS3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:GetObject",
```

```
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:GetObjectVersion",
                "s3:DeleteObjectVersion",
                "s3:GetBucketPolicy",
                "s3:PutBucketPolicy",
                "s3:PutEncryptionConfiguration"
            ],
            "Resource": [
                "arn:aws:s3:::wspool-logs-*",
                "arn:aws:s3:::wspool-app-settings-*",
                "arn:aws:s3:::wspool-home-folder-*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        }
    ]
}
```

Amazon GovCloud (US) Regions

以下策略 JSON 适用于商业 Amazon GovCloud (US) Regions。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ProvisioningWorkSpacesPoolPermissions",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeRouteTables",
                "s3:ListAllMyBuckets"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "WorkSpacesPoolS3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:GetObjectVersion",
                "s3:DeleteObjectVersion",
                "s3:GetBucketPolicy",
                "s3:PutBucketPolicy",
                "s3:PutEncryptionConfiguration"
            ],
            "Resource": [
                "arn:aws-us-gov:s3:::wspool-logs-*",
                "arn:aws-us-gov:s3:::wspool-app-settings-*",
                "arn:aws-us-gov:s3:::wspool-home-folder-*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        }
    ]
}
```

WorkSpaces Amazon托管策略的更新

查看 WorkSpaces 自该服务开始跟踪这些更改以来Amazon托管策略更新的详细信息。

更改	描述	日期
the section called “AmazonWorkSpacesPoolServiceAcces” - 添加了新策略	WorkSpaces 添加了新的托管策略，以授予查看亚马逊 EC2 VPCs 和相关资源以及查看和管理 WorkSpaces 池的 Amazon S3 存储桶的权限。	2024 年 6 月 24 日
the section called “AmazonWorkSpacesAdmin”：更新策略	WorkSpaces 在 Amazon WorkSpacesAdmin 托管策略中为 WorkSpaces 池添加了多项操作，授予管理员管理 WorkSpace 池资源的权限。	2024 年 6 月 24 日
the section called “AmazonWorkSpacesAdmin”：更新策略	WorkSpaces 将`workspaces:RestoreWorkspace` 操作添加到 Amazon WorkSpacesAdmin 托管策略中，授予管理员恢复 WorkSpaces权限。	2023 年 6 月 25 日
the section called “AmazonWorkspacesPCAAccess” - 添加了新策略	WorkSpaces 添加了一个新的托管策略，用于授予管理 Amazon私有 CA 以管理基于证书的身份验证的`acm-pca`权限。	2022 年 11 月 18 日
WorkSpaces 已开始跟踪更改	WorkSpaces 开始跟踪其 WorkSpaces 托管策略的更改。	2021 年 3 月 1 日

对流媒体实例的访问权限 WorkSpaces 和脚本

在 WorkSpaces 流媒体实例上运行的应用程序和脚本必须在 Amazon API 请求中包含Amazon凭据。您可以创建一个 IAM 角色来管理这些凭证。IAM 角色指定了一组可用于访问Amazon资源的权限。但是，此角色并非与一个人唯一关联。相反，任何需要它的人都可以代入该角色。

您可以将 IAM 角色应用于 WorkSpaces 流媒体实例。当流实例切换到（代入）角色时，该角色提供临时安全凭证。您的应用程序或脚本使用这些凭据在流媒体实例上执行 API 操作和管理任务。WorkSpaces 为您管理临时凭证切换。

内容

- 将 IAM 角色与 WorkSpaces 流媒体实例配合使用的最佳实践
- 配置现有 IAM 角色以用于 WorkSpaces 流式处理实例
- 如何创建用于 WorkSpaces 流媒体实例的 IAM 角色
- 如何将 IAM 角色用于 WorkSpaces 流式处理实例

将 IAM 角色与 WorkSpaces 流媒体实例配合使用的最佳实践

当您将 IAM 角色用于 WorkSpaces 流式处理实例时，我们建议您遵循以下做法：

- 限制您授予 Amazon API 操作和资源的权限。

  在创建 IAM 策略并将其附加到与 WorkSpaces 流媒体实例关联的 IAM 角色时，请遵循最低权限原则。当您使用需要访问 Amazon API 操作或资源的应用程序或脚本时，请确定所需的特定操作和资源。然后，创建允许应用程序或脚本仅执行这些操作的策略。有关更多信息，请参阅 IAM 用户指南中的授予最低权限。
- 为每个 WorkSpaces 资源创建一个 IAM 角色。

  为每个 WorkSpaces 资源创建唯一的 IAM 角色是一种遵循最低权限原则的做法。这样做还允许您修改一个资源的权限，而不会影响其他资源。
- 限制可以使用凭证的位置。

  通过 IAM 策略，您可以定义可使用 IAM 角色访问资源的条件。例如，您可以包含条件以指定请求可以来自的 IP 地址范围。这样做可以防止在您的环境之外使用凭证。有关更多信息，请参阅《IAM 用户指南》中的使用策略条件来增强安全性。

配置现有 IAM 角色以用于 WorkSpaces 流式处理实例

本主题介绍如何配置现有 IAM 角色以便您可以将其与一起使用 WorkSpaces 。

先决条件

要与之配合使用的 IAM 角色 WorkSpaces 必须满足以下先决条件：

- IAM 角色必须与 WorkSpaces 流媒体实例位于同一个亚马逊 Web Services 账户中。
- IAM 角色不能是服务角色。
- 附加到 IAM 角色的信任关系策略必须将 WorkSpaces 服务作为委托人。委托人是Amazon可以执行操作和访问资源的实体。该策略还必须包括 `sts:AssumeRole` 操作。此策略配置定义 WorkSpaces 为可信实体。

- 如果您要将 IAM 角色应用于 WorkSpaces，则 WorkSpaces 必须运行在 2019 年 9 月 3 日当天或之后发布的 WorkSpaces 代理版本。如果您要将 IAM 角色应用于 WorkSpaces，则 WorkSpaces 必须使用使用在同一日期或之后发布的代理版本的映像。

使 WorkSpaces 服务委托人能够担任现有 IAM 角色

要执行以下步骤，您必须以具有列出和更新 IAM 角色所需权限的 IAM 用户身份登录账户。如果您没有所需的权限，则要求您的 Amazon Web Services 账户管理员在您的账户中执行这些步骤或授予您所需权限。

1. 使用 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 在导航窗格中，选择角色。
3. 在您的账户的角色列表中，选择要修改的角色的名称。
4. 选择 信任关系 选项卡，然后选择 编辑信任关系。
5. 在策略文档下，验证信任关系策略是否包含 `workspaces.amazonaws.com` 服务主体的 `sts:AssumeRole` 操作：

   JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "workspaces.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
```

```
}
```

6. 在编辑完信任策略后，请选择更新信任策略以保存所做更改。
7. 您选择的 IAM 角色将显示在 WorkSpaces 控制台中。此角色授予对应用程序和脚本的权限，以便在流实例上执行 API 操作和管理任务。

如何创建用于 WorkSpaces 流媒体实例的 IAM 角色

本主题介绍如何创建新的 IAM 角色以便您可以将其用于 WorkSpaces

1. 使用 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 在导航窗格中，选择角色，然后选择创建角色。
3. 对于Select type of trusted entity（选择受信任实体的类型），选择 Amazon service（服务）。
4. 从Amazon服务列表中选择WorkSpaces。
5. 在 “选择您的用例” 下，WorkSpaces “允许 WorkSpaces 实例代表您调用Amazon服务” 已选中。选择下一步: 权限。
6. 如果可能，选择要用作权限策略的策略，或选择 Create policy（创建策略）以打开新的浏览器选项卡并从头开始创建新策略。有关更多信息，请参阅《IAM 用户指南》中创建 IAM 策略（控制台）过程的步骤 4。

   在您创建策略后，关闭该选项卡并返回到您的原始选项卡。选中要拥有的权限策略旁边的复选框。WorkSpaces
7. （可选）设置权限边界。这是一项高级功能，可用于服务角色，但不可用于服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的 IAM 实体的权限边界。
8. 选择下一步：标签。您可以选择附加标签作为键值对。有关更多信息，请参阅《IAM 用户指南》中的标记 IAM 用户和角色。
9. 选择下一步：审核。
10. 对于角色名称，请键入在 Amazon Web Services 账户中唯一的角色名称。由于其他Amazon资源可能会引用该角色，因此您无法在角色创建后对其名称进行编辑。
11. 对于 Role description (角色描述)，请保留默认角色描述或键入新角色描述。
12. 检查该角色，然后选择创建角色。

如何将 IAM 角色用于 WorkSpaces 流式处理实例

创建 IAM 角色后，您可以在启动 WorkSpaces 时将其应用于该角色 WorkSpaces。您也可以将 IAM 角色应用于现有角色 WorkSpaces。

当您向应用 IAM 角色时 WorkSpaces，会 WorkSpaces 检索临时证书并在实例上创建 workspaces_machine_role 凭证配置文件。临时凭证有效期为 1 小时，每小时检索一次新凭证。以前的凭证不会过期，因此只要它们有效，您就可以使用它们。您可以使用您选择的语言使用Amazon命令行界面 (CL Amazon I)、Amazon工具或 Amazon SDK，以编程方式使用凭证配置文件来调用Amazon服务。 PowerShell

当您进行 API 调用时，请将 workspaces_machine_role 指定为凭证配置文件。否则，由于权限不足，操作将失败。

WorkSpaces 在预配置流媒体实例时担任指定角色。由于 WorkSpaces 使用连接到 VPC 的弹性网络接口进行 Amazon API 调用，因此您的应用程序或脚本必须等待弹性网络接口可用后才能进行 Amazon API 调用。如果在弹性网络接口可用之前进行 API 调用，则调用将失败。

以下示例显示了如何使用 workspaces_machine_ role 凭据配置文件来描述流媒体实例（实EC2 例）和创建 Boto 客户端。Boto 是适用于 Python 的 Amazon Web Services（Amazon）SDK。

使用 Amazon CLI 描述流式处理EC2 实例（实例）

```
aws ec2 describe-instances --region us-east-1 --profile workspaces_machine_role
```

使用以下Amazon工具描述流式处理EC2 实例（实例） PowerShell

您必须使用适用于 3.3.563.1 或更高 PowerShell 版本的Amazon工具，以及适用于.NET 的 Amazon Web Services SDK 版本 3.3.103.22 或更高版本。[您可以从 PowerShell网站的Amazon工具中下载适用于 Windows 的工具安装程序，其中包括适用于.NET 的Amazon工具 PowerShell 和适用于.NET 的 Amazon Web Ser Amazon vices SDK。]

```
Get-EC2Instance -Region us-east-1 -ProfileName workspaces_machine_role
```

使用适用于 Python 的Amazon软件开发工具包创建 Boto 客户端

```
session = boto3.Session(profile_name=workspaces_machine_role')
```

Amazon WorkSpaces 控制台操作权限参考

某些 Amazon WorkSpaces API 只能通过 Amazon 管理控制台进行调用。它们不是公共 API，无法以编程方式调用，也未由任何 SDK 提供。这些 API 操作包括：

- workspaces:DirectoryAccessManagement
- workspaces:CreateRootClientCertificate
- workspaces:UpdateRootClientCertificate
- workspaces:DeleteRootClientCertificate
- workspaces:DescribeConsent
- workspaces:UpdateConsent

WorkSpaces 控制台操作和必需的操作权限

控制台使用额外 API 操作实现其功能，因此 WorkSpaces 公共 API 可能没有足够的权限。例如，有权通过 CLI/SDK 使用 CreateWorkspaces API 的用户在尝试在控制台上创建 WorkSpace 时可能会遇到错误，因为他们缺少选择或创建用户的某些权限。下表列出了仅在 WorkSpaces 控制台上可用的功能，以及允许用户使用控制台的这些特定部分所需的额外权限。

策略示例部分提供了对 Personal、Pools 和 BYOL WorkSpaces 执行所有 WorkSpaces 任务所需的权限列表。

或者，您也可以使用精细许可，应用最低权限许可来执行某项任务。

下表列出了依赖于 SDK 未提供的 API 的 WorkSpaces 控制台功能，以及允许用户使用控制台的这些特定部分所需的权限。这些是除了 SDK 提供的 API 所需的其他操作外还应添加的权限。

WorkSpaces 控制台操作	所需的权限
WorkSpaces 个人版快速设置	workspaces:DirectoryAccessManagement ds:* ec2:CreateVpc ec2:CreateSubnet ec2:CreateNetworkInterface

WorkSpaces 控制台操作	所需的权限
	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:AuthorizeSecurityGroupIngress ec2:AuthorizeSecurityGroupEgress iam:CreateRole iam:GetRole iam:PutRolePolicy workspaces:DescribeAccount workspaces:DescribeWorkspaceDirectories

WorkSpaces 控制台操作	所需的权限
	workspaces:CreateWorkspaces workspaces:DescribeWorkspaces workspaces:RegisterWorkspaceDirectory workspaces:DescribeWorkspaceBundles workspaces:DescribeWorkspaces
将 WorkSpaces 个人版访问限定于受信任设备	workspaces:CreateRootClientCertificate workspaces:UpdateRootClientCertificate workspaces:DeleteRootClientCertificate ds:DescribeDirectories ec2:DescribeSubnets ec2:DescribeSecurityGroups workspaces:DescribeAccount workspaces:DescribeWorkspaceDirectories workspaces:DescribeTags workspaces:DescribeClientProperties workspaces:DescribeConnectClientAddins workspaces:DirectoryAccessManagement

WorkSpaces 控制台操作	所需的权限
在 WorkSpaces Personal 控制台中创建 WorkSpace – create/search/describe 目录服务目录用户	workspaces:DirectoryAccessManagement workspaces:DescribeAccount workspaces:CreateWorkspaces workspaces:DescribeWorkspaces workspaces:DescribeWorkspaceDirectories workspaces:DescribeWorkspaceBundles workspaces:DescribeTags workspaces:CreateTags workspaces:DescribeClientProperties kms:ListKeys kms:ListAliases kms:DescribeKey ds:DescribeTrusts ds:DescribeDirectories ec2:DescribeSubnets ec2:DescribeSecurityGroups

WorkSpaces 控制台操作	所需的权限
在 WorkSpaces Personal 中管理用户 – 编辑用户并向用户发送邀请电子邮件	workspaces:DirectoryAccessManagement workspaces:DescribeAccount workspaces:DescribeWorkspaceDirectories workspaces:DescribeWorkspaces workspaces:DescribeTags workspaces:DescribeWorkspaceBundles workspaces:DescribeWorkspacesConnectionStatus workspaces:DescribeWorkspaceAssociations workspaces:DescribeWorkspaceSnapshots workspaces:DescribeWorkspaceImages workspaces:DescribeConnectionAliases

WorkSpaces 控制台操作	所需的权限
更新 WorkSpaces 个人版的 AD Connector 账户（AD Connector	workspaces:DirectoryAccessManagement ds:DescribeDirectories ds:UpdateDirectory ec2:DescribeSubnets ec2:DescribeSecurityGroups workspaces:DescribeAccount workspaces:DescribeWorkspaceDirectories workspaces:DescribeTags workspaces:DescribeClientProperties workspaces:DescribeConnectClientAddins
为 WorkSpaces 个人版选择组织部门	workspaces:DirectoryAccessManagement ds:DescribeDirectories ec2:DescribeSubnets ec2:DescribeSecurityGroups workspaces:DescribeAccount workspaces:DescribeWorkspaceDirectories workspaces:DescribeTags workspaces:DescribeClientProperties workspaces:DescribeConnectClientAddins workspaces:ModifyWorkspaceCreationProperties

WorkSpaces 控制台操作	所需的权限
启用 BYOL 账户 – 确认了解使用 BYOL WorkSpaces 的要求	workspaces:DescribeConsent workspaces:UpdateConsent workspaces:DescribeAccount workspaces:ListAccountLinks workspaces:DescribeWorkspaceBundles workspaces:DescribeWorkspaceImages workspaces:DescribeWorkspaceDirectories

Amazon WorkSpaces 的合规性验证

作为多项 Amazon 合规性计划的一部分，第三方审计员将评估 Amazon WorkSpaces 的安全性和合规性。其中包括 SOC、PCI、FedRAMP、HIPAA 及其他。

有关特定合规性计划范围内的 Amazon 服务列表，请参阅合规性计划范围内的 Amazon 服务。有关常规信息，请参阅Amazon合规性计划。

您可以使用 Amazon Artifact 下载第三方审计报告。有关更多信息，请参阅、在 Amazon Artifact 中下载报告。

您使用 WorkSpaces 的合规性责任取决于您数据的敏感度、您公司的合规性目标以及适用的法律法规。Amazon 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Amazon上部署基于安全性和合规性的基准环境的步骤。
- Amazon Web Services 上的 HIPAA 安全性和合规性架构设计– 此白皮书介绍了公司如何使用 Amazon 创建符合 HIPAA 标准的应用程序。
- Amazon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。
- 《Amazon Config 开发人员指南》中的使用规则评估资源 – Amazon Config；评测您的资源配置对内部实践、行业指南和法规的遵循情况。
- Amazon Security Hub CSPM – 此Amazon服务提供了Amazon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操。

Amazon WorkSpaces 中的故障恢复能力

Amazon 全球基础设施围绕 Amazon 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、容错能力和可扩展性。

有关 Amazon 区域和可用区的更多信息，请参阅 Amazon全球基础设施。

Amazon WorkSpaces 还提供跨区域重定向，该功能可与域名系统 (DNS) 故障转移路由策略配合使用，以便在 WorkSpaces 用户的主 WorkSpaces 不可用时将其重定向到其他 Amazon 区域的备用 WorkSpaces。有关更多信息，请参阅 个人版跨区域重定向 WorkSpaces 。

Amazon 的基础设施安全 WorkSpaces

作为一项托管服务，Amazon WorkSpaces 受到Amazon全球网络安全的保护。有关Amazon安全服务以及如何Amazon保护基础设施的信息，请参阅Amazon云安全。要使用基础设施安全的最佳实践来设计您的Amazon环境，请参阅 S Amazonecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用Amazon已发布的 API 调用 WorkSpaces 通过网络进行访问。客户端必须支持以下内容：

- 传输层安全性协议（TLS）。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密（PFS）的密码套件，例如 DHE（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

内容

- 网络隔离
- 物理主机上的隔离
- 企业用户授权
- 创建接口 VPC 端点并进行流式传输
- 通过 VPC WorkSpaces 接口终端节点发出 Amazon API 请求
- 为 Amazon WorkSpaces 创建 VPC 端点策略
- 将您的专用网络连接到 VPC

网络隔离

虚拟私有云（VPC）是 Amazon 云内您自己的逻辑隔离区域中的虚拟网络。您可以在 VPC 的私有子网中部署您的 WorkSpaces。有关更多信息，请参阅 为 WorkSpaces 个人版配置 VPC。

要仅允许来自特定地址范围（例如，来自您的企业网络）的流量，请更新 VPC 的安全组或使用 IP 访问控制组。

您可以使用有效证书将 WorkSpace 访问限制为受信任的设备。有关更多信息，请参阅 将 WorkSpaces 个人版访问限定于受信任设备。

物理主机上的隔离

同一物理主机上的不同 WorkSpace 通过管理程序彼此隔离。这就好像它们位于单独的物理主机上。删除 WorkSpace 后，管理程序会在分配给新 WorkSpace 之前清理分配给它的内存（设置为零）。

企业用户授权

借助 WorkSpaces，可通过 Amazon 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 个人版的目录。

要进一步控制对 WorkSpaces 的访问，请使用多重身份验证。有关更多信息，请参阅如何为 Amazon 服务启用多重身份验证。

创建接口 VPC 端点并进行流式传输

Virtual Private Cloud (VPC) 是 Amazon Web Services Cloud 内您自己的逻辑隔离区域中的虚拟网络。如果您使用 Amazon Virtual Private Cloud 托管Amazon资源，则可以在您的 VPC 和之间建立私有连接 WorkSpaces。您可以使用此连接实现 WorkSpaces 与您的 VPC 上的资源进行通信，而无需通过公共互联网。

接口终端节点由一项技术提供支持 AmazonPrivateLink，该技术允许您使用私有 IP 地址将流式传输流量保持在您指定的 VPC 内。当您将带有 Di Amazon rect Connect 或Amazon虚拟专用网络隧道的 VPC 使用时，您可以将流式传输流量保留在您的网络中。

您可以使用Amazon账户中的 VPC 终端节点来限制您的 Amazon VPC 之间和 WorkSpaces Amazon网络之间的所有流式传输流量。创建终端节点后，请配置您的 WorkSpaces 目录以使用该终端节点。

先决条件和限制

在为设置 VPC 终端节点之前 WorkSpaces，请注意以下先决条件和限制。

- 该功能目前支持 IPv4 或 IPv6 DNS 记录 IP 类型。不支持双堆栈 DNS 记录 IP 类型。
- 您只能配置与您的目录相同Amazon Web Services 账户的 VPC 终端节点。不支持其他Amazon Web Services 账户中的 VPC 终端节点，包括共享终端节点 VPCs。
- 该功能目前仅支持为 VPC 端点配置私有 DNS 名称。VPC 端点的私有 DNS 名称不可公开解析。
- 该功能目前仅适用于 WorkSpaces 个人。 WorkSpaces 池不支持 VPC 终端节点进行流式传输。
- VPC 终端节点功能仅适用于 WorkSpaces 使用 Amazon DCV。当您为目录配置 VPC 端点时，用户无法通过互联网从 Amazon DCV 进行流式传输。但是，在配置 VPC 终端节点期间，您可以为同一目录 WorkSpaces 中的 PCo IP 启用互联网流式传输。
- 要维护 VPC 内的流式传输流量，请使用流式传输 VPC 端点。您的 WorkSpaces 客户需要互联网连接才能进行用户身份验证。在端口 443（包括 UDP 和 TCP）上启用出站访问以处理身份验证流量。此外，您必须根据所选的身份验证方法将所需的域和 IP 地址添加到允许列表中。有关每个类别的域的完整列表，请参阅要添加到允许列表的域和 IP 地址。
  - 验证码
  - 目录设置
  - 会话前智能卡身份验证端点（如果您使用智能卡）
  - 用户登录页面
  - WS 代理
  - WorkSpaces SAML 单点登录 (SSO) 的终端节点
- 用户设备所连接的网络必须能够将流量路由到 VPC 端点。
- 您 Amazon 账户中的 IAM 用户或 IAM 角色必须具有 IAM 权限策略，才能执行 `ec2:DescribeVpcEndpoints` API 操作。
- WorkSpaces 流式传输 VPC 终端节点目前不支持 FIPS 加密。如果您已经为目录启用了 FIPS 加密，则需要在配置 VPC 端点之前禁用 FIPS 加密。
- Amazon通过 VPC 终端节点进行流式传输时，全球加速器 (AGA) 集成不可用。
- 为目录配置 VPC 端点后，为该目录指定的 IP 访问控制组将不再适用。

设置用于 WorkSpaces 流式传输的 VPC 终端节点

要设置用于 WorkSpaces 流式传输的 VPC 终端节点，请完成以下步骤：

步骤 1：创建安全组

在此步骤中，您将创建一个安全组，允许 WorkSpaces 客户端与您将要创建的 VPC 终端节点进行通信。

1. 在 Amazon EC2 控制台的导航窗格中，前往 “网络和安全”，然后转到 “安全组”。
2. 选择创建安全组。
3. 在基本详细信息下，输入以下信息：
   - 对于安全组名称，输入标识安全组的唯一名称。
   - 对于描述，输入一些描述安全组用途的文本。
   - 对于 VPC，选择 VPC 端点所在的 VPC。
4. 转至入站规则并选择添加规则，为 TCP 流量创建入站规则。
5. 输入以下信息：
   - 对于类型，选择“自定义 TCP”。
   - 对于端口范围，输入以下端口号：443、4195。
   - 对于源类型，选择“自定义”。
   - 对于源 — 输入您的用户连接到 VPC 终端节点 IDs 的私有 IP CIDR 范围或其他安全组。确保允许来自 IPv4 或 IPv6 地址源的入站流量。
6. 对每个 CIDR 范围或安全组重复步骤 4 和 5。
7. 转至入站规则，选择添加规则，为 UDP 流量创建入站规则。
8. 输入以下信息：
   - 对于类型，选择自定义 UDP。
   - 对于端口范围，输入以下端口号：443、4195。
   - 对于源类型，选择自定义。
   - 对于来源 — 输入在步骤 5 中 IDs 输入的相同私有 IP CIDR 范围或安全组。确保允许来自 IPv4 或 IPv6 地址源的入站流量。
9. 对每个 CIDR 范围或安全组重复步骤 7 和 8。
10. 选择创建安全组。

步骤 2：创建 VPC 端点

在 Amazon VPC 中，VPC 终端节点允许您将自己的 VPC 连接到支持的Amazon服务。在此示例中，您将配置 Amazon VPC，以便您的 WorkSpaces 用户可以从中进行流式传输 WorkSpaces。

1. 打开 Amazon VPC 控制台。
2. 在导航窗格中，依次选择端点、创建端点。

3. 选择创建端点。
4. 确保进行以下配置：
   - 对于服务类别，确保选中 Amazon 服务。
   - 服务名称 — 选择 com.amazonaws。 ***Region***. Highlander。
   - 对于 VPC，选择要在其中创建接口端点的 VPC。只要网络将流量路由到 VPC 终端节点，您就可以选择与具有 WorkSpaces 资源的 VPC 不同的 VPC。
   - 对于启用私有 DNS 名称，确保选中该复选框。如果您的用户使用网络代理访问流式实例，请禁用与私有端点相关联的域和 DNS 名称上的任何代理缓存。应允许通过代理使用 VPC 端点 DNS 名称。要成功解析 DNS 名称，必须使用 VPC 内的私有 DNS 服务器，这是因为公有 DNS 服务器无法解析 VPC 端点 DNS 名称。
   - DNS 记录 IP 类型-选择 IPv4 或 IPv6。目前不支持双堆栈 DNS 记录 IP 类型。如果您选择 Dualstack，您将无法 WorkSpaces 使用 VPC 终端节点进行流式传输。
   - 对于子网，选择要创建 VPC 端点的子网（可用区）。建议您至少选择两个子网。
   - IP 地址类型 — 根据您选择 IPv4的子网支持的内容选择 IPv6 或 Dualstack。
   - 在安全组面板中，选择以前创建的安全组。
5. （可选）在标签面板中，可以创建一个或多个标签。
6. 选择创建端点。

在端点可供使用时，状态列中的值将变为可用。

步骤 3：配置 WorkSpaces 目录以使用 VPC 终端节点

您需要将 WorkSpaces 目录配置为使用您为流媒体创建的 VPC 终端节点。

1. 在与 VPC 终端节点相同的Amazon区域中打开WorkSpaces 控制台。
2. 在导航窗格中，选择目录，然后
3. 选择您要使用的目录。
4. 转至 VPC 端点部分，然后选择编辑。
5. 在编辑 VPC 端点对话框的流式传输端点下，选择您创建的 VPC 端点。
6. 或者，您可以启用 “允许拥有 PCo IP 的用户从互联网 WorkSpaces 进行直播”。

> **Note**
>
> 启用后，您的用户就可以 WorkSpaces 通过公共互联网从他们 PCo的 IP 进行流式传输。否则，由 WorkSpaces 于 PCo IP 不支持 VPC 终端节点进行流式传输，因此目录中的 PCo IP WorkSpaces 将变得无法访问。

7. 选择保存。

新的流式传输会话的流量都将路由通过此 VPC 端点。但是，当前流式传输会话的流量将继续通过先前指定的端点进行路由。

> **Note**
>
> 指定了 VPC 终端节点后，拥有 DCV 的用户 WorkSpaces 无法使用公共互联网进行直播。

通过 VPC WorkSpaces 接口终端节点发出 Amazon API 请求

您可以通过虚拟私有云 (VPC) 中的接口终端节点直接连接到 Amazon WorkSpaces API 终端节点，而不必通过互联网进行连接。当您使用 VPC 接口终端节点时，您的 VPC 和 Amazon WorkSpaces API 终端节点之间的通信将在Amazon网络内完全安全地进行。

> **Note**
>
> 此功能只能用于连接 WorkSpaces API 端点。要 WorkSpaces 使用 WorkSpaces 客户端进行连接，需要互联网连接，如中所述 WorkSpaces 个人的 IP 地址和端口要求。

亚马逊 WorkSpaces API 终端节点支持由提供支持的亚马逊虚拟私有云（亚马逊 VPC）接口终端节点Amazon PrivateLink。每个 VPC 终端节点都由一个或多个网络接口（也称为弹性网络接口或 ENIs）表示，其私有 IP 地址位于您的 VPC 子网中。

VPC 接口终端节点将您的 VPC 直接连接到 Amazon WorkSpaces API 终端节点，无需互联网网关、NAT 设备、VPN Amazon Direct Connect 连接或连接。您的 VPC 中的实例不需要公有 IP 地址即可与 Amazon WorkSpaces API 终端节点通信。

您可以使用Amazon Web Services 管理控制台或 Amazon Command Line Interface (Amazon CLI) 命令创建连接到 Amazon WorkSpaces 的接口终端节点。有关说明，请参阅创建接口端点。

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 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 端点启用专用 DNS 主机名，您不需要指定端点 URL。CLI 和亚马逊 SD WorkSpaces K 默认使用的亚马逊 WorkSpaces API DNS 主机名 (https://api.workspaces。 *Region*.amazonaws.com) 解析到您的 VPC 终端节点。

Amazon WorkSpaces API 终端节点在同时提供亚马逊 VP C 和亚马逊 WorkSpaces的所有Amazon区域都支持 VPC 终端节点。Amazon WorkSpaces 支持在您的 VPC APIs 内向其所有公共用户发出呼叫。

要了解更多信息Amazon PrivateLink，请参阅Amazon PrivateLink文档。有关 VPC 端点的价格，请参阅 VPC 定价。要了解有关 VPC 和端点的更多信息，请参阅 Amazon VPC。

要查看按地区划分 WorkSpaces 的 Amazon API 终端节点列表，请参阅 WorkSpaces API 终端节点。

为 Amazon WorkSpaces 创建 VPC 端点策略

您可以为 Amazon WorkSpaces 的 Amazon VPC 端点创建一个策略，用于指定以下内容：

- 可执行操作的主体。
- 可执行的操作。
- 可对其执行操作的资源。

有关更多信息，请参阅《Amazon VPC 用户指南》中的使用 VPC 端点控制对服务的访问。

> **Note**
>
> 联邦信息处理标准 (FIPS) Amazon WorkSpaces 端点不支持 VPC 端点策略。

以下示例 VPC 端点策略指定有权访问 VPC 接口端点的所有用户都可以调用名为 `ws-f9abcdefg` 的 Amazon WorkSpaces 托管端点。

```
{
     "Statement": [
         {
             "Action": "workspaces:*",
             "Effect": "Allow",
             "Resource": "arn:aws:workspaces:us-west-2:1234567891011:workspace/ws-
f9abcdefg",
             "Principal": "*"
         }
     ]
}
```

在本例中，拒绝以下操作：

- 调用除 `ws-f9abcdefg` 之外的 Amazon WorkSpaces 托管端点。
- 对指定资源以外的任何资源执行操作（WorkSpace ID：`ws-f9abcdefg`）。

> **Note**
>
> 在本例中，用户仍然可以从 VPC 外部调用其他 Amazon WorkSpaces API 操作。要将 API 调用限制为 VPC 内的资源，请参阅 的身份和访问管理 WorkSpaces，以了解有关使用基于身份的策略控制对 Amazon WorkSpaces API 端点的访问的信息。

将您的专用网络连接到 VPC

要通过您的 VPC 调用 Amazon WorkSpaces API，您必须从位于 VPC 中的实例进行连接，或者使用 Amazon Virtual Private Network (Amazon VPN) 或 Amazon Direct Connect 将您的专用网络连接到 VPC。相关信息，请参阅《Amazon虚拟私有云用户指南》中的 VPN 连接。有关 Amazon Direct Connect 的信息，请参阅《Amazon Direct Connect 用户指南》中的创建连接。

WorkSpaces 中的更新管理

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进行更新，也可以自行更新。有关更多信息，请参阅 WorkSpaces 个人版的维护。

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，也可以遵循应用程序供应商提供的安装更新的建议。

Amazon WorkSpaces 配额

> **Important**
>
> WorkSpaces Pools 功能不在北京和宁夏区域提供。

Amazon WorkSpaces 提供了不同的资源，您可以在给定区域的账户中使用这些资源，包括 WorkSpaces、映像、捆绑包、目录、连接别名和 IP 控制组。在您创建 Amazon Web Services 账户时，我们会根据您创建的资源的数量设置默认配额（也称为限额）。

以下是您的 Amazon 账户的 WorkSpaces 默认配额。您可以使用服务配额控制台查看默认配额和应用的配额，或者请求增加配额来调整配额。

在某些不提供服务配额功能的区域，您必须提交支持案例才能请求提高限额。有关更多信息，请参阅《服务配额用户指南》中的查看服务配额和申请增加配额。

资源	默认值	描述	可调整	使用量
WorkSpaces	1	您可以在当前区域中的此账户中创建的 WorkSpaces 的最大数目。	支持	是
Graphics WorkSpaces	0	当前区域中此账户中 Graphics WorkSpaces 的最大数目。 **Note** 2023 年 11 月 30 日之后，不再支持 Graphics	是	不支持

资源	默认值	描述	可调整	使用量
		捆绑包。建议将您的 WorkSpaces 迁移到 Graphics.g4dn 捆绑包。有关更多信息，请参阅 以 WorkSpaces 个人 WorkSpace 方式迁移。		
GeneralPurpose.4xlarge WorkSpaces	1	当前区域的此账户中 GeneralPurpose.4xlarge WorkSpaces 的最大数目。	支持	是
GeneralPurpose.8xlarge WorkSpaces	1	当前区域的此账户中 GeneralPurpose.8xlarge WorkSpaces 的最大数目。	支持	是
Graphics.g4dn WorkSpaces	0	当前区域中此账户中的 Graphics.g4dn WorkSpaces 的最大数目。	支持	是

资源	默认值	描述	可调整	使用量
GraphicsPro WorkSpaces	0	当前区域中此账户中的 GraphicsPro WorkSpaces 的最大数目。（GraphicsPro 捆绑包的生命周期将于 2025 年 10 月 31 日结束。请考虑使用其他支持的捆绑包来替换。）	支持	是
GraphicsPro.g4dn WorkSpaces	0	当前区域中此账户中的 GraphicsPro.g4dn WorkSpaces 的最大数目。	支持	是
Standby WorkSpaces	5	您可以在当前区域中的此账户中创建的 WorkSpaces 的最大数目。	支持	是
捆绑包	50	当前区域中此账户中的捆绑包的最大数目。此配额仅适用于自定义捆绑包，而不适用于公有捆绑包。	否	是

资源	默认值	描述	可调整	使用量
连接别名	20	当前区域中此账户中的连接别名的最大数目。	否	是
目录	50	当前区域的此账户中，可注册用于 Amazon WorkSpaces 的目录的最大数目。	否	是
图像	40	当前区域中此账户中的映像的最大数目。	支持	是
IP 访问控制组	100	当前区域中此账户中的 IP 访问控制组的最大数目。	否	是
每个目录的 IP 访问控制组数	25	当前区域的此账户中，每个 IP 访问控制组的最大数目。	否	不支持
每个 IP 访问控制组的规则数	10	当前区域的此账户中，每个 IP 访问控制组的最大规则数。	否	不支持
WorkSpaces Pools	10	在当前区域的此账户中创建的 WorkSpaces Pools 的最大数目。	支持	是

资源	默认值	描述	可调整	使用量
WorkSpaces Pools 的通用 Value 流式传输实例	10	可在当前区域内此账户中用于 WorkSpaces Pools 的通用 Value 流式传输实例的最大数量。	支持	是
WorkSpaces Pools 的通用 Standard 流式传输实例	10	可在当前区域内此账户中用于 WorkSpaces Pools 的通用 Standard 实例的最大数量。	支持	是
WorkSpaces Pools 的通用 Performance 流式传输实例	10	可在当前区域内此账户中用于 WorkSpaces Pools 的通用 Performance 流式传输实例的最大数量。	支持	是
用于 WorkSpaces 虚拟桌面池的通用 Power 流式传输实例	10	可在当前区域内此账户中用于 WorkSpaces Pools 的通用 Power 流式传输实例的最大数量。	支持	是

资源	默认值	描述	可调整	使用量
用于 WorkSpaces 虚拟桌面池的通用 PowerPro 流式传输实例	10	可在当前区域内此账户中用于 WorkSpaces Pools 的通用 PowerPro 流式传输实例的最大数量。	支持	是
用于 WorkSpaces Pools 的 Graphics g4dn xlarge 流式传输实例	0	可在当前区域内此账户中用于 WorkSpaces Pools 的 Graphics.g4dn xlarge 流式传输实例的最大数量。	支持	是
用于 WorkSpaces Pools 的 Graphics g4dn 4xlarge 流式传输实例	0	可在当前区域内此账户中用于 WorkSpaces Pools 的 Graphics.g4dn 4xlarge 流式传输实例的最大数量。	支持	是
WorkSpaces Core 托管实例	1000	当前区域的此账户中 WorkSpaces 托管实例的最大数目。	是	不支持

资源	默认值	描述	可调整	使用量
处于分配状态的并发 WorkSpaces 托管实例	700	当前区域的此账户中，处于分配状态的并发 WorkSpaces 托管实例的最大数目。	是	不支持

API 节流

允许的速率为每秒两次调用。有关更多信息，请参阅节流列外。

WorkSpaces 客户端应用程序的生命周期终止政策

Amazon 生命周期 WorkSpaces 终止 (EOL) 政策适用于 WorkSpaces 个人版和 WorkSpaces 矿池版 WorkSpaces 客户端的特定主要版本（及其所有次要版本）。

WorkSpaces 客户端版本的生命周期分为三个阶段：一般支持、技术指导和生命周期结束 (EOL)。一般支持阶段从 WorkSpaces 客户首次公开发布之日开始，持续一段固定的期限。在一般支持阶段， WorkSpaces 支持团队为配置问题提供全面支持。缺陷解决方案和功能请求是针对该主要版本和 WorkSpaces 客户端的关联次要版本实现的。

从一般支持阶段结束到生命周期终止日期，均提供技术指导。在技术指导阶段，您只能获得有关受支持配置的支持和指导。缺陷解决方案和功能请求仅适用于最新版本的 WorkSpaces 客户端。不会为旧版本实施缺陷解决方案和特征请求。在技术指导阶段，如果需要修复， Amazon 将安排在即将发布的公开发行版本中进行修复，并且您可以选择升级到最新 WorkSpaces 版本以获得与修复相关的支持。

当一般支持和技术指导阶段都已结束时，主要版本的生命周期将终止。在停产日期之后，不再提供进一步的支持或维护。 Amazon 停止测试兼容性问题。要获得持续支持，您必须升级到最新的 WorkSpaces 客户端版本。

有关特定版本支持的更多信息，请参阅此表。

> **Important**
>
> 以下客户端版本已于 2025 年 11 月 15 日到期 (EOL)。请务必在 2026 年 2 月 28 日之前升级到支持的客户端版本，以免服务中断。
>
> - 用于 Ubuntu 22.04 的 Linux 2024.6-2024.8
> - 用于 Ubuntu 20.04 的 Linux 2024.6-2024.8

Windows 客户端	一般支持	技术指导	EOL	注意
5.22.1+	2024 年 9 月 3 日			支持

Linux 客户端	一般支持	技术指导	EOL	注意
适用于 Ubuntu 的 2025.1+ 24.04	2025 年 12 月 12 日			支持
用于 Ubuntu 22.04 的 2025.0+	2025 年 5 月 28 日			支持
用于 Ubuntu 20.04 的 2025.0+	2025 年 5 月 28 日			支持
用于 Ubuntu 22.04 的 2024.6-2024.8	2024 年 9 月 6 日	2025 年 8 月 29 日	2025 年 11 月 15 日	请务必在 2026 年 2 月 28 日之前升级到最新的客户端版本。
用于 Ubuntu 20.04 的 2024.6-2024.8	2024 年 9 月 6 日	2025 年 8 月 29 日	2025 年 11 月 15 日	请务必在 2026 年 2 月 28 日之前升级到最新的客户端版本。

macOS 客户端	一般支持	技术指导	EOL	注意
5.22.1+	2024 年 9 月 3 日			支持

iPad 客户端	一般支持	技术指导	EOL	注意
2.x	2019			支持

Android 客户端	一般支持	技术指导	EOL	注意
5.0.1+	2024 年 11 月 6 日			支持

Web 访问	一般支持
Google Chrome	当前版本以及两个最新的主要版本
Mozilla Firefox	当前版本以及两个最新的主要版本
Microsoft Edge	当前版本以及两个最新的主要版本

不受支持的客户端版本

不支持以下 WorkSpaces 客户端。

操作系统	客户端版本	一般支持	技术指导	EOL	注意
Windows	5.0-5.22.0	2022 年 6 月 2 日	2024 年 11 月 21 日	2025 年 3 月 31 日	不支持
Windows	5.11	2023 年 7 月 3 日	2023 年 10 月 1 日	2023 年 10 月 1 日	不支持
Windows	5.10	2023 年 6 月 19 日	2023 年 10 月 1 日	2023 年 10 月 1 日	不支持
Windows	5.9	2023 年 5 月 9 日	2023 年 10 月 1 日	2023 年 10 月 1 日	不支持
Windows	4.x	2021 年 6 月 30 日	2024 年 11 月 21 日	2025 年 3 月 31 日	不支持
Windows	3.x	2019 年 11 月 25 日	2024 年 11 月 21 日	2025 年 3 月 31 日	不支持
Windows	2.x	2018	2023 年 3 月 31 日	2023 年 8 月 31 日	不支持
Ubuntu	用于 Ubuntu 22.04 的	2024 年 9 月 6 日	2025 年 8 月 29 日	2025 年 11 月 15 日	不支持

操作系统	客户端版本	一般支持	技术指导	EOL	注意
	2024.6-2024.8				
Ubuntu	用于 Ubuntu 20.04 的 2024.6-2024.8	2024 年 9 月 6 日	2025 年 8 月 29 日	2025 年 11 月 15 日	不支持
Ubuntu	用于 Ubuntu 22.04 的 2024.0-2024.5	2024 年 2 月 28 日	2024 年 11 月 21 日	2025 年 3 月 31 日	不支持
Ubuntu	用于 Ubuntu 20.04 的 2024.0-2024.5	2023 年 8 月 24 日	2024 年 11 月 21 日	2025 年 3 月 31 日	不支持
Ubuntu	适用于 Ubuntu 的 2023.x 22.04	2023 年 8 月 24 日	2024 年 11 月 21 日	2025 年 3 月 31 日	不支持
Ubuntu	适用于 Ubuntu 的 2023.x 20.04	2023 年 8 月 24 日	2024 年 11 月 21 日	2025 年 3 月 31 日	不支持
Ubuntu	适用于 Ubuntu 的 4.x 20.04	2022 年 10 月 27 日	2024 年 11 月 21 日	2025 年 3 月 31 日	不支持
Ubuntu	4.x for Ubuntu 18.04	2021 年 8 月 12 日	2023 年 3 月 31 日	2023 年 8 月 31 日	不支持
Ubuntu	3.x for Ubuntu 18.04	2019 年 11 月 25 日	2023 年 3 月 31 日	2023 年 8 月 31 日	不支持

操作系统	客户端版本	一般支持	技术指导	EOL	注意
macOS	5.1-5.22.0	2022 年 6 月 30 日	2024 年 11 月 21 日	2025 年 3 月 31 日	不支持
macOS	4.x	2021 年 8 月 5 日	2024 年 11 月 21 日	2025 年 3 月 31 日	不支持
macOS	3.x	2019 年 11 月 25 日	2024 年 11 月 21 日	2025 年 3 月 31 日	不支持
macOS	2.x	2019	2023 年 3 月 31 日	2023 年 8 月 31 日	不支持
macOS	1.x	2018	2023 年 3 月 31 日	2023 年 8 月 31 日	不支持
iPad	1.x	2018	2023 年 3 月 31 日	2023 年 8 月 31 日	不支持
Android	5.0.0	2024 年 2 月 26 日	2024 年 11 月 21 日	2025 年 3 月 31 日	不支持
Android	4.x	2022 年 5 月 12 日	2024 年 11 月 21 日	2025 年 3 月 31 日	不支持
Android	3.x	2021 年 6 月 30 日	2024 年 11 月 21 日	2025 年 3 月 31 日	不支持
Android	2.x	2019	2023 年 3 月 31 日	2023 年 8 月 31 日	不支持
Android	1.x	2018	2023 年 3 月 31 日	2023 年 8 月 31 日	不支持

EOL FAQs

我使用的 WorkSpaces 客户端版本已达到 EOL。我应该怎么做才能升级到受支持的版本？

前往WorkSpaces 客户端下载页面，下载并安装完全支持的版本 WorkSpaces。

我能否使用已达到 EOL 且支持 WorkSpace版本的 WorkSpaces 客户端？

强烈建议将客户端升级到最新版本，因为之前的解决方案和功能不再适用于已到达生命周期终止日期的客户端版本。如果您使用的客户端版本已到期，请联系 Amazon 支持团队以获取更多信息。

我使用的 WorkSpaces 客户端版本已达到 EOL。我还能报告相关问题吗？

您必须先升级到受支持的版本，然后尝试重现该问题。如果问题在受支持的版本中仍然存在，请向 Amazon 支持团队提交支持案例。

我在已达到 EOL 的操作系统上使用支持的 WorkSpaces 客户端版本。我还能报告相关问题吗？

对于已达到 EOL 的操作系统，将不再提供技术援助和软件更新， Amazon 也不为使用已停产操作系统的 WorkSpaces 客户提供支持。使用支持的操作系统来确保为 WorkSpaces 客户提供支持。

DCV 支持的 SDK 扩展

DCV 支持针对各种工作负载和使用案例实现 WorkSpaces 实例的高性能远程访问。借助 Amazon DCV Extension SDK，开发人员可以为最终用户自定义 DCV WorkSpaces 体验，包括：

- 为自定义硬件支持提供便利。
- 提高第三方应用程序在远程会话中的可用性。例如，为 VoIP 应用程序添加本地音频终端，或为会议应用程序添加本地视频播放
- 为屏幕阅读器等辅助功能软件提供有关远程会话和远程运行的应用程序的信息。
- 允许安全软件分析本地端点的安全状况，以允许有条件的访问策略。
- 通过已建立的远程会话执行任意数据传输。

要开始使用 Amazon DCV Extension SDK，请参阅 Amazon DCV Extension SDK 文档。您可以在 Amazon DCV Extension SDK GitHub 存储库中找到该 SDK 本身。此外，可在 Amazon DCV Extension SDK 示例 GitHub 存储库中找到该 SDK 的集成示例。

WorkSpaces 支持以下内容。

- 流式传输协议 - DCV
- WorkSpaces Windows 客户端 - Windows：5.9.0.4110 及更高版本。

> **Note**
>
> WorkSpaces Android、iOS 客户端、Web Access 不支持 DCV Extension SDK。

- 支持的 WorkSpaces - Windows、Linux 和 Ubuntu 服务器

的文档历史记录 WorkSpaces

下表描述了自 2018 年 1 月 1 日起对该 WorkSpaces 服务和《亚马逊 WorkSpaces 管理指南》所做的重要更改。我们还经常更新文档来处理发送给我们的反馈意见。

要获得有关这些更新的通知，您可以订阅 WorkSpaces RSS feed。

变更	说明	日期
DCV 的 USB 重定向	您可以为基于 DCV 的 Windows 配置 USB 重定向 WorkSpaces ，以允许用户在其虚拟桌面环境中访问本地 USB 设备。	2025 年 10 月 28 日
增加了对配置网络摄像头分辨率的支持	使用 DCV WorkSpaces 时，你可以在 Windows 上配置网络摄像头分辨率。	2025 年 10 月 21 日
增加了对配置服务器键盘布局的支持	现在， WorkSpaces 在使用 DCV 时，除了默认的客户端布局外，您还可以将 Windows 配置为使用服务器端键盘布局。	2025 年 10 月 21 日
为 IPv6 网络添加了 Support	Amazon WorkSpaces 支持 IPv4 IPv6 使用 VPC 终端节点进行 WorkSpaces 直播。	2025 年 10 月 21 日
运行模式	矿 WorkSpaces 池的运行模式决定了其即时可用性以及您的付款方式。创建 WorkSpaces 池时，可以在两种运行模式之间进行选择。	2025 年 5 月 15 日
Microsoft Entra ID 目录	支持 IAM 身份中心和 WorkSpaces 之间的跨区域集成。	2025 年 2 月 27 日

Microsoft Entra ID 目录	您可以创建一个专用 Microsoft Entra ID 目录。	2024 年 8 月 26 日
Microsoft Visual Studio	管理应用程序支持 Microsoft Visual Studio 捆绑包。	2024 年 8 月 1 日
Amazon DCV WebRTC 重定向扩展	您可以安装 Amazon DCV WebRTC 重定向扩展以使用 WebRTC 重定向。	2024 年 8 月 1 日
WorkSpaces 泳池现已在 Amazon GovCloud (US) Region	WorkSpaces Pools 提供非永久性虚拟桌面，专为需要按需访问临时基础架构上托管的精心策划的桌面环境的用户量身定制。	2024 年 7 月 23 日
WorkSpaces 泳池现已可用	WorkSpaces Pools 提供非永久性虚拟桌面，专为需要按需访问临时基础架构上托管的精心策划的桌面环境的用户量身定制。	2024 年 6 月 27 日
AmazonWorkSpacesAdmin 托管策略更新和新的 AmazonWorkSpacesPoolServiceAccess托管策略	WorkSpaces 更新了 AmazonWorkSpacesAdmin 托管策略并添加了新的 AmazonWorkSpacesPoolServiceAccess 托管策略。	2024 年 6 月 27 日
AmazonWorkSpacesAdmin 托管策略更新	WorkSpaces 在 AmazonWorkSpacesAdmin托管策略中添加了 workspaces: actiRestoreWorkspace on，授予管理员恢复权限。 WorkSpaces	2023 年 7 月 17 日

DCV 支持的 SDK 扩展	借助 Amazon DCV 扩展软件开发工具包，开发人员可以为最终用户自定义 DCV WorkSpaces 体验。	2023 年 5 月 25 日
DCV 主机代理版本	DCV 的版本信息。	2023 年 5 月 8 日
亚马逊在 AmazonGovCloud（美国东部）WorkSpaces 推出	亚马逊 WorkSpaces 在 AmazonGovCloud（美国东部）有售。	2023 年 5 月 3 日
Amazon WorkSpaces 网络摄像头支持	亚马逊 WorkSpaces 现在通过使用 DCV 将本地网络摄像头视频输入无缝重定向到 Windows WorkSpaces 桌面，从而支持实时音频-视频 (AV)。	2021 年 4 月 5 日
m WorkSpaces acOS 客户端应用程序支持亚马逊 WorkSpaces 智能卡	现在，您可以使用带有通用访问卡 (CAC) 和个人身份验证 (PIV) 智能卡的 Amazon WorkSpaces macOS 客户端应用程序。 WorkSpaces 使用 DCV 时支持智能卡。	2021 年 4 月 5 日
亚马逊 WorkSpaces 捆绑包管理 APIs	Amazon WorkSpaces 捆绑包管理 APIs 现已推出。这些 API 操作支持分发 WorkSpaces 包的创建、删除和图像关联操作。	2021 年 3 月 15 日
亚马逊在亚太地区（孟买）上 WorkSpaces 市	WorkSpaces Amazon 已在亚太地区（孟买）地区上市。	2021 年 3 月 8 日

智能卡	亚马逊 WorkSpaces 现在支持在（美国西部）地区的 Windows 和 Linux 上进行会话前 AmazonGovCloud （登录）和会话 WorkSpaces 中的智能卡身份验证。	2020 年 12 月 1 日
DCV	DCV 现在适用于包含许可证（Windows Server 2016）和 BYOL Windows 10，适用于除图形和之外的所有 WorkSpaces 捆绑包类型。GraphicsProDCV 还可用于 AmazonGovCloud （美国西部） WorkSpaces 地区的 Linux。	2020 年 12 月 1 日
共享自定义映像	现在，您可以跨Amazon账户共享自定义 WorkSpaces 镜像。共享图像后，收件人账户可以复制该图像并使用它来创建用于发布新 WorkSpaces图像的捆绑包。	2020 年 10 月 1 日
跨区域重定向	现在，您可以使用跨区域重定向，该功能可与您的域名系统 (DNS) 路由策略配合使用，在主域名系统 (DNS) 路由策略 WorkSpaces 不可用 WorkSpaces 时，将您的用户重定向到替代方案。	2020 年 9 月 10 日
订阅微软 Office 2016 或 2019 版 BYOL WorkSpaces	你现在可以订阅 Bring Your Own Windows 许可证 (BYOL) Amazon WorkSpaces 上提供的微软 Office Professional 2016 或 2019。	2020 年 9 月 3 日

BYOL Automation 在中国（宁夏）地区推出	你可以使用自带许可 (BYOL) 自动化来简化 WorkSpaces 在中国（宁夏）使用 Windows 10 桌面许可证的流程。	2020 年 4 月 2 日
映像检查程序	图像检查器工具可以帮助你确定你的 Windows 是否 WorkSpace 满足图像创建的要求。Image Checker 会对要 WorkSpace 用来创建图像的进行一系列测试，并就如何解决发现的任何问题提供指导。	2020 年 3 月 30 日
迁移 WorkSpaces	Amazon m WorkSpaces igrate 功能使您能够将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。WorkSpace 你可以使用此功能 WorkSpaces 从 Windows 7 桌面体验迁移到 Windows 10 桌面体验。您也可以使用此功能 WorkSpaces 从一个公共或自定义捆绑包迁移到另一个捆绑包。	2020 年 1 月 9 日
PrivateLink 亚马逊集成 WorkSpaces APIs	您可以通过虚拟私有云 (VPC) 中的接口终端节点直接连接到 Amazon WorkSpaces API 终端节点，而不必通过互联网进行连接。当您使用 VPC 接口终端节点时，您的 VPC 和 Amazon WorkSpaces API 终端节点之间的通信将在Amazon 网络内完全安全地进行。	2019 年 11 月 25 日
适用于亚马逊的 Linux 客户端 WorkSpaces	用户现在可以使用 Linux 客户端访问他们 WorkSpaces的。	2019 年 11 月 25 日

亚马逊在中国（宁夏）上 WorkSpaces 线	WorkSpaces Amazon 在中国（宁夏）区域上市。	2019 年 11 月 13 日
恢复 WorkSpaces 到上次已知的健康状态	您可以使用还原功能将 a 还原 WorkSpace 到其上次已知的正常状态。	2019 年 9 月 18 日
FIPS 端点加密	为了遵守联邦风险和授权管理计划 (FedRAMP) 或国防部 (DoD) 云计算安全要求指南 (SRG)，您可以将 WorkSpace s 亚马逊配置为在目录级别使用联邦信息处理标准 (FIPS) 端点加密。	2019 年 9 月 12 日
复制 WorkSpace 图像	您可以在同一区域内或跨区域复制映像。	2019 年 6 月 27 日
为用户提供自助服务 WorkSpace 管理功能	您可以为用户启用自助服务 WorkSpace 管理功能，让他们能够更好地控制自己的体验。	2018 年 11 月 19 日
BYOL Automation	你可以使用自带许可证 (BYOL) 自动化来简化使用你的 Windows 7 和 Windows 10 桌面许可证的过程。 WorkSpace s	2018 年 11 月 16 日
PowerPro 和 GraphicsPro 捆绑包	PowerPro 和 GraphicsPro 捆绑包现已推出。 WorkSpaces	2018 年 10 月 18 日
监控成功 WorkSpace 登录	您可以使用 Amazon Events 中的 CloudWatch 事件来监控和响应成功 WorkSpace 登录。	2018 年 9 月 17 日
URI 登录	您可以使用统一资源标识符 (URIs) 为用户提供对其的访问权限 WorkSpaces。	2018 年 7 月 31 日

Amazon Linux WorkSpaces	您可以为用户配置 Amazon WorkSpaces Linux。	2018 年 6 月 26 日
IP 访问控制组	您可以控制用户可以访问他们的 IP 地址 WorkSpaces。	2018 年 4 月 30 日
就地升级	你可以将 Windows 10 BYOL 升级 WorkSpaces 到较新版本的 Windows 10。	2018 年 3 月 9 日

早期更新

下表描述了 2018 年 1 月 1 日之前对 Amazon WorkSpaces 服务及其文档集的重要补充。

更改	描述	日期
灵活的计算选项	您可以在 “超值”、“标准”、“性能” 和 “功率” 套装 WorkSpaces 之间切换	2017 年 12 月 22 日
可配置存储	您可以在启动根卷和用户卷 WorkSpaces 时为其配置大小，稍后再增加这些卷的大小。	2017 年 12 月 22 日
控制设备访问	您可以指定有权访问的设备类型 WorkSpaces。此外，您可以限制对可信设备（也称为受管设备）的访问。 WorkSpaces	2017 年 6 月 19 日
林间信任	你可以在你的Amazon托管 Microsoft AD 和你的本地 Microsoft Active Directory 域之间建立信任关系，然后 WorkSpaces为本地域中的用户进行配置。	2017 年 2 月 9 日
Windows Server 2016 捆绑包	WorkSpaces 提供的捆绑包包括 Windows 10 桌面体验，由 Windows Server 2016 提供支持。	2016 年 11 月 29 日
每小时 WorkSpaces	您可以将您的 WorkSpaces 配置为按小时向用户计费。	2016 年 8 月 18 日

更改	描述	日期
Windows 10 BYOL	你可以将你的 Windows 10 桌面许可证带到 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 WorkSpaces.	2016 年 5 月 17 日
已保存的注册	每次您输入新的注册码时， WorkSpaces 客户端都会将其存储。这使得 WorkSpaces 在不同的目录或区域之间切换变得更加容易。	2016 年 1 月 28 日
Windows 7 BYOL、WorkSpace	你可以将你的 Windows 7 桌面许可证带到 WorkSpaces (BYOL)然后使用加密。WorkSpace	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的 auto 会话重新连接功能的信息。	2015 年 3 月 31 日
公有 IP 地址	您可以自动为您分配公有 IP 地址 WorkSpaces。	2015 年 1 月 23 日
WorkSpaces 在亚太地区（新加坡）推出	WorkSpaces 已在亚太地区（新加坡）区域推出。	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	您可以根据已自定义的图像创建映像 WorkSpace ，也可以使用该图像创建自定义 WorkSpace 捆绑包。	2014 年 10 月 28 日
PCoIP 零客户端支持	您可以访问 WorkSpaces PCo IP 零客户端设备。	2014 年 10 月 15 日

更改	描述	日期
WorkSpaces 在亚太地区（东京）推出	WorkSpaces 已在亚太地区（东京）区域推出。	2014 年 8 月 26 日
本地打印机支持	您可以为自己启用本地打印机支持 WorkSpaces。	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	您可以选择存放 WorkSpace 计算机帐户的默认组织单位 (OU)，以及创建 WorkSpace 计算机帐户的单独域。	2014 年 7 月 7 日
添加安全组	您可以将安全组添加到您的 WorkSpaces。	2014 年 7 月 7 日
WorkSpaces 在亚太地区（悉尼）推出	WorkSpaces 已在亚太地区（悉尼）区域推出。	2014 年 5 月 15 日
WorkSpaces 在欧洲（爱尔兰）推出	WorkSpaces 已在欧洲（爱尔兰）地区上市。	2014 年 5 月 5 日
公开测试版	WorkSpaces 已作为公开测试版提供。	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。